TS0867/TS0869
Intelligent 4-Door/4-Lift Controller
programming guide
GE and GE Security are registered trademarks of the General Electric Company. Other product and company names herein may be the trademarks of their respective owners.

This publication may contain examples of screens and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual business enterprises and persons is entirely coincidental.

Disclaimer

The customer is responsible for testing and determining the suitability of this product for specific applications. In no event is GE Security Pty Ltd responsible or liable for any damages incurred by the buyer or any third party arising from its use, or their inability to use the product.

Due to ongoing product development, the contents of this manual can change without notice. We make every effort to ensure the accuracy of this manual. However, GE Security Pty Ltd assumes no responsibility for errors or omissions in this manual or their consequences. Please notify us if you find errors or omissions.

Software versions

This Version 8 Four Door / 4 Lift Controller is ONLY compatible with Version 7 or Version 8 Challenger Alarm Panels.

If this 4 Door / 4 Lift Controller is to be used to expand a Version 6 Challenger system, the Challenger Panel MUST be upgraded to Version 7 software, or replaced with a Version 8 Challenger Panel. Any existing 4 Door / 4 Lift Controllers on the system would also have to be upgraded to suit the Challenger Panel, and reprogrammed.

Important information

This manual provides detailed explanations for programming the TS0867/TS0869 Four Door/Lift Intelligent Controller and includes detailed explanations for the entire door / lift menus. All references to the programming menus, and their numbers, are menus within Remote Controllers, (Installer menu 19-28).

When installing a new Four-Door / Four-Lift Intelligent Controller it is strongly recommended that you first initialise the Intelligent Controller using Menu 3 - Initialise Database by using a RAS (remote arming station) on the Challenger system LAN. This command will set all programming to factory defaults (as listed in this programming manual). Once initialised, the Intelligent Controller may be programmed using a RAS or a computer running management software.

The TS0867 and TS0869 are the same physical products except for the firmware (software) EPROM. The factory defaults are different for each product: these are listed in the programming sheets in this guide.

Whenever the Intelligent Controller is mentioned, both the TS0867 and the TS0869 are included except where explicitly stated.
Contents

Programming sequence ........................................................................................................................................................................6
Controller set up tasks .............................................................................................................................................................................6
Door/lift set up tasks ..................................................................................................................................................................................7
Advanced set up tasks ..............................................................................................................................................................................9
   Adding alarm control functions .........................................................................................................................................................9
   Adding anti-passback facilities ......................................................................................................................................................9
How to program the options ....................................................................................................................................................................10
   Accessing the installer programming menu .............................................................................................................................................10
   Programming the menu options ............................................................................................................................................................11
Accessing the door/lift programming menu ........................................................................................................................................12
Programming reference .............................................................................................................................................................................14

1. Controller options ............................................................................................................................................................................14
   1.1. Relay controllers ..............................................................................................................................................................................14
   1.2. Site code A ..............................................................................................................................................................................................................14
   1.3. Site code A card offset ..........................................................................................................................................................................15
   1.4. Site code B ..............................................................................................................................................................................................................15
   1.5. Site code B card offset ..........................................................................................................................................................................15
   1.6. Alarm code prefix length ......................................................................................................................................................................15
   1.7. Poll RAS ............................................................................................................................................................................................................16
   1.8. RAS's with LCD's fitted .....................................................................................................................................................................16
   1.9. RAS's with egress enabled ...............................................................................................................................................................16
   1.10. RAS's with toggle enabled ............................................................................................................................................................17
   1.11. Poll DGP ...........................................................................................................................................................................................................17
   1.12. Tamper monitoring .........................................................................................................................................................................18
   1.13. Card to PIN time ...................................................................................................................................................................................................18
   1.14. Dual custody time ...................................................................................................................................................................................................18
   1.15. Mode time .......................................................................................................................................................................................................19
   1.16. Lock relock time ..................................................................................................................................................................................................19
   1.17. Region count threshold .....................................................................................................................................................................19
   1.18. Enable siren monitoring ...............................................................................................................................................................20
   1.19. Forced door debounce time ............................................................................................................................................................20

2. Door/lift options ................................................................................................................................................................................21
   Accessing the door / lift options ..........................................................................................................................................................21
   2.1. Access options ....................................................................................................................................................................................21
      2.1.1. Access time ..................................................................................................................................................................................................21
      2.1.2. Extended access time .................................................................................................................................................................21
      2.1.3. Shunting options .........................................................................................................................................................................22
      2.1.4. Shunt time .......................................................................................................................................................................................................22
      2.1.5. Extended shunt time .................................................................................................................................................................22
      2.1.6. Shunt warning time ..................................................................................................................................................................23
      2.1.7. Shunt until door closes ............................................................................................................................................................23
      2.1.8. Cancel shunt after door secures ..................................................................................................................................................23
      2.1.9. Low security time zone ..............................................................................................................................................................23
      2.1.10. IN reader card & PIN ...............................................................................................................................................................24
      2.1.11. OUT reader card & PIN ...........................................................................................................................................................24
      2.1.12. IN reader inhibit PIN ...............................................................................................................................................................24
      2.1.13. OUT reader inhibit PIN ...........................................................................................................................................................24
      2.1.14. IN reader inhibit region 0 users ................................................................................................................................................25
      2.1.15. OUT reader inhibit region 0 users ...........................................................................................................................................25
      2.1.16. Anti-passback options ..............................................................................................................................................................25
      2.1.17. Anti-passback notes .................................................................................................................................................................26
      2.1.18. IN reader region ......................................................................................................................................................................26

TS0867/TS0869 Intelligent 4-Door/4-Lift Controller Programming Manual 4.1
2.1.18.  OUT reader region.................................................................................................................................................. 27
2.1.19.  Anti-passback time................................................................................................................................................ 27
2.1.20.  IN reader dual custody........................................................................................................................................ 27
2.1.21.  OUT reader dual custody.................................................................................................................................... 28
2.2.  Egress options .................................................................................................................................................................. 28
2.2.1.  Egress time zone .......................................................................................................................................................... 28
2.2.2.  Egress time zone .......................................................................................................................................................... 28
2.2.3.  Out egress disabled if secure.................................................................................................................................... 29
2.2.4.  Egress options .......................................................................................................................................................... 29
2.2.5.  Egress reporting ......................................................................................................................................................... 30
2.3.  Alarm control ..................................................................................................................................................................... 31
2.3.1.  Alarm group ................................................................................................................................................................. 31
2.3.2.  Alarm control options .................................................................................................................................................. 31
2.3.3.  In denied if area secure ................................................................................................................................................ 32
2.3.4.  Out denied if area secure ........................................................................................................................................... 32
2.3.5.  Authorised RAS ........................................................................................................................................................... 32
2.4.  Reader options ..................................................................................................................................................................... 33
2.4.1.  Card format options ...................................................................................................................................................... 33
2.4.2.  Input holds door unlocked ........................................................................................................................................ 34
2.4.3.  Door unlocked until door open ..................................................................................................................................... 34
2.4.4.  Override time zone ....................................................................................................................................................... 34
2.4.5.  Override after entry ....................................................................................................................................................... 34
2.4.6.  Report door unsecured/secure ..................................................................................................................................... 35
2.4.7.  Map [un]secure to [unlocked] .................................................................................................................................. 35
2.4.8.  Report door open/close .................................................................................................................................................. 35
2.4.9.  Report forced door ........................................................................................................................................................ 36
2.4.10.  Report DOTL............................................................................................................................................................... 36
2.4.11.  Reader LED options .................................................................................................................................................... 36
2.4.12.  Pulsed lock and unlock relays ................................................................................................................................... 37
2.5.  Hardware options .................................................................................................................................................................. 40
2.5.1.  Lock relay ....................................................................................................................................................................... 40
2.5.2.  Input.................................................................................................................................................................................. 41
2.5.3.  Monitor 2nd door input ................................................................................................................................................... 41
2.5.4.  Forced relay ................................................................................................................................................................. 41
2.5.5.  Shunt input .................................................................................................................................................................... 41
2.5.6.  Warning relay ............................................................................................................................................................... 41
2.5.7.  DOTL input ................................................................................................................................................................. 42
2.5.8.  DOTL relay ................................................................................................................................................................. 42
2.5.9.  Egress input ................................................................................................................................................................. 42
2.5.10.  Door interlock ............................................................................................................................................................ 42
2.5.11.  Areas assigned to door ............................................................................................................................................. 43
2.5.12.  Fault relay ................................................................................................................................................................. 43
2.6.  Lift options .......................................................................................................................................................................... 43
2.6.1.  Starting floor ................................................................................................................................................................. 43
2.6.2.  Last floor ....................................................................................................................................................................... 44
2.6.3.  Starting physical relay ................................................................................................................................................... 44
2.6.4.  Inputs monitor floor selected ...................................................................................................................................... 44
2.6.5.  Wait for floor selection ................................................................................................................................................ 45
2.6.6.  Starting physical input .................................................................................................................................................. 45
2.6.7.  Lift override group ....................................................................................................................................................... 45
2.6.8.  Security input ............................................................................................................................................................... 45
2.6.9.  Lift security group ....................................................................................................................................................... 46
2.6.10.  Total floors ................................................................................................................................................................. 46
2.6.11.  Lift bank ...................................................................................................................................................................... 46
2.6.12.  Lift car ......................................................................................................................................................................... 46
2.6.13.  Floor landings 1-32 .................................................................................................................................................... 46
2.6.14.  Floor landings 33-64 .................................................................................................................................................. 47
2.6.15.  Monitor high level floor landing ............................................................................................................................... 47
Programming sequence

The following sections are provided as overview of common programming tasks. Refer to the Programming reference starting on page 14 for specific details.

Perform the following tasks to enable cards being read and door opening due to a valid card.

Controller set up tasks

Perform the following tasks for each Intelligent Controller.

1. Set the Intelligent Controller's DIP switches to program the address (1 to 12 available).
2. Ensure that the RAM in the Intelligent Controller matches the Challenger panel.
3. Program and set the RAS or DGP addresses connected to the Intelligent Controller sub-LAN. Refer to Table 1 on page 16 for details of addressing IN and OUT readers.
4. In the Challenger installer programming [menu 19. Install]:
   - Activate polling (menu 4. DGP) for the Intelligent Controller and set the DGP type.
   - Check and note (menu 7. System Options) the settings for Input Tamper Monitoring and Alarm Prefix Length.
   - Program time zones required (menu 13. Time zones) for access control functions (egress, override time zone, and door groups).
   - Determine which area/s (menu 2. Area Database), will inhibit Egress or will inhibit access through a door when the area(s) are armed.
5. Go to menu 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 go to menu 1. Relay controllers. Program or select the following items (as applicable):
   6.1. Number of relay controllers fitted to the Intelligent Controller.
   6.2. Site code A (see page 14).
   6.3. Card offset for site code A (see page 15).
   6.4. Site code B (see page 15).
   6.5. Card offset for site code B (see page 15).
   6.6. Alarm code prefix length (see page 15).
   6.7. Poll readers connected to the Intelligent Controller sub-LAN (see page 16).
   6.8. RAS's with LCD (see page 16).
   6.9. RAS's with egress input enabled (see page 16).
   6.10. RAS's that have toggle mode enabled (see page 17).
   6.11. Poll DGPs connected to the Intelligent Controller sub-LAN (see page 17).
   6.12. Tamper monitoring (see page 18).
   6.13. Card to PIN time (see page 18).
   6.15. Mode time (see page 19).
   6.16. Lock relock time (see page 19).
   6.17. Region count threshold (see page 19).
   6.18. Enable siren monitoring (see page 20).
   6.19. Forced door debounce time (see page 20).
Door/lift set up tasks

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

1. In the Intelligent Controller programming menu go to menu 2. Door/Lift Options and then select the number of the door you wish to program.

2. Select option 1. Access Options to program or select the following items (as applicable):
   2.1. Access time (see page 21).
   2.2. Extended access time (see page 21).
   2.3. Shunting options (see page 22).
   2.4. Shunt time (see page 22).
   2.5. Extended shunt time (see page 22).
   2.6. Shunt warning time (see page 23).
   2.7. Shunt until door closes (see page 23).
   2.8. Cancel shunt after door secures (see page 23).
   2.9. Low security time zone (see page 23).
   2.10. IN reader card & PIN (see page 24).
   2.11. OUT reader card & PIN (see page 24).
   2.12. IN reader inhibit PIN (see page 24).
   2.13. OUT reader inhibit PIN (see page 24).
   2.14. IN reader inhibit region 0 user (see page 25).
   2.15. OUT reader inhibit region 0 user (see page 25).
   2.16. Anti-passback options (see page 25).
   2.17. IN reader region (see page 26).
   2.18. OUT reader region (see page 27).
   2.19. Anti-passback time (see page 27).
   2.20. IN reader dual custody (see page 27).
   2.21. OUT reader dual custody (see page 28).

3. If egress is to be used, select option 2. Egress Options to program or select the following items (as applicable):
   3.1. Egress time zone (see page 28).
   3.2. In egress disabled if secure (see page 29).
   3.3. Out egress disabled if secure (see page 29).
   3.4. Egress options (see page 30).
   3.5. Egress reporting (see page 30).

4. Select option 4. Reader Options to program or select the following items (as applicable):
   4.1. Card format (see page 33).
   4.2. Input holds door unlocked (see page 34).
   4.3. Door unlocked until door open (see page 34).
   4.4. Override time zone (see page 34).
   4.5. Override after entry (see page 34).
   4.6. Report door unsecured/secure (see page 35).
   4.7. Map (un)secure to (un)locked (see page 35).
   4.8. Report door open/close (see page 35).
   4.9. Report forced door (see page 36).
   4.10. Report DOTL (see page 36).
   4.11. Reader LED options (see page 36).
   4.12. Pulsed lock and unlock relays (see page 37).
   4.13. Disable duress (see page 40).
5. Select option **5. Hardware Options** to program or select the following items (as applicable):
   
   5.1. Lock relay number (see page 40).
   5.2. Input number (see page 41).
   5.3. Monitor 2nd door input (see page 41).
   5.4. Forced relay number (see page 41).
   5.5. Shunt input number (see page 41).
   5.6. Warning relay number (see page 41).
   5.7. DOTL input number (see page 42).
   5.8. DOTL relay number (see page 42).
   5.9. Egress input number (see page 42).
   5.10. Door interlock number (see page 42).
   5.11. Areas assigned to door number (see page 43).
   5.12. Fault relay number (see page 43).

6. If programming a TS0869 4-Lift DGP, select option **6. Lift Options** to program or select the following items (as applicable):
   
   6.1. Starting floor (see page 43).
   6.2. Last floor (see page 44).
   6.3. Starting physical relay (see page 44).
   6.4. Inputs monitor floor selected (see page 44).
   6.5. Wait for floor selection (see page 45).
   6.6. Starting physical input (see page 45).
   6.7. Lift override group (see page 45).
   6.8. Security input (see page 45).
   6.9. Lift security group (see page 46).
   6.10. Total floors (see page 46).
   6.11. Lift bank (see page 46).
   6.12. Lift car (see page 46).
   6.13. Floor landings 1-32 (see page 46).
   6.14. Floor landings 33-64 (see page 47).
   6.15. Monitor high level floor landing (see page 47).

7. When out of the Hardware options (or Lift Options, if used), press 0 [ENTER] to exit the sub-menu, and then press [ENTER] 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 [installer menu 1 Input].
Advanced set up tasks

The advanced set up adds alarm control and anti-passback to the basic set up performed in Controller set up tasks on page 6 and Door/lift set up tasks on page 7.

Adding alarm control functions

1. In the Challenger installer programming:
   - 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 menu 2. Door/Lift Options and then select the number of the door or lift you wish to program. For the selected door or lift:
   - Select menu 3. Alarm control (see page 31).
   - Enter the required Alarm group (see page 31).
   - Select the required Alarm control options (see page 31).
   - Select the required settings for In denied if area secure and/or Out denied if area secure on page 32.
   - Select the Authorised RAS on the Intelligent Controller sub-LAN (if required). See page 32.

3. Assign an alarm group to users that should have alarm control on the Intelligent Controller (User Menu 14. Program Users).

Adding anti-passback facilities

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 16). Make sure both IN and OUT readers are available and are polled.

1. In the Challenger installer menu, program the time zones required for anti-passback.

2. In the Intelligent Controller programming menu, select menu 2. Door/Lift Options and then select the number of the door or lift you wish to program. For the selected door or lift:
   - Select menu 1. Access options (see page 21).
   - Select the required settings for IN reader inhibit region 0 user and/or OUT reader inhibit region 0 user (see page 25).
   - Select the required Anti-passback option (see page 25).
   - Enter the IN reader region and OUT reader region (see page 26).
How to program the options

For information on which keys to use while programming, please refer to these pages.

Accessing the installer programming menu

The Challenger system is programmed from the Installer programming menu. Before accessing the programming menu, you must first disarm the system.

How to disarm the system:

1. Press 4346 (Master PIN code) and then [OFF].
2. Press 0 and [ENTER].

How to access the installer programming menu

1. Start with this LCD display:

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

2. Enter [MENU*] 4346 (Master PIN code) and press [ENTER].
   The following display appears:

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

3. Press 19 and [ENTER], and the following display appears:

```
Install Menu
0-Exit, Menu:
```

You may now select the menu option you wish to program. See page 74 for the programming map that lists all menu options available. The chapter and section numbering in the manual follows the menu option numbering. For example, Chapter 1 describes menu 1 “Input database”.

Move between the menu options by pressing the following keys:

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ENTER] or [#] or [↓]</td>
<td>To scroll forwards one menu option at a time.</td>
</tr>
<tr>
<td>[MENU*] or [*] or [↑]</td>
<td>To scroll backwards one menu option at a time.</td>
</tr>
<tr>
<td>Menu number and [ENTER] or [#]</td>
<td>To jump directly to the menu option.</td>
</tr>
<tr>
<td>[0] and [ENTER] or [#]</td>
<td>Exit programming menu and return to the user menu.</td>
</tr>
</tbody>
</table>
Programming the menu options

What the LCD display tells you

The LCD display on the keypad has two lines of characters. Each line represents different information.

System information

Remote DGP Setup
DGP No:

Instructions and the characters you may enter on the keypad

Programming the menu options

Once you have selected the menu option you wish to program, most options may be programmed using a standard procedure shown below in How to program.

How to program

The method of programming depends on the options to be programmed. Some options require a value others require a YES/NO setting.

How to program values

? [ENTER] Enter the new information and press the ENTER key.

[ENTER] Press the ENTER key again to save the displayed information and to move to the next menu option display.

How to program YES/NO options

[MENU*] Press the MENU* key to toggle between options.

[ENTER] Press the ENTER key to save the displayed information and move to the next menu option display.

Some programming options allow multiple values to be entered, for example Poll RAS. In these cases, enter the value and press [ENTER] to add or delete the option.

Some programming menus need certain values to be entered, while others are used to select YES/NO. Programming lines containing YES/NO options often also allow the 0-key to be pressed. Use this key to skip a number of options. On the second line, the display will indicate if the 0-key may be used.

Programming menus like ‘Poll RAS’, ‘Poll DGP’ or ‘Entry time’ show the status of the current values. To update the values, press [MENU*].

Many time settings may be entered with seconds or minutes resolution. This may be recognised when the bottom left corner of the display shows “*-Min” or ”*-Sec”. Use [*] or [MENU*] to select seconds or minutes.

Where programming of an option does not follow this procedure, the (additional) keys available are described in the How to program section for the option.
Accessing the door/lift programming menu

Access to the Door programming menu is via the Challenger Installer menu 28, Remote Controllers. When programming in the door/lift programming menu, you are actually programming the Intelligent Controller.

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

- Connected.
- Addressed.
- Programmed to be polled.
- The DGP type must be programmed as a "Door Controller" or a "Lift Controller" in the Challenger installer programming menu 4, DGP database.

If you are denied access to “Remote Controllers”, it is because one or more of the above hardware or programming criteria have not been met.

1. The display shows:

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

   Enter the type of Remote device you wish to program. Select 1 (DGP).

2. The display shows:

   Remote DGP Setup
   DGP No:

   Enter the number of the Remote device you wish to program. The DGP number is the same as the DGP address.

3. The following is briefly displayed:

   Connecting...
   Enter to Abort

4. You have now accessed the programming menu for the Intelligent Controller that you have selected.

   The display shows the 4-Door programming menu display:

   *#*‘-Move On  **‘-Move Back
   Menu:

   See Programming the menu options on page 11 for the available keys.
### Intelligent Controller programming menus (see also Programming map on page 74).

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Controller Options</td>
<td>Global options valid for all doors/lifts of the selected 4-door / 4-lift DGP (Intelligent Controller).</td>
</tr>
<tr>
<td>2.</td>
<td>Door Options</td>
<td>Options valid for each individual door or lift on the Intelligent Controller.</td>
</tr>
<tr>
<td>3.</td>
<td>Initialize Database</td>
<td>Allows initialisation of door or lift database. Resets all data in the DGP to the factory default settings.</td>
</tr>
<tr>
<td>4.</td>
<td>Display Card</td>
<td>Displays card details on LCD for the last card that is badged.</td>
</tr>
<tr>
<td>5.</td>
<td>Door Groups</td>
<td>Allows door group details to be programmed or viewed.</td>
</tr>
<tr>
<td>6.</td>
<td>Lift Groups</td>
<td>Allows floor group details to be programmed or viewed.</td>
</tr>
<tr>
<td>7.</td>
<td>System Options</td>
<td>Allows Intelligent Controller relays to be activated to indicate system faults on the Intelligent Controller.</td>
</tr>
<tr>
<td>8.</td>
<td>Macro Logic</td>
<td>Enables outputs and internal events to be generated by logic functions using Intelligent Controller events.</td>
</tr>
<tr>
<td>10.</td>
<td>Remote Controllers</td>
<td>Enables you to access the remote devices on the DGP LAN.</td>
</tr>
<tr>
<td>11.</td>
<td>Display IUM User</td>
<td>Enables you to check the raw card data (RCD) associated with a user number.</td>
</tr>
</tbody>
</table>
Programming reference

1. Controller options

DGP options valid for all doors or lifts on the selected Intelligent Controller.

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

1.1. Relay controllers

XX, Relay Controllers 0
*-Dis, Ctrl:

Enter the number of relay controllers fitted to the Intelligent Controller.

| 0  | Disabled. No clocked relay card, but there are four open collector relays available on the Intelligent Controller for a TS0840 4-way relay card. These have relays 5 to 8 assigned for the selected DGP address. |
| 1-8 | Enter a value of 1 for every 8 relays fitted to the controller. 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 32 relays are used. |

1.2. Site code A

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

“Site code” is also called “Facility code”.

Records the first site identification number used in cards. Each system has a unique site ID.

Two site code numbers and associated card offsets can be programmed to enable the system to be used with two sets of cards on different site codes (e.g. for ease of use during a changeover period when a system has been commissioned using a set of cards on loan while awaiting delivery of customised cards).
1.3. Site code A card offset

This record specifies a 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 which is used when programming users, and which is reported to the printer and computer.

Example — Actual physical card ID number is 5001, and the card offset is programmed as -5000. The card will be programmed as user 1 and will report as user 1.

1.4. Site code B

Records the second site identification number used in cards. Each system has a unique site ID.

Refer to Site code A on page 14 for details.

1.5. Site code B card offset

This record specifies a number that is added to, or subtracted from, the actual card ID number for cards on site code B.

Refer to Site code A card offset above for details.

1.6. Alarm code prefix length

Records the difference between the number of digits in an alarm control code and the number of digits in a door control code.

The complete user code is the alarm control code, and the prefix is omitted to make the door control code.


The alarm code prefix length entered, must be the same as the value entered for the alarm code prefix length in the Challenger installer programming menu 7. System Options.
1.7. Poll RAS

Enter the RAS addresses of all the RAS’s connected to the Intelligent Controller sub-LAN. The display shows the RAS’s currently recorded.

- **RAS number followed by , = online**
- **RAS number followed by : = offline**

Example:

```
1, 2, 3: 4:
```

The above example indicates that RAS’s 1, 2, 3, and 4 are being polled, and only RAS’s 1 and 2 are online (3 and 4 are offline). Press the * button to update the display.

- **Readers polled on the Intelligent Controller sub-LAN can function as ‘IN’ or ‘OUT’ readers (i.e. mounted on opposite sides of the same door). ‘IN’ or ‘OUT’ functionality is determined by the readers’ RAS address, as listed in Table 1.**

<table>
<thead>
<tr>
<th>Function:</th>
<th>In</th>
<th>In</th>
<th>Out</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Door</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>2nd Door</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>3rd Door</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>4th Door</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

*Table 1 — RAS addresses for IN and OUT functionality*

1.8. RAS’s with LCD’s fitted

Program the address of RAS’s (remote arming stations) being polled that have a LCD (Liquid Crystal Display) fitted. The display shows the RAS’s currently recorded.

1.9. RAS’s with egress enabled

Enter the address of RAS’s being polled that require the Egress button to be wired to the IN, or EGRESS, terminal on the arming station. The display shows the RAS’s currently recorded.

- **Since the RAS’s Egress input does not provide tamper monitoring, it is preferable to wire any Egress buttons to inputs on the Intelligent Controller.**
1.10. RAS’s with toggle enabled

Records the address of RAS’s being polled that have “Toggle mode” enabled. Operation for the ‘Toggle Mode’ is explained below. This option only applies to RAS’s with keypads.

In this instance, toggle mode refers to the Toggle Area Status programming option for keypad RAS’s connected to the Intelligent Controller LAN. RAS’s connected to the control panel 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

<table>
<thead>
<tr>
<th>Keypad input</th>
<th>Toggle Mode</th>
<th>Effect on area(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN + [ENTER] or [#]</td>
<td>Enabled</td>
<td>Toggles the arm/disarm state</td>
</tr>
<tr>
<td>PIN + [MENU*] or [*]</td>
<td>Enabled</td>
<td>Toggles the arm/disarm state</td>
</tr>
<tr>
<td>PIN + [ENTER] or [#]</td>
<td>Disabled</td>
<td>Arms</td>
</tr>
<tr>
<td>PIN + [MENU*] or [*]</td>
<td>Disabled</td>
<td>Disarms</td>
</tr>
</tbody>
</table>

Table 3 — Toggle mode operation for small LCD keypads

<table>
<thead>
<tr>
<th>Keypad input</th>
<th>Toggle Mode</th>
<th>Effect on area(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN + [ON]</td>
<td>Enabled</td>
<td>Arms</td>
</tr>
<tr>
<td>PIN + [OFF]</td>
<td>Enabled</td>
<td>Disarms</td>
</tr>
<tr>
<td>PIN + [ENTER]</td>
<td>Disabled</td>
<td>Arms</td>
</tr>
<tr>
<td>PIN + [OFF]</td>
<td>Disabled</td>
<td>Disarms</td>
</tr>
</tbody>
</table>

1.11. Poll DGP

Enter the address of DGP’s connected to the TS0869 4-Lift Controller LAN (this option is not functional on the TS0867 4-Door Controller). The display shows the DGP’s currently recorded.

The TS0869 can poll up to 15 DGPs on its local sub-LAN, with each of the 15 DGPs providing up to 16 inputs (typically for floor-buttons).
1.12. Tamper monitoring

**XX,Yes - Tamper Monitoring**

* - Change

Defines whether the Intelligent Controller inputs are monitored for Tamper Alarm.

<table>
<thead>
<tr>
<th>YES</th>
<th>The inputs are monitored for 4 states - Alarm, Seal, Open, Short.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The inputs are monitored for 2 states - Alarm, Seal.</td>
</tr>
</tbody>
</table>

Must be set to the same function as set in the Challenger Installer menu Option 7 - System Options.

1.13. Card to PIN time

**XX,Card to PIN Time 8 Seconds**

* - Min, Time:

This setting is only applicable when a user is required to present a card and enter a PIN to gain access.

The Card to Pin Time is the amount of time allowed between presenting a valid card to a door reader and entering a valid PIN (last digits) on the keypad. If the PIN is not entered before the time expires, the user will need to repeat the door opening function.

🔗 See also Access options (page 21)

1.14. Dual custody time

**XX, Dual Custody Time 8 Seconds**

* - Min, Time:

This setting is only applicable when two users must present their card or PIN to open a door or when a user is identified as a visitor or guard and must be accompanied.

The dual custody time is the amount of time allowed between the first user presenting a card or entering a PIN and the second user presenting a card or entering a PIN. If the second card/PIN is not presented before the time expires, the door opening function will have to be repeated.

🔗 See also IN reader dual custody and OUT reader dual custody (page 28).
1.15. Mode time

This setting is only applicable where the door has been programmed so that presentation of a card three times will arm/disarm the system and the user is authorised to arm/disarm.

The mode time is the amount of time allowed between the first presentation of the card and the third presentation of the card. If the card is not presented three times before the time expires, the user will need to commence the function again.

*See also Alarm control options (page 31)*

1.16. Lock relock time

This setting only applies 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 drop bolts, maglocks, etc. where the door must be closed before the lock relay locks the door. The re-lock delay time is the amount of time between the door being closed and the lock relay deactivating [re-lock]. This allows a settling time to ensure that the lock mechanisms are aligned.

*See also Input holds door unlocked (page 34).*

1.17. Region count threshold

When the number of users reaches this limit (set by the value entered in this option – range, 0 to 65,535), the Intelligent Controller sets an internal flag (Region count limit) that can be used in door macro logic. You may activate events when a certain number of users are in a region. The Challenger system can have up to 256 regions, numbered 0 to 255.

Examples:

1. Activate a sign when a car park is full.

2. Arm area(s) when the last person has left the region or disarm area(s) when the first person enters the region.

*See also IN reader region (page 26)*
1.18. Enable siren monitoring

Enable siren monitoring in order to perform the siren monitor test.

1.19. Forced door debounce time

Enter the forced door debounce value in milliseconds times 100 (the default is 7, which equals 700 milliseconds). Acceptable values are in the range 4 through 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.
2. Door/lift options

Accessing the door / lift options

Use this menu for programming data for individual doors and lifts. Each door may be programmed with specific settings. Before obtaining access to the available menu options for door and lift programming, select the door to program.

The door numbers relevant to the Intelligent Controller being programmed are displayed:

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

In the following sections, the characters "XX" represent the number of the selected device.

2.1. Access options

2.1.1. 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 40.

2.1.2. 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.
2.1.3. Shunting options

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No shunting</td>
</tr>
<tr>
<td>1</td>
<td>Input Shunting</td>
</tr>
<tr>
<td>2</td>
<td>Input Shunting &amp; DOTL</td>
</tr>
<tr>
<td>3</td>
<td>Auto Shunting &amp; DOTL</td>
</tr>
</tbody>
</table>

2.1.4. Shunt 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 (page 41).

2.1.5. Extended shunt 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.
2.1.6. **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 41 and Shunt input on page 41.*

2.1.7. **Shunt until door closes**

XX, NO Shunt Until Door Closes  
*-Change

Set the shunt period to when the door input is resealed.

<table>
<thead>
<tr>
<th>YES</th>
<th>Shunt the defined input(s) as programmed in hardware options “Shunt input” until the door is closed (door input is resealed). When the door is open and the shunt is not active the input will generate an alarm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Shunt timer is used.</td>
</tr>
</tbody>
</table>

2.1.8. **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.

<table>
<thead>
<tr>
<th>YES</th>
<th>Shunt the programmed inputs until the door has closed. Opening the door again within the shunt time is not possible, as this will generate an alarm (there is always a debounce time of approx. 2 seconds).</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Shunt timer will be used.</td>
</tr>
</tbody>
</table>

2.1.9. **Low security time zone**

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

Enter a time zone number from 1 through 24. When the time zone is valid, only a valid card or PIN is required to open the door. When the time zone is not valid and “Card and PIN code Reader” is set to YES, a valid card and PIN code must be entered to open the door.

*Time zones are programmed in the Challenger in installer menu 13. Time Zones.*
2.1.10. IN reader card & PIN

Specify what method is required to open the door from the IN reader. This is programmed separately for the IN and OUT readers.

<table>
<thead>
<tr>
<th>YES</th>
<th>Unlock the door by presenting a valid card to the reader AND entering a PIN on the reader’s keypad.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Unlock the door by presenting a valid card to the reader OR a valid PIN on the reader’s keypad.</td>
</tr>
</tbody>
</table>

2.1.11. OUT reader card & PIN

Specify what method is required to open the door from the OUT reader. This is programmed separately for the IN and OUT readers.

<table>
<thead>
<tr>
<th>YES</th>
<th>Unlock the door by presenting a valid card to the reader AND entering a PIN on the reader’s keypad.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Unlock the door by presenting a valid card to the reader OR a valid PIN on the reader’s keypad.</td>
</tr>
</tbody>
</table>

2.1.12. IN reader inhibit PIN

This menu determines which method is used to open the door during the low security time zone and is programmed separately for the IN and OUT readers.

<table>
<thead>
<tr>
<th>YES</th>
<th>During the low security time zone, ONLY a valid card is required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>During the low security time zone, a valid card OR a valid PIN is required.</td>
</tr>
</tbody>
</table>

2.1.13. OUT reader inhibit PIN

This menu determines which method is used to open the door during the low security time zone and is programmed separately for the IN and OUT readers.

<table>
<thead>
<tr>
<th>YES</th>
<th>During the low security time zone, ONLY a valid card is required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>During the low security time zone, a valid card OR a valid PIN is required.</td>
</tr>
</tbody>
</table>
2.1.14. IN reader inhibit region 0 users

For users in region 0 (region 0 is typically offsite), a special security feature is available to provide access only via another region.

| YES | Any user in region 0 will be denied access. To access, the user first has to be in another region. |
| NO  | Users from region 0 will gain access. |

2.1.15. OUT reader inhibit region 0 users

For users in region 0 (region 0 is typically offsite), a special security feature is available to provide access only via another region.

| YES | Any user in region 0 will be denied access. To access, the user first has to be in another region. |
| NO  | Users from region 0 will access. |

2.1.16. Anti-passback options

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 on page 26).

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).

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No anti-passback</td>
</tr>
<tr>
<td>1</td>
<td>Soft anti-passback</td>
</tr>
<tr>
<td>2</td>
<td>Hard anti-passback</td>
</tr>
<tr>
<td>3</td>
<td>Timed anti-passback (not fully supported at present)</td>
</tr>
</tbody>
</table>
Anti-passback notes

- A region has to be programmed for the door’s readers (see IN reader region below, and OUT reader region on page 27).
- Door contacts must be fitted and wired to the Intelligent Controller.
- After badging the card, the door must be opened before a user is logged into a region.
- To clear a hard or soft 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 (the region record is reset when the reprogrammed user is downloaded to Intelligent Controller).
- For region numbers below 200, anti-passback functionality is overridden by users with ‘Privileged’ status.

2.1.17. IN reader region

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 page 25), 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 the IN reader for each door. 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’.

See also Anti-passback options (page 25).

Important: The four onboard Wiegand interfaces (I/F) are, by default, the ‘IN’ readers for the four doors. You may, however, make them function as ‘IN’ and ‘OUT’ readers. For this to occur, change the ‘Lock Relay’ number, in the ‘Hardware Options’ menu, and the ‘Lock Relay’ of the wanted ‘OUT’ reader to the same number as the ‘Lock Relay’ of the ‘IN’ Reader.

Example: Wiegand I/F 1 has ‘Lock Relay’ 33 (Door 21, DGP2) and is the ‘IN’ reader. To set Wiegand I/F 2 as the ‘OUT’ reader, set its ‘Lock Relay’ to 33 (same as Wiegand I/F 1).
2.1.18. OUT reader region

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 page 25), 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 the OUT reader for each door. 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’.

See also Anti-passback options (page 25).

Important: The four onboard Wiegand interfaces (I/F) are by default the ‘IN’ readers for the four doors. You may, however, make them function as ‘IN’ and ‘OUT’ readers. For this to occur, change the ‘Lock Relay’ number, in the ‘Hardware Options’ menu, and the ‘Lock Relay’ of the wanted ‘OUT’ reader to the same number as the ‘Lock Relay’ of the ‘IN’ Reader.

Example: Wiegand I/F 1 has ‘Lock Relay’ 33 (Door 21, DGP2) and is the ‘IN’ reader. To set Wiegand I/F 2 as the ‘OUT’ reader, set its ‘Lock Relay’ to 33 (same as Wiegand I/F 1).

2.1.19. Anti-passback time

This option is not fully supported at present.

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 (page 25).

2.1.20. IN reader dual custody

Controls if two user cards or PINs are required to gain access. Separate programming records are provided for the IN and OUT reader for each door.

<table>
<thead>
<tr>
<th>YES</th>
<th>Two different users need to present their card and/or PIN in succession for the door to unlock.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Only one user is needed to present a card and/or PIN.</td>
</tr>
</tbody>
</table>
2.1.21. **OUT reader dual custody**

<table>
<thead>
<tr>
<th>XX, NO - Out Reader Dual Custody</th>
<th>*=Change</th>
</tr>
</thead>
</table>

Controls if two user cards or PINs are required to gain access. Separate programming records are provided for the IN and OUT reader for each door.

<table>
<thead>
<tr>
<th>YES</th>
<th>Two different users need to present their card and/or PIN in succession for the door to unlock.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Only one user is needed to present a card and/or PIN.</td>
</tr>
</tbody>
</table>

2.2. **Egress options**

2.2.1. **Egress time zone**

<table>
<thead>
<tr>
<th>XX, Egress Time Zone 0</th>
<th>*=Dis, TZ:</th>
</tr>
</thead>
</table>

Enter a time zone number 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) when the Egress should always be available.

📅 *Time zones are programmed in the Challenger in menu 13. Time Zones. Only time zones 0 to 24 can be entered.*

🔗 *See also Egress input (page 42).*
2.2.2. In egress disabled if secure

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

“IN Egress disabled if secure” is used if the Egress button is wired to an input on the Intelligent Controller (recommended).

This menu controls the ability to use the Egress button on an input or the IN reader (exit button) to open the door if any of the areas assigned to the door are armed.

| YES | The Egress button does not unlock the door if any of the areas assigned to the door are armed |
| NO  | The Egress button unlocks the door regardless of the status of the area(s) assigned to the door. |

⚠️ If the Intelligent Controller loses communication with the Challenger, then the Intelligent Controller remembers the latest status of the area.

⚠️ See also Areas assigned to door on page 43.

2.2.3. Out egress disabled if secure

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

“OUT Egress Disabled If Secure” is used if the Egress button is wired to an input on the Intelligent Controller (recommended).

This menu controls the ability to use the Egress button on an input or the OUT reader (exit button) to open the door if any of the areas assigned to the door are armed.

| YES | The Egress button does not unlock the door if any of the areas assigned to the door are armed |
| NO  | The Egress button unlocks the door regardless of the status of the area(s) assigned to the door. |

⚠️ If the Intelligent Controller loses communication with the Challenger, then the Intelligent Controller remembers the latest status of the area.

⚠️ See also Areas assigned to door on page 43.
### 2.2.4. Egress options

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Egress Times Door Open</td>
</tr>
<tr>
<td></td>
<td>When the Egress button is pressed, the door unlocks for the programmed unlock time.</td>
</tr>
<tr>
<td>1</td>
<td>Egress Holds Door Open</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Egress Shunts Only</td>
</tr>
<tr>
<td></td>
<td>When the Egress button is pressed, the input is shunted.</td>
</tr>
</tbody>
</table>

Defines the operation of the Egress button (exit button).

### 2.2.5. Egress reporting

<table>
<thead>
<tr>
<th>XX, NO - Egress Reporting</th>
</tr>
</thead>
</table>

This menu determines if the Egress function for the door should be reported.

<table>
<thead>
<tr>
<th>YES</th>
<th>Door Egress report is sent to the printer and to the computer when Egress input is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>No report is sent when Egress input is used.</td>
</tr>
</tbody>
</table>
2.3. Alarm control

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

2.3.1. Alarm group

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.

See also Challenger Installer menu 5, Alarm Groups.

2.3.2. Alarm control options

Specify what type of alarm control will be available for the door/reader.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reader Has No Alarm Control It is not possible to arm/disarm using the reader.</td>
</tr>
<tr>
<td>1</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Alarm Control on 3rd Badge Presentations of a valid card three times arm/disarms the areas in the alarm group.</td>
</tr>
<tr>
<td>3</td>
<td>Alarm Control with Buttons Allows user to access the function on the button interface.</td>
</tr>
<tr>
<td>4</td>
<td>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.</td>
</tr>
</tbody>
</table>
2.3.3. In denied if area secure

Stop a user opening a door using the IN reader when any of the areas assigned to the door are armed. Separate programming records are provided for each door with an IN reader.

<table>
<thead>
<tr>
<th>YES</th>
<th>A valid card or PIN will not open a door if any of the areas assigned to the door are armed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>A valid card or PIN will open a door regardless of the area's armed status.</td>
</tr>
</tbody>
</table>

*If the Intelligent Controller loses communication with the Challenger, then the Intelligent Controller remembers the latest status of the area.*

See also Areas assigned to door on page 43.

2.3.4. Out denied if area secure

Stop a user opening a door using the OUT reader when any of the areas assigned to the door are armed. Separate programming records are provided for each door with an OUT reader.

<table>
<thead>
<tr>
<th>YES</th>
<th>A valid card or PIN will not open a door if any of the areas assigned to the door are armed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>A valid card or PIN will open a door regardless of the area's armed status.</td>
</tr>
</tbody>
</table>

*If the Intelligent Controller loses communication with the Challenger, then the Intelligent Controller remembers the latest status of the area.*

See also Areas assigned to door on page 43.

2.3.5. Authorised RAS

This function gives the user the ability to badge their card on a reader-equipped RAS on the Intelligent Controller sub-LAN in order to selectively arm or disarm area(s) normally controlled via the Challenger LAN. Specifically, badging at the door's reader simulates the user entering their PIN at the authorised Challenger RAS and provides a means of selecting area(s). Selection of area(s) is not otherwise available from a RAS on the sub-LAN.

*If a RAS number is entered, then this door's readers may only be used to operate the authorised RAS (i.e. the readers no longer provide door access). The authorised RAS must also have the option "Toggle Keyboard Control" set to YES (programmed in the Challenger Installer menu 3, RAS Database).*

Example — This door has RAS 3 designated as an authorised RAS. A user may arm or disarm area(s) by badging their card at this door's reader-equipped RAS and then selecting the area(s) via the keypad.
2.4. Reader options

Program settings specific to this reader.

2.4.1. Card format options

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

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

TS0862 (Smart Door Controller) can be used on the Intelligent Controller LAN supporting any Intelligent Controller card formats.
2.4.2. Input holds door unlocked

XX, NO - Input Holds Door Unlocked
*-Change

This record determines when the door will re-lock using the re-lock delay.

<table>
<thead>
<tr>
<th>YES</th>
<th>The door lock will not re-lock until the door is closed. This is used where the lock mechanism, when locked, will stop the door closing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The door lock will re-lock (after the unlock time has expired, etc.) regardless of the door being open or closed.</td>
</tr>
</tbody>
</table>

2.4.3. Door unlocked until door open

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.

<table>
<thead>
<tr>
<th>YES</th>
<th>The door relay will stay activated (initialised by a valid card or PIN) until the door input is unsealed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The door relay will perform standard operation.</td>
</tr>
</tbody>
</table>

2.4.4. Override time zone

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

The programmed time zone will automatically unlock the door for the programmed time periods. Free access is allowed when the time zone is valid.

📌 Time zones are programmed in the Challenger in menu 13. Only Time zones 0 to 24 can be entered.

2.4.5. Override after entry

XX, NO - Override After Entry
*-Change

Select if the override takes effect immediately the time zone commences or after a user has entered.

<table>
<thead>
<tr>
<th>YES</th>
<th>Before the time zone will unlock the door, a user needs to enter the area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Automatic unlock will start at the time zones start time.</td>
</tr>
</tbody>
</table>
2.4.6. Report door unsecured/secure

Select if a door is to report.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>When a user badges their card on a door and/or access is granted, the door lock will unlock and send an “unsecured” message to history. When the door locks, a “secured” message will be sent to history.</td>
</tr>
<tr>
<td>NO</td>
<td>No reporting unless an alarm occurs (depends on input type).</td>
</tr>
</tbody>
</table>

This is only a reporting function. There is no event specified in the control panel. This function can only be used in conjunction with the next option!

2.4.7. Map (un)secure to (un)locked

Select if a door open and locked needs to be reported as unlocked.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>When a user badges their card on a door and/or access is granted, the door lock will unlock and send an unlocked message to history. When the door locks, a locked message will be sent to history.</td>
</tr>
<tr>
<td>NO</td>
<td>No reporting of unlocking.</td>
</tr>
</tbody>
</table>

This is only a reporting function

2.4.8. Report door open/close

Select if opening or closing of the door needs to be reported.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>Send a report to the printer and to management software when the input assigned to the door is sealed and then resealed.</td>
</tr>
<tr>
<td>NO</td>
<td>No reporting unless an alarm occurs (depends on input type).</td>
</tr>
</tbody>
</table>

This is only a reporting function
2.4.9. Report forced door

Select if the opening of a door without a valid card, PIN or egress should be reported.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>Report opening of the door without a valid card, PIN or Egress to printer and management software.</td>
</tr>
<tr>
<td>NO</td>
<td>No reporting unless an alarm occurs (depends on input type).</td>
</tr>
</tbody>
</table>

*This is only a reporting function*

2.4.10. Report DOTL

Report when the door is open too long. This is only a reporting function

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>Report to the printer and to management software when the input assigned to the door is in the &quot;DOTL&quot; state, for example, still open after the shunt timer expires.</td>
</tr>
<tr>
<td>NO</td>
<td>No reporting unless an alarm occurs (depends on input type).</td>
</tr>
</tbody>
</table>

2.4.11. Reader LED options

This record specifies the states indicated by reader LEDs (not applicable for readers on the sub-LAN).

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>LED 1 On When Locked LED 1 is on, when the door is locked.</td>
</tr>
<tr>
<td>1</td>
<td>LED 1 On When Unlocked LED 1 is on, when the door is unlocked.</td>
</tr>
<tr>
<td>2</td>
<td>LED 1 On When Area is Armed 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).</td>
</tr>
<tr>
<td>3</td>
<td>LED 1 Off When Area is Armed 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.)</td>
</tr>
<tr>
<td>4</td>
<td>Two LED Access/Secure Readers with dual LED control lines connected indicate the area disarmed and armed with different LED colours.</td>
</tr>
<tr>
<td>5</td>
<td>Two LED Valid/Void Readers with dual LED control lines connected indicate User Valid or Void using different LED colours.</td>
</tr>
<tr>
<td>6</td>
<td>LED's Disabled No LED control.</td>
</tr>
</tbody>
</table>
On readers with dual LED control lines, LED 2 may also be programmed to indicate other conditions using Intelligent Controller's macro logic programming.

See also Areas assigned to door on page 43.

2.4.12. Pulsed lock and unlock relays

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

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 (see page 40).
- The second relay number is automatically assigned by the Intelligent Controller, which takes the next sequential relay number.

For example, if 17 is entered in Lock Relay, and relay option is set to 'Yes', then relays 17 and 18 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 (see page 41).
- 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).

Operation

**Door Open process** — 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).

![Door Open process timing diagram](image)

**Door Lock process** — The second relay will pulse on for 0.5 seconds (refer to Figure 2).
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.

### 2.4.13. Random percentage

<table>
<thead>
<tr>
<th>XX, Random Percentage 0</th>
<th>Percentage:</th>
</tr>
</thead>
</table>

Records a percentage value between 0 and 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 were set to 20, the door random bit event would be activated an average of once every five times a valid card or PIN is successfully used at the reader.

### 2.4.14. Time & attendance reader

| XX, Yes – Time & Attendance Reader | *-Change |

This option is not fully supported at present.

If set to YES, the LCD RAS can be used as a time and attendance reader.

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:59</td>
<td>03/02/05</td>
</tr>
</tbody>
</table>

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

**Method 1: Clock On**

To clock on, key in the user PIN code and press On. The current time and date will appear for about a second before this screen appears:
Method 1: Clock Off

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

Access granted
Clocked off

Method 2: Clock On (LCD keypad only)

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

8:59 03/02/03
Clock On _

Method 2: Clock Off (LCD keypad only)

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

8:59 03/02/03
Clock Off _

Wiegand options: If a door is set up with two Wiegand readers (marked “doors” on the control panel PCB), one reader for Clock On and one for Clock Off, and the readers share a lock relay (Hardware options: Lock Relay Number), the panel will always regard the reader with the lower door number as the Clock On reader. The panel will also regard the reader with the higher door number as the Off reader. Onboard Wiegand interfaces are designated to be In, unless they share the same lock relay.

Example, reader 17, the Clock On reader (door 17 on the panel PCB) is connected to a lock relay no.17. Reader 18 (door 18 on the PCB), the second reader at the door, is connected to the same lock relay, and its reader (door) number 18 was unlocked to share lock relay 17. It now becomes another reader 17. The panel will always regard the second reader (originally 18, but now 17) as the Out reader, because it has the higher original reader (door) number.

On a card reader, badging a card automatically clocks you on or off.

The default RAS settings on the Intelligent Controller LAN are 1-8 in, and 9-16 out. The table below lists the defaults for the Clock On and Off readers on the panel.

<table>
<thead>
<tr>
<th>Door</th>
<th>Default Clock On Readers</th>
<th>Default Clock Off Readers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

Note that RAS 5-18 and RAS 16-16 are used where PIN and prox combination are used on the same door.
2.4.15. Disable duress

<table>
<thead>
<tr>
<th>XX, NO - Disable Duress</th>
<th>*-Change</th>
</tr>
</thead>
</table>

This option is used to disable duress codes from functioning.

<table>
<thead>
<tr>
<th>YES</th>
<th>No duress function available at this door.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The Duress function is available.</td>
</tr>
</tbody>
</table>

2.5. Hardware options

<table>
<thead>
<tr>
<th>5-Hardware Options</th>
<th>XX, Menu:</th>
</tr>
</thead>
</table>

Challenger input and relay numbers are used in these records. All numbers used in the Intelligent Controller installer programming menus should correspond with the numbers used in the Challenger Installer menus.

The Intelligent Controller, when assigned an address, automatically calculates its default input and relay numbers (see Door/lift data hardware defaults, page 58). The Intelligent 4-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.

If inputs are disabled, they revert to being normal DGP system inputs.

Any input assigned as Door Contact input or DOTL input also have to be programmed in the Challenger Installer menu 1. Input Database (defines how the Challenger responds to alarms on these inputs).

See also Table 4 on page 57.

2.5.1. Lock relay

<table>
<thead>
<tr>
<th>XX, Lock Relay nn</th>
<th>*-Dis, Relay:</th>
</tr>
</thead>
</table>

This menu specifies the Intelligent Controller relay number 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 (see page 37), the relay number is entered in this menu.
2.5.2.  **Input**

<table>
<thead>
<tr>
<th>XX, Input nnn</th>
</tr>
</thead>
<tbody>
<tr>
<td>*-Dis, Input:</td>
</tr>
</tbody>
</table>

This menu specifies the input number to be used for a Door contact on the Intelligent Controller.

If using pulsed lock and unlock, the input number is entered in this menu (see page 37).

2.5.3.  **Monitor 2nd door input**

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

When programmed, the spare input is used as a second door contact.

<table>
<thead>
<tr>
<th>YES</th>
<th>Treat the spare input as second door contact.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The spare input remains available as spare.</td>
</tr>
</tbody>
</table>

2.5.4.  **Forced relay**

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

The Intelligent Controller relay number to be activated when an input is in a "Forced Door" condition, for example, the door has been opened without a valid command.

2.5.5.  **Shunt input**

<table>
<thead>
<tr>
<th>XX,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shunt Input:</td>
</tr>
</tbody>
</table>

The input number(s) on the Intelligent Controller that require to be shunted when the door is accessed (typically the same number as the input number).

2.5.6.  **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.
2.5.7. 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).

2.5.8. 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.

2.5.9. 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.

2.5.10. Door interlock

Door not Interlocked
Int. Input:

This menu stipulates the input numbers on the Intelligent Controller that prevents the doors being accessed at the same time. 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.
2.5.11. Areas assigned to door

<table>
<thead>
<tr>
<th>No Areas Assigned To Door</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area:</td>
</tr>
</tbody>
</table>

The area(s) specified here are used for:

- Controlling reader LEDs, if options #2 or #3 are selected in Reader LED options on page 36.
- Controlling access through a door when denied if the area is secure (see page 32).
- Controlling the use of egress functionality when egress is denied if the area is secure (see page 29).

Although the area(s) listed here are NOT used for area control, the Intelligent Controller DOES need to identify the status of these area(s) to know whether to send an arm or disarm command to the Challenger. This is only when using cards by themselves for arming/disarming, e.g. 'Alarm Control on 1st or 3rd badge'. Please remember that the Alarm group in 'Menu 3' determines the area(s) allowed to be armed/disarmed by a user, not the area(s) listed here.

2.5.12. Fault relay

<table>
<thead>
<tr>
<th>XX, Fault Relay Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>*-Dis, Relay:</td>
</tr>
</tbody>
</table>

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.

2.6. Lift options

<table>
<thead>
<tr>
<th>6 Lift Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>XX, Menu</td>
</tr>
</tbody>
</table>

These options apply to the TS0869 4-Lift Intelligent Controller.

2.6.1. Starting floor

<table>
<thead>
<tr>
<th>XX, First Floor 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>*-Dis, Floor:</td>
</tr>
</tbody>
</table>

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. Also, see the next option, 'Last Floor'.

2.6.2. 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. Also, see the previous option, ‘Starting Floor’.

2.6.3. 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 disarm and arm floors.

For example, if this lift was controlling floors 1 to 8 and the relays used to disarm those floors, were outputs 21 to 28 on the TS0869, then enter 21 here. When this value is entered, the TS0869 interprets this as follows:

- Physical relay is 21 (‘physical’ meaning the actual relay on board the TS0869).
- Starting floor is 1 and last floor is 8, meaning 8 floors.
- Therefore, the physical relay range is 21 to 28 (relays 21 to 28 on this TS0869 are used for this lift to arm and disarm floors).

The TS0869 automatically calculates the last relay number required to arm and disarm the floors it controls, as defined by ‘Starting Floor’ and ‘Last Floor’.

2.6.4. Inputs monitor floor selected

XX, NO - Inputs Monitor Floor Selected
*-Change

This record enables TS0869 inputs to monitor the floor selected, up to a maximum of 64 floors.

<table>
<thead>
<tr>
<th>YES</th>
<th>The TS0869 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If set to ‘YES’ then Security input cannot be used.</td>
</tr>
<tr>
<td>NO</td>
<td>Inputs are used as normal system alarm inputs, and the Security input, if enabled.</td>
</tr>
</tbody>
</table>
2.6.5. Wait for floor selection

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No - Wait For</td>
<td>The lift will wait for only one floor to be selected before going on.</td>
</tr>
<tr>
<td>Floor Selection</td>
<td></td>
</tr>
<tr>
<td>*-Change</td>
<td></td>
</tr>
</tbody>
</table>

Wait for floor selection before going on.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>The lift will wait for only one floor to be selected before going on.</td>
</tr>
<tr>
<td>NO</td>
<td>When the user is allowed access to multiple floors, multiple floors may be selected.</td>
</tr>
</tbody>
</table>

2.6.6. Starting physical input

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

This menu configures the starting input number for the TS0869 that it will be used to monitor the floors. When the user accesses a floor (a floor button pressed in the lift), the TS0869 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 TS0869 will be used to monitor the floors. Floor 1 uses input 9; Floor 2 uses input 10, etc.

The TS0869 automatically calculates the last input by the number of floors it is controlling. The floor range is configured using the options 'Starting Floor' and 'Last Floor'.

2.6.7. Lift override group

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

Records a Floor group number. Each floor group is programmed with floor(s) and a time zone.

The Lift override group determines the floor(s) that may be freely accessed in the lift controls, and the times during which they can be disarmed without using a valid card or PIN at the lift reader.

2.6.8. Security input

XX, Security Input Disabled
*-Dis, Input:

This menu specifies the input number on the TS0869 that will control the "Lift Security Group". See "Lift Security Group" description below.

⚠️ "Inputs Monitor Floor Selected" must be set to NO if the Security Group Input is used.
2.6.9. **Lift security group**

Records a floor group number. Each floor group is programmed with floor(s) and a time zone. The *Lift override group* determines the floor(s) that maybe freely accessed in the lift controls, and the times during which they may be accessed provided that the Security Input (keyswitch) is switched on.

See previous option "Security Input " above.

2.6.10. **Total floors**

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

2.6.11. **Lift bank**

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

2.6.12. **Lift car**

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

2.6.13. **Floor landings 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
```
2.6.14. **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 for an example of the display.

2.6.15. **Monitor high level floor landing**

Select whether the floor that the lift is currently at is monitored. Usually set to NO due to the large amount of data generated.

<table>
<thead>
<tr>
<th>YES</th>
<th>Monitor floor landings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Do not monitor floor landings.</td>
</tr>
</tbody>
</table>

3. **Initialize database**

**Initialise database**

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

**CAUTION!** Programming menu 3, Initialise Database, defaults the Intelligent Controller database, resetting ALL programming options to the factory defaults.

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

The display will show the doors that are being initialised.
4. Display card

Display card detail of the last card badged

Display Card
Menu:

This menu is available 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 menu may be used to reveal the card’s site code.

**CAUTION!** Part of the programming must to be completed before the correct information will be displayed. The readers must be working, available, and configured for the correct card formats.

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 (0)
ENTER - Exit:

When a card has been badged:

USER
256:SC722,ID256[240.0.0.3.4.1.0]

In this example, the site code is 722, the card ID is 256, 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).
5. Door groups

CAUTION! This 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.

Permanent changes to door groups should be programmed in the Challenger User Menu 20, “Door Groups and Floor Groups”

Viewing door group details

5-Door Groups
Menu:

Select a door group to view/modify. Each door group contains a list of all doors. In this menu, only doors that belong to the Intelligent Controller being programmed are displayed along with the time zone assigned to that door.

Select a door number to view. View time zones for the door. Be careful when modifying data.

Authorised access is only valid (will be granted) during the time zone.

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.

Example of the display:

Select a door group to program.

Door Group To Program
Group:

Select a door number to program.

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

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

Group 1, D17-**, D18-**, D19-**,
*-Dis, Door17TZ:
6. Lift groups

**CAUTION! This 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.**

*Permanent changes to lift groups should be programmed in the Challenger User Menu 20, *Door Groups and Floor Groups* *

Viewing lift group details

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

Select a floor group to view or modify. Each floor group contains a list of 64 possible floors. In this menu, all 64 floors are displayed along with the time zone assigned to each floor.

Select a floor number to view. View time zones for the lift (be careful when modifying data).

Authorised access is only valid (will be granted) during the time zone.

- **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.

Example of the display:

Select a lift group to program.

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

Select a floor number to program.

```
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:
```
7. System options

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 the Challenger Installer’s programming menu 16, Relay Mapping. 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.

For a list of available outputs, see Short list of available inputs and outputs per DGP address on page 57

7.1. Mains fail relay

XX, Mains Fail Relay Disabled
*Dis, Relay:

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

7.2. Low battery relay

XX, Low Battery Relay Disabled
*Dis, Relay:

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

7.3. Tamper relay

XX, Tamper Relay Disabled
*Dis, Relay:

This menu specifies the Intelligent Controller relay number to be activated when a “Cabinet Tamper” or a “Siren Fault” condition exists on the Intelligent Controller.
8. Macro logic

Macro logic programming

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

Up to four macro inputs may be included in the logic equation. A macro input is an event flag. 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, which may be; a pulse, timed, on delay, off delay or latched when activated.

The event flags are pre-defined Event flag Numbers as listed in the table, Macro event flags (page 59). Some can only be used for macro inputs; some for macro outputs and others may be used for both.

For more information on Macro Logic programming, refer to the programming guide for any Challenger.

CAUTION! It is very important to plan the Macro Logic carefully on paper, noting all details before attempting to program.

8.1. Macro logic program number

Enter the number of the Macro logic program. There are 48 programs available.
8.2. Function and output 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>This macro logic program is disabled.</td>
</tr>
<tr>
<td>Non Timed</td>
<td>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.</td>
</tr>
<tr>
<td>On Pulse</td>
<td>Activates for the programmed time or the active period of the logic result, whichever is the shortest.</td>
</tr>
<tr>
<td>On Timed</td>
<td>Activates for the programmed time regardless of the macro inputs changing.</td>
</tr>
<tr>
<td>On Delay</td>
<td>Activates after the programmed time period unless the result of the logic equation is no longer valid.</td>
</tr>
<tr>
<td>Off Delay</td>
<td>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.</td>
</tr>
<tr>
<td>Latched</td>
<td>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).</td>
</tr>
</tbody>
</table>

How to program

Press one of these keypad buttons to:

- [MENU*] Display a new output function.
- 0 Leave the menu
- * [ENTER] Enter the event flag number. Activates if the result of the logic equation is true.
- [ENTER] Save the displayed function and move to the next display.

8.3. Time

The time period (1 – 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).
8.4. Logic equation

Program up to four macro inputs (e.g., Intelligent Controller 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.

How to program

Press one of these keypad buttons to:

? [ENTER] Enter and display new event flag number. Enter the same number twice to invert the macro input. Before calculating the result of the macro logic equation, the input is inverted. An inverted input is recognised by the exclamation mark (!) preceding the “E”.

[MENU*] Toggle between OR or AND function.

[ENTER] Save the displayed details and move to the next display.
9. Version number

This menu is used to retrieve version number information from the Challenger control panel. The display will first show the Intelligent Controller Firmware version with copyright information.

Abbreviations used:
- NIUM = no IUM installed
- LIUM = large IUM installed
- SIUM = small IUM installed

10. Remote controllers

The Intelligent Controller allows RASs to be connected to the Intelligent Controller LAN. This Intelligent Controller LAN is often used to connect Wiegand readers to the DGP over large distances using the TS0862 Smart Door Controller. This menu is available for programming the TS0862 in the same way you program TS0862s on the Challenger LAN with menu 28.

After the menu has been entered, select the device type (RAS or DGP), and then select the device’s address. After this, the selected device may be programmed.
11. Display IUM user

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 check the following:
- The user number exists in the Intelligent Controller’s memory.
- The raw card data (RCD) is associated with the user number.
Additional reference topics

RAS programming

Refer to the RAS’s specifications and the particular application to know whether to program the options for:

- LCD RAS
- Card reader options
- Egress mode
- Toggle mode

Short list of available inputs and outputs per DGP address

The following list shows the available physical inputs and outputs per DGP address.

**NOTE:** The four on-board lock relays are treated as the first four output numbers assigned to the DGP address.

*Table 4 — Hardware options: physical inputs and outputs per DGP address*

<table>
<thead>
<tr>
<th>DGP no’s</th>
<th>Door numbers</th>
<th>Physical inputs</th>
<th>Physical outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17 – 20</td>
<td>17 – 32</td>
<td>17 – 32</td>
</tr>
<tr>
<td>2</td>
<td>21 – 24</td>
<td>33 – 48</td>
<td>33 – 48</td>
</tr>
<tr>
<td>3</td>
<td>25 – 28</td>
<td>49 – 64</td>
<td>49 – 64</td>
</tr>
<tr>
<td>5</td>
<td>33 – 36</td>
<td>81 – 96</td>
<td>81 – 96</td>
</tr>
<tr>
<td>6</td>
<td>37 – 40</td>
<td>97 – 112</td>
<td>97 – 112</td>
</tr>
<tr>
<td>7</td>
<td>41 – 44</td>
<td>113 – 128</td>
<td>113 – 128</td>
</tr>
<tr>
<td>8</td>
<td>45 – 48</td>
<td>129 – 144</td>
<td>129 – 144</td>
</tr>
<tr>
<td>9</td>
<td>49 – 52</td>
<td>145 – 160</td>
<td>145 – 160</td>
</tr>
<tr>
<td>10</td>
<td>53 – 56</td>
<td>161 – 176</td>
<td>161 – 176</td>
</tr>
<tr>
<td>11</td>
<td>57 – 60</td>
<td>177 – 192</td>
<td>177 – 192</td>
</tr>
<tr>
<td>12</td>
<td>61 – 64</td>
<td>193 – 208</td>
<td>193 – 208</td>
</tr>
</tbody>
</table>
Door/lift data hardware defaults

Table 5 — Hardware options: default input/output number assignments

<table>
<thead>
<tr>
<th>Function</th>
<th>Door</th>
<th>DGP No. (address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 2 3 4 5 6 7 8 9 10 11 12</td>
</tr>
<tr>
<td>Lock relay</td>
<td>1st door</td>
<td>17 33 49 65 81 97 113 129 145 161 177 193</td>
</tr>
<tr>
<td></td>
<td>2nd door</td>
<td>18 34 50 66 82 98 114 130 146 162 178 194</td>
</tr>
<tr>
<td></td>
<td>3rd door</td>
<td>19 35 51 67 83 99 115 131 147 163 179 195</td>
</tr>
<tr>
<td></td>
<td>4th door</td>
<td>20 36 52 68 84 100 116 132 148 164 180 196</td>
</tr>
<tr>
<td>Input</td>
<td>1st door</td>
<td>17 33 49 65 81 97 113 129 145 161 177 193</td>
</tr>
<tr>
<td></td>
<td>2nd door</td>
<td>20 36 52 68 84 100 116 132 148 164 180 196</td>
</tr>
<tr>
<td></td>
<td>3rd door</td>
<td>23 39 55 71 87 103 119 135 151 167 183 199</td>
</tr>
<tr>
<td></td>
<td>4th door</td>
<td>26 42 58 74 90 106 122 138 154 170 186 202</td>
</tr>
<tr>
<td>DOTL input</td>
<td>1st door</td>
<td>32 48 64 80 96 112 128 144 160 176 192 208</td>
</tr>
<tr>
<td></td>
<td>2nd door</td>
<td>31 47 63 79 95 111 127 143 159 175 191 207</td>
</tr>
<tr>
<td></td>
<td>3rd door</td>
<td>30 46 62 78 94 110 126 142 158 174 190 206</td>
</tr>
<tr>
<td></td>
<td>4th door</td>
<td>29 45 61 77 93 109 125 141 157 173 189 205</td>
</tr>
<tr>
<td>Egress input</td>
<td>1st door</td>
<td>19 35 51 67 83 99 115 131 147 163 179 195</td>
</tr>
<tr>
<td></td>
<td>2nd door</td>
<td>22 38 54 70 86 102 118 134 150 166 182 198</td>
</tr>
<tr>
<td></td>
<td>3rd door</td>
<td>25 41 57 73 89 105 121 137 153 169 185 201</td>
</tr>
<tr>
<td></td>
<td>4th door</td>
<td>28 44 60 76 92 108 124 140 156 172 188 204</td>
</tr>
<tr>
<td>Shunt input</td>
<td>1st door</td>
<td>17 33 49 65 81 97 113 129 145 161 177 193</td>
</tr>
<tr>
<td></td>
<td>2nd door</td>
<td>20 36 52 68 84 100 116 132 148 164 180 196</td>
</tr>
<tr>
<td></td>
<td>3rd door</td>
<td>23 39 55 71 87 103 119 135 151 167 183 199</td>
</tr>
<tr>
<td></td>
<td>4th door</td>
<td>26 42 58 74 90 106 122 138 154 170 186 202</td>
</tr>
</tbody>
</table>

Table 6 — Lift options: relay and input numbers

<table>
<thead>
<tr>
<th>Lift values</th>
<th>Starting physical relay</th>
<th>Starting physical input</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st lift</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2nd lift</td>
<td>65</td>
<td>65</td>
</tr>
<tr>
<td>3rd lift</td>
<td>129</td>
<td>129</td>
</tr>
<tr>
<td>4th lift</td>
<td>193</td>
<td>193</td>
</tr>
</tbody>
</table>

Refer to Table 1 on page 16 for details of RAS addresses for IN and OUT functionality.
## Macro event flags

### Door & floor related pre-defined events

<table>
<thead>
<tr>
<th>Event name</th>
<th>Description</th>
<th>Input (I), Output (O)</th>
<th>Door</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOOR OPEN</strong></td>
<td>Door Open command is active (to unlock / start shunt)</td>
<td>I / O</td>
<td>1 2 3 4</td>
</tr>
<tr>
<td><strong>DOOR UNLOCKED</strong></td>
<td>Lock output is active to unlock the door</td>
<td>I / O</td>
<td>9 10 11 12</td>
</tr>
<tr>
<td><strong>DOOR LOCK</strong></td>
<td>Lock output is de-activated to lock the door</td>
<td>O</td>
<td>17 18 19 20</td>
</tr>
<tr>
<td><strong>DOOR OVERRIDE</strong></td>
<td>The override time zone assigned to the door is valid</td>
<td>I / O</td>
<td>25 26 27 28</td>
</tr>
<tr>
<td><strong>DOOR OVERRIDE INHIBIT</strong></td>
<td>The override time zone is inhibited</td>
<td>I / O</td>
<td>33 34 35 36</td>
</tr>
<tr>
<td><strong>DOOR DISABLED</strong></td>
<td>Door is disabled completely (from keypad or computer)</td>
<td>I / O</td>
<td>41 42 43 44</td>
</tr>
<tr>
<td><strong>DOOR ENABLED</strong></td>
<td>Door is enabled</td>
<td>O</td>
<td>49 50 51 52</td>
</tr>
<tr>
<td><strong># DOOR READER DISABLED</strong></td>
<td>Reader is disabled</td>
<td>I / O</td>
<td>57 58 59 60</td>
</tr>
<tr>
<td><strong>DOOR READER ENABLED</strong></td>
<td>Reader is enabled</td>
<td>O</td>
<td>65 66 67 68</td>
</tr>
<tr>
<td><strong>DOOR DUAL CUSTODY INSIDE</strong></td>
<td>Dual Custody access is required at the &quot;IN&quot; reader</td>
<td>I / O</td>
<td>73 74 75 76</td>
</tr>
<tr>
<td><strong>DOOR DUAL CUSTODY OUTSIDE</strong></td>
<td>Dual Custody access is required at the &quot;OUT&quot; reader</td>
<td>I / O</td>
<td>81 82 83 84</td>
</tr>
<tr>
<td><strong>DOOR LOW SECURITY INSIDE</strong></td>
<td>Card and PIN required to access at the &quot;IN&quot; reader</td>
<td>I / O</td>
<td>89 90 91 92</td>
</tr>
<tr>
<td><strong>DOOR LOW SECURITY OUTSIDE</strong></td>
<td>Card and PIN required to access at the &quot;OUT&quot; reader</td>
<td>I / O</td>
<td>97 98 99 100</td>
</tr>
<tr>
<td><strong>DOOR ANTI PASSBACK</strong></td>
<td>Anti Passback is active</td>
<td>I / O</td>
<td>101 102 103 104</td>
</tr>
<tr>
<td><strong>DOOR SHUNTING</strong></td>
<td>Shunt timer is running</td>
<td>I / O</td>
<td>113 114 115 116</td>
</tr>
<tr>
<td><strong>DOOR SHUNT WARNING</strong></td>
<td>Shunt warning timer is running</td>
<td>I</td>
<td>121 122 123 124</td>
</tr>
<tr>
<td><strong>DOOR AREA SECURE</strong></td>
<td>Area assigned to door is secure</td>
<td>I / O</td>
<td>129 130 131 132</td>
</tr>
<tr>
<td><strong>DOOR INTERLOCK</strong></td>
<td>Interlock input(s) are unsealed</td>
<td>I / O</td>
<td>137 138 139 140</td>
</tr>
<tr>
<td><strong>DOOR FORCED</strong></td>
<td>Door Contact is unsealed with no valid door command</td>
<td>I</td>
<td>145 146 147 148</td>
</tr>
<tr>
<td><strong>DOOR KEYPAD DURESS</strong></td>
<td>Duress PIN code entered at door keypad</td>
<td>I</td>
<td>153 154 155 156</td>
</tr>
<tr>
<td><strong>DOOR READER FAULT</strong></td>
<td>Fault detected on reader (Comms / tamper / etc)</td>
<td>I</td>
<td>161 162 163 164</td>
</tr>
<tr>
<td><strong>DOOR LOCK FAULT</strong></td>
<td>Cable tamper / fault detected on lock relay wiring</td>
<td>I</td>
<td>169 170 171 172</td>
</tr>
<tr>
<td><strong>DOOR DOTL</strong></td>
<td>Door Contact is unsealed after shunt timer has expired</td>
<td>I</td>
<td>177 178 179 180</td>
</tr>
<tr>
<td><strong>DOOR LED 1</strong></td>
<td>LED 1 output is active</td>
<td>I / O</td>
<td>185 186 187 188</td>
</tr>
<tr>
<td><strong>DOOR LED 2</strong></td>
<td>LED 2 output is active</td>
<td>I / O</td>
<td>193 194 195 196</td>
</tr>
<tr>
<td>Event name</td>
<td>Description</td>
<td>Input (I), Output (O)</td>
<td>Door 1</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>*** DOOR BUZZER</td>
<td>BUZZER output is active</td>
<td>I / O</td>
<td>209</td>
</tr>
<tr>
<td>*** DOOR RANDOM BIT</td>
<td>An event is generated at random when the door is accessed</td>
<td>I</td>
<td>217</td>
</tr>
<tr>
<td>DOOR ACCESS DENIED</td>
<td>Door access has not been allowed</td>
<td>I</td>
<td>225</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED</td>
<td>Door access has been allowed</td>
<td>I</td>
<td>233</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED TRACED</td>
<td>Door access has been granted to a user with trace On</td>
<td>I</td>
<td>241</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED 1ST BADGED</td>
<td>Door access has been granted when badged once</td>
<td>I</td>
<td>249</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED 2ND BADGED</td>
<td>Door access has been granted when badged twice</td>
<td>I</td>
<td>257</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED 3RD BADGED</td>
<td>Door access has been granted when badged three times</td>
<td>I</td>
<td>265</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED IN BUTTON</td>
<td>Door access has been granted and IN button pressed</td>
<td>I</td>
<td>273</td>
</tr>
<tr>
<td>DOOR ACCESS GRANTED OUT BUTTON</td>
<td>Door access has been granted and OUT button pressed</td>
<td>I / O</td>
<td>281</td>
</tr>
<tr>
<td>DOOR FIRE OVERRIDE</td>
<td>Secondary override is active</td>
<td>I / O</td>
<td>289</td>
</tr>
<tr>
<td>DOOR SECURE</td>
<td>When the door is LOCKED and the door is CLOSED.</td>
<td>I</td>
<td>297</td>
</tr>
<tr>
<td>*** FLOOR ACCESSED</td>
<td>Free access available to floor (64 events - 1 per floor)</td>
<td>I / O</td>
<td>1537</td>
</tr>
<tr>
<td>*** FLOOR CALL BUTTON</td>
<td>Floor selection button pressed (64 events - 1 per floor)</td>
<td>I</td>
<td>2049</td>
</tr>
<tr>
<td>*** FLOOR DISABLED</td>
<td>Floor is disabled from being selected (64 events - 1 per floor)</td>
<td>I</td>
<td>2561</td>
</tr>
<tr>
<td>*** FLOOR LANDED</td>
<td>Floor where lift car is currently landed (64 events - 1 per floor)</td>
<td>I</td>
<td>3073</td>
</tr>
<tr>
<td>*** FLOOR SEND</td>
<td>Command to send lift car to floor (64 events - 1 per floor)</td>
<td>O</td>
<td>3585</td>
</tr>
</tbody>
</table>

* 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.
## Other events

<table>
<thead>
<tr>
<th>Event name</th>
<th>Description</th>
<th>Input (I)</th>
<th>Output (O)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Access</td>
<td>Area in access (16 events - 1 per area)</td>
<td>I</td>
<td></td>
<td>513-528</td>
</tr>
<tr>
<td>Area Alarm</td>
<td>Input(s) in alarm in area (16 events - 1 per area)</td>
<td>I</td>
<td></td>
<td>529-544</td>
</tr>
<tr>
<td>* Area Isolated</td>
<td>Input(s) isolated in area (16 events - 1 per area)</td>
<td>I</td>
<td></td>
<td>545-560</td>
</tr>
<tr>
<td>* Area Unsealed</td>
<td>Input(s) unsealed in area (16 events - 1 per area)</td>
<td>I</td>
<td></td>
<td>561-576</td>
</tr>
<tr>
<td>DGP Relays</td>
<td>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.</td>
<td>I</td>
<td></td>
<td>577-592</td>
</tr>
<tr>
<td>RAS Offline</td>
<td>RAS on Intelligent Controller sub-LAN is offline (16 events - 1 per RAS address)</td>
<td>I</td>
<td></td>
<td>593-608</td>
</tr>
<tr>
<td>DGP Offline</td>
<td>DGP on Intelligent Controller sub-LAN is offline.</td>
<td>I</td>
<td></td>
<td>609-624</td>
</tr>
<tr>
<td>Inputs</td>
<td>Input on this DGP is unsealed (16 events - 1 per input)</td>
<td>I/O</td>
<td></td>
<td>769-784</td>
</tr>
<tr>
<td>*Auxiliary 1 Input Event</td>
<td>Special interface required. (32 events)</td>
<td>I</td>
<td></td>
<td>801-832</td>
</tr>
<tr>
<td>*Auxiliary 2 Input Event</td>
<td>Special interface required. (32 events)</td>
<td>I</td>
<td></td>
<td>833-864</td>
</tr>
<tr>
<td>*Auxiliary 3 Input Event</td>
<td>Special interface required. (32 events)</td>
<td>I</td>
<td></td>
<td>865-896</td>
</tr>
<tr>
<td>*Auxiliary 4 Input Event</td>
<td>Special interface required. (32 events)</td>
<td>I</td>
<td></td>
<td>897-928</td>
</tr>
<tr>
<td>Region Limit</td>
<td>When the number of people in any region reaches the present limit (255 events - 1 per region)</td>
<td>I</td>
<td></td>
<td>1025-1280</td>
</tr>
<tr>
<td>Physical Relays</td>
<td>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.</td>
<td>I/O</td>
<td></td>
<td>1281-1536</td>
</tr>
<tr>
<td>* Controller Mains Fail</td>
<td>Mains fail condition exists on the Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4081</td>
</tr>
<tr>
<td>* Controller Low Battery</td>
<td>Low battery condition exists on the Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4082</td>
</tr>
<tr>
<td>* Controller Battery Test Active</td>
<td>The battery test on this Controller is running (1 event)</td>
<td>I</td>
<td></td>
<td>4083</td>
</tr>
<tr>
<td>* Controller Battery Test Fail</td>
<td>The battery test failed on this Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4084</td>
</tr>
<tr>
<td>* Controller Fuse Fail</td>
<td>Fuse Fail condition exists on the Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4085</td>
</tr>
<tr>
<td>* Controller Siren Fail</td>
<td>Siren fail (siren tamper) condition exists on this Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4086</td>
</tr>
<tr>
<td>* Controller Siren Active</td>
<td>The siren output (16th relay) is active (1 event)</td>
<td>I</td>
<td></td>
<td>4087</td>
</tr>
<tr>
<td>* Controller Tamper</td>
<td>Cabinet tamper condition exists on this Controller (1 event)</td>
<td>I</td>
<td></td>
<td>4088</td>
</tr>
<tr>
<td>* Controller DGP Offline</td>
<td>Controller is not communicating with the Challenger (1 event)</td>
<td>I</td>
<td></td>
<td>4089</td>
</tr>
</tbody>
</table>

* Denotes the event is currently not enabled.
### Intelligent Controller Programming Sheets

#### Menu 1. Controller Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>Programmed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Controllers</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Site Code A</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Card Offset A</td>
<td>Positive 0</td>
<td>Positive 0</td>
<td></td>
</tr>
<tr>
<td>Site Code B</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Card Offset B</td>
<td>Positive 0</td>
<td>Positive 0</td>
<td></td>
</tr>
<tr>
<td>Alarm Code Prefix Length</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Poll RAS</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>RAS with LCD</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>RAS with Egress enabled</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>RAS with Toggle mode</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Poll DGP</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Tamper Monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Card to PIN Time</td>
<td>8 Seconds</td>
<td>8 Seconds</td>
<td></td>
</tr>
<tr>
<td>Dual Custody Time</td>
<td>8 Seconds</td>
<td>8 Seconds</td>
<td></td>
</tr>
<tr>
<td>Mode Time</td>
<td>5 Seconds</td>
<td>5 Seconds</td>
<td></td>
</tr>
<tr>
<td>Lock Release Time</td>
<td>3 Seconds</td>
<td>3 Seconds</td>
<td></td>
</tr>
<tr>
<td>Region Count Threshold</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Siren Monitoring</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Forced Door Debounce Time</td>
<td>700 ms</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

#### Menu 7. System Options

<table>
<thead>
<tr>
<th>System options</th>
<th>Door defaults</th>
<th>Lift defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mains Fail Relay</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Low Battery Relay</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tamper Relay</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Menu 2. Door Options > 1. Access Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Time</td>
<td>5 Seconds</td>
<td>5 Seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Access Time</td>
<td>10 Seconds</td>
<td>10 Seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shunting</td>
<td>No Shunting</td>
<td>No Shunting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shunt Time</td>
<td>60 Seconds</td>
<td>0 Seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Shunt Time</td>
<td>90 Seconds</td>
<td>0 Seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shunt Warning Time</td>
<td>15 Seconds</td>
<td>0 Seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Security Time Zone</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Reader Card &amp; PIN</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Reader Card &amp; PIN</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Reader Inhibit PIN</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Reader Inhibit PIN</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti Passback</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Region</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Region</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANTI Passback Time</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Reader Dual Custody</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Reader Dual Custody</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Menu 2. Door Options > 2. Egress Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Time Zone</td>
<td>0</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Egress Dis. If Secure</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Egress Dis. if Secure</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress Control</td>
<td>Times Door Open</td>
<td>Times Door Open</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress Reporting</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Menu 2. Door Options > 3. Alarm Control

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Group</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Control</td>
<td>None</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN Denied if Secure</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUT Denied if Secure</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorised RAS Number</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Menu 2. Door Options > 4. Reader Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Format</td>
<td>Tecom ASC</td>
<td>Tecom ASC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Holds Door Unlocked</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override Time zone</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override After Entry</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open/Close Reporting</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forced Door Reporting</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOTL Reporting</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reader LED Option</td>
<td>LED 1 on when locked</td>
<td>LED 1 on when locked</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulsed Lock &amp; Unlock</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time &amp; Attendance Reader</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable Duress</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Menu 2. Door Options > 5. Hardware Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Relay No.</td>
<td>See page 58</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Number</td>
<td>See page 58</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forced Door Relay</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shunt Input</td>
<td>See page 58</td>
<td>NONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning Relay</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOTL Input</td>
<td>See page 58</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOTL Relay</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress Input</td>
<td>See page 58</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interlock Input</td>
<td>Door not interlocked</td>
<td>Door not interlocked</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area/s Assigned</td>
<td>None</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault Relay</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Menu 2. Door Options > 6. Lift Options

<table>
<thead>
<tr>
<th>Function</th>
<th>Door defaults</th>
<th>Lift defaults</th>
<th>1st Door or Lift No:</th>
<th>2nd Door or Lift No:</th>
<th>3rd Door or Lift No:</th>
<th>4th Door or Lift No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Floor</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Floor</td>
<td>64</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Starting Physical Relay</td>
<td>See page 58</td>
<td>See page 58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zones Monitor Floor</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Starting Physical Input</td>
<td>See page 58</td>
<td>See page 58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lift Override Group</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Zone</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lift Security Group</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Menu 8. Macro Logic

<table>
<thead>
<tr>
<th>Macro Logic</th>
<th>Output Event</th>
<th>1st Input Event</th>
<th>And / Or</th>
<th>2nd Input Event</th>
<th>And / Or</th>
<th>3rd Input Event</th>
<th>And / Or</th>
<th>4th Input Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Function</td>
<td>Time</td>
<td>NOT</td>
<td>No.</td>
<td>Logic</td>
<td>NOT</td>
<td>No.</td>
<td>Logic</td>
</tr>
</tbody>
</table>
Glossary

Access control  The control of entry to, or exit from, a secure area.

Active  See Sealed/Unsealed/Tamper/Inhibited

Alarm  See Burglar alarm

Alarm group  Alarm groups define the options available to users, arming stations or door reader to allow alarm control. Alarm groups are defined by, areas, alarm control functions and menu options.

Input types for area control (keyswitches) also make use of alarm groups.

Alarm group restriction  An alarm group restriction may be assigned to an alarm group to enable different types of user to:

- Use the timed disarm option for specific areas(s)
- Restrict alarm control to “Arm/reset only” on specific areas(s)
- Utilise the “User Count” or “Emergency” function.

Alarm reporting  A procedure to transmit alarm and other events to a central station by a dialler using a set of rules called a protocol.

Alarm control  The control of alarm functions.

Anti-passback  A record is kept on the movement of users. To be able to perform the operation, users need to present their card or PIN when entering or leaving premises. Anti-passback might inhibit users entering the premises if they did not register leaving.

Area  A section of a premise with specific security requirements. The Challenger system allows any premise to be divided into 16 areas (max) each having different security requirements and its own inputs. Every area is identified by a unique number and name. e.g. Area 1 Office, Area 2 Workshop, Area 3 Boardroom, etc.

Armed  The condition of an area where a change in the status of any input (from sealed to unsealed) causes an alarm. An area or premise is normally only armed when it is unoccupied. Some inputs (like vaults) may always be armed.

Arming stations (RAS)  A device that is the user’s control panel to control security functions for an area(s) or access points (doors). The arming station may be an Challenger console (LCD keypad or reader) or any other device that may be used to perform security functions, such as arm/disarm, open doors, etc.

Burglar alarm  An alarm triggered by a security device such as a PIR or door contact, indicating someone has entered without authorised access.

Card  A credit card sized device that holds information to identify a user. The information, to identify a user, can be available on a magnetic strip, a bar-coded strip, and a Wiegand card or in a chip (smart cards).

Central station  A company that monitors alarms that may occur in a security system. A central station is usually located away from the premise or area it monitors.

Control panel  An electronic device that is used to gather all data from inputs within a premise. Depending on the programming and the status of the areas, it will generate alarm signals. If required, alarms and other events may be reported to a central station.

Cursor  A flashing underline character on the liquid crystal display (LCD) that indicates where the next character, entered at the keypad, will appear.

DGP  Data Gathering Panel. A device that collects data from other security devices within an area, and transfers it to the Challenger control panel or a 4-door/4-lift DGP.

Dialler  An electronic device that allows the Challenger system to transmit alarms and other events to a central station. May also be used to perform up/download.

Disarmed  The condition of an area when it is occupied and when the security system has been set so that normal activity does not cause an alarm.

Door contact  A magnetic contact used to detect when a door or window is opened.

Door control  The control over door functions.
Door group
An Challenger feature that assigns a group of doors or lifts to a user, in order to allow access to those doors/lifts. Access to each door in a group may be restricted by a time zone.

DUAL
Dual detector. A security device used to detect intruders in a certain part of an area or premises. The technique used is based on two technologies such as PIR and microwave or PIR and Ultrasonic.

Duress
A situation where a user is being forced to breach the system security (e.g. forced at gunpoint to open the premises). The Challenger duress facility allows a signal to be activated (e.g. notification to a central station) by the user. This is done by entering a duress digit in conjunction with a PIN code.

Engineer
Technician from a security company able to install and service the alarm system.

Event flags
A signal activated by; an input condition, an area condition, the system's status or fault condition, a door command (on doors 1 to 16) or a shunt condition. The main purpose of an event flag is to activate an output.

Fire alarm
An alarm triggered by fire or smoke detectors indicating a fire.

Floor group
An Challenger feature that assigns a group of floors to a user, to allow of floors to be selected when accessing a lift reader. Access to each floor in a group may be restricted by a time zone.

Floor control
See Door control.

History
A list of past alarm and access control events stored in memory that may be viewed on an LCD arming station or sent to a printer.

Hold-up
A (silent) alarm that is triggered by a hold-up button. Normally it will not trigger any sirens, only send a message to a central station.

Inhibit
See Normal/Active/Tamper/Inhibited

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.

Interlock
A method that stops two doors, close to each other, being opened at the same time. Used, for example, in vaults.

Installer
A security company technician that installs and services security equipment.

Keypad
A remote arming station with keys to input data (keypad). Used to program the control panel, perform user functions, view alarms, etc.

Keyswitch
A key operated device using a switch to arm or disarm areas etc.

LCD
(Liquid Crystal Display). The part of an arming station where messages are displayed.

LED
(Light Emitting Diode). A light on an arming station that conveys a condition (e.g. An area in alarm, a communication fault, etc).

Local alarm
An alarm that is signalled only within a premises and occurs when an area is occupied. The circumstances that cause a local alarm may be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be reported to a central station.

Logic equation
A logic expression that combines macro inputs in a specific manner. The result of a logic equation is called a macro output.

Macro input
An event flag or an output that is used in a logic equation. Each macro input is an event flag or output.

Macro logic program
A set of rules that is created by; macro inputs, logic equations and macro outputs that is used to trigger event flags or inputs.

Macro output
A macro output holds the result of a logic equation. The macro output may have a timing element. Macro outputs trigger event flags or inputs.

Nuisance alarm
An alarm that is triggered by a security device, without burglary. Could be caused by open windows, pets or incorrect alignment of security equipment.

Online/offline
Operational/non-operational. A device may be offline due to a malfunction in the device itself or it may be disconnected from the control equipment.
**Output controller**  A PCB module connected to the Challenger control panel or a DGP to provide relay or open collector outputs. When programming, one Output controller equals 8 outputs.

**Physical input/output** Intelligent Controller terminology. Includes the 4 onboard DGP relays and any controller boards to the same DGP LAN. These devices have an independent, LAN on which devices may be connected such as RAS’s or DGP’s. The control panel cannot address the physical relays.

**PIN code**  A 4 to 10 digit number given to, or selected by, a user. It is necessary to enter a PIN code at an Challenger keypad as a pre-requisite to performing most Challenger functions. In the Challenger programming the PIN code is associated with a user number that identifies the PIN code holder to the system.

**PIR**  Passive Infrared detector. A security device used to detect intruders in a certain part of an area or premises. The technology used is based on infrared detection.

**Poll**  An inquiry message continuously sent by an Challenger control panel to DGP’s and arming stations. Allows the remote device to transfer data to the control panel.

**RAS**  Remote Arming Station. See Arming station.

**Reader**  A device used for access control that can read cards to allow access. Depending on the needs and the type of cards, the reader may be a magnetic swipe reader or proximity reader.

**Region**  An area within a building used for access control features like anti-passback.

**Reporting**  See alarm reporting.

**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.

**Sealed/Unsealed/Tamper/Inhibited**  Describes the condition of an input.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sealed</td>
<td>The input is NOT activated, e.g. Fire Exit Door close.</td>
</tr>
<tr>
<td>Unsealed</td>
<td>The input is activated, e.g. Fire Exit Door open.</td>
</tr>
<tr>
<td>Tamper</td>
<td>The input is open or short-circuited. Someone may have tried to tamper with the security device.</td>
</tr>
<tr>
<td>Inhibited</td>
<td>The input has been inhibited from indicating normal or active status. It is excluded from functioning as part of the alarm system.</td>
</tr>
</tbody>
</table>

**Shunt**  A procedure automatically inhibiting an input from creating an alarm when it’s activated, e.g. shunts stop a door creating an alarm when opened for a short time.

**Tamper**  A situation where an arming station, control panel, an input, a DGP or associated wiring is tampered with, accidentally damaged, or an enclosure is opened. The Challenger tamper facility activates a signal when a tamper occurs. Tamper alarms from inputs are called input tampers.

**Time zone**  A programmed setting that identifies specific time periods on specific days. Time zones are allocated to Challenger functions to control the activity of that function by time and day and are primary used to restrict access for example, automatically arm or disarm areas or open doors.

**Up/Download**  A protocol providing means to view the status of an Challenger system or change parameters in the system programming either locally or remotely.

**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.
Index

Access time for doors/lifts, 21
Alarm code prefix digits, 15
Alarm control
  assigning, 31
  assigning alarm groups, 31
  IN/OUT disabled if area secure, 32
Alarm group assignment, 31
Anti-passback
  different types, 25
  programming, 25
Arming stations. See RAS
Automatic unlock after entry, 34
Cabinet tamper
  specifying output number, 51
Card to PIN time
  programming, 18
Cards
  displaying details, 48
  specifying card formats, 33
  zone holds door unlocked, 34
Database
  initialising, 47
Defaults, 47
DGP
  poll, 17
DGP options, 14
  Addresses being polled, 17
  alarm code prefix length, 15
  Card to PIN time, 18
  Lock Relock time, 19
  mode time, 19
  programming, 14
  RAS numbers, 16
  RAS requiring Egress, 16
  RAS with toggle mode, 17
  RAS's with LCD, 16
  region count limit, 19
  relay controllers, 14
  two cards time, 18
Disarming
  disarming the system, 10
Door and lifts
  selecting door/lift number, 21
Door groups
  programming, 49
  view, 49
Door/lift access options, 21–46
  access time, 21
  anti-passback, 25
  cancel shunt after door closed, 23
  deny region 0 user access, 25
  extended access time, 21
  extended shunt time, 22
  IN reader Two card function, 27
  IN/OUT reader regions, 26, 27
  inhibit PIN code, 24
  low security timezone, 23
  method for opening doors, 24
  OUT reader Two card function, 28
  overriding after entry, 34
  overriding timezones, 34
  region count limits, 19
  shunt conditions, 22
  shunt time, 22, 23
  shunt until door closed, 23
Door/lift alarm control options
  alarm group, 31
  function, 31
  IN/OUT disarmed if area secure, 32
Door/lift egress options
  IN/OUT egress disabled, 29
  programming, 28
  timezones, 28
Door/lift Egress options
  Egress control, 30
  IN/OUT RTE disabled, 29
  reporting, 30
Door/lift hardware options
  DOTL output number, 42
  DOTL zone number, 42
  Reporting DOTL alarm condition, 42
Door/lift options
  last floor of lift, 44
  lift bank selection, 46
  lift car selection, 46
  lift options programming, 43
  lift override group, 45
  lift security group, 46
  monitor high level floor landings, 47
  security group zone number, 45
  select floor landing, 46
  starting floor of lift, 43
  Starting floor of lift, 43
  starting physical relays, 44
  starting zone of lift, 45
  total number of floors, 46
  wait for floor to be selected, 45
  zones monitoring floor selected, 44
Door/lift programming menu
  accessing the menu, 12
Door/lift reader options
  card format, 33
  duress functionality, 40
  LED options, 36
  pulsed lock and unlock, 37
  report opening/closing door, 35
  reporting forced door, 36
  zone holds door unlocked, 34
DOTL
  DOTL alarm and shunt time, 22
  output number, 42
  reporting DOTL alarm condition, 42
Duress functionality, 40
Egress
  control, 30
  defining the operation, 30
  method for opening doors, 24
  OUT reader Two card function, 28
  overriding after entry, 34
  overriding timezones, 34
  region count limits, 19
  shunt conditions, 22
  shunt time, 22, 23
  shunt until door closed, 23
  zone number, 42
Extended access time for door and lifts, 21
Extended shunt time for doors/lifts, 22
Floor
landings, 46
Floor groups
programming floor group number, 45
Floors
first floor of lift, 43
Floors available, 46
Forced door
DOTL and forced door, 22
reporting, 36
Forced door debounce, 20
Function and output event
macro logic programming, 53
IN/OUT Egress disabled if area armed, 29
IN/OUT reader regions
programming access controlled region, 27
IN/OUT readers
 card & PIN, 24
egress disabled if area secure, 29
opening doors if area secure, 32
programming access controlled region, 26
Inhibit Pin code for opening doors, 24
Initialising the database, 47
Input numbers available, 57
Interlock zone numbers, 42
Lift bank selection, 46
Lift car selection, 46
Lift options
 floor landing, 46
floors available, 46
last floor of lift, 44
lift bank selection, 46
lift car selection, 46
lift override group, 45
lift security group, 46
monitor high level floor landings, 47
programming, 43
relay and input numbers, 58
security group zone number, 45
starting floor, 43
starting floor of lift, 43
starting physical relay, 44
starting zone of lift, 45
wait for floor to be selected, 45
zones monitor floor selected, 44
Lift security group, 46
List of available inputs and outputs, 57
List of physical relays and inputs, 58
Lock/reader fault
 activating output number, 43
Low battery condition
 output number, 51
Low security timezone
programming door opening, 24
Low security timezone for doors/lifts, 23
Macro logic
 function and output event number, 53
logic equations, 54
program number, 52
Mains fail condition
 output number, 51
Menu options
 explanation of the LCD display, 11
how to program, 11
how to program values, 11
how to program YES/NO options, 11
moving around between them, 10
programming, 11
Monitor high level floor landings, 47
Opening doors
card & PIN required, 24
programming method used during low security
timezone, 23
two cards required, 27, 28
Opening/closing doors
reporting, 35
Output numbers
activating when zone in, 41
list, 57
specifying physical outputs for lift, 44
Programming menu
accessing, 10
 explanation of the LCD display, 11
how to program, 11
Master engineer code, 10
moving around between the menu options, 10
Programming sheets
DGP options, 62
door options menu 1-3, 63
Pulsed lock and unlock, 37
door lock procedure, 37
door open procedure, 37
RAS
addresses to be polled, 16
Reader LED options
specifying, 36
Reader options
 automatic unlock after entry, 34
automatic unlock timezones, 34
card format, 33
DOTL zone number, 42
duress functionality, 40
Egress zone number, 42
fault output number, 43
forced door entry, 36
forced output number, 41
interlock zone numbers, 42
LED options, 36
opening/closing of doors, 35
output activating on DOTL, 42
pulsed lock and unlock, 37
shunting zone numbers, 41
unlock relay number, 40
zone holds door unlocked, 34
Region count limit
programming, 19
Relay controllers
number fitted, 14
Relay numbers
activating when door accessed, 40
Re-lock delay time
drop bolts and Magnalocks, 19
Security group zone number, 45
Short list of available inputs and outputs per DGP type, 57
Shunt conditions for doors/lifts, 22
DOTL alarm generated, 22
Shunt time for doors/lifts, 22
cancel shunt after door closed, 23
extending shunt time, 22
until door closed, 23
warning shunt time, 23
Shunting zone numbers, 41
Siren monitoring, 20
Siren tamper
specifying output number, 51
System options
low battery output number, 51
mains fail output number, 51
tamper output number, 51
Tamper output number, 51
Time and Attendance options
  Wiegand options and lock relay numbering, 39
Timer settings in minutes or seconds, 21
Timers
  access, 21
  Card to PIN, 18
  extended access, 21
  extended shunt, 22
  lock relock, 19
  mode time, 19
  shunt, 22
  shunt warning, 23
  Two cards, 18
  Timezone
    specifying when automatic unlock takes effect, 34
  Timezone number
    for opening doors, 23
    programming, 34
  Toggle mode
    programming RAS, 17
  Two cards
    programming time, 18
  Unlock time for doors/lifts
    extended access time, 21
  View card details, 48
  Warning shunt time for doors/lifts, 23
  Wiegand interface, 26, 27
Programming map

The Relay Controller Menu numbers correspond with the chapter numbers in this manual (for example, the box below “1. Controller Options” maps to Controller options on page 14). The characters “XX” represent the number of the selected device.

19. Install Menu

28. To Remote devices

1. DGP, 2. RAS

(Select 1 for DGP)

Enter DGP number

Relay Controller Menu

1. Controller Options

XX, Relay Controllers

XX, Site Code A

XX, Site Code A Card Offset

XX, Site Code B

XX, Site Code B Card Offset

XX, Alarm Code Prefix Length

Poll RAS

RAS’s with LCD Fitted

RAS’s with Egress Enabled

RAS’s with Toggle Enabled

Poll DGP

XX, Tamper Monitoring

XX, Card to PIN Time

XX, Dual Custody Time

XX, Mode Time

XX, Lock Relock Time

XX, Region Count Threshold

XX, Enable Siren Monitoring

XX, Forced Door Debounce

Continued...
2. Door Options

1. Access Options

   XX, Access Time
   XX, Extended Access Time
   XX, Shunting Options
   XX, Shunt Time
   XX, Extended Shunt Time
   XX, Shunt Warning Time
   XX, Shunt Until Door Closes
   XX, Cancel Shunt After Door Secures
   XX, Low Security Time Zone
   XX, In Reader Card & PIN
   XX, Out Reader Card & PIN
   XX, In Reader Inhibit PIN
   XX, Out Reader Inhibit PIN
   XX, In Reader Inhibit Region
   XX, Out Reader Inhibit Region
   XX, Anti-Passback Options
   XX, In Region
   XX, Out Region
   XX, Anti-Passback Time
   XX, In Reader Dual Custody
   XX, Out Reader Dual Custody

0. No Shunting
   1. Input Shunting
   2. Input Shunting & DOTL
   3. Auto Shunting & DOTL

0. No Anti-Passback
   1. Soft Anti-Passback
   2. Hard Anti-Passback
   3. Timed Anti-Passback

Continued...
2. Egress Options

- XX, Egress Time Zone
- XX, In Egress Disabled if Secure
- XX, Out Egress Disabled if Secure
- XX, Egress Options
- XX, Egress Reporting

3. Alarm Control

- XX, Alarm Group
- XX, Alarm Control Options
- XX, In Denied if Area Secure
- XX, Out Denied if Area Secure
- XX, Authorised RAS

4. Reader Options

- XX, Card Format
- XX, Input Holds Door Unlocked
- XX, Door Unlocked Until Door Opens
- XX, Override Time Zone Disabled
- XX, Override After Entry
- XX, Report Door Unsecure/Secure
- XX, Map (un)secure to (un)locked
- XX, Report Door Open/Close
- XX, Report Forced Door
- XX, Report DOTL
- XX, LED Options
- XX, Pulsed Lock & Unlock Relays
- XX, Random Percentage
- XX, Time & Attendance Reader
- XX, Disable Duress

0. Egress Times Door Open
   1. Egress Holds Door Open
   2. Egress Shunts Only

0. Reader Has No Alarm Control
   1. Alarm Control on 1st Badge
   2. Alarm Control on 3rd Badge
   3. Alarm Control with Buttons
   4. Alarm Control Always

0. Wiegand 27 Bit
   1. Spare (do not use)
   2. Tecom ASC
   3. K 32 Bit
   4. Wiegand 26 Bit
   5. Indala ASC 27 Bit
   6. Indala ASC 26 Bit
   7. Wiegand 32 Bit
   8. Mag. Card Tecom
   10. C 36 Bit

0. LED 1 On When Locked
   1. LED 1 On When Unlocked
   2. LED 1 On When Alarm is Armed
   3. LED 1 Off When Alarm is Armed
   4. Two LED Access/Secure
   5. Two LED Valid/Void
   6. LED's Disabled

Continued...