



CDC4(-EN) Door Controller Programming Manual

Copyright

© 2022 Carrier. All rights reserved. Specifications are subject to change without prior notice.

Trademarks and patents

Aritech, CDC4(-EN) Door Controller name and logo are trademarks of Carrier Fire & Security.

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

Manufacturer

PLACED ON THE MARKET BY:
Carrier Fire & Security Americas Corporation Inc.
13995 Pasteur Blvd
Palm Beach Gardens, FL 33418, USA

AUTHORIZED EU REPRESENTATIVE:
Carrier Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Product warnings and disclaimers

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

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

Certification**European Union directives**

Carrier Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of the Directive 2014/30/EU and/or 2014/35/EU. For more information see firesecurityproducts.com or www.aritech.com.

REACH

Product may contain substances that are also Candidate List substances in a concentration above 0.1% w/w, per the most recently published Candidate List found at ECHA Web site.

Safe use information can be found at <https://firesecurityproducts.com/en/content/intrusion-intro>



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: recyclethis.info

Product documentation

Please consult the following web link to retrieve the electronic version of the product documentation.

This link will guide you to the EMEA regional contact page. On this page you can request your login to the secured web portal where all manuals are stored.

<https://firesecurityproducts.com/en/contact>

Contact information

firesecurityproducts.com or www.aritech.com

Content

	Important information	ii
	Product overview	iii
Chapter 1	System functions	1
	Function list	2
	Operating modes	3
	Doors	6
	Lifts	8
	Lock types	11
	Example door operation scenarios	13
	Interlocking doors	15
	Regions	17
	Panel schedules	19
	Door schedules	20
	Macro logic	21
	Alarm control	22
	Bus formats	24
	Flexible device locations	26
	Input and output mapping	29
	Overriding door state	32
	Random lockout time	35
	LED area mapping for door readers	36
	Time and attendance readers	37
Chapter 2	Programming	39
	Recommended programming sequence	40
	Downloader connection	42
Chapter 3	Menu reference	45
	Expander devices	46
	Access configuration>Doors	61
	Access Configuration>Regions	78
	Users	79
Appendix A	Door controller events	83
Appendix B	CDC4(-EN) defaults	89
	Glossary	91

Important information

Limitation of liability

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

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

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

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.



Safety sign identifies actions or practices that are required by EN 60950 Safety Standard.

Product overview

This manual is intended for use only by trained installation and configuration technicians. To use this document effectively, you should have the following minimum qualifications:

- Basic knowledge of alarm systems and components
- Basic knowledge of electrical wiring and low-voltage electrical connections

Read these instructions and all ancillary documentation entirely before installing or operating this product.

Up to 12X CDC4(-EN) can be connected to an Advisor Advanced panel system data bus.

Caution: Ensure that there are door controllers of only one type (CDC4(-EN) or ATS125x) installed on the system bus, to avoid any configuration conflicts.

CDC4(-EN) has two local data buses to connect readers for doors, keypads, and expanders.

Caution: The heatsink on the device board may be hot. Do not touch. Take appropriate precautions if working on an active or recently de-powered device. The fuses on the device board may be very hot if they are in the tripped state or close to tripping. Do not touch.

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

Chapter 1

System functions

Summary

This section lists and describes all functionality functions provided by CDC4(-EN) Door Controller.

Content

Function list	2
Operating modes	3
Doors	6
Door groups	6
Floor groups	7
Lifts	8
User control	8
Lift override	8
Lift control levels	9
Scheduled actions	9
Override hierarchy	9
Lock types	11
Example door operation scenarios	13
Interlocking doors	15
Regions	17
Anti-passback	17
High security	17
Panel schedules	19
Door schedules	20
Macro logic	21
Alarm control	22
Bus formats	24
Flexible device locations	26
Input and output mapping	29
Overriding door state	32
Random lockout time	35
LED area mapping for door readers	36
Time and attendance readers	37

Function list

Table 1 below provides an alphabetic list of CDC4(-EN) door controller functions and their description references.

Table 1: Function list

Function	Reference
Alarm control	"Alarm control" on page 22
Anti-passback	"Regions" on page 17
Bus	"Bus formats" on page 24
Device locations	"Flexible device locations" on page 26
Door schedules	"Overriding door state" on page 32
Doors	"Doors" on page 6, "Example door operation scenarios" on page 13
Door groups	"Doors" on page 6
Floor groups	"Lifts" on page 8
High security regions (HSR)	"High security" on page 17
High security users (HSU)	"High security" on page 17
Input mapping	"Input and output mapping" on page 29
Interlocking doors	"Interlocking doors" on page 15
LEDs	"LED area mapping for door readers" on page 36
Lifts	"Lifts" on page 8
Locks	"Lock types" on page 11
Operating mode	"Operating modes" on page 3
Output mapping	"Input and output mapping" on page 29
Outputs	"Overriding door state" on page 32
Random lockout time	"Random lockout time" on page 35
Regions	"Regions" on page 17
Time and attendance	"Time and attendance readers" on page 37
Zones	"Input and output mapping" on page 29

Operating modes

The door controller can be configured in the following ways depending on your current system and access requirements:

- Standard mode: The door controller only communicates with the control panel.
- Extended mode: In this mode, management software has a direct IP connection to CDC4(-EN).

Note: The operating mode can only be set for all connected door controllers during the initial installation of the Advisor Advanced panel. See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* for more information.

The limits for users and other entities vary according to the operating mode, as shown in Table 2 below.

Table 2: CDC4(-EN) limits per mode

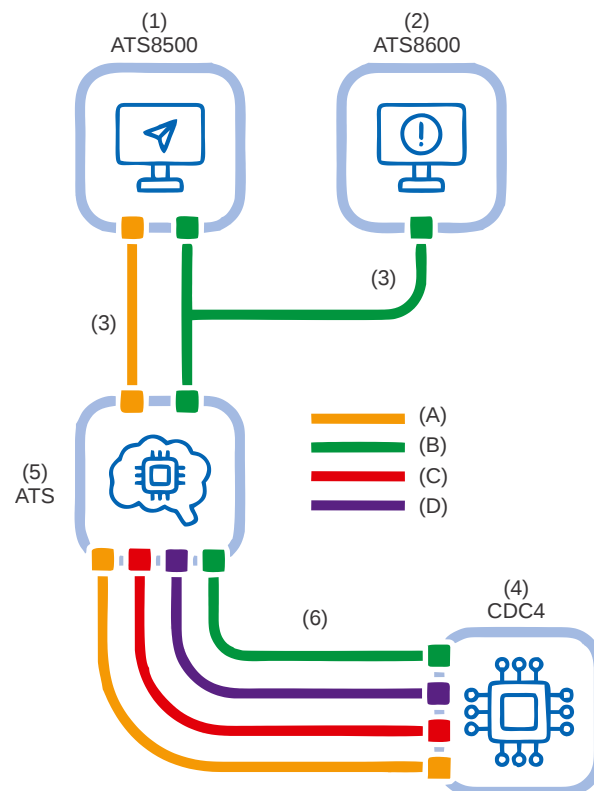
	Standard	Extended
Doors or Lifts	4	8
Users	65532	100000
Floors	64	255
Door groups	128	10000
Floor groups	128	1000
Schedules	24	2000
Sub schedules	4	8
Holiday types	8	8
Card bit length	56	56
History event buffer	50000	50000

The modes are described in more detail in the following sections.

Standard mode

Standard mode can be used for direct upgrade of ATS125x four-door controller with minimal changes. In addition to access control, CDC4(-EN) provides alarm control functionality in conjunction with an Advisor Advanced panel.

CDC4(-EN) is polled as an expander on the first Advisor Advanced system bus.

Figure 1: Standard mode

- (1) Configuration software
- (2) Management software
- (3) Ethernet
- (4) CDC4(-EN) Door Controller
- (5) Advisor Advanced control panel
- (6) RS485 data bus

- (A) Hardware/Door configuration
- (B) User credentials and user groups configuration
- (C) Intrusion events
- (D) Access events

In this mode, the configuration software downloads all configuration to the CDC4(-EN) door controller through Advisor Advanced control panel.

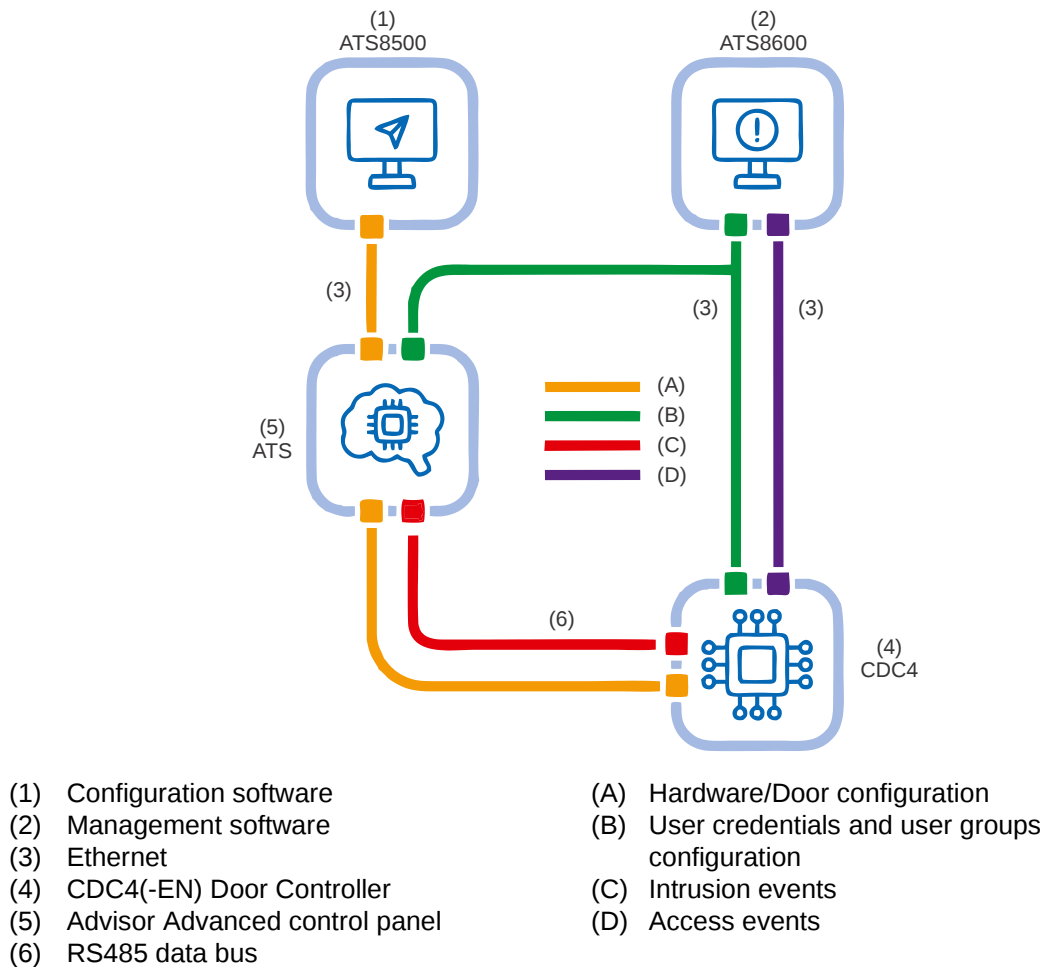
Since the Advisor Advanced is responsible for the distribution of users, door groups etc. to CDC4(-EN), the numbers allowed are limited, as shown in Table 2 on page 3.

History events, alarms, and CDC4(-EN) status are sent from CDC4(-EN) to the Advisor Advanced panel.

Note: Inputs will only register alarms in the Advisor Advanced panel if they are mapped to Advisor Advanced inputs. See the “Input and output mapping” section on page 29 for information on Advisor Advanced input mapping.

Extended mode

Extended mode allows software to communicate with CDC4(-EN) directly via IP rather than through an Advisor Advanced panel, while retaining the alarm control and reporting functionality of a CDC4(-EN) in Standard mode.

Figure 2: Extended mode

In this mode, management software downloads users, door groups, etc. directly to CDC4(-EN), allowing CDC4(-EN) to utilise its maximum capacities, as shown in Table 2 on page 3. CDC4(-EN) retains its own database of users, door groups etc. from the Advisor Advanced panel.

The number of users that can exercise alarm control from CDC4(-EN) is limited by the user capacity of the Advisor Advanced panel. See the “Alarm control” section on page 22 for more information.

Access events are sent directly via IP to management software, while alarms and CDC4(-EN) status are sent to the Advisor Advanced panel.

Note that hardware configuration can only be made by the configuration software connected to the Advisor Advanced control panel.

Notes

- CDC4(-EN) will still be fully functional if it is disconnected from management software.
- Inputs will only register alarms in the Advisor Advanced panel if they are mapped to Advisor Advanced inputs. See the “Input and output mapping” section on page 29 for information on Advisor Advanced input mapping.

Doors

CDC4(-EN) can support up to four doors in standard mode, and up to eight doors in extended mode. The doors are numbered from 17 to 64 or from 17 to 112, depending on which operating mode CDC4(-EN) is working in.

Door controllers may use the first 12 addresses on the Advisor Advanced system bus. Table 3 below the address of CDC4(-EN) (set via DIP switches), the DGP number that CDC4(-EN) is polled as, and the ranges of door numbers.

Table 3: Door numbers per expander address

Address	Polled as	Doors	
		Standard mode	Extended mode
1	Exp 1	17 to 20	17 to 24
2	Exp 2	21 to 24	25 to 32
3	Exp 3	25 to 28	33 to 40
4	Exp 4	29 to 32	41 to 48
5	Exp 5	33 to 36	49 to 56
6	Exp 6	37 to 40	57 to 64
7	Exp 7	41 to 44	65 to 72
8	Exp 8	45 to 48	73 to 80
9	Exp 9	49 to 52	81 to 88
10	Exp 10	53 to 56	89 to 96
11	Exp 11	57 to 60	97 to 104
12	Exp 12	61 to 64	105 to 112

Each door controlled by CDC4(-EN) can have two door contact inputs, an RTE (request to exit) input, two lock outputs, a DOTL (Door Open Too Long) output, a forced door output, a warning output, and six assigned readers in any combination of IN and OUT readers.

Each door has various options for access, shunting, RTE, high security users, and anti-passback. There are also options for alarm control.

Doors are programmed on the Doors form in Downloader. See the “Access configuration>Doors” section on page 61.

Door groups

Door groups functionality allows you to assigns a group of doors or lifts to a user, in order to allow access to those doors or lifts. Access to each door in a group can be restricted via a schedule.

See also “Programming door groups” on page 79.

Floor groups

Floor groups functionality allows you to assign a group of floors to a user, in order to allow access to those floors. Access to each floor in a group can be granted via a schedule.

See also “Programming floor groups” on page 79.

Lifts

As a lift controller, CDC4(-EN) can support four doors and lifts in standard mode, and up to eight door and lifts in extended mode.

Note: To create a lift, create a door first, and then change its type to lift. See “Door type” on page 63 for details.

Access to the particular lifts and floors can be provided using the following functions.

- User control
- Lift override and lift security key override with lift control levels
- Scheduled actions
- Computer commands

User control

A security system user requires two levels of authority before they can access a secured floor:

- Door group. This group defines which lifts the user can access. See “Door groups” on page 6.
- Floor group. This group defines which floor buttons can be pressed by the user, and therefore which floors he can access. See “Floor groups” on page 7.

Lift override

Lift automatic override

The lift override allows one or more floors to automatically access during specified time frames, and secured outside of these frames. For example: Level 5 (Canteen) should be freely accessible Monday to Friday between the hours of 9:00 and 16:00.

When the lift is disabled, the override will not operate.

The time of access can be defined by the following functions:

- Lift control levels. See “Lift control levels” on page 9.
- Floor groups. See “Floor groups” on page 7.
- Both methods above: the lift evaluates both and logically OR the floors that should be accessed.

Security key override

The lift security key override feature allows one or more floors to be accessed under three conditions:

- The security key input for the lift car must be active.

- The specified time frame must be active.
- The lift must be enabled. If the lift is disabled, all floors will remain secure.

A security key is often given to emergency service personnel or security installers. Generally, the key allows access to all floors that are normally secured.

The time of access can be defined by the following functions:

- Lift control levels. See “Lift control levels” below.
- Floor groups. See “Floor groups” on page 7.
- Both methods above: the lift evaluates both and logically OR the floors that should be accessed.

Lift control levels

A lift control level defines one or more floors, and up to 8 time frames, in which these floors can be accessed. Once created, the lift control level can be assigned to either a Lift override and a Security key override on any of the controllers lifts.

100 lift control levels can be configured on each controller.

Scheduled actions

A scheduled action can be performed on a lift or a specific floor. The action can be used to temporarily override normal operation of the lift. For example, a scheduled action might be used is to disable a lift that is in maintenance for a period of 3 days.

Floor action

The available actions for a floor are Access and Secure.

While the action is active, the floor for the particular lift will remain in the configured state.

Lift Action

The available actions for a lift are enable and disable.

While the action is active, the lift will remain in the configured state.

Override hierarchy

When all floors are secured and the lift is Enabled, lift control functions have the following priorities.

1. (Lowest priority) Lift Override Timezone and Lift Security override timezone. Floors will access when the timezone is valid for any floor in the lift override timezone. Floors will access when the key is turned and the timezone is valid for any floor in the lift security override timezone.

2. Scheduled action. Scheduled actions that hold the floor in secure will prevent lower priority functions from accessing the floor. For example: If floor 1 is accessed by a Lift override and the scheduled action to secure the floor is activated, the floor will secure and remain secured for the action duration.
3. User Credential. A user presenting a card will be able to access secured floors for the period of the access time.
4. (Highest priority) Computer command. If a command is issued to secure the floor, the floor will be secured. If a scheduled action holds the floor in access it will be cancelled. If an override timezone is holding the floor in access, the floor will secure until the next timezone change.

Disabling a lift from the computer will prevent all floors from being accessed under any condition.

Lock types

The CDC4(-EN) door controller supports the following lock types:

- **Strike.** This lock in the unlocked state allows opening and closing door. In the locked state it still allows you to close the door. The lock state does not depend on the door state.
- **Maglock/drop bolt.** This lock can only be locked when the door is closed, therefore the door opening status must be monitored.
- **Turnstile.** The lock of the rotating door, which can operate in two directions. Each direction is controlled by a separate lock output.

Note that the turnstile lock type has the following limitations:

- The long access motor delay function is disabled if the turnstile lock type is selected.
- An RTE input configured on the door will operate only the OUT side of the door (lock output 2).
- Management software activation of the door (open, timed open, unlock) will activate the IN side of the door allowing a person to enter the building.
- Scheduled actions can control only the IN side of the door allowing a person to move from the outside to the inside region. **Note:** While an action is active, no OUT access is allowed. RTE buttons do not function until the door is locked.
- Interlocking is not recommended for use on a turnstile door.

There are two inputs for each door, and two lock outputs for each door:

- **Door input 1:** Connected to the door to indicate if the door is open or closed. This is usually the reed switch.
- **Door input 2:** Connected to the lock monitor on Strike, Maglock, and Drop bolt locks.
- **Lock output 1:** Unlocks the door. In case of turnstile lock, unlocks the door in the IN direction.
- **Lock output 2:** Unlocks the door. In case of turnstile lock, unlocks the door in the OUT direction.

The door lock type, and inputs and outputs are programmed in Downloader on the Hardware tab for the door. See the “Hardware tab” section on page 62 for instructions.

The following timers can be defined:

- **Pre-Lock time:** Once the door open input (door input 1) has been deactivated, CDC4(-EN) waits for the pre-lock time to expire before locking the door. If the door open input activates during the pre-lock time, the door is deemed open and the pre-lock timer is cancelled. The shunt continues during the pre-lock time.

- **Post-lock time:** The post-lock time allows time for a lock to fully engage. After the post-lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door open input activates during the post-lock time, the door is deemed open and the post-lock timer is cancelled. The shunt continues during the post-lock time.

Note: There are also two roller door specific timers that are reserved for future use.

The timers are programmed in Downloader on the Access tab for the door. See the “Access tab” section on page 63 for instructions.

Example door operation scenarios

Simple door unlock with no inputs

At the start of the access time, the door is unlocked (via lock output 1) and is locked at the end of the access time. There are no inputs assigned. At the end of the access time, the door is deemed to be closed and secure.

See Figure 3 below, item A.

There is no shunting, forced door or DOTL support.

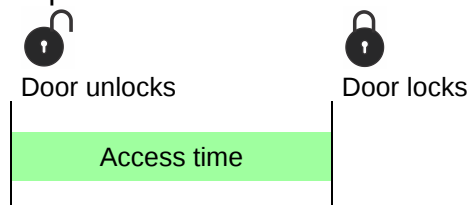
Door unlock with one input for open door

At the start of the access time, the door is unlocked (via lock output 1). If the door is opened within the access time (for example, door input 1 is active), then the shunt timer starts. When the door is subsequently closed, the pre-lock timer starts. After the pre-lock time, the door is deemed closed. At that time, maglocks and drop bolts can be locked. After the post-lock time, the shunt is cancelled, and the door is deemed secure. See Figure 3 below, item B.

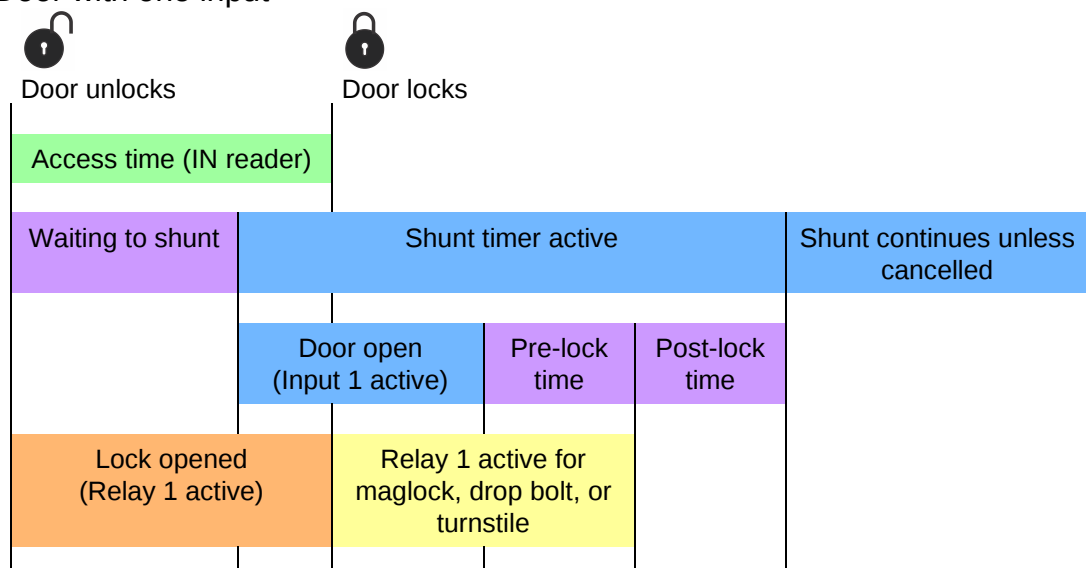
If the shunt timer expires while the door is open, or expires during the pre-lock or post-lock time, then a normal alarm or DOTL occurs. See Figure 3 below, item C, for an example.

Figure 3: Lock and unlock diagrams

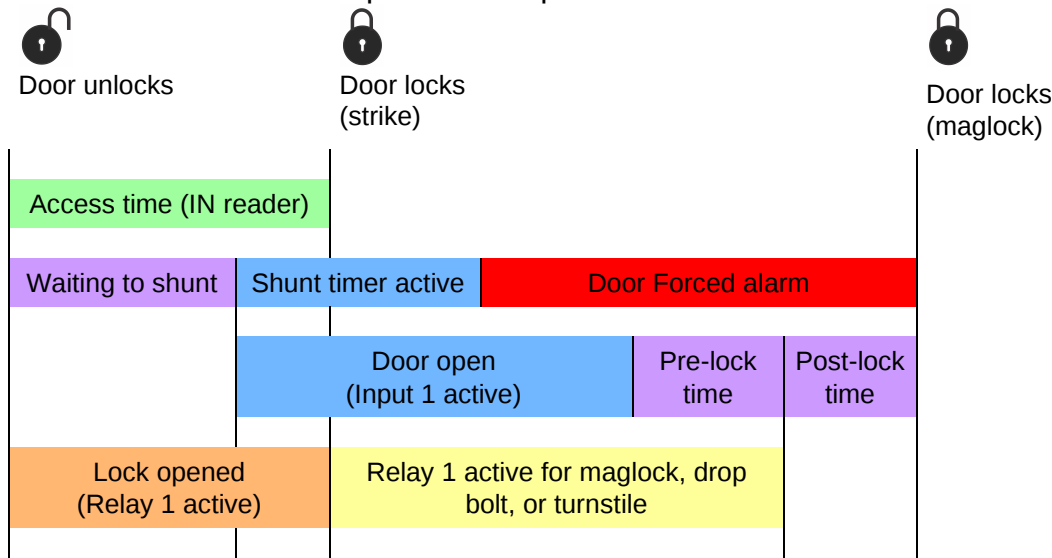
A: Simple unlock



B: Door with one input



C: Door Forced alarm after input shunt expiration



Interlocking doors

Interlocking is a method that stops two or more doors from being opened at the same time. Interlocking may be used in a vault, for example.

When programming a door on CDC4(-EN), there are two ways to specify an interlock door: either another door on the same CDC4(-EN), or a door on a separate controller.

Interlocking doors on the same controller

CDC4(-EN) has simplified configuration of interlocking doors on the same controller.

When programming the door, navigate to the door “Hardware tab” described on page 62 and select the required interlock doors in the Interlock doors list.

When an attempt to open/unlock the programmed door occurs (either from user action or from management software), CDC4(-EN) will check all other locally linked doors to ensure that no other door is unsecure, before allowing the door to open.

When internal interlocking option is enabled on CDC4(-EN), a special interlocking timer (300 ms if only internal interlocking is enabled) is started when a user credential is presented. Any repeated attempt to gain access by providing a user credential while the timer is running and the remaining time is greater than 100 ms will cause Access Denied Void and 7 error beeps. If access is granted and the door becomes in access, this waiting time is bypassed and all the consequent credential requests are processed without that delay.

A proposed sequence of user action on the interlocked doors is below:

1. Present a credential (hear a single beep if it is a card, or press Enter if it is a PIN).
2. Wait for CDC4(-EN) to confirm. CDC4(-EN) confirms with either 2 beeps if the credential has a right to access or 7 beeps in case of a wrong credential. The waiting time may be less than a second if no external interlocking is enabled or about 3 seconds if external interlocking is enabled.
3. Proceed to the next step.

Interlocking is programmed on the “Hardware tab” of the Doors form. See the “Interlocks” section on page 63.

Interlock door on external controller

There are three external input fields provided for CDC4(-EN) to check for interlocking on external controllers.

To interlock with a door on an external controller, a contact from the external door must be wired to a spare input connected to CDC4(-EN), and vice versa.

When programming the door on CDC4(-EN), navigate to the door “Hardware tab” described on page 62 and define the locations of the inputs connected to external door contacts in the External input fields.

When an attempt is made to open/unlock the programmed door (either by user action or from management software), then CDC4(-EN) will check the state of these external inputs. If any of the external inputs is active, access will be denied immediately.

If all external inputs are inactive, CDC4(-EN) will activate the “Door unlocked” event. A macro should be created which takes the “Door unlocked” event and activates an output linked to the other controllers.

When external interlocking option is enabled on CDC4(-EN), a special interlocking timer (3 s if only external interlocking is enabled) is started when a user credential is presented. Any repeated attempt to gain access by providing a user credential while the timer is running and the remaining time is greater than 100 ms will cause Access Denied Void and 7 error beeps. If access is granted and the door becomes in access, this waiting time is bypassed and all the consequent credential requests are processed without that delay.

A proposed sequence of user action on the interlocked doors is below:

1. Present a credential (hear a single beep if it's a card or press enter if it's a pin).
2. Wait for the CDC4(-EN) to confirm. CDC4(-EN) confirms with either 2 beeps if the credential has a right to access or 7 beeps in case of a wrong credential. The waiting time may be less than a second if no external interlocking is enabled or about 3 seconds if external interlocking is enabled.
3. Proceed to the next step.

Interlocking is programmed on the “Hardware tab” of the Doors form (see “Hardware tab” on page 62). See also the “Interlocks” section on page 63.

Regions

A region is a defined access control area having doors acting as boundaries.

Regions are programmed in “Panel > Access Configuration>Regions” on page 78.

Regions are used by the following functions:

- Areas set and unset
- Anti-passback functions to keep track of users
- User number count and restriction
- High security function to allow users in the region under high security users (HSU) supervision

Anti-passback

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 the “Anti-passback options” section on page 70), the system may:

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

Separate programming fields are provided for each door IN reader and OUT readers. See the “In region” section on page 71 and the “Out region” section on page 71.

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 1 to region 254. Region 1 acts as outside. Region 255 is used for “Region disabled”.

Users in region 1 (outside) can be prevented from unlocking doors at IN readers and/or OUT readers. See the “Deny region 1 users” section on page 67 (the inhibit outside users option can be configured separately for IN readers and OUT readers).

Note: If the system is in the extended mode, the anti-passback functionality will work in regions only if these regions are synchronized between different door controllers. See “Region synchronization” on page 46 for details.

High security

High security regions (HSR) require a certain number of high security users (HSU) present in them to allow any normal users inside. If a high security user leaves the region causing too few HSU present in it, an alarm is raised, preceded by prewarning time.

The system does not allow the normal user to stay in the HSR without HSU inside, so the last high security user will not be permitted to leave the high security area if there are normal users inside.

Note: Privileged users are still allowed to access the regions where the limits for users or high security users are exceeded. See also “Users” on page 79.

Set HSU options in “Expander devices > Region/HSU Configuration tab” on page 57.

High security user requires the Access user type option to be set to High Security User. See also “Users” on page 79.

Alarm control by region

If the alarm control by region is enabled, the last user leaving the region assigned to door automatically sets the area, and the first user entering the region unsets it.

To configure the functionality, do the following:

- Set the following options in Expander devices > Region/HSU Configuration tab:
 - Set the region number for alarm control in “Region” on page 57.
 - Enable “Alarm control by region” on page 59.
 - If necessary, enable “Delayed Arming” on page 59. If enabled, the keypad will prompt to activate a delay for the set. See *Advisor Advanced AT5x500A Installation and Programming Manual* for more details on the delayed set.
 - Set the required alarm control levels in “Alarm Levels 1..6” on page 59. These levels define the areas that should be set or unset.
- Set the following options in Access configuration>Doors > Shunt/AntiPassback tab:
 - Set the region being set in “In region” on page 71.
 - Set “Out region” on page 71 to the number of the region that users are moved to after the area is set.
- Set the following options in Access configuration>Doors > Alarm control tab:
 - Set the “IN alarm control” on page 75 to Alarm control via region count.
 - Set the “OUT alarm control” on page 75 to Alarm control via region count.

Panel schedules

Panel schedules can be used in the door controller for the following:

- Door groups
- Floor groups
- Override schedule and low security schedule (in door access options)
- RTE schedule (in door RTE options)

In standard mode, CDC4(-EN) uses the same panel schedules as the Advisor Advanced panel.

Note: In case of CDC4(-EN) schedules only general data and time frames are downloaded to the device. The assigned actions are only applicable for the Advisor Advanced panel.

To add a panel schedule, follow these steps in Downloader:

1. Select Calendar > Schedules to open the Schedules form.
2. Click the New button in the toolbar to add a new panel schedule record.
3. Enter a name and a description for the schedule.
4. Program the Start date, End date, and define up to four Time frames for the schedule.

Note: Schedule 1 is 24-hour schedule called “Always” (always valid). It cannot be edited or deleted.

Refer to the *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* and the Downloader online help for more information.

Door schedules

Up to 100 door schedules can be programmed in the CDC4(-EN), allowing for very flexible locking and unlocking as well as disabling and enabling doors.

For more information on door schedules, see the “Overriding door state” section on page 32.

Macro logic

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

Up to 48 macros can be defined for the door controller.

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

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

Macro logic is programmed in "Expander devices > Macro logic tab" described on page 54.

Alarm control

The CDC4(-EN) door controller can perform alarm control functions, such as arming areas. Alarm control for each CDC4(-EN) door is determined through alarm control levels, which are analogous to user groups in Advisor Advanced.

Each alarm control level must have a schedule assigned to it.

Each alarm control level can be allocated a list of up to ten areas for arming and disarming.

A CDC4(-EN) door can have up to six alarm control levels, which are then assigned to a door side (either IN or OUT) in any combination. Up to six alarm control levels can be assigned to a door side.

If a user initiates some alarm control functionality at a reader (for example, they badge their card three times to arm areas), CDC4(-EN) checks the alarm control levels for the door that apply to the reader (depending on whether the reader is an IN or OUT reader).

If any of the assigned alarm controls levels has a schedule that is valid, then the user credential information is sent to the Advisor Advanced panel, along with information about any applicable alarm control levels. The Advisor Advanced panel checks the user credentials in its user database and checks the corresponding Advisor Advanced user group.

Note: CDC4(-EN) can only request to control (set/unset) up to 10 areas. Therefore you must ensure that there is no more than 10 areas in all alarm control levels.

If the corresponding Advisor Advanced user group and the reader alarm control level allow an alarm function, then the alarm function proceeds.

Note: In the Extended mode, the number of users that can exercise alarm control from CDC4(-EN) is limited by the user capacity of the Advisor Advanced panel.

Alarm control levels are set up in Downloader on the Alarm control levels tab for the door. Alarm control levels must also be assigned to the door readers, which can be done on the Alarm tab for the door. The alarm control functionality is programmed in Downloader on the Alarm tab for the door. See the “Alarm control tab” section on page 75 for instructions.

In order for alarm control to function, the door must be assigned at least one alarm control level.

The following is a suggested programming sequence for alarm control for a door:

1. Configure alarm control levels on the Alarm control levels tab of the Expander form. See “Alarm control level tab” on page 60.
2. Assign alarm control levels to doors on the Alarm control tab of the Doors form. See “Alarm control tab” on page 75.

Note: Alarm control may be also controlled automatically by High Security user number. See “Alarm control by region” on page 59 for details.

Exit time indication

Unlike keypads and reader connected to the control panel, readers connected to one of CDC4(-EN) local buses do not indicate the exit time during area set. To indicate the exit time by a buzzer, you must create a macro, which will activate the buzzer when the flag `AreaInWarning` is active.

The same macro must be used if the following functionalities are active in the control panel:

- **Autoset.** The Advisor Advanced system allows you to set areas automatically by the calendar. See *Advisor Advanced ATsx500A Installation and Programming Manual* for more information.
- **Delayed set by regions.** Areas can be set automatically by a High Security Users number. See “Alarm control by region” on page 59 for details.

Bus formats

There are two local data buses on the CDC4(-EN) door controller. Each bus can have up to 16 RAS devices. Each bus can support readers other than ATS readers.

Each bus supports the following protocols:

- ATS
- OSDP (Open Supervised Device Protocol) version 2
- SALLIS by SALTO Systems
- Aperio

Each bus can use one protocol at a time, but the two buses can use different protocols.

The bus format for each bus is defined on the Details tab of the Expander devices list for CDC4(-EN). See the “Bus options” section on page 49. If the bus format is OSDP, then the baud rate of the bus can be configured, and encryption can be enabled by entering the OSDP encryption key. OSDP encryption uses the AES 128-bit encryption algorithm.

When assigning a RAS to CDC4(-EN) via the Assigned RAS tab of the Expander form, specify the bus format that the reader will use (which depends on the RAS number). See the “Assigned RAS tab” section on page 50.

Non-ATS devices must meet certain requirements to work with CDC4(-EN), as described in the following sections.

OSDP

The CDC4(-EN) Door Controller supports OSDP version 2.

Note: OSDP has a fixed baud rate of 9600 baud.

OSDP reader addresses

If the OSDP reader has DIP switches, refer to the manual for the reader to configure the reader’s address using the DIP switches. If the reader does not have DIP switches, then the reader’s address must be configured using a configuration card. Assign the reader the desired address by badging the appropriate configuration card at the reader.

OSDP encryption

Without an encryption key configured for the CDC4(-EN) bus, the CDC4(-EN) communicates with the OSDP devices using a default encryption key as specified in the OSDP standard. To use a non-default encryption key with OSDP readers, set the 128-bit AES encryption key for the bus in Downloader. See the “Bus encryption key” section on page 50. The encryption key will be set on each OSDP reader attached to the bus once the encryption key is defined.

Once set, the encryption key on an OSDP reader cannot be changed by changing the encryption key for the bus. To reset the encryption key used by an OSDP reader, the reader must be changed to Install Mode.

Aperio

The CDC4(-EN) door controller supports Aperio protocol.

Note: Aperio protocol has a fixed baud rate of 19200 baud.

SALLIS

The CDC4(-EN) door controller supports SALLIS protocol.

Note: SALLIS protocol has a fixed baud rate of 38400 baud.

Flexible device locations

With the CDC4(-EN) Door Controller, there is flexibility in how devices such as inputs, outputs and readers can be physically wired up to CDC4(-EN) and how they are addressed.

Devices can be connected directly to CDC4(-EN) or can be connected to DGPs or RASs on one of the CDC4(-EN) buses. Thus, when programming CDC4(-EN), devices are not addressed by their number alone, but must be defined according to how they have been physically wired up to CDC4(-EN).

When specifying a device attached to CDC4(-EN) in Downloader, the operator must enter information in the following fields:

- Location: Select the device location from the following options:
 - On-board: The device is connected directly to the CDC4(-EN) on-board terminals (or an output on an attached output controller). Enter the device number in the Device number field.
 - DGP: The device is connected to a DGP that is connected to one of the CDC4(-EN) local buses. Enter the address of the DGP in the Address field, and the device number on the DGP in the Device number field. The DGP must be assigned to the CDC4(-EN) controller and polled on the bus.
 - RAS: The device is a RAS, or is an input or output connected to a RAS, which is connected to one of the CDC4(-EN) buses. Enter the address of the RAS in the Address field. The RAS must be assigned to the CDC4(-EN) controller and polled on the bus.
- Address: If the device is connected to a DGP or RAS on one of the CDC4(-EN) local buses, then the address of this DGP or RAS must be specified.
 DGP addresses from 1 to 15 are defined to be on bus 1, and DGP addresses from 17 to 31 are defined to be on bus 2 (the DGP with address 16 is the CDC4(-EN) controller itself).
 Similarly, RAS addresses from 1 to 16 are defined to be on bus 1, and RAS addresses from 17 to 32 are defined to be on bus 2.
 There can be 30 DGPs and 32 RASs attached to CDC4(-EN).
- Device number: The device number (address) of the device attached to RAS, DGP, or CDC4(-EN).

The four on-board lock outputs are treated as the first four output numbers assigned to CDC4(-EN). If an output is connected to CDC4(-EN) via an attached output controller board, then the outputs are numbered from 5 onward. The number of output controller boards must be configured on the CDC4(-EN) options tab of the DGP form. See the “Output modules number” option on page 47.

If the Location is set to RAS or DGP, then the RAS or DGP must be assigned to CDC4(-EN) using the Assigned RAS or Assigned DGP tab of the DGPs form,

respectively, and must be polled. See the “Assigned RAS tab” section on page 50, and the “Assigned DGPs tab” section on page 51 for more information.

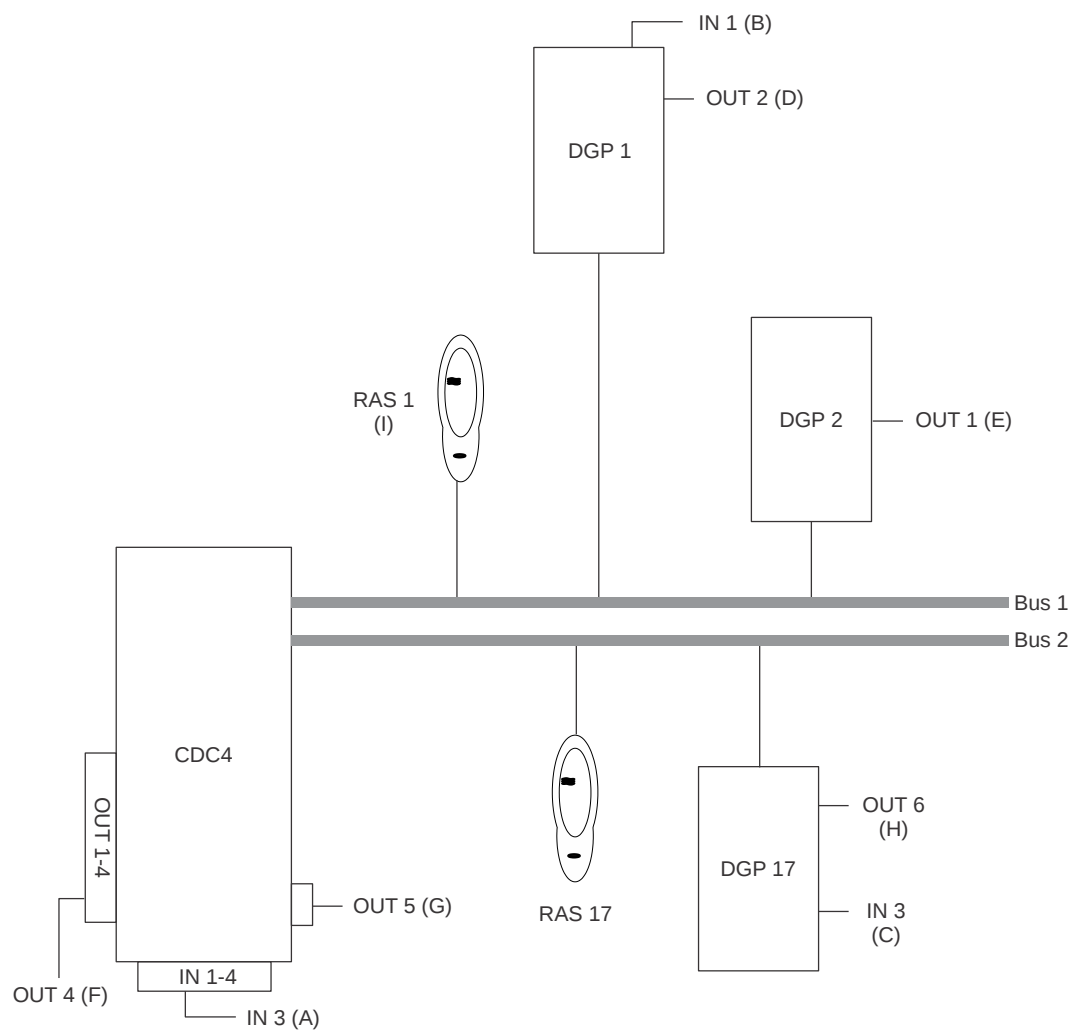
Device locations example

The following example demonstrates the flexibility of specifying devices on CDC4(-EN) and on RASs or DGPs attached to its local buses, using a single door attributes (inputs, outputs, and readers). In this example, both local buses use the ATS protocol.

A single door can have two door inputs, an RTE input, two lock outputs, a DOTL output, a forced door output, a warning output, and up to six assigned readers. The diagram in Figure 4 on page 28 shows devices attached to CDC4(-EN) and RASs/DGPs attached to its local buses that must be configured for use with the door. Table 4 below shows how an operator would specify the device locations when configuring the door. See also Figure 2 on page 5.

Table 4: Door example

Door 1 device	Location	Address	Input / output	Figure item
Door input 1	On-board inputs	–	3	(A)
Door input 2	DGP input	1	1	(B)
RTE input	DGP input	17	3	(C)
Lock output 1	DGP output	1	2	(D)
Lock output 2	DGP output	2	1	(E)
DOTL output	On-board relay	–	4	(F)
Forced door output	On-board (expander) relay	–	5	(G)
Warning output	DGP output	17	6	(H)
Assigned reader 1	RAS	1	1	(I)
Assigned reader 4	–	–	–	–
Assigned reader 5	–	–	–	–
Assigned reader 6	–	–	–	–

Figure 4: Device locations example

Input and output mapping

The CDC4(-EN) door controller can present up to 32 inputs for the Advisor Advanced to respond to and up to 16 outputs for the Advisor Advanced to activate, without complex use of macros or other programming.

These inputs and outputs must be configured in CDC4(-EN) via input and output mappings. The Advisor Advanced control panel must also be programmed with additional inputs and outputs, with their numbering depending on the CDC4(-EN) address (set via its DIP switches) and which Advisor Advanced system data bus the CDC4(-EN) controller is attached to.

Input mapping

Each input presented to the Advisor Advanced can reflect the inactive or active state of an input attached to CDC4(-EN) (either directly on-board, or attached to a DGP or RAS on one of its buses), or can reflect the state of a CDC4(-EN) door (for example, a Forced door condition).

An input mapping must be set up in CDC4(-EN) to map the state of the input or door to an input number in the range 1 to 32.

Each mapped input has a type, which may be one of the following:

- Not used: The input always reports as passive. This type of input cannot be assigned to a door.
- Forced: The input is a logical input associated with a door and is active when the door has a Forced Door alarm (from the Door input 1 being active) or there is a tamper condition.
- RTE (request to exit): The input is a logical input associated with a door and is active when the door is in RTE condition (i.e. the door RTE input is active) or there is a tamper condition.
- DOTL: The input is a logical input associated with a door and is active when the door has a Door Open Too Long (DOTL) alarm (from the door's Door input 1 being active).
- Shunted pass through: The input is a physical input which is passed through to the Advisor Advanced panel if the associated door is not shunting.
- Direct pass through: The input is a physical input which is passed directly through to the Advisor Advanced panel. This type of input should not be assigned to a door.

Note: CDC4(-EN) inputs are masked from the Advisor Advanced if they are not mapped.

Input mapping is programmed in Downloader on the Mapped Inputs tab of the Expander form for CDC4(-EN). See “Mapped inputs tab” on page 52 for instructions.

Since CDC4(-EN) can have flexible device locations, any physical input must be programmed using the scheme described in the “Flexible device locations” section on page 26.

Shunted pass through operation

When the door is shunting, and the input goes active, the input will not pass through, i.e. the Advisor Advanced will see the input as remaining inactive.

If the door shunt expires for any reason (Forced or DOTL), and the input is active, CDC4(-EN) will pass through the input state to the Advisor Advanced panel.

If the input activates when the door is not shunted, or the door is in alarm, the input will pass through and report the active state to the Advisor Advanced panel.

If the input is active when the door shunt starts, the Advisor Advanced panel will not see a change in the input state.

A tamper on these inputs will be passed through to the Advisor Advanced panel immediately regardless of the shunt state.

Output mapping

Each output presented to the Advisor Advanced is a direct map of an output attached to CDC4(-EN) (either directly on-board, or attached to a DGP or RAS on one of its buses).

An output mapping must be set up in CDC4(-EN) to map the output to an output number in the range 1 to 16. Activating the Advisor Advanced output number will activate the specified output attached to CDC4(-EN).

Each mapped output has a type, which may be one of the following:

- Disabled: The output is not mapped to a physical output. The output may be used as an input to a macro.
- Direct map: The output is directly mapped to a physical output attached to CDC4(-EN).

Output mapping is programmed in Downloader on the Mapped Outputs tab of the Expander form for CDC4(-EN). See “Mapped outputs tab” on page 53 for instructions.

Since CDC4(-EN) can have flexible device locations, any physical output must be programmed using the scheme described in the “Flexible device locations” section on page 26.

Advisor Advanced input and output numbering

Advisor Advanced allocates 32 inputs and 16 outputs per expander address. To allow Advisor Advanced to utilise the maximum possible number of inputs and outputs on a CDC4(-EN), up to 32 mapped inputs and up to 16 mapped outputs can be configured on CDC4(-EN).

Note: The input and output mappings are specific to each CDC4(-EN). Additional door controllers require additional mappings of inputs and outputs.

The mapped input and output numbers are indexes into the Advisor Advanced panel device numbering scheme, which depends on the CDC4(-EN) address (set via its DIP switches).

Door controllers may use the first 12 addresses on the Advisor Advanced system bus. Table 5 below lists the address of CDC4(-EN) (set via the CDC4(-EN) DIP switches), the expander number that the CDC4(-EN) controller is polled as, and the ranges of Advisor Advanced input and output numbers.

Table 5: Advisor Advanced inputs and outputs per expander address

Address	Polled as	Advisor Advanced inputs	Advisor Advanced outputs
1	Expander 1	17 to 48	17 to 48
2	Expander 2	49 to 80	49 to 80
3	Expander 3	81 to 112	81 to 112
4	Expander 4	113 to 144	113 to 144
5	Expander 5	145 to 176	145 to 176
6	Expander 6	177 to 208	177 to 208
7	Expander 7	209 to 240	209 to 240
8	Expander 8	241 to 272	241 to 272
9	Expander 9	273 to 304	273 to 304
10	Expander 10	305 to 336	305 to 336
11	Expander 11	337 to 368	337 to 368
12	Expander 12	369 to 496	369 to 400

In order for Advisor Advanced to utilise the mapped inputs and outputs, you must also program the Advisor Advanced input and outputs. See the “Programming mapped inputs and outputs” section on page 54 for instructions.

Overriding door state

In addition to being able to define an override schedule for a door, there are additional methods for overriding a door default state. These methods are:

- Direct control by management and configuration software (for example, open/unlock command)
- Unlock schedule programmed in door settings.
- Scheduled actions (see also “Scheduled actions” section below).

Door state priorities

The priorities for controlling the state of a door are as follows, from highest to lowest priority:

1. Direct control from management software (for example, ATS8600), or configuration software, such as Downloader, for example, an operator sends a door open/unlock command.
2. User access, for example, a user badges their card at a door card reader.
3. Scheduled actions, set using the configuration software.
4. The door programmed unlock schedule, set using configuration software.

Scheduled actions

Up to 100 door schedules can be programmed in CDC4(-EN), allowing for very flexible door locking and unlocking schedules.

Door schedules have an active period (set via a start date and an optional end date). If no end date is set, then the active period is for the start date only. You can also specify if the door schedule is active on particular days of the week (and/or holidays) during the active period.

Door schedules must be configured with a start time for when the start action (for example, door unlock) will be executed.

Start actions can be either timed or immediate:

- Timed actions have an action duration that can be configured from 1 second to 366 days. The door will remain in the state defined by the start action for the action duration.

If the door state is overridden (for example, by management software or a user badging a card), then at the conclusion of the overriding state, the door will revert to the state defined by the start action. At the end of the active duration, the end action, if defined, will be executed.

If no end action is defined, then the door will revert to its default state.

- If no action duration is configured, then the start action is immediate. The door will remain in the state defined by the start action.

If the door state is overridden (for example, by management software or a user badging a card), then at the conclusion of the overriding state, the door will revert to its default state. The start action will no longer have any bearing on the state of the door.

The possible door actions, which can be configured to execute at the start time or the end time, are:

- Unlock
- Lock
- Disable
- Enable

Door schedules are programmed in Downloader on the Expander form > Scheduled Actions tabs. See “Scheduled actions tab” on page 56 for instructions.

Notes

- With reference to the priorities for overriding a door state (see the “Door state priorities” section on page 32), a door schedule end action has a lower priority than any override schedule in effect, unless the end action is to disable the door.
- A door schedule will not override the operation of a door schedule that has already started.
- Door schedules that have reached the end of their active period can be deleted via management software.

Door Unlock action

If the start action is Unlock, then the door will unlock at the start time and remain unlocked for the specified action duration (or indefinitely if there is no action duration configured).

During this time if an existing override schedule ends (the door programmed unlock schedule), then the door will remain unlocked.

When the action duration has completed, the end action will occur. However, if the start action ends and an existing override schedule is active (the door programmed unlock schedule), then the door will remain unlocked.

A manual lock command sent from management software will lock the door and cancel the start action.

If the door has “Door unlock after entry” enabled (see the “Door unlock after entry” section on page 68), the door will not unlock until a valid user PIN or card is presented at the door.

Door Lock action

If the start action is Lock, then the door will lock at the start time and remain locked for the specified action duration (or indefinitely if there is no action duration configured).

During this time if an existing override schedule becomes active (the door programmed override schedule), then the door will remain locked.

Authorised PIN/card users can open the door as normal.

An unlock command issued from management or configuration software will unlock the door and cancel the start action.

An open door or timed open door command issued from management software will perform the function but will not cancel the start action.

Cancelling a start action

A start action that is running can be cancelled by overriding its operation from management or configuration software. For example:

- Where a start action is holding the door unlocked, the action can be cancelled by locking the door via management or configuration software. The cancellation is only for the current iteration of the door schedule and future iterations will still operate.
- In the case where the door is being unlocked by the start action and an unlock command is sent from management or configuration software, the action will continue to operate and is not affected.

When a start action is cancelled, the end action is not performed. The door will return to its default state (locked) if no other override or macro is active.

If a start action that enables the door is cancelled then the door will remain enabled. Similarly, if a start action that disables the door is cancelled then the door will remain disabled.

Deleting a door schedule

When deleting an active door schedule, the start action is immediately cancelled and the cancellation rules described in the “Cancelling a start action” section above apply. Once the running action has been terminated, the door schedule record is removed from CDC4(-EN) so that no future iterations of the door schedule can occur.

When deleting a door schedule that is not active, the door schedule is immediately deleted and no future iterations of the start action can occur.

Random lockout time

When the “Door random bit” event triggers on a door controller door (which can occur if the door Random setting is non-zero), then there is a new setting which locks out the door for a specified amount of time, called Random lockout time. The lockout time can also be specified as indefinite. During this time, the door can only be opened by users with the “Privileged” flag; the door cannot be opened by any other users.

Any LCD RAS attached to the door will display “Locked Out”.

Note: Users with the “Privileged” flag cannot cause a door lockout.

A door random lockout time can be programmed in Downloader on the Access tab of the Doors form. See the “Random lockout time” section on page 66.

LED area mapping for door readers

It is possible to map the LEDs on door readers to specific areas, in the same way as can be done for an Advisor Advanced keypad.

The LED area mapping is programmed in the Door reader dialog, accessed from the Readers tab of the Doors form. See the “LED mapping” section on page 75.

Time and attendance readers

The readers may be used for time and attendance functionality (clocking on and off).

There can be up to 32 RASs (readers or keypads) on the CDC4(-EN) local buses designated as time and attendance readers (see the “Time and attendance” section on page 69).

Using RASs for time and attendance

If using card readers on the CDC4(-EN) data buses, the functionality is determined by whether the reader is an IN reader or an OUT reader. IN readers are Clock On readers and OUT readers are Clock Off readers.

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

Chapter 2

Programming

Summary

This chapter explains how to use the Advisor Advanced programming menu to program the system.

Content

Recommended programming sequence 40

Downloader connection 42

 Uploading default configuration 42

 Upgrading firmware 42

 Programming IP communications 43

Recommended programming sequence

The following is a suggested programming sequence for a Door Controller:

1. Set the CDC4(-EN) DIP switches.
2. Default CDC4(-EN).
3. Connect CDC4(-EN) to Advisor Advanced.
4. Connect Downloader to the Advisor Advanced panel. See “Downloader connection” on page 42.
5. Add CDC4(-EN) as a remote expander in Downloader. See “Expander tab” on page 46.
6. Upload the default configuration from CDC4(-EN) to Downloader. See “Uploading default configuration” on page 42.
7. Upgrade the CDC4(-EN) firmware to the latest version. See “Upgrading firmware” on page 42.
8. Program the CDC4(-EN) IP communications if CDC4(-EN) will operate in extended mode. See “Programming IP communications” on page 43.
9. Program CDC4(-EN):
 - Program the CDC4(-EN) general controller options.
 - Assign RAS to CDC4(-EN).
 - Assign DGP to CDC4(-EN).
10. Program special days if required.
11. Program schedules if required.
12. Program regions if required.
13. Program the CDC4(-EN) doors:
 - Program hardware options for each door.
 - Assign readers to each door.
 - Program access options for each door.
 - Program shunt, passback and RTE options for each door.
 - Program alarm control for each door, if applicable.
14. Program zone and output mappings for Advisor Advanced, if applicable.
15. Program the CDC4(-EN) macro logic, if required.
16. Program user information:
 - Program door groups.
 - Program floor groups.
 - Program users.

The following sections describe each step of the recommended programming sequence above. In the descriptions, Downloader is used for programming CDC4(-EN).

Note: If ATS8600 will be used for management of CDC4(-EN), then some aspects of programming should not be done in Downloader, since ATS8600 will be responsible for those aspects. ATS8600 can be used to configure and manage:

- Holidays
- Schedules
- Door groups
- Floor groups
- Users

In addition to the initial setup and programming of CDC4(-EN), ongoing management can be performed via management software.

For information on management via Downloader, see *ATS8500 Downloader Online Help*.

Downloader connection

The following sections describe how to connect to CDC4(-EN).

Connecting CDC4(-EN)

Connect CDC4(-EN) to the Advisor Advanced panel data bus 1, as required.

Add CDC4(-EN) as a new expander to an existing Advisor Advanced panel.

Using Downloader, follow these steps:

1. Connect Downloader to the Advisor Advanced panel. See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* and Downloader online help for more information.
2. Select the Expander devices settings.
3. Click the New button in the selected data toolbar to add a new expander.
4. Select “At position” from the drop-down list and enter the CDC4(-EN) address (1 to 12).
5. Set the Expander type to CDC4(-EN).

New tabs will appear on the DGPs form to allow the operator to program CDC4(-EN).

If desired, you can set up IP communications on CDC4(-EN). See the “Programming IP communications” section on page 43.

Uploading default configuration

It is important to upload the default values from the door controller into the Downloader database.

To upload the data from the appropriate control panel:

1. Connect Downloader to the Advisor Advanced panel. See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* and Downloader online help for more information.
2. Read the panel configuration by clicking the Read icon.

Upgrading firmware

Firmware on the Door Controller is upgradeable in all operating modes. It is highly recommended that the installer upgrade to the most recent firmware version upon installation.

Note: It is recommended that firmware upgrade be performed via IP where possible, since it is faster than upgrade via an Advisor Advanced panel.

Programming IP communications

If the Door Controller is operating in IP Extended mode, then set up IP communications on the CDC4(-EN).

Configuring Ethernet

Configure Ethernet communications on the CDC4(-EN). Using Downloader, follow these steps:

1. Click the Expander devices list on the Panel data window to open the Expander list.
2. Select the CDC4(-EN) expander.
3. On the Details tab, configure Onboard Ethernet option. Click Browse “...” and provide all the connection details: enable Ethernet, and provide door controller IP configuration.

Configuring communications path

Configure an IP communications path on the CDC4(-EN) for management software. Using Downloader, follow these steps:

1. On the expander list, select the CDC4(-EN) and select Comm paths tab to open the Comm paths form.
2. Select the required path and Click Browse “...” to configure it. In the Common Data Path tab, set Enabled to On. In the IP path tab, set IP protocol to TCP/IP, Client to Server, Dynamic computer address to On, and Listening and Host ports to 3001.

The configured communications path can be used by the management software. If required, set up additional communications paths by repeating the steps in this section with a different communications path.

Chapter 3

Menu reference

Summary

This chapter contains descriptions of all programming menu entries of CDC4(-EN) Door Controller.

Content

Expander devices	46
Expander tab	46
Details tab	47
Assigned RAS tab	50
Assigned DGPs tab	51
Mapped inputs tab	52
Mapped outputs tab	53
Programming mapped inputs and outputs	54
Communication paths tab	54
Macro logic tab	54
Scheduled actions tab	56
Region/HSU Configuration tab	57
Alarm control level tab	60
Lift control level tab	60
Access configuration>Doors	61
Door tab	61
Hardware tab	62
Access tab	63
Shunt/ AntiPassback tab	69
Readers tab	73
Alarm control tab	75
Lifts tab	76
Floor output mapping tab	77
Floor input mapping tab	77
Access Configuration>Regions	78
Users	79
Programming door groups	79
Programming floor groups	79
Programming users	80

Expander devices

The Door Controller is programmed via the *Expander devices* form.

The following tabs appear on the form when a CDC4(-EN) record is selected:

- Expander tab
- Details tab
- Input type
- Assigned RAS tab
- Assigned DGPs tab
- Mapped inputs tab
- Communication paths tab
- Macro logic tab
- Scheduled actions tab
- Region/HSU Configuration tab
- Alarm control level tab
- Lift control level tab

Expander tab

The tab contains general expander settings except the following options, which cannot be configured from the control panel.

Region count limit

When the number of users reaches this limit (0 to 65535), the door 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.

Examples:

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

Region synchronization

The option defines if the selected door controller synchronizes the users in regions with other door controllers for the anti-passback control purposes. The following values are available:

- Only in this CDC4(-EN): The regions are not synchronized with other door controllers. Anti-passback detection only works in the regions that belong to this CDC4(-EN).
- To other CDC4(-EN)s: The regions are synchronized with other door controllers. Anti-passback functions are applicable to all regions in the Advisor Advanced system.

Note: This function is only available if the door controller works in the extended mode.

See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* for details.

Note: Particular door controller settings are disabled in this tab, and can be set only in “Details tab” below.

Details tab

Each field is explained in the following sections.

Output modules number

Enter a value in the range 1 to 8 in order to use clocked output expansion boards. Alternatively, enter 0 (disabled) to use an ATS1810 four-way relay card, or for no output expansion.

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

- Enter a value of 1 if one ATS1811 eight-way relay card is used.
- Enter a value of 2 if one ATS1820 16-way open collector card is used.
- Enter a value of 4 if four ATS1811 eight-way relay cards are used.

Tamper monitoring

If the Advisor Advanced panel monitors input circuits for tamper conditions, then CDC4(-EN) must do the same.

When enabled, the system can detect inactive, active, and fault (open and short circuit) states. When disabled, the system can detect inactive and active states only. Open and short circuit states are detected as active.

Siren monitoring

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

EOL resistor

The EOL (End-Of-Line) resistor is used to detect the electrical states of input circuits. This read-only field shows the actual resistor value.

The EOL resistor value is set in the “Expander tab” on page 46. Note that this value applies to all assigned DGPs.

Siren mode

The on-board siren output can be configured for use with a standard siren, or for use with an integrated siren/strobe unit that requires a 12 V DC supply.

Alternatively, the 12 V DC output can be used for a device that requires 12 V DC power when the CDC4(-EN) siren output is active.

Duress mode

Duress mode allows a user to signal a duress condition (for example, a holdup) by entering a special duress code on a keypad RAS instead of their usual door code.

The system will behave as if the user PIN was entered (for example, to open a door), and it will initiate a duress alarm. The duress alarm can be reset (cancelled) by entering the normal PIN.

Select the duress mode from the following options:

- Disabled: Duress codes are not supported by the CDC4(-EN).
- Increment last digit: The duress code is the user PIN with the last digit incremented by 1. For example, if the user PIN is 1234, then the duress code is 1235. If the user PIN is 1239, then the duress code is 1230.
- Add last digit: The duress code is the user PIN with an extra 5 appended. For example, if the user PIN is 1239, then the duress code is 12395.

Note: This option is not compatible with 10 digit PINs.

- Add first digit: The duress code is the user PIN with an extra 5 prepended. For example, if the user PIN is 1239, then the duress code is 51239.

Note: This option is not compatible with 10 digit PINs.

Onboard Ethernet

To enable the IP communication, follow these steps:

1. Set Enable Ethernet to On.
2. Set static IP data like IP address, gateway address, subnet mask, DNS server addresses.

Long Access Motor Delay [0.1 s]

Set the delay between door relay output 1 and 2 activation.

The value is multiplied by 0.1 s. For example, value 10 means 1 second delay.

If output 1 is used to unlock the door, and output 2 controls the door opening motor, the delay is necessary to prevent the door lock or motor damage.

See also “Unlock Output 2” on page 62.

Arm by Pressing ENTER 3 times after PIN

If this option is set to On, you can set the premises by entering PIN and then pressing Enter three times.

Battery 1 fitted**Battery 2 fitted**

If the option is set to On, the door controller monitors the corresponding battery presence, and generates Battery 1 or Battery 2 fault if this battery is disconnected.

If no battery is connected, Battery missing fault is generated regardless of this setting.

Note: The option is only available in CDC4-EN door controller.

Tamper output location

Program the output to be activated when a “Cabinet Tamper” or a “Siren Fault” condition exists on CDC4(-EN).

Note: Program appropriate outputs using the scheme described in the “Flexible device locations” section on page 26.

Mains fail output location

Program the output to be activated when a “Mains Fail” condition exists on CDC4(-EN).

Low battery output location

Program the output to be activated when a “Low Battery” condition exists on CDC4(-EN).

Bus options

Each bus can have devices other than ATS devices. Each bus supports the OSDP (Open Supervised Device Protocol), SALLIS (by SALTO Systems), and Aperio protocols. Each bus can use one protocol at a time, but the two buses can use different protocols.

See “Bus formats” on page 24 for more information.

Bus format

Each bus format may be one of:

- ATS: ATS protocol for adding devices from the ATS family of products
- Aperio: Aperio protocol
- SALLIS (SALTO): SALLIS protocol by SALTO systems
- OSDP: Open Supervised Device Protocol version 2

Bus baud rate

If the Bus format is not set to ATS, the baud rate on the bus can be configured to be one of the following:

- 4800 baud
- 9600 baud
- 19200 baud

- 38400 baud
- 57600 baud
- 115200 baud

If the Bus format is set to OSDP, then set the baud rate to 9600 baud.

If the Bus format is set to Aperio, then set the baud rate to 19200 baud.

If the Bus format is set to SALLIS (SALTO), then set the baud rate to 38400 baud.

Note: If the Bus format is set to ATS, then the baud rate is fixed at 4800 baud.

Bus encryption key

To use encryption with OSDP readers, set the 128-bit AES encryption key for the bus. There is a 16-character limit on the key length.

The encryption key will be set on each OSDP reader attached to the bus once the encryption key is defined.

Notes

- Once set, the encryption key on an OSDP reader cannot be changed by changing the encryption key for the bus. To reset the encryption key used by an OSDP reader, the reader must be reconfigured with the appropriate OSDP configuration card.
- A single OSDP configuration card cannot be used twice in succession to configure an OSDP reader. Different configuration card must be used in between.

Assigned RAS tab

Keypads and readers attached to one of the door controller local buses must be assigned to CDC4(-EN) on the Assigned RAS tab of the Expander form.

Select the appropriate keypad and click Browse “...” to open the Assigned RAS form.

The following settings are available.

Name

When a RAS is created, it is given the default name “RAS <n>”, where <n> is the RAS number. Enter this menu to edit the current name.

RAS type

This read-only field shows the format used by the bus for the selected RAS. See the “Bus options” section on page 49.

RAS model

If the Bus format field is set to ATS, then the RAS model can be selected from the following:

- ATS1190/1192: ATS smart card reader
- ATS1197: ATS smart card reader with keypad
- ATS1160N/ATS1161N: ATS Mifare DESFire & EV1 reader (with keypad)
- ATS1151: ATS keypad with 3 LED
- ATS1156: ATS magstripe card reader with keypad
- ATS1155: ATS heavy-duty keypad
- ATS1170: ATS Wiegand/reader interface
- ATS118x: ATS smart card readers

Aperio EAC

If the Bus format for the bus is set to Aperio, then enter the Aperio EAC (Electronic Access Control) number in this field. Values can range from 1 to 255.

Poll

Set the option to On to poll the device.

Remove

Click Remove to delete the selected device.

Assigned DGPs tab

Expanders attached to one of the door controller local buses must be assigned to CDC4(-EN) on the Assigned DGP tab of the Expander form.

Select the appropriate expander and click Browse “...” to open the Assigned DGP form.

The following settings are available.

DGP name

When a DGP is created, it is given the default name “DGP <n>”, where <n> is the expander number. Enter this menu to edit the current name.

DGP type

Select the type of expander:

- ATS1201/ATS1201E 8 to 32 Zone DGP
- ATS1210/ATS1211/ATS1210E/ATS1211E 8-Zone DGP
- CDC-2DWIF: Dual Wiegand Interface

Poll

Set the option to On to poll the device.

Remove

Click Remove to delete the selected device.

Mapped inputs tab

See the “Input and output mapping” section on page 29 for information on input and output mapping.

The tab shows a list of input mappings.

Click the Browse “...” button to open the Mapped input dialog to edit the selected input mapping.

On the Mapped input dialog, click the Remove button to remove the selected input data.

Note: CDC4(-EN) inputs are masked if they are not mapped to Advisor Advanced input numbers.

Input no

Enter a number in the range 1 to 32. The mapped input number is an index into the Advisor Advanced input numbering scheme. Thus, for the CDC4(-EN) with address 1 on the Advisor Advanced panel bus 1, mapped input numbers 1 to 32 correspond to Advisor Advanced input numbers 17 to 48. See the “Input and output mapping” section on page 29 for information on Advisor Advanced input mapping.

Input type

Specify the input type for the input mapping. The input types are:

- Not used (reports inactive): The input always reports as inactive.
- Forced: The input is a logical input associated with a door and is active when the door has a Forced Door alarm (from the Door input 1 being active) or there is a tamper condition. Specify the door in the Door field.
- RTE: The input is a logical input associated with a door and is active when the door is in RTE condition (i.e. the door RTE input is active) or there is a tamper condition. Specify the door in the Door field.
- DOTL: The input is a logical input associated with a door and is active when the door has a Door Open Too Long (DOTL) alarm (from the door’s Door input 1 being active). Specify the door in the Door field.
- Shunted Pass through: The input is a physical input which is passed through to the Advisor Advanced panel if the associated door is not shunting. Specify the door in the Door field. The input location must be specified in the Input field.

- **Direct pass through:** The input is a physical input which is passed directly through to the Advisor Advanced panel. This type of input cannot be assigned to a door. The input location must be specified in the Input field.

Door

If the Input type field is one of Forced, RTE, DOTL, or Shunted pass through, then you must specify a door to be associated with the input mapping.

Enter the door number to associate the door with the input mapping.

Input location

If the Input type field is one of Shunted pass through or Direct pass through, then an input device must be specified in the Input field, using the scheme described in the “Flexible device locations” section on page 26.

Mapped outputs tab

See the “Input and output mapping” section on page 29 for information on input and output mapping.

The tab shows a list of output mappings.

Click the Browse “...” button to open the Mapped output dialog to edit the selected output mapping.

On the Mapped output dialog, click the Remove button to remove the selected output data.

The mapped output number is an index into the Advisor Advanced output numbering scheme. Thus, for CDC4(-EN) with address 1 on the Advisor Advanced panel data bus 1, mapped output numbers 1 to 16 correspond to Advisor Advanced output numbers 17 to 32. See the “Input and output mapping” section on page 29 for information on output mapping.

Activating the Advisor Advanced output will activate the specified output device attached to the CDC4(-EN).

Note: Outputs that are not mapped to a device may be used as an input to a macro.

Output type

Specify the output type for the output mapping. The output types are:

- **Disabled:** The output is disabled.
- **Direct map:** The output is directly mapped from the Advisor Advanced to the output specified in the Output field.

Output location

The output location must be specified using the scheme described in the “Flexible device locations” section on page 26.

Programming mapped inputs and outputs

On the attached Advisor Advanced, program the mapped inputs and outputs as required.

Programming mapped inputs

You can configure its settings in the Panel data window > Zones list.

Programming mapped outputs

You can configure its settings in the Panel data window > Outputs list.

Communication paths tab

Configure an IP communications path on the CDC4(-EN) for management software. Follow these steps:

1. On the expander list, select the CDC4(-EN) and select Comm paths tab to open the Comm paths form.
2. Select the required path and Click Browse “...” to configure it. In the Common Data Path tab, set Enabled to On. In the IP path tab, set IP protocol to TCP/IP, Client to Server, Dynamic computer address to On, and Listening and Host ports to 3001.

Other options are for future use.

The configured communications path can be used by the management software. If required, set up additional communications paths by repeating the steps in this section with a different communications path.

Macro logic tab

Up to 48 macros can be defined for the door controller. See “Macro logic” on page 21 for details.

Select the appropriate macro and click Browse “...” to open the Macro form.

On the Macro form, click Remove to remove the macro data.

The following settings are available.

Output function

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

- Disabled: This macro logic program is disabled.

- Non-timed: Follows the result of the logic equation only. If a macro input for this macro changes, the logic equation will be calculated again.
- On pulse (1 to 255) seconds: Activates for the programmed time or the active period of the logic result, whichever is the shortest.
- On pulse (1 to 255) minutes: Activates for the programmed time or the active period of the logic result, whichever is the shortest.
- On timed (1 to 255) seconds: Activates for the programmed time regardless of the macro inputs changing.
- On timed (1 to 255) minutes: Activates for the programmed time regardless of the macro inputs changing.
- On delay (1 to 255) seconds: Activates after the programmed time period unless the result of the logic equation is no longer valid.
- On delay (1 to 255) minutes: Activates after the programmed time period unless the result of the logic equation is no longer valid.
- Off delay (1 to 255) seconds: 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.
- Off delay (1 to 255) minutes: Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active.
- Latched: Activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input (any programmed AND / OR function is not used).

Duration

Enter the time period (1 to 255 seconds or minutes) that is used when any of the timed macro output functions are selected (On pulse, On timed, On delay, or Off delay).

When

Enables programming of up to four logic inputs, which can be a wide variety of conditions such as Door open too long, each corresponding to a specific DGP event. For each logic input, select the logic input type, then select the specific device (in the Item field) by entering the number of the device (for example, input) directly into the field.

The events used as macro conditions are pre-defined as listed in Appendix A “Door controller events” on page 83. Some can only be used for macro inputs, some for macro outputs, and others may be used for either inputs or outputs.

The input can be set to Disabled to disable the condition.

The logic connecting the four logic inputs can be programmed for AND or OR functions. A NAND or NOR function can be achieved by inverting the logic of the particular input with the NO check box.

Activate

This programmed DGP event will be activated when the result of the logic equation is true and any timing conditions are met. Select the type of entity to activate (for example, Door lock), then select the specific device the DGP event relates to (for example, door) by entering the number of the device (for example, input) directly into the field.

The output can be set to Disabled to disable its activation.

Scheduled actions tab

To configure a door schedule in Downloader, click Scheduled actions tab.

Select the appropriate door schedule and click Browse “...” to open the Schedule form.

On the Schedule form, click Remove to remove the schedule data.

The following settings are available.

Door number

Enter the door number on the CDC4(-EN) to select the door.

Enabled

Select On to enable the door schedule.

Start date

Enter the start date for the active period.

Note: If “End date” below is not set, or “Use end date” below is off, the start date is the only day when the schedule is active. In this case, the option “Active on days” described below is not applicable.

Use end date

Select On to enable the use of an end date for the active period.

End date

Enter the end date for the active period, if required.

See also “Start date” above.

Active on days

Select the days of the week that the door schedule will be On (active) during the active period.

Note: The selection is only applicable if both start date and end date are set.

Start time

Enter the start time for the start action.

Action duration

The action duration is the period of time that the Start action should remain in effect. When the action duration expires, the End action will be triggered.

Enter a number of seconds, minutes, hours, and days.

Start action

Select the start action from the following options:

- No action: Take no action
- Unlock: Unlock the door
- Lock: Lock the door
- Disable: Disable the door
- Enable: Enable the door

End action

If an Action duration is defined, select the end action from the options. The options are the same as for the Start action field. See the “Start action” section above.

Region/HSU Configuration tab

Up to 16 High Security User (HSU) configurations can be defined. See “High security” on page 17 for more information.

Click Browse “...” button to open the HSU configuration form.

On the HSU configuration form, click Remove to remove the HSU configuration data.

The following settings are available.

Region

Select a region for the selected HSU configuration.

See also “Regions” on page 17.

Low limit

The minimum number of users required in the selected region. When the number of users in the region is below the programmed value, the output defined in “Below Low limit Output BUS” below is active.

The allowed values are 0 to 65 532. 0 means no limit.

Below Low limit Output BUS

The defined output is active when the number of users in the region is below the value programmed in “Low limit” above. The option is disabled if the Low limit value is set to 0.

High Limit

The maximum number of users required in the selected region. When the number of users reaches the programmed value, the output defined in “High Limit Output BUS” below activates.

The allowed values are 0 to 65 532. 0 means no limit.

High Limit Output BUS

The defined output activates when the number of users in the region reaches the value programmed in “High Limit” above. The option is disabled if the High limit value is set to 0.

Minimum HSU

The minimum number of high security users (HSU) required in the selected region.

The option is similar to “Low limit” on page 57, but applies to high security users.

Below Minimum HSU Output BUS

The defined output is active when the number of high security users in the region is below the value programmed in “Minimum HSU” above.

The option is similar to “Below Low limit Output BUS” on page 57, but applies to high security users.

Maximum HSU

The maximum number of HSU required in the selected region.

The option is similar to “High Limit” above, but applies to high security users.

Maximum HSU Output BUS

The defined output activates when the number of high security users in the region reaches the value programmed in “Maximum HSU” above.

The option is similar to “High Limit Output BUS” above, but applies to high security users.

HSU Warning Time

The time (in seconds) for the warning timer. When the number of high security users is below the minimum, the warning timer starts.

The timer resets if the number of HSU increases to the minimum threshold.

HSU Warning Output BUS

The defined output is active when the warning timer set in “HSU Warning Time” above is running.

HSU Alarm output BUS

The defined output activates when the warning time set in “HSU Warning Time” on page 58 expires and an alarm is raised.

The output is deactivated when the number of HSU increases to the minimum threshold, or when all users leave this region.

Schedule

The schedule is used for the releasing users from the region. See “Release users from region on timezone start” below and “Release users from region on timezone end” below.

Alarm Levels 1..6

Select alarm control levels for the selected region.

The option has no effect if “Alarm control by region” below is disabled.

High Security Users

Activate or deactivate the HSU functionality in the selected region.

If the functionality is disabled, all HSU related options described above have no effect.

Alarm control by region

If the alarm control by region is enabled, the last user leaving the region assigned to door automatically sets the area, and the first user entering the region unsets it.

This functionality is described in “Alarm control by region” on page 18.

Delayed Arming

If enabled, the alarm control by region will cause a delayed set prompt prior to the area set.

Release users from region on timezone start

The users are removed from the region every time the “Schedule” above is started (each segment becomes active).

Release users from region on timezone end

The users are removed from the region every time a segment of the “Schedule” above ends.

Deny access

If the option is set, and there are more users in the region that it is configured by “High Limit” on page 58, entering the region is denied until the user count becomes smaller than this value.

Alarm control level tab

The tab shows a list of alarm control levels for the door controller.

Click Browse “...” button to open the Alarm control level dialog.

Name

Define a name for the selected alarm control level.

Schedule

Specify a panel schedule to apply to this alarm control level. The alarm control level is only available if the schedule is valid.

Areas

An alarm control level can only control the functions of areas that are assigned to it. An alarm control level can be linked to multiple areas. For each area, the alarm control level can control the area permissions for arming, disarming, alarm reset, and for timing.

Click the Browse “...” button to open a dialog to assign a particular area to the alarm control level. In the dialog, select the required area from the Areas list.

The following permissions for each area can be changed:

- Arm: A user with the appropriate alarm group can arm the area.
- Disarm: A user with the appropriate alarm group can disarm the area.

Click the Delete button to remove the selected area data.

Lift control level tab

The tab shows a list of lift control levels for the door controller.

Click Browse “...” button to open the Lift control level dialog.

Name

Define a name for the selected lift control level.

Floors

Select floors that the selected lift control level grants access to.

Time frames

Define up to 8 time frames when the selected lift control level grants access to the floors selected in “Floors” above.

Each time frame contains start time and end time of the day, and week days when it is active.

Access configuration>Doors

Note: Depending on the door type, different options can be available. See “Door type” below.

The following tabs appear on the form when a CDC4(-EN) door or lift is selected:

- Door tab
- Hardware tab (door only)
- Access tab
- Shunt/ AntiPassback tab (door only)
- Readers tab
- Alarm control tab (door only)
- Lifts tab (lift only)
- Floor output mapping tab (lift only)
- Floor input mapping tab (lift only)

The following is a suggested programming sequence for door controller doors:

1. Program hardware options for each door.
2. Assign readers to each door.
3. Program access options for each door.
4. Program shunt, passback and RTE options for each door.
5. Program alarm control for each door, if necessary.

For lifts, you can follow the steps below:

1. Assign readers to each lift.
2. Program access options for each lift.
3. Program override and security key options for each door.
4. Map floor inputs and outputs for lift button control.

Click Doors on the Panel data to open the Door list.

Door tab

The tab contains general door settings except the following option, which cannot be configured from the control panel.

Door type

The following door types are available:

- Standard: A standard door controlled by the control panel.
- ATS125X door: An intelligent door controlled by an ATS125x four-door expander.
- CDC4(-EN) door: An intelligent door controlled by a CDC4(-EN) door controller.

- CDC4(-EN) lift: A lift car controlled by a CDC4(-EN) door controller.

See also *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual*.

Hardware tab

Note: This tab is only available for controller doors.

The tab contains hardware options for the selected door.

The following settings are available.

Lock type

To support simple programming of complex door operation, CDC4(-EN) has various lock types, with associated inputs, outputs and timers. The lock type determines which inputs and outputs are used and how they are used.

The lock types are:

- Strike
- Maglock / drop bolt
- Turnstile

See Chapter 1 “System functions > Lock types” on page 11 for more details.

Devices location

The group contains various input and output locations described below.

Program the locations using the scheme described in the “Flexible device locations” section on page 26.

Unlock Output 1

Specify the output to be activated to unlock the door.

Unlock Output 2

Specify the second output to be activated to unlock the door (in the OUT direction in case of turnstile door), or to drive a motorized lock together with a strike or maglock controlled by unlock output 1.

Door Input 1

Specify the input used to indicate if the door is open or closed. This is usually the reed switch.

Door Input 2

Specify the input connected to the lock monitor on Strike, Maglock, and Drop bolt lock types.

Forced output

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

Warning output

Specify the output to be activated during the “Warning time” when the shunt timer is about to expire, for example, may be used to activate a buzzer above a door to indicate the door needs to be closed.

DOTL output

Specify the output to be activated when an input is in a DOTL condition, for example, the door left open after the shunt timer has expired.

RTE input

Specify the input that activates the request-to-exit function for the door being programmed.

RTE functionality is programmed on the door’s *Shunt/Passback* tab. See the “RTE options” on page 71.

Interlocks

For more information on door interlocking, see the “Interlocking doors” on page 15.

Interlock doors

Tick the door numbers on the same CDC4(-EN) that will be prevented from being accessed at the same time as the door being programmed.

External input 1, 2, 3

CDC4(-EN) can check up to three external inputs for interlocking. If an input is wired up to an external controller door contact, then specify the input in one of the external input fields. Program each input location using the scheme described in the “Flexible device locations” section on page 26.

Access tab

The tab contains access options for the selected door.

The following settings are available.

Door name

When a door is created, it is given the default name “Door <n>”, where <n> is the door number. Enter this menu to edit the current name.

Door type

The Door type field is for future use. Currently, the door type is set as Door and cannot be changed.

Unlock time

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

Enter the time in seconds.

Extended unlock time

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

Enter the time in seconds.

Dual Badge Time

Note: By default, if two-badge functionality is enabled, only the second user is reported as having accessed a door. Thus if a visitor and an accompanying guard badge their cards to open a door, only the guard is considered as having accessed the door.

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

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

Enter the time in seconds.

See “Dual badge” on page 67 (the two-badge option can be configured separately for IN readers and OUT readers). Also see the “Two badge unlock, one badge relock” section on page 67.

Card to PIN time

Note: Card to PIN time can be set per door on the CDC4(-EN).

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

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

Enter the time in seconds.

See the “Card and PIN” section on page 66 (the card and PIN option can be configured separately for IN readers and OUT readers).

Roller door up time

Reserved for future use.

Roller door down time

Reserved for future use.

Pre-lock time

Once the door open input (door input 1) has been deactivated, the door controller waits for the pre-lock time to expire before locking the door. If the door open input activates during the pre-lock time, the door is deemed open and the pre-lock timer is cancelled. The shunt continues during the pre-lock time.

Door input 1 is programmed on the Hardware tab for the door.

Enter the time in seconds.

Post lock time

The post-lock time allows time for a lock to fully engage. After the post lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door open input (Door input 1) activates during the post-lock time, the door is deemed open and the post lock timer is cancelled. The shunt continues during the post-lock time.

Door input 1 is programmed on the “Hardware tab” on page 62.

Enter the time in seconds.

Multi-badge time

Note: Multi badge time can be set per door on the CDC4(-EN) door controller.

If “Two-badge” on page 67 is enabled for the door, then this field defines the amount of time permitted between the first and second badges. If the time expires, then the user will need to repeat the three badges in order to set or unset the area. See also “Two badge unlock, one badge relock” on page 67.

Additionally, if a reader alarm control options specify three-badge alarm control for users who are authorised to set and unset areas, this field defines the amount of time permitted between the first and third badges. If the time expires, then the user will need to repeat the three badges in order to set or unset the area.

Enter a number in seconds.

Random

The value defines the average percentage of the number of times that a valid card or PIN is presented to open the door that the door’s “Door random bit” event will be activated.

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

Alternatively, if the Random lockout time (below) has a value, then the “Door random bit” event locks out the door for the specified time. During this time, the door cannot be opened by any user.

Enter a number in the range 0 to 100.

Random lockout time

When the “Door random bit” event triggers (as described in “Random” on page 65), the door can be locked out for the amount of time specified in this field. During this time, the door can only be opened by a user with the “Privileged” flag. Any LCD RAS attached to the door will display “Locked Out”.

Enter the time in seconds.

Unlocked Schedule

The option controls the time when the door can be opened without the need to use a valid card or PIN. Free access is allowed when the schedule is valid.

Click Browse “...” to open the Schedule list. Uncheck Disabled check box and then select an appropriate schedule.

Low Security Schedule

The option controls the time when the door can be opened with either a card *or* a PIN if the door is configured to require card *and* PIN. Only a valid card *or* PIN code is needed to open the door when the schedule is valid.

Click Browse “...” to open the Schedule list. Uncheck Disabled check box and then select an appropriate schedule.

IN reader options

Each door can have up to six readers in any combination of IN readers and OUT readers.

A reader is defined as an IN reader if its Door side field is set to IN reader when it is added using the Door reader dialog (accessed from the Readers tab for the door). Similarly, a reader is defined as an OUT reader if its Door side field is set to OUT reader when it is added using the Door reader dialog.

Card and PIN

Select this option to require that both a card *and* a PIN must be used to unlock the door via any of the IN readers. If not selected, then either a card *or* a PIN will unlock the door via any of the IN readers.

See also “Low Security Schedule” above.

No PIN if Low Security

Select this option to require that only a card must be used to unlock the door via any of the IN readers during the low security schedule (see the “Low Security Schedule” section above). If not selected, then both a card and a PIN must be

used to unlock the door via any of the IN readers during the low security schedule.

Deny region 1 users

Select this option to prevent users who are currently recorded as being off-site (i.e. in region 1) from unlocking this door via any of the IN readers.

See the “Regions” on page 17 for more information about regions.

Two-badge

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

The presentation of card and/or PIN must occur within the two-badge time (see the “Dual Badge Time” on page 64).

Once the two valid card and/or PINs have been presented to the reader, a 60 second timer starts, which allows the second user to perform functions such as locking the door, or alarm control.

For example, if the *IN alarm control* for the door is set to *Alarm control on 1st badge*, then the second user can present their card to disarm areas. See the “IN alarm control” section on page 75.

Similarly, if *2 badge unlock, 1 badge re-lock* is configured for the door, then the second user can present their card to lock the door. See the “Two badge unlock, one badge relock” section below.

OUT reader options

The options for IN readers can also be applied to OUT readers.

See “IN reader options” on page 66 for details.

Other options

The following options are available.

Dual badge

If two-badge functionality is used, then enabling this option means that both users are reported as having accessed a door. In addition, anti-passback rules and region rules (including region count) will be applied to both users. If either user fails for any reason, for example, passback, then the door will remain locked and access will be denied when the failed user presents their card or PIN.

Disabling this option means that only the second user is reported as having accessed a door. Thus if a visitor and an accompanying guard badge their cards to open a door, only the guard is considered as having accessed the door.

Two badge unlock, one badge relock

As an alternative to two-badge, two badge unlock avoids unintended unlocking of a door if a user accidentally presents their card to a reader, for example, by

brushing past the reader with the card in a pocket. When two badge unlock is enabled (and the low security schedule is not valid), the user may unlock the door by presenting the same card twice within the two-badge time (see “Dual Badge Time” on page 64). If the low security schedule is valid, then the two badge unlock setting is ignored (see the “Low Security Schedule” section on page 66).

The door will remain unlocked until a user badges a card at the reader.

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

OUT reader no schedule required

If selected, OUT readers will allow access even if a user door group does not have a valid schedule.

Door unlocked until opened

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

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

Door unlock after entry

This field determines whether the override schedule (see the “Unlocked Schedule” section on page 66) takes effect immediately the schedule commences or after a user enters.

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

Report open/close

When set to On, a report is sent to management software when the *Door input 1* is active (opened) or inactive (closed).

This is only a reporting function.

Report forced door

When set to On, a report is sent to management software when the *Door input 1* is active without valid access (card, PIN, or RTE request).

This is only a reporting function.

Report DOTL

When set to On, a report is sent to management software when the *Door input 1* is in the door open too long (DOTL) state. For example, the door is still open after the shunt timer expires.

This is only a reporting function.

Time and attendance

When set to On, the reader can be used as a time and attendance reader. See the “Time and attendance readers” section on page 37 for more information.

Note: Some management software applications do not support time and attendance functionality.

Disable duress

When set to On, the system keypad duress functionality cannot be used at this door.

Shunt/ AntiPassback tab

Note: This tab is only available for controller doors.

The tab includes options for shunting, RTE and anti-passback for the selected door.

Shunt options

Shunting is a procedure that stops an open door causing an alarm for a set time.

Shunt type

This field defines shunt conditions. The options are:

- No shunting: The door will not be shunted.
- Input shunting: The door will be shunted and will generate a forced door alarm if it is left open (i.e. Door input 1 is active) longer than the programmed Shunt time (or Ext. shunt time, if applicable).
- Input shunting & DOTL: The door will be shunted and will generate a DOTL (Door Open Too Long) alarm if it is left open (i.e. Door input 1 is active) longer than the programmed Shunt time (or Ext. shunt time, if applicable).
- Auto shunting & DOTL: If the areas assigned to the door are in access (disarmed), shunting of the door will commence when the Door input 1 is active. No card or PIN is required. A DOTL alarm is generated if it is left open longer than the programmed Shunt time.

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.

Enter the time in seconds.

Ext. shunt time

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

Enter the time in seconds.

Shunt warning

Program the amount of time for an output to activate, to sound a warning device, before the Shunt time (or Ext. shunt time, if applicable) expires.

Enter the time in seconds.

Shunt until door closes

Select this option to ignore the programmed Shunt time (or Ext. shunt time), and to shunt Door input 1 until the door closes (the door input is deactivated).

Cancel shunt after door closed

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

Select this option to use the programmed Shunt time (or Ext. shunt time) to shunt Door input 1 and then to cancel the shunt when the door closes (the door input is deactivated).

Anti-passback options

The anti-passback options control the operation of the reader if a card or PIN is used to enter the same region that the user is currently in.

This is valid only when a region is programmed for the door. See the “In region” section on page 71 and the “Out region” section on page 71.

Anti-passback violation is reported to management software.

Notes

- To clear an anti-passback violation, the card must be used at another appropriate reader to change the region number that the user is recorded against. Alternatively, the user can be assigned to the desired region using the configuration software (in standard mode) or management software (in extended mode).
- The door must be opened after the reader is used before anti-passback will take effect.
- Anti-passback settings do not apply to users with the “Privileged” flag in regions 0 to 199.

Anti-passback

Select the type of anti-passback desired:

- No anti-passback: The anti-passback functionality is not active. The card will open the door without generating an alarm.
- Soft anti-passback: A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
- Hard anti-passback: The card will not open the door when used a second time and the attempt will generate an alarm.
- Timed anti-passback: The card will not open the door when used a second time in succession at the same door within the programmed time and the attempt will generate a report.

Timed anti-passback period

Enter the time delay that forces the user to wait until the delay timer expires.

Enter a number of seconds.

In region

Specifies a region which represents the IN readers for each door.

When a valid card or PIN is entered at the door reader, the region that the user is entering into is recorded against the user code. The system is then able to report an anti-passback violation.

Type the region number directly into the field.

Note: The door must be opened for this to be effective.

Out region

Specifies a region which represents the OUT readers for each door.

When a valid card or PIN is entered at the door reader, the region that the user is entering into is recorded against the user code. The system is then able to report an anti-passback violation.

Type the region number directly into the field.

Note: The door must be opened for this to be effective.

RTE options

The RTE options define the operation of the RTE button (exit button).

There are the following options for setting up an RTE button:

- The request-to-exit button is wired to the RTE input defined on the Hardware tab for the door. See the “RTE input” section on page 63.
- A reader assigned to the door is defined as having an RTE input. See the “Enable RTE” section on page 74.

- In case of a turnstile type door, the RTE input always activates Unlock output 2, therefore this input must be enabled for the OUT reader only. See “Enable RTE” on page 74 for details.

Note: There must be an RTE schedule defined for RTE functionality to work.

RTE control

Defines the operation of the RTE button:

- RTE time door open: When the RTE button is pressed, the door will unlock for the Access time programmed on the Access tab for the door. See the “Unlock time” section on page 64.
- RTE holds door open: Allows the door to be held unlocked for as long as the Request To Exit button is pressed or for the programmed unlock time, whichever is longer.

Note: This functionality only works for onboard or DGP input used as RTE. Dedicated RAS RTE input will not hold the door open.

- RTE shunts only: When the RTE button is pressed, the input is shunted.

RTE schedule

The RTE schedule controls the times when an RTE button will unlock a door to allow exit. When the schedule is valid, a user can press the RTE button and the door will unlock.

Select the schedule by clicking the Browse “...”.

IN RTE disabled when set

This option controls the ability to use the RTE button on any IN reader to open the door if any of the areas assigned to the door (via an access control level) are set, i.e. armed. If any of the areas assigned to the door are set then the RTE button will not unlock the door.

OUT RTE disabled when secure

This option controls the ability to use the RTE button on any OUT reader to open the door if any of the areas assigned to the door (via an access control level) are set, i.e. armed. If any of the areas assigned to the door are set then the RTE button will not unlock the door.

RTE report

When selected, a report is sent to management software when the RTE function is used.

This is only a reporting function.

Readers tab

Each door can have up to six door readers associated with it in any combination of IN and OUT readers.

Readers can be assigned to doors on the *Readers* tab of the Doors form.

Note: If the reader is attached to one of the CDC4(-EN) local buses, then the appropriate RAS must be assigned to CDC4(-EN) on the Assigned RAS tab of CDC4(-EN), and polled. See the “Assigned RAS tab” section on page 50.

The *Readers* tab shows a list of assigned readers for the door.

Click the Browse “...” button to open the Reader configuration dialog to edit the settings of the selected reader in the RAS list.

Click the Remove button to remove the selected reader data.

Reader name

Enter the reader name.

Reader enabled

Set to On to enable the reader.

Door side

Select the door side, which may be one of the following:

- *Out (IN reader)*: IN reader placed on the outside of the door.
- *In (OUT reader)*: OUT reader placed on the inside of the door.

Card format

Select the card format for the reader from the following options:

- Automatic / Not available: The CDC4(-EN) will automatically determine the card format from the card used.
- ATS 27 bit: For range of ATS proximity readers supplied by Carrier Fire & Security.
- ASP 27 bit: For Indala ASP range of proximity readers using 27-bit Wiegand format.
- ASP 26 bit: For Indala ASP range of proximity readers using 26-bit Wiegand format.
- Wiegand 32 bit: For 32-bit Wiegand format readers. Uses a 16-bit card number and 16-bit site code.
- Wiegand Chubb (36 bit): For Wiegand Chubb 36 bit format.
- Wiegand 26 bit: For standard 26-bit Wiegand format readers. Has a 16-bit card number (0-65534) and an 8-bit site code (0-255).
- Mag card ATS: For ATS format magnetic swipe cards.

- Mag card Midas: For Midas format magnetic swipe cards.
- Kastel 32 bit: For Kastel format cards.

LCD RAS

Set to On if the reader has LCD (liquid crystal display).

Enable RTE

Set to On if the reader has an RTE button connected to the reader IN or RTE terminal.

Note: For turnstile type door RTE activates door in the OUT direction, so you can enable RTE for OUT reader only.

RAS location

Program the reader's location using the scheme described in the "Flexible device locations" section on page 26.

Wiegand LED behaviour

Note: This option has impact only on the on-board Wiegand interface and 2-door Wiegand Interface.

Select the reader LED behaviour from the following options:

- LED 1 on when locked: LED 1 is on when the door is locked.
- LED 1 on when unlocked: LED 1 is on when the door is unlocked.
- 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).
- 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.)
- Two LED access/secure: Readers with dual LED control lines connected indicate the area disarmed and armed with different LED colours.
- Two LED valid/void: Readers with dual LED control lines connected indicate User Valid or Void using different LED colours.
- LEDs disabled: No LED control.
- Legacy LED 1 on when locked, Legacy LED 1 on when unlocked, Legacy LED 1 on when area is armed, Legacy LED 1 off when area is armed, Legacy Two LED access/secure, Legacy Two LED valid/void: These options provide backward compatibility with earlier firmware versions, where LED 2 functions as an alarm LED.

Note: On readers with dual LED control lines, LED 2 may also be programmed to indicate other conditions via the CDC4(-EN) macro logic programming.

LED mapping

The LED mapping allows the operator to program which area number is assigned to the reader area LEDs, if applicable.

In each LED field, enter an area number to select an area.

Alarm control tab

Note: This tab is only available for controller doors.

See “Alarm control” on page 22 for more information.

IN alarm control

This field determines whether the door’s IN readers can be used to control the alarm system (arm/disarm) and if so, the way in which it can be controlled:

- No Alarm control: It is not possible to arm/disarm via the reader.
- Alarm control on 1st badge: Presentation of a valid card at the reader will disarm the system on the first badge. (Three badges are still required to arm system).
- Alarm control on 3rd badge: Presentation of a valid card three times at the reader will arm/disarm system.
- Alarm control always (off = IN, on = OUT): Presentation of a valid card at the IN reader will disarm the system and presentation of a valid card at the OUT reader will arm the system.
- Alarm control via region count: The last user leaving the panel region assigned to door automatically sets the area, and the first user entering the region unsets it. This option is similar to option “Alarm control on 1st badge”, but works only for the last and the first user in the region. See “Regions” on page 17 for more details.

Note: Panel regions must be configured in Panel > Regions menu. See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* for more details on panel regions.

OUT alarm control

This field determines whether the door’s IN readers can be used to control the alarm system (set/unset) and if so, the way in which it can be controlled. The options are the same as for the IN alarm control field. See the “IN alarm control” section above.

IN denied when set

When set to On, a valid card or PIN will not open a door if any of the areas assigned to the door are set.

OUT denied when set

When set to On, a valid card or PIN will not open a door if any of the areas assigned to the door are set.

Low Security when IN areas disarmed

If the option is set to Yes, the user authorization mode changes from Card and PIN to Card or PIN after the state of door IN alarm control areas is changed to unset.

Lock door when IN areas armed

If the option is set to Yes, the door is locked automatically after the state of door IN alarm control areas is changed to set. **Note:** This option influences only the setting process. Manual or calendar action can unlock the door. Changing this option will not change the door state on the configuration update.

Unlock door when IN areas disarmed

If the option is set to Yes, the door is unlocked automatically after the state of door IN alarm control areas is changed to unset. **Note:** This option influences only the unsetting process. Manual or calendar action can unlock the door. Changing this option will not change the door state on the configuration update.

IN alarm control levels

This field shows a list of alarm control levels for the door IN readers, as configured on the *Readers* tab for the door. Alarm control levels are defined on the door *Alarm control levels* tab (see “Alarm control level tab” on page 60).

Open the list to assign alarm control levels to the door IN readers. In the dialog, select the required alarm control levels.

OUT alarm control levels

This field shows a list of alarm control levels for the door OUT readers, as configured on the *Readers* tab for the door. Alarm control levels are defined on the door *Alarm control levels* tab (see “Alarm control level tab” on page 60).

Open the list to assign alarm control levels to the door OUT readers. In the dialog, select the required alarm control levels.

Lifts tab

Note: This tab is only available for controller lifts.

Override group

Click Browse “...” to open theFloor group list. Uncheck Undefined check box and then select an appropriate floor group to override the lift control with a floor group.

See “Lift automatic override” on page 8 for details.

Note: This option works only in standard mode.

Security group

Click Browse “...” to open the Floor group list. Uncheck Undefined check box and then select an appropriate floor group to override the lift control by a security key with a floor group.

See “Security key override” on page 8 for details.

Note: This option works only in standard mode.

Security key

Program an input that will be used for a security key lock.

Enter the input location for this input.

Caution: RAS inputs cannot be used as security keys.

Wait for floor selection

When the option is set to On, the floor selection is available until a floor button is pressed. This option overrides access time configured in “Unlock time” on page 64.

Lift override levels

Select up to 10 lift control levels for the lift automatic override.

Lift control levels are defined in “Expander devices > Lift control level tab” on page 60.

Security key override levels

Select up to 10 lift control levels for the lift security key override.

Lift control levels are defined in “Expander devices > Lift control level tab” on page 60.

Floor output mapping tab

Note: This tab is only available for controller lifts.

The tab allows you to map physical outputs to floor button selection.

Select a floor, and then choose an output, which controls this floor availability as well as indication.

Floor input mapping tab

Note: This tab is only available for controller lifts.

The tab allows you to map physical inputs to floor buttons.

Select a floor, and then choose an input, which this floor button is connected to.

Access Configuration>Regions

A region is a defined access control area having doors acting as boundaries.

Regions are used by the following functions:

- Areas set and unset
- Anti-passback functions to keep track of users.
- High security function to allow users in the region under high security users (HSU) supervision.

To define a region in a CDC4(-EN), follow these steps in Downloader:

1. Click the Regions item on the Panel programming form to open the Regions list.
2. On the Panel programming form, click the New button in the toolbar to add a new region record.
3. Enter a name for the region in the Record name field.
4. Enter a description for the region in the Record description field.

Note: Region 1 is an outside region. It cannot be changed.

See *Advisor Advanced AT5x500A(-IP) Installation and Programming Manual* for more details.

See also “Regions” on page 17.

Users

Programming door groups

Note: Typically, door groups will be configured using ATS8600. The following information is for using Downloader to program door groups if required.

A CDC4(-EN) in Standard mode inherits the door groups of the Advisor Advanced it is connected to, so is limited to 128 door groups. You can add CDC4(-EN) doors to existing door groups or create new Advisor Advanced door groups for the CDC4(-EN) doors.

A CDC4(-EN) in Extended mode uses CDC4(-EN) door groups, of which there can be up to 10,000.

To add a door group to an Advisor Advanced panel, follow these steps:

1. Click the Door groups on the Panel data window to open the Door groups list.
2. On the Door groups list, click the New button in the toolbar to add a new door group record.
3. Enter a name and a description for the door group.
4. On the Door group doors, click the Browse “...” button to select the appropriate doors.
5. On the Door Group Data Editor form, select the appropriate door and click Browse “...” to select the schedule for the selected door.
6. On the Schedule selector form, select up to two panel schedules for the selected door.

Refer to the *Advisor Advanced Programming Manual* for more information on door groups.

Programming floor groups

Note: Typically, floor groups will be configured using ATS8600. The following information is for using Downloader to program floor groups if required.

A CDC4(-EN) in Standard mode inherits the floor groups of the Advisor Advanced it is connected to, so is limited to 128 floor groups. You can add CDC4(-EN) floors to existing floor groups or create new Advisor Advanced floor groups for the CDC4(-EN) floors.

A CDC4(-EN) in Extended mode uses CDC4(-EN) floor groups, of which there can be up to 10,000.

Note: In Extended mode floor groups can be programmed only by the ATS8600 management software. The control panel does not support this functionality.

To add a floor group to an Advisor Advanced panel, follow these steps:

1. Click the Floor groups on the Panel data window to open the Floor groups list.
2. On the Floor groups list, click the New button in the toolbar to add a new floor group record.
3. Enter a name and a description for the floor group.
4. On the Floor group doors, click the Browse “...” button to select the appropriate floors.
5. On the Floor Group Data Editor form, select the appropriate floor and click Browse “...” to select the schedule for the selected floor.
6. On the Schedule selector form, select one panel schedule for the selected floor.

Programming users

Note: Typically, users will be configured using ATS8600. The following information is for using Downloader to program users if required.

A CDC4(-EN) inherits the users of the Advisor Advanced panel it is connected to, so is limited to 65532 users.

You can add new users for the CDC4(-EN), or configure CDC4(-EN) access and credentials for existing users in the Downloader database.

To add a new user to a CDC4(-EN), follow these steps:

1. Click Users on the Panel data window to open the Users list.
2. On the Users list, click the New button in the toolbar to add a new user record.
3. Enter the required information on the User tab.
4. Ensure that the Door group field has a door group entry that has CDC4(-EN) doors. Click the Browse “...” button to open a door group selection dialog and assign the appropriate door groups.
5. If there are lifts programmed, ensure there is a floor group entry that has CDC4(-EN) floors.

Note: If the “Privileged” checkbox for the selected user is set, the user is still allowed to access the regions where the limits for users or high security users are exceeded. See “High security” on page 17 for details. Also, the anti-passback limitations are not applied to privileged users.

Refer to the *Advisor Advanced AT5x500A Installation and Programming Manual* for more information on users.

Note: A CDC4(-EN) in Standard mode is limited to 56 bits of card data. A CDC4(-EN) in Extended mode supports up to 128 bits of card data. However, in extended mode, cards with more than 56 bits of card data cannot be used for alarm control functionality.

Appendix A

Door controller events

For Door events, see Table 6 below. For other events, see Table 7 on page 85.

For macro event ranges, refer to the following tables:

- Table 8 on page 85 for doors
- Table 9 on page 87 for areas
- Table 10 on page 87 for data buses

Table 6: Door macro event descriptions

Name	Description	Input	Output
Door access denied	Door access has not been allowed	Yes	No
Door access granted	Door access has been allowed	Yes	No
Door access granted 1st badge	Door access has been granted when badged once	Yes	No
Door access granted 2nd badge	Door access has been granted when badged twice	Yes	No
Door access granted 3rd badge	Door access has been granted when badged three times	Yes	No
Door access granted in button	Door access has been granted and IN button pressed	Yes	No
Door access granted out button	Door access has been granted and OUT button pressed	Yes	No
Door access granted traced	Door access has been granted to a user with trace On	Yes	No
Door anti-passback [2]	Anti-passback is active	Yes	No
Door area secure	Area assigned to door is secure	Yes	Yes
Door buzzer [3]	Buzzer output is active	Yes	Yes
Door disabled	Door is disabled completely (from keypad or computer)	Yes	Yes
Door two-badge inside [2]	Two-badge access is required at the "IN" reader	Yes	Yes
Door two-badge outside [2]	Two-badge access is required at the "OUT" reader	Yes	Yes
Door enabled	Door is enabled	No	Yes

Name	Description	Input	Output
Door fire override	Secondary override is active	Yes	Yes
Door forced	Door Contact is open with no valid door command	Yes	No
Door interlock	Interlock input(s) are active	Yes	Yes
Door interlock override [1]	If the interlock has been overridden	Yes	Yes
Door keypad duress [3]	Duress PIN code entered at door keypad	Yes	No
Door LED1 [3]	LED 1 output is active	Yes	Yes
Door LED2 [3]	LED 2 output is active	Yes	Yes
Door lock	Lock output is de-activated to lock the door	No	Yes
Door low security inside [2]	Card and PIN required to access at the “IN” reader	Yes	Yes
Door low security outside [2]	Card and PIN required to access at the “OUT” reader	Yes	Yes
Door open	Door Open command is active (to unlock / start shunt)	Yes	Yes
Door open too long	Door Contact is open after shunt timer has expired	Yes	No
Door override	The override schedule assigned to the door is valid	Yes	Yes
Door override inhibit [1]	The override schedule is inhibited	Yes	Yes
Door random bit	An event is generated at random when the door is accessed	Yes	No
Door reader disabled [4]	Reader is disabled	Yes	Yes
Door reader enabled	Reader is enabled	No	Yes
Door closed and locked	When the door is locked and the door is closed	Yes	No
Door shunt warning	Shunt warning timer is running	Yes	No
Door shunting	Shunt timer is running	Yes	Yes
Door unlock	Lock output is active to unlock the door	Yes	Yes
Door reader fault [3]	Fault detected on reader (Comms / tamper / etc.)	Yes	No
Door lock fault [3]	Cable tamper / fault detected on lock output wiring	Yes	No
Turnstile override – IN [5]	The override schedule assigned to the turnstile door is valid, IN direction	No	Yes
Turnstile override – OUT [5]	The override schedule assigned to the turnstile door is valid, OUT direction	No	Yes

[1] Denotes rule can only be activated as a result of another door macro.

[2] 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)

[3] Denotes the event is currently not enabled.

[4] User with the “Privilege” attribute set can override the “Reader disabled” function.

[5] For turnstile overrides, the macro will override credentials being entered. Nobody will be able to enter (turnstile override – OUT active) or exit (turnstile override – IN active) the premises via the turnstile when the macro is active.

Table 7: Other macro event descriptions

Name	Description	Input	Output
Area disarmed	Area in access (99 events, 1 per area)	Yes	No
Area alarm	Input(s) in alarm in area (99 events, 1 per area)	Yes	No
CDC4(-EN) battery test active [1]	The battery test on this Controller is running (1 event)	Yes	No
CDC4(-EN) battery test fail [1]	The battery test failed on this Controller (1 event)	Yes	No
CDC4(-EN) low battery [1]	Low battery condition exists on the Controller (1 event)	Yes	No
CDC4(-EN) fuse fail [1]	Fuse Fail condition exists on the Controller (1 event)	Yes	No
CDC4(-EN) mains fail [1]	Mains fail condition exists on the Controller (1 event)	Yes	No
CDC4(-EN) offline [1]	Controller is not communicating with the Challenger (1 event)	Yes	No
CDC4(-EN) siren active [1]	The siren output (16th output) is active (1 event)	Yes	No
CDC4(-EN) siren fail [1]	Siren fail (siren tamper) condition exists on this Controller (1 event)	Yes	No
CDC4(-EN) tamper [1]	Cabinet tamper condition exists on this Controller (1 event)	Yes	No
DGP output active	System output assigned to this DGP is active (16 events, 1 per output). The first 16 outputs on DGP can also be activated by physical output function.	Yes	Yes
DGP zone active	Input on this DGP is active (16 events, 1 per input)	Yes	Yes
Physical output	Output connected to this DGP is active (255 events, 1 per output). If the physical output is numbered higher than the first 16 in the DGP, then it can only be activated by door macro.	Yes	Yes
DGP offline	DGP on door controller local bus is offline	Yes	No
RAS offline	RAS on door controller local bus is offline (16 events, 1 per RAS address)	Yes	No
Region limit [1]	When the number of people in any region reaches the present limit (255 events, 1 per region)	Yes	No

[1] Denotes the event is currently not enabled.

Table 8: Macro event range for doors

Name	Input – I, Output – O, Both – I/O	D1	D2	D3	D4	D5	D6	D7	D8
Door open	I/O	1	2	3	4	5	6	7	8
Door unlocked	I/O	9	10	11	12	13	14	15	16
Door lock	O	17	18	19	20	21	22	23	24
Door override	I/O	25	26	27	28	29	30	31	32

Name	Input – I, Output – O, Both – I/O	D1	D2	D3	D4	D5	D6	D7	D8
Door override inhibit	I/O	33	34	35	36	37	38	39	40
Door disabled	I/O	41	42	43	44	45	46	47	48
Door enabled	O	49	50	51	52	53	54	55	56
Door reader disabled	I/O	57	58	59	60	61	62	63	64
Door reader enabled	O	65	66	67	68	69	70	71	72
Door two-badge inside	I/O	73	74	75	76	77	78	79	80
Door two-badge outside	I/O	81	82	83	84	85	86	87	88
Door low security inside	I/O	89	90	91	92	93	94	95	96
Door low security outside	I/O	97	98	99	100	101	102	103	104
Door anti passback	I/O	105	106	107	108	109	110	111	112
Door shunting	I/O	113	114	115	116	117	118	119	120
Door shunt warning	I	121	122	123	124	125	126	127	128
Door area secure	I/O	129	130	131	132	133	134	135	136
Door interlock	I/O	137	138	139	140	141	142	143	144
Door interlock override	I/O	145	146	147	148	149	150	151	152
Door keypad duress	I	153	154	155	156	157	158	159	160
Door reader fault	I	161	162	163	164	165	166	167	168
Door lock fault	I	169	170	171	172	173	174	175	176
Door dotl	I	177	178	179	180	181	182	183	184
Door forced	I	185	186	187	188	189	190	191	192
Door LED 1	I/O	193	194	195	196	197	198	199	200
Door LED 2	I/O	201	202	203	204	205	206	207	208
Door buzzer	I/O	209	210	211	212	213	214	215	216
Door random bit	I	217	218	219	220	221	222	223	224
Door access denied	I	225	226	227	228	229	230	231	232
Door access granted	I	233	234	235	236	237	238	239	240
Door access granted traced	I	241	242	243	244	245	246	247	248
Door access granted 1st badged	I	249	250	251	252	253	254	255	256
Door access granted 2nd badged	I	257	258	259	260	261	262	263	264
Door access granted 3rd badged	I	265	266	267	268	269	270	271	272
Door fire override	I/O	289	290	291	292	293	294	295	296
Door closed and locked	I	297	298	299	300	301	302	303	304
Turnstile override – IN	O	401	402	403	404	405	406	407	408
Turnstile override – OUT	O	417	418	419	420	421	422	423	424

Table 9: Macro event range for areas

Events	AREA NUMBER									
	1	2	3	~	~	~	~	97	98	99
Note: These events can only be used as input conditions to a door macro not as an output activation of an door macro										
Area Accessed [1]	4091	4092	4093	~	~	~	~	4187	4188	4189
Area Alarm [1]	4190	4191	4192	~	~	~	~	4186	4287	4288
DGP Outputs	577	578	579	~	~	~	~	590	591	592

[1] These events are not currently enabled.

Table 10: Macro event range for data buses

	RAS offline		DGP offline	
	Bus 1	Bus 2	Bus 1	Bus 2
1	625	641	657	673
2	626	642	658	674
3	627	643	659	675
4	628	644	660	676
5	629	645	661	677
6	630	646	662	678
7	631	647	663	679
8	632	648	664	680
9	633	649	665	681
10	634	650	666	682
11	635	651	667	683
12	636	652	668	684
13	637	653	669	685
14	638	654	670	686
15	639	655	671	687
16	640	656	672	688

Appendix B

CDC4(-EN) defaults

Table 11: Access and Shunt/RTE/Passback Defaults

	Function	Defaults
Access TAB	Door Type	Door
	Access Time	5 sec
	Two-badge time	8 sec
	Pre lock time	2 sec
	Random event %	0
	Override TZ	
	Multi badge time	5 sec
	Long access time	15 sec
	Card to PIN time	8 sec
	Post lock time	2 sec
	Random % lockout time	
	Low security TZ	
	Report DOTL	Enabled
	Report forced door	Enabled
Shunt/RTE/Passback TAB	Shunt options	
	Shunt type	Input shunting& DOTL
	Ext. shunt time	90 sec
	Shunt time	1 min
	Warning time	15 sec
	Anti-passback options	
	Anti-passback	Disabled
	RTE options	
	RTE	RTE timed
	RTE schedule	0-(24 Hours)
	RTE reporting	Enabled

Table 12: Hardware Options: Default Input/Output number assignments

	Door number	Location	Device number
Lock output 1	1 st Door	On-board	1
	2 nd Door	On-board	2
	3 rd Door	On-board	3
	4 th Door	On-board	4
	5 th Door	On-board	NONE
	6 th Door	On-board	NONE
	7 th Door	On-board	NONE
	8 th Door	On-board	NONE
Door input 1	1 st Door	On-board	1
	2 nd Door	On-board	3
	3 rd Door	On-board	5
	4 th Door	On-board	7
	5 th Door	On-board	NONE
	6 th Door	On-board	NONE
	7 th Door	On-board	NONE
	8 th Door	On-board	NONE
RTE input	1 st Door	On-board	2
	2 nd Door	On-board	4
	3 rd Door	On-board	6
	4 th Door	On-board	8
	5 th Door	On-board	NONE
	6 th Door	On-board	NONE
	7 th Door	On-board	NONE
	8 th Door	On-board	NONE

Glossary

Access control	The control of entry to, or exit from, a security area through doors.
Action	Action is a user programmed function, which can be done automatically according to the programmed schedule.
Action list	Action lists are used to group configured actions. They can be done automatically according to the programmed schedule.
Active	See Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault.
Alarm	The state of a security system when a device connected to a zone is activated and the condition of the area is such that activation should be signalled. For example, a door lock is broken, causing a siren to sound.
Alarm control	The control over alarm functions.
Alarm reporting	A procedure to transmit alarm events or other events to the central station by means of a dialler and a set of rules called a protocol.
Anti-passback	Anti-passback function enables users to transfer from one region to another. Entering a region twice in succession is either not possible, or will result in an event being logged and reported to the operator.
Area	A section of premises that has specific security requirements. The Advisor Advanced system allows any premises to be divided into different areas having different security requirements. Each area has its zones. Each area is identified by a number or a name. For example, area 1, Workshop, etc.
Armed	See Set.
Armed display	Armed display activates on a keypad after particular idle time. In this mode, the information displayed on LCD and LED is very limited for security reasons. A user intervention is necessary for return to a normal display mode.
Arming station (RAS)	See Keypad.
Audio device	Audio devices are used for two-way audio alarm verification.
Autoset	An automatic setting of the premises started by a schedule. See Schedule.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.

Central station	A company that monitors whether an alarm has occurred in a security system. The central station is located away from the premises/area it monitors.
Condition filter	A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.
Control panel	An electronic device that is used to gather all data from zones on the premises. Depending on programming and status of areas, it generates alarm signals. If required, alarms and other events can be reported to the central station.
Cursor	A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.
Detector test	Alarm system function for detectors with a dedicated test input. After the detector test input is activated, the panel checks if proper alarm signal is provided by the detector to the system. This functionality allows testing detectors that are difficult to access.
DGP	Data gathering panel. See Expander.
Dialler	An electronic device that allows the Advisor Advanced system to transmit alarms and other events to a central station. Can also be used to perform up/download.
Disarmed	See Unset.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control of doors. Part of access control features.
Door controller	A door controller expander is an access control panel, which extends the ATS system with advanced access control functions.
Door group	Door groups specify when access to a specific door is granted. Door groups are assigned to users. Each Door group may have a different time period (schedule) when access to the door may be granted.
DTMF	Dual-tone multi-frequency signalling. DTMF allows the central station operator to send specific commands to the control panel using an active audio session.
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 techniques like PIR and RADAR or PIR and Ultrasonic.
Duress	A situation where a user is being forced to breach the system security (for example, forced at gunpoint to open the door). The Advisor Advanced duress facility allows a signal to be activated (for example, notification to a central station) by the user. This is done by entering a duress digit in conjunction with a PIN.
Engineer	Personnel from an installer that is able to install and service the control panel.
Expander	A device that collects data from other security devices within an area, and transfers it to the Advisor Advanced control panel.
Fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
Fob	A personal wireless device, which is used to perform programmed functions, for example, set or unset premises, open doors.

High Security Region (HSR)	High security regions (HSR) require a certain number of high security users (HSU) present in them to allow any normal users inside. If a high security user leaves the region causing too few HSU present in it, an alarm is raised, preceded by prewarning time. The system does not allow the normal user to stay in the HSR without HSU inside, therefore the last high security user will not be permitted to leave the high security area if there are normal users inside.
High Security User (HSU)	See High Security Region.
History	A list of past alarm and access control events stored in memory that can be viewed on an LCD keypad or through PC connections.
Hold-up	A (silent) alarm that is triggered by a hold-up button. Normally it does not trigger any siren, only sends a message to a central station. Sometimes also referred to as Panic button.
Inhibit	See Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault.
Installer	A company that installs and services security equipment.
Intelligent door	There are two types of doors in the ATS system: - Intelligent door: A door controlled by a door controller. This door can be used for advanced access control. - Standard door: A door controlled by the control panel. It only allows basic access control functions.
Inverted walk test	A test based on counting days of inactivity for each zone.
Key switch	A device using a switch to arm or disarm areas. The switch needs a key to switch.
Keypad	A device that is the user control panel for security options for areas or for access points (doors). The keypad can be a console (LCD keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as set/unset, open doors, etc.
LCD	Liquid crystal display. The part of a keypad where messages are displayed.
LED	Light emitting diode. A light indicator on a keypad which conveys a condition. For example, area in alarm, communication fault, etc.
Listen-in	See Two-way audio.
Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault	Describes the condition of a zone. • Normal: The zone is <i>not</i> activated. For example, fire exit door closed. • Active: The zone is activated. For example, fire exit door open. • Tamper: The zone is open or short-circuited. Someone may have tried to tamper the security device. • Inhibited: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system for particular time. However, tampers are still monitored. • Isolated: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system permanently. • Masked: Detector is masked. • Fault: Detector reports an internal fault.

Nuisance alarm	An alarm that is triggered by a security device, without any burglar. It could be caused by open windows, pets or incorrect projection 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.
Output expander	A PCB module that connects to the Advisor Advanced control panel or an expander to provide relay or open collector outputs.
Panic button	See hold-up.
Part set	The condition of part of an area where a change in the status of certain zones (from normal to active) causes an alarm. An area or premise is part set when it is partially unoccupied like the outside of a home is part set but the inside is still unset.
PIN	A 4 to 10 digit number given to, or selected by, a user. It is necessary to enter a PIN on an Advisor keypad as a prerequisite to perform most Advisor Advanced options. In the Advisor Advanced configuration the PIN is associated with a user number, which identifies the PIN holder to the system.
PIR	Passive infrared detector. A security device used to detect intruders in a certain part of an area or premise. The technique used is based on infrared detection.
PIR camera	See Wireless PIR camera.
Poll	An inquiry message continually sent by the Advisor Advanced control panel to expanders and keypads. Polling allows the remote unit to transfer data to the control panel.
RAS	Remote arming station. See Keypad.
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 can for example be a magnetic swipe reader or proximity reader. May be integrated into a keypad.
Region	A region is a defined access control area having doors acting as boundaries. Regions are used by the anti-passback functions to monitor in which regions users are present. Transfers from one region to another may be prohibited by the anti-passback settings.
Remote expander	See Expander.
Remote keypad	See Keypad.
Reporting	See Alarm reporting.
Request to Exit zone	A zone that is programmed to open a door using a button or PIR. Used to allow users to exit without using the door reader. Request to exit is often abbreviated to RTE. Also called egress.
Schedule	A timed set of actions.
Screen saver	See Armed display.
Set	The condition of an area where a change in the status of any zone (from normal to active) causes an alarm. An area or premise is only set when it is unoccupied. Some zones (like vaults) can remain armed continually.

Shunt	A procedure that automatically inhibits a zone from generating an alarm when it is activated. E.g. shunts stop a door generating an alarm when opened for a short time.
Special day	A date when alternative time frames in an active schedule are valid.
Tamper	A situation where a zone, a keypad, control panel, expander or associated wiring are tampered with, or accidentally damaged. The Advisor Advanced tamper facility activates a signal when tamper occurs. Tamper alarms from zones are called zone tampers.
Trigger	Triggers are system variables that can be used in condition filters to control outputs remotely. Each trigger has 7 independent flags that can be set or reset. The flags can be controlled by the various means, for example: schedule, SMS command, key fob, PC software.
Two-way audio	Two-way audio allows the central station operator to listen to the live audio from the protected premises in alarm, and speak back.
Unset	The condition of an area when it is occupied and normal activity does not set off an alarm.
Up/Download	A protocol providing means to view the status of an Advisor Advanced system or change parameters in the system either local or remote.
User	Anybody making use of the Advisor Advanced system. Users are identified to the Advisor Advanced system by a unique number that is associated with the user PIN or card.
User group	User groups define the options and permissions available to users.
Virtual zone	A zone, which state depends on the state of a programmed output rather than on an electrical signal on an input. Virtual zones are used in advanced functionality programming.
Walk test	A test performed by a user or installer. To pass the test, the user or installer has to walk past detectors to activate these. The intention is to test the functionality of the security system.
Wireless expander	An expander that collects data from wireless sensors and fobs, and transfers it to the control panel.
Wireless PIR camera	A wireless PIR detector with built-in digital camera, which can make photos and send them to the control panel when particular zones become active.
Wireless PIR camera expander	A wireless expander that collects data from wireless PIR cameras and transfers it to the control panel.
Zone	An electrical signal from a security device or a group of devices (PIR detector, door contact) to the Advisor Advanced system. Each device is identified by a zone number or a name. For example, zone 14, Fire Exit Door.

