



Axon x700 Control Panel Manager Manual

Copyright	© 2023 Carrier. All rights reserved. Specifications are subject to change without prior notice.
Trademarks and patents	<p>Aritech, Axon x700 name and logo are trademarks of Carrier Fire & Security.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	<p>Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands</p>
Product warnings and disclaimers	<p>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.</p> <p>WARNING! Fire alarm and smoke detection products used with Axon x700 systems are intended solely for convenience and should not be used as life safety products. The combination does not meet requirements set by law for life safety products or for use as fire detection systems. Carrier accepts no liability for any damages caused by incorrect application of the products.</p> <p>For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the QR code.</p>
	
Version	<p>This document applies to the following Axon x700 firmware version: MR 2.0</p> <p></p>
Certification	<p>EN 50131-1:2006+A1:2009+A2:2017+A3:2020; EN 50131-3:2009; EN 50131-6:2017+A1:2021; EN 50131-10:2013 Grade 3, Class II EN 50136-2:2013 Pass through</p> <ul style="list-style-type: none"> - SP4: IP with Ultrasync - SP5: IP with OH receiver, GPRS with OH or Ultrasync receiver - DP3: IP and GPRS with Ultrasync receiver - DP4: IP and GPRS with OH receiver <p>Tested and certified by KIWA Nederland B.V.</p> <p>This product has not been designed to comply with EN 50134 and EN 54 norms.</p>
European Union directives	<p>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.</p>
REACH	<p>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.</p> <p>Safe use information can be found at https://firesecurityproducts.com/en/content/intrusion-intro</p>



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 iv

Typographical conventions iv

Important note iv

Keypads and readers 1

The LCD display 4

The LEDs 5

Armed display 6

User identification 7

User groups 7

Using a PIN and/or a badge 7

Duress 9

Door access 10

Set and unset the system 11

When to set 11

When to part set 11

When to unset 11

The time limit to leave the premises once set 11

The time limit when unset 12

Unset when there is an alarm 12

When you cannot set or unset 12

Set areas via LCD keypad 14

Part set areas via LCD keypad 15

Unset areas via LCD keypad 15

Set areas via keypad without LCD 15

Unset areas via keypad without LCD 16

Autoset 16

Areas displayed during set and unset 17

What to do when there is an alarm 19

What happens when there is an alarm 19

Viewing an alarm 20

Resetting an alarm 20

Confirming an alarm 20

Acknowledging the alarm 20

Performing a walk test 20

Problems that can occur 21

Further information about alarms 21

Mobile Application 23

The Axon x700 menu 24

How the menu option sections are organised in this manual 24

Option availability 25

Accessing menu 25

Zone options 26

Inhibiting / uninhibiting zones 26

Shunting zones 27

Cameras 27

Isolating / deisolating 29

Log 30

Panel status 31

Settings 32

Door control 35

Users 36

User data lock 36

User settings 37

Service 44

Calendar 51

Viewing calendar 52

Schedules 54

Schedule settings 54

User programmable functions 60

Fobs programming 63

Fob activation 65

Common key sequences 66

Common key sequences for LCD keypad 66

Common key sequences for keypad without LCD 67

Function keys 68

Programming records	69
Users	70
User groups	72
Condition filters	73
Schedule	75
Special days	76
SMS commands	77
Appendix A. SMS control	79
SMS control requirements	79
Command syntax	79
User authentication	79
SMS command list	80
Glossary	87
Index	93
User menu map	96

Important information

This manual explains how to use the Axon x700 system if you are responsible for managing the system. There is also a shorter user guide available that explains everyday usage. To use this documentation effectively, you should have a basic knowledge of alarm systems.

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

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Keys	Capitalized, for example “press Enter”.
Note	Notes alert you to information that can save you time and effort.
Caution	Cautions identify conditions or practices that may result in damage to the equipment or other property.
<input type="checkbox"/>	Check boxes let you indicate whether a particular option is available or not. The installer can provide details on the available options.

Important note

This manual provides information for all Axon x700 control panels in all variations. “Axon x700 control panel” refers to any variant of the Axon x700 control panels, unless specifically stated otherwise.

List of panel variants

- ATS1700, ATS3700: Medium metal enclosure MM+

Note: Not all variants may be available.

Keypads and readers

Figure 1: ATS111xA keypad

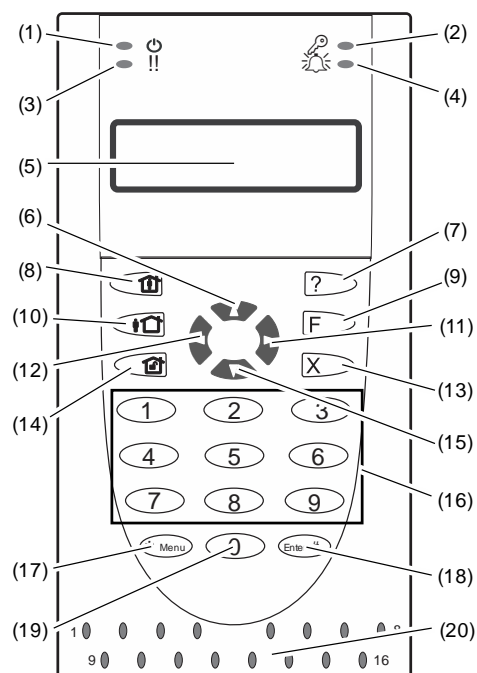


Figure 2: ATS1125 keypad

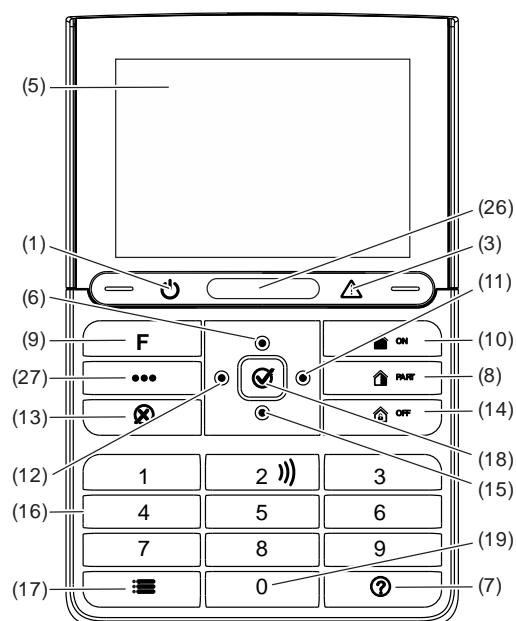
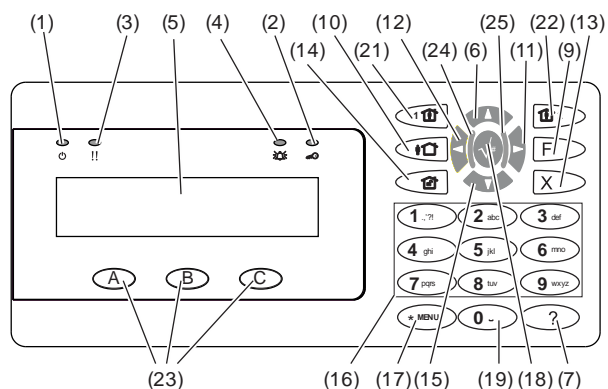


Figure 3: ATS113x keypad



(1)	AC mains LED	Green on: AC mains supply on
(2)	Access LED	Blue flashes: card read
(3)	Fault LED	Yellow on: system fault active Yellow flashing: general alert (EN 50131)
(4)	Alarm LED	Red on: alarm condition active
(5)	LCD display	Displays messages
(6)	▲ / Up	Scroll up in the menus Change value Delete
(7)	? / Help	Show help Scroll text (ATS113x only)

(8)	Partset	Part set an area Scroll text (ATS111x only)
(9)	F / Function	Show active zones / faults Function key modifier Scroll text (ATS113x only)
(10)	On	Full set an area
(11)	► / Right	Enter the selected menu Move cursor right
(12)	◄ / Left	Return to the previous menu Move cursor left
(13)	X / Clear	Exit the current user function Volume control modifier
(14)	Off	Unset an area
(15)	▼ / Down	Scroll down in the menus Change value Backspace
(16)	Alphanumeric keys	Keys 1 to 9, alphanumerical data
(17)	Menu, *	Request entry to the menus
(18)	Enter, #	Complete the step Enter the selected menu entry
(19)	0	Key 0 Toggle selection
(20)	Area LEDs 1 to 16	On: area set. See also “Access control indication note” on page 4. Off: area unset. Flashing: area alarm condition.
(21)	Partset 1	Part set 1 of areas
(22)	Partset 2	Part set 2 of areas
(23)	A, B, C	Programmable function keys
(24)	LED1	Programmable LED 1
(25)	LED2	Programmable LED 2
(26)	Status LED bar	Red On: Areas set Red flashing: Alarm condition active Orange On: Part set Orange flashing: System fault active / General alert (EN 50131) Green On: System is ready to set Green flashing: Entry / exit time active Blue flash: Valid card presented / Access granted Off: Not ready to set / Armed display active
(27)	Action key	For future use

Figure 4: ATS118x readers

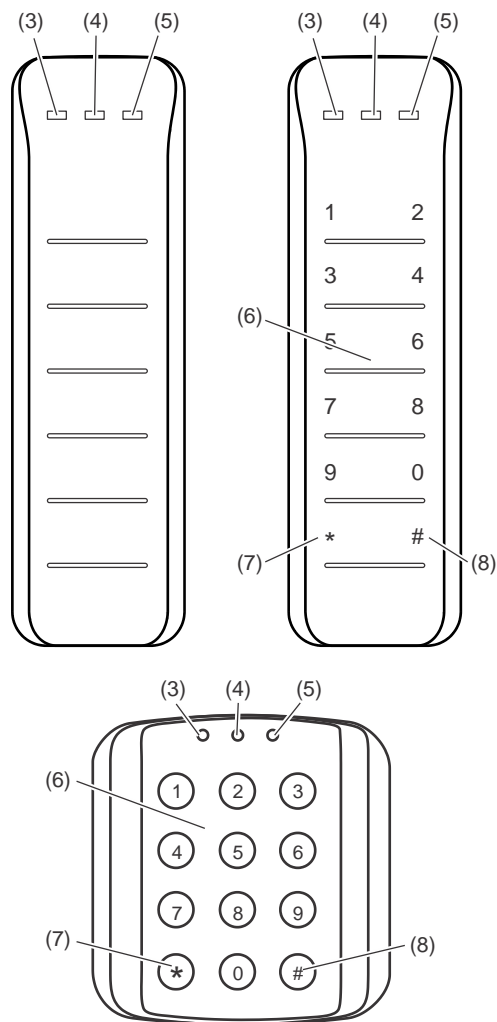


Figure 5: ATS1190/ATS1192 readers

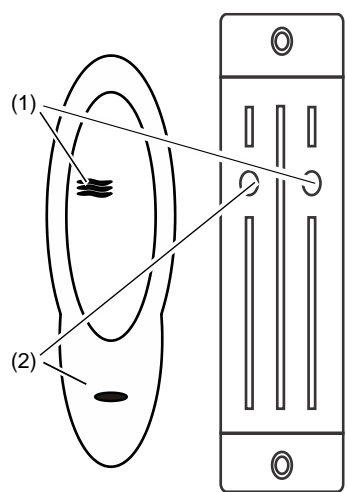


Figure 6: ATS1197 reader with keypad

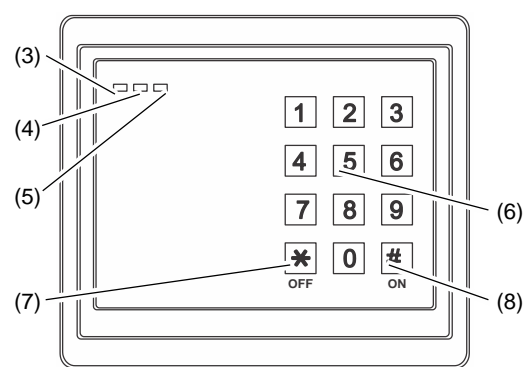
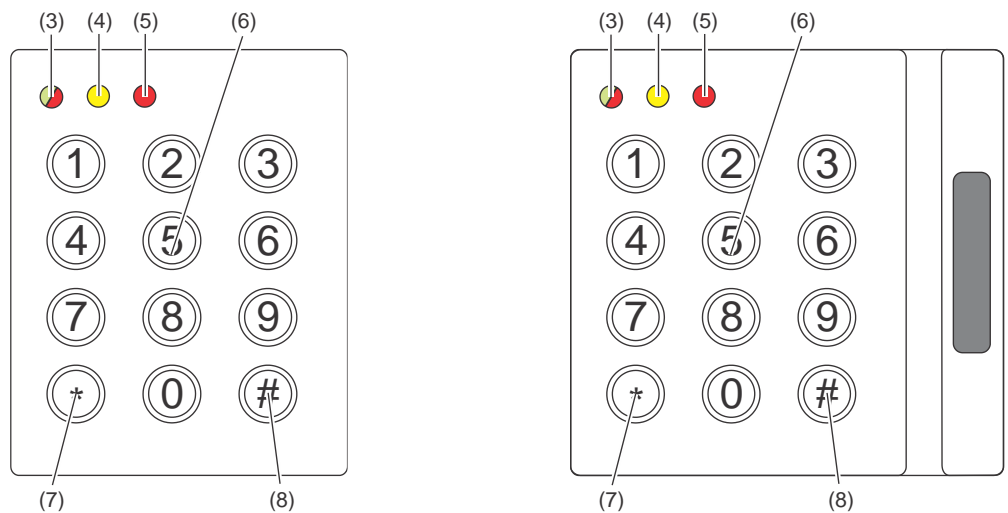


Figure 7: ATS1151/ATS1156 readers



(1)	Blue LED	Access granted
(2)	Red LED	On: area set Flashing: general alert (EN 50131)
(3)	Dual LED	Green on: AC mains supply on, all areas unset Green flashing: AC mains supply off, or unlocked while unset. Red on: all areas set. See also "Access control indication note" below. Red flashing: unlocked while set.
(4)	Yellow LED	On: all zones are in normal state / system fault Note: This functionality depends on system settings. Flashing: general alert (EN 50131) ATS125x: always on CDC4: system fault
(5)	Red LED	Flashing: alarm
(6)	Numeric keys	Keys 0 to 9, numerical data
(7)	Off	Unset an area
(8)	On	Full set an area

Access control indication note

Access control keypads and readers, which are connected to door controllers instead of the control panel, indicate areas in a different way:

- Dual LED is lit red when *any* associated area is set.
- Area 1 LED is on when *any* associated area is set. Area LEDs 2 to 16 are not used.

The LCD display

Messages are displayed on the liquid crystal display (LCD) on the keypad. They guide you through the menu options and possible problems of the Axon x700 system. The display is also used to show information you have entered on the keypad.

The first line of the display shows system information and scrolls if there are more characters than can be displayed, depending on the arming station type. The second line or last line of the display shows instructions and characters you enter on the keypad.

```
CARRIER F&S
TUE 29 Apr 08:55
```

Your system might display a custom message instead of the one shown above if it has been programmed to do so, for example:

```
Main warehouse
TUE 29 Apr 08:55
```

The LEDs

The LEDs on the Axon x700 keypad and the information shown on the display allow you to determine the system status at a glance. Not all LEDs are available on all arming stations.

Area LEDs

The area LEDs, one for each of the possible security areas, indicate the status of the particular area. The status of the area LED can be:

- On: The area is unoccupied and set.
- Off: The area is occupied, and the security system has been set to allow normal access.
- Blinking: An alarm has occurred in the area while the area was unset (LED flashes slow), or an alarm has occurred in the area while the area was set (LED flashes fast).

Programmable LEDs

The programmable LEDs 1 and 2 can be configured in two ways:

- ☐ Different areas are indicated.

An area can be assigned to LED 1 or LED 2. A LED is green when all assigned areas are ready to set. The status of a LED can be:

- Green: All areas assigned are ready to set.
- Red: Any area is set or part set.
- Blinking green: Entry or exit time is started.
- Blinking red: An alarm has occurred in an area while unset (a LED flashes slow), or an alarm has occurred in an area while set (a LED flashes fast).

- ☐ One area is indicated.

Both LEDs show a single area state. The status of the LEDs can be:

- Both green: The area is ready to set.
- Both red: The area is set or part set.
- LED 1 red, LED 2 off: The area is in part set 1.
- LED 1 off, LED 2 red: The area is in part set 2.

System alarm LEDs (available on some arming stations only)

The system alarm LEDs indicate a breach of security. One of the system alarm LEDs flashes when an alarm has occurred (the area's set LED also flashes to indicate the location of the alarm). Alarm LEDs operate as follows:

- Unset alarm: Flashes when an alarm has occurred in an occupied area, and the area was unset.
- 24-hour alarm: Flashes when an alarm has occurred in an area where a zone has been programmed for 24-hour alarm.

- Set alarm: Flashes when an alarm has occurred in a set area.
- Tamper alarm: Flashes when an alarm has occurred due to tamper.

System faults (available on some arming stations only)

System faults are displayed on the arming station keypads if the arming station has an LCD fitted and/or has “System faults” LEDs. Fault LEDs operate as follows:

- Comms fail: When there is a failure in the communications between the Axon x700 control panel and a central station.
- Keypad fail: When a keypad is offline.
- Expander fail: When a remote expander is offline.
- Battery fail: When the auxiliary battery power is found to be low.
- Trouble: When there is a trouble in the system (keypad fail, low battery, etc.)

General alert indicator (EN 50131)

To comply with the EN 50131, this indicator is enabled if the system is unset and the armed display is active. The alert indicator flashes in case of any fault, alarm, or pending alarm.

Armed display

Some installations require the use of an armed display.

The armed display prevents unauthorized users from viewing details about the security system status.

The armed display is deactivated when performing any action that requires an authorization with a valid user code or a valid badge.

Depending on settings, the armed display can function in different ways:

- ☐ When the armed display is active, only a general alert message can be displayed. Area LEDs are off.
- ☐ When the armed display is active, LEDs are off. The armed display can also be deactivated on pressing Clear key.

User identification

All users of the Axon x700 system need a PIN and/or a card that is set up in a user account. A PIN is unique code and has between 4 and 10 digits. It is a combination of numbers between 0 and 9.

PINs and/or card details are part of the setup of a user account. The user account is set up to allow users to perform specific tasks, such as set or unset the system. These task or options are defined in user groups.

Predefined users

There are two predefined users in the system:

- Installer is used to enter the Axon x700 system configuration. It has user group “Installer group” assigned.
- Supervisor is used to grant access for a service engineer. It has user group “Supervisor group” assigned. The default PIN is 1122.

Note: If the PIN length is configured for more than four digits, zeroes are added to the default PIN values. For example, if the system is configured for a six-digit PIN, the supervisor PIN is 112200.

User groups

A user group allows users to control the Axon x700 system alarm options (also called alarm control). This provides flexibility when determining a user’s access to, and control of, the system.

A user can have more than one user group assigned. In this case, if any of those groups grants permission to a particular option, the user has this permission.

For example: A user has two user groups assigned: “R&D” and “Managers”. If “Managers” user group allows inhibiting but the “R&D” group does not, the user is able to inhibit a zone.

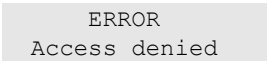
Note: The system always includes an installer group. This group can be assigned to only one user, the default installer user.

Using a PIN and/or a badge

When you enter your PIN on the Axon x700 keypad, each key pressed is indicated by * on the display.

If you enter the wrong PIN, or present a card with a PIN that is not valid at the particular keypad, the keypad beeps quickly seven times. Correct a wrong code by pressing Clear and enter the correct code. If you access a menu and do not press any key for three minutes, the system time out function automatically exits from the menu. It is good practice to exit the menu using the Clear button rather than using this time out facility. If someone else uses the menu before it times out, the option used is logged against your user account.

Users can only access the menu options enabled for the user groups assigned to the user account. When they try to access an option that they are not authorised to access, they get the message:

A light gray rectangular box containing the text "ERROR" and "Access denied".

ERROR
Access denied

See also: “Users” on page 36.

Duress

The duress function activates a silent signal to alert security personnel. If you are asked, under threat, to breach your system security (for example, forced to unset the system), this function lets you do so while at the same time activating the system duress facility. However, your Axon x700 system must be programmed to use this function.

You use a duress digit in conjunction with your PIN. There are three methods for entering a duress code.

Table 2: Duress methods

Option	Description	Example	Available
Increment last digit	The duress code is your PIN with the last digit of your PIN incremented by one (1)	Example: PIN = 1234, duress code = 1235. If the last digit of your PIN is 9, then the duress digit becomes 0. Example: PIN = 2349, duress code = 2340.	<input type="checkbox"/>
Add last digit	The duress code is a code with an additional digit "5" at the end	Example: PIN = 1234, duress code = 12345	<input type="checkbox"/>
Add first digit	The duress code is a code with an additional digit "5" on the beginning	Example: PIN = 1234, duress code = 51234	<input type="checkbox"/>

Caution: Systems with door controllers only allow the option Increment last digit. If a system with door controllers has duress functionality enabled, it is also required for all user groups in this system to have the Duress code option allowed. See *Axon x700 Control Panel Installation and Programming Manual*, "User groups", for more information.

To activate duress, provide an allowed key sequence indicated in "Common key sequences" on page 66.

To reset the duress alarm, enter a valid PIN or card with PIN.

Notes

- If duress was activated under conditions that are no longer valid (a false alarm), and it has been reset, you must contact your central station company to ensure that they take no further action.
- Using your PIN with the duress digit still activates the options configured for your user group.

Door access

If programmed, it is possible to get access through a particular door using the keypad or the reader assigned to the door.

Provide an allowed key sequence indicated in “Common key sequences” on page 66.

Set and unset the system

When to set

The security system should be set if you are the last person to leave the premises (or your area), for example at the end of the day. When set, any security device detecting intruders activates an alarm.

When to part set

In case you are still on the premises (or in your area) it is possible to perform a part set of it. For example, you can secure your garage using part set while you remain in the house. Notification to the central station may happen depending on system configuration settings. Contact your installer for more information.

You can use part set for perimeter protection, for example when you secure your house at night but stay inside. You can move inside of the house, but if someone tries to enter without unset, this triggers an alarm. Notification to the central station may be sent depending on system configuration settings. Your installer can provide details.

Depending on the keypad model, you may be prompted to choose an appropriate set to part set:

```
1>Part set 1
2 Part set 2
```

When to unset

If the area you want to enter is set, you must first unset the alarm system before you can enter as otherwise you will trigger an alarm. Depending on system configuration you may be able to tell when an area is set because the LED on the keypad is lit red. If the armed display is enabled, only the Mains LED will be lit. Once a valid code is entered, the system status will be shown.

In most cases an entry beeper sounds indicating that the system needs to be unset or an alarm will occur.

The time limit to leave the premises once set

Once you have set the system, you must leave the premises (or area) within a pre-set time (“exit time”) as otherwise you will set off the alarm. The manager of the system needs to inform everyone about this time limit.

Normally, you will hear a beeper during the time allowed to leave the building.

Make sure you know which route to take when leaving the premises.

The time limit when unset

Once the system is set, you have to unset the area within a pre-set time (“entry time”) as otherwise you will set off the alarm. The manager of the system needs to inform everyone about this time limit.

You will normally hear a beeper during the time allowed to unset.

Note: There can be programmed an extended entry time. After the main entry time passes, the entry timer is extended for a programmed time period and a local alarm activates. See “Local alarm” on page 19 for more details.

Unset when there is an alarm

If there is an alarm condition while you are unsetting the system, the alarm is reset. You must then find out what caused the alarm and make sure it does not happen again. See “What to do when there is an alarm” on page 19.

Unsetting while the system is in alarm is described in “Resetting an alarm” on page 20.

Use menu “3 Display logs” on page 30” to list recent alarms.

When you cannot set or unset

WARNING
No access

You might not be authorised to set/unset specific areas on the premises because:

- Your keypad has been programmed to set/unset specific areas of the premises only. Make sure you know which keypad to use if there is more than one present of the premises.
- Your PIN and/or card have been programmed to set/unset only specific areas of the premises. Make sure you know which areas you are authorised to set/unset.
- Your alarm system might have more than one control panel. If so, each will have been programmed to set/unset only specific areas of the premises. Make sure you use the correct keypad for the areas you want to set/unset.

Active zones

You cannot set an area if it has a zone that is open, such as the magnetic contacts of a door or window. So, before setting, make sure that all doors and windows are properly closed.

If a zone is open when you try to set, you get the message:

CHECK SYSTEM
Devices open

All the active zones are listed:

```
1 Zone active
   Zone 1
```

Setting the areas is now disallowed. If the indicated zones have to stay open (for example, you need to leave a window open), the problem may be resolved using one of the following methods:

- Cancel the setting using the Clear button. Log on to the menu and inhibit the zone if it should remain active. See “Inhibiting / uninhibiting zones” on page 26 for more information. After active zone is inhibited, attempt the setting procedure again.
- Inhibit the zone from the set menu. This is only allowed if you have the proper options available. It only works on zones that are allowed to inhibit. Press Off to inhibit.

```
>1 Zone 1
-----
```

```
Inhibited
Alarms
```

If any more zones are active, this step may be repeated.

- Use forced set.

You can activate forced set only if you have the proper options available. The system configuration also needs to include this option. Forced set is an automatic inhibiting of open zones and some faults. The conditions for inhibiting and uninhibiting items are configured in the system. The manager must inform users when they are allowed to use forced set.

To activate forced set, press On. All open zones and faults are inhibited, and the appropriate warning is displayed. See “Inhibited zones and faults” below.

Active faults

```
CHECK SYSTEM
Faults
```

You cannot set an area if certain system faults are present. The list of faults preventing setting the system is defined by the installer. It is possible to temporarily disable these warnings in the same way as for active zones (see above). The manager must inform users whether or not they are authorized to disable faults in this way.

Inhibited zones and faults

If there are inhibited faults or zones, it is necessary to confirm information about it.

```
WARNING
Inhibited
```

All the inhibited zones and faults are listed:

Inhibited
Zone 1

Battery fault
Inhibited

- Press Enter to confirm the warning. After this the setting procedure continues.
— or —
- Cancel the setting using the Clear button. After you have determined which zones are active, check these and resolve the problem (for example, close the door). Attempt the setting procedure again.

Note: If you do not cancel the setting, after fixing the problem the setting procedure is continued automatically, and you can raise an alarm when you proceed to the exit after closing the zone.

The manager of the system must inform users which keypads they can use, and which areas they can set and unset.

Set areas via LCD keypad

To set areas via LCD keypad:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 66.
2. If prompted, choose areas. See “Areas displayed during set and unset” on page 17 for more information.

If there are inhibited or isolated zones in selected areas, they are listed on the display.

3. If you want to continue setting, press Enter. Otherwise, press Clear to cancel the set process.

See “Inhibiting / uninhibiting zones” on page 26 and “Isolating / deisolating” on page 29 for more information.

The exit tone sounds. This may be a continuous tone or an intermittent tone.

4. Exit the premises using the designated entry/exit route.

The exit tone switches off.

When an area is set, its LED lights up red.

If programmed, after a delay the armed display is engaged, and LEDs are extinguished.

Part set areas via LCD keypad

To part set areas via LCD keypad:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 66.
2. If prompted, choose the appropriate part set.
3. If prompted, choose areas. See “Areas displayed during set and unset” on page 17 for more information.

If there are inhibited or isolated zones in selected areas, they are listed on the display.

4. If you want to continue setting, press Enter. Otherwise, press Clear to cancel the set process.

See “Inhibiting / uninhibiting zones” on page 26 and “Isolating / deisolating” on page 29 for more information.

If programmed, the exit tone sounds. This may be a continuous tone or an intermittent tone.

The exit tone switches off.

When an area is partially set, its LED lights up red.

If programmed, after a delay the armed display is engaged, and LEDs are extinguished.

Unset areas via LCD keypad

To unset areas via LCD keypad:

1. Enter the premises using the designated entry/exit route.

An intermittent entry tone starts, and the following prompt is displayed:

```
Enter card/code  
to unset
```

2. Provide an allowed key sequence indicated in “Common key sequences” on page 66.
3. If prompted, choose areas. See “Areas displayed during set and unset” on page 17 for more information.

The entry buzzer stops, and the areas are unset.

LEDs are extinguished, and the time and date is displayed.

Set areas via keypad without LCD

To set areas via keypad without LCD:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 66.

If the operation is not possible, the keypad beeps seven times. See “When you cannot set or unset” on page 12 for more information.

The exit tone sounds. This may be a continuous tone or an intermittent tone.

2. Exit the premises using the designated entry/exit route.

The exit tone switches off.

When an area is set, its LED lights up red.

If programmed, after a delay the armed display is engaged, and LEDs are extinguished.

Unset areas via keypad without LCD

To unset areas via keypad without LCD:

1. Enter the premises using the designated entry/exit route.

An intermittent entry tone starts.

2. Provide an allowed key sequence indicated in “Common key sequences” on page 66.

The entry buzzer stops, and the areas are unset.

LEDs are extinguished.

Autoset

The system can be configured so that the premises are set automatically at a particular time and a day of the week.

Before the autoset begins, the warning time starts. The system may warn the users by a sound. The following message is displayed:

```
INFO
Auto setting
```

Depending on system settings and user privileges, you can postpone the autoset during the warning time. To do this, press Clear and authorize.

If you are authorized to postpone or cancel the autoset, you will be asked to choose the appropriate autoset delay.

```
Retry time
>15 minutes<
```

Choose one of the following:

- Off: Cancel the autoset.
- 15 min, 30 min, 1 h, 2 h, 3 h, 4 h: Set an appropriate time period to delay the autoset.

Areas displayed during set and unset

If your system has not been programmed to display the areas assigned to your PIN on the LCD, those areas are automatically set/unset (provided all zones were normal).

The area LEDs illuminate when the set or unset procedure is successful.

If you are authorized to operate both on areas and area groups, you will be prompted to choose between areas and area groups.

```
Select mode
>Areas<
```

Choose between areas and area groups, and then press Enter.

Area list

If the areas assigned to your PIN are displayed, any of those areas that are set (or unset) will be listed. Depending on the keypad model and its settings, areas are shown as a list or a symbolic line. For example:

```
0> All
1 * Office
```

— or —

```
1 2 3 4 5 6 7 8
█ [ ] √ x ? + +
```

Each area in the list has an indicator that describes its status. The following area statuses are available.

Table 3: Area statuses and indicators for different keypads

Area status	List	Symbolic line
Ready to set	Space	√
Not ready to set	?	?
Exit time	x	x
Alarm	!	🔔
Set	*	█
Part set 1	—	[
Part set 2	=]
Selected	+	+ (blinking)

Depending on the type of the list, you now have the following options.

Selecting areas in the list

- To select or deselect an area, enter the area number. Note that you can only select areas that are currently shown on the display.
- To continue with selected, or with all areas if none selected, press Enter, or Right, or 0.

- To cancel, press Clear.

Selecting areas in the symbolic line

All areas are selected by default.

- To select or unselect an area, enter the area number. Note that you can only select areas that are currently shown on the display.
- To set or unset selected areas, press Enter or 0.
- To cancel, press Clear.

Area group list

If you are authorized to set or unset area groups, these will be displayed instead of single areas.

Set or unset area groups the same way as described for areas above.

What to do when there is an alarm

When there is an alarm, the LED of the area in alarm and the alarm LED flashes on the keypad. If the armed display is active, the LEDs start flashing when a user code has been entered. The time and date message is no longer displayed.

An area can have several zones associated with it. When there is an alarm, it is important that you know exactly which zone is causing the alarm so that you can quickly deal with it.

What happens when there is an alarm

There are different types of alarm, and they occur under different situations.

Alarm

An alarm is raised if:

- The area is set and one of its zones has been activated. For example, a door lock has been forced open causing a siren to sound.
- The area is unset, and a 24-Hour zone was activated. Examples: a hold-up button is activated, or a tamper switch is open.

The exact type of alarm signal depends on how the system has been programmed (strobes, sirens etc.) The LED on the keypad flashes quickly. The area LED on the panel identifies the location of the alarm.

When programmed, the alarm is sent to the central station.

Local alarm

The alarm is only heard inside the premises and is dealt with locally. An internal siren activates. The area LED on keypad flashes (depending on how it has been programmed). The keypad beeps until someone acknowledges the alarm at the keypad.

It occurs, for example, when a zone programmed as fire door has been activated.

The central station does not need to be contacted.

System alarm

This alarm can occur at any time. The exact type of alarm signal depends on how the system has been programmed (strobes, sirens etc.) It occurs when the security equipment (such as the panel) has been tampered with, or detects a fault.

You can only reset a system alarm if your PIN has been authorised to do so, and only after the fault is restored.

When programmed, the central station is contacted automatically by the system.

Viewing an alarm

After disarming all the alarms are listed on the screen.

```
Alarm
Pending >0<
```

```
Zone 1
Pending >0<
```

The first screen shows the type of the alarm. The second shows the source of the alarm. The second line shows if there are more alarms for this source.

Resetting an alarm

To switch off sirens or bells, you must unset the appropriate area.

If an alarm is active, the reset procedure is the same as for a standard unset. After the system is unset, you are prompted to acknowledge the alarms. This is possible only if the problem has been resolved.

Confirming an alarm

If you are permitted, you can confirm an alarm to switch off sirens or bells without area unset.

If there is an alarm in an area that is set, repeat the set procedure using the Set button to confirm alarms. After a proper authorization you will be prompted to acknowledge alarms. The area remains in the set state, and alarms or faults are confirmed and silenced.

Acknowledging the alarm

If you are permitted, you can acknowledge the alarm by pressing Off.

The alarm cannot be acknowledged if its cause is still active, for example, if there is a zone tamper. The fault should be fixed prior to acknowledging the alarm caused by this fault.

All alarms must be acknowledged. A counter during the alarm acknowledgement process indicates the number of outstanding alarms to still be acknowledged. If you don't acknowledge the alarms after the unset, you are prompted to do so before next set or after the next unset, until all alarms are acknowledged.

Performing a walk test

If the system is programmed for user walk tests, sometimes while setting the area, the system may ask you to perform the area walk test. To pass the walk test, you need to go to all the zones displayed. The system lists all zones still to be tested.

The necessity of the walk test depends on:

- System settings
- Activity of the programmed zones in last 4 hours

You can perform the walk test manually using “8.2.1 Walk test” menu (described on page 44).

Problems that can occur

There is a faulty zone

A faulty zone continues to cause an alarm until it is isolated from the system (see “Isolating / deisolating” on page 29 for more information).

As soon as the faulty zone is isolated or the problem has been resolved, the alarm is reset automatically.

Your PIN does not work when you try to acknowledge an alarm

There are two possible reasons why your PIN may not work when you attempt to acknowledge an alarm:

- You can only acknowledge an alarm for an area if your PIN is assigned to it. If it is not and you try to acknowledge an alarm, you might set/unset the area instead.
- You cannot acknowledge a system alarm unless your PIN is authorised to do so.

The keypad does not respond to key presses

The keypad may not respond to key presses even when there is no fault in the system. The keypad is locked after a wrong PIN is entered three or more times.

When you press a key on a locked keypad, it beeps seven times.

After 2 minutes the keypad becomes available again.

Further information about alarms

If the alarm conditions are no longer valid, and the alarm has been reset, you must contact your central station company to ensure that they take no further action.

If you are unable to reset an alarm because of a faulty zone, refer to the section “Isolating / deisolating” on page 29.

You can only reset an alarm for an area that is assigned to your PIN. If you are unable to reset the alarm, ensure that the flashing area LED is for an area you can disarm with your PIN. If not, your attempt to reset the alarm results in arming/disarming your system.

Engineer reset

The system can be programmed in such a way that certain alarms (like tamper alarms) require a specific action from your installer. Some events require an engineer reset.

The engineer reset procedure depends on whether the engineer reset by user is available or not.

If the engineer reset can be done by user, the display may show the following.

```
Eng. reset  
Code:23353
```

— or —

```
Call +485555555  
Code:23353
```

To do an engineer reset:

1. Note the engineer code that is displayed in the engineer reset request.
2. Contact your installer and give him the engineer code.

The installer will give you the resulting code required for the reset.

3. Log in the system.

The following prompt appears:

```
Eng reset code  
> <
```

4. Enter the code given by the installer to perform the engineer reset.

If engineer reset cannot be done by user, there is the following prompt.

```
WARNING  
Eng reset req
```

— or —

```
WARNING  
Call +485555555
```

Contact your installer. The installer should do an engineer reset locally.

Mobile Application

Advisor Advanced Pro mobile application allows users to monitor and control your Axon x700 security system via TCP/IP using a smartphone running Android or iOS operating system.

Note: Your control panel must be connected to the Ethernet or to the Internet (for example, via GPRS connection). The following settings must be also applied if the panel is connected to a home router:

- Configure port forwarding in your home router
- Instead of the panel, connect to the router IP address or DNS name

Note: Advisor Advanced Pro cannot be used by panel installer. Therefore, installer PIN will not grant access to the application user.

Connecting to the panel via UltraSync cloud

To connect to the panel from the mobile application via UltraSync cloud, do the following:

1. Run Advisor Advanced Pro mobile application.
2. Set UltraSync as the communication channel.
3. Enter your panel serial number in the SID number field.
4. Enter your UltraSync password.
5. Enter your panel name for identification in the mobile application.
6. Tap Next.

Enter your panel remote login and password, and select the login prompt mode.

Note: After 10 unauthorized access attempts via Downloader or mobile application the remote login is locked for 90 seconds.

Tap Log in, or Setup next panel if required.

If the application is run for the first time, the end-user license agreement (EULA) is prompted. Read and accept the agreement to start using the application and connect to the panel.

For more information see *Advisor Advanced Pro Mobile Application User Manual* and *Advisor Advanced Pro Mobile Application Online Help*.

User management

Panel user management is available using the Advisor Advanced Pro application only for the Supervisor user configured in the panel at position 2.

The Axon x700 menu

The Axon x700 system uses a menu structure to present the various options and commands available. The availability of these depends on system configuration and on the permissions in your user group. You may not always see all the items described in this manual.

If you access the menu and do not press any key for three minutes, the system time out function automatically exits from the menu. It is good practice to make sure you exit the menu using the Clear button rather than this time out facility. If someone else uses the menu before it times out, the options used will be logged against your user account.

If you attempt to select an option that is not authorised in your user account, the display shows the message:

ERROR
Access denied

Although you might be authorised to access a menu option, you might not be allowed to access all the information it provides. You are only allowed to access information for the areas assigned to your user account.

Area selection

Depending on the system settings and your user group, you may be prompted to choose areas that you are going to operate on.

Select areas
to operate

The area selection list is the same as the set/unset area list. See “Areas displayed during set and unset” on page 17 for details.

The selected areas will be excluded from normal operation. Other users will not be able to control these selected areas until you exit the menu.

Note: Door access functionality is not affected by the programming mode.

How the menu option sections are organised in this manual

Menu options are numbered in the Axon x700 system. This numbering system is also used in this manual, so menu option 1 “Inhibit zones” is topic “1 Inhibit zones”.

The menu number also refers to the key sequence that can be pressed to enter the menu. For example, if you want to enter menu “7.2 Walk test”, you can press 7, then 2 after entering the menu system.

Option availability

Not all options described below may be available. Option availability depends on the following:

- Firmware version
- Panel model
- Installed expansions (for example, wireless expander or GSM communication module)

Accessing menu

Before commencing, ensure that the welcome or status screen is shown on the display.

CARRIER F&S
TUE 29 Apr 08:55

— or —

1 2 3 4 5 6 7 8
■ [] √ x ? + +

Provide an allowed key sequence indicated in “Common key sequences” on page 66.

From the display you can now:

Option	Action	Result
Change the selection	Press Up or Down	Select previous or next menu option
Enter the menu option	Enter menu option number — or — Press Enter or Right to enter the selected one	Jump to a specific menu option
Show help	Press Help	Display a description of the selected menu entry (if available)
Exit a menu option	Press Left or Clear	Exit the menu option

Zone options

1 Zone options

```
1>Inhibit zones
2 Camera menu
```

The menu allows inhibiting zones and performing user operations on cameras.

Inhibiting / uninhibiting zones

1.1 Inhibit zones

The Inhibit function is used to inhibit zones and exclude them from the security system until the next unset.

There may be occasions when you want to inhibit a zone. For example, if you want to leave a window open when the system is set. By inhibiting the zone associated with the window, when you set the system, you will not activate an alarm.

Note: It is also possible to inhibit active zones while setting an area. See “Active zones” on page 12 for more information.

Enter the “Inhibit zones” menu to inhibit or uninhibit zones. What happens next depends on whether or not there are active zones:

All zones are normal

You can inhibit normal zones if you know their zone number.

```
1>Zone 1
Uninhibited
```

1. Press Up or Down to scroll through the zones.
2. Press the zone number, or use Enter to select a zone.
3. Change the zone state using Up and Down.
4. Confirm the changes by pressing Enter.
5. Press Clear twice to exit programming.

Active zones

When one or more zones are active, the system displays:

```
1>Zone 1
Active
```

The active zones are listed one by one.

1. Press the Up and Down buttons to scroll through the zones.
2. To inhibit the selected zone, press Enter. The confirmation is displayed:

```
1>Zone 1
Inhibited
```

3. If you do not have rights to inhibit the selected zone, the following warning is displayed:

```
WARNING
No access
```

4. Press Clear to exit programming.

Shunting zones

1.2 Shunt zones

The shunt function is used to inhibit zones for a certain time period.

Enter the “Shunt zones” menu to switch zone shunts on or off.

```
1>Zone 1
    Shunt off
```

1. Press Up or Down to scroll through the zones.
2. Press the zone number, or use Enter to select a zone.
3. Change the zone state using Up and Down.
4. Confirm the changes by pressing Enter.
5. Press Clear twice to exit programming.

Cameras

Note: These menus are available only if the wireless PIR camera expander is installed and configured.

1.3 Camera menu

```
17>Camera 17
18 Camera 18
```

Use camera menu to take pictures manually.

Select an appropriate camera.

1.3.n Select camera

```
4>Isolate
    No
```

Select an appropriate camera to configure.

1.3.n.4 Isolate

```
4 Isolate
    >No<
```

When the camera is isolated, it does not take pictures. Also, pictures cannot be sent to the panel.

1.3.n.5 Max pics 24h

```
5 Max pics 24h
  >Infinity<
```

Maximum picture number defines how many pictures can be taken by the camera for 24 hours period of set or unset state.

The counter is reset when the area changes its set state.

The allowed range is 1 to 999, or 0 (infinity), which means unlimited number of pictures.

If the limit is reached, the camera switches off and an appropriate event is recorded in the log.

1.3.n.6 Remote pics

```
6 Remote pics
  >Yes<
```

If remote picture triggering is enabled, you can take a picture remotely, using configuration software.

1.3.n.7 Test pic to CS

```
1>CS 1
-----
```

The command allows you to take picture and send it to a selected central station.

Choose a central station to send the picture.

```
Calling CS 1...
Transmitting
```

The current picture transmission status is shown in the bottom line of the screen.

1.4 Delete pics

```
1>Expander 1
-----
```

Delete all pictures from the wireless PIR camera expander.

Select expander, then select OK and press Enter to remove all pictures from the selected expander.

Isolating / deisolating

2 Isolate

The isolate function is used to isolate zones or devices, and exclude them from the security system.

Note: Isolated devices do not raise tampers or faults, but still remain operational.

You do this, for example, when a zone is faulty or broken. By isolating it, you stop it from causing an alarm until the problem has been resolved.

This differs from inhibiting a zone, because an isolated zone is not automatically deisolated when the system is unset.

2.1 Isolate zones

Enter the “Isolate zones” menu to isolate or deisolate zones. What happens next depends on whether or not there are active faults:

All zones are normal

You can isolate normal zones if you know their zone number.

```
1>Zone 1
    Deisolated
```

1. Press Up or Down to scroll through the zones.
2. Press the zone number, or press Enter to select a zone for editing.
3. Press Up and Down to change the zone state.
4. Confirm the changes by pressing Enter.
5. Press Clear twice to exit programming.

Active zones

When one or more zones are active, the system displays:

```
1>Zone 1
    Active
```

The active zones are listed one by one.

1. Press Up and Down to scroll through the zones.
2. To isolate the zone, press Enter. The confirmation is displayed:

```
1>Zone 1
    Isolated
```

3. Press Clear to exit programming.

2.2 Isolate expander

2.3 Isolate keypad

Isolating an expander or keypad works the same way as isolating a zone, except the devices remain operational.

Log

3 Display logs

The Display logs list provides you with a quick alarm history. It is a fast and easy way to determine where alarms have happened. This information is useful when you have had to reset an alarm without checking its cause immediately.

To view messages, select one of the following message types.

- 1 All: All events
- 2 Mandatory: Only events that are considered as mandatory by EN 50131-1 (set/part set/unset, alarms, hold-up, tamper, fault, user change, engineer reset etc.)
- 3 Non mandatory: Events other than mandatory events mentioned above
- 4 Installer: Events caused by the installer (programming mode, PC connection etc.)
- 5 Access: Access events, like access granted and access denied
- 6 Dialer: Dialer and communication events

The display shows where the event occurred.

```
1>Access granted
      User 3
```

You can now:

- Scan recent alarms. Press Up or Down.
- View details. Press Enter.

```
05May08 15:04:54
      System
```

- Exit history. Exit the alarm history and return to the initial display. Press Clear.

Note: You cannot see events from the area if you don't have permission for the area, or if the keypad is not programmed for access to the area.

Panel status

4 Panel status

The "Panel status" function lists zones that are in alarm or tamper alarm, zones that are inhibited or active, plus system alarms.

There are menu options that display each of these conditions separately. However, this option can be used to check on all zones that need attention.

If you are allowed, you can see the panel current status using the "4 Panel status" menu.

The following data can be viewed:

- 1 View open zones: Displays zones that are not in normal state. The top line shows the zone that is not in normal state. The bottom line shows the zone status.
- 2 Alarms: Displays and lets you to acknowledge pending alarms.
- 3 Faults: Displays active faults.

Settings

5 Settings

```
1>PIN code
2 Remote opts
```

Use the menu to change PIN and configure SMS and voice settings.

5.1 PIN code

```
1>Change PIN
*****
```

Use the menu to change your PIN.

5.1.1 Change PIN

```
1 Change PIN
> <
```

If you are allowed, you can change your PIN using Change PIN menu.

The PIN policy in the Axon x700 system can be configured in one of the following ways:

- ☐ PINs are generated by the system. The user can request a new PIN generation, but PINs cannot be entered manually or edited.

The PIN is generated when pressing Enter in this menu. Once generated the code is then displayed.

- ☐ PINs are entered manually.

If you are allowed to do it, you can enter the unique PIN you want to have.

Pressing Enter lets you enter or edit a PIN.

To confirm the PIN, enter it again.

PINs must be unique. A PIN cannot be assigned to more than one user. The system does accept entry of PINs that are already in use.

5.2 Remote opts

```
1>Remote login
name@email.com
```

The menu contains configuration menus for remote access.

5.2.1 Remote login

```
1 Remote login
>name@email.com<
```

The menu allows you to configure your remote access.

After the new login is set, you are prompted to provide the remote password.

```
New password
> <
```


Note: It is highly recommended to follow these requirements to ensure proper remote password complexity:

- The password is minimum 8 characters long
- Contains minimum 1 uppercase letter, 1 lowercase letter, 1 digit, and 1 special character (+ - * % & < > / @ space)
- Doesn't contain your user name, real name, or company name
- Doesn't contain a complete word
- Differs significantly from previous passwords

If the login and password are set successfully, the following message is displayed:

```
INFO
Login/Passwd set
```

To remove the existing remote login, enter the empty string instead.

5.2.2 Change passwd

```
2 Chg rem passwd
> <
```

Use the menu to change your remote password.

If the password is changed successfully, the following message is displayed:

```
INFO
Password changed
```

5.2.3 Mobile number

```
3 Mobile number
> <
```

The menu lets you set your personal mobile phone number.

This phone number is used if the GSM reporting destination type is set to User or User Group.

This mobile phone number also identifies a sender of an SMS command. See *SMS Control Reference Manual* for more information.

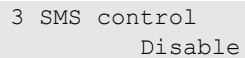
5.2.4 SMS reporting

```
2 SMS reporting
Off
```

The SMS reporting menu lets you enable or disable SMS reporting to you.

This option is editable only if you belong to a user group that has SMS reporting privilege enabled.

5.2.5 SMS control

A screenshot of a user interface menu. It shows a grey rectangular button with the text "3 SMS control" on the top line and "Disable" on the bottom line, both in a light grey font.

The SMS control menu allows you to see whether you have a possibility to send SMS commands.

See “Appendix A. SMS control” on page 79 for more information on SMS control.

Note: SMS control for a user is disabled after 10 attempts to perform an unauthorized SMS command. See *SMS Control Reference Manual* for more information.

Door control

6 Door control

```
1>Door open
```

The menu allows you to send a direct command to a specific door.

- 1 Door open: Open a specific door for a time period configured for this door.
- 2 Door lock: Lock a specific door.
- 3 Door unlock: Unlock a specific door until Door lock command is sent.
- 4 Door disable: Disable a specific door. This makes access for all users denied.
- 5 Door enable: Enable a disabled door.

Select a command, then select a door from the door list, and press Enter.

Users

7 Users

```
0>Add user
2 Supervisor
```

Use the “Users” menu to add, edit, or delete users of the Axon x700 system. Up to 50 users can be programmed.

For each user, the system records these options:

- Number
- Name
- PIN
- Card ID number
- Mobile number
- Remote login and password
- User group (which determines options the user can access)
- Door group (which determines regions the user can access)
- Language
- Various programmed options

Note: Your own user group might not allow you to program PINs. If it does allow use of this option, there might still be restrictions on which user groups you are allowed to update.

Maximum user number in the system depends on the panel variant.

Note: Connecting door controllers to the Axon x700 system increases the maximum user number in the system. However, additional users do not have the following records:

- Phone number
- Language

There are two predefined users in the system. See “Predefined users” on page 7.

User data lock

If the system is configured as EN 50131 compliant, it does not allow you to modify existing users. The new user can be configured only when added, and the existing user can be only removed. The supervisor can only modify own settings, and other users can modify their own settings.

After the new user is added via menu “7.0 Add user” on page 37, the supervisor can configure this user. After the modification is done and the supervisor is going to exit the user menu, the following confirmation request appears:

```
Lock user data?
    >Cancel<
```

Choose OK to confirm the new user configuration. After it, only this user is able to modify own settings.

Otherwise, choose Cancel to return to the user configuration.

User settings

7.0 Add user

```
Add mode
    >Manual<
```

Access the menu to add users.

Choose manual or sequential mode for user adding.

In the manual mode, a user is created at the first unoccupied number in the user list. If the user is created successfully, the following message appears:

```
INFO
User added
```

After this, you can start editing the user details for the new user.

In the sequential mode, you are prompted to badge the new user card.

```
Badge card
Rkp 1
```

Badge the card on the reader programmed in System Options.

If the card is valid and the user is created successfully, the following message is displayed:

```
User 13
Card assigned
```

Next, you are prompted to badge another card. Press Cancel to exit the sequential user programming and go to the user configuration.

If the card is already used, the error is displayed.

```
ERROR
Card in use
```

7.n Edit user

Select a user to edit.

The following options can be configured.

7.n.1 User name

```
1 User name
>User 6    <
```

Press Enter to edit the name, or Clear to exit.

The default user name is “User N”, where N is the user number.

The name can have up to 16 characters.

7.n.2 PIN

```
1>Change PIN
*****
```

The PINs policy in the Axon x700 system can be configured in one of the following ways:

- ☐ PINs are generated by the system. The user can request a new PIN, but PINs cannot be entered manually or edited.

A PIN is generated by selecting Yes and pressing Enter in this menu. The generated PIN will show until Enter is pressed again.

- ☐ PINs are entered manually.

Pressing Enter lets you enter or edit the PIN of the selected user.

Contact the system installer to set the PIN change mode.

PIN length is programmable in the Axon x700 system. The number of available PINs varies from 10000 (for 4-digit PINs) to 10000000000 (for 10-digit PINs).

No PINs are reserved for system use. Any PIN can be generated or entered for use. The system will not accept generate or accept entry of PINs already in use.

7.n.3 User card

```
3>User card
*****
```

The User card menu allows you to enter the user card number. Press Enter and present the card to the keypad.

7.n.4 RF Fobs

```
0>Add fob
1 Fob 1
```

This menu lets you see all fobs programmed for the selected user, select an existing fob, or create a new one.

7.n.4.0 Add fob

To add a fob, follow one of the procedures described in “Fobs programming” on page 63.

7.n.4.m Select fob

```
1>Fob name
Fob 1
```

Select an existing fob to program.

7.n.4.m.1 Fob name

```
1 Fob name
>Fob 1 <
```

Use the Fob name option to set a fob name. The fob name identifies the fob to the end-user for alarm reporting or for display of status or error message.

When a fob is created, it is given the default name “Fob Ex.y”, where <x> is the expander number, and <y> is an expander input number. For example, default fob name “Fob E2.8” is given to the fob assigned to input 8 on the expander 2.

A fob name can consist of 16 characters.

7.n.4.m.4 RF details

```
1>Sensor ID
    4232C1
```

The RF device menu allows you to program a wireless device manually, or remove it from the wireless expander.

7.n.4.m.4.1 Sensor ID

```
1>Sensor ID
    4232C1
```

The screen allows you to view the sensor ID.

7.n.4.m.4.2 Remove RF dev

```
Remove RF dev?
    >Cancel<
```

Select Ok and press Enter to remove the wireless device from the wireless expander database.

7.n.4.m.5 Remove fob

```
Remove fob?
    >Cancel<
```

Use the Remove fob command to remove the fob from the system. Select Ok and press Enter. The fob is deleted bot from the panel and the wireless expander database.

7.n.5 Language

```
5>Language
    ENGLISH UK
```

The Axon x700 system can display menus in the preferred language of each user.

7.n.6 User groups

```
1>Not set
2 Not set
```

Use the “User groups” menu to assign user groups to the selected user. A user can have up to 16 user groups assigned.

To change a user group assignment, select the appropriate slot.

If the selected slot is empty (the user group is not assigned), you are prompted to select one of the available user groups.

```
02>Supervisor G>
03 Area 1
```

Select the appropriate user group to assign to the selected user.

If the selected slot already contains an assigned user group, you are moved to the “Change UG” menu.

```
1>Change UG
  User Group 3
```

Now you can take one of the following actions:

- Change the assigned group: press 1, or Enter, or Right to go to the user group list and select a group.
— or —
- Delete the assigned group: press 2, or go the next menu entry and press Enter.

For more information on user groups see “User groups” on page 7.

7.n.7 Remote opts

```
1>Remote login
  name@email.com
```

The menu contains configuration menus for remote access.

7.n.7.1 Remote login

```
1 Remote login
>name@email.com<
```

The menu allows you to configure the user remote access.

After the new login is set, you are prompted to provide the remote password.

```
New password
> <
```

If the login and password are set successfully, the following message is displayed:

```
INFO
Login/Passwd set
```

To remove the existing remote login, enter the empty string instead.

7.n.7.2 Change passwd

```
2 Chg rem passwd
> <
```

Use the menu to change the user remote password.

If the password is changed successfully, the following message is displayed:

```
INFO
Password changed
```


7.n.7.3 Mobile number

```
3 Mobile number
> <
```

The menu lets you set the user's personal mobile phone number.

This phone number is used if the GSM reporting destination type is set to User or User Group.

This mobile phone number also identifies a sender of an SMS command. See *SMS Control Reference Manual* for more information.

7.n.7.4 SMS reporting

```
2 SMS reporting
Off
```

The SMS reporting menu lets you enable or disable SMS reporting to the selected user. The reporting can have one of the following states:

- Always: The reporting is enabled
- Off: The reporting is disabled
- Off until re-setting: The reporting is temporarily disabled until the next system set

This option is editable only if you belong to a user group that has SMS reporting privilege enabled.

7.n.7.5 SMS control

```
3 SMS control
Disable
```

The SMS control menu allows you to see whether you have a possibility to send SMS commands.

See "Appendix A. SMS control" on page 79 for more information on SMS control.

Note: SMS control for a user is disabled after 10 attempts to perform an unauthorized SMS command. See *SMS Control Reference Manual* for more information.

7.n.8 Access options

```
1>Door group
Not used
```

Use the menu to configure access control options for the selected user.

7.n.8.1 Door group

```
1 Door group
Not used
```

Assign a door group to the selected user.

7.n.8.2 Floor group

1 Floor group
Not used

Assign a floor group to the selected user.

7.n.8.3 Trace

3 Trace
>No<

If set to Yes, all access events related to this user will be sent from door controllers to the panel and stored in its log, so the panel operator can trace him.

7.n.8.4 Privileged

4 Privileged
>No<

If set to Yes, this user can override the anti-passback functionality and gain access to regions that should be restricted for a normal user due to anti-passback limitations.

7.n.8.5 Extended access

5 Ext. access
>No<

If set to Yes, the selected user has an extended door unlock time granted after badging a valid card or entering PIN. The extended time is set separately for each door.

7.n.8.6 Acc. user type

6 Acc. user type
>Normal<

Defines the type of user for enhanced security.

- Normal: Normal operation.
- Two cards: Requires two valid user codes or cards to be presented to perform any alarm or access control functions.
- Guard: The user code or card can only perform functions when used in conjunction with a visitor code or card.
- Visitor: Requires a code or card from a user who has a Guard user type.
- High security user: only when required number of those users is reached within a high security region, normal users are also permitted to be inside.

7.n.9 Select mode

```
9 Select mode
   >Areas<
```

Depending on the selection, the user operates on areas or area groups. The following options are available:

- Areas. The user can only set and unset particular areas. This is the default value.
- Area groups. The user can only set and unset particular area groups.
- All. The user can set and unset areas as well as area groups.

7.n.10 Delete user

To remove a user, select a user using the cursor, or by entering the user number, and go to the Delete user menu.

The display shows:

```
10 Delete user
   >Cancel<
```

Choose Ok and press Enter. This removes the user.

Repeat this to delete other users, or press Clear to exit and return to the higher menu level.

Note: You cannot delete a user unless your user group authorizes you to do so.

Service

8 Service menu

The Service menu allows performing the maintenance tasks described below.

8.1 Time and date

```
1>Time zone
    UTC+1
```

The Time and date menu allows you to set the system time and date, as well as set up daylight saving time.

The following options are available.

- 8.1.1 Time zone: The system time zone.
- 8.1.2 Date: Date format is DD-MM-YYYY.
- 8.1.3 Time: Time format is 24 hours.
- 8.1.4 Daylight saving time beginning month: The DST start month.
- 8.1.5 Daylight saving time beginning week: The DST start week. The available options are: 1st week, 2nd week, 3rd week, 4th week, last week.
- 8.1.6 Daylight saving time ending month: As above.
- 8.1.7 Daylight saving time ending week: As above.
- 8.1.8 Set correction: Allows configuring time correction if necessary.
 - 8.1.8.1 Time/7days: This submenu allows setting the time correction that is performed each 7 days of panel work.
Maximum value is 5 min 40 s. Positive value means the clock is set forward, negative — backward.

During daylight saving time change, the time always advances on Sunday at 2:00, and rewinds at 3:00.

Note: See “Daylight saving note” on page 52 for information on daylight saving time change on programmed actions.

8.2 Test menu

```
1>Walk test
2 Input test
```

The menu contains functions that allow the user to test the alarm system.

8.2.1 Walk test

```
Walk test
in progress
```

Walk test allows the user to test all detectors in the selected areas.

To perform the walk test:

1. Enter the menu.

Next, you are prompted to choose between total and reduced walk test.

```
Walktest scope
>Total<
```

The following options are available:

- Total: Standard walk test. All appropriate zones are tested.
- Reduced: Reduced walk test. This test is limited only zones that were not active recently, during last 4 hours, or since the last set.

Choose a walk test scope and press Enter.

The display lists all zones to be tested.

```
1>Zone 1
Need Active
```

2. Walk along all detection points and make sure the detector is activated either by walking in front of it or by opening a door or window.

Each activated zone is removed from the list on the display.

3. Return to the keypad and verify the result.

If the test is passed, the following message is displayed:

```
Walk test OK
Press Enter
```

Otherwise, there still is a list of untested zones. Contact the installer if you are unable to pass the walk test.

See also “Performing a walk test” on page 20 for more information.

8.2.2 Test input

```
0>Zone
1 Panel
```

Enter the Input test menu to test inputs.

Select Zone to enter zone number. Alternatively, select the input location first (panel, internal or external expander), then enter the (physical) input number on this location.

Zone number, name, and input state are displayed.

```
12>Warehouse
Normal
```

You can now:

- Scroll through the list of zones. Press Up or Down.
- Scroll between input state, zone type and zone location. Press Left or Right.

```
12>Warehouse
Alarm
```

```
12>Warehouse  
Panel Exp 1.12
```

- Exit input test. Press Clear.

8.3 Manual test call

```
01>CS 1  
02 CS 2
```

The Manual test call option allows you to test the central station reporting. Select the central station. The panel now tries to establish a connection with the selected central station.

The call progress status is shown on the display.

8.4 Siren test

```
1>Internal siren  
2 External siren
```

The Siren test menu allows you to test internal and external sirens as well as strobes.

Note: this function works only with certain settings programmed. Please contact system installer to confirm that this function is available.

Available options for testing are the following:

- 1 Internal siren: Toggle the state of the internal siren
- 2 External siren: Toggle the state of the external siren
- 3 Strobe: Toggle the state of the strobe

Enter the appropriate menu and press Enter to activate the output. Press Enter again to deactivate it. Press Clear to exit from the menu.

8.5 Communications

```
1>CS  
2 PC connection
```

The menu is used to change particular communication settings.

Note: The option availability depends on the user group permissions.

8.5.1 CS (central station)

```
01>CS 1  
02 CS 2
```

Axon x700 allows you to change phone numbers for central stations that are programmed for voice communication.

8.5.1.n Select CS

```
1>Phone
```

Select central station to change the phone number.

8.5.1.n.1 Phone

```
1 Phone  
> <
```

Every central station reports to one telephone number. The phone number can contain up to 20 digits. The following special characters are available:

- P: Pause (3 s).
- T: Waiting for dial tone.

To enter a character, press the corresponding key twice.

Note: Only voice communication phone numbers can be changed.

8.5.2 PC connection

```
01>PC conn 1  
02 PC conn 2
```

The PC connection menu allows connecting to a PC from the panel. Select the appropriate PC connection to activate.

8.5.3 Credit

```
3>Credit  
-----
```

Enter Credit menu to receive the GSM account state.

8.5.4 UltraSync

```
2>SID number  
3 Settings
```

The menu allows you to configure the UltraSync cloud communication.

8.5.4.2 SID number

```
1>SID number  
084400412454
```

The informational screen that shows the panel serial number.

8.5.4.3 Settings

```
1>Password  
*****
```

The menu contains UltraSync connection settings.

8.5.4.3.1 Password

```
1 Password
  >      <
```

The UltraSync password is necessary to connect to the panel remotely using Downloader or Mobile Application via UltraSync secure cloud.

8.5.4.4 Notification list

```
1>Notification 1
2 Notification 2
```

The menu allows you to configure and remove push notifications for smartphones.

Note: The panel menu does not allow you to add notifications. You can add notifications only using a smartphone application.

8.5.4.4.n Select notification

```
1>Name
  Notification 1
```

Select a notification to configure it.

8.5.4.4.n.1 Notification name

```
1 Name
>Notification 1<
```

Every push notification can be programmed with a name to identify it.

Use the menu to enter or change the push notification name. The push notification name can contain up to 16 characters.

8.5.4.4.n.2 Identifier

```
2>Identifier
```

The informational screen that shows the smartphone notification identifier.

8.5.4.4.n.3 User

```
3>User
  User 3
```

The informational screen that shows the user, which receives the selected push notification.

8.5.4.4.n.4 Status

```
4>Status
  Active
```

The informational screen that shows the status of the selected notification.

- Active: The notification is active and can be received by the user.

- Inactive: The notification is disabled by the installer or supervisor, or the user group permissions do not allow the user to receive notifications, or no event types are enabled for push notifications in “8.5.4.4.n.5 Event types” below.

8.5.4.4.n.5 Event types

```
1>Alarms
    Enabled
```

The menu allows you to select types of events that will be sent to the smartphone.

If the option is enabled, any event of that category is sent via push notification to the assigned user.

The following options are available:

- 1 Alarms: Alarms pending, Panic, RF Jamming, Tamperers, Soak, Technical
- 2 Set/unset: Set, Unset, Part set, Inhibit
- 3 Power: Battery fault, Battery low, Mains fault, PSU fault
- 4 System: Engineer reset, Service, Local programming, RFU events, Auto CS test, Isolation
- 5 Video: Picture memory full, Picture deleted, Picture taken
- 6 Fault: Ethernet link, Communication, Fuse, Power and internal faults and restores
- 7 Access: Access denied, access granted

8.5.4.4.n.6 Delete notification

```
6 Delete notif.
    >Cancel<
```

Use the menu to remove the selected push notification from the system. To remove the notification, select OK and press Enter again. The notification is deleted.

8.6 Chime

```
1>Area 1
    Enable
```

The Chime menu allows you to enable or disable chimes for selected areas and keypads.

Note: If the chime is set to auto in system settings, the chime in the area may automatically become enabled or disabled when the area is armed or disarmed. Please contact the installer for more information.

8.7 Trigger state

```
1>Trigger 1
2 Trigger 2
```

The trigger state menu allows you to manually change trigger flag states.

Choose the trigger and then choose the appropriate flag. Next, set the required state.

```
1>SCHEDULE
    Off
```

8.8 Service in

```
8>Service in
    Enabled
```

Certain regulations prohibit the installer from accessing the menus without permission from the manager (or supervisor). In this case the manager must use the Installer in-time menu to allow the installer to log on to the system menus. Log on permission is granted for a specific time period.

Note: Once the installer enters the installer menu, he can stay in programming mode with no time limit.

8.9 Check card

```
Badge card
Keypad 1
```

Use the menu to read data from a user card.

Badge card on the keypad indicated on the screen the same way as it is done when user card programming (see “7.n.3 User card” on page 38).

If the card is programmed in the system, its holder user information is displayed:

```
User 05
J.Smith
```

Otherwise, if the card is unknown, its type and data is displayed in the same format as in the event log.

```
CARD/TAG
98832665774
```

Badge another card, or press X to exit the menu.

8.10 Uns Time Left

```
Time left 06 min
* to extend time
```

The time left until the delayed ATM autoset occurs.

Press * to extend the timer by the pre-programmed time period.

Calendar

9 Calendar

1>Actions

>>>

The Calendar lets you to configure an automatic execution of specific actions at particular time and date. Panel settings can be automatically adjusted according to the schedule.

The Calendar functionality is based on schedules.

Schedules

Each schedule includes start and end dates, time frames, and actions to be performed. It also defines special days, and a filter that activates actions in this schedule.

Schedules are defined by the following parameters.

- **Date:** Start date and end date determine a time period, when the schedule is valid, or two days when the actions will be activated, depending on time frame configuration.
- **Time:** It is possible to define up to 4 time frames for each schedule.

Caution: Time frames should not overlap.

The time frame is determined by start and end time of the day, and selected days of the week.

If no weekday is selected, the time frame will be valid only on the start and end days of the schedule (non-recurring schedule). Otherwise, the schedule will repeat every week (recurring schedule).

Note: Non-recurring schedule only allows one time frame to be defined.

- **Action list:** A list of actions that must be performed by the system when the schedule is active. See “Actions” below.
- **Special day time:** Alternative time frames, which become valid if the current day is a special day. See “Special days in schedules” on page 52.
- **Filter:** A conditional filter that enables actions in the schedule when becomes true.

Actions

Action is a user programmed function, which can be done automatically by the system according to the programmed schedule.

Every action has the following settings:

- **Name**
- **User function:** See “User programmable functions” on page 60.

Counteractions

Every action has a counteraction that is opposite to this action. For example:

- Counteraction of area set is area unset
- Counteraction of zone uninhibit is zone inhibit
- Counteraction of toggle trigger is toggle trigger, etc.

Counteraction is defined in the schedule automatically if the time frame end is set. In this case the action is performed at the time frame start, and the counteraction is executed at the time frame end. If the time frame end is not set (00:00), the counteraction is not activated.

Special days in schedules

You can assign special day time frames to each schedule. If a schedule contains a special day time frame defined, it will be also activated on special days.

Caution: Special days can only be configured in recurring schedules, which have weekdays selected and are repeated annually.

Special days are assigned to dates in the menu “9.1 View” below.

Daylight saving note

Actions planned between 2:00 and 3:00 on daylight saving time change do not occur when clocks are advanced, and occur twice when clocks are rewind.

For more information on daylight saving programming, see “8.1 Time and date” on page 44.

Viewing calendar

9.1 View

```
1>10-03-2016
2 11-03-2016
```

Use the View menu to see actions and contractions planned for the particular day.

It is possible to disable an action planned for the current day. To do so, select an action and toggle between On and Off.

9.1.n Date

```
1>Auto Set
2 By object
```

Select or enter a date to see planned actions, or to change its status, and press Enter.

9.1.n.1 Auto setting

```
0>All areas
>>>
```

Enter the menu to see all automatic setting actions in particular areas planned for the selected day.

Select All areas, or choose the appropriate area.

9.1.n.2 By object

```
1>Area
2 Rkp
```

Enter the menu to see all actions planned on the selected day for particular objects.

Select object name or type. The available objects are described in “User programmable functions” on page 60.

9.1.n.3 Special day

```
1>Day type
Normal Day
```

Enter the menu to configure the selected day as a special day.

For more information, see “Special days in schedules” on page 52.

9.1.n.3.1 Day type

```
1 Day type
>Normal day<
```

Choose a type for the selected day:

- Normal day: A normal day. A special day time frame is not valid.
- Holiday, Special day 2 etc.: The day is one of special days defined in “9.2.n.6 Special days” on page 57.

9.1.n.3.2 Recurring

```
2 Recurring
>Yes<
```

If set to Yes, the special day repeats every year. Otherwise, it is valid only once on the defined date.

9.1.n.3.3 Until date

```
3 Until date
>10.03.2016<
```

If the end date is set, the special day object will cover a time period from the selected day to the end date set in the Until date menu.

Note: A time period overwrites other special days in case of overlapping.

Schedules

9.2 Schedules

```
0>Add Schedule
1 Schedule 1
```

Each panel action performed automatically can be driven by up to two schedules. Use the Schedules menu to add and modify schedules.

For more information on schedules see “Schedules” on page 51.

Schedule settings

9.2.0 Add schedule

Access the menu to add a schedule. If the schedule is created successfully, the following message appears:

```
INFO
Schedule added
```

The new schedule is given the default name “Schedule N” and placed on the end of the schedule list. You can now start editing the schedule details for the new schedule.

9.2.n Select schedule

```
1>Name
Schedule 1
```

Select a schedule to program.

9.2.n.1 Schedule name

```
1 Name
>Schedule 1 <
```

Every schedule can be programmed with a name to identify it.

Use the Schedule name screen to enter or edit the schedule name. The schedule name can contain up to 16 characters.

9.2.n.2 Active

```
2 Active
>Off<
```

If set to On, the schedule is currently active.

9.2.n.3 Date

```
1>Start date
01.01.2016
```

Enter the following dates:

- 1 Start date: The date of the schedule start.

- 2 End date: The date of the schedule end. Note that this date cannot be earlier than the Start date.

9.2.n.4 Time

```
0>Add time frame
1 Time frame 1
```

Define time frames when the schedule activates.

9.2.n.4.0 Add time frame

Access the menu to add a time frame. If the time frame is created successfully, the following message appears:

```
INFO
Time frame added
```

The new time frame is given the name “Time frame N” and placed on the end of the action list. You can now start editing the action details for the new action.

Caution: Time frames should not overlap.

9.2.n.4.m Select time frame

```
1>Start time
00:00
```

Select a time frame to program.

9.2.n.4.m.1 Start time

```
1 Start time
>00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected time frame starts.

Note: Value 24:00 means that the time frame is not configured.

9.2.n.4.m.2 End time

```
2 End time
>00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected time frame ends. The value 00:00 means that the end time is not set, and therefore the counteraction is not performed. See “Counteractions” on page 52 for more information.

9.2.n.4.m.3 Week days

```
Week days
>M.WT...<
```

Select days of the week when the selected time frame is active.

If no weekday is selected, the schedule will only be valid on the first and the last day (non-recurring schedule). In this case only one time frame can be used. See also “Schedules” on page 51.

9.2.n.4.m.4 Delete time frame

To remove a time frame, select a time frame using the cursor, or by entering the time frame number, and go to the Delete time frame menu.

The display shows:

```
4 Delete TF
    >Cancel<
```

Choose Ok and press Enter. This removes the time frame.

Repeat the command to delete other time frames, or press Clear to exit and return to the higher menu level.

Note: You cannot delete a time frame unless your user group authorizes you to do so.

9.2.n.5 Action list

```
0>Add Action
1 Action 1
```

Select actions that must be performed by the system according to the selected schedule.

Each action can be programmed with a number of options. Before going any further, select the action to program.

9.2.n.5.0 Add action

Access the menu to add an action. If the action is created successfully, the following message appears:

```
INFO
Action added
```

The new action is given the default name “Action N” and placed on the end of the action list. You can now start editing the action details for the new action.

9.2.n.5.m Select action

```
1>Name
    Action 1
```

Select an action to program.

9.2.n.5.m.1 Action name

```
1 Name
>Action 1    <
```

Every action can be programmed with a name to identify it.

Use the Action name screen to enter or edit the action name. The action name can contain up to 16 characters.

9.2.n.5.m.2 Object type

9.2.n.5.m.3 Function

9.2.n.5.m.4 Parameters

Available object types, functions and parameters are described in “User programmable functions” on page 60.

9.2.n.5.m.5 Delete action

To remove an action, select an action using the cursor, or by entering the action number, and go to the Delete action menu.

The display shows:

```
5 Delete action
  >Cancel<
```

Choose Ok and press Enter. This removes the action.

Repeat the command to delete other actions, or press Clear to exit and return to the higher menu level.

Note: You cannot delete an action unless your user group authorizes you to do so.

9.2.n.6 Special days

```
0>Add sp day
1 Holiday
```

Configure special days associated with this schedule.

9.2.n.6.0 Add special day

Access the menu to add a special day. If the special day is created successfully, the following message appears:

```
INFO
Sp day added
```

The first special day is given the default name “Holiday”, while subsequent special days are named “Special day 2”, “Special day 3”, etc.

9.2.n.6.m Select special day

```
1>Name
    Holiday
```

Select a special day to program.

9.2.n.6.m.1 Special day name

```
1 Name
>Holiday  <
```

Every special day can be programmed with a name to identify it.

Use the Special day name screen to enter or edit the special day name. The special day name can contain up to 16 characters.

Note: Special day names are common for all schedules.

9.2.n.6.m.2 Start time

```
1 Start time
   >00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected special day time frame starts.

9.2.n.6.m.3 End time

```
1 Start time
   >00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected special day time frame ends.

9.2.n.6.m.4 Delete special day

To remove a special day, select a special day using the cursor, or by entering the special day number, and go to the Delete special day menu.

The display shows:

```
5 Delete sp day
   >Cancel<
```

Choose Ok and press Enter. This removes the special day.

Repeat the command to delete other special days, or press Clear to exit and return to the higher menu level.

Note: You cannot delete a special day unless your user group authorizes you to do so.

9.2.n.7 Filter

```
00>Not used
01 Internal Sire
```

Assign an additional condition filter to the schedule.

If this filter is deactivated, the schedule is disabled. If no condition filter is assigned, the schedule is executed unconditionally.

9.2.n.8 Delete schedule

To remove a schedule, select a schedule using the cursor, or by entering the schedule number, and go to the Delete schedule menu.

The display shows:

```
8 Delete sched
   >Cancel<
```

Choose Ok and press Enter. This removes the schedule.

Repeat the command to delete other schedules, or press Clear to exit and return to the higher menu level.

Note: You cannot delete a schedule unless your user group authorizes you to do so.

User programmable functions

You can program your own user functions that can later be activated automatically or manually. For example, you can program a user function for setting an area or switching on an output, and then define a schedule for it.

Programming menu

The function programming menu is accessible from various menus where user programmable functions are used.

The list of allowed functions may vary for different menus.

To program a user function:

```
1 Type
    >None<
```

First, choose an appropriate function type.

Note: Depending on the user menu entry, you may need to select an object type first, for example, Door or Area.

Next, configure function parameters.

Available parameters depend on the selected function type. For particular types parameters are disabled.

Note: Particular functions require user code entering. To disable it, switch off the “User Code Req” parameter, if allowed.

Depending on the activation method, the following function types and parameters may be available.

Table 4: Available function types and parameters

Type	Description	Available parameters
None	No function is assigned	None
Set	Set areas [1][2]	1. Area selection 2. Area groups selection 3. User code requirement
Unset	Unset areas [1]	1. Area selection 2. Area groups selection
Trigger	Change a trigger state	1. Trigger name 2. State change: Clear, Set, or Toggle
Part set 1	Part set 1 for areas [1][2]	1. Area selection 2. User code requirement
Part set 2	Part set 2 for areas [1][2]	1. Area selection 2. User code requirement
Inhibit	Inhibit zones [1][3]	None
Test call	Execute a test call [3][4]	None
PC connection	Establish connection with the PC [1][3]	None

Type	Description	Available parameters
Service in	Allow service in [5]	None
Panic	Activate panic alarm	None
Chime area	Change a chime functionality status in the area	1. Area selection 2. Status change: Clear, Set, or Toggle
Chime keypad	Change a chime functionality status on the keypad	1. Keypad selection 2. Status change: Clear, Set, or Toggle
Set without exit	Immediate set (without exit time) [1]	1. Area selection 2. Area groups selection 3. User code requirement
Fire reset	Reset fire detectors [1]	1. Area selection
Show open zones	Show open zones [1]	1. User code requirement
Active alarms	Show zones in alarm state [1]	1. User code requirement
Active faults	Show faulty zones [1]	1. User code requirement
Alarm memory	Show acknowledged alarms [1]	1. User code requirement
Alarms to ACK	Show unacknowledged alarms [1]	None
UG control	Change user group privileges	1. UG identifier 2 and further - user group privilege. Choose a privilege, and then change it. Note that the user group type must allow this change.
Keypad control	Change keypad options	1. Keypad identifier 2. State change: lock or unlock
Walk test	Run walk test [1]	1. Area selection
Output test	Test outputs [1][4]	1. Output selection. 4 outputs can be assigned. 2. User code requirement.
Test pic to CS	Take a picture and send it to a central station	1. Camera 2. Central station
Fire	Raise a fire alarm	None
Medical alarm	Raise a medical alarm	None
Show inhibited	Show inhibited zones	None
GSM credit	Check GSM credit	None
UG area access	Change user access to areas	1. UG identifier 2. Area selection 3. Area groups selection
Prohibit unset	Disable area unset	1. Area selection 2. State change: On or Off
Shunt	Allow shunt in areas	1. Area selection 2. State change: Shunt, Unshunt, Toggle
Show shunted	Show shunted zones	None

Type	Description	Available parameters
Show isolated	Show isolated zones, keypads, and expanders	None
Unlocked	Unlock doors	1. Door selection
RTE	Enable Request To Exit input for specific doors	1. Door selection
Low security	Enable Low security mode for specific doors	1. Door selection
Access enabled	Enable access to doors in a door group [6]	1. Door group selection

- [1] Depending on system settings, the function may require logging in of a user with the appropriate privileges.
- [2] Set and part set function start time is the time when the warning timer is started. The warning time must be considered.
- [3] The function is an entry to the appropriate user menu.
- [4] The function requires logging in of the supervisor or the installer.
- [5] The function requires logging in of the supervisor.
- [6] Caution: This function should be only performed in a time frame with specified end time. See also “Counteractions” on page 52.

The described functions can be activated by one of the following:

- Schedule. See “Calendar” on page 51 for more details.
- Function key. See “Function keys” on page 68.
- Fob. See “Fobs programming” on page 63 for more details.

Fobs programming

To add a fob, follow one of the following procedures.

Sequential mode

In sequential mode, you can learn a range of fobs.

To learn fobs in sequential mode:

1. Go to the “7.n.4.0 Add fob” menu described on page 38.

```
1>Expander 1
2 Expander 2
```

2. Select fob zone location.

```
Learn mode
>Sequential<
```

3. Choose Sequential mode and press Enter.

```
Input number
> <
```

4. Choose an input number.

```
INFO
Program fob 1
```

5. Press the programming key sequence to activate the fob. See “Fob activation” on page 65 for more information about activation.

If an error occurs, the keypad shows an error message and beeps seven times.

```
WARNING
ERROR
```

The error can occur, for example, when you try to learn a fob, which is already programmed in the wireless expander.

If the fob is programmed successfully, the keypad shows an information message and beeps once.

```
INFO
Fob learned
```

If there are more fobs to program, and there are fob inputs available in the wireless expander, repeat learning another fob.

```
INFO
Program fob 2
```

To stop the learning process and exit the menu, press Clear.

Proceed with the fob configuration.

Manual mode

In manual mode, you can learn and configure a fob.

To learn a fob in manual mode:

1. Go to the “7.n.4.0 Add fob” menu described on page 38.

```
1>Expander 1
2 Expander 2
```

2. Select zone location.

```
Learn mode
  >Manual<
```

3. Choose Manual mode and press Enter.

```
Input number
  > <
```

4. Enter the input number.

If the input is free, you are prompted to activate the wireless device.

```
Program fob 1
Press # for ID
```

5. Press the programming key sequence to activate the fob, or press Enter to enter fob identifier and fob encryption key manually. See “Fob activation” on page 65 for more information about activation.

```
Fob ID
  > <
```

```
Fob key
  > <
```

If the input has been already programmed, you are informed by a message and seven beeps.

```
INFO
Fob exists
```

Next you are asked if you want to replace the programmed fob.

```
Replace fob?
  >No<
```

If the fob is programmed successfully, the keypad shows an information message and beeps once.

```
INFO
Fob learned
```

Next you are asked if you want to edit the new fob.

```
Edit fob?
  >No<
```

Chose Yes and press Enter to edit fob settings.

Otherwise you are asked if you want to learn another fob.

```
Next fob?
  >No<
```


Chose Yes if you need to configure more fobs. The procedure will be then repeated.

Fob activation

To activate a fob:

1. Press the unlock button quickly two times, then press and hold until fob LED flashes 3 times. Release the button immediately after third flash.
2. Press the unlock button quickly, then press and hold until fob LED flashes 2 times. Release the button immediately after the second flash.
3. Press and hold the unlock button until touchpad light flashes once, and then release the button immediately.

Common key sequences

See “Set and unset the system” on page 11.

The authorization method depends on system settings. Consult the system installer to define the authorization method.

Common key sequences for LCD keypad

Table 5: Common key sequences for LCD keypad

Action	Programmed method	Key sequence	[1]
Set	Set with key	On	<input type="checkbox"/>
		On, PIN, Enter	<input type="checkbox"/>
	Set with PIN	PIN, On	<input type="checkbox"/>
		Card	<input type="checkbox"/>
		On, card	<input type="checkbox"/>
	Set with card	3 x card	<input type="checkbox"/>
		On, card, PIN, Enter	<input type="checkbox"/>
		Card, PIN, On	<input type="checkbox"/>
	Set with card and PIN	Card, PIN, On	<input type="checkbox"/>
Unset	Unset with PIN	Off, PIN, Enter	<input type="checkbox"/>
		PIN	
		PIN, Off	<input type="checkbox"/>
	Unset with card	Card	<input type="checkbox"/>
		Off, card	<input type="checkbox"/>
	Unset with card and PIN	Off, card, PIN, Enter	<input type="checkbox"/>
		Card, PIN, Off	<input type="checkbox"/>
		Card, PIN	
	Unset with card and PIN	Card, PIN	
Part set	Part set with key	Partset	<input type="checkbox"/>
		Partset, PIN, Enter	<input type="checkbox"/>
	Part set with PIN	PIN, Partset	<input type="checkbox"/>
		Card	<input type="checkbox"/>
		Partset, card	<input type="checkbox"/>
	Part set with card	3 x card	<input type="checkbox"/>
		Partset, card, PIN, Enter	<input type="checkbox"/>
		Card, PIN, Partset	<input type="checkbox"/>
	Part set with card and PIN	Card, PIN, Partset	<input type="checkbox"/>
Door access	Door access with PIN	PIN, Enter	<input type="checkbox"/>
	Door access with card	Card	<input type="checkbox"/>
	Door access with card and PIN	Card, PIN, Enter	<input type="checkbox"/>

Action	Programmed method	Key sequence	[1]
Menu access	Menu access with PIN	Menu, PIN, Enter	<input type="checkbox"/>
		PIN, Menu	<input type="checkbox"/>
	Menu access with card	Menu, card	<input type="checkbox"/>
	Menu access with card and PIN	Menu, card, PIN, Enter	<input type="checkbox"/>
		Card, PIN, Menu	<input type="checkbox"/>
Duress	Duress with PIN	Any set key (On / Off / Partset), duress code, Enter	<input type="checkbox"/>
		Duress code, any set key	<input type="checkbox"/>
	Duress with card and PIN	Any set key (On / Off / Partset), duress code, card, Enter	<input type="checkbox"/>
		Card, duress code, any set key	<input type="checkbox"/>
Change keypad buzzer volume	Increase volume	X + Right	<input type="checkbox"/>
	Decrease volume	X + Left	<input type="checkbox"/>
Panic	Panic alarm	1 + 3	<input type="checkbox"/>
Active alarms	Display active zones and faults that should be acknowledged	Function, Function	<input type="checkbox"/>
Alarm memory	Display alarms that occurred when set	Enter, Enter	<input type="checkbox"/>

[1] Availability must be defined by the installer.

See also “Areas displayed during set and unset” on page 17.

Common key sequences for keypad without LCD

Table 6: Common key sequences for keypad without LCD

Action	Programmed method	Key sequence	[1]
Set	Set with PIN	On, PIN, On	<input type="checkbox"/>
		PIN, On	<input type="checkbox"/>
	Set with card	Card	<input type="checkbox"/>
		On, card	<input type="checkbox"/>
		3 x card	<input type="checkbox"/>
	Set with card and PIN	On, card, PIN, On	<input type="checkbox"/>
		Card, PIN, On	<input type="checkbox"/>
Unset	Unset with PIN	Off, PIN, On	<input type="checkbox"/>
		PIN	<input type="checkbox"/>
		PIN, Off	<input type="checkbox"/>
	Unset with card	Card	<input type="checkbox"/>
		Off, card	<input type="checkbox"/>
	Unset with card and PIN	Off, card, PIN, On	<input type="checkbox"/>
		Card, PIN, Off	<input type="checkbox"/>

Action	Programmed method	Key sequence	[1]
		Card, PIN	
Part set	Part set with card	Card	<input type="checkbox"/>
		3 x card	<input type="checkbox"/>
Door access	Door access with PIN	PIN, Off	<input type="checkbox"/>
	Door access with card	Card	<input type="checkbox"/>
	Door access with card and PIN	Card, PIN, On	<input type="checkbox"/>
Duress	Duress with PIN	Any set key (On / Off), duress code, Enter	<input type="checkbox"/>
		Duress code, any set key	<input type="checkbox"/>
	Duress with card and PIN	Any set key (On / Off), duress code, card, Enter	<input type="checkbox"/>
		Card, duress code, any set key	<input type="checkbox"/>
Panic	Panic alarm	1 + 3	<input type="checkbox"/>

[1] Availability must be defined by the installer.

When a PIN can be entered, the keypad beeps twice and flashes the red and green LEDs. When an operation fails the keypad beeps seven times. See “When you cannot set or unset” on page 12 for more information.

Function keys

See also “User programmable functions” on page 60.

Table 7: Function keys

Action [1]	Key	[1]
	A	<input type="checkbox"/>
	B	<input type="checkbox"/>
	C	<input type="checkbox"/>
	F1 (F + 1)	<input type="checkbox"/>
	F2 (F + 2)	<input type="checkbox"/>
	F3 (F + 3)	<input type="checkbox"/>
	F4 (F + 4)	<input type="checkbox"/>

[1] Functionality and availability must be defined by the installer.

Programming records

Use the following pages to record the configuration and programming details for your system. The following areas are covered:

- Users
- User groups
- Condition filters
- Schedule
- Special days
- SMS commands

We suggest that you complete the forms using a pencil so that you can erase obsolete entries and thereby keep your records up to date and compact.

It may be necessary to make copies of certain record sheets where the number of records exceeds the space allowed, for example, if your system uses more than four schedules.

We recommend that you store this manual and your record sheets together in a safe place, and ensure that they are always kept up to date.

Users

User groups

Condition filters

This information is provided by the installer.

Schedule

[illegible]

Special days

SMS commands

[illegible]

Appendix A. SMS control

This section specifies the SMS commands available in the systems equipped with AT5734x GSM communication modules. You can send commands to the alarm system via SMS messages. These commands are listed in “SMS command list” on page 80.

See *SMS Control Reference Guide* for more information.

SMS control requirements

In order to use SMS control functions, you must follow these rules:

- Have a valid phone number defined in user options.
This setting is available both locally and remotely. See the Register and Unregister command, as well as the Phone command description.
- Belong to the user group with the SMS control allowance.
- Have SMS control enabled. See the enable and Disable command description for more details.

Command syntax

The following syntax is used for all commands:

```
[<PIN>] <command> [<parameters>] [, <command>
[<parameters>] ]
```

The following principles apply:

- Commands are case-insensitive.
- Any number of consecutive blank characters (spaces, tabs, CRs, etc.) are interpreted as a single space.
- You can have up to 10 commands in one SMS message. Commands must be separated with a comma.
- In most cases <list> is a space-separated list, or “all”. If <list> is “all”, or is omitted, this is equivalent to a list of all objects for which the user has rights for the selected action.
- If the parameter is a phone number, it should be given in the fully expanded form, with country code preceded by “+”. For example: +48555223322.

User authentication

The user is authenticated by the phone number sending the SMS message.

Only registered phone numbers are allowed to send SMS commands.

The PIN field is required, if:

- The “User PIN req.” option is set to Yes

— or —

- The same phone number is programmed for more than one user. The PIN is then required to identify the user.

If the PIN field is required and the command does not contain the PIN code, the following message is returned:

Command rejected, PIN required.

If the PIN field is required and the PIN is invalid, the following message is returned:

Command rejected, invalid PIN.

If the PIN field is not required, the PIN must *not* be present in SMS message.

SMS command list

Table 8: SMS commands

Command	Description	Example
status st	Get system status. The command returns the following: alarm in areas, areas set, areas being set, partset, unset, areas not ready, and fault list.	st Get system status.
area <area list> ar <area list>	Get area names.	area 2 Get area 2 name. ar 2 3 5 Get names of areas 2, 3, and 5.
set [<area list> s [<area list>]	Set areas. If <area list> is “all”, or is omitted, this is equivalent to a list of all areas for which the user has rights for the selected action.	set Set all allowed areas. set 1 Set area 1. s 2 3 5 Set areas 2, 3, and 5. s all Set all allowed areas.
unset [<area list> u [<area list>]	Unset areas. Parameters are equal to the Set command.	unset Unset all allowed areas. unset 1 Unset area 1. u 2 3 5 Unset areas 2, 3, and 5. u all Unset all allowed areas.

Command	Description	Example
partset1 [<area list> p1 [<area list> partset2 [<area list> p2 [<area list>	Part set 1 or part set 2 areas. Parameters are equal to the Set command.	partset1 Part set 1 all allowed areas. partset2 1 Part set 2 area 1. p1 2 3 5 Part set 1 areas 2, 3, and 5. p2 all Part set 2 all allowed areas.
forceset [<area list> fs [<area list>	Forced set areas. Parameters are equal to the Set command.	forceset Forced set all allowed areas. forceset 1 Forced set area 1. fs 2 3 5 Forced set areas 2, 3, and 5. fs all Forced set all allowed areas.
forcepartset [<area list> fp [<area list>	Forced part set areas. Parameters are equal to the Set command.	forcepartset Forced part set all allowed areas. forcepartset 1 Forced part set area 1. fp 2 3 5 Forced part set areas 2, 3, and 5. fp all Forced part set all allowed areas.
zone <zone list> zn <zone list>	Get zone details. The command returns zone name, areas that the zone belongs to, and zone type, for each zone in the list. Up to 10 zone entries can be returned.	zone 2 Get details for zone 2. zn 2 3 5 Get details for zones 2, 3, and 5.
zone status [<area list> zs [<area list>	Get open and inhibit status of all zones in the areas listed. If <area list> is “all”, or is omitted, this is equivalent to a list of all areas for which the user has rights for the selected action.	zone status Get status for all zones in all allowed areas. zone status 1 Get status for zones of area 1. zs 2 3 5 Get status for zones of areas 2, 3, and 5. zs all Get status from all zones in all allowed areas.

Command	Description	Example
zone faults [<area list>] zf [<area list>]	Get fault, tamper, and isolate status of all zones in the areas listed. Parameters are equal to the Zone Status command.	<pre> zone faults Get faults for all zones in all allowed areas. zone faults 1 Get faults for zones of area 1. zf 2 3 5 Get faults for zones of areas 2, 3, and 5. zf all Get faults from all zones in all allowed areas.</pre>
inhibit <zone list> inh <zone list>	Inhibit listed zones.	<pre> inhibit 2 Inhibit zone 2. inh 1 2 3 7 Inhibit zones 1, 2, 3, and 7.</pre>
uninhibit <zone list> uninh <zone list>	Uninhibit listed zones.	<pre> uninhibit 2 Uninhibit zone 2. uninh 1 2 3 7 Uninhibit zones 1, 2, 3, and 7.</pre>
isolate <zone list> iso <zone list>	Isolate listed zones.	<pre> isolate 2 Isolate zone 2. iso 1 2 3 7 Isolate zones 1, 2, 3, and 7.</pre>
unisolate <zone list> uniso <zone list>	Unisolate listed zones.	<pre> unisolate 2 Unisolate zone 2. uniso 1 2 3 7 Unisolate zones 1, 2, 3, and 7.</pre>
event [<type>] [<num>] ev [<type>] [<num>]	<p>Get a selected event.</p> <p>Events are numbered starting from 1 (the most recent event) to 255.</p> <p>Type can be one of the following:</p> <ul style="list-style-type: none"> • “Mandatory” or “m”: mandatory events • “Nonmandatory” or “n”: non-mandatory events • “Installer” or “i”: installer events • “Access” or “a”: access events • “All”: all events <p>If the <type> parameter is omitted, only the mandatory events are listed.</p> <p>If the number is omitted, the most recent event is returned.</p>	<pre> event 23 Get mandatory event 23. event access 3 Get access event 3. ev all Get the last event. event all 13 Get event 13. ev Get the last mandatory event.</pre>

Command	Description	Example
events [<type>] [<num1>] [<num2>] evs [<type>] [<num1>] [<num2>]	<p>Get events from the range, including <num1> and <num2>.</p> <p>Type usage is equal to the “event” command, with the following exceptions:</p> <ul style="list-style-type: none"> If one number is omitted, all events up to <num1> are returned (or <num1> of most recent events). If both numbers are omitted, 10 most recent events are returned (1 to 10). <p>Parameters num1 and num2 can have values from 1 (the most recent event) to 255.</p> <p>Up to 25 events can be returned.</p>	events 23 Get mandatory events from 1 to 23. events access 3 13 Get access events from 3 to 13. ev all Get 10 last events. event all 13 Get events 1 to 13. ev 2 50 Get events 2 to 26 (only 25 events can be returned).
on <trigger list>	Activate listed triggers.	on 1 Activate trigger 1. on 2 5 6 Activate triggers 2, 5, and 6.
off <trigger list>	Deactivate listed triggers.	off 1 Deactivate trigger 1. off 2 5 6 Deactivate triggers 2, 5, and 6.
toggle <trigger list>	Toggle listed triggers states.	toggle 1 Toggle trigger 1. toggle 2 5 6 Toggle triggers 2, 5, and 6.
trigger <trigger list> trig <trigger list>	Get trigger names and states.	trigger 1 Get trigger 1 name and state. tr 2 3 5 Get names and states for triggers 2, 3, and 5.
output <num> out <num>	Get output state.	output 3 Get output 3 status. out 7 Get output 7 status.
outputs [<output list>] outs [<output list>]	Get listed outputs states.	outputs 3 Get output 3 status. outs 7 8 11 Get status of outputs 7, 8, and 11.
start reporting [<num>] start [<num>]	Start SMS reporting to the user <num>, or for the sender, if <num> is omitted [2][3].	start reporting 6 Start reporting for user 6. start Start reporting for yourself.

Command	Description	Example
stop reporting [<num>] stop [<num>]	Stop SMS reporting to the user <num>, or for the sender, if <num> is omitted, until the next system set [2][3].	stop reporting 6 Stop reporting for user 6, until the next system set. stop Stop SMS reporting for yourself, until the next system set.
stop reporting permanent [<num>] stop perm [<num>]	Stop SMS reporting to the user <num>, or for the sender, if <num> is omitted, until started again via the “start reporting” command [2][3].	stop reporting permanent 6 Stop reporting for user 6, until it is allowed by the “start reporting” command. stop perm Stop reporting for yourself, until started again.
register <phone> <num> r <phone> <num>	Change phone number of the user <num> to the new <phone> [1]. Note: You cannot change your own phone number using this command. Use “Phone” command instead.	register +48555223322 6 Change phone number of user 6 to the new one. r +48223322555 9 Change phone number of user 9 to the new one.
unregister <num> unr <num>	Delete phone number of the user <num> [1]. Note: You cannot delete your own phone number using this command.	unregister 6 Delete phone number of user 6. unr 9 Delete phone number of user 9.
phone <phone>	Change own phone number to <phone>. The command must be sent from the old (currently registered) phone number. The registered phone is changed permanently once the next valid command is sent from the new phone number. If the next valid command is sent from the old phone number, the operation is cancelled.	phone +48555223322 Change the registered phone number of the sender for the new one. The next command must be sent from the +48555223322.
pin <PIN> [<num>]	Change PIN for the user <num>, or for the sender, if <num> is omitted [2].	pin 1234 6 Set user 6 PIN to 1234. pin 4321 Set own PIN to 4321.
disable <num> dis <num>	Disable SMS control for the user <num> [1][4].	disable 6 Disable control for user 6 dis 9 Disable control for user 9
enable <num> en <num>	Enable SMS control for the user <num> [1][4].	enable 6 Enable control for user 6 en 9 Enable control for user 9

Command	Description	Example
user <num>	Get user <num> details [1]. The command returns user name, phone number, language, SMS control and reporting privileges.	user 6 List user 6 details u 9 List user 9 details
users [<num 1> <num2>]	List users from <num 1> to <num2> range together with their phone numbers, SMS control and reporting privileges [1]. If the user range is omitted, the list contains only the users that belong to the user groups with "SMS reports allowed" or "SMS control allowed" privileges set.	users 6 9 List users from 6 to 9 and their phone numbers. users List all users that have "SMS reports" and "SMS control" allowed.
language <language> [<num>]	Change language of the user <num>, or for the sender, if <num> is omitted. <Language> is the localized language name, for example, English, Deutsch, Suomi.	language english 6 Set language for user 6 to English. language polski Set own language to Polish.
credits cr	Get GSM network credit information [1]. The answer format may vary for different GSM operators.	cr Get credit information.
connect <num> conn <num>	Start remote PC connection <num> [1]	connect 2 Start PC connection 2. conn 4 Start PC connection 4.
help	Get list of the allowed SMS commands.	help Get command list

- [1] Only the Supervisor can execute this command.
- [2] Non-supervisor users can perform this operation only for themselves. Only the Supervisor can execute this command for a different user than himself.
- [3] The command affects the "SMS reporting" option in the user settings. The command can be performed only for those users that are allowed to receive SMS reports, for example, the user belongs to the User Group with the SMS reporting allowed.
- [4] The command affects "SMS control" option in User settings. The command can be performed only for those users that belong to the User Group with SMS control allowed.

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 Axon x700 system allows any premises to be divided into different areas having different security requirements. Each area has its own zones. Each area is identified by a number and a name. For example, Area 1 Office, Area 2 Workshop, Area 3 Boardroom, 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.
Autoset	An automatic setting of the premises started by a schedule or an exception. See Schedule, Exception.
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.
DGP	Data gathering panel. See Expander.
Dialler	An electronic device that allows the Axon x700 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 four-door expander is an access control panel, which extends the 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.
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 Axon x700 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.
Exception	Particular time periods when a schedule is extended or changed.
Expander	A device that collects data from other security devices within an area, and transfers it to the Axon x700 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)	<p>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.</p> <p>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.</p>
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	<p>There are two types of doors in the system:</p> <ul style="list-style-type: none"> - 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.
Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault	<p>Describes the condition of a zone.</p> <ul style="list-style-type: none"> • 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 Axon x700 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 a keypad as a prerequisite to perform most Axon x700 options. In the Axon x700 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.

Poll	An inquiry message continually sent by the Axon x700 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 with a weekly structure.
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.
Tamper	A situation where a zone, a keypad, control panel, expander or associated wiring are tampered with, or accidentally damaged. The Axon x700 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, keyfob, PC software.
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 Axon x700 system or change parameters in the system either local or remote.
User	Anybody making use of the Axon x700 system. Users are identified to the Axon x700 system by a unique number that is associated with the user's 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 (PIR detector, door contact) to the Axon x700 system. Each device is identified by a zone number and name. For example, 14 Reception Hold-up Button, 6 Fire Exit Door.

Index

A

- access menu, 25
- accessing doors, 10
- acknowledge the alarm, **20**
- action, **51**, 56
 - creating, 56
 - deleting, 57
 - name, 56
- action list, 51
- actions
 - view, 52
- active zones
 - forced set, 13
 - when set/unset, 12
- add
 - action, 56
 - fob, 38, 63
 - schedule, 54
 - special day, 57
 - time frame, 55
 - user, 37
- adding a schedule, 54
- adding a special day, 57
- adding a time frame, 55
- adding a user to the system, 37
- adding an action, 56
- Advisor Advanced Pro, **23**
- alarm
 - description, 19
 - local alarm, 19
- alarm history, 30
- alarms
 - listing alarm history, 30
 - listing zones, 31
 - resetting, 20
 - valid PIN, 21
 - view, 20
 - what to do when there is an alarm, **19**
 - when to contact the central station company, 21
- area
 - selection mode, 42
- area selection mode, 42
- areas displayed, **17**
- armed display, **6**, 11
- autoset, 16

C

- calendar, 51
- card
 - check, 50
- card reader, **3**
- central station, 46
- change PIN, **32**, 38

- changing a user in the system, 37
- check card, 50
- code tamper, 21
- common key sequences, 66
- communication, **46**
 - central station, 46
 - phone number, 47
- condition filter, 58
- configure
 - fob, 38
- creating a schedule, 54
- creating a special day, 57
- creating a time frame, 55
- creating a user, 37
- creating an action, 56

D

- daylight saving time, 44
- deisolate, 29
- delete
 - notification, 49
- deleting a schedule, 58
- deleting a special day, 58
- deleting a time frame, 56
- deleting a user from the system, 43
- deleting an action, 57
- dialler, **46**
- disable door, 35
- door
 - control, 35
- door access, **10**
- door control, 35
- DST, 44
- duress, **9**
 - description, 9
 - resetting, 9

E

- enable door, 35
- end time, 55, 58

F

- faulty zone, **21**
- fob, 38
 - add, 38, 63
 - name, 38
 - remove, 39
- forced set, **13**

G

- glossary, **87**

I

input test, 45
installer, **7**
isolate, 29

K

key sequences, **66**
keypad, **1**
keypad lockout, 21

L

LCD display
 description of message display, 4
learn card, 38
LEDs
 area LEDs, 5
 blinking quickly, 5
 blinking slowly, 5
 on/off, 5
 system alarm lights, 5
 system faults, 6
 what the LEDs mean, 4
local alarm, 19
lock door, 35
lock user data, 36
lockout, 21
log, **30**

M

manual test call, **46**
menu, **24**
 accessing, 25
 panel status, 31
 program users, 36
 scrolling the list of menus, 25
 time out facility, 24
 unauthorised access, 24
 using PIN, 24
messages
 LCD display, 4
mobile application, **23**
mobile phone number, 33, 41

N

notational and typographical conventions, iv
notification
 delete, 49
 event, 49
 identifier, 48
 name, 48
 status, 48
 user, 48

O

open door, 35

P

panel status
 listing zone status, 31
 status codes, 31
part set the system, **15**
 when to part set, 11
PIN
 description, 7
 using, 7
predefined users, 7
preface, iv
program users, 36
programmable functions, 60
programming record sheets, **69**
 condition filters, 73
 schedule, 75
 SMS commands, 77
 special days, 76
 user groups, 72
 user records, 70
programming users, 36

R

remote login, 32
remove
 fob, 39
 RF device, 39
reporting
 phone numbers, 47
resetting alarm, 20
RF device, 39
 remove, 39

S

schedule, **51**
 action list, 56
 active schedule, 54
 condition filter, 58
 creating, 54
 date, 54
 deleting, 58
 name, 54
 special day, 57
 time, 55
 time frame, 55
scrolling the list of menu options, 25
serial number, 47
service, 44
set the system, **14, 15**
 active zones, 12
 autoset, 16
 cannot set system, 12
 time limit, 11
 when to set, 11
SMS
 control, 34, 41

- special day, 57
 - creating, 57
 - deleting, 58
 - end time, 58
 - name, 57
 - start time, 58
- start time, 55, 58
- supervisor, **7**
- system alarm, **19**

T

- tamper alarms
 - listing zones, 31
- telephone number, 47
- test, 44
- test call, 46
- time and date, 44
 - menu options, 44
- time frame
 - creating, 55
 - deleting, 56
 - end, 55
 - start, 55
 - week days, 55
- time limit
 - when set, 11
 - when unset, 12
- timed open, 35
- trigger
 - state, 49
- troubleshooting, **12**, 21

U

- unlock door, 35
- unset the system, **15**, 16
 - alarm, 12
 - time limit, 12
 - when to unset, 11
- user
 - area selection mode, 42
 - card, 38
 - changing, 37
 - creating, 37
 - deleting, 43
 - language, 39
 - name, **37**
 - PIN, 38
 - programming, 36
 - user group, 39
- user card, 38
- user data lock, 36
- user group
 - what is a user group, 7
- user management, 36
- user name, **37**
- user phone, 33, 41
- user programmable functions, 60

V

- view alarm, 20

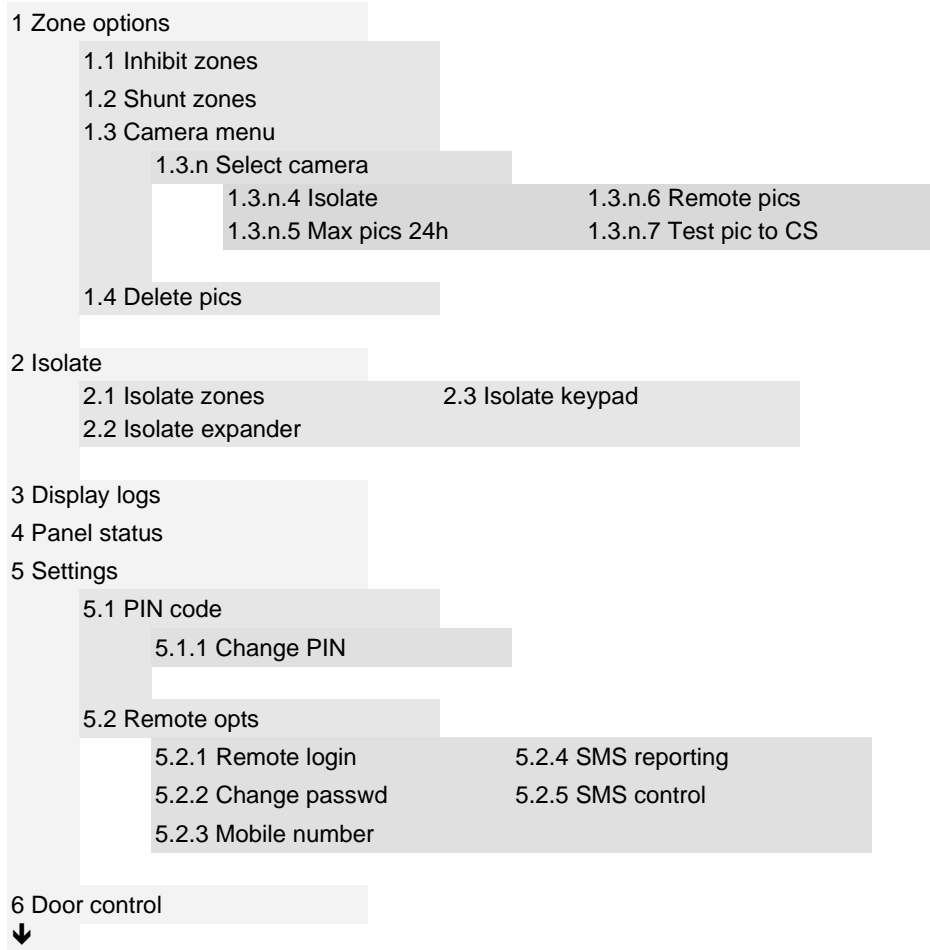
W

- walk test, **20**, 44
- week days, 55
- wireless device, 39

Z

- zones
 - listing active zones, 31
 - listing status, 31

User menu map



7	Users		
7.0	Add user		
7.n	Edit user		
7.n.1	User name		
7.n.2	PIN		
7.n.3	User card		
7.n.4	RF Fobs		
7.n.4.0	Add fob		
7.n.4.m	Select fob		
7.n.4.m.1	Fob name		
7.n.4.m.4	RF details	7.n.4.m.4.1	Sensor ID
7.n.4.m.5	Remove fob	7.n.4.m.4.2	Remove RF dev
7.n.5	Language		
7.n.6	User groups		
7.n.7	Remote opts		
7.n.7.1	Remote login	7.n.7.4	SMS reporting
7.n.7.2	Change passwd	7.n.7.5	SMS control
7.n.7.3	Mobile number		
7.n.8	Access options		
7.n.8.1	Door group	7.n.8.4	Privileged
7.n.8.2	Floor group	7.n.8.5	Extended access
7.n.8.3	Trace	7.n.8.6	Acc. user type
7.n.9	Select mode		
7.n.10	Delete user		
8	Service menu		
8.1	Time and date		
8.2	Test menu		
8.2.1	Walk test	8.2.2	Test input
8.3	Manual test call		
8.4	Siren test		
8.5	Communications		
8.5.1	CS (central station)		
8.5.1.n	Select CS		
8.5.1.n.1	Phone		
8.5.2	PC connection		
8.5.3	Credit		
8.5.4	UltraSync		
8.5.4.2	SID number		
8.5.4.3	Settings		
8.5.4.3.1	Password		
8.5.4.4	Notification list		
8.5.4.4.n	Select notification		
8.5.4.4.n.1	Notification name	8.5.4.4.n.4	Status
8.5.4.4.n.2	Identifier	8.5.4.4.n.5	Event types
8.5.4.4.n.3	User	8.5.4.4.n.6	Delete notification
↓			
↓			

8.6 Chime	
8.7 Trigger state	
8.8 Service in	
8.9 Check card	
8.10 Uns Time Left	
9 Calendar	
9.1 View	
9.1.n Date	
9.1.n.1 Auto setting	
9.1.n.2 By object	
9.1.n.3 Special day	9.1.n.3.1 Day type
	9.1.n.3.2 Recurring
	9.1.n.3.3 Until date
9.2 Schedules	
9.2.0 Add schedule	
9.2.n Select schedule	
9.2.n.1 Schedule name	
9.2.n.2 Active	
9.2.n.3 Date	
9.2.n.4 Time	
9.2.n.4.0 Add time frame	
9.2.n.4.m Select time frame	9.2.n.4.m.1 Start time
	9.2.n.4.m.2 End time
	9.2.n.4.m.3 Week days
	9.2.n.4.m.4 Delete time frame
9.2.n.5 Action list	
9.2.n.5.0 Add action	
9.2.n.5.m Select action	9.2.n.5.m.1 Action name
	9.2.n.5.m.2 Object type
	9.2.n.5.m.3 Function
	9.2.n.5.m.4 Parameters
	9.2.n.5.m.5 Delete action
9.2.n.6 Special days	
9.2.n.6.0 Add special day	
9.2.n.6.m Select special day	9.2.n.6.m.1 Special day name
	9.2.n.6.m.2 Start time
	9.2.n.6.m.3 End time
	9.2.n.6.m.4 Delete special day
9.2.n.7 Filter	
9.2.n.8 Delete schedule	