



Four-Door & Four-Lift Controller Programming Manual

Copyright	© 2013 UTC Fire & Security Australia Pty Ltd. All rights reserved.
Trademarks and patents	The Challenger name and logo are trademarks of UTC Fire & 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	UTC Fire & Security Australia Pty Ltd t/a Interlogix A UTC Building & Industrial Systems company Level 1, 271–273 Wellington Road, Mulgrave, VIC, 3170, Australia
ACMA compliance	 N4131 Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
Contact information	For contact information, see www.interlogix.com.au .

Content

Important information	iii
Limitation of liability	iii
Agency compliance	iii
Product overview	1
About this manual	2
Related documentation	2
Recommended programming sequence	3
Programming via a RAS	3
Challenger10 input and relay numbering	3
Setting up a controller	4
Time zones	4
Setting up doors or lifts	5
Setting up advanced functionality	5
Command reference	7
DGP menu	7
Option 1 – Controller options	8
Option 2 – Door/lift options	14
Door/lift access options	14
Door/lift egress options	20
Door/lift alarm control options	21
Door/lift reader options	23
Door/lift hardware options	27
Lift options	30
Option 3 – Initialize database	32
Option 4 – Display card	33
Option 5 – Door groups	34
Option 6 – Lift groups	35
Option 7 – System options	35
Option 8 – Macro logic	36
Option 9 – Version number	38
Option 10 – Remote controllers	39
Option 11 – Display IUM user	39
Appendix A. Reference materials	40
Using time and attendance readers	40
Using pulsed lock and unlock relays	41
Using regions	43
Input and relay numbering	43
Door/lift hardware defaults	44
Macro event flags	49
Programming map	54

Appendix B. Programming worksheets 58

Introduction 58

Controller and system options worksheet 58

Door/lift access options worksheet 59

Door/lift egress options worksheet 60

Door/lift alarm control options worksheet 60

Door/lift reader options worksheet 61

Door/lift hardware options worksheet 62

Lift options worksheet 64

DGP macro logic worksheet 65

Glossary 67

Index 71

Important information

Limitation of liability

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

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

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

Agency compliance

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

Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Product overview

This manual applies to models TS0866 Four-Door Controller, TS0867 Four-Door Controller, and TS0869 Four-Lift Controller. These devices are also known as Intelligent Access Controllers, controllers, or DGPs.

The above models were originally designed to be used with Challenger V8 panels. The following firmware versions (or later) allow the controllers to be used with Challenger10 panels:

- Four-Door Controller firmware version R-110613.801
- Four-Lift Controller firmware version L-110613.803

Challenger V8 panels can have 12 Intelligent Access Controllers on its RS-485 LAN. Challenger10 panels have two RS-485 LANs, and can have 24 Intelligent Access Controllers. In each case, Intelligent Access Controllers can occupy the first 12 DGP addresses on the LAN.

Challenger V8 panels can be configured with various memory sizes and can use Intelligent User Memory (IUM) or be non-IUM. Challenger10 panels are native IUM, and can have 2,000 users (standard) and can be expanded to 65,535 users. An Intelligent Access Controller without memory expansion can have:

- 2,000 IUM users when connected to a Challenger10 panel or to a Challenger V8 panel in IUM mode.
- 11,466 non-IUM users when connected to a non-IUM Challenger V8 panel.

A Challenger10 panel can have various end-of-line (EOL) resistor values for input tamper monitoring (default is 10 k Ω). Intelligent Access Controllers use only 10 k Ω EOL resistors to detect the state of alarm input circuits.

Intelligent Access Controllers have a local RS-485 LAN to connect readers (for doors or lifts). Four-Lift Controllers can also have up to 15 DGPs on its local LAN, with each DGP providing up to 16 inputs (typically for floor-buttons).

Intelligent Access Controllers provide enhanced access control functionality to the Challenger system. This manual contains:

- Recommended programming sequence
- Programming via a remote arming station (RAS)
- Command reference
- Reference materials
- Programming worksheets

This manual is intended for use only by trained Challenger installation and configuration technicians.

About this manual

This manual is based on the programming options as displayed on an LCD RAS. Options listed as YES or NO on the RAS correspond with enabled or disabled selected or deselected in the management software user interface. In some cases the NO option is omitted where it is obviously the opposite of the YES option (for example, a RAS either has an LCD or it doesn't).

Unless otherwise specified, it is assumed that the use of a card or a PIN (personal identification number) always mean a valid card or a valid PIN.

The term “*Challenger Programming Manual*” should be taken to mean either the *Challenger10 Programming Manual* or the *Challenger V8 & V9 Programming Manual*, as applicable.

Related documentation

The *Challenger Programming Manual* provides detailed information about Challenger system configuration and programming.

The Challenger system is modular. Refer also to the documentation that is shipped with each module that you intend to use.

Recommended programming sequence

The following sections are provided as overview of common programming tasks. Refer to “Command reference” on page 7 for specific details.

Perform the following tasks to enable the system to read cards and to unlock doors.

Programming via a RAS

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

Example of text displayed on an LCD RAS:

```
Remote Type: 1-DGP, 2-RAS  
Device:
```

To make a selection, you would press the corresponding number on the keypad (for example 1), and then press the [ENTER] key. This sequence is indicated in this manual as “Enter 1”.

Yes/No options typically show the current state. Press the [ENTER] key to accept the current state.

If you are programming a controller via a RAS, it is assumed that you have the necessary permissions and knowledge to access and use the Challenger system’s Install menu (option 19 of the User menu).

Refer to the *Challenger Programming Manual* for detailed information.

Challenger10 input and relay numbering

A controller’s input and relay numbers depend on whether the controller is connected to a Challenger10 panel or a Challenger V8 panel:

- When connected to a Challenger10 panel the controller’s input and relay numbering is relative to the controller regardless of the DGP address. Input and relay numbers start at 1 regardless of the address.
- When connected to a Challenger V8 panel the controller’s input and relay numbering depends on the DGP address. For example, a controller addressed as DGP 1 has input and relay numbers starting at 17.

Unless otherwise noted, input and relay number examples assume that the controller is connected to a Challenger10 panel. See “Input and relay numbering” on page 43 for details.

Setting up a controller

Perform the following tasks for each Intelligent Controller.

1. Set the Intelligent Controller's DIP switches to program the DGP address in the range 1 to 12.
Note: On a Challenger10 LAN2, DIP switch addresses 1 to 12 are used for Intelligent Controllers that are polled as 17 to 28. See Table 5 on page 44.
2. Ensure that the memory module used in the Intelligent Controller matches the Challenger panel.
3. Program and set the RAS or DGP addresses connected to the Intelligent Controller's local LAN. Refer to Table 1 on page 10 for details of addressing IN and OUT readers.
4. In the Challenger Install menu programming:
 - Activate polling (option 4 – DGP) for the Intelligent Controller and set the DGP type.
 - Check and note (option 7 – System Options) the settings for Input Tamper Monitoring and Alarm Prefix Length.
 - Program time zones required for access control functions (egress, override time zone, and door groups).
Note: On a Challenger10 system either hard or soft time zones may be used. On a Challenger V8 system only hard time zones may be used.
 - Determine which areas (option 2 – Area Database) will inhibit Egress or will inhibit access through a door when the areas are armed.
5. Go to option 28 – Remote Controllers, select type 1 (DGP) and press [ENTER]. Enter the DGP address and press [ENTER]. You are now in the Intelligent Controller programming menu.
6. In the Intelligent Controller programming menu select option 1 – Controller options. Program or select the items described in “Option 1 – Controller options” on page 8 (as applicable).

Time zones

Time zones can be used for:

- Door groups and floor groups
- Low security time zone (in door/lift access options)
- Egress time zone (in door/lift egress options)
- Override time zone (in door/lift reader options)

The time zones that an Intelligent Access Controller can use depend on the Challenger panel version:

- In a Challenger10 system, hard or soft time zones 1 to 63 may be used.

- In a Challenger V8 system with firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules, hard time zones 1 to 24 and 42 to 63 may be used.
- In other Challenger systems hard time zones 1 to 24 may be used.

Setting up doors or lifts

Perform the following tasks for each of the Intelligent Controller's doors or lifts.

1. In the Intelligent Controller programming menu select option 2 – Door/lift options, and then select the number of the door or lift you wish to program.
2. Select option 1 – Access Options, and then program or select the items described in “Door/lift access options” on page 14 (as applicable).
3. If egress functionality is needed, select option 2 Egress Options, and then program or select the items described in “Door/lift egress options” on page 20 (as applicable).
4. Select option 4 – Reader Options, and then program or select the items described in “Door/lift reader options” on page 23 (as applicable).
5. Select option 5 – Hardware Options, and then program or select the items described in “Door/lift hardware options” on page 27 (as applicable).
6. If programming a Four-Lift Controller, select option 6 – Lift Options, and then program or select the items described in “Lift options” on page 30 (as applicable).
7. When out of the Hardware options (or Lift Options, if used), press 0 [ENTER] to exit the sub-menu again to exit the Door selection menu. Press 0 [ENTER] again to exit the Intelligent Controller programming menu.
8. Set up the required door groups in the Challenger user program (menu 20).
9. Program users that require access control on the Intelligent Controller (menu 14).
10. Program inputs available on the Intelligent Controller (Install menu 1 Input).

Setting up advanced functionality

The advanced set up adds alarm control and anti-passback to the basic set up performed above.

Adding alarm control functions

To enable alarm control:

1. In the Challenger Install menu:
 - Program time zones required for alarm control functions (used in alarm groups).
 - Program alarm groups (if required) for access control functions.

2. In the Intelligent Controller programming menu, select option 2 – Door/lift options, and then select the number of the door or lift you wish to program.
3. Select option 3 – Alarm Control, and then program or select the applicable items described in “Door/lift alarm control options” on page 21.
4. Assign an alarm group to users that should have alarm control on the Intelligent Controller (User Menu 14 – Program Users).

Adding anti-passback facilities

Anti-passback controls how the system responds when a user attempts to enter a region twice in succession (without leaving the region, or within the anti-passback time), as if they passed their card back to the outside for someone else to use.

For anti-passback to function, readers are required to enter and exit. The reader address specifies if the reader is used as an IN (entry) or OUT (exit) reader (see Table 1 on page 10).

To enable anti-passback:

1. Make sure both IN and OUT readers are available and are polled.
2. In the Intelligent Controller programming menu, select option 2 – Door/Lift Options and then select the number of the door or lift you wish to program.
3. Select option 1 – Access Options, and then program or select the following items described in “Door/lift access options” on page 14.
 - Select the required settings for IN reader inhibit region 0 user and/or OUT reader inhibit region 0 user.
 - Select the required anti-passback option.
 - Enter the IN reader region and OUT reader region.

Command reference

Before being granted access to the door/lift programming menu the Intelligent Controller must be correctly:

- Connected
- Addressed
- Programmed to be polled
- The DGP type must be programmed as a Door Controller or a Lift Controller in the Challenger Install menu option 4, “DGP Database”.

The controller is programmed from Install menu option 28, “Remote Controllers”.

```
Remote Type: 1-DGP, 2-RAS
Device:
```

Enter 1 to access the controller programming menu.

```
Remote DGP Setup
DGP No:
```

Enter the DGP address in the range 1 to 12 (and 17 to 28 for Challenger10) to program the controller options.

DGP menu

```
"#"-Move On  "*" -Move Back
Menu:
```

The DGP menu contains the options described on the following pages. Enter one of the following option numbers to access the option.

- “Option 1 – Controller options” is described on page 8
- “Option 2 – Door/lift options” is described on page 14
- “Option 3 – Initialize database” is described on page 32
- “Option 4 – Display card” is described on page 33
- “Option 5 – Door groups” is described on page 34
- “Option 6 – Lift groups” is described on page 35
- “Option 7 – System options” is described on page 35
- “Option 8 – Macro logic” is described on page 36
- “Option 9 – Version number” is described on page 38
- “Option 10 – Remote controllers” is described on page 39
- “Option 11 – Display IUM user” is described on page 39

Note: In the following sections, the characters “XX” represent the number of the selected device.

Option 1 – Controller options

At the DGP menu (“DGP menu” on page 7) enter 1 to access the Controller options programming screens.

The first programming screen is for relay controllers.

Relay controllers

```
XX, Relay Controllers 0
*-Dis, Ctrl:
```

Enter a value in the range 1 to 8 in order to use TS0841 or TS0842 clocked relay expansion cards. Alternatively, enter 0 (disabled) to use a TS0840 4-Way Relay Card, or for no expansion.

Use a value that represents groups of eight clocked relays or open collectors. For example:

- Enter a value of 1 if one 8-way relay card is used (TS0841).
- Enter a value of 2 if one 16-way open collector card is used (TS0842).
- Enter a value of 4 if four 8-way relay cards are used (TS0841).

Site code A

This option applies to Challenger V8 panels and is not used by Challenger10 panels.

```
XX, Site Code A 0
*-Dis, Site Code:
```

Enter the first site code (or facility code). A site can have two site codes.

Two site code numbers and associated card offsets can be used to enable the system to have two sets of cards on different site codes (for example, to use during a changeover period when a system has been commissioned with a set of cards on loan and awaiting delivery of customised cards).

Site code A card offset

This option applies to Challenger V8 panels and is not used by Challenger10 panels.

```
XX, Site Code A Card Offset
*-Neg, No:
```

Enter a positive or negative number that is added to, or subtracted from, the actual card ID number for cards on site code A.

The resulting card ID (after processing) is the number that is used when programming users, and is reported to the printer and to management software. For example, if the card ID number is 5001, and the card offset is programmed as -5000, then the card will be programmed as user 1 and will report as user 1.

Site code B

This option applies to Challenger V8 panels and is not used by Challenger10 panels.

```
XX, Site Code B 0
*-Dis, Site Code:
```

Enter second first site code (or facility code). A site can have two site codes.
See also “Site code A” on page 8.

Site code B card offset

This option applies to Challenger V8 panels and is not used by Challenger10 panels.

```
XX, Site Code B Card Offset
*-Neg, No:
```

Enter a positive or negative number that is added to, or subtracted from, the actual card ID number for cards on site code B.

See also “Site code A card offset” on page 8.

Alarm code prefix length

If the Challenger panel uses an alarm code prefix value, then controllers must use the same value.

```
XX, Alarm Code Prefix Length 0
*-Dis, Length:
```

Enter the alarm code prefix length.

The alarm code prefix is the difference between the number of digits in an alarm control code and the number of digits in a door control code.

The alarm code prefix value enables users to enter a door code (a shorter PIN) for access control. For example, if a user’s full PIN is six digits long (for example, 123456), and the alarm code prefix value is 2, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN (for example, 3456).

The door code must be at least four digits long, so if the alarm code (user PIN) is five digits, then the only possible prefix length is one. Alarm codes can be up to ten digits.

Poll RAS

```
No RAS's Being Polled
Poll RAS:
```

Enter the addresses of RASs connected to the controller’s RS-485 local LAN.
The display shows the RASs currently being polled.

```
1, 2, 3: 4:
Poll RAS:
```

The character following the RAS number indicates the communication state. A comma “,” means the RAS is responding to polling. A colon “:” means the RAS is not responding to polling. Press the [*] key to refresh the display.

The RS-485 local LAN supports 16 RASs so that each door can have a pair of in readers and a pair of out readers. Two in or out readers would be required for card plus PIN functionality if the card reader and the keypad are separate devices.

Table 1: RAS addresses for IN and OUT functionality

	In	In	Out	Out
First door	1	5	9	13
Second door	2	6	10	14
Third door	3	7	11	15
Fourth door	4	8	12	16

Note: RASs 5 to 8 and RASs 13 to 16 are used where card plus PIN are used on the same door. For example, door 1 may require the user to badge at RAS 1 and enter a PIN at RAS 5, where both RAS 1 and RAS 5 are on the same side of the door.

RASs with LCDs fitted

```
No RAS with LCD's Fitted
LCD RAS:
```

Enter the addresses of RASs connected to the controller’s RS-485 local LAN that have LCD (liquid crystal display).

RASs with egress enabled

```
No RAS's with Egress Enabled
Egress RAS:
```

Enter the addresses of RASs connected to the controller’s RS-485 local LAN that have an egress button connected to the RAS’s IN or EGRESS terminal.

Tip: Since the RAS’s egress input does not provide tamper monitoring, it may be better to wire egress buttons to inputs on the controller.

RASs with toggle enabled

```
No RAS with Toggle Enabled
Toggle RAS:
```

Enter the addresses of RASs with keypads connected to the controller’s RS-485 local LAN that have toggle mode enabled.

In this instance, toggle mode refers to the Toggle Area Status programming option for keypad RASs connected to the controller's RS-485 local LAN. RASs connected to the system LAN operate differently.

The following tables list the effect of having toggle mode enabled and disabled.

Table 2: Toggle mode operation, except as described in Table 3

Keypad input	Toggle Mode	Effect on areas
PIN + [ENTER] or [#]	Enabled	Toggles the arm/disarm state
	Disabled	Arms
PIN + [MENU*] or [*]	Enabled	Toggles the arm/disarm state
	Disabled	Disarms

Table 3: Toggle mode operation for small LCD keypads

Keypad input	Toggle Mode	Effect on areas
PIN + [ENTER]	Enabled	Toggles the arm/disarm state
	Disabled	Arms
PIN + [ON]	Enabled	Arms
	Disabled	
PIN + [OFF]	Enabled	Disarms
	Disabled	

Poll DGP

This option applies only to Four-Lift Controllers.

```
No DGP's Being Polled
Poll DGP:
```

Enter the addresses of DGPs connected to the Four-Lift Controller's RS-485 local LAN.

The display shows the RASs currently being polled. The character following the RAS number indicates the communication state:

- A comma “,” means the DGP is responding to polling.
- A colon “:” means the DGP is not responding to polling.

Press the [*] key to refresh the display.

A Four-Lift Controller can poll up to 15 DGPs on its RS-485 local LAN, with each DGP providing up to 16 inputs (typically for floor-buttons).

Tamper monitoring

If the Challenger panel monitors input circuits for tamper conditions, then controllers must do the same.

```
XX, Yes - Tamper Monitoring
*-Change
```

Select Yes to enable input tamper monitoring. When enabled, the system can detect sealed, unsealed, and fault (open and short circuit) states.

Select No to disable input tamper monitoring. When disabled, the system can detect sealed and unsealed states only. Open and short circuit states are detected as unsealed.

Card to PIN time

If card plus PIN functionality is used, you can define the amount of time permitted between a user badging their card and entering their entire PIN.

If the PIN is not completely entered before the time expires, then the user will need to repeat the door opening function.

```
XX, Card to PIN Time 8 Seconds
*-Min, Time:
```

Enter the number of seconds required.

Dual custody time

If dual custody functionality is used, you can define the amount of time permitted between a visitor and an accompanying guard badging their cards to open a door, or between the first and second instances of badging when two badge unlock is used.

If the time expires before the second badging, then the door is not unlocked and the operation must be recommenced.

```
XX, Dual Custody Time 8 Seconds
*-Min, Time:
```

Enter the number of seconds required.

See also “IN reader dual custody” on page 19, “OUT reader dual custody” on page 19, and “Two badge unlock” on page 19.

Mode time

If the reader’s alarm control options specify three-badge alarm control for users who are authorised to arm and disarm areas, you can define the amount of time permitted between the first and third badges.

If the time expires, then the user will need to repeat the three badges in order to arm or disarm the area.

```
XX, Mode Time 5 Seconds
*-Min, Time:
```

Enter the number of seconds required.

See also “Alarm control options” on page 21.

Lock relock time

This setting applies only where the door has been programmed so the lock relay will not re-lock until after the door is closed.

This feature is provided for hardware such as drop bolts and magnetic locks, where the door must be closed before the lock relay locks the door. The relock delay time is the amount of time between the door being closed and the lock relay deactivating (relock). This allows a settling time to ensure that the lock mechanisms are aligned.

```
XX, Lock Relock Time 3 Seconds
*-Min, Time:
```

Enter the number of seconds required.

See also “Input holds door unlocked” on page 23.

Region count threshold

If the system tracks the number of users in regions (defined by IN and OUT readers), you can define a number as the region count threshold. When the number of users reaches the threshold, a region limit event is generated.

The region limit event can be used as a DGP macro logic input to, for example:

- Activate a sign when a car park is full.
- Arm areas when the last person has left the region or disarm areas when the first person enters the region.

```
XX, Region Count Threshold
*-Dis, Length:
```

Enter a number in the range 0 to 65,535.

Enable siren monitoring

The use of a siren on a controller is optional and siren monitoring is disabled by default. The siren circuit is not monitored for fault conditions unless siren monitoring is enabled.

```
XX, NO - Enable Siren Monitoring
*- Change:
```

Select Yes to enable siren monitoring.

Forced door debounce time

The forced door debounce time is a value in milliseconds times 100 (the default is 7, which equals 700 milliseconds). Acceptable values are in the range 4 to 15.

Forced door debounce time delays the generation of a forced door alarm for the specified interval (or until cancelled by a valid access or an egress push button). It caters for certain locks, which may cause erroneous Forced Door reporting.

```
XX, Forced Door Debounce 7 *100  
ms *100:
```

Enter a number in the range 4 to 15 (400 ms to 1500 ms).

Starting LCD Area (Challenger10 only)

The controller can have 16 RASs on its local LAN, each with up to 16 area LEDs to indicate up to 16 of a Challenger10 panel's 99 areas.

```
XX, Starting LCD Area 1  
*-Dis, Area:
```

Enter the number of the area that is to be indicated by the LCD RAS's first area LED. Each subsequent area LED will indicate the state of subsequent areas. For example, if LED 1 indicates area 12, then LED 2 indicates area 13, and so on. Any LEDs mapped past area 99 will not operate.

Option 2 – Door/lift options

At the DGP menu ("DGP menu" on page 7) enter 2 to access the Door/lift options programming screens.

The first programming screen is to select a door or lift number (the numbers displayed relate to the DGP address).

```
Select Door 17, 18, 19, 20  
Door:
```

Enter one of the displayed door numbers.

Door/lift access options

Access time

```
XX, Access Time 5 Seconds  
*-Min, Time:
```

Program the amount of time for the door to unlock when a user enters a valid card or PIN at the door reader. The user is then able to open the unlocked door during the time period of unlock.

See also "Lock relay" on page 27.

Extended access time

```
XX, Extended Access Time 10 Seconds
*-Min, Time:
```

Program the amount of time for the door to unlock when a user, with the “LONG ACCESS” flag enabled, presents a valid card or PIN at the door reader. The user is then able to open the unlocked door during the time period of the extended unlock time.

Shunting options

```
XX, No Shunting
*-Change, Opt:
```

This record configures the door shunting options. Shunting is a procedure that prevents an open door from reporting an alarm for a specified time.

Option		Function
0	No shunting	The door is not shunted.
1	Input Shunting	The door is shunted. Generates a standard alarm, based on the input type settings, if left open longer than the programmed shunt time.
2	Input Shunting & DOTL	The door is shunted and generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time. Enables Forced Door and DOTL to be reported on separate input numbers (as recorded in “Hardware Options”).
3	Auto Shunting & DOTL	If the area assigned to the door is disarmed, shunting of the door commences when the door input is unsealed (no code or card required). A DOTL (Door Open Too Long) alarm is generated if it is left open longer than the programmed shunt time. Forced Door and DOTL are reported on separate input numbers (as recorded in “Hardware Options”).

Shunt time

```
XX, Shunt Time 60 Seconds
*-Min, Time:
```

Program the amount of time that the door may be opened for without causing an alarm (shunted). This allows time for a user to pass through the door and shut it again.

See also “Shunt input” on page 28.

Extended shunt time

```
XX, Extended Shunt Time 90 Seconds
*-Min, Time:
```

Program the amount of time for the door to be shunted when a user, with the “LONG ACCESS” flag enabled, presents a valid card or PIN at the door reader.

Shunt warning time

```
XX, Shunt Warning Time 15 Seconds  
*-Min, Time:
```

Program the amount of time for a relay to activate, to sound a warning device, before the Shunt Time or Extended Shunt Time expires.

See also “Warning relay” on page 28 and “Shunt input” on page 28.

Shunt until door closes

```
XX, NO Shunt Until Door Closes  
*-Change
```

Select this option to ignore the programmed shunt time, and to shunt the inputs programmed in “Shunt input” on page 28 until the door closes (the door input is resealed).

Cancel shunt after door secures

```
XX, NO Cancel Shunt After Door Secures  
*-Change
```

For security reasons, it may be required to limit the shunt period as much as possible in order to detect the door being opened again during the shunt time (after the debounce time of approximately 2 seconds).

Select this option to use the programmed shunt time to shunt the inputs programmed in “Shunt input” on page 28, and then to cancel the shunt when the door closes (the door input is resealed).

Low security time zone

```
XX, Low Security Time Zone Disabled  
*-Dis, TZ:
```

Enter a time zone number (see “Time zones” on page 4). When the time zone is valid, only a card or PIN is required to open the door. When the time zone is not valid and the reader’s Card & PIN option is set to YES, then a valid card and PIN must be entered to open the door.

When the low security time zone is valid, two badge unlock is disabled (see “Two badge unlock” on page 19).

IN reader card & PIN

```
XX, NO - In Reader Card & PIN  
*-Change
```

Select this option to require that both a card and a PIN must be used to unlock the door via the IN reader.

If not selected, then either a card or a PIN will unlock the door via the IN reader.

OUT reader card & PIN

XX, NO - Out Reader Card & PIN
*-Change

Select this option to require that both a card and a PIN must be used to unlock the door via the OUT reader.

If not selected, then either a card or a PIN will unlock the door via the OUT reader.

IN reader inhibit PIN

XX, NO - In Reader Inhibit PIN
*-Change

Select this option to require that only a card must be used to unlock the door via the IN reader during the “Low security time zone” on page 16.

If not selected, then both a card and a PIN must be used to unlock the door via the IN reader during the “Low security time zone” on page 16.

OUT reader inhibit PIN

XX, NO - Out Reader No PIN
*-Change

Select this option to require that only a card must be used to unlock the door via the OUT reader during the “Low security time zone” on page 16.

If not selected, then both a card and a PIN must be used to unlock the door via the OUT reader during the “Low security time zone” on page 16.

IN reader inhibit region 0 users

XX, NO-In reader Inhibit Region 0 Users
*-Change

Region 0 typically means off site.

Select this option to prevent users who are currently recorded as being in region 0 from unlocking this door via the IN reader.

OUT reader inhibit region 0 users

XX, NO-Out reader Inhibit Region 0 Users
*-Change

Region 0 typically means off site.

Select this option to prevent users who are currently recorded as being in region 0 from unlocking this door via the OUT reader.

Anti-passback options

XX, No Anti-Passback
*-Change, Opt:

Anti-passback controls the operation of the reader if a card or PIN is used to attempt to enter a region that the user is currently assigned to (see “Anti-passback notes” below).

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).

Option		Function
0	No anti-passback	No control of passback. A valid card or PIN opens the door without generating an alarm. Entering a region twice without leaving is possible.
1	Soft anti-passback	A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
2	Hard anti-passback	A valid card or PIN does not open the door when used to enter the region a second time without leaving first. An attempt to do so generates a report.
3	Timed anti-passback	The card will not open the door when used a second time in succession at the same door within the programmed time and the attempt will generate a report. See “Anti-passback time” on page 19.

Anti-passback notes

- A region has to be programmed for the door’s readers (see “IN reader region” on page 19, and “OUT reader region” on page 19).
- After badging the card, the door must be opened before a user is logged into a region.
- To clear an anti-passback violation, the card must be either used at another appropriate reader to change the region number that the user is recorded against, or the card must be reprogrammed in User Menu Option 14. Program Users (the region record is reset when the reprogrammed user is downloaded to Intelligent Controller). Alternatively, use management software to clear the violation.
- For region numbers below 200, anti-passback functionality does not apply to users with ‘Privileged’ status.
- Anti-passback functionality requires that every DGP that is polled to be online (responding to polling). If any DGPs are not communicating with the Challenger panel, then it is not possible to track the assignment of users to regions. As a result, anti-passback is disabled system-wide.

IN reader region

```
XX, In Region Disabled  
*-Dis, Region:
```

If using anti-passback, enter the region number for the IN reader. See “Using regions” on page 43 for details.

OUT reader region

```
XX, Out Region Disabled  
*-Dis, Region:
```

If using anti-passback, enter the region number for the OUT reader. See “Using regions” on page 43 for details.

Anti-passback time

```
XX, Anti-Passback Time  
*-Min, Time:
```

The card will not open the door when used a second time in succession at the same door within the programmed time, and the attempt will generate a report.

See also “Anti-passback options” on page 18.

IN reader dual custody

```
XX, NO - In Reader Dual Custody  
*-Change
```

When selected, two different users must present their card and/or PINs in succession in order to unlock the door via the IN reader.

OUT reader dual custody

```
XX, NO - Out Reader Dual Custody  
*-Change
```

When selected, two different users must present their card and/or PINs in succession in order to unlock the door via the OUT reader.

Two badge unlock

```
XX, NO - Two Badge Unlock  
*-Change
```

Note: This option applies only to Four-Door Controller firmware R-150411.801 or later.

As an alternative to dual custody, two badge unlock avoids unintended unlocking of a door if a user accidentally presents their card to a reader, for example, by brushing past the reader with the card in a pocket. When two badge unlock is enabled (and the low security time zone is not valid), the user may unlock the door by presenting the same card twice within the dual custody time (see “Dual custody time” on page 12). If the low security time zone is valid, then the two badge unlock setting is ignored.

Note: When two badge unlock is enabled and two different cards are presented within the dual custody time (regardless whether dual custody is used), then the door is not unlocked and a door access denied message is generated.

Door/lift egress options

```
2-Egress Options  
XX, Menu
```

The egress menu provides options for using a push button to open a door.

Egress time zone

```
XX, Egress Time Zone 0  
*-Dis, TZ:
```

Enter a time zone number (see “Time zones” on page 4) that will control the time period during which an Egress button (exit button) will unlock a door to allow exit. When the time zone is valid, a user may press the Egress button and the door will unlock.

Select time zone 0 (= always) if the egress should always be available.

See also “Egress input” on page 28.

In egress disabled if secure

```
XX, NO - In Egress Disabled If Secure  
*-Change
```

This option is used when the Egress button (exit button) is connected to an input on the Intelligent Controller (recommended).

When selected, the Egress button on an input or the IN reader will not unlock the door if any of the areas assigned to the door are armed.

If the Intelligent Controller loses communication with the Challenger panel, then the Intelligent Controller remembers the latest state of the area.

See also “Areas assigned to door” on page 29.

Out egress disabled if secure

```
XX, NO - Out Egress Disabled If Secure  
*-Change
```

This option is used when the Egress button (exit button) is connected to an input on the Intelligent Controller (recommended).

When selected, the Egress button on an input or the OUT reader will not unlock the door if any of the areas assigned to the door are armed.

If the Intelligent Controller loses communication with the Challenger panel, then the Intelligent Controller remembers the latest state of the area.

See also “Areas assigned to door” on page 29.

Egress options

```
XX, Egress Times Door Open
*-Change, Opt:
```

Select the required operation of the Egress button (exit button).

Option	Function
0 Egress Times Door Open	When the Egress button is pressed, the door unlocks for the programmed unlock time.
1 Egress Holds Door Open	Allows the door to be held unlocked for as long as the Egress button is pressed or for the programmed unlock time, whichever is longer.
2 Egress Shunts Only	When the Egress button is pressed, the input is shunted.

Egress reporting

```
XX, NO - Egress Reporting
*-Change
```

When selected, a Door Egress report is sent to the printer and to management software when the Egress input is used.

Door/lift alarm control options

```
3-Alarm Control
XX, Menu:
```

This menu provides options for arming/disarming using the access control features.

Alarm group

```
XX, Alarm Group 1
*-Dis, Grp:
```

Alarm groups may be assigned to doors to restrict alarm control from that door to the areas assigned to the alarm group.

Restrictions on the level of alarm control available (for example Disarm Only), and the time period (time zone) when the alarm control functions can be performed, may also be specified in the alarm group.

Alarm control options

```
XX, Reader Has No Alarm Control
*-Change, Opt:
```

Select the type of alarm control that can be used by the door or reader.

Option	Function
0 Reader Has No Alarm Control	It is not possible to arm/disarm using the reader.

Option	Function
1 Alarm Control on 1st Badge	Presentation of a valid card at the reader will disarm the areas in the alarm group on first badge. Badging three times will arm the areas.
2 Alarm Control on 3rd Badge	Presentations of a valid card three times arm/disarms the areas in the alarm group.
3 Alarm Control with Buttons	Allows user to access the function on the button interface.
4 Always Alarm Control (IN=OFF OUT=ON)	Presentation of a valid card at the IN reader disarms the areas in the alarm group. Presentation of a valid card at the OUT reader arms the areas in the alarm group.

In denied if area secure

```
XX, NO - In Denied If Area Secure
*-Change
```

When selected, a user cannot unlock the door from the IN reader if any of the areas assigned to the door are armed.

If the Intelligent Controller loses communication with the Challenger panel, then the Intelligent Controller remembers the latest state of the area.

See also “Areas assigned to door” on page 29.

Out denied if area secure

```
XX, NO - Out Denied If Area Secure
*-Change
```

When selected, a user cannot unlock the door from the OUT reader if any of the areas assigned to the door are armed.

If the Intelligent Controller loses communication with the Challenger panel, then the Intelligent Controller remembers the latest state of the area.

See also “Areas assigned to door” on page 29.

Authorised RAS

```
XX, RAS Number Disabled
*-Dis, RAS:
```

Program a system RAS number 1 to 16 (and 65 to 80 for Challenger10) for this Intelligent Access Controller's local RAS (reader) to ‘authorise’ this reader to arm/disarm and select areas via the system RAS when a valid badge is presented at the local reader (the reader must also have a keypad for area selection). The local reader can no longer be used to open this door: it is dedicated to arming and disarming areas controlled by the nominated system RAS.

The RAS on the system LAN that is selected for arm control must also have the option “Toggle Keyboard Control” set to Yes.

For example, RAS 3 has been designated as an authorised RAS. When User 23 badges his card on this reader, the Challenger system will treat the card as a valid PIN being entered on RAS 3. All he has to do now is enter the areas he wishes to arm or disarm.

Door/lift reader options

```
4-Reader Options
XX, Menu
```

Program settings specific to this reader.

Card format

```
XX, Tecom ASC
*-Change, Opt:
```

Set the data format of the reader and card, key or token being used.

Option	Function
0 Wiegand 27 bit	For Indala ESP range of proximity readers supplied by UTC Fire & Security.
1 Spare – Do NOT Use	Do not use
2 Tecom ASC	For TS0870 proximity readers.
3 K 32 bit	Kastle format cards.
4 Wiegand 26 bit (ID = 16, FC = 8)	For standard 26-bit Wiegand format readers. Has a 16-bit card number (0-65534) and an 8-bit site code (0-255).
5 Indala ASC 27 bit	For Indala ASP range of proximity readers using 27-bit Wiegand format.
6 Indala ASC 26 bit	For Indala ASP range of proximity readers using 26-bit Wiegand format.
7 Wiegand 32 bit	For 32-bit Wiegand format readers. Uses a 16-bit card number and 16-bit site code.
8 Mag. Card Tecom	For Tecom format magnetic swipe cards.
9 Mag. Card Midas	For Midas format magnetic swipe cards.
10 C36 bit	For C36 bit format.

Tip: TS0862 Smart Door Controllers can be used on the Intelligent Controller LAN and support the same data formats as the Intelligent Controller.

Input holds door unlocked

```
XX, NO - Input Holds Door Unlocked
*-Change
```

When selected, the door lock will not re-lock until the door is closed. This is used where the lock mechanism, when locked, will prevent the door from closing.

Door unlocked until door opens

```
XX, NO - Door Unlocked Until Door Opens  
*-Change
```

For security reasons, it is possible for the door to re-lock at the moment it opens. The door relay will be de-activated after the door is opened. This option will override the unlock time. The door will stay unlocked until opened.

When selected, after a door is unlocked by a card or PIN, the door lock relay will remain activated until the door input is unsealed.

Override time zone

```
XX, Override Time Zone Disabled  
*-Dis, TZ:
```

Enter the override time zone number (see “Time zones” on page 4). The override time zone automatically unlocks the door for the programmed times. Free access is allowed when the time zone is valid.

Override after entry

```
XX, NO - Override After Entry  
*-Change
```

When selected, the override time zone takes cannot unlock the door for the programmed times unless a user has entered.

Report door unsecured/secure

```
XX, NO - Report Door Unsecured/Secure  
*-Change
```

When selected, and access is granted to a user, an “unsecured” message is sent to history. When the door relocks, a “secured” message is reported to history.

This is only a reporting function. There is no event specified in the control panel. This function can only be used in conjunction with “Map (un)secure to (un)locked” below.

Map (un)secure to (un)locked

```
XX, NO- (un)secure to (un)locked  
*-Change
```

When selected, and access is granted to a user, an “unlocked” message is sent to history. When the door relocks, a “locked” message is reported to history.

This is only a reporting function.

Report door open/close

XX, NO - Report Door Open/Close
*-Change

When selected, a report is sent to the printer and to management software when the input assigned to the door is unsealed (opened) or resealed (closed).

This is only a reporting function.

Report forced door

XX, NO - Report Forced Door
*-Change

When selected, a report is sent to the printer and to management software when the input assigned to the door is unsealed without valid access (card, PIN, or egress request).

This is only a reporting function.

Report DOTL

XX, NO - Report DOTL
*-Change

When selected, a report is sent to the printer and to management software when the input assigned to the door is in the door open too long (DOTL) state, for example, still open after the shunt timer expires.

This is only a reporting function

Wiegand reader LED options

XX, LED1 On When Locked
*-Change:

For TS0867 and TS0869 models only, select the LED functionality required for this door's Wiegand reader (not for readers on the Intelligent Controller's local LAN).

Option	Functionality
LED on when door locked	LED 1 is on, when the door is locked.
LED on when door unlocked	LED 1 is on, when the door is unlocked.
LED on when area secured	LED 1 indicates if the area assigned to the door is armed (if more than one area is assigned, all areas assigned to the door must be armed before LED changes state).
LED on when area accessed	LED 1 indicates if the area assigned to the door is disarmed (if more than one area is assigned, all areas assigned to the door must be disarmed before LED changes state.)
Two LEDs access/secure	Readers with dual LED control lines connected indicate the area disarmed and armed with different LED colours.
Two LEDs valid/void	Readers with dual LED control lines connected indicate User Valid or Void using different LED colours.

Option	Functionality
No LEDs	No LED control.

Note: On readers with dual LED control lines, LED 2 may be programmed to indicate other conditions by using DGP macro logic programming.

See also “Areas assigned to door” on page 29.

Pulsed lock and unlock relays

```
XX, NO - Pulsed Lock & Unlock Relays
*-Change
```

When selected, two separate relays are pulsed at different times for a lock to open, and two separate inputs are monitored. Normal lock-strike opening is disabled.

See “Using pulsed lock and unlock relays” on page 41 for details.

Random percentage

```
XX, Random Percentage 0
, Percentage:
```

Records a percentage value in the range 0 to 100%.

The “Door Random Bit” event assigned to the door will be activated an average of once per the percentage value of the number of times that the reader is used to access the door.

The random bit event may then be used in the controller's macro logic programming to activate a relay or another event. For example, if the percentage value was set to 20, the door random bit event would be activated an average of once every five times a card or PIN is successfully used at the reader.

Time & attendance reader

Some management software applications do not support time & attendance functionality.

```
XX, Yes - Time & Attendance Reader
*-Change
```

When selected, the LCD RAS can be used as a time and attendance reader.

See “Using time and attendance readers” on page 40 for details.

Disable duress

```
XX, NO - Disable Duress
*-Change
```

When selected, the system's keypad duress functionality cannot be used at this door.

Door/lift hardware options

```
5-Hardware Options  
XX, Menu:
```

Challenger input and relay numbers are used in these records. Refer to “Input and relay numbering” on page 43 for details.

The Intelligent Controller, when assigned an address, automatically calculates its default input and relay numbers (see Table 5 on page 44). The Four-Door Controller has four relays onboard that are assigned as lock relays by default.

When assigning input and relay numbers to these functions, only numbers associated with the DGP address can be entered. These Intelligent Controller relay assignments only activate relays connected to it.

See “Door/lift hardware defaults” on page 44 for default input numbers. Inputs that are not used as door inputs function as normal alarm system inputs and require end-of-line (EOL) resistors to be used in the circuit.

Any input assigned as a door contact input or DOTL input also have to be programmed in the Install menu option 1, “Input Database” to define how the Challenger responds to alarms on these inputs.

Lock relay

```
XX, Lock Relay nn  
*-Dis, Relay:
```

Enter the number of the Intelligent Controller relay to be activated when the door is accessed. By default, this is one of the four onboard relays. The relay number specified refers to system relay numbers.

If using “Pulsed lock and unlock relays” on page 26, the relay number is entered here.

Input

```
XX, Input nnn  
*-Dis, Input:
```

Enter the number of the input to be used for a door contact on the Intelligent Controller.

If using “Pulsed lock and unlock relays” on page 26, the input number is entered here.

Monitor 2nd door input

```
XX, NO - Monitor 2nd Door Input  
*-Change
```

Optionally, enter the number of the second input to be used for a second door contact on the Intelligent Controller. Input numbers are listed in “Input and relay numbering” on page 43.

Forced relay

```
XX, Forced Relay Disabled  
*-Dis, Relay:
```

Enter the number of the relay to be activated when an input is in a “Forced Door” condition, for example, the door has been opened without a valid command.

Shunt input

```
XX,  
Shunt Input:
```

Enter the number of the input that is required to be shunted when the door is accessed (typically the same number as the door input number).

Warning relay

```
XX, Warning Relay Disabled  
*-Dis, Relay:
```

This menu specifies the Intelligent Controller relay number to be activated during the “Warning time” when the shunt timer is about to expire, for example, may be used to activate a buzzer above a door to indicate the door needs to be closed.

DOTL input

```
XX, DOTL Input nnn  
*-Dis, Input:
```

This menu specifies the input number on the Intelligent Controller that reports the DOTL (door open to long) alarm condition for the door being programmed (if DOTL is enabled in Shunting options).

DOTL inputs must not have any alarm devices connected to them, and must be sealed with EOL resistors.

Default DOTL input numbers are listed in “Input and relay numbering” on page 43.

DOTL relay

```
XX, DOTL Relay Disabled  
*-Dis, Relay:
```

This menu specifies the Intelligent Controller relay number to be activated when an input is in a “DOTL” condition, for example, the door left open after the shunt timer has expired.

Egress input

```
XX, Egress Input nnn  
*-Dis, Input:
```

This menu specifies the input number on the Intelligent Controller that activates the Egress function for the door being programmed.

Door interlock

```
Door not Interlocked  
Int. Input:
```

Enter the input numbers on the Intelligent Controller that prevents the doors being accessed at the same time.

Note: Numbers must be input numbers on the same Intelligent Controller.

To interlock with a door on another Intelligent Controller, a contact from that door must be wired to a spare input on the first Intelligent Controller and vice versa. In this case, if an input is being used for interlocking and no door on the Intelligent Controller has that input as its 'Door Contact', then the Intelligent Controller automatically inserts a two-second delay before a door opens to allow for settling times across door controllers. Please remember that this two-second delay only occurs when an input is being used for interlocking and that input comes from another door not on this door controller.

Areas assigned to door

```
No Areas Assigned To Door  
Area:
```

The areas specified here are used for:

- Controlling reader LEDs, if options 2 or 3 are selected in “Wiegand reader LED options” on page 25.
- Controlling access through a door when “In denied if area secure” on page 22.
- Controlling the use of egress functionality when “Out denied if area secure” on page 22.

Although the areas listed here are not used for area control, the Intelligent Controller does need to identify the status of these areas in order to know whether to send an arm or disarm command to the Challenger panel. This is only when using cards by themselves for arming/disarming, for example, when “Alarm Control on 1st or 3rd badge” is used.

Note: Challenger10 panels can have 99 areas; Challenger V8 panels can have 16 areas.

Please remember that the alarm group nominated in “Alarm group” on page 21 determines the areas allowed to be armed/disarmed by a user, not the areas listed here.

Fault relay

```
XX, Fault Relay Disabled  
*-Dis, Relay:
```

This menu specifies the Intelligent Controller relay number to be activated when a lock fault or reader fault is detected.

This function is not currently implemented.

Lift options

```
6 Lift Options  
XX, Menu
```

These options apply only to Four-Lift Controllers.

Starting floor

```
XX, First Floor 1  
*-Dis, Floor:
```

This record sets up the starting floor number the lift will control. For example, if this lift was controlling floors 1 to 8, then this 'Starting Floor' option needs to be 1. See also "Last floor" below.

Last floor

```
XX, Last Floor 64  
*-Dis, Floor:
```

This record sets up the last floor number the lift will control. For example, if this lift was controlling floors 1 to 8, then this 'Last Floor' option needs to be 8. See also "Starting floor" above.

Starting physical relay

```
XX, First Physical Relay 1  
*-Dis, Relay:
```

This record configures the physical starting relay number for the range of relays that the lift uses to access floors.

For a Challenger10 example, if this lift was controlling floors 1 to 8 and the relays used to access those floors are relays 5 to 12 on the Four-Lift Controller, then enter 5 here. When this value is entered, the Four-Lift Controller interprets this as follows:

- Physical relay is 5 ('physical' meaning the actual relay on board the Four-Lift Controller).
- Starting floor is 1 and last floor is 8, meaning 8 floors.
- Therefore, relays 5 to 12 on this Four-Lift Controller are used for this lift to access floors.

The Four-Lift Controller automatically calculates the last relay number required to access the floors it controls, as defined by 'Starting Floor' and 'Last Floor'.

Inputs monitor floor selected

```
XX, NO - Inputs Monitor Floor Selected  
*-Change
```

When selected, the Four-Lift Controller's inputs may be used to monitor the floor selected, which generates a report to the printer and computer. The input range used is configured in "Starting physical input" on page 31.

Wait for floor selection

```
No - Wait For Floor Selection
*-Change
```

When selected, lift will wait for only one floor to be selected before going on. Otherwise, multiple floors may be selected (if the user is allowed access to multiple floors).

Starting physical input

```
XX, First Physical Input 1
*-Dis, Input:
```

Enter the starting input number that the Four-Lift Controller will use to monitor the floors.

When the user accesses a floor (a floor button pressed in the lift), the Four-Lift Controller will know which floor the user has selected. For example, if this lift was controlling floors 1 to 8, (8 floors) and this option has been set to 9, then inputs 9 to 16 on the Four-Lift Controller will be used to monitor the floors. Floor 1 uses input 9; Floor 2 uses input 10, and so on.

The Four-Lift Controller automatically calculates the last input by the number of floors it is controlling. The floor range is configured using the options “Starting floor” on page 30 and “Last floor” on page 30.

Lift override group

```
XX, Lift Override Group Disabled
*-Dis, Grp:
```

Enter the number of a designated floor group that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, without using a valid card or PIN at the lift reader.

Security input

```
XX, Security Input Disabled
*-Dis, Input:
```

Enter the input number on the Four-Lift Controller that will control the “Lift security group” below.

Note: The security input number must not be used as a floor input.

Lift security group

```
XX, Lift Security Group Disabled
*-Dis, Grp:
```

Enter the number of a designated floor group that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, provided that the Security input (key switch) is switched on.

See “Security input” above.

Total floors

```
XX, Total Floors 0
*-Dis, Floors:
```

Enter the total number of floors that are available. This information may be obtained from the lift installation company.

Lift bank

```
XX, Lift Bank Disabled
*-Dis, Bank:
```

Enter the lift bank or the group that the lift is part of. This information may be obtained from the lift installation company.

Lift car

```
XX, Lift Car Disabled
*-Dis, Car:
```

Enter the lift's car within the bank. This information may be obtained from the lift installation company.

Floor landings 1–32

```
XX, No floor landings
LandFlr 1-32:
```

Enter the floors, from 1 to 32 that the lift's car can stop at with respect to the total floors available. When entered, the display will show four sets of eight digits (one digit for each floor). The digits are 1 or 0. A 1 indicates a floor landing is available. A 0 indicates that no floor landing is available.

```
11001111 11000000 00000000 00000000
LandFlr 1-32:
```

Floor landings 33–64

Enter the floors, from 33 to 64 that the lift's car can stop at in relation to the total floors available. When entered, the display will show four sets of eight digits (one digit for each floor). The digits are 1 or 0. A 1 indicates a floor landing is available. A 0 indicates that no floor landing is available. See "Floor landings 1–32" above for an example of the display.

Monitor high level floor landing

When selected, the Four-Lift Controller monitors the lift's floor landings. This option is typically set to NO due to the large amount of data generated.

Option 3 – Initialize database

At the DGP menu ("DGP menu" on page 7) enter 3 to access the Initialise Database option.

Before starting initial programming, initialise the database to ensure all options have been set to default and to create a base for efficient programming.

Note: Programming menu 3, “Initialise Database”, defaults the Intelligent Controller database, resetting ALL programming options to the factory defaults.

```
3-Initialise Database
Menu:
```

When selected, the display shows what doors will be initialised. Press [*] or [MENU*] to start the initialisation process.

```
Initialize Doors xx,xx,xx & xx
*-Initialize
```

The display will show the doors that are being initialised.

```
Initializing Doors xx,xx,xx & xx
Please Wait...
```

Option 4 – Display card

At the DGP menu (“DGP menu” on page 7) enter 4 to access the Display Card option. This option displays card detail of the last card badged.

Note: The programming must to be completed, at least in part, before the correct information will be displayed. The readers must be working, available, and configured for the correct card formats.

```
4-Display Card
Menu:
```

The Display Card option is used to verify if the card settings are correct (the card read has the correct card numbers). After a card is badged, all details concerning the site code and the card number are displayed. If the site code is unknown, this option may be used to reveal the card’s site code.

When checking the site code for a set of cards, always check several cards to ensure that the site code is the same for all cards in the set. This also helps to indicate that the correct card format has been selected in the reader options.

If different cards in the same set of cards show different site codes, re-check the card format selected.

Example of display before badging a card:

```
Waiting For Card to be Badged (20)
ENTER - Exit:
```

Tip: The number in brackets after Waiting For Card to be Badged tells you how many users are currently stored in the controller.

Example of display after badging a card:

```
USER
30: SC1028,ID30[27.0.0.4.4.0.30]
```

In this example, the site code is 1028, the card ID is 30, and the number in brackets is what the controller believes to be the raw card data (assuming that the controller has IUM and the card format is recognised by the reader).

Option 5 – Door groups

At the DGP menu (“DGP menu” on page 7) enter 5 to access the Door Groups option.

```
5-Door Groups
Menu:
```

The Door Groups option is provided as a diagnostic tool for the installer/programmer. It enables the door group details relating to the four doors on the Intelligent Controller being programmed to be viewed and modified for testing purposes.

Note: Use this option only as a diagnostic tool. Permanent changes to door groups should be programmed in User menu option 20, “Door and Floor Groups”.

To view or modify a door group, enter a door group number.

```
Door Group To Program
Group:
```

The door group contains the doors (and their time zones) that belong to the Intelligent Controller. Authorised access is only valid (will be granted) during the time zone.

Enter a door number.

```
Group 1, D17-**, D18-**, D19-**,
Door:
```

Program a time zone for the door, or disable the door.

```
Group 1, D17-**, D18-**, D19-**,
*-Dis, Door17TZ:
```

Door and time zone information is displayed as follows:

- DXX-00 Door XX has time zone 0 assigned (standard 24-Hour access)
- DXX-** Door XX has no time zone assigned.
- DXX-nn Door XX has time zone nn assigned to restrict access at the door to a specific time period.

Option 6 – Lift groups

At the DGP menu (“DGP menu” on page 7) enter 6 to access the Lift Groups option.

```
6-Lift Groups
Menu:
```

The Lift Groups option is only provided as a diagnostic tool for the installer/programmer. It enables the floor group details relating to the floors on the Intelligent Controller being programmed to be viewed and modified for testing purposes.

Note: Use this option only as a diagnostic tool. Permanent changes to lift groups should be programmed in User menu option 20, “Door and Floor Groups”.

To view or modify a lift group, enter a lift group number.

```
Lift Group To Program
Group:
```

Each lift group contains a list of 64 possible floors. All 64 floors are displayed along with the time zone assigned to each floor (press * to see additional floors). Authorised access is only valid (will be granted) during the time zone.

Enter a floor number.

```
Group 1, F1-**, F2-**, F3-**, F4-**
Floor:
```

Program a time zone for the floor, or disable the floor.

```
Group 1, F1-**, F2-**, F3-**, F4-**
*-Dis, Floor1 Tz:
```

Floor and time zone information is displayed as follows:

- FXX-00 Floor XX has time zone 0 assigned (standard 24-Hour access)
- FXX-** Floor XX no time zone assigned.
- FXX-nn Floor XX has time zone nn assigned to restrict access at the floor to a specific time period.

Option 7 – System options

At the DGP menu (“DGP menu” on page 7) enter 7 to access the System Options menu.

```
7-System Options
Menu:
```

The System Options menu is used to assign system relays. The relay numbering used in these records is the same as used by the Challenger. Therefore the relay numbers used in the Door Programming menu correspond with the numbers used in Install menu option 16 “Map Relays”.

When assigning relay numbers to these functions, only relay numbers associated with the DGP address can be entered. These Intelligent Controller assignments only activate the relays connected to the DGP being programmed.

Challenger relay numbers are used in these records. Refer to “Input and relay numbering” on page 43 for details.

Mains fail relay

```
XX, Mains Fail Relay Disabled  
*-Dis, Relay:
```

Enter the relay number to be activated when a “Mains Fail” condition exists on the Intelligent Controller.

Low battery relay

```
XX, Low Battery Relay Disabled  
*-Dis, Relay:
```

Enter the relay number to be activated when a “Low Battery” condition exists on the Intelligent Controller.

Tamper relay

```
XX, Tamper Relay Disabled  
*-Dis, Relay:
```

Enter the relay number to be activated when a “Cabinet Tamper” or a “Siren Fault” condition exists on the Intelligent Controller.

Option 8 – Macro logic

At the DGP menu (“DGP menu” on page 7) enter 8 to access the Program Macro Logic menu.

```
8-Program Macro Logic  
Menu:
```

Macro logic provides a powerful tool for activating (or deactivating) event flags controlled by programmed conditions. The programmed conditions are logic equations combining the macro inputs (macro event flags) and timed or latched output conditions.

Numbered macro event flags are used as the macro logic program’s inputs. Up to four macro inputs may be included in the logic equation. Each macro input in the logic equation can be programmed as an AND or an OR function and may be inverted to formulate NAND and NOR equations.

Options are provided so that the macro’s result will trigger a macro output (event flag), which may be a pulse, timed, on delay, off delay or latched when activated. The output event flag can be inverted.

The event flags are pre-defined event flag numbers as listed in “Macro event flags” on page 49. Some can only be used for macro inputs, some for macro outputs, and others may be used for either inputs or outputs.

For more information on macro logic programming, refer to the Challenger programming manual.

Note: It is very important to plan the macro logic carefully on paper, noting all details before attempting to program. Worksheets are provided in “DGP macro logic worksheet” on page 65.

Macro logic program number

```
Macro Logic Number
Macro No:
```

Enter the number of the macro logic program number. There are 48 programs available.

Function and output event

```
MX, E0 Disabled
*-Chg, Event:
```

The result of the macro’s logic and the macro’s output function will trigger an event flag. The macro’s output may have timing functions.

Option	Function
Disabled	This macro logic program is disabled.
Non Timed	Follows the result of the logic equation only. If a macro input (an event flag or an output) for this macro changes, the logic equation will be calculated again.
On Pulse	Activates for the programmed time or the active period of the logic result, whichever is the shortest.
On Timed	Activates for the programmed time regardless of the macro inputs changing.
On Delay	Activates after the programmed time period unless the result of the logic equation is no longer valid.
Off Delay	Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active.
Latched	Activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input (any programmed AND / OR function is not used).

To program via a RAS, press:

- [MENU*] to display a new output function.
- 0 to leave the menu
- nnn [ENTER] to enter the event flag number. Activates if the result of the logic equation is true. Enter the number a second time to invert the output. An inverted output is indicated by an exclamation mark (!) preceding the event flag number.

- [ENTER] to save the displayed function and move to the next display.

Time

```
Macro X, E0 On Pulse 0 Sec
*-Chg, Event:
```

The time period (1 to 255 seconds or minutes) that is used when any of the timed macro output functions are selected (pulse, on timed, on delay or off delay). When programming 1 to 4 minute periods, program the value in seconds to improve the accuracy (e.g. 60, 120, 180 or 240 seconds).

Logic equation

```
MX, E0 OR E0 OR E0 OR E0
1st Event:
```

Program up to four macro inputs (event flag numbers). The logic connecting the four inputs may be the AND or OR function. A NAND or NOR function can be achieved by inverting the logic of the particular input.

When all conditions of the logic equation have been met the result is true and the event programmed in the previous steps will be activated (depending on any timing function programmed).

Any macro logic inputs not used MUST be left as an OR function.

To program via a RAS, press:

- nnn [ENTER] to enter and display new event flag number. Enter the same number twice to invert the macro input. An inverted input is indicated by an exclamation mark (!) preceding the “E”. Before calculating the result of the macro logic equation, the input is inverted.
- [MENU*] to toggle between OR or AND function.
- [ENTER] to save the displayed function and move to the next display.

Option 9 – Version number

At the DGP menu (“DGP menu” on page 7) enter 9 to retrieve information from the Intelligent Controller.

The Version number option displays copyright information, the Intelligent Controller firmware version, and memory configuration.

```
@2013 Interlogix
R-DDMMYY.nnn SIUM
```

Abbreviations used:

- NIUM = no IUM (neither hardware IUM nor software IUM are used)
- MIUM = mini IUM (hardware IUM is not used but software IUM is used)
- SIUM = small IUM (4 MB hardware IUM is used)
- LIUM = large IUM (8 MB hardware IUM is used)

Option 10 – Remote controllers

At the DGP menu (“DGP menu” on page 7) enter 10 to access the Remote Controllers menu.

```
10-Remote Controllers
Menu:
```

The Remote Controllers menu is used to program RASs or TS0862 Smart Door Controllers on the Intelligent Controller’s local LAN in a similar manner to the Challenger panels Install menu option 28 “Remote Controllers”.

```
Sub-Remote Type: 1-DGP, 2-RAS
Device Type:
```

Enter 2 to select RAS.

```
Sub-Remote RAS Setup
RAS No:
```

Select the device’s address.

```
Connecting...
Enter to abort
```

Tip: The Intelligent Controller’s local LAN may be used to connect a Wiegand reader to the Intelligent Controller over large distances by using a TS0862 Smart Door Controller. TS0862 Smart Door Controllers are polled as RASs.

Four-Lift Controllers can poll DGPs on their local LAN, but there are currently no DGPs with a menu that can be accessed from the DGP option.

Option 11 – Display IUM user

At the DGP menu (“DGP menu” on page 7) enter 11 to access the Display IUM user Controllers option.

This command is available as a diagnostic tool (e.g. to investigate why a particular card is not recognised at a reader when it should be).

```
Display User Data
User:
```

Enter the user number to verify the following:

- The user number exists in the Intelligent Controller’s memory.
- The raw card data (RCD) is associated with the user number.

Appendix A. Reference materials

Using time and attendance readers

There are two types of readers that may be used for time and attendance functionality (clocking on and off):

- There can be 16 RASs (readers or keypads) on the controller's local LAN designated as time and attendance readers (see "Time & attendance reader" on page 26).
- Models TS0867 and TS0869 can have four additional readers connected to the onboard Wiegand interfaces (marked "DOOR 1", "DOOR 2" and so on).

Using RASs for time and attendance

If using card readers on the controller's local LAN, the functionality is determined by the RAS address. By default, there are eight Clock On readers and eight Clock Off readers on the local LAN, as listed in Table 4 below.

Badging a card on a Clock On card reader automatically clocks you on. Badging a card on a Clock Off card reader automatically clocks you off.

Table 4: Local LAN default RAS functionality

Door	Default Clock On Readers		Default Clock Off Readers	
1	1	5	9	13
2	2	6	10	14
3	3	7	11	15
4	4	8	12	16

Using an LCD RAS

When used as a time and attendance reader, the LCD RAS will display the time and date similar to the following:

```
8:59    03/02/13
Clock On
```

Users can clock on and off using two methods, described as follows.

Method 1: Clock On

To clock on, key in the user PIN and press On. The current time and date will appear for about a second before this screen appears:

```
Access granted
Clocked on
```

Method 1: Clock Off

To clock off, key in the user PIN and press Off. The current time and date will appear for about a second before this screen appears:

```
Access granted
Clocked off
```

Method 2 (LCD keypad only): Clock On

To clock on, first press * to toggle the state so that Clock On is displayed, then key in the user PIN and press Enter.

```
8:59    03/02/13
Clock On _
```

Method 2 (LCD keypad only): Clock Off

To clock off, first press * to toggle the state so that Clock Off is displayed, then key in the user PIN and press Enter.

```
8:59    03/02/13
Clock Off _
```

Using Wiegand readers for time and attendance

The four onboard Wiegand interfaces are considered as IN readers for the four doors or lifts, unless they are assigned the same lock relay.

If two Wiegand interfaces (for example, “DOOR 1” and “DOOR 2”) use the same lock relay (“Lock relay” on page 27), then the one with the lower door number is the Clock On reader and the one with the higher door number is the Clock Off reader.

Using pulsed lock and unlock relays

This option is programmed in “Pulsed lock and unlock relays” on page 26.

This function is only used on special electronic locks that require two separate relays to be pulsed at different times for it to open, and two separate inputs for monitoring. If this function is set to 'Yes', then normal lock-strike opening is disabled. This option should always be set to 'No' unless otherwise specified.

Two relays are required, and are numbered as follows:

- The first relay number is specified in hardware options “Lock relay” on page 27.
- The second relay number is automatically assigned by the Intelligent Controller, which takes the next sequential relay number.

For example, if 1 is entered in Lock Relay, and relay option is set to 'Yes', then relays 1 and 2 are used for the lock.

Two inputs are also required, and are numbered as follows:

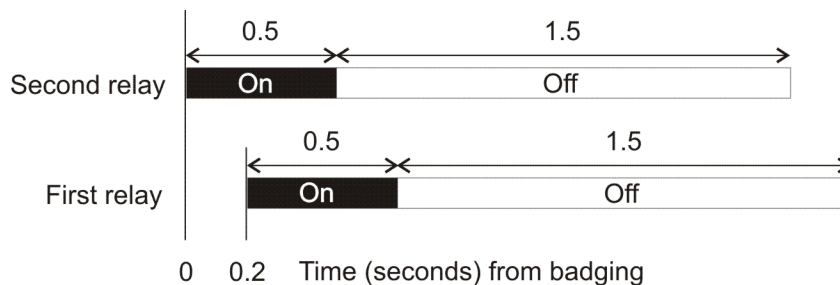
- The first input is for the normal door open contact (for example, reed switch) and is specified in hardware options “Input” on page 27.

- The second input number is used to monitor the door lock state, and is automatically assigned by the Intelligent Controller, which takes the next sequential input number (similar to relays, above).

Door open operation

On presenting a valid user at this reader, the second relay will pulse on for 0.5 sec. After 0.2 sec of the second relay switching on, the first relay will pulse on for 0.5 seconds (refer to Figure 1).

Figure 1: Door open process timing diagram



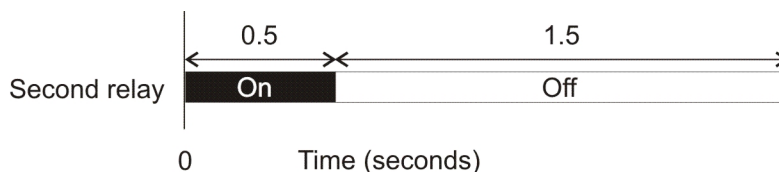
If, according to the input monitoring (explained below), the door has not opened, the process repeats every 1.5 seconds, and ends based on the following:

- Door Open command — the process repeats during the Access Time.
- Door Unlock command — the process repeats until a 'Door Lock' command is sent.

Door lock operation

The second relay will pulse on for 0.5 seconds (refer to Figure 2).

Figure 2: Door lock process timing diagram



If, according to the input monitoring (explained below), the door has not closed, this process repeats until it does.

Input monitoring

The first input is the reed switch, and the second input is from the electronic lock indicating the door lock position.

- 'Door Open' or 'Door Unlock' — The second input is unsealed and the first input is sealed.
- 'Door Lock' — The second input is sealed and the first input is unsealed.

Using regions

A region is a defined access control area having 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.

Depending on the anti-passback settings (see “Anti-passback options” on page 18), the system may:

- Deny access and report an anti-passback violation.
- Allow access and report an anti-passback violation.

Separate programming records are provided for each door’s IN reader and OUT reader. See “IN reader region” on page 19 and “OUT reader region” on page 19.

When a valid card or PIN is entered at the door reader, the number of the region that the user is entering into is recorded against the user code. The range is from region 0 to region 254. Region 0 acts as ‘Off premises’. Region 255 is used for ‘Region disabled’.

Note: The four onboard Wiegand interfaces are, by default, the ‘IN’ readers for the four doors or lifts. You may, however, make two of them function as ‘OUT’ readers by assigning them with the same lock relay (“Lock relay” on page 27) as their IN reader.

For a Challenger10 example (see Table 6 on page 45), Wiegand interface 1 has the ‘Lock Relay’ 1 (Door 21, DGP2) and is the ‘IN’ reader. To set Wiegand interface 2 as the ‘OUT’ reader, set its ‘Lock Relay’ to 1 (same as Wiegand interface 1).

Input and relay numbering

TS0867 and TS0869 Intelligent Controllers have 16 inputs onboard and cannot be expanded. TS0866 Intelligent Controllers have 8 inputs onboard, and may be expanded to 16 inputs via one TS0021 Eight-Input Expansion Module.

The controller’s input and relay numbers depend on the type of Challenger panel to which the controller is connected:

- Challenger10 allocates 32 inputs per DGP address. Intelligent Controllers can only have 16 physical inputs, so inputs 17 to 32 can be used only as logical inputs (for example, as macro inputs).
- Challenger V8 allocates 16 inputs per DGP address, any more make the next higher DGP number unusable. Intelligent Controllers can only have 16 physical inputs, so inputs 17 to 32 can be used only as logical inputs.
- A Challenger10 controller’s input and relay numbers start at 1 regardless of the DGP address.
- A Challenger V8 controller’s input and relay numbers use the Challenger system number, which is based on the DGP address.

Table 5 below lists the LAN number, DGP addressing via the Intelligent Controller's DIP switches, DGP number polled, door or lift numbers, and the input and relay (system) numbers for all applicable DGP addresses.

Table 5: Physical inputs and relays per DGP address

LAN	Address	Polled as	Doors or lifts	Challenger 10 inputs	Challenger V8 inputs	Physical relays
LAN 1	1	DGP 1	17 to 20	17 to 32	17 to 32	17 to 32
LAN 1	2	DGP 2	21 to 24	49 to 64	33 to 48	33 to 48
LAN 1	3	DGP 3	25 to 28	81 to 96	49 to 64	49 to 64
LAN 1	4	DGP 4	29 to 32	113 to 128	65 to 80	65 to 80
LAN 1	5	DGP 5	33 to 36	145 to 160	81 to 96	81 to 96
LAN 1	6	DGP 6	37 to 40	177 to 192	97 to 112	97 to 112
LAN 1	7	DGP 7	41 to 44	209 to 224	113 to 128	113 to 128
LAN 1	8	DGP 8	45 to 48	241 to 256	129 to 144	129 to 144
LAN 1	9	DGP 9	49 to 52	273 to 288	145 to 160	145 to 160
LAN 1	10	DGP 10	53 to 56	305 to 320	161 to 176	161 to 176
LAN 1	11	DGP 11	57 to 60	337 to 352	177 to 192	177 to 192
LAN 1	12	DGP 12	61 to 64	369 to 384	193 to 208	193 to 208
LAN 2	1	DGP 17	81 to 84	497 to 512	N/A	257 to 272
LAN 2	2	DGP 18	85 to 88	529 to 544	N/A	273 to 288
LAN 2	3	DGP 19	89 to 92	561 to 576	N/A	289 to 304
LAN 2	4	DGP 20	93 to 96	593 to 608	N/A	305 to 320
LAN 2	5	DGP 21	97 to 100	625 to 640	N/A	321 to 336
LAN 2	6	DGP 22	101 to 104	657 to 672	N/A	337 to 352
LAN 2	7	DGP 23	105 to 108	689 to 704	N/A	353 to 368
LAN 2	8	DGP 24	109 to 112	721 to 736	N/A	369 to 384
LAN 2	9	DGP 25	113 to 116	753 to 768	N/A	385 to 400
LAN 2	10	DGP 26	117 to 120	785 to 800	N/A	401 to 416
LAN 2	11	DGP 27	121 to 124	817 to 832	N/A	417 to 432
LAN 2	12	DGP 28	125 to 128	849 to 864	N/A	433 to 448

Door/lift hardware defaults

Refer to the following tables of default input and relay numbers for the Intelligent Controller:

- Table 6 on page 45 for Challenger10 numbering.
- Table 7 on page 47 for Challenger V8 numbering

Note: The four onboard lock relays are treated as the first four relay numbers assigned to the DGP address.

Table 6: Challenger10 input and relay defaults (system numbers in brackets)

DGP	Door/Lift	Door input	Spare input	Egress input	DOTL input	Lock relay
1	17	1 (17)	2 (18)	3 (19)	16 (32)	1 (17)
1	18	4 (20)	5 (21)	6 (22)	15 (31)	2 (18)
1	19	7 (23)	8 (24)	9 (25)	14 (30)	3 (19)
1	20	10 (26)	11 (27)	12 (28)	13 (29)	4 (20)
2	21	1 (49)	2 (50)	3 (51)	16 (64)	1 (33)
2	22	4 (52)	5 (53)	6 (54)	15 (63)	2 (34)
2	23	7 (55)	8 (56)	9 (57)	14 (62)	3 (35)
2	24	10 (58)	11 (59)	12 (60)	13 (61)	4 (36)
3	25	1 (81)	2 (82)	3 (83)	16 (96)	1 (49)
3	26	4 (84)	5 (85)	6 (86)	15 (95)	2 (50)
3	27	7 (87)	8 (88)	9 (89)	14 (94)	3 (51)
3	28	10 (90)	11 (91)	12 (92)	13 (93)	4 (52)
4	29	1 (113)	2 (114)	3 (115)	16 (128)	1 (65)
4	30	4 (116)	5 (117)	6 (118)	15 (127)	2 (66)
4	31	7 (119)	8 (120)	9 (121)	14 (126)	3 (67)
4	32	10 (122)	11 (123)	12 (124)	13 (125)	4 (68)
5	33	1 (145)	2 (146)	3 (147)	16 (160)	1 (81)
5	34	4 (148)	5 (149)	6 (150)	15 (159)	2 (82)
5	35	7 (151)	8 (152)	9 (153)	14 (158)	3 (83)
5	36	10 (154)	11 (155)	12 (156)	13 (157)	4 (84)
6	37	1 (177)	2 (178)	3 (179)	16 (192)	1 (97)
6	38	4 (180)	5 (181)	6 (182)	15 (191)	2 (98)
6	39	7 (183)	8 (184)	9 (185)	14 (190)	3 (99)
6	40	10 (186)	11 (187)	12 (188)	13 (189)	4 (100)
7	41	1 (209)	2 (210)	3 (211)	16 (224)	1 (113)
7	42	4 (212)	5 (213)	6 (214)	15 (223)	2 (114)
7	43	7 (215)	8 (216)	9 (217)	14 (222)	3 (115)
7	44	10 (218)	11 (219)	12 (220)	13 (221)	4 (116)
8	45	1 (241)	2 (242)	3 (243)	16 (256)	1 (129)
8	46	4 (244)	5 (245)	6 (246)	15 (255)	2 (130)
8	47	7 (247)	8 (248)	9 (249)	14 (254)	3 (131)
8	48	10 (250)	11 (251)	12 (252)	13 (253)	4 (132)
9	49	1 (273)	2 (274)	3 (275)	16 (288)	1 (145)
9	50	4 (276)	5 (277)	6 (278)	15 (287)	2 (146)
9	51	7 (279)	8 (280)	9 (281)	14 (286)	3 (147)
9	52	10 (282)	11 (283)	12 (284)	13 (285)	4 (148)

DGP	Door/Lift	Door input	Spare input	Egress input	DOTL input	Lock relay
10	53	1 (305)	2 (306)	3 (307)	16 (320)	1 (161)
10	54	4 (308)	5 (309)	6 (310)	15 (319)	2 (162)
10	55	7 (311)	8 (312)	9 (313)	14 (318)	3 (163)
10	56	10 (314)	11 (315)	12 (316)	13 (317)	4 (164)
11	57	1 (337)	2 (338)	3 (339)	16 (352)	1 (177)
11	58	4 (340)	5 (341)	6 (342)	15 (351)	2 (178)
11	59	7 (343)	8 (344)	9 (345)	14 (350)	3 (179)
11	60	10 (346)	11 (347)	12 (348)	13 (349)	4 (180)
12	61	1 (369)	2 (370)	3 (371)	16 (384)	1 (193)
12	62	4 (372)	5 (373)	6 (374)	15 (383)	2 (194)
12	63	7 (375)	8 (376)	9 (377)	14 (382)	3 (195)
12	64	10 (378)	11 (379)	12 (380)	13 (381)	4 (196)
17	81	1 (497)	2 (498)	3 (499)	16 (512)	1 (257)
17	82	4 (500)	5 (501)	6 (502)	15 (511)	2 (258)
17	83	7 (503)	8 (504)	9 (505)	14 (510)	3 (259)
17	84	10 (506)	11 (507)	12 (508)	13 (509)	4 (260)
18	85	1 (529)	2 (530)	3 (531)	16 (544)	1 (273)
18	86	4 (532)	5 (533)	6 (534)	15 (543)	2 (274)
18	87	7 (535)	8 (536)	9 (537)	14 (542)	3 (275)
18	88	10 (538)	11 (539)	12 (540)	13 (541)	4 (276)
19	89	1 (561)	2 (562)	3 (563)	16 (576)	1 (289)
19	90	4 (564)	5 (565)	6 (566)	15 (575)	2 (290)
19	91	7 (567)	8 (568)	9 (569)	14 (574)	3 (291)
19	92	10 (570)	11 (571)	12 (572)	13 (573)	4 (292)
20	93	1 (593)	2 (594)	3 (595)	16 (608)	1 (305)
20	94	4 (596)	5 (597)	6 (598)	15 (607)	2 (306)
20	95	7 (599)	8 (600)	9 (601)	14 (606)	3 (307)
20	96	10 (602)	11 (603)	12 (604)	13 (605)	4 (308)
21	97	1 (625)	2 (626)	3 (627)	16 (640)	1 (321)
21	98	4 (628)	5 (629)	6 (630)	15 (639)	2 (322)
21	99	7 (631)	8 (632)	9 (633)	14 (638)	3 (323)
21	100	10 (634)	11 (635)	12 (636)	13 (637)	4 (324)
22	101	1 (657)	2 (658)	3 (659)	16 (672)	1 (337)
22	102	4 (660)	5 (661)	6 (662)	15 (671)	2 (338)
22	103	7 (663)	8 (664)	9 (665)	14 (670)	3 (339)
22	104	10 (666)	11 (667)	12 (668)	13 (669)	4 (340)
23	105	1 (689)	2 (690)	3 (691)	16 (704)	1 (353)
23	106	4 (692)	5 (693)	6 (694)	15 (703)	2 (354)

DGP	Door/Lift	Door input	Spare input	Egress input	DOTL input	Lock relay
23	107	7 (695)	8 (696)	9 (697)	14 (702)	3 (355)
23	108	10 (698)	11 (699)	12 (700)	13 (701)	4 (356)
24	109	1 (721)	2 (722)	3 (723)	16 (736)	1 (369)
24	110	4 (724)	5 (725)	6 (726)	15 (735)	2 (370)
24	111	7 (727)	8 (728)	9 (729)	14 (734)	3 (371)
24	112	10 (730)	11 (731)	12 (732)	13 (733)	4 (372)
25	113	1 (753)	2 (754)	3 (755)	16 (768)	1 (385)
25	114	4 (756)	5 (757)	6 (758)	15 (767)	2 (386)
25	115	7 (759)	8 (760)	9 (761)	14 (766)	3 (387)
25	116	10 (762)	11 (763)	12 (764)	13 (765)	4 (388)
26	117	1 (785)	2 (786)	3 (787)	16 (800)	1 (401)
26	118	4 (788)	5 (789)	6 (790)	15 (799)	2 (402)
26	119	7 (791)	8 (792)	9 (793)	14 (798)	3 (403)
26	120	10 (974)	11 (975)	12 (796)	13 (797)	4 (404)
27	121	1 (817)	2 (818)	3 (819)	16 (832)	1 (417)
27	122	4 (820)	5 (821)	6 (822)	15 (831)	2 (418)
27	123	7 (823)	8 (824)	9 (825)	14 (830)	3 (419)
27	124	10 (826)	11 (827)	12 828()	13 (829)	4 (420)
28	125	1 (849)	2 (850)	3 (851)	16 (864)	1 (433)
28	126	4 (852)	5 (853)	6 (854)	15 (863)	2 (434)
28	127	7 (855)	8 (856)	9 (857)	14 (862)	3 (435)
28	128	10 (858)	11 (859)	12 (860)	13 (861)	4 (436)

Table 7: Challenger V8 input and relay defaults

DGP	Door/Lift	Door input	Spare input	Egress input	DOTL input	Lock relay
1	17	17	18	19	32	17
1	18	20	21	22	31	18
1	19	23	24	25	30	19
1	20	26	27	28	29	20
2	21	33	34	35	48	33
2	22	36	37	38	47	34
2	23	39	40	41	46	35
2	24	42	43	44	45	36
3	25	49	50	51	64	49
3	26	52	53	54	63	50
3	27	55	56	57	62	51
3	28	58	59	60	61	52

DGP	Door/Lift	Door input	Spare input	Egress input	DOTL input	Lock relay
4	29	65	66	67	80	65
4	30	68	69	70	79	66
4	31	71	72	73	78	67
4	32	74	75	76	77	68
5	33	81	82	83	96	81
5	34	84	85	86	95	82
5	35	87	88	89	94	83
5	36	90	91	92	93	84
6	37	97	98	99	112	97
6	38	100	101	102	111	98
6	39	103	104	105	110	99
6	40	106	107	108	109	100
7	41	113	114	115	128	113
7	42	116	117	118	127	114
7	43	119	120	121	126	115
7	44	122	123	124	125	116
8	45	129	130	131	144	129
8	46	132	133	134	143	130
8	47	135	136	137	142	131
8	48	138	139	140	141	132)
9	49	145	146	147	160	145
9	50	148	149	150	159	146
9	51	151	152	153	158	147
9	52	154	155	156	157	148
10	53	161	162	163	176	161
10	54	164	165	166	175	162
10	55	167	168	169	174	163
10	56	170	171	172	173	164
11	57	177	178	179	192	177
11	58	180	181	182	191	178
11	59	183	184	185	190	179
11	60	186	187	188	189	180
12	61	193	194	195	208	193
12	62	196	197	198	207	194
12	63	199	200	201	206	195
12	64	202	203	204	205	196

Table 8: Four-Lift Controller floor, input and relay defaults

	First lift	Second lift	Third lift	Fourth lift
Starting floor	1	1	1	1
Last floor	64	64	64	64
Starting relay	1	65	129	193
Starting input	1	65	129	193

Macro event flags

Refer to the following tables:

- Table 9: Door and floor macro event flag descriptions below.
- Table 10: Door and floor macro event flag programming on page 50.
- Table 11: Other macro event flag programming on page 52.

Table 9: Door and floor macro event flag descriptions

Name	Description
DOOR OPEN	Door Open command is active (to unlock / start shunt)
DOOR UNLOCKED	Lock output is active to unlock the door
DOOR LOCK	Lock output is de-activated to lock the door
DOOR OVERRIDE	The override time zone assigned to the door is valid
* DOOR OVERRIDE INHIBIT	The override time zone is inhibited
DOOR DISABLED	Door is disabled completely (from keypad or computer)
DOOR ENABLED	Door is enabled
# DOOR READER DISABLED	Reader is disabled
DOOR READER ENABLED	Reader is enabled
** DOOR DUAL CUSTODY INSIDE	Dual Custody access is required at the "IN" reader
** DOOR DUAL CUSTODY OUTSIDE	Dual Custody access is required at the "OUT" reader
** DOOR LOW SECURITY INSIDE	Card and PIN required to access at the "IN" reader
** DOOR LOW SECURITY OUTSIDE	Card and PIN required to access at the "OUT" reader
** DOOR ANTI PASSBACK	Anti Passback is active
DOOR SHUNTING	Shunt timer is running
DOOR SHUNT WARNING	Shunt warning timer is running
DOOR AREA SECURE	Area assigned to door is secure.
DOOR INTERLOCK	Interlock input(s) are unsealed
* DOOR INTERLOCK OVERRIDE	If the interlock has been overridden
*** DOOR KEYPAD DURESS	Duress PIN code entered at door keypad
*** DOOR READER FAULT	Fault detected on reader (Comms / tamper / etc)
*** DOOR LOCK FAULT	Cable tamper / fault detected on lock relay wiring
DOOR DOTL	Door Contact is unsealed after shunt timer has expired

Name	Description
DOOR FORCED	Door Contact is unsealed with no valid door command
*** DOOR LED 1	LED 1 output is active
*** DOOR LED 2	LED 2 output is active
*** DOOR BUZZER	BUZZER output is active
DOOR RANDOM BIT	An event is generated at random when the door is accessed
DOOR ACCESS DENIED	Door access has not been allowed
DOOR ACCESS GRANTED	Door access has been allowed
DOOR ACCESS GRANTED TRACED	Door access has been granted to a user with trace On
DOOR ACCESS GRANTED 1ST BADGED	Door access has been granted when badged once
DOOR ACCESS GRANTED 2ND BADGED	Door access has been granted when badged twice
DOOR ACCESS GRANTED 3RD BADGED	Door access has been granted when badged three times
DOOR ACCESS GRANTED IN BUTTON	Door access has been granted and IN button pressed
DOOR ACCESS GRANTED OUT BUTTON	Door access has been granted and OUT button pressed
DOOR FIRE OVERRIDE	Secondary override is active
DOOR SECURE	When the door is LOCKED and the door is CLOSED.
*** FLOOR ACCESSED	Free access available to floor (64 events, 1 per floor)
*** FLOOR CALL BUTTON	Floor selection button pressed (64 events, 1 per floor)
*** FLOOR DISABLED	Floor is disabled from being selected (64 events, 1 per floor)
*** FLOOR LANDED	Floor where lift car is currently landed (64 events, 1 per floor)
*** FLOOR SEND	Command to send lift car to floor (64 events, 1 per floor)

* Denotes rule can only be activated as a result of another door macro.

** Denotes rule can only be activated as a result of another door macro and the function of the door (the macro input is always true if the function is set in the programming)

*** Denotes the event is currently not enabled.

User with the 'Privilege' attribute set can override the 'Reader disabled' function.

Table 10: Door and floor macro event flag programming

Name	Input	Output	D1	D2	D3	D4
DOOR OPEN	Yes	Yes	1	2	3	4
DOOR UNLOCKED	Yes	Yes	9	10	11	12
DOOR LOCK	No	Yes	17	18	19	20
DOOR OVERRIDE	Yes	Yes	25	26	27	28
* DOOR OVERRIDE INHIBIT	Yes	Yes	33	34	35	36
DOOR DISABLED	Yes	Yes	41	42	43	44
DOOR ENABLED	No	Yes	49	50	51	52
# DOOR READER DISABLED	Yes	Yes	57	58	59	60

Name	Input	Output	D1	D2	D3	D4
DOOR READER ENABLED	No	Yes	65	66	67	68
** DOOR DUAL CUSTODY INSIDE	Yes	Yes	73	74	75	76
** DOOR DUAL CUSTODY OUTSIDE	Yes	Yes	81	82	83	84
** DOOR LOW SECURITY INSIDE	Yes	Yes	89	90	91	92
** DOOR LOW SECURITY OUTSIDE	Yes	Yes	97	98	99	100
** DOOR ANTI PASSBACK	Yes	Yes	105	106	107	108
DOOR SHUNTING	Yes	Yes	113	114	115	116
DOOR SHUNT WARNING	Yes	No	121	122	123	124
DOOR AREA SECURE	Yes	Yes	129	130	131	132
DOOR INTERLOCK	Yes	Yes	137	138	139	140
* DOOR INTERLOCK OVERRIDE	Yes	Yes	145	146	147	148
*** DOOR KEYPAD DURESS	Yes	No	153	154	155	156
*** DOOR READER FAULT	Yes	No	161	162	163	164
*** DOOR LOCK FAULT	Yes	No	169	170	171	172
DOOR DOTL	Yes	No	177	178	179	180
DOOR FORCED	Yes	No	185	186	187	188
*** DOOR LED 1	Yes	Yes	193	194	195	196
*** DOOR LED 2	Yes	Yes	201	202	203	204
*** DOOR BUZZER	Yes	Yes	209	210	211	212
DOOR RANDOM BIT	Yes	No	217	218	219	220
DOOR ACCESS DENIED	Yes	No	225	226	227	228
DOOR ACCESS GRANTED	Yes	No	233	234	235	236
DOOR ACCESS GRANTED TRACED	Yes	No	241	242	243	244
DOOR ACCESS GRANTED 1ST BADGED	Yes	No	249	250	251	252
DOOR ACCESS GRANTED 2ND BADGED	Yes	No	257	258	259	260
DOOR ACCESS GRANTED 3RD BADGED	Yes	No	265	266	267	268
DOOR ACCESS GRANTED IN BUTTON	Yes	No	273	274	275	276
DOOR ACCESS GRANTED OUT BUTTON	Yes	No	281	282	283	284
DOOR FIRE OVERRIDE	Yes	Yes	289	290	291	292
DOOR SECURE	Yes		297	298	299	300
*** FLOOR ACCESSED	Yes	Yes	1537– 1600	1601– 1664	1665– 1728	1729– 1792
*** FLOOR CALL BUTTON	Yes	No	2049– 2112	2113– 2176	2177– 2240	2241– 2304
*** FLOOR DISABLED	Yes	No	2561– 2624	2625– 2688	2689– 2752	2753– 2816
*** FLOOR LANDED	Yes	No	3073– 3136	3137– 3200	3201– 3264	3265– 3328
*** FLOOR SEND	No	Yes	3585– 3648	3649– 3712	3713– 3776	3777– 3840

Name	Input	Output	D1	D2	D3	D4
* Denotes rule can only be activated as a result of another door macro.						
** Denotes rule can only be activated as a result of another door macro and the function of the door (the macro input is always true if the function is set in the programming)						
*** Denotes the event is currently not enabled.						
# User with the 'Privileged' attribute set can override the 'Reader disabled' function.						

Table 11: Other macro event flag programming

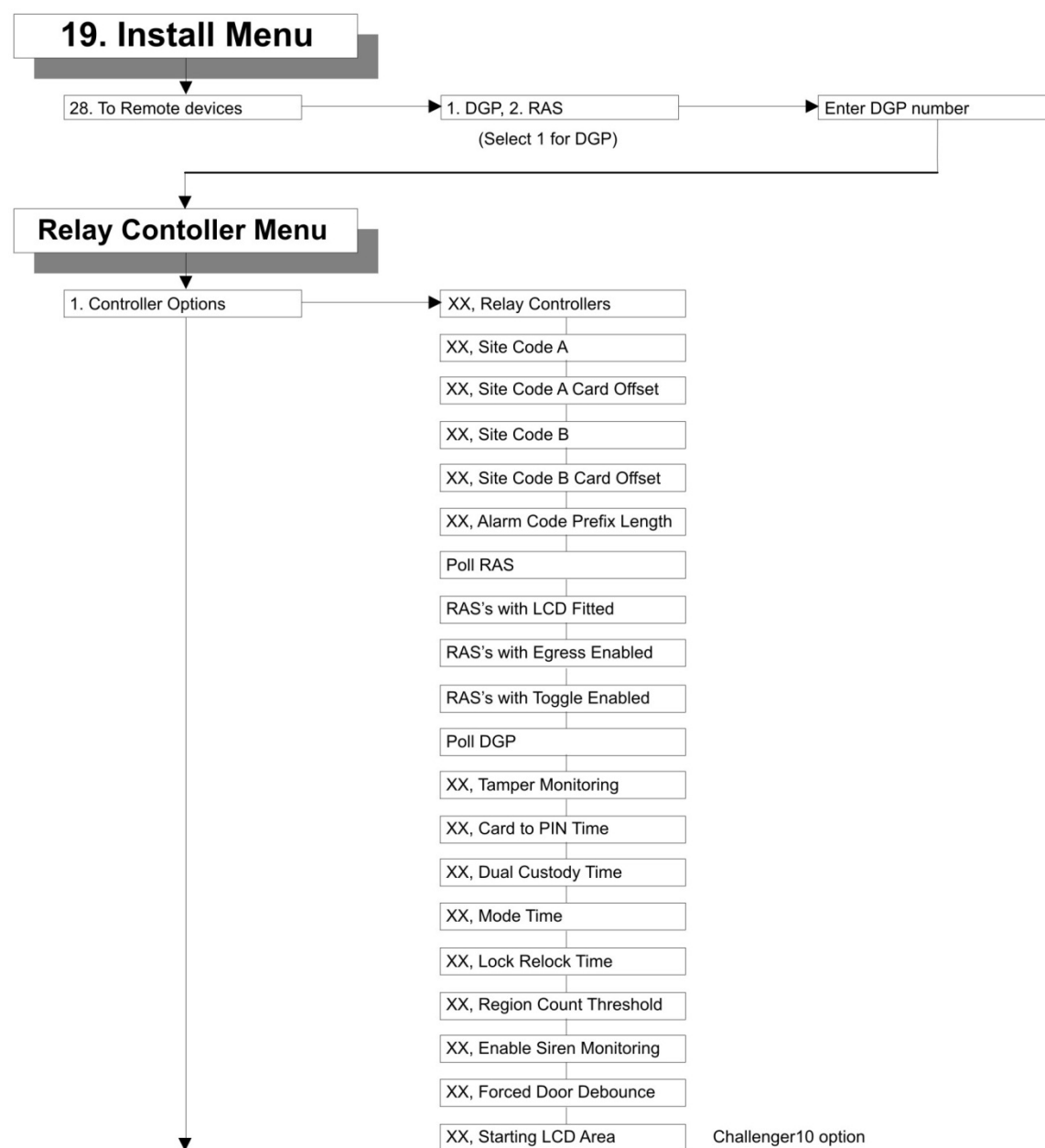
Name	Description	Input	Output	Event numbers
Area Access (Challenger10)	Area in access (99 events, 1 per area)	Yes	No	4091 to 4189
Area Alarm (Challenger10)	Input(s) in alarm in area (99 events, 1 per area)	Yes	No	4190 to 4288
Area Access (Challenger V8)	Area in access (16 events, 1 per area)	Yes	No	513–528
Area Alarm (Challenger V8)	Input(s) in alarm in area (16 events - 1 per area)	Yes	No	529–544
* Area Isolated	Input(s) isolated in area (16 events, 1 per area)	Yes	No	545–560
* Area Unsealed	Input(s) unsealed in area (16 events, 1 per area)	Yes	No	561–576
DGP Relays	System relay assigned to this DGP is active (16 events, 1 per relay). The first 16 relays on DGP can also be activated by physical relay function.	Yes	No	577–592
RAS Offline	RAS on Intelligent Controller sub-LAN is offline (16 events, 1 per RAS address)	Yes	No	593–608
DGP Offline	DGP on Intelligent Controller sub-LAN is offline.	Yes	No	609–624
Inputs	Input on this DGP is unsealed (16 events, 1 per input)	Yes	Yes	769–784
*Auxiliary 1 Input Event	Special interface required. (32 events)	Yes	No	801–832
*Auxiliary 2 Input Event	Special interface required. (32 events)	Yes	No	833–864
*Auxiliary 3 Input Event	Special interface required. (32 events)	Yes	No	865–896
*Auxiliary 4 Input Event	Special interface required. (32 events)	Yes	No	897–928
Region Limit	When the number of people in any region reaches the present limit (255 events, 1 per region)	Yes	No	1025–1280
Physical Relays	Relay connected to this DGP is active (255 events, 1 per relay). If the physical relay is numbered higher than the first 16 in the DGP, then it can only be activated by door macro.	Yes	Yes	1281–1536
* Controller Mains Fail	Mains fail condition exists on the Controller (1 event)	Yes	No	4081

Name	Description	Input	Output	Event numbers
* Controller Low Battery	Low battery condition exists on the Controller (1 event)	Yes	No	4082
* Controller Battery Test Active	The battery test on this Controller is running (1 event)	Yes	No	4083
* Controller Battery Test Fail	The battery test failed on this Controller (1 event)	Yes	No	4084
* Controller Fuse Fail	Fuse Fail condition exists on the Controller (1 event)	Yes	No	4085
* Controller Siren Fail	Siren fail (siren tamper) condition exists on this Controller (1 event)	Yes	No	4086
* Controller Siren Active	The siren output (16th relay) is active (1 event)	Yes	No	4087
* Controller Tamper	Cabinet tamper condition exists on this Controller (1 event)	Yes	No	4088
* Controller DGP Offline	Controller is not communicating with the Challenger (1 event)	Yes	No	4089

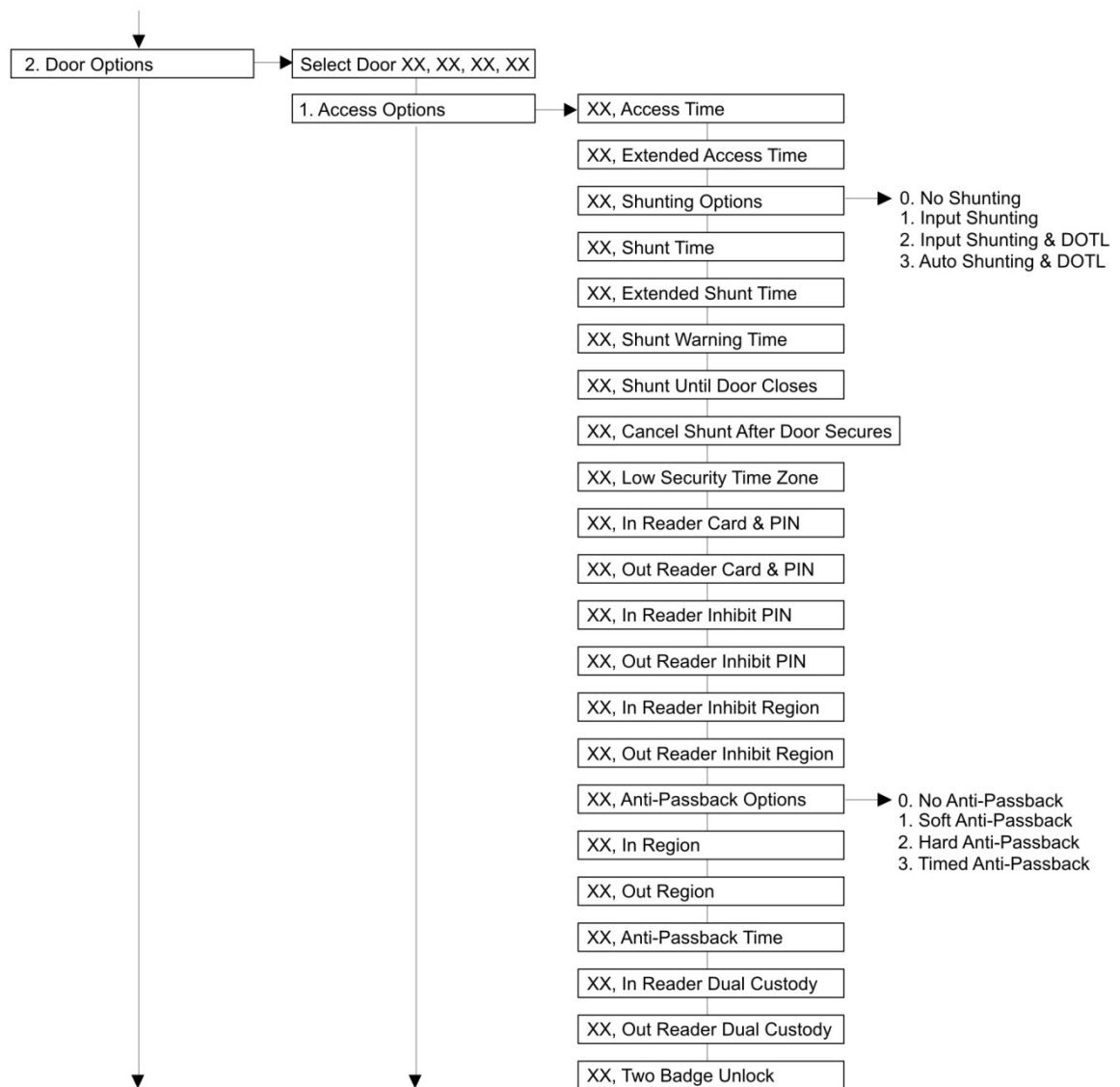
* Denotes the event is currently not enabled.

Programming map

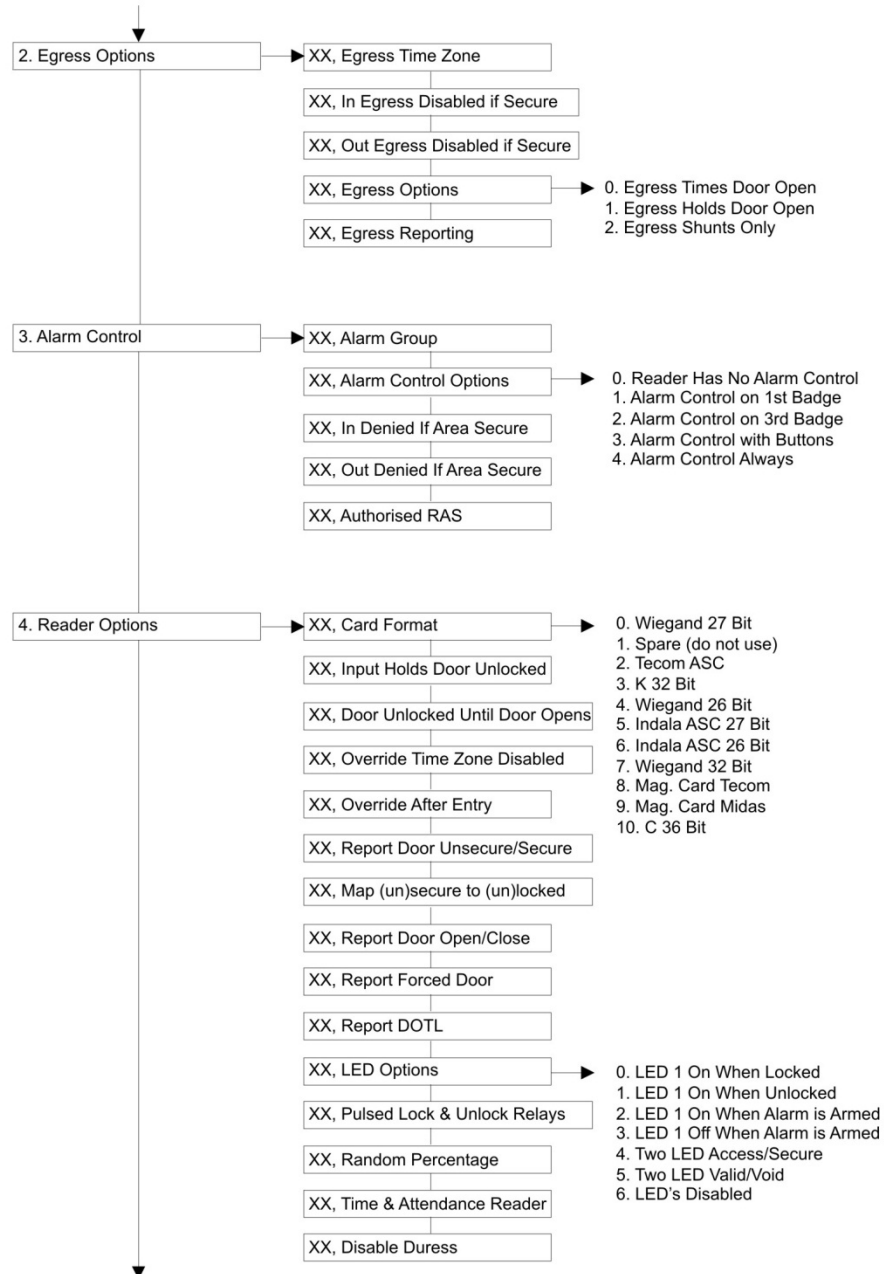
The Relay Controller Menu numbers correspond with heading numbers in this manual (for example, “1. Controller Options” below corresponds with “Option 1 – Controller options” on page 8). The characters “XX” represent the number of the selected device.



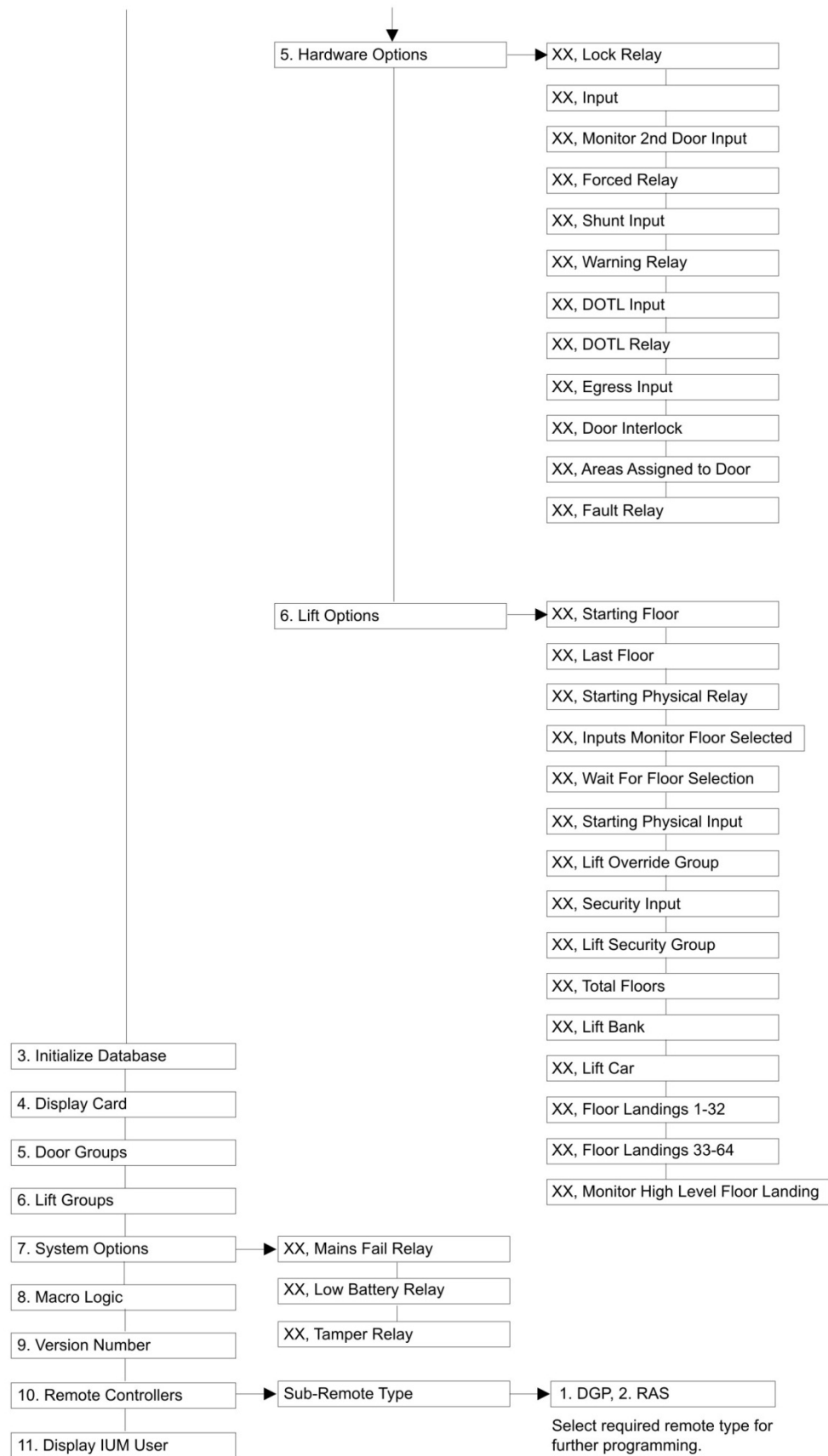
Continued...



Continued...



Continued...



Appendix B. Programming worksheets

Introduction

As stated in “Programming via a RAS” on page 3, this manual is based on the programming options as displayed on an LCD RAS. However, this appendix is also based on the programming options as displayed in system management software (SMS).

The reason for this difference is that programming is typically done via the graphical user interface of SMS instead of the text-based user interface of a RAS. As a result, the options listed in the worksheets may not appear in the same order as listed on a RAS, and the option names may vary slightly.

Controller and system options worksheet

Refer to “Option 1 – Controller options” on page 8 and “Option 7 – System options” on page 35 for details.

Figure 3: Controller and system options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional	Controller and System Options													
Relay controllers Range 0 to 8		Region count threshold Range 0 to 65,535		Alarm code prefix length System-wide value												
Challenger V8 options																
Site code A		Offset		Site code B												
		Offset														
Mark check boxes to indicate YES ☒ Tamper (input fault) monitoring ☐ Siren monitoring ☐																
Card to PIN time Default 8 s		☐ S ☐ M	Mode time Default 5 s		☐ S ☐ M											
Lock release time Default 3 s		☐ S ☐ M	Forced door debounce Default 700 ms		Starting LCD area Challenger10 only											
RAS & DGP options																
	First IN reader				Second IN reader				First OUT reader				Second OUT reader			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Poll RAS	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
RAS with LCD	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
RAS egress input	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Toggle RAS	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Poll DGP (lift controllers only)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
System Options																
Mains fail relay																
Low battery relay																
Tamper relay																

Door/lift access options worksheet

Refer to “Door/lift access options” on page 14 for details.

Figure 4: Door/lift access options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional	Door/Lift Access Options			
Mark check boxes to indicate YES ☒			First	Second	Third	Fourth
Doors ☐	Lifts ☐	Door or lift numbers:				
Programming item		Door/lift defaults				
Access time		5 s/5 s				
Extended access time		10 s/10 s				
Shunting options, select one:	No shunting	Default	☐	☐	☐	☐
	Input Shunting		☐	☐	☐	☐
	Input Shunting & DOTL		☐	☐	☐	☐
	Auto Shunting & DOTL		☐	☐	☐	☐
Shunt time		60 s/0 s				
Extended shunt time		90 s/0 s				
Shunt warning time		15 s/0 s				
Shunt until door closes		No/No				
Cancel shunt when door closes		No/No				
Low security timezone		Disabled				
IN reader region		Disabled				
OUT reader region		Disabled				
Anti-passback options, select one:	Disabled	Default	☐	☐	☐	☐
	Soft		☐	☐	☐	☐
	Hard		☐	☐	☐	☐
	Timed hard		☐	☐	☐	☐
Anti-passback time		0 s/0 s				
IN reader options:	Card plus PIN	No/No	☐	☐	☐	☐
	Inhibit PIN	No/No	☐	☐	☐	☐
	Dual custody	No/No	☐	☐	☐	☐
	Inhibit offsite users	No/No	☐	☐	☐	☐
OUT reader options:	Card plus PIN	No/No	☐	☐	☐	☐
	Inhibit PIN	No/No	☐	☐	☐	☐
	Dual custody	No/No	☐	☐	☐	☐
	Inhibit offsite users	No/No	☐	☐	☐	☐
(Requires firmware R-150411.801 or later)	Two badge unlock	No/No	☐	☐	☐	☐

Door/lift egress options worksheet

Refer to “Door/lift egress options” on page 20 for details.

Figure 5: Door/lift egress options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional		Door/Lift Egress Options			
Mark check boxes to indicate YES ☒				First	Second	Third	Fourth
Doors ☐ Lifts ☐		Door or lift numbers:					
Programming item		Door/lift defaults					
Egress time zone		0/Disabled					
Egress options, select one:	Egress times door open	Yes/Yes	☐	☐	☐	☐	☐
	Egress holds door open	No/No	☐	☐	☐	☐	☐
	Egress shunts only	No/No	☐	☐	☐	☐	☐
	In egress disabled if secure	No/No	☐	☐	☐	☐	☐
Out egress disabled if secure		No/No	☐	☐	☐	☐	☐
Egress reporting		No/No	☐	☐	☐	☐	☐

Door/lift alarm control options worksheet

Refer to “Door/lift alarm control options” on page 21 for details.

Figure 6: Door/lift alarm control options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional		Door/Lift Alarm Control Options			
Mark check boxes to indicate YES ☒				First	Second	Third	Fourth
Doors ☐ Lifts ☐		Door or lift numbers:					
Programming item		Door/lift defaults					
Alarm group		1/1					
Alarm control, select one:	No alarm control	Default	☐	☐	☐	☐	☐
	Alarm control on 1st badge		☐	☐	☐	☐	☐
	Alarm control on 3rd badge		☐	☐	☐	☐	☐
	Alarm control with button int.		☐	☐	☐	☐	☐
	Alarm control always		☐	☐	☐	☐	☐
Authorised RAS		No/No	☐	☐	☐	☐	☐
In denied if area secured		No/No	☐	☐	☐	☐	☐
Out denied if area secured		No/No	☐	☐	☐	☐	☐

Door/lift reader options worksheet

Refer to “Door/lift reader options” on page 23 for details.

Figure 7: Door/lift reader options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional	Door/Lift Reader Options			
Mark check boxes to indicate YES ☒			First	Second	Third	Fourth
Doors ☐	Lifts ☐	Door or lift numbers:				
Card format, select one:	Programming item	Door/lift defaults				
	Wiegand 27 bit	Default	☐	☐	☐	☐
	Tecom ASC		☐	☐	☐	☐
	K 32 bit		☐	☐	☐	☐
	Wiegand 26 bit		☐	☐	☐	☐
	Indala ASC 27 bit		☐	☐	☐	☐
	Indala ASC 26 bit		☐	☐	☐	☐
	Wiegand 32 bit		☐	☐	☐	☐
	Mag. Card Tecom		☐	☐	☐	☐
	Mag. Card Midas		☐	☐	☐	☐
	C36 bit		☐	☐	☐	☐
	Override time zone	Disabled	☐	☐	☐	☐
	Random event percentage	0/0	☐	☐	☐	☐
Wiegand reader LED options, select one:	LED options	Door/lift defaults				
	LED on when door locked	Default	☐	☐	☐	☐
	LED on when door unlocked		☐	☐	☐	☐
	LED on when area accessed		☐	☐	☐	☐
	Two LEDs access/secure		☐	☐	☐	☐
	Two LEDs valid/void		☐	☐	☐	☐
	No LEDs		☐	☐	☐	☐
	Input holds door unlocked	No/No	☐	☐	☐	☐
	Override after entry	No/No	☐	☐	☐	☐
	Report door open/close	No/No	☐	☐	☐	☐
	Report forced door	No/No	☐	☐	☐	☐
	Hold door unlocked until door opens	No/No	☐	☐	☐	☐
	Report door unsecured/secure	No/No	☐	☐	☐	☐
	Report DOTL	No/No	☐	☐	☐	☐
	Time & attendance reader	No/No	☐	☐	☐	☐
	Pulsed lock & unlock	No/No	☐	☐	☐	☐
	Disable duress	No/No	☐	☐	☐	☐
	Map unsecured/secured to unlocked/locked	No/No	☐	☐	☐	☐

Door/lift hardware options worksheet

Refer to “Door/lift hardware options” on page 27 for details.

Figure 8: Door/lift hardware options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional	Door/Lift Hardware Options			
Mark check boxes to indicate YES ☒			First	Second	Third	Fourth
Doors ☐	Lifts ☐	Door or lift numbers:				
Programming item	Door/lift defaults					
Lock relay number	Default relay number/Disabled					
Forced relay number	Disabled/Disabled					
Warning relay number	Disabled/Disabled					
DOTL input number	Default input number/Disabled					
DOTL relay number	Disabled/Disabled					
Egress input number	Default input number/Disabled					
Input number	Default input number/Disabled					
Monitor 2nd door input	No/No		☐	☐	☐	☐

Also assign inputs and areas via Figure 9 on page 63.

Figure 9: Door/lift hardware inputs and areas worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)	Description Optional	Door/Lift Hardware Options Input and Area assignments
Mark check boxes to indicate YES ☒		
First door/lift		
Shunt inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Interlock inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Areas	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
	☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32	
	☐ 33 ☐ 34 ☐ 35 ☐ 36 ☐ 37 ☐ 38 ☐ 39 ☐ 40 ☐ 41 ☐ 42 ☐ 43 ☐ 44 ☐ 45 ☐ 46 ☐ 47 ☐ 48	
	☐ 49 ☐ 50 ☐ 51 ☐ 52 ☐ 53 ☐ 54 ☐ 55 ☐ 56 ☐ 57 ☐ 58 ☐ 59 ☐ 60 ☐ 61 ☐ 62 ☐ 63 ☐ 64	
	☐ 65 ☐ 66 ☐ 67 ☐ 68 ☐ 69 ☐ 70 ☐ 71 ☐ 72 ☐ 73 ☐ 74 ☐ 75 ☐ 76 ☐ 77 ☐ 78 ☐ 79 ☐ 80	
	☐ 81 ☐ 82 ☐ 83 ☐ 84 ☐ 85 ☐ 86 ☐ 87 ☐ 88 ☐ 89 ☐ 90 ☐ 91 ☐ 92 ☐ 93 ☐ 94 ☐ 95 ☐ 96	
	☐ 97 ☐ 98 ☐ 99	
Second door/lift		
Shunt inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Interlock inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Areas	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
	☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32	
	☐ 33 ☐ 34 ☐ 35 ☐ 36 ☐ 37 ☐ 38 ☐ 39 ☐ 40 ☐ 41 ☐ 42 ☐ 43 ☐ 44 ☐ 45 ☐ 46 ☐ 47 ☐ 48	
	☐ 49 ☐ 50 ☐ 51 ☐ 52 ☐ 53 ☐ 54 ☐ 55 ☐ 56 ☐ 57 ☐ 58 ☐ 59 ☐ 60 ☐ 61 ☐ 62 ☐ 63 ☐ 64	
	☐ 65 ☐ 66 ☐ 67 ☐ 68 ☐ 69 ☐ 70 ☐ 71 ☐ 72 ☐ 73 ☐ 74 ☐ 75 ☐ 76 ☐ 77 ☐ 78 ☐ 79 ☐ 80	
	☐ 81 ☐ 82 ☐ 83 ☐ 84 ☐ 85 ☐ 86 ☐ 87 ☐ 88 ☐ 89 ☐ 90 ☐ 91 ☐ 92 ☐ 93 ☐ 94 ☐ 95 ☐ 96	
	☐ 97 ☐ 98 ☐ 99	
Third door/lift		
Shunt inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Interlock inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Areas	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
	☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32	
	☐ 33 ☐ 34 ☐ 35 ☐ 36 ☐ 37 ☐ 38 ☐ 39 ☐ 40 ☐ 41 ☐ 42 ☐ 43 ☐ 44 ☐ 45 ☐ 46 ☐ 47 ☐ 48	
	☐ 49 ☐ 50 ☐ 51 ☐ 52 ☐ 53 ☐ 54 ☐ 55 ☐ 56 ☐ 57 ☐ 58 ☐ 59 ☐ 60 ☐ 61 ☐ 62 ☐ 63 ☐ 64	
	☐ 65 ☐ 66 ☐ 67 ☐ 68 ☐ 69 ☐ 70 ☐ 71 ☐ 72 ☐ 73 ☐ 74 ☐ 75 ☐ 76 ☐ 77 ☐ 78 ☐ 79 ☐ 80	
	☐ 81 ☐ 82 ☐ 83 ☐ 84 ☐ 85 ☐ 86 ☐ 87 ☐ 88 ☐ 89 ☐ 90 ☐ 91 ☐ 92 ☐ 93 ☐ 94 ☐ 95 ☐ 96	
	☐ 97 ☐ 98 ☐ 99	
Fourth door/lift		
Shunt inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Interlock inputs	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
Areas	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16	
	☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32	
	☐ 33 ☐ 34 ☐ 35 ☐ 36 ☐ 37 ☐ 38 ☐ 39 ☐ 40 ☐ 41 ☐ 42 ☐ 43 ☐ 44 ☐ 45 ☐ 46 ☐ 47 ☐ 48	
	☐ 49 ☐ 50 ☐ 51 ☐ 52 ☐ 53 ☐ 54 ☐ 55 ☐ 56 ☐ 57 ☐ 58 ☐ 59 ☐ 60 ☐ 61 ☐ 62 ☐ 63 ☐ 64	
	☐ 65 ☐ 66 ☐ 67 ☐ 68 ☐ 69 ☐ 70 ☐ 71 ☐ 72 ☐ 73 ☐ 74 ☐ 75 ☐ 76 ☐ 77 ☐ 78 ☐ 79 ☐ 80	
	☐ 81 ☐ 82 ☐ 83 ☐ 84 ☐ 85 ☐ 86 ☐ 87 ☐ 88 ☐ 89 ☐ 90 ☐ 91 ☐ 92 ☐ 93 ☐ 94 ☐ 95 ☐ 96	
	☐ 97 ☐ 98 ☐ 99	

Lift options worksheet

Refer to “Lift options” on page 30 for details.

Figure 10: Lift options worksheet

DGP address 1 to 12 and 17 to 28 (Challenger10)		Description Optional					Lift Options
Mark check boxes to indicate YES ☒		Lift numbers:					
Programming item	Defaults						
Lift override group	Disabled						
Lift security group	Disabled						
Security input	Disabled						
Starting floor	1						
Last floor	64						
Starting physical relay	Disabled						
Starting physical input	Disabled						
Lift bank	Disabled						
Lift car	Disabled						
Total floors	0						
Inputs monitor floor	No	☐	☐	☐	☐	☐	☐
Monitor high level floor landings	No	☐	☐	☐	☐	☐	☐
Wait for floor selection	No	☐	☐	☐	☐	☐	☐
Floor landings for each lift							
First lift		Second lift					
All ☐ Or as marked:	1 8 9 16 17 24 25 32 33 40 41 48 49 56 57 64	All ☐ Or as marked:	1 8 9 16 17 24 25 32 33 40 41 48 49 56 57 64				
Third lift		Fourth lift					
All ☐ Or as marked:	1 8 9 16 17 24 25 32 33 40 41 48 49 56 57 64	All ☐ Or as marked:	1 8 9 16 17 24 25 32 33 40 41 48 49 56 57 64				

DGP macro logic worksheet

Refer to “Option 8 – Macro logic” on page 36 for details.

Figure 11: DGP macro logic worksheet

DGP address		Description	DGP Macro Logic
1 to 12 and 17 to 28 (Challenger10)		Optional	
Mark check boxes to indicate YES ☒			
Macro logic program number		Macro or output description	
Range 1 to 48		Optional	
Output event flag number		Invert output	☐
Disabled	☐	Non-timed	☐
Latched	☐	On pulse	☐
		On timed	☐
		On delay	☐
		Off delay	☐
		Time	
		Seconds	
		Minutes	
Macro output is generated from the following macro event flags:			
Input 1: Event flag Invert ☐ AND ☐ OR ☐ Input 2: Event flag Invert ☐ AND ☐ OR ☐ Input 3: Event flag Invert ☐ AND ☐ OR ☐ Input 4: Event flag Invert ☐ AND ☐ OR ☐			
For latched functionality macro input 4 is used to reset the output. The and/or selection does not apply.			

DGP address		Description	DGP Macro Logic
1 to 12 and 17 to 28 (Challenger10)		Optional	
Mark check boxes to indicate YES ☒			
Macro logic program number		Macro or output description	
Range 1 to 48		Optional	
Output event flag number		Invert output	☐
Disabled	☐	Non-timed	☐
Latched	☐	On pulse	☐
		On timed	☐
		On delay	☐
		Off delay	☐
		Time	
		Seconds	
		Minutes	
Macro output is generated from the following macro event flags:			
Input 1: Event flag Invert ☐ AND ☐ OR ☐ Input 2: Event flag Invert ☐ AND ☐ OR ☐ Input 3: Event flag Invert ☐ AND ☐ OR ☐ Input 4: Event flag Invert ☐ AND ☐ OR ☐			
For latched functionality macro input 4 is used to reset the output. The and/or selection does not apply.			

Note: See “Macro event flags” on page 49 for event flag numbers.

Glossary

The glossary describes the terms used this manual that may differ from terms used in the *Challenger Programming Manual* or in various types of management software.

access	Same as disarmed. Permission to open a door or to occupy an area without triggering an intrusion detection alarm.
access control	The control of entry to, or exit from, a secure area.
access time	For doors 17 to 64 and 81 to 128 (connected to an Intelligent Access Controller), the door will unlock for the time programmed in door or lift access time. For doors 1 to 16 and 65 to 80 (connected to a Challenger panel), the door event flag will unlock the door for the time programmed in door(s) unlock time.
alarm	An intrusion detection system state that should be signalled, for example, a door is opened by someone who does not have authority to do so. Alarms can also indicate equipment faults, such as communications failure or a tamper condition.
alarm code	Same as a user's PIN. See alarm code prefix.
alarm code prefix length	If an alarm code prefix length is defined, then the user will have a longer alarm code (PIN) and a door code (shortened by the alarm code prefix length). See door code.
alarm control	The ability of a user to operate the intrusion detection system, such as to arm or disarm areas.
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.
anti-passback	Anti-passback controls how the system responds when a user attempts to enter a region twice in succession (without leaving the region), as if they passed their card back to the outside for someone else to use.
area	A section of a premise with specific security requirements. The Challenger system can be divided into 16 areas, each having different security requirements and its own inputs. Every area is identified by a unique number and name, such as "Area 1 Office", "Area 2 Workshop", "Area 3 Boardroom", and so on.
armed	See secure.
arming stations (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, a card reader, or any other device which can be used to perform security functions such as arm or disarm, open doors, and so on.
authorised RAS	A RAS on the Intelligent Access Controller's local LAN can be authorised to arm or disarm areas normally controlled via the system LAN.

card	A credit card sized device that holds information to identify a user. The information can be available on a magnetic strip, a bar-coded strip, and a Wiegand card, or in a chip (smart cards). The term may also be used to indicate devices with similar functionality but different dimensions, such as a key fob.
control panel	An electronic device that is used to gather all data from inputs within a premises. Depending on the programming and the status of the areas, it will generate alarm signals when certain conditions are met. If required, alarms and other events may be reported to a central station.
disarmed	See access.
DGP	Data gathering panel, a device that collects data from other security devices, and transfers it to the control panel or Intelligent Access Controller.
door code	An optional version of the user's PIN shortened by the number of digits specified in the alarm code prefix length. The door code is used for access control (for example, to open a door) without potentially revealing the entire PIN used for alarm control.
door control	The ability of a user to operate the access control system, such as to open doors.
DOTL	Door open too long.
dual custody	In Challenger system programming, "dual custody" means that two users must enter their codes before access is granted to user programming. In Intelligent Access Controller programming, "dual custody" refers to whether two user cards or PINs are required to gain access to a door or lift. Two users must present their card or PIN to open a door (for example, when a user is identified as a visitor or guard and must be accompanied). Dual custody time is a programmable option.
duress	A situation where a user is being forced to breach the system security. The user may wish to send a duress alarm to a remote monitoring company. The duress alarm may be generated by a dedicated input device (holdup button), or by the user entering a duress code on a keypad. See duress code.
duress code	Also called 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 and may also be enabled or disabled for individual keypads connected to an Intelligent Access Controller.
egress input	An input that is programmed to activate a door event flag, e.g. a button provided inside a door (egress button) to allow users to exit without using the door reader.
event flags	For Intelligent Access Controllers, event flags refer to input and output events that can be used in up to 48 macro logic programs.
forced door debounce	Forced door debounce time delays the generation of a forced door alarm for a specified interval to cater for certain lock types.

IN reader	A door's reader (RAS) that is used to request entry to a specified region therefore located outside of the region. See also OUT reader.
input	An electrical signal from a security device (PIR detector, door contact) to the Challenger system. Each device is identified by an input number and name, e.g. "14 Reception PA Button, 6 Fire Exit Door".
input tamper monitoring	By default, input circuits are monitored for fault detection (open circuit or short circuit conditions) as well as for sealed and unsealed states. This is also known as four-state monitoring. When disabled, open circuit or short circuit conditions are detected as unsealed, so the only states detected are sealed and unsealed. This is also known as two-state monitoring.
Intelligent Access Controller	Also known as a four-door or four-lift DGP. Intelligent Access Controllers expand the Challenger system by providing door relays, interlocking door functionality, greater system capacity, and advanced access control functionality such as anti-passback, DOTL, extended access time, and more. Intelligent Access Controllers have onboard memory that enables them to provide access control functionality even if disconnected from the Challenger panel.
interlock	A method that stops two doors from being opened at the same time. Used, for example, in vaults.
keypad duress	See duress code.
lock relock time	Also known as lock release time in management software. Lock relock time is a programmed value used for hardware such as drop bolts and magnetic locks, where the door must be closed before the lock relay locks the door. This allows a settling time to ensure that the lock mechanisms are aligned before the lock relay releases the door lock.
low security time zone	When the time zone is valid, a valid card or a PIN code is required to open a door. When the time zone is not valid and "Card and PIN code reader" is set to YES, then both a valid card and PIN code are required to open a door.
macro logic program	A logic expression that combines up to four macro input events in a specific manner to trigger a macro output event. An Intelligent Access Controller can have up to 48 macro logic programs.
mode time	The amount of time permitted between the first and third badges when three-badge arming is used. For a RAS connected to a control panel, the mode time is fixed at 10 seconds. For a RAS connected to an Intelligent Access Controller, the mode time is programmable.
OUT reader	A door's reader (RAS) that is used to request exit from a specified region, therefore located inside of the region. See also IN reader.
PIN	A personal identity number of 4* to 10 digits entered on a RAS keypad to authenticate the user to the Challenger system. See also alarm code, door code, and duress code. * 5 to 10 digits for a Challenger system where the Financial Options programming is set to YES.

RAS	Remote arming station. See arming station.
region	An access control concept where doors with IN and OUT readers act as region boundaries. Regions are used by the anti-passback functions to keep track of users, and by region count functionality to activate an event when a defined limit is reached. Region 0 is considered to be off premises.
secure	Same as armed. An area is secured when unoccupied and there is nobody present to trigger an intrusion detection alarm.
shunt	A procedure that automatically inhibits an unsealed input from generating an alarm for a defined interval (shunt time) when it is armed. This allows time for a user to pass through the door and shut it again.
siren monitoring	When siren monitoring is enabled, the siren circuit is monitored for fault conditions. Siren monitoring is disabled by default.
tamper	A condition where a device has been removed, or its cover opened, or cabling disturbed. Tamper alarms include panel tamper and input tamper. See input tamper monitoring.
two badge unlock	Two badge unlock avoids unintended unlocking of a door if a user accidentally presents their card to a reader, for example, by brushing past the reader with the card in a pocket.
user	Anybody using the Challenger system. Users are identified to the Challenger system by a unique number that is associated with the user's PIN code or proximity card number.
zone input	See input.

Index

A

- Access time for doors/lifts, 14
- Alarm control
 - assigning, 21
 - assigning alarm groups, 21
 - IN/OUT disabled if area secure, 22
- Alarm group assignment, 21
- Anti-passback
 - different types, 18
 - programming, 18
- Automatic unlock after entry, 24

C

- Cabinet tamper
 - specifying relay number, 36
- Cards
 - displaying details, 33
 - specifying card formats, 23

D

- Database
 - initialising, 33
- default inputs and relays
 - Challenger V8, 47
 - Challenger10, 44
 - Lift controller, 49
- Defaulting the controller, 33
- Door/lift access options
 - access time, 14
 - anti-passback, 18
 - extended access time, 15
 - extended shunt time, 16
 - IN/OUT reader regions, 43
 - low security time zone, 16
 - overriding after entry, 24
 - overriding timezones, 24
 - shunt conditions, 15
 - shunt time, 15, 16
- Door/lift alarm control options
 - alarm group, 21
 - function, 21
 - IN/OUT disarmed if area secure, 22
- Door/lift egress options
 - programming, 20
 - timezones, 20
- Door/lift Egress options
 - Egress control, 21
- Door/lift hardware options
 - DOTL input number, 28
 - DOTL relay number, 28
 - Egress input number, 29
 - fault relay number, 29

- forced output number, 28
 - input number to prevent accessing door, 29
 - programming, 27
 - shunt input numbers, 28
 - unlock relay number, 27
- Door/lift numbers, 44
- Door/lift options
 - last floor of lift, 30
 - lift bank selection, 32
 - lift car selection, 32
 - lift options programming, 30
 - lift override group, 31
 - monitor high level floor landings, 32
 - select floor landing, 32
 - Starting floor of lift, 30
 - starting input of lift, 31
 - starting physical relays, 30
 - total number of floors, 32
- Door/lift reader options
 - card format, 23
 - duress functionality, 27
 - input holds door unlocked, 24
 - LED options, 25
 - pulsed lock and unlock, 41
 - report opening/closing door, 25
 - reporting forced door, 25
- DOTL
 - DOTL alarm and shunt time, 15
 - relay number, 28
 - reporting DOTL alarm condition, 28
- dual custody, 19
- dual custody time, 12
- Duress functionality, 27

E

- Egress
 - control, 21
 - defining the operation, 21
 - input number, 29
 - options, 20
 - timezones, 20
- Extended access time for door and lifts, 15
- Extended shunt time for doors/lifts, 16

F

- Floor
 - landings, 32
- Floor groups
 - programming floor group number, 31
- Floors
 - first floor of lift, 30
- Floors available, 32
- Forced door
 - DOTL and forced door, 15

- reporting, 25
- Function and output event
 - macro logic programming, 37

I

- IN/OUT readers
 - opening doors if area secure, 22
 - programming access controlled region, 43
- Initialising the database, 33
- input holds door unlocked, 24
- Input numbers, 44
- Interlock input numbers, 29

L

- Lift bank selection, 32
- Lift car selection, 32
- Lift options
 - floor landing, 32
 - floors available, 32
 - last floor of lift, 30
 - lift bank selection, 32
 - lift car selection, 32
 - lift override group, 31
 - monitor high level floor landings, 32
 - programming, 30
 - starting floor, 30
 - starting input of lift, 31
 - starting physical relay, 30
- Lock/reader fault
 - activating relay number, 29
- Low battery condition
 - relay number, 36
- Low security time zone for doors/lifts, 16

M

- Macro logic
 - function and output event number, 37
 - logic equations, 38
 - program number, 37
- Mains fail condition
 - relay number, 36
- Monitor high level floor landings, 32

O

- Opening doors
 - programming method used during low security time zone, 16
- Opening/closing doors
 - reporting, 25
- Output numbers
 - activating when input in, 28

P

- product overview, 1
 - about this manual, 1
 - related documentation, 2
- Pulsed lock and unlock, 41

- door lock procedure, 42
- door open procedure, 42

R

- Reader LED options
 - specifying, 25
- Reader options
 - automatic unlock after entry, 24
 - automatic unlock timezones, 24
 - card format, 23
 - DOTL input number, 28
 - duress functionality, 27
 - Egress input number, 29
 - fault relay number, 29
 - forced door entry, 25
 - forced output number, 28
 - input holds door unlocked, 24
 - interlock input numbers, 29
 - LED options, 25
 - opening/closing of doors, 25
 - pulsed lock and unlock, 41
 - relay activating on DOTL, 28
 - shunting input numbers, 28
 - unlock relay number, 27
- Relay numbers, 44
 - activating when door accessed, 27
 - specifying physical relays for lift, 30

S

- Shunt conditions for doors/lifts, 15
 - DOTL alarm generated, 15
- Shunt time for doors/lifts, 15
 - extending shunt time, 16
 - warning shunt time, 16
- Shunting input numbers, 28
- Siren tamper
 - specifying relay number, 36
- System options
 - low battery relay number, 36
 - mains fail relay number, 36
 - tamper relay number, 36

T

- Tamper relay number, 36
- Time and Attendance options
 - Wiegand options and lock relay numbering, 41
- Timer settings in minutes or seconds, 14
- Timers
 - access, 14
 - extended access, 15
 - extended shunt, 16
 - shunt, 15
 - shunt warning, 16
- Timezone
 - specifying when automatic unlock takes effect, 24
- Timezone number

- for opening doors, 16
- programming, 24
- two badge unlock, 19

U

- Unlock time for doors/lifts
 - extended access time, 15

V

- View card details, 33

W

- Warning shunt time for doors/lifts, 16
- Wiegand interface, 43

