



AXON Control Panel Installation and Programming Manual

Copyright	© 2025 KGS. All rights reserved. Specifications are subject to change without prior notice.
Trademarks and patents	Aritech, AXON name and logo are trademarks of KGS. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	KGS B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands
Product warnings and disclaimers	THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. KGS 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. WARNING! Fire alarm and smoke detection products used with AXON 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. KGS accepts no liability for any damages caused by incorrect application of the products. For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the QR code.
	
Version	This document applies to the following AXON firmware version: MR 3.2 
Certification	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 - SP4: IP with Ultrasync - SP5: IP with OH receiver, GPRS with OH or Ultrasync receiver - DP4: IP and GPRS with OH or Ultrasync receiver Tested and certified by KIWA Nederland B.V. Important: To comply with the above standards, it is required to configure the system according to settings listed in Chapter 8 “Regulations” on page 377 onwards. This product has not been designed to comply with EN 50134 and EN 54 norms.
European Union directives	KGS hereby declares that this device is in compliance with the applicable requirements and provisions of the Directive 2014/30/EU and/or 2014/35/EU. For more information see firesecurityproducts.com or www.aritech.com.
REACH	Product may contain substances that are also Candidate List substances in a concentration above 0.1% w/w, per the most recently published Candidate List found at ECHA Web site. Safe use information can be found at https://firesecurityproducts.com/en/content/intrusion-intro



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

**Product
documentation**



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

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

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

Contact information

firesecurityproducts.com or www.aritech.com

Content

	Important information	iii
Chapter 1	Quick installation and programming	1
	Quick installation	2
	Quick programming	3
Chapter 2	Installation	7
	General installation information	8
	Maintenance	19
	Mounting	22
	Earthing	24
	Shielding	25
	Cabling	26
	Configuration	33
	Specifications	38
Chapter 3	System functions	45
	Function list	47
	Zones	49
	Areas	55
	Set and unset	57
	Inhibit and isolate	59
	Keys	61
	Bus devices	67
	Users	69
	User groups	71
	PIN	76
	Outputs	78
	Access control	79
	Condition filters	86
	Triggers	88
	Calendar	89
	Events	92
	Tests and diagnostics	94
	Alarm reporting	98
	User programmable functions	104
	Autoset	108
	Wireless device programming	109
	Using wireless cameras	116
	Engineer reset	120
	Timed unset / ATM	121
	UltraSync	122
	Mobile Application	125
	Site Manager	126

	Securing card data	127
Chapter 4	Programming	131
	Programming methods	132
	The AXON menu	133
	Programming the system using LCD keypad	135
	Programming the system using Touchscreen	140
	Programming the system using WebApp	159
	Remote access	162
	Initial start-up	163
Chapter 5	Menu reference	167
	Service	170
	Device menu	194
	User menu	219
	Zones and areas	228
	Doors Menu	256
	Outputs and filters	280
	Calendar	288
	System options	296
	Communication	329
Chapter 6	Software	363
	Connecting configuration software	364
	Upgrading AXON firmware	366
Chapter 7	Troubleshooting	371
	Recovery procedure	372
	Device troubleshooting	373
Chapter 8	Regulations	377
	Options affected by EN 50131 regulations	378
	Options affected by other regulations	384
Chapter 9	Programming maps	387
	Keypad programming map	388
	Keypad programming option list	404
	WebApp programming map	413
Appendix A	AXON events	421
Appendix B	AXON reporting codes	437
	Glossary	449
	Index	455

Important information

This document includes an overview of the product and detailed instructions explaining how to install your AXON system and program it.

To use this document effectively, you should have the following minimum qualifications:

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

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

Important note

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

List of panel variants

- ATS1700, ATS3700: Medium metal enclosure MM+

See “Specifications” on page 38 for more details on panel variant differences.

Note: Not all variants may be available.

Limitation of liability

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

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

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

Advisory messages

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

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

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

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



Safety sign identifies actions or practices that are required by EN 60950-1 Safety Standard.

Warnings and cautions



Caution: Hot parts! Risk of burn. Burned fingers when handling parts. Allow parts to cool down before handling.



WARNING! Dangerous voltage! Risk of injury or death. Fuse may be in the neutral. The mains should be disconnected to de-energize the phase conductors.



WARNING! Risk of fire, explosion, or safeguard malfunction if the battery is replaced by an incorrect type. Disposal into fire, placing into a hot oven, leaving in an extremely high temperature surrounding environment, subjecting to extremely low air pressure, mechanically crushing or cutting of a battery can result in an explosion or leakage of flammable liquid or gas.



WARNING! If the housing cover is removed, there is no safeguard against electrically caused fire that might occur during system malfunction.

The housing cover must be reassembled according to this installation instruction after each interference by a user.

Chapter 1

Quick installation and programming

Summary

The chapter contains basic steps of connection and programming of AXON control panel and auxiliary devices.

For more detailed description of the installation process, see Chapter 2 “Installation” on page 7.

For details on programming, see Chapter 4 “Programming” on page 131 and Chapter 5 “Menu reference” on page 167.

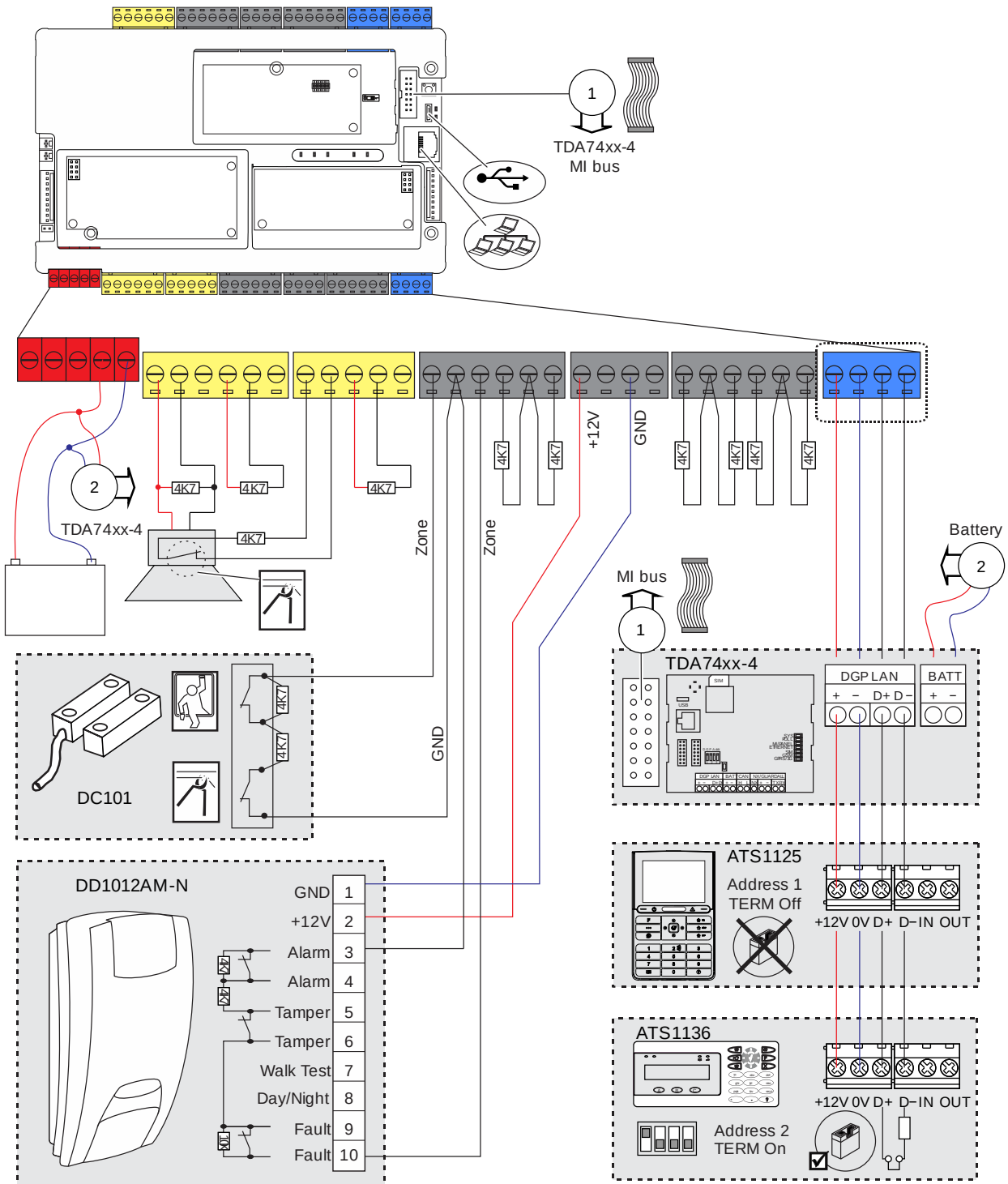
Content

Quick installation 2

Quick programming 3

Quick installation

The figure below shows an example of basic system connections.



Quick programming

Initial start-up

Note: See “The AXON menu” on page 133 for menu explanation.

Switch the panel on. The further messages and menus are listed in the table below.

Display	Instructions
INFO Inst required	Press Enter to continue
1>Panel language	Choose your language
2>Defaults	Choose the default settings compliant with your local regulations.

Caution: For EN 50131 Grade 3 compliance, choose EN 50131 Grade 3. See Chapter 8 “Regulations” on page 377 for more information.

3>Time&date	Set current time and date
4>UltraSync	Set UltraSync options

If required, enable UltraSync connectivity, and then enter UltraSync password. If UltraSync is enabled, the panel communication will be configured via security cloud.

5>Other options	Set other panel options
-----------------	-------------------------

The following options can be set:

- Duress method
- PIN length
- PIN change mode
- Battery capacity

6>Remote opts	Set remote options
---------------	--------------------

The following options can be set:

- Direct IP Protocol
- Remote login

See also “Initial start-up” on page 163.

7 Install >Cancel<	Choose OK
Change PIN Installer	Press Enter to continue
New PIN >_	Enter the new installer PIN and press Enter
Verify >_	Next, enter the PIN again to verify it.
Change PIN Supervisor	Press Enter to continue
New PIN >_	Enter the new supervisor PIN and press Enter
Verify >_	Next, enter the PIN again to verify it.

The panel restarts.

Auto configuration

Auto Config? >Yes<	Press Enter to continue.
Rkp 1-16 BUS1 R-?----- Exp 1-15 BUS1 -?-----	Wait until the panel configures all bus devices and zones.
Added R:1 D:0 Z:8	Press Enter to continue.

Enabling service in

Aritech THU 05 Mar 12:21	Enter the supervisor PIN and press Menu
1>Zone options 2 Isolate	Go to menu 8.8 Service in
8>Service in Enable?	Enable Installer in time

Press Cancel, Cancel to log off.

Programming menu entry

Aritech THU 05 Mar 12:21	Enter the installer PIN and press Menu
Inh reports >No<	Press Enter to continue

```
Inh tamper
Unset areas
```

```
1>Service menu
2 Device menu
```

The installer menu is displayed.

Changing encryption key

Caution: It is highly recommended to change the default encryption key.

Go to Encryption key 1 and Encryption key 2 (see page 356).

```
3 Encrypt.key 1
>00000000000000<
```

Provide encryption key 1.

```
4 Encrypt.key 2
>00000000000000<
```

Provide encryption key 2.

Configuring zones

Caution: Select the required object numbering scheme before programming zones. See “Object scheme” on page 320 for details.

Go to Zone menu (see page 228).

```
4>Zones&Areas
```

Press Enter.

```
1>Zone menu
```

Press Enter.

```
0>Add zone
1 Zone 1
```

Select a zone.

For each zone used in the system, enter zone name in Zone name (page 229).

```
01 Zone name
>1 Zone 1 <
```

Next, set its zone type in Zone type (see page 229).

```
02 Zone type
>Entry/Exit 1<
```

Adding users

Go to menu Users (see page 219).

```
0>Add user
1 Installer
```

Press Enter to add a user.

```
Add mode
>Manual<
```

Press Enter.

```
INFO
User added
```

```
01>User name
User 3
```

Press Enter.

```
01 User name
>User 3 <
```

Enter a new user name.

Configure other options of the user:

- PIN (page 220)
- User card (page 220)
- User groups (page 221), etc.

Repeat for other users.

When leaving the user configuration, confirm locking the user data.

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

Choose OK and confirm.

Configuring areas

Go to Areas (see page 244).

Change the area name in Area name (see page 244).

```
1 Area name
>Area 1 <
```

Enter a new area name

Configure other options of the area:

- Exit time (see page 245)
- Entry time (see page 245), etc.

Caution: Before enabling Dual unset (see page 248), make sure to add users that can assist the unset. See “Adding users” above.

Configuring Central Station

Configure the communication path in Path options (page 339).

```
1>IP
```

Select the required path and configure it depending on the hardware used.

Next, go to menu Central station (page 329).

```
0>Add CS
1 CS 1
```

Add a new CS, or choose an existing one.
Configure the following parameters:

- CS name (page 330)
- Transm path (page 330)
- Protocol (page 330)
- Accounts (page 330)
- Other options, depending on the communication path used.

Test the communication using menu Man.
test call (page 181), where <n> is the
number of the configured Central Station.

```
Calling CS 1...  
Ready
```

Regulations

If necessary, follow the instructions given in
Chapter 8 “Regulations” on page 377 to
configure other options, required by the
appropriate standards and norms.

Chapter 2

Installation

Summary

This chapter includes an overview of the product and detailed instructions explaining how to install the components of your AXON system.

Note: A qualified installer, complying with all applicable codes, should perform whatever hardware installation is required.

Content

General installation information	8
Control panel housing	8
Control panel PCB	10
Keypads and readers	14
Maintenance	19
Mains power connection	19
Battery installation	20
Battery replacement	20
Mounting	22
General installation guidelines	22
Earthing	24
Shielding	25
Cabling	26
System data bus preferred wiring	26
System data bus connection	27
Zone connection	27
Values for end-of-line resistors	29
EOL connection types	31
Siren connection	32
Other connections	32
Configuration	33
Defaulting the panel	33
Zone configuration	33
Outputs	33
Zone, output, and door addressing	34
Specifications	38
Auxiliary current and battery capacity	42

General installation information

Control panel housing

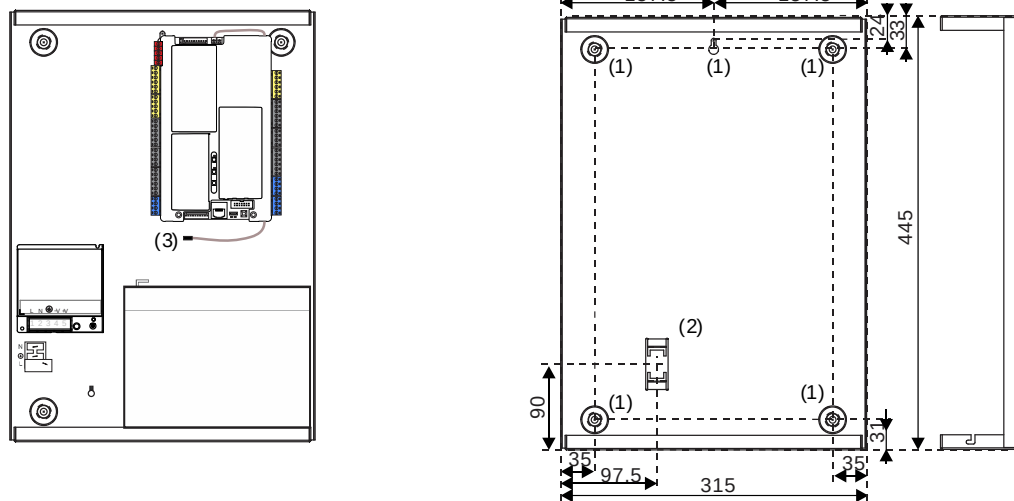
The housings with mounting holes (items 1) are shown in figures below.

Item 2 indicates the pry-off tamper wall stub location.

All dimensions are given in mm.

Figure 1

Medium metal housing (MM+)



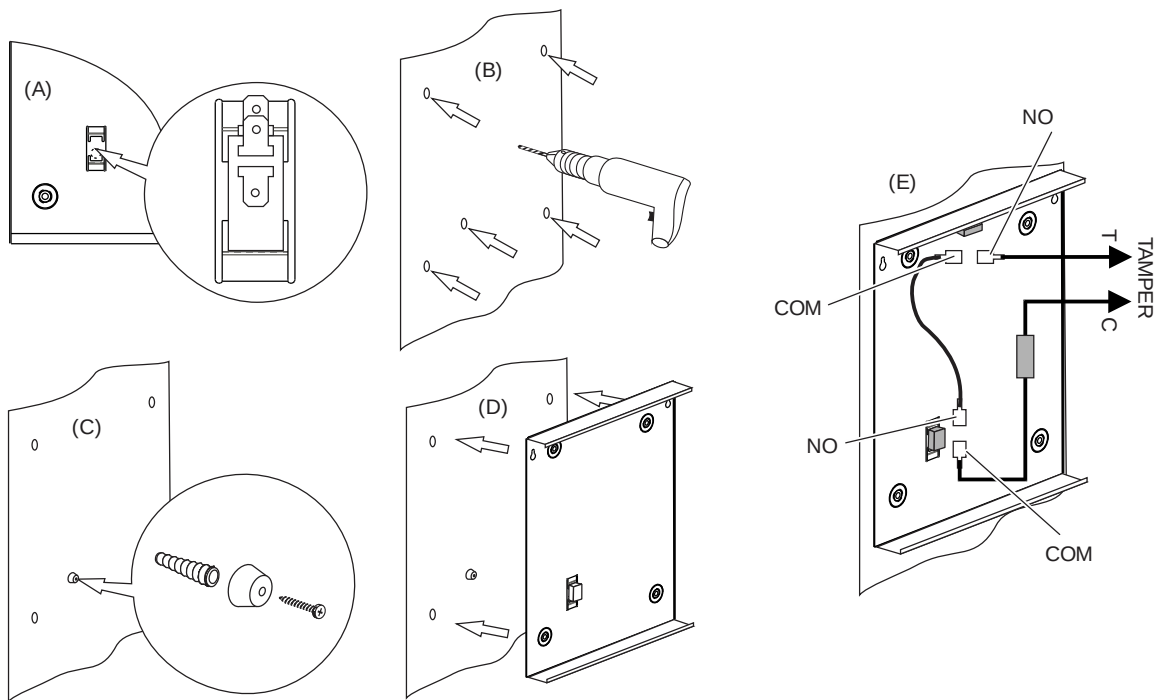
Caution: NTC temperature sensor must be mounted close to the battery and connected to the panel PCB to comply with EN 50131 requirements. The sensor socket is shown in Figure 3 on page 10 as item 2. An example of NTC temperature sensor mount is shown in Figure 1 above (item 3). The sensor is mounted inside the housing with cable ties.

For more details on connections and connecting devices to the AXON panel, see “Cabling” on page 26.

For details on connecting pry-off tampers, see “Pry-off tamper mounting” below.

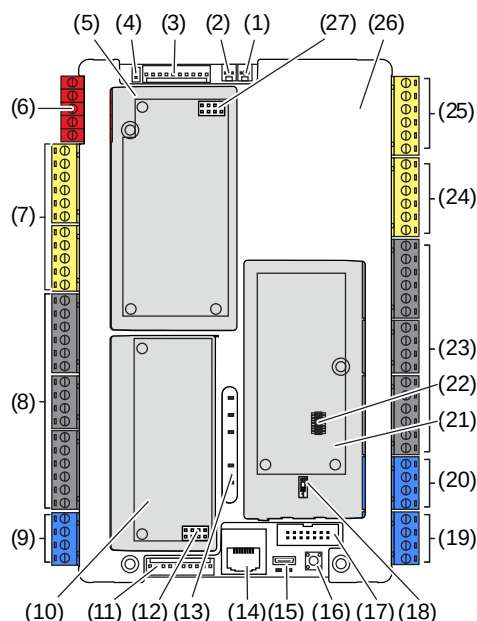
Pry-off tamper mounting

Follow the steps in Figure 2 on page 9.

Figure 2: Pry-off tamper mount

Control panel PCB

Figure 3: AXON PCB layout



- (1) Tamper contact socket
- (2) NTC temperature sensor socket
- (3) Legacy output expander interface
- (4) Jumper for legacy output expander
- (5) Output expander slot
- (6) Power supply connector
- (7) Siren connection terminals
- (8) Zone input terminals (1 to 8) and auxiliary power
- (9) Data bus 1 terminals
- (10) Input expander slot
- (11) Legacy input expander interface
- (12) Input expander interface
- (13) LEDs
- (14) Ethernet RJ-45 connector
- (15) USB connector (micro-A/B type)
- (16) PIN bypass push button
- (17) MI-bus connector for MI devices
- (18) DIP switch
- (19) Data bus 2 terminals
- (20) Data bus 3 terminals
- (21) Cellular dialler slot
- (22) Interface for add-on module
- (23) Zone input terminals (9 to 16) and auxiliary power
- (24) Relay output terminals (1 and 2)
- (25) Relay output terminals (3 and 4)
- (26) PCB cover
- (27) Output expander interface

Note: Not all connectors may be available in particular AXON panel variants. See “Specifications” on page 38 for details.

Connection terminals

Table 1: Connection terminals

Terminal block	Terminal	Description
Power supply (Figure 3, item 6)	EARTH	Earthing connection
	+24V	Power supply input
	0V	
	BATT+	
	BATT-	Battery connection
Siren connection (item 7)	SIR 12V	Siren power supply
	SIR1 OUT	Siren 1 OC output
	SIR 0V	Siren output ground
	SIR 12V	Siren 2 power supply
	SIR2 OUT	Siren 2 OC output
	SIR 0V	Siren output ground

Terminal block	Terminal	Description
	SIR TAM	Siren tamper input
	SIR 0V	Siren output ground
	SIR 12V	Siren 3 power supply
	SIR3 OUT	Siren 3 OC output
	SIR 0V	Siren output ground
Zone inputs 1 to 8 (item 8)	IN 1	Zone input 1 terminal
	C	Common terminal
	IN 2	Zone input 2 terminal
	IN 3	Zone input 3 terminal
	C	Common terminal
	IN 4	Zone input 4 terminal
	AUX +12V	Auxiliary power supply
	AUX +12V	
	AUX 0V	
	AUX 0V	
	IN 5	Zone input 5 terminal
	C	Common terminal
	IN 6	Zone input 6 terminal
	IN 7	Zone input 7 terminal
	C	Common terminal
	IN 8	Zone input 8 terminal
Data bus 1 (item 9)	DB1 +12V	Bus 1 power supply
	DB1 0V	
	DB1 +	Bus 1 data
	DB1 –	
Terminal block	Terminal	Description
Data bus 2 (item 19)	DB2 +12V	Bus 2 power supply
	DB2 0V	
	DB2 +	Bus 2 data
	DB2 –	
Data bus 3 (item 20)	DB3 +12V	Bus 3 power supply
	DB3 0V	
	DB3 +	Bus 3 data
	DB3 –	

Terminal block	Terminal	Description
Zone inputs 9 to 16 (item 23)	IN 9	Zone input 9 terminal
	C	Common terminal
	IN 10	Zone input 10 terminal
	IN 11	Zone input 11 terminal
	C	Common terminal
	IN 12	Zone input 12 terminal
	AUX +12V	Auxiliary power supply
	AUX +12V	
	AUX 0V	
	AUX 0V	
	IN 13	Zone input 13 terminal
	C	Common terminal
	IN 14	Zone input 14 terminal
	IN 15	Zone input 15 terminal
	C	Common terminal
	IN 16	Zone input 16 terminal
Relay output (1 and 2) (item 24)	R1 NO	Relay 1 output
	R1 COM	
	R1 NC	
	R2 NO	Relay 2 output
	R2 COM	
	R2 NC	
Relay output (3 and 4) (item 25)	R3 NO	Relay 3 output
	R3 COM	
	R3 NC	
	R4 NO	Relay 4 output
	R4 COM	
	R4 NC	

LEDs

Table 2: LEDs

Position	LED	Description	State
PCB cover (Figure 3, item 13)	L1 to L3	Data bus LEDs	Red blinking (1 Hz): Sending data
			Red blinking (2 Hz): Sending data on advanced high speed
			Green blinking: Receiving data

Position	LED	Description	State
	L4	System LED	Off: CPU and power supply fault Green blinking: System is OK Red on: CPU heartbeat fault Red blinking: 24 VDC power fault
	L5	Battery	Off: Battery missing Red blinking: Battery faulty Green blinking: Battery charging Green on: Battery is charged
Ethernet connector (item 14)		Ethernet LEDs	Green off: No link Green on: Link is active Green blinking: Sending or receiving data Yellow off: Port speed is 10 Mbps Yellow on: Port speed is 100 or 1000 Mbps
USB connector (item 15)		USB LEDs	Off: No connection Red on: USB fault Green on: USB active

DIP switch

See Figure 3, item 18.

1. RESCUE: Use for firmware upgrade. See “Upgrading AXON firmware” on page 366 for details.

Keypads and readers

Figure 4: ATS111xA keypad

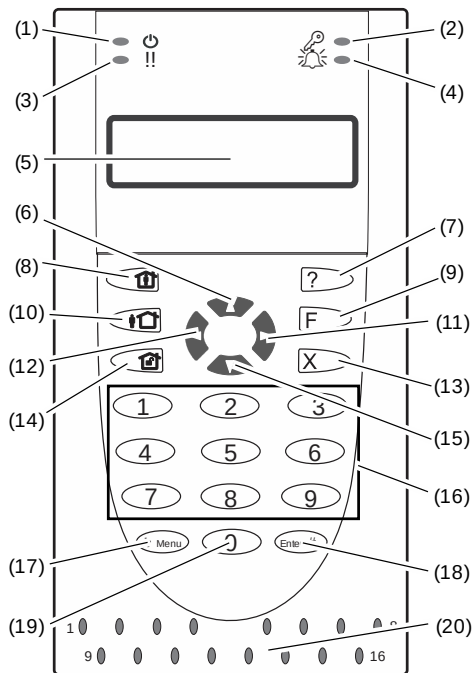


Figure 5: ATS1125 keypad

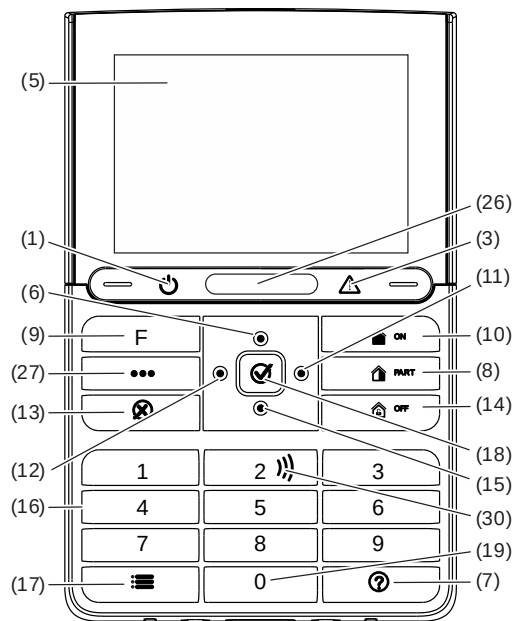


Figure 6: ATS113x keypad

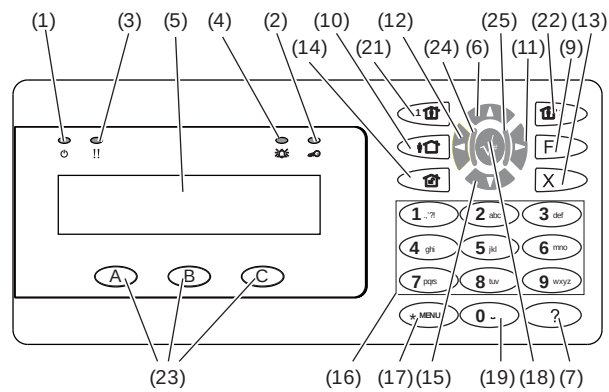
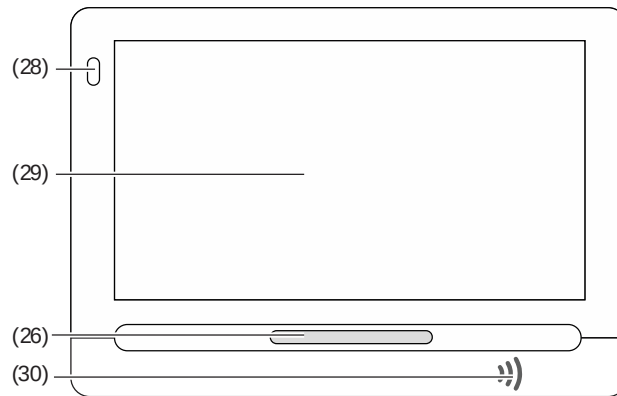
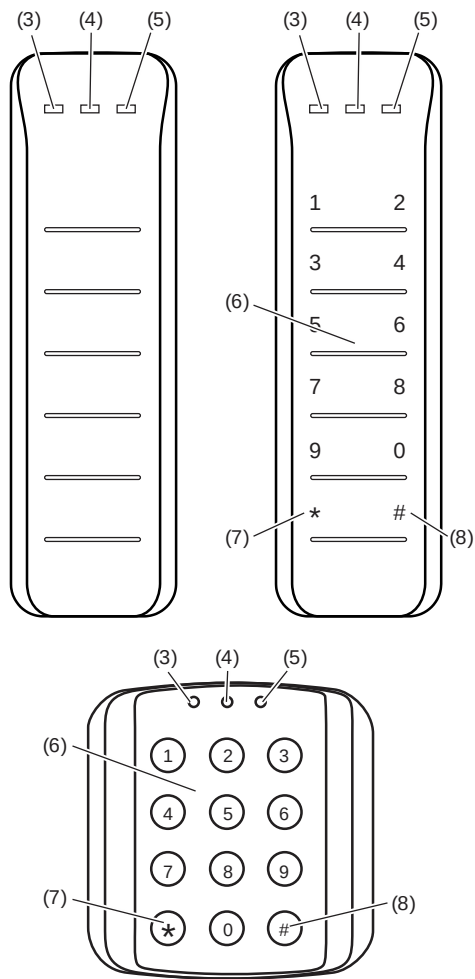
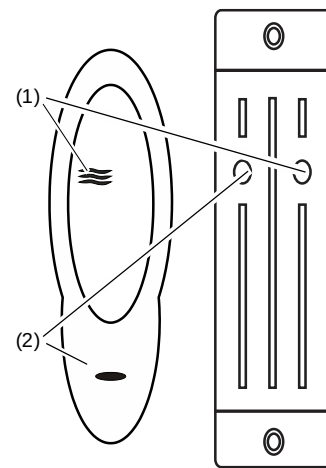
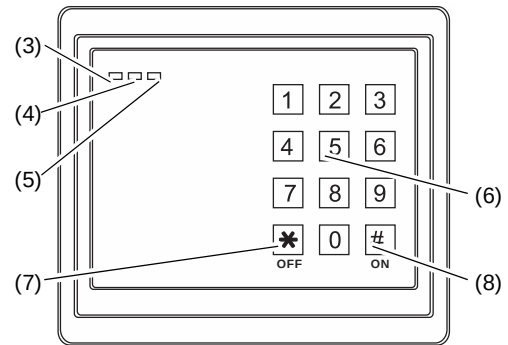
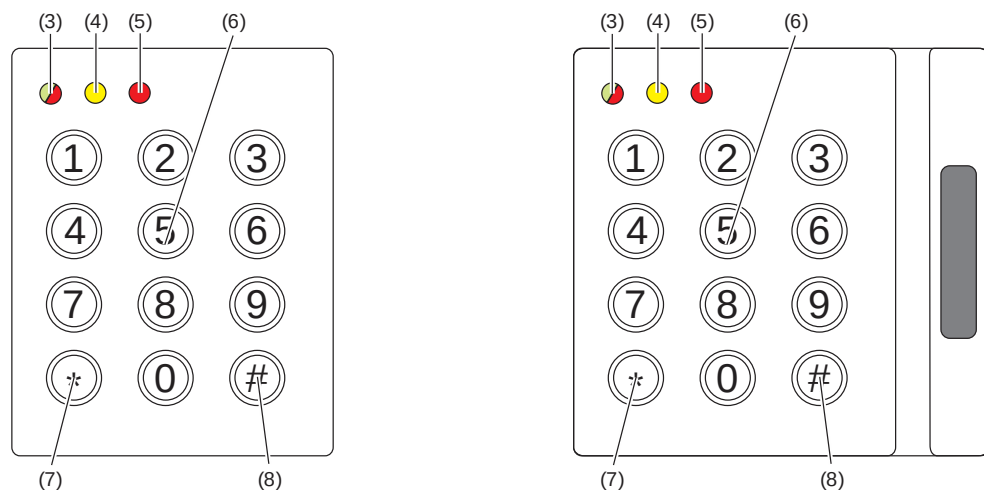


Figure 7: ATS1140 Touchscreen

(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. See "Keypad layout" on page 139.
(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 18. 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
(28)	Presence sensor	Detects the user presence in front of the touchscreen, and wakes up the device (if configured).
(29)	Touchscreen display	Displays graphical user interface. Allows you to control and program the security system.
(30)	Mifare card reader	Mifare card reader active area

Figure 8: ATS118x readers**Figure 9: ATS1190/ATS1192 readers****Figure 10: ATS1197 reader with keypad****Figure 11: 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. See “Non LCD RAS Orange LED Indication” on page 326. Flashing: general alert (EN 50131) ATS125x: always on CDC4(-EN): 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.



Maintenance

The intrusion control panel is only allowed to be serviced by dedicated service personal. The screw of the housing is intended to protect the product from unintended use.

To open the housing, remove the housing screw and open the cover.

After the maintenance, replace the cover and fix it with the cover screw.



Mains power connection

Electrical installation should be carried out by a skilled person.

Solid insulation of the building mains cables should meet the technical and the environmental specifications of the equipment.

Wire insulation of cables connected to the equipment must conform to IEC 60332-1-2 and IEC 60332-1-3 or IEC 60332- 2-2, depending on the wire cross-sectional area, or IEC TS 60695-11-21, regardless of cross-sectional area.

Alternatively, such wires must comply with UL 2556 VW-1. Appropriate wire cross-sectional area must be selected to withstand 2 A current.

Use the mains connector terminal for connecting the AC mains supply. A fixed cable or flexible mains lead to earthed mains outlet can be used. When fixed wiring is used, insert a dedicated all-pole circuit breaker in the power distribution network. In all cases the mains connection must comply with local regulations.

Always connect the building protective earthing wire and ensure the connection is reliable. See also “Earthing” on page 24.

In case the panel is connected to the power grid using fixed wiring, it is recommended that earth wire is longer than line and neutral.

Do connect incoming line and neutral to mains connection block according to the label. This assures that the line will be protected by the mains fuse, and that service can be done by service personnel.

Make sure that before connecting the mains power, the mains power supply is disconnected.

When installing the mains power, use strain reliefs such as cable ties and coupling PG16s to ensure proper wiring and minimize the risk of wire damage during installation and use. If product entry hole breakouts are used, it is required to also make use of UL-V2 (or better) approved PG16 cable gland. Refer to PG16 specification to meet minimum and maximum cable diameters.

In all cases local regulations must be observed.

WARNING: Electrocution hazard. To avoid personal injury or death from electrocution, remove all sources of power and allow stored energy to discharge before installing or removing equipment.

Battery installation

WARNING! Using incorrect types of batteries may cause risk of fire, explosion or chemical leakage. Use only types of batteries listed in “Power supply specifications” on page 38

To install the battery, do the following:

1. Make sure that your product settings allow you to open its cover without starting the tamper alarm.
 2. Make sure that the mains power is off, and remove the cover.
 3. If necessary, remove the battery shield, unscrewing four screws.
 4. Connect the battery, sliding the product wires on the wire connectors. Note that depending on the battery model, the connectors can be located differently.
 5. Mount the battery shield using four screws.
-

WARNING! The battery shield must be mounted during normal device operation.

Note: After every battery installation or replacement it is necessary to set battery capacity in the control panel settings. See “Battery capacity” on page 188 for details.

Battery replacement

This product may contain one (or more) sealed, rechargeable, BS-type lead-acid battery. Because removing the battery may affect the product configuration settings or trigger an alarm, only a qualified installer should remove the battery.

To remove the battery, do the following:

1. Make sure that your product settings allow you to open its cover without starting the tamper alarm.
2. Switch off the mains power, if necessary, and remove the cover.
3. If necessary, remove the battery shield, unscrewing four screws.
4. Disconnect the battery, sliding the product wires off the wire connectors. Note, that depending on the battery model, the connectors can be located differently.
5. Remove the battery from the holder.

For proper recycling, dispose of all batteries as required by local ordinances or regulations.

See the specifications for your product or contact technical support for information on replacement batteries.

Note: After every battery installation or replacement it is necessary to set battery capacity in the control panel settings. See “Battery capacity” on page 188 for details.

Mounting

The unit is mounted with screws or bolts through the mounting holes in the rear section of the enclosure.



Important: When the product is mounted to the wall, assure that at least 3 times the weight of the product can be supported. The product weight is the product itself plus battery and accessories.

Ensure that the unit is mounted on a flat, solid, vertical surface such that the base will not flex or warp when the mounting screws and bolts are tightened.

Leave a 50 mm clearance between equipment enclosures mounted side by side and 25 mm between the enclosure and the sidewall.

The rechargeable battery must not be fitted until the control panel is secured to the fixing surface. Under no circumstances should the panel be transported with a battery fitted.

Take care that wire terminals are isolated. The use of cable ties to neatly secure cables is recommended.

WARNING! Use cables that comply with IEC 60332-1-2 and IEC 60332-1-3, or IEC 60332-2-2, or IEC TS 60695-11-21, or UL 2556 VW-1.

Use cables and connections that can withstand at least 2 A current.

General installation guidelines

The AXON control panels have been designed, assembled, and tested to meet the requirements of current relevant standards for safety, emission, and immunity to environmental electrical and electromagnetic interference.

If the following guidelines are followed, the system will give many years of reliable service.

In addition to the following guidelines, during the installation of the AXON control panel, it is essential to follow any country-dependent local standard requirements applicable to the installation. Only a qualified electrician or other suitably trained and qualified person should attempt to wire this system to the AC mains or to the public telephone network.

- Ensure that there is a good earth available for the alarm system.
- Maintain a separation between low voltage and mains supply cables. Use separate points of cable entry to the control panel cabinet.
- If the upper and/or lower cabinet entry cable holes are used to route wiring into the control panel, always use a proper pipe fitting system by means of an appropriate conduit and junction box. For this purpose, use only materials of suitable flammability class (HB or better).

- For mains power connection, use the mains connector terminal either through a permanent wiring or a flexible mains cable to an earthed mains outlet. Always use cable ties to fix the mains cable at the dedicated fixing point provided near the mains terminal connector.
 - When installing permanent, fixed wiring, insert an easily accessible, dedicated all-pole circuit breaker in the power distribution network.
 - Never attempt to solder mains connection wires at the ends where they will be wired to the terminal connectors.
- Avoid loops of wire inside the control panel cabinet and route cables so that they do not lie on top or underneath of the printed circuit board. The use of cable ties is recommended and improves neatness of the wiring within the box.
- The battery used with this unit, must be made of materials of suitable flammability class (HB or better).
- Any circuit connected either directly to the onboard relay contacts or to the external relay contacts through the onboard electronic output must be rated as a SELV (safety extra-low voltage) operating circuit.
 - A mains switching relay must not be fitted inside the control panel cabinet.
 - Always place a suppression diode (1N4001) across the relay coil.
 - Use only relays with good insulation between the contacts and the coil.
 - Maximum cable length for open collector output connection may not exceed 30 m. For longer distances, use a relay.
- Only use these units in a clean environment and not in humid air. Environmental requirements are given in “Specifications” on page 38.
- For the panel terminal connections, the recommended torque is 0,3 to 0,4 N·m. This torque setting is independent from the AWG (thickness) of the wires used. A value of 0,4 N·m is also the maximum allowed torque for this connector.

Earthing

WARNING: The correct earthing procedures must be followed.

Earthing of one cabinet containing several devices

All devices designed for the system have earth connections via metal studs to the metal housing. Make sure that these metal studs make good connection to the housing (beware of paint). The earth connections of every piece of equipment in the system can be used for connecting the screen of shielded cables. Ensure that all internal protective bonding wires make reliable connection with the building protective earthing wire.

Earthing panels in a single building

In one building several cabinets or devices are earthed to a safety ground.

The safety ground for the building must be checked by a licensed contractor.

Earthing panels in more buildings

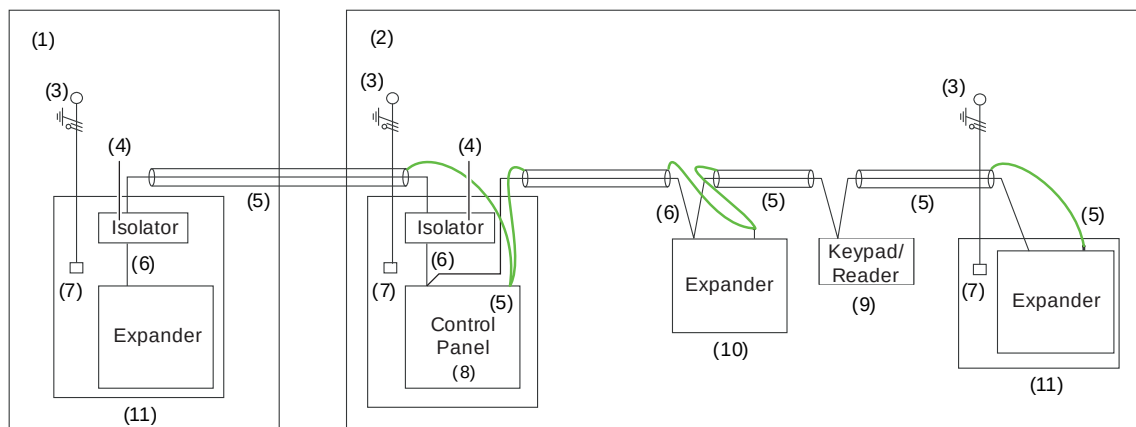
If the wiring extends to separate buildings, more than one common earth system will be used. Use ATS1740 isolator/repeaters to isolate the system data bus. In this way the system is protected against variations in earth potential.

Shielding

The shielding of all shielded cables used in the system should only be connected at one side to one common earthing point in a building (see Figure 12 below). If a shielded data bus cable is routed via more than one plastic device the shielding from incoming and outgoing cable must be connected.

In case the IP connection is used, take care that the Ethernet FTP cable remains within a single building. Do make use of a proper router or switcher to isolate Ethernet cables between various buildings.

Figure 12: System shielding



- | | |
|---|---|
| (1) Building 1 | (8) AXON control panel |
| (2) Building 2 | (9) Keypad / reader (for example, ATS1125 or ATS1136) |
| (3) Mains power with local earth | (10) Remote expander in plastic housing (for example, ATS1210E) |
| (4) Bus isolator (for example, ATS1740) | (11) Remote expander in metal housing (for example, ATS1201E) |
| (5) Earth and shielding | |
| (6) System data bus | |
| (7) Mains power connector | |

Cabling

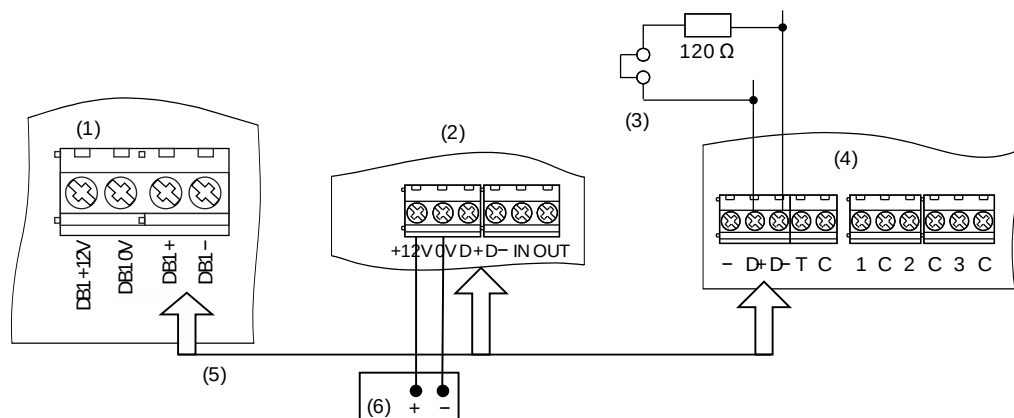
System data bus preferred wiring

The terminator jumper (also called TERM link), or DIP switch must be ON, or a 120 Ω resistor must be fitted on the devices installed at the extreme ends of the data bus.

Caution: Star configuration of any data bus is not recommended.

In the control panel you can activate built-in predefined data bus EOL using menu “Databus EOL termination” on page 218.

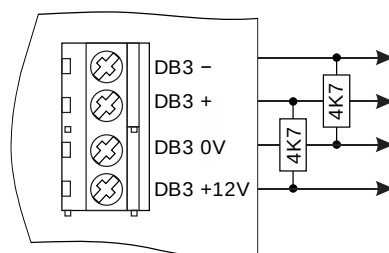
Figure 13: System data bus wiring



- | | |
|--|--|
| (1) AXON control panel variants. | (5) Preferred data cable type is WCAT 52 (two twisted pairs). |
| (2) LCD keypad (TERM is set to OFF). | (6) Separate 12 V power supply (required if keypad is more than 100 m from the nearest panel or expander. Connect the negative terminal of the power supply to the “-” wire of the data bus. |
| (3) TERM link fitted (last device on local data bus). | |
| (4) Any remote expander like ATS1201(E) or ATS1210(E). | |

Note: BUS3 data bus must be terminated on the control panel data bus connection block with two resistors 4.7 k Ω connected between the following terminals:

- DB3 +12V and DB3 +
- DB3 0V and DB3 -



System data bus connection

The system data bus is used to connect remote expanders (to provide extra zones) and keypads to the AXON control panel. Remote devices can be up to 1.5 km from an AXON control panel.

Keypads and remote expanders must be connected via a shielded data cable with two twisted pairs from the system data bus connection (WCAT 52 is recommended).

We recommend that you use a separate power supply for a keypad when the distance between that keypad and the nearest device is more than 100 meters. See the appropriate installation manual for information on the required power supply specifications.

If the keypad is powered with a separate power supply, do not connect “+” from the system data bus. Connect “+” of the local power supply to “+” on the keypad, and connect 0 volts from the power supply and 0 volts from the system data bus to the keypad terminal marked “-”. The maximum number of devices allowed on the data bus is given in “General features” on page 39.

Zone connection

The inputs are set up as standard EOL freely programmable zones. However, by programming the zones as dual loop, zone inputs can be programmed to give a few states indication for the same zone.

Note: Zone connection type and EOL can be configured:

- Individually for each onboard zone
- Individually for each zone on internal zone expander card
- For all zones in each external zone expander.

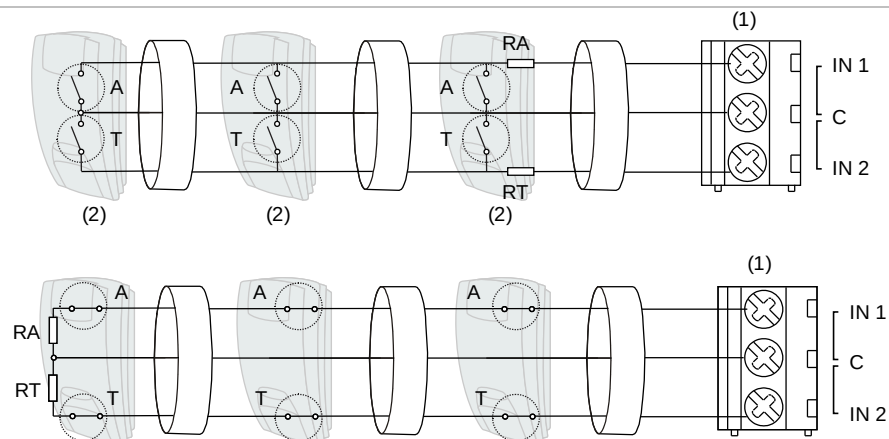
Depending on the detector model, do the following to set up zones:

- Choose your EOL connection type. See “EOL connection types” on page 31.
- Program input modes. See “Input mode” on page 239 for panel inputs and internal input expanders, or “Input mode” on page 207 for remote expanders.
- Set end-of-line resistor values. See “End of line resistor” on page 240 for panel inputs and internal input expanders, or “End of line resistor” on page 207 for remote expanders.
- Configure anti-masking option. See “Anti mask” on page 232.

Single loop zone wiring

In single loop zone wiring, two zones are required, one zone for alarm and one zone for tamper. The tamper contacts are wired in series with an EOL resistor.

Figure 14: Single loop examples



- (1) Zone terminal
 C Common terminal
 Z1 Zone 1 input
 Z2 Zone 2 input

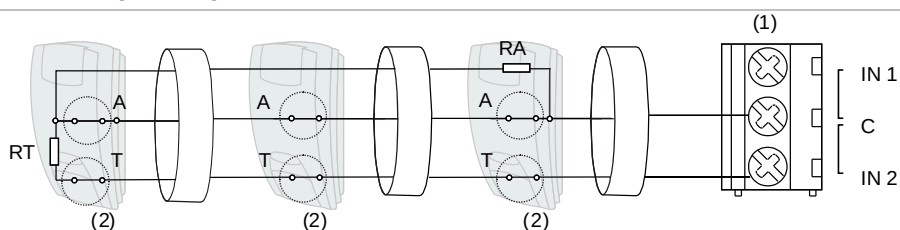
- (2) Detector
 A Alarm relay
 T Tamper relay

Dual loop zone wiring

In dual loop wiring, one zone can detect a few detector states. At least two resistors are used to define alarm and tamper states. Depending on the programmed settings, there can be additional states defined as masking alarm or sensor fault. These states can be the following:

- Short (tamper)
- Active (alarm)
- Normal
- Masking
- Sensor fault
- Open (tamper)

Figure 15: Dual loop example



- (1) Zone terminal
 C Common terminal
 Z1 Zone 1 input
 Z2 Zone 2 input

- (2) Detector
 A Alarm relay
 T Tamper relay

Possible EOL connections are listed in “EOL connection types” on page 31.

Values for end-of-line resistors

The following list contains the values for end-of-line resistors and possible zone states. Both the resistance and the voltage measured across the zone are shown.

Depending on the input type and anti-masking option, the following EOL values can be available.

EOL	Connection details [1]	Measure [2]	Zone state					
			Short	Masking	Normal	Alarm	Fault	Open
Single NC	(Item 1)							
No EOL		R (kΩ)	—	—	<1	>1	—	—
		U (V)	—	—	<3.5	>3.5	—	—
Note: Values for other EOL are equal to Dual, except all ranges but normal are alarm ranges.								
Single NO	(Item 2)							
No EOL		R (kΩ)	—	—	>55	<55	—	—
		U (V)	—	—	>11.14	<11.14	—	—
Note: Values for other EOL are equal to Dual, except all ranges but normal are alarm ranges.								
Dual								
10K	(Item 4)	R (kΩ)	<3.33	3.33–6.67	6.67–13.33	13.33–26.67	—	>26.67
RA=10 kΩ, RT=5 kΩ, RF=5 kΩ		U (V)	<5.70	5.70–8.10	8.10–10.20	10.20–11.70	—	>11.70
4K7	(Item 3)	R (kΩ)	<1.00	—	1.00–6.67	6.67–16.84	—	>16.84
RA=4.7 kΩ, RT=4.7 kΩ		U (V)	<2.41	—	2.41–8.07	8.07–10.74	—	>10.74
4K7	(Item 4)	R (kΩ)	<1.00	1.00–3.42	3.42–6.67	6.67–16.84	—	>16.84
RA=4.7 kΩ, RT=2.35 kΩ, RF=2.35 kΩ		U (V)	<2.41	2.41–5.79	5.79–8.07	8.07–10.74	—	>10.74
4K7	(Item 7)	R (kΩ)	<1.00	16.84–55.00	1.00–6.67	6.67–11.75	11.75–16.84	>55.00
RA=4.7 kΩ, RT=4.7 kΩ, RF=10 kΩ		U (V)	<2.41	10.74–12.70	2.41–8.07	8.07–9.82	9.82–10.74	>12.70
2K2	(Item 4)	R (kΩ)	<0.73	0.73–1.47	1.47–2.93	2.93–5.87	—	>5.87
RA=2.2 kΩ, RT=1.1 kΩ, RF=1.1 kΩ		U (V)	<1.90	1.90–3.30	3.30–5.30	5.30–7.70	—	>7.70

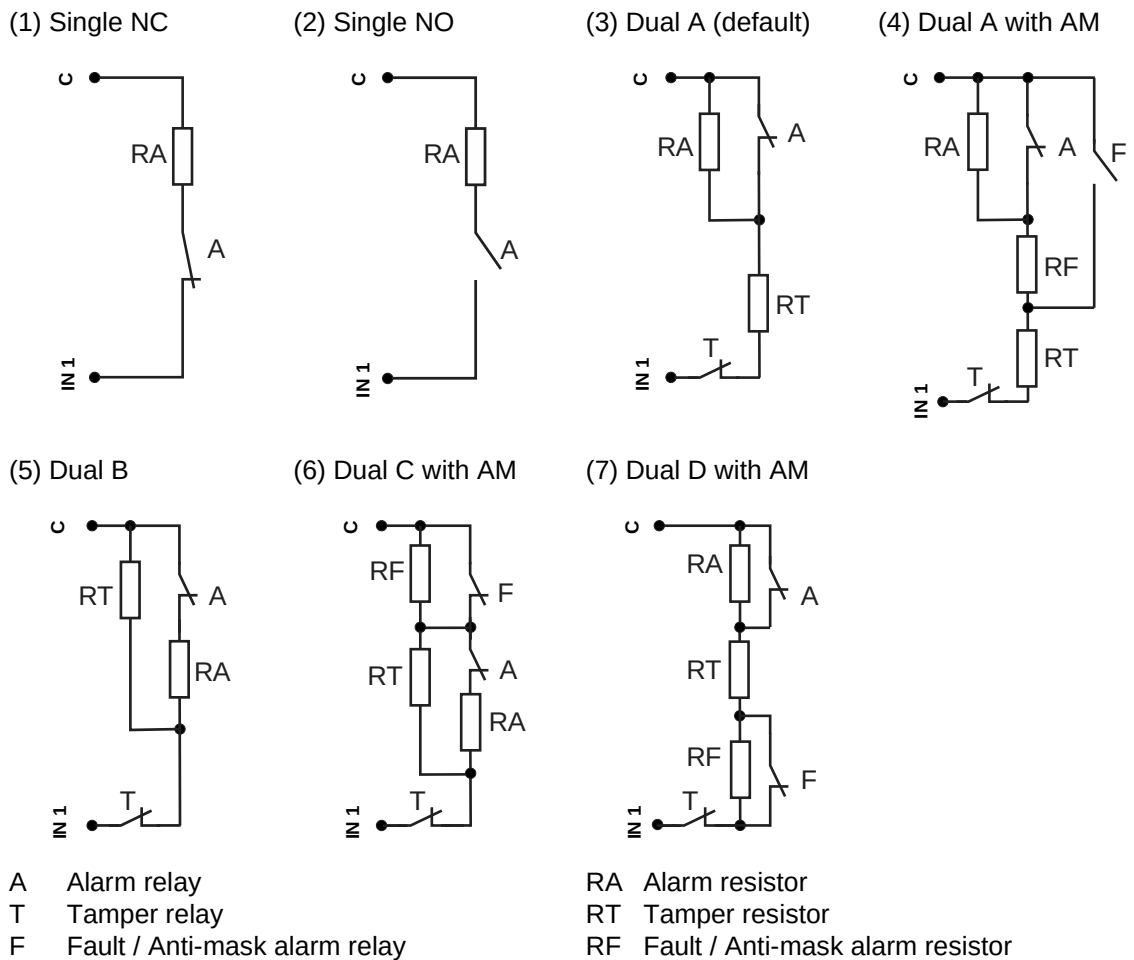
EOL	Connection details [1]	Zone state						
		Measure [2]	Short	Masking	Normal	Alarm	Fault	Open
6K8	(Item 4)	R (kΩ)	<2.27	2.27– 4.53	4.53– 9.07	9.07– 18.13	—	>18.13
	RA=6.8 kΩ, RT=3.4 kΩ, RF=3.4 kΩ	U (V)	<4.50	4.50– 6.80	6.80– 9.10	9.10– 11.00	—	>11.00
5K6	(Item 4)	R (kΩ)	<1.87	1.87– 3.73	3.73– 7.47	7.47– 14.93	—	>14.93
	RA=5.6 kΩ, RT=2.8 kΩ, RF=2.8 kΩ	U (V)	<3.90	3.90– 6.10	6.10– 8.50	8.50– 10.50	—	>10.50
3K74	(Item 4)	R (kΩ)	<1.25	1.25– 2.45	2.45– 4.99	4.99– 9.98	—	>9.98
	RA=3.74 kΩ, RT=1.87 kΩ, RF=1.87 kΩ	U (V)	<2.90	2.90– 4.80	4.80– 7.10	7.10– 9.40	—	>9.40
3K3	(Item 4)	R (kΩ)	<1.10	1.10– 2.20	2.20– 4.40	4.40– 8.80	—	>8.80
	RA=3.3 kΩ, RT=1.65 kΩ, RF=1.65 kΩ	U (V)	<2.60	2.60– 4.40	4.40– 6.70	6.70– 9.00	—	>9.00
2K	(Item 4)	R (kΩ)	<0.67	0.67– 1.33	1.33– 2.67	2.67– 5.33	—	>5.33
	RA=2 kΩ, RT=1 kΩ, RF=1 kΩ	U (V)	<1.70	1.70– 3.00	3.00– 5.00	5.00– 7.30	—	>7.30
1K5	(Item 4)	R (kΩ)	<0.50	0.50– 1.00	1.00– 2.00	2.00– 4.00	—	>4.00
	RA=1.5 kΩ, RT=0.75 kΩ, RF=0.75 kΩ	U (V)	<1.30	1.30– 2.40	2.40– 4.10	4.10– 6.30	—	>6.30
2K2+4K7	(Item 3)	R (kΩ)	<3.60	—	3.60– 5.60	5.60– 8.20	—	>8.20
	RA=2.2 kΩ, RT=4.7 kΩ	U (V)	<6.00	—	6.00– 7.50	7.50– 8.80	—	>8.80
1K	(Item 7)	R (kΩ)	<0.51	4.52– 40.00	0.51– 1.52	1.52– 2.94	2.94– 4.52	>40.00
	RA=1 kΩ, RT=1 kΩ, RF=12 kΩ	U (V)	<1.35	6.24– 12.33	1.35– 3.36	3.36– 5.29	5.29– 6.74	>12.33
8K2	(Item 5)	R (kΩ)	<1.50	—	1.50– 5.84	5.84– 14.25	—	>14.25
	RA=8.2 kΩ, RT=8.2 kΩ	U (V)	<3.33	—	3.33– 7.52	7.52– 10.33	—	>10.33
8K2	(Item 6)	R (kΩ)	<1.50	14.25– 45.00	1.50– 5.84	5.84– 10.07	10.07– 14.25	>45.00
	RA=8.2 kΩ, RT=8.2 kΩ, RF=8.2 kΩ	U (V)	<3.33	10.33– 12.48	3.33– 7.52	7.52– 9.37	9.37– 10.33	>12.48

- [1] Refer to Figure 16 below.
- [2] Zone resistance R (k Ω), zone voltage U (V).
- The state is not available

EOL connection types

The following EOL connections are used for different input types and EOL values. See “Values for end-of-line resistors” on page 29 for more details.

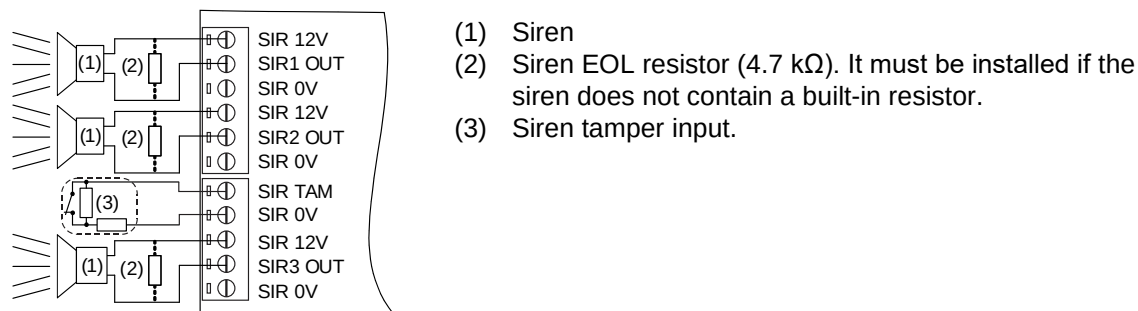
Figure 16: Connection type



Caution: When using connection types (4), (6) and (7), the antimask option of the zone must be enabled. Other zones must have this option disabled. See “Anti mask” on page 232.

Siren connection

Figure 17: Siren connection examples



Siren tamper input is connected in the same way as zone inputs, but configured separately. For the siren tamper input configuration, see “Siren options” on page 322.

Caution: If the siren output is in a LOW state, the system cannot monitor this output circuit for tamper conditions. The siren outputs are in LOW state when:

- The outputs are On, and Invert is set to Off
- The outputs are Off, and Invert is set to On

Note: Siren output can be configured as internal or external. This is accomplished via panel settings, not by configuring the panel hardware. See “Default output assignments” on page 34 and “Outputs” on page 78.

Other connections

Ethernet connection

The Ethernet port is an IEEE 802.3u based connection supporting 10BASE-T or 100BASE-TX link speeds.

Use only FTP Cat 5e type cable or better for Ethernet connections.

Configuration

Defaulting the panel

When the panel is initially powered up, you are prompted to choose the appropriate default settings. Choose the correct settings for your local regulations. The panel then completes the installation process. See “Initial start-up” on page 163.

Note: At least one keypad with an LCD should be connected to the system data bus.

Zone configuration

Internal expansion

The number of zones connected directly to the control panel can be extended using the ATS608 module. The maximum internal zone capacity for each control panel is shown in “Specifications > General features” on page 39.

External expansion

Expanders can be used to expand the AXON control panels with external zones. The maximum zone number for each control panel is listed in “Specifications > General features” on page 39.

A standard expander can have eight zones connected to it. Some of them can be expanded in increments of 8, up to 32, so an expander can have 8, 16, 24 or 32 zones.

Note: Zone capacity is the number of configurable zones in the system. These zones may be located at any available input. See “Specifications > General features” on page 39.

Outputs

Depending on the panel variant, there are 4 or 5 outputs on the panel PCB. Internal output expander can be used to add another 16 outputs inside the panel.

Internal output expanders are also used to expand the number of outputs on a remote expander. An internal output expander expands the outputs by 4 or 8. A remote expander can have two internal output expanders connected, increasing the outputs to a maximum of 16 per remote expander.

A keypad can have only one output in current panel version.

The maximum output number for each control panel is shown in “Specifications > General features” on page 39.

Note: Set keypad output 7 to activate continuous keypad buzzer sound, or output 8 to activate intermittent sound.

Siren outputs

The siren outputs on the AXON control panel have addresses starting from 1 (see Table 3 below).

On expanders with siren speaker outputs, output 16 is the siren output.

To enable the siren output, the programmed output must have the required condition filter assigned (defined by an alarm event or a siren event, depending on the preference settings). See “Outputs” on page 78 for more details.

Default output assignments

The default output assignments are shown in Table 3 below.

Table 3: Default output assignments

Output	Name	Type	Default output function
Panel 1	S1	High current output	EN 50131 Grade 3: Internal siren output S1 VdS: External siren output S1
Panel 2	S2	High current output	EN 50131 Grade 3: External siren output S2 VdS: External siren output S2
Panel 3	S3	High current output	EN 50131 Grade 3: Programmable siren output VdS: External strobe output S3
Relay 1	R1	Relay	Depends on default settings. See also “Defaults” on page 190.
Relay 2	R2	Relay	Depends on default settings. See also “Defaults” on page 190. Note: Relay 2 is available in ATS3700 only.
Keypad 7	—	Virtual	Continuous buzzer sound
Keypad 8	—	Virtual	Intermittent buzzer sound

Note: Output assignments may require adjustment to comply with EN 50131.

Zone, output, and door addressing

Zones and outputs

Table 4 below shows the zone and output addressing in the AXON system.

Note: This is the default numbering in a classic numbering scheme. To change it and create objects with numbering independent on physical inputs or outputs, use menu “Object scheme” on page 320.

Table 4: Zone and output numbering

Device	Zones	Outputs	Device	Zones	Outputs
Panel	1–16	1–8	Internal output expanders	—	9–48 [2]
Input expander (ATS608, ATS1202)	17–48	—	See Table 5 on page 35 for details on expander modules.		

Device	Zones	Outputs	Device	Zones	Outputs
Expander 1	17–48	17–48	Keypad 1	—	1001–1008
Expander 2	49–80	49–80	Keypad 2	—	1009–1016
Expander 3	81–112	81–112	Keypad 3	—	1017–1024
Expander 4	113–144	113–144	Keypad 4	—	1025–1032
Expander 5	145–176	145–176	Keypad 5	—	1033–1040
Expander 6	177–208	177–208	Keypad 6	—	1041–1048
Expander 7	209–240	209–240	Keypad 7	—	1049–1056
Expander 8	241–272	241–272	Keypad 8	—	1057–1064
Expander 9	273–304	273–304	Keypad 9	—	1065–1072
Expander 10	305–336	305–336	Keypad 10	—	1073–1080
Expander 11	337–368	337–368	Keypad 11	—	1081–1088
Expander 12	369–400	369–400	Keypad 12	—	1089–1096
Expander 13	401–432	401–432	Keypad 13	—	1097–1104
Expander 14	433–464	433–464	Keypad 14	—	1105–1112
Expander 15	465–480 [1]	465–496	Keypad 15	—	1113–1120
			Keypad 16	—	1121–1128

[1] Inputs 17 to 32 of Expander 15 cannot be used.

[2] Output 17 to 48 states are duplicated on output expanders and external expander 1.

Table 5: Internal output expander configuration

Device	Outputs	Note
ATS624 installed on the main board (see Figure 3, item 27)	9–12	
ATS624 + 1X ATS1810 [1]	9–16	ATS1810 is connected to ATS624 legacy expander interface
ATS626 installed on the main board	9–16	
ATS626 + 2X ATS1810	9–24	ATS1810 is connected to ATS626 legacy expander interface
2X ATS1810 connected to the legacy expander interface (see Figure 3, item 3)	25–32	Clocked outputs must be set to Off. See “Clocked outputs” on page 327.
4X ATS1811 connected to the legacy expander interface	17–48	Clocked outputs must be set to On. See “Clocked outputs” on page 327.
2X ATS1820 connected to the legacy expander interface	17–48	Clocked outputs must be set to On. See “Clocked outputs” on page 327.

[1] When using ATS624 relay card with the ATS1810 expander attached, expander output 8 state is inverted.

Doors

There are two types of doors, intelligent and standard. Standard doors (1 to 16) are handled by the control panel. Keypads or readers 1 to 32 connected to the AXON control panel data buses are used for standard access control functions.

Intelligent doors (17 to 64) are controlled by door controllers. Keypads or readers connected to local data buses of door controllers are named “door controller readers (DC readers)” and are used for advanced access control functions.

See “Doors” on page 79 for more details.

Table 6 below shows the door, zone, and output numbering for door controllers.

Table 6: Door, zone, and output numbering in door controllers

Door controller	Doors	Zones	Outputs
1	17–20	17–48	17–48
2	21–24	49–80	49–80
3	25–28	81–112	81–112
4	29–32	113–144	113–144
5	33–36	145–176	145–176
6	37–40	177–208	177–208
7	41–44	209–240	209–240
8	45–48	241–272	241–272
9	49–52	273–304	273–304
10	53–56	305–336	305–336
11	57–60	337–368	337–368
12	61–64	369–400	369–400

Table 7 below shows the default zone and output assignment for door controllers.

Table 7: Default zone and output assignment in door controllers

Function	Door	Door controller											
		1	2	3	4	5	6	7	8	9	10	11	12
Unlock relay	1st door	17	49	81	113	145	177	209	241	273	305	337	369
	2nd door	18	50	82	114	146	178	210	242	274	306	338	370
	3rd door	19	51	83	115	147	179	211	243	275	307	339	371
	4th door	20	52	84	116	148	180	212	244	276	308	340	372
Zone no	1st door	17	49	81	113	145	177	209	241	273	305	337	369
	2nd door	19	51	83	115	147	179	211	243	275	307	339	371
	3rd door	21	53	85	117	149	181	213	245	277	309	341	373
	4th door	23	55	87	119	151	183	215	247	279	311	343	375

Function	Door	Door controller											
		1	2	3	4	5	6	7	8	9	10	11	12
DOTL zone no	1st door	17	49	81	113	145	177	209	241	273	305	337	369
	2nd door	19	51	83	115	147	179	211	243	275	307	339	371
	3rd door	21	53	85	117	149	181	213	245	277	309	341	373
	4th door	23	55	87	119	151	183	215	247	279	311	343	375
Request to exit zone no	1st door	18	50	82	114	146	178	210	242	274	306	338	370
	2nd door	20	52	84	116	148	180	212	244	276	308	340	372
	3rd door	22	54	86	118	150	182	214	246	278	310	342	374
	4th door	24	56	88	120	152	184	216	248	280	312	344	376
Shunt zone no	1st door	17	49	81	113	145	177	209	241	273	305	337	369
	2nd door	19	51	83	115	147	179	211	243	275	307	339	371
	3rd door	21	53	85	117	149	181	213	245	277	309	341	373
	4th door	23	55	87	119	151	183	215	247	279	311	343	375

Table 8 below shows the default assignment of door controller local data bus readers to specific doors.

Table 8: Default reader assignment in door controllers

Reader function	IN reader	IN reader 2	OUT reader	OUT reader 2
1st door	1	5	9	13
2nd door	2	6	10	14
3rd door	3	7	11	15
4th door	4	8	12	16

Specifications

For a list of panel models see “List of panel variants” on page iii.

Mains power specifications

Mains input voltage	230 VAC +10%, –15%, 50 Hz
Current consumption at 230 VAC ATS1700 ATS3700	650 mA max. 800 mA max.
Power supply unit output	24 VDC, 3.2 A, 75 W

Power supply specifications

Power supply type	Type A per EN 50131-6 Note: Power supply is not suitable for use outside of the supervised premises.
Power supply input voltage [1]	24 VDC $\pm$ 1 V
Maximum power supply current (full load) ATS1700 ATS3700	2.6 A at 24 V (PSU), 3.1 A at 12 V (battery) 3.1 A at 24 V (PSU), 3.9 A at 12 V (battery)
Maximum main board consumption	110 mA at 24 V (PSU), 160 mA at 12 V (battery)
Maximum system current available [2]: ATS1700 ATS3700	2500 mA at 13.8 VDC $\pm$ 0.4 V 3500 mA at 13.8 VDC $\pm$ 0.4 V
Auxiliary power output [3]	13.8 VDC $\pm$ 0.4 V, 1.3 A max.
Battery power output [4][5]	13.8 VDC $\pm$ 0.2 V, 2.0 A max.
Battery type	Lead acid rechargeable: [6] 7.2 Ah, 12 V nom. (BS127N) 12 Ah, 12 V nom. (BS130N) 18 Ah, 12 V nom. (BS131N)
Standby use battery life [7] Typical Maximum	3 years under 20°C floating charge condition 5 years
Cycle use battery life	200 cycles at 100% discharge 225 cycles at 80% discharge 500 cycles at 50% discharge
Battery cables	Provided with the product
Battery low condition	From 9.5 to 10.5 VDC
Battery low condition restore	>10.5 VDC
Battery test level [8]	11.2 VDC
Minimum voltage (battery recharging) at power supply, auxiliary power output and battery power output [9][10]	9.4 VDC
Maximum ripple voltage V, p-p [11]	100 mV typical, 300 mV max.

Overvoltage trigger value [12]	14.2 VDC min.
Battery recharge voltage limit [13]	8.5 VDC
Battery capacity in charged state	100%

- [1] The power supply voltage is monitored according EN 50131 Grade 3 and VdS-C regulations.
- [2] Current available for auxiliary power output.
- [3] Maximum permanent current to power devices external to the control equipment in the absence of alarm conditions. The sum of the auxiliary and COMM power output current cannot exceed the maximum current specified in “Auxiliary current and battery capacity” on page 42.
- [4] Battery output provides battery shortcut protection (according to VdS requirements).
- [5] Constant current charger, MCU control charging current and voltage depend on the battery status.
- [6] The housings applicable for particular batteries are specified in “Auxiliary current and battery capacity” on page 42.
- [7] High temperature and multiple charge cycles may greatly reduce battery lifetime. See the specifications for your battery for more information.
- [8] If during a manual or a programmed battery test the battery voltage drops below this threshold, the battery test fails.
- [9] Deep discharge protection mechanism monitors the battery voltage and disconnects the battery if the voltage falls below indicated value, as required by EN 50131 Grade 3 and VdS-C regulations.
- [10] A specific fail message is generated when any output fails.
- [11] Maximum ripple voltage only when empty battery is charging.
- [12] Overvoltage protection mechanism monitors the power supply voltage and shuts down the PSU if the voltage raises above indicated value, as required by EN 50131 Grade 3 and VdS-C regulations.
- [13] If the battery voltage falls below this limit, the battery will not be automatically recharged.

General features	
Code combinations	From 10,000 (4 digits) to 10 billion (10 digits)
End-of-line resistor	1 kΩ, 1.5 kΩ, 2 kΩ, 2.2 kΩ, 2.2 kΩ + 4.7 kΩ, 3.3 kΩ, 3.74 kΩ, 4.7 kΩ (default), 5.6 kΩ, 6.8 kΩ, 8.2 kΩ, 10 kΩ, no EOL
Onboard zones	
ATS1700	8
ATS3700	16

Note: Can be expanded with another 8 zones on the ATS608 zone expander, or with up to 24 zones using 3X ATS1202 zone expanders.

Maximum zone number	
ATS1700	48 (for FW version MR3.2 and newer)
ATS3700	256
Onboard outputs	
ATS1700	4 (3 siren outputs, 1 relay)
ATS3700	5 (3 siren outputs, 2 relays)

Note: Can be expanded to 48 outputs with ATS624, ATS626, ATS1810, ATS1811, and ATS1820 output expanders. See Table 5 on page 35 for details.

See also “Standard onboard outputs” on page 41.

Maximum output number	128
-----------------------	-----

Areas	
ATS1700	4
ATS3700	16
Data buses	
Maximum keypad / RAS number	
ATS1700	8
ATS3700	16
Maximum touchscreen interfaces	8
Maximum expander / DGP number	
ATS1700	7
ATS3700	15
Maximum user number (for users with SMS reporting functionality)	2000, which includes: -1000 full data users -1000 card-only users
User groups	256
User group types	7
Inhibit / isolate / shunt limit, max.	
ATS1700	32
ATS3700	256
Schedules	46
Time frames	4 per schedule
Special days	8
Actions per schedule	20
Event log capacity:	
Mandatory events	10000
Non-mandatory and other events	- 1500 non-mandatory events - 10000 access events (ATS1700), 20000 access events (ATS3700) - 1000 installer events - 1000 alarm transmitter events - 1000 extended events
See also "Events" on page 92.	
Data retention (log, program settings)	20 years
Access control features	
Door controllers supported	
ATS1700	7
ATS3700	12
Standard doors	
ATS1700	4
ATS3700	8
Intelligent doors	
CDC4(-EN) standard mode	
ATS1700	28
ATS3700	48

Regions	256
Door groups	128
Floors	64
Floor groups	128
Maximum user number (with door controllers connected):	
CDC4(-EN)	65532
ATS125x without IUM	2000
ATS1250 with ATS1831 IUM	17488
ATS1250 with ATS1832 IUM	65532

Note: SMS reporting features are only available for a limited user number. Maximum number of users with full control and reporting functionality is given in “General features” on page 39.

UltraSync features

Maximum number of push notifications	16
--------------------------------------	----

Ethernet connection

Supported standard	IEEE 802.3u
Speed	10BASE-T or 100BASE-TX
Duplex	Half-duplex and full-duplex
Cabling	FTP (foiled twisted pair) Cat 5e cable or better
Autonegotiation	MDIX

Standard onboard outputs

S1, S2, S3	High current electronic output, rating: 1 A at 13.8 VDC
R1	5 A at 30 V AC/DC
R2 (ATS3700 only)	5 A at 30 V AC/DC

Environmental

Dimensions	315 x 445 x 88 mm
Weight (without batteries)	4.9 kg
Operating temperature	0 to +40°C
Tested temperature according EN 50131	-10 to +55°C
Humidity	95% noncondensing
IP protection grade	IP31
Housing colour	White, beige
Safety class	Class I
Enclosure type	Enclosure (meets UL94V-0)
Earthing cables	Provided with the product
Overvoltage category	Category II
Maximum altitude, or minimum air pressure	2000 m above mean sea level

Fuses

Battery charger	Electronic fuse 4.4 A
12 V aux	Siren 1: Electronic fuse 1.3 A
System data bus	Sirens 2 and 3: Shared electronic fuse 1.3 A
	AUX / zone outputs: Electronic fuse 1.3 A
	Data bus 1: Electronic fuse 1.3 A
	Data buses 2 and 3: Shared electronic fuse 1.3 A

Note: The total current is 2.5 A distributed over five fuses. None of the outputs can deliver more than 1.3 A per output.

Battery, battery cables	5x20 mm, 6.3 A, 230 V, slow, IEC 60127-2 sheet 3
Mains, mains fuse	T-2A 230 VAC, slow, Aritech

Note: Mains fuse is part of the Aritech 120494888 mains terminal block.

WARNING: Before removing the mains fuse, mains power must be disconnected (see “Mains power connection” on page 19).

Auxiliary current and battery capacity

Table 9: AXON maximum available auxiliary current

Battery capacity, Ah			7.2	12	18
Applicable housing			MM+		
Security approval / Grade	Discharge time, h	Charge time, h			
EN Grade 2	12	72	400	800	1300
EN Grade 3	30 [1]	24	—	200	400
EN Grade 3	60	24	—	—	100
INCERT Grade 2	24	48	100	300	550
INCERT Grade 3	60	24	—	—	100
NF&A2P Grade 2	36	72	—	130	300
NF&A2P Grade 3	60	24	—	—	100

[1] This mode is only allowed when the mains fault reporting is active.

Example for EN Grade 2

When using battery backup as specified for EN Grade 2 using a 12 Ah battery, the maximum available auxiliary current is 800 mA.

Example for EN Grade 3

When using battery backup as specified for EN Grade 3 using an 18 Ah battery, the maximum available auxiliary current is 400 mA.

This current is the maximum grand total available current that may be used for auxiliary components such as:

- Devices on the AXON system data bus
- Devices on all auxiliary power outputs
- Communication devices via MI-bus (for example, GSM, IP)

Temporary used current such as: Sirens and Strobes are not included.

Fuse rating must be taken into account.

Battery status information

Various detection ways are provided to understand the status of a battery.

A short battery test will be applied to detect following within 10 seconds:

- Battery fail (or battery missing) to inform installer no battery is attached or a poor battery is attached. Event will be logged and notified.
- Low battery as soon as battery becomes below 10.5 V with or without mains. Event will be logged, notified and reported.

Another battery test will be applied once per day to even better understand battery status. In case battery wears out a battery fail message will be logged, notified and reported.

System monitoring

The system provides monitoring for the following items.

Table 10: Monitored items

Monitoring function	Message	Cause
AC Mains	Mains fail	Loss of external power supply [1][2]
Battery	Battery low	Battery low voltage [1]
	Power unit fault	Exhausted battery Battery charger fail
	Fuse/power output fail	Output overload
Power outputs	Fuse/power output fail	Exhausted fuse
		Fuse loss
		Short circuit
		Overload
Power supply	Power unit/power output fail	Power unit failure
		Overvoltage
Tampers	Device tamper	Device sabotage

[1] Mains fail and Battery low will finally result in Battery deep discharge protection.

- [2] Mains fault message is indicated in case of AC trouble or PSU fault. View the panel event log to identify the fault source.

Chapter 3

System functions

Summary

This section lists and describes all functionality functions provided by AXON control panels.

Note: Particular functionality may be unavailable depending on panel variant, firmware version or hardware configuration.

Content

Function list 47

Zones 49

 Zone types 49

Areas 55

Set and unset 57

 Delayed unset 58

Inhibit and isolate 59

 Inhibit 59

 Isolate 59

 Zone shunt 59

Keys 61

 Common key sequences for LCD keypad 61

 Common key sequences for Touchscreen 62

 Common key sequences for keypad without LCD 64

 Function keys 65

Bus devices 67

 Bus device numbering 67

 Adding keypad with a higher number 67

 Keypads 67

 Expanders 68

Users 69

 Predefined users 69

 User data lock 70

User groups 71

PIN 76

Outputs 78

Access control	79
Door controller	79
Doors	79
Door groups	80
Floors	80
Floor groups	80
Basic access control functions	80
Advanced access control functions	80
Door controller macro logic	81
Pulsed lock and unlock	83
Condition filters	86
Triggers	88
Calendar	89
Schedule shortcut menu	90
Events	92
Log	92
Programming	92
Tests and diagnostics	94
Walk test	94
Other tests	97
Alarm reporting	98
Reporting principles	98
Reporting order	99
Failed to communicate (FTC)	100
VdS channel reporting	101
User programmable functions	104
Autoset	108
Wireless device programming	109
Learning wireless sensors	109
Learning fobs	111
Two-zone RF sensors	113
Device activation	114
Using wireless cameras	116
Configuration	116
Diagnostics	118
Troubleshooting	118
Engineer reset	120
Timed unset / ATM	121
UltraSync	122
Mobile Application	125
Site Manager	126
Securing card data	127

Function list

Table 11 below provides an alphabetic list of AXON functions and their description references.

Table 11: Function list

Function	Reference
Access control	"Access control" on page 79
Areas	"Areas" on page 55
ATM	"Timed unset / ATM" on page 121
Autoset	"Autoset" on page 108
Calendar	"Calendar" on page 89
Cameras	"Using wireless cameras" on page 116
Condition filters	"Condition filters" on page 86
Diagnostics	"Tests and diagnostics" on page 94
Doors	"Doors" on page 79
Events	"Events" on page 92
Expanders / DGPs	"Bus devices" on page 67, "Expanders" on page 68
Inhibit	"Inhibit and isolate" on page 59
Inputs	"Zones" on page 49
Isolate	"Inhibit and isolate" on page 59
Keypads / RASes	"Bus devices" on page 67, "Keypads" on page 67
Keys	"Keys" on page 61
Mobile Application	"Mobile Application" on page 125
Outputs	"Outputs" on page 78
Part set	"Set and unset" on page 57
PIN	"PIN" on page 76
Reporting	"Alarm reporting" on page 98
Secure channel	"Securing card data" on page 127
Secure mode	"Securing card data" on page 127
Set	"Set and unset" on page 57
Shunt	"Zone shunt" on page 59, "Door shunt" on page 80
Site Manager	"Site Manager" on page 126
Tests	"Tests and diagnostics" on page 94
Timed unset	"Timed unset / ATM" on page 121
Triggers	"Triggers" on page 88
UltraSync	"UltraSync" on page 122
Unset	"Set and unset" on page 57
User groups	"User groups" on page 71

Function	Reference
User programmable functions	“User programmable functions” on page 104
Users	“Users” on page 69
Walk test	“Walk test” on page 94
Wireless devices	“Wireless device programming” on page 109
Zones	“Zones” on page 49

Zones

Zone is an electrical signal from a security device or a group of devices (PIR detector, door contact) to the AXON system. Each device can be identified by a zone number or a name. For example, zone 14, Fire Exit Door.

Zone connection is described in Chapter 2 “Installation” > “Zone connection” on page 27.

For zone configuration, see “Zone configuration” on page 33.

Zone addressing is described in “Zone, output, and door addressing” on page 34.

Zone programming is done via “Zone menu” on page 228 (in Chapter 5 “Menu reference”).

Zone types

The following zone types are available.

1. Alarm

Generates no alarm when the area is unset.

Generates an alarm when the area is set.

Example: Internal door, PIR (motion detector).

2. Entry/Exit 1

Generates no alarm when the area is unset.

When the area is set, the exit timer starts and activating the zone generates no alarm. If the zone is activated when the exit time has expired, the entry timer starts. Only when the entry time has expired, an alarm is generated.

Example: Front door.

You need to program the entry/exit time. See “Areas” on page 244 for more information.

3. Access

Generates no alarm when the area is unset.

Generates an alarm when the area is set, and the no exit timer or entry timer is not running.

Example: PIR at entrance with a door contact on the entry door.

You need to program the entry/exit time. See “Areas” on page 244 for more information.

4. Fire

Generates a fire alarm regardless of the status of the area.

Fire alarm causes pulsing siren sound. This alarm has higher priority than an intrusion alarm.

Example: Smoke detector.

WARNING! Fire alarm and smoke detection products used with AXON 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. See also Chapter 8 “Regulations > Options affected by other regulations” on page 384

5. Panic

Generates a panic alarm regardless of the status of the area.

Example: panic button.

See also “Panic mode” on page 321.

6. 24H

Generates an intrusion alarm regardless of the status of the area.

7. Tamper

Generates a tamper alarm regardless of the status of the area.

Example: Panel tampers.

8. Exit terminator

This zone type is used to terminate an exit time. If the zone switches from active to normal, the exit time is terminated and the area(s) are completely set as soon as the final set delay has expired (see also “Final set delay” on page 298).

9. Keyswitch

When the zone switches, the area is set / unset / part set depending on the zone options selected.

Example: Key switch next to Front door.

See options “Key latch” on page 233, “Key set” on page 234, “Key unset” on page 234.

10. Medical

Generates a medical alarm regardless of the status of the area.

11. Technical

Generates a technical alarm regardless of the status of the area.

Example: temperature sensor.

See options “Technical full set” on page 234, “Technical unset” on page 234.

12. Transmission path fault

Monitors the external reporting device.

13. Fire door

If there is no fire alarm present, generate an intrusion alarm regardless of the status of the area. Otherwise, no intrusion alarm is generated.

Note: The internal siren activation depends on “Chime” zone option. See “Chime” on page 232.

Example: Fire doors or emergency doors.

See also “4. Fire” on page 50.

14. Aux mains fault

Monitors the auxiliary mains supply.

15. Aux batt fault

Monitors battery of the auxiliary power supply.

16. Key box

Monitors a box that holds a key to premises. It allows you to open for a short period after setting an area (specified in key box timer, see “Key box time” on page 300). It generates an alarm when opened outside of this period.

17. Eng. reset

This zone activation causes the engineer reset.

18. Entry/Exit 2

An alternative entry/exit zone.

Example: Back entrance.

Entry/exit 2 zone initiates alternative entry/exit timers. See “Exit time” on page 245 and “Entry time” on page 245.

See also “2. Entry/Exit 1” on page 49 for more details.

19. Shunt

Zone activation causes shunt of all area zones that have shunting allowed. Shunt is allowed by the option “Shunt” on page 239.

Note: When the zone with this type returns to normal state, the zones shunted by this zone will be unshunted only when they are in normal state. Active zones will remain shunted until they change their states to normal.

See also “Zone shunt” on page 59.

20. Fire door – EE

If the area is unset, the zone works as “13. Fire door” described on page 51.

If the area is set, the zone works as an Entry/Exit zone. See also “2. Entry/Exit 1” on page 49 and “18. Entry/Exit 2” on page 51.

Note that in the set state all condition filters mapped to this zone are disabled.

Table 12: Available zone options

Options:	Zone type	1. Alarm	2. Entry/Exit 1	3. Access	4. Fire	5. Panic	6. 24H	7. Tamper	8. Exit terminator	9. Keypress	10. Medical	11. Technical	12. Transmission	13. Fire door	14. Aux mains fault	15. Aux batt fault	16. Key box	17. Eng. reset	18. Entry/Exit 2	19. Shunt	20. Fire door – EE
Inhibit		+	+	+	+	-	+	+	+	+	+	+	+	+	+	+	+		+	+	+
Isolate		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-	-	+
Exclude in part set 1		-	-	-					-	-							-		-	-	
Exclude in part set 2		-	-	-					-	-							-		-	-	
Double knock		-			-		-					-	-	-	-	-					-
Swinger shunt [1]		-	-	-			-	-				-		-	-	-	-		-		-
Anti mask		-	-	-			-					-		-					-		-
Zone pairing		-			-							-		-							-
Chime		-	-	-								-		-					-		+
Soak test		-	-	-	-	-	-	-				-		-	-	-	-		-		-
Engineer walk test		+	+	+	+	+	+	+			+	+	+	+	+	+		+		+	+
User walk test		+	+	+		+	+				+	+		+	+	+		+		+	+
Shock sensor		-	-	-			-							-					-		
Extend EE			-																-		
Final door			-	-															-		
Key latch										-											
Key set — full set										-											
Key set — part set										-											
Key unset										-											
Technical full set												+									
Technical unset												+									
Technical part set												+									
Keypad LCD							-				-	-	-	-	-	-					-
Log		•	•	•	•	•	•		+	+	+	•	•	+	+	+		•			
CS report		•	•	•	•	•	•		+	+	+	•	•	+	+	+		•			
Delay timer												-	-		-	-					

Options:	Zone type	1. Alarm	2. Entry/Exit 1	3. Access	4. Fire	5. Panic	6. 24H	7. Tamper	8. Exit terminator	9. Keypress	10. Medical	11. Technical	12. Transmission	13. Fire door	14. Aux mains fault	15. Aux batt fault	16. Key box	17. Eng. reset	18. Entry/Exit 2	19. Shunt	20. Fire door – EE
ACK on keypad																					
ACK by user																					
Sensor type																					
Virtual zone																					-
Zone held open																					-
EE set check																					
Alarm in PS1																					
Alarm in PS2																					
Report as																					
Detector Auto Test																					
Shunt		-	-			-								-							-
View isolated																			+	+	
Limit reports		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Input mode																					
End of line resistor																					
Indication		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Reporting code																					

[1] These options depend on the defaults selected in the initial panel start-up.
See also “Initial start-up” on page 163.

Legend:

- + (yes): The option is programmable, the default value is Yes.
- (no): The option is programmable, the default value is No.
- (always): The option is not programmable, the value is always Yes.

Menu reference

The following menus are applicable for zones.

Menu	Page	Description
Expander range	206	View zone range of the selected expander
Zone menu	228	Add, remove, and configure zones
Pictures by zone	253	Choose zones that can trigger the camera when active.
Door zones	259	Assign required zones to the selected door
Zones	272	Select zones that must be shunted on the door opening.
Zone timer menu	299	Configure timers used in zone configuration options

Menu	Page	Description
Zone options	314	Configure system options for zones
Alarm confirm	316	Configure A and B zone confirmation (ACPO)
Object scheme	320	Configure zone numbering scheme

Areas

Area is a section of premises that has specific security requirements. The AXON system allows any premises to be divided into different areas having different security requirements. Each area has zones assigned to it. Each area is identified by a number or an identifier. For example: Area 1, Main Office, etc.

Each area can have one of the following statuses:

- Set (armed)
- Part set
- Unset (disarmed)

See “Set and unset” on page 57 for details.

Areas are configured in “Areas” on page 244 in Chapter 5 “Menu reference”.

Area groups

Particular panel models allow to group areas in area groups. Users are allowed to perform area operations with area groups in the same way as with areas: for example, set an area group.

Area groups are configured in “Area groups” on page 249.

Note: Area group availability depends on the control panel variant. See “Specifications” on page 38 in Chapter 2 “Installation”.

Area hierarchy

The area hierarchy defines the order, in which high security areas should be set or unset. A lower value means a higher hierarchy. Areas with higher hierarchy should be set in the first turn, and unset as the last ones.

This functionality is available only in areas with area hierarchy higher than 0.

An example is a bank vault. It should be impossible to unset the vault (hierarchy 1) before the vault hall (hierarchy 2) is unset. Also, you cannot set the vault hall before the vault is set.

Area hierarchy is set via menu “Hierarchy level” on page 248.

Menu reference

The following menus are applicable for areas.

Menu	Page	Description
View areas, View Area Group	197	Specify which area and area group will display information on the keypad without a user authorization.
Control areas, Control Area Group	197	Select areas and area groups that can be set and unset by the keypad.
Area indication for LED 1, Area indication for LED 2	201	Assign areas to programmable LEDs of the keypad.
Tamper area (keypad), Tamper area (expander),	196	Determine which area receives the selected device tamper and fault events.

Menu	Page	Description
Select mode	225	Specify if the user operates on areas or area groups.
User group areas, User group area group	226	Define which areas and area groups the user can control.
Zone areas	230	Assign areas to the zone that have to alarm when the zone is activated, and area set or unset status meets the requirement for the zone type.
Areas	244	Configure areas.
Area groups	249	Assign areas to area groups.
Door areas, Door area groups	259	Assign the selected door to areas and area groups for area status indication on readers.

Set and unset

Each area can have one of the following statuses:

- **Set (armed):** 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.
- **Unset (disarmed):** The condition of an area when it is occupied, and normal activity does not set off an alarm.
- **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.

See also “Areas” on page 55.

Areas can be set or unset in one of the following ways:

- By users via a keypad or a reader. See “Users” on page 69 and “Bus devices” on page 67. The available key sequences are listed in “Keys” on page 61.
- By users via SMS command. See *SMS Control Reference Manual* for details.
- By operators remotely via management software. See Chapter 6 “Software” on page 363.
- Automatically via the autosest functionality. See “Autoset” on page 108 for details.

How to use part set

When users perform a part set, the system sets all requested areas with all full set (perimeter) zones supervised but all part set (interior) zones ignored. As this setting mode is for personal safety, reporting to the central station depends on option “Report BA” (see page 308). Further, any alarms that occur while part set is applied, are treated as local alarms that activate sirens, keypad buzzers (if enabled), and keypad indicators.

If a zone is assigned multiple areas, it is not set until all assigned areas are set. If there is a mixture of part set and full set areas assigned to the zone, the zone obeys the part set condition.

Delayed unset

The area unset can be delayed. A delayed unset is used in banking applications, like ATM cash refill and vault opening.

During the delay the area keypad or reader is locked. The following message is displayed on the keypad LCD screen:

```
Unset delay
Please wait
```

On a keypad or a reader without LCD the unset delay is indicated by slowly blinking area LED.

The delay period is set in “Unset delay” on page 247.

There is no way to manually override the delay.

Menu reference

The following menus are applicable for setting, partial setting, and unsetting.

Menu	Page	Description
Control areas, Control Area Group	197	Select areas and area groups that can be set and unset by the keypad.
Card and PIN mode	198	Select an authorization method for the keypad.
One time badge to set/unset	198	Define if the selected keypad allows you to set or unset areas with one badge.
Three time badge to set	198	Define if the selected keypad allows you to set areas with triple badge.
Quick set mode	200	Allow setting areas without providing user PIN or card.
Select mode	225	Specify if the user operates on areas or area groups.
User group areas, User group area group	226	Define which areas and area groups the user can control.
Exit time	245	Set area exit timers.
Entry time	245	Set area entry timers.
Unset delay	247	Set timer for delayed unset.
Set/unset options	247	Set various system setting and unsetting options.
Alarm control	259	Set alarm control options for the selected door.
Final set delay	298	Define the delay time between the completion of an area being set by an exit terminator or final door set and the area being armed.
Set options	307	Define the set conditions.
Easy unset	318	If enabled, you can unset premises entering a PIN or reading a valid card without pressing any other keys.
Timed Unset / ATM	327	Configure the ATM (automated teller machine) interface options, for example, unset delay and extended unset delay.

Inhibit and isolate

A faulty device can be inhibited or isolated.

Inhibit

A zone is inhibited from indicating normal or active status. It becomes excluded from functioning as part of the system for particular time. However, tampers are still monitored.

The zone is inhibited until the next unset.

A zone can be inhibited automatically when using the forced set functionality. It is configured via menu “Forced set” on page 309 in Chapter 5 “Menu reference”.

Isolate

A zone or a bus device is inhibited from indicating normal or active status. It is excluded from functioning as part of the system permanently, until de-isolating by the manager or installer.

Zone shunt

A shunt procedure inhibits zones, when active, from generating an alarm during a certain period.

A zone can be shunted in the following ways:

- Manually by the installer. Use menu “Shunt zones” on page 174.
- By a schedule. See “Calendar” on page 89 for details.
- By a conditional filter. See “Condition filters” on page 86 for details.
- By a zone with Shunt type. See “Zone types” on page 49 for details.

Caution: There is a limitation of the number of zones that can be shunted simultaneously. The limit is set in “Shunt limit” on page 249.

During the shunt time the zone is inhibited.

If the zone is still active after the shunt time has expired, the zone will generate an alarm, depending on the zone type and the status of the area.

For certain users (depending on their user options) the shunt is active during an extended shunt time.

Before the shunt timer expires, a warning may be given.

Menu reference

The following menus are applicable for inhibition, isolation, and zone shunt.

Menu	Page	Description
Shunt zones	174	Shunt zones manually.
Isolate keypad	200	Isolate the tamper fault events on the selected keypad (the keypad remains functional).
Isolate expander	207	Isolate the tamper fault events on the selected expander (the expander remains functional).
Isolate	230	Isolate or de-isolate the selected zone.
Inhibit	231	If set to Yes, this zone can be inhibited by users.
Isolate	231	If set to Yes, this zone can be isolated by users.
Swinger shunt	231	If set to Yes, the number of alarms from the zone is limited to the specified number for one set/unset cycle.
Shunt	239	If set to Yes, the zone can be shunted.
View isolated	239	If set to On, users are warned about this zone being isolated when attempting to set or unset the appropriate area.
Limits	249	Limit the number of system elements that can be isolated, inhibited, or shunted at any one time.
Isolated	254	Isolate the selected camera.
Swinger shunt	314	Define the number of alarms from a zone until it is shunted

Keys

The authorization method depends on system settings. See “Control options” on page 198 for more information.

Note: When an incorrect PIN is entered three times the keypad is locked for 120 seconds.

Common key sequences for LCD keypad

Table 13: Common key sequences for LCD keypad

Action	Programmed method	Key sequence	[1]
Set [2]	Set with key	On	☐
	Set with PIN	On, PIN, Enter	☐
		PIN, On	☐
	Set with card	Card	☐
		On, card	☐
		3 x card	☐
	Set with card and PIN	On, card, PIN, Enter	☐
		Card, PIN, On	☐
Unset [2][3]	Unset with PIN	Off, PIN, Enter	☐
		PIN	
		PIN, Off	☐
	Unset with card	Card	☐
		Off, card	☐
	Unset with card and PIN	Off, card, PIN, Enter	☐
		Card, PIN, Off	☐
		Card, PIN	
Part set [2]	Part set with key	Partset	☐
	Part set with PIN	Partset, PIN, Enter	☐
		PIN, Partset	☐
	Part set with card	Card	☐
		Partset, card	☐
		3 x card	☐
	Part set with card and PIN	Partset, card, PIN, Enter	☐
		Card, PIN, Partset	☐
Door access [2][3]	Door access with PIN	PIN, Enter	☐
	Door access with card	Card	☐
	Door access with card and PIN	Card, PIN, Enter	☐

Action	Programmed method	Key sequence	[1]
Menu access [2]	Menu access with PIN	Menu, PIN, Enter	☐
		PIN, Menu	☐
	Menu access with card	Menu, card	☐
	Menu access with card and PIN	Menu, card, PIN, Enter	☐
		Card, PIN, Menu	☐
Duress [4]	Duress with PIN	Any set key (On / Off / Partset), duress code, Enter	☐
		Duress code, any set key	☐
	Duress with card and PIN	Any set key (On / Off / Partset), duress code, card, Enter	☐
		Card, duress code, any set key	☐
Change keypad buzzer volume	Increase volume	X + Right	☐
	Decrease volume	X + Left	☐
Panic [5]	Panic alarm	1 + 3	☐
Exit [6]	Quick exit from the programming	Menu + Clear	☐
Active alarms [7]	Display active zones and faults that should be acknowledged	Function, Function	☐
Alarm memory [7]	Display alarms that occurred when set	Enter, Enter	☐

[1] Use the check box to note which options are available for this system.

[2] The functionality depends on “Card and PIN mode” on page 198.

[3] The functionality depends on “Easy unset” on page 318.

[4] The functionality depends on “Duress method” on page 315.

[5] Panic alarm functionality depends on the “Panic mode” option described on page 321. It also depends on the “1+3 keys” option described on page 203.

[6] The function works only if there is no prompt that requires a user response or action. It is disabled, for example, during wireless devices learning.

[7] The functionality depends on “Alarm list” on page 306.

Common key sequences for Touchscreen

Table 14: Common key sequences for Touchscreen

Action	Programmed method	Key sequence	[1]
Set [2]	Set with key	 ON	☐
	Set with PIN	 ON, PIN,  Enter	☐
	Set with card	Card	☐
		 ON, card	☐
		3 x card	☐
	Set with card and PIN	 ON, card, PIN,  Enter	☐
Unset [2]	Unset with PIN	 OFF, PIN,  Enter	☐
	Unset with card	 OFF, card	☐

Action	Programmed method	Key sequence	[1]
Part set [2]	Unset with card and PIN	🏠 OFF, card, PIN, ➡ Enter	☐
	Part set with key	🏠 PART	☐
	Part set with PIN	🏠 PART, PIN, ➡ Enter	☐
	Part set with card	Card	☐
		🏠 PART, card	☐
		3 x card	☐
	Part set with card and PIN	PART, card, PIN, ➡ Enter	☐
Door access [2]	Door access with PIN	🚪 OPEN, PIN, ➡ Enter	☐
	Door access with card	Card	☐
	Door access with card and PIN	Card, PIN, ➡ Enter	☐
Menu access [2]	Menu access with PIN	Authorization [3], PIN, ➡ Enter	☐
	Menu access with card	Authorization [3], card	☐
	Menu access with card and PIN	Authorization [3], card, PIN, ➡ Enter	☐
Duress [4]	Duress with PIN	Any set key (ON / OFF / PART), duress code, ➡ Enter	☐
	Duress with card and PIN	Any set key (ON / OFF / PART), duress code, card, ➡ Enter	☐
Emergency alarms [5]	Fire alarm	Slide down, FIRE	☐
	Panic alarm [6]	Slide down, PANIC	☐
	Medical alarm	Slide down, MEDICAL	☐
Function keys [5][7]	F1	Slide left, F1	☐
	F2	Slide left, F2	☐
	F3	Slide left, F3	☐
	F4	Slide left, F4	☐

[1] Use the check box to note which options are available for this system.

[2] The functionality depends on “Card and PIN mode” on page 198.

[3] Tap on the authorization bar. See “Authorization” on page 142.

[4] The functionality depends on “Duress method” on page 315.

[5] Slide the main screen to navigate to the additional screens.

[6] Panic alarm functionality depends on the “Panic mode” option described on page 321.

[7] See “Function keys” on page 65 for details.

See “Programming the system using Touchscreen” on page 140 for more information.

Common key sequences for keypad without LCD

Table 15: Common key sequences for keypad without LCD

Action	Programmed method	Key sequence	[1]
Set [2]	Set with PIN	On, PIN, On	☐
		PIN, On [6]	☐
	Set with card	Card [6]	☐
		On, card	☐
		3 x card	☐
	Set with card and PIN	On, card, PIN, On	☐
		Card, PIN, On [6]	☐
Unset [2][3]	Unset with PIN	Off, PIN, On	☐
		PIN	☐
		PIN, Off [6]	☐
	Unset with card	Card	☐
		Off, card	☐
	Unset with card and PIN	Off, card, PIN, On	☐
		Card, PIN, Off [6]	☐
		Card, PIN	☐
Part set	Part set with card	Card	☐
		3 x card	☐
Door access [2]	Door access with PIN	PIN, On [6]	☐
		PIN, Off [6]	☐
	Door access with card	Card [6]	☐
	Door access with card and PIN	Card, PIN, On [6]	☐
		Card, PIN, Off [6]	☐
Duress [4]	Duress with PIN	Any set key (On / Off), duress code, Enter	☐
		Duress code, any set key	☐
	Duress with card and PIN	Any set key (On / Off), duress code, card, Enter	☐
		Card, duress code, any set key	☐
Panic [5]	Panic alarm	1 + 3	☐

[1] Use the check box to note which options are available for this system.

[2] The functionality depends on “Card and PIN mode” on page 198.

[3] The functionality depends on “Easy unset” on page 318.

[4] The functionality depends on “Duress method” on page 315.

[5] Panic alarm functionality depends on the “Panic mode” option described on page 321.

[6] Particular key sequences can have conflicting functions. In this case the functionality depends on the “Key/Card Sequence Mode” option described on page 199.

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.

Function keys

Use Table 16 below to describe function keys functionality and availability.

See also “Function keys” on page 201.

Table 16: Function keys

Action	Key	[1]
	A	☐
	B	☐
	C	☐
	F1	☐
	F2	☐
	F3	☐
	F4	☐

[1] Use the check box to note which functions are available in this system.

Menu reference

The following menus are applicable for key configuration.

Menu	Page	Description
Card and PIN mode	198	Select a control method.
One time badge to set/unset	198	Define if the selected keypad allows you to set or unset areas with one badge.
Three time badge to set	198	Define if the selected keypad allows you to set areas with triple badge.
Quick set mode	200	Allow setting areas without providing user PIN or card.
Function keys	201	Assign a user programmable function to any of available function keys.
ACK on keypad	202	Select an additional LCD keypad that displays an acknowledgement prompt after the system is unset.
1+3 keys	203	Enable a panic alarm by combination of 1 and 3 keys.
Select mode	225	Specify if the user operates on areas or area groups.
Card and PIN	265	Specify what method is required to open the door from the selected reader.
Two cards	265	Define if two user cards or PINs are required to gain access.
Control type	269	Specify what type of alarm control is available for the selected door.
Card and PIN	298	Set the maximum delay time between presenting the card and entering the PIN.

Menu	Page	Description
Easy unset	318	If enabled, you can unset premises entering a PIN or reading a valid card without pressing any other keys.

Bus devices

There are the following kinds of bus devices:

- Keypads are used to provide system control, such as setting or unsetting areas. Depending on the type of keypad, additional functions may be available, such as LCD displays, menus to set time and date etc.
- Expanders are used to provide remote inputs and outputs.
- Readers are connected to door controllers and used to control intelligent doors. See “Access control” on page 79 for details.

Bus device numbering

Devices use DIP switches to set bus address. The AXON normally uses the keypad/expander number. For the dependence between device address and its number, refer to the appropriate bus device installation manual. The address of the programmed device can be viewed in “Keypad address” and “Expander address”.

See also Chapter 2 “Installation > Zone, output, and door addressing” on page 34.

Adding keypad with a higher number

If the number programmed in a keypad is higher than the maximum number allowed in the system, the keypad cannot be added. But it is possible to change this number from the panel via the keypad internal menu. Adding a higher keypad number brings you to a simplified menu that contains only own keypad menu entry.

For example, to program keypad with programmed number 16 in a system with 8 keypads:

1. Add keypad 16. It will bring you to “Keypad menu” (described on page 205).
2. Enter keypad menu.
3. Change keypad address to 7. Refer to the appropriate keypad manual.
4. Add keypad 7.

Keypads

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.

Keypads and readers can be also referred as remote arming stations (RASes).

Keypads are configured in “Keypad devices” on page 195 in Chapter 5 “Menu reference”.

Expanders

Expanders are devices that expand number of inputs or outputs in the AXON system. There are two kinds of expanders:

- Internal expanders: Expansion boards that are installed inside the control panel housing.
- External expanders: Bus devices that collect data from other security devices within an area and transfer it to the AXON control panel. They are also referred as expanders or data gathering panels (DGP).

Expander installation and wiring is described in Chapter 2 “Installation” on page 7.

Expander options are set in “Expander devices” on page 205 in Chapter 5 “Menu reference”.

Menu reference

The following menus are applicable for bus devices.

Menu	Page	Description
Device menu	194	View and configure bus devices.
DGP options	312	Door controller settings.

Users

Users are identified to the AXON system by a unique number that is associated with the user's PIN or card.

Note: If the system is EN 50131 compliant, you can edit only your own settings, and configure only newly added users. See “User data lock” on page 70 for more details.

For each user, the system records the following:

- Number
- Name
- PIN
- Card ID number
- Mobile number
- Remote login and remote 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 is defined in “Specifications” on page 38.

Note: Connecting door controllers to the AXON system increases the maximum user number in the system (see “Specifications > Access control features” on page 40 for details). However, additional users do not have the following records:

- Phone number
- Language

Predefined users

There are two predefined users in the system:

- Installer is used to enter the AXON system configuration. He has user group “Installer group” assigned.
- A user with default name Supervisor who can grant access to the installer menu for the service engineer. He has user group “Supervisor group” assigned.

If the option “Many installers” on page 305 is enabled, a few installers can be configured in the panel. However, only one installer can be logged in from a keypad at any time.

See also “User groups” on page 71.

User data lock

When a system is configured as EN 50131 compliant, you are not allowed to modify settings for an existing user (other than yourself). A new user can be configured only when added, and an existing user can only be removed. The installers can only modify their own settings, and the other users can modify their own settings via user menus (see *AXON Control Panel User Manual* and *AXON Control Panel Manager Manual* for more details).

After a new user is added via menu “Add user” on page 219, the installer can configure this user. After the modification is done and the installer exits from the user menu, the following confirmation request appears:

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

Choose OK to confirm the new user configuration. After confirmation only this user can modify own settings.

Otherwise, choose Cancel to return to the user configuration.

Menu reference

The following menus are applicable for users.

Menu	Page	Description
Check card	188	Read data from a user card.
Service in	192	Disallow the Installer in function before the Installer in-time expires.
User menu	219	Add, edit, or delete users and user groups.
Assigned user	251	Assign an existing user to the selected fob.
High Security User options	274	Configure high security user options.
Engineer options	301	Configure options that apply to maintenance and installation functions.
Card learn-in	323	Choose a keypad or a door for user card learning.
Destination	336	Configure GSM communication with users.

User groups

A user group allows users to control the AXON 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 the "Managers" user group allows inhibiting but the "R&D" group does not, the user is allowed to inhibit a zone.

Note: The system always includes an installer group.

User group types

User group type defines what user group options are allowed for the user, which belongs to a group of this type. For example, a guard does not have a permission to add users, while a normal user cannot change date and time.

Depending on the panel variant, the following types of user groups may be available:

- Normal user
- Supervisor
- Installer
- Guard
- Timed Unset / ATM
- Reset only
- Log

These types are provided to comply with EN 50131. User group type defines the default user group options, as well as allowed changes.

Note: Only the Installer user group has type Installer. Also, this is only possible type for this group.

User group type is set in "User group type" on page 226.

Table 17 below denotes default and allowed user group options (user privileges).

Note: Not all read-only options are visible for particular user group types.

Table 17: User group types and allowed options [1]

#	Option	User group type						
		Normal user	Supervisor	Installer	Guard	Timed Unset / ATM	Reset only	Log
1.	Full set	Yes	Yes	Yes	Yes	[Yes]	[No]	[No]
2.	Part set 1	No	Yes	Yes	Yes	[No]	[No]	[No]
3.	Part set 2	No	Yes	Yes	Yes	[No]	[No]	[No]

#	Option	User group type						
		Normal user	Supervisor	Installer	Guard	Timed Unset / ATM	Reset only	Log
4.	Unset	Yes	Yes	Yes	Yes	[Yes]	[No]	[No]
5.	Reset only	Yes	Yes	Yes	Yes	[Yes]	[No]	[No]
6.	Inhibit	Yes	Yes	Yes	Yes	No	Yes	[No]
7.	Isolate	[No]	Yes	[Yes]	[No]	[No]	[No]	[No]
8.	Time and date	[No]	Yes	[Yes]	Yes	[No]	[No]	[No]
9.	User adding (none / restricted / all) [2]	[none]	all	[all]	[none]	[none]	[none]	[none]
10.	Forced set	No	Yes	Yes	[No]	No	[No]	[No]
11.	Change PIN	Yes	Yes	[Yes]	No [3]	No	[No]	[No]
12.	Walk test	No	Yes	[Yes]	Yes	[No]	[No]	[No]
13.	Engineer reset	[No]	Yes	[Yes]	No	[No]	[No]	[No]
14.	Duress code	No	Yes	Yes	No	No	[No]	[No]
15.	Reporting test	[No]	Yes	[Yes]	[No]	[No]	[No]	[No]
16.	Remote connection	No	Yes	[Yes]	[No]	[No]	[No]	[No]
17.	Cleaner	No	No	[No]	[No]	[No]	[No]	[No]
18.	UG area list	No	Yes	[Yes]	No	No	[No]	[No]
19.	Menu access	Yes	Yes	[Yes]	Yes	[Yes]	Yes	Yes
20.	Inst. access	[No]	Yes	[No]	[No]	Yes	[No]	[No]
21.	Logs access	No	Yes	[Yes]	Yes	Yes	Yes	Yes
22.	Stop report	No	Yes	[Yes]	[No]	[No]	[No]	[No]
23.	SMS reporting	No	Yes [1]	Yes	[No]	[No]	[No]	[No]
24.	SMS control	No	Yes [1]	Yes	[No]	[No]	[No]	[No]
25.	Card and PIN mode (PIN only, card only, card or PIN)	Card or PIN	Card or PIN	Card or PIN	Card or PIN	Card or PIN	Card or PIN	Card or PIN
26.	No OP/CL reports	No	No	[No]	[No]	[No]	[No]	[No]
27.	Schedule access (none, view, control/view)	view	control / view	[control / view]	control / view	[none]	[none]	[none]
28.	Fob learning	[No]	Yes	[Yes]	[No]	[No]	[No]	[No]
29.	Remote pics	No	Yes	Yes	No	[No]	[No]	[No]
30.	Pic deletion	No	Yes	Yes	No	[No]	[No]	[No]

#	Option	User group type						
		Normal user	Supervisor	Installer	Guard	Timed Unset / ATM	Reset only	Log
31.	CS configuration	No	Yes	[Yes]	No	[No]	[No]	[No]
32.	Shunt	No	No	[Yes]	[No]	[No]	[No]	[No]
33.	Region ctrl	No	[Yes]	Yes	No	No	No	[No]
34.	Door control	No	[Yes]	Yes	No	No	No	[No]
35.	Notif. report	Yes	Yes	Yes	Yes	Yes	Yes	Yes
36.	Notif. ctrl	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[value]: Option is read only.

- [1] The value may depend on defaults selected during the initial start-up. See “Initial start-up” on page 163 for details.
- [2] See “User privilege limitation” below for details.
- [3] Guard user can only be modified by the installer. If the option “Allow Supervisors to Edit Guard Users” described on page 320 is enabled, the supervisor can also modify guard users.

For detailed descriptions of user group options, see “User group options” below.

User privilege limitation

The User adding option determines whether the user can add new users and what user rights these newly created users have.

- None: User cannot create new users.
- Restricted: User can create new users, but he is only allowed to set permissions equal to or lower than his own.

For example, if his user group does not allow changing the date and time, he cannot provide this permission to any user by editing a user group, nor assign a user to an existing user group with that permission. This affects options as well as areas. For example, if the user has access only to Area 1, he cannot give access to Area 2 to another user.

- All: User can create new users with any permission.

See also “User data lock” on page 70.

User group options

User group options are set in menu “User group options” on page 227.

The following options are available.

Table 18: User group options as user privileges

#	Option	Description
1.	Full set	Set the premises.
2.	Part set 1	Perform a partial set 1.

#	Option	Description
3.	Part set 2	Perform a partial set 2.
4.	Unset	Unset.
5.	Reset only	Confirm alarms without unsetting the system.
6.	Inhibit	Inhibit zones.
7.	Isolate	Isolate zones, bus devices, cameras etc.
8.	Time and date	Change system time and date.
9.	User adding	Create new users (see also “User privilege limitation” on page 73).
10.	Forced set	Perform a forced set. The availability of this option depends on the system configuration.
11.	Change PIN	Change own PIN.
12.	Walk test	Perform a walk test.
13.	Engineer reset	Perform an engineer reset.
14.	Duress code	Use a duress code.
15.	Reporting tests	Make a test call to the particular central station.
16.	Remote connection	Respond to a remote access request.
17.	Cleaner	Leave zones inhibited after the unset.
18.	User group area list	Display the list of areas.
19.	Menu access	Enter the user menu.
20.	Inst. access	Grant the Installer an access to the system configuration.
21.	Logs access	Access the panel logs.
22.	Stop report	Stop reporting in progress.
23.	SMS reporting	Receive SMS reports.
24.	SMS control	Control the system via SMS.
25.	Card and PIN mode	Set the mode for this particular user group (if possible). The following modes are available: • PIN only • Card only • Card or PIN
26.	No OP/CL reports	Open/close events generated by users of the user group are not reported
27.	Schedule access	Access to schedule. The following options are available: • None: No access • View: Restricted access. Users can view schedule and cancel actions for the present day. • Configure: Full access.
28.	Fob learning	Program a fob.
29.	Remote pics	Enable remote picture triggering.
30.	Pic deletion	Delete pictures.
31.	CS configuration	Configure CS communication.

#	Option	Description
32.	Shunt	Shunt zones.
33.	Region ctrl	Move users between regions.
34.	Door control	Control door state: lock, unlock, open, timed open, enable and disable.
35.	Notif. report	Create and receive notifications.
36.	Notif. ctrl	Edit and delete notifications.

Menu reference

The following menus are applicable for user groups.

Menu	Page	Description
User menu	219	Add, edit, or delete users and user groups.
Destination	336	Configure GSM communication with users.

PIN

PIN (Personal Identification Number) is 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 options. In the AXON configuration the PIN is associated with a user, which identifies the PIN holder to the system.

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

- ☐ PINs are generated by the system. The user can request a new PIN generation.

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

- ☐ PINs are entered manually.

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

The PIN change mode can be set in menu “PIN change mode” (see page 316).

PIN length is programmed using “PIN length” on page 315. 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. PINs must be unique. A PIN cannot be assigned to more than one user. The system will not generate or accept entry of PINs already in use.

The selected user PIN can be changed in “PIN” on page 220 if the user data is not locked. See “User data lock” on page 70 for more information.

See also “Keys” on page 61.

Menu reference

The following menus are applicable for PIN configuration and use.

Menu	Page	Description
Card and PIN mode	198	Select a control method.
EE PIN lock	199	If set to Yes, it is not possible to use a PIN during the entry time.
Quick set mode	200	Allow setting areas without providing user PIN or card.
PIN	220	Change user PIN.
Low Security	260	Define when the user authorization is changed from Card <i>and</i> PIN to Card <i>or</i> PIN.
EE PIN lock	260	If set to Yes, it is not possible to use a PIN during the entry time.
Card and PIN	265	Specify what method is required to open the door from the selected reader.
If PIN sets	269	Configure the door operation if the area is set using PIN.

Menu	Page	Description
Low Security	272	Define when the user authorization is changed from Card <i>and</i> PIN to Card <i>or</i> PIN.
Card and PIN	298	Set the maximum delay time between presenting the card and entering the PIN.
Inst in-time	299	Configure the time in which an engineer is allowed to access when granted by a user.
User code required	301	Define if a user is required to grant the installer an access to the programming menu.
Service in	304	Disallow the Installer in function before the Installer in time expires.
Challenge code	304	Activate challenge code functionality.
Card to PIN time	311	The amount of time allowed between presenting a valid card to a door reader and entering a valid PIN.
PIN length	315	Change the PIN length.
PIN change mode	316	Choose the appropriate PIN change mode.
Easy unset	318	If enabled, you can unset premises entering a PIN or reading a valid card without pressing any other keys.

Outputs

Outputs are logical elements that control physical outputs (relays and open collectors). Physical outputs are used to control doors, sirens, and other device control.

See Chapter 2 “Installation” on page 7 for details on physical outputs.

Outputs are assigned to physical outputs and configured in the menu “Outputs and filters” described on page 280 in Chapter 5 “Menu reference”.

These outputs can be controlled by zones, user actions, triggers, schedule, or system events using condition filters. See “Condition filters” on page 86 for more details.

Menu reference

The following menus are applicable for outputs.

Menu	Page	Description
Output test	175	Check outputs and LEDs.
Test No Bells	179	Verify of the whole alarm system functionality.
Output modules number	213	Number of output controllers fitted to the door controller.
Outputs and filters	280	Configure outputs.
Siren options	297	Set timers applicable to internal and external sirens.
Map relays	313	Define whether door controller unlock outputs can be controlled as standard outputs.

Access control

The AXON system allows controlling user access to certain regions using doors. There are the following types of access control functions:

- Basic access control function is controlling alarm function by shunting door contact when an authorized user reads a valid card or enters a valid PIN, or presses request to exit button. Such access control functions are provided using standard doors.

See “Door shunt” on page 80 for more information on door shunts.

See also “Doors” below, “Zone shunt” on page 59.

- Advanced access control functions include anti-passback, high security regions etc. These functions are only available while using intelligent doors, which are controlled by door controllers (see “Door controller” below).

See also “Advanced access control functions” on page 80.

Door controller

The advanced access control functions are handled by a door controller, which is an expander connected to the system bus.

One door controller can control up to four intelligent doors.

Currently there are the following door controllers available: CDC4 and CDC4-EN. The system also supports legacy door controllers ATS1250, ATS1251, ATS1252, ATS1253, ATS1254.

See “Expanders” on page 68 for more information on expander installation.

Doors

A door is a basic element of the access control functionality. There are two types of doors:

- Standard door: A door with a reader or a keypad assigned to each side of the door, and a request to exit button for an exit. Unauthorised door opening causes an intrusion alarm. See “Basic access control functions” on page 80.
- Intelligent door: A door, which can be used for advanced access control. Such door has up to two readers and a region assigned to each side, entry and exit. Such doors are controlled by door controllers. See “Advanced access control functions” on page 80.

Note: Intelligent doors controlled by AT1250 or ATS125x door controllers can be configured using the control panel menu (see “Doors Menu” on page 256). Intelligent doors controlled by CDC4 door controllers can only be configured using the configuration software. See also *CDC4(-EN) Door Controller Programming Manual*.

Use menu “Doors Menu” on page 256 to configure doors.

For reader, door zone and lock outputs default addressing, see “Zone, output, and door addressing” on page 34 in Chapter 2 “Installation”.

Note: It is not required to configure triggers to control door locks. The output set in menu “Door output” on page 257 overwrites output configuration.

Door groups

Door groups specify when access to a specific door is granted. Door groups are assigned to users. Each door group may have a different period (schedule) when access to different doors may be granted.

Door groups are programmed in “Door groups” on page 275.

You can assign door groups to users in “Door group” on page 224.

Floors

A floor is an element of the lift control functionality. A floor is a common area for all lift cars.

Floor groups

Floor groups specify when access to a specific floor is granted. Floor groups are assigned to users. Each floor group may have a different period (schedule) when access to different floors may be granted.

Floor groups are used in conjunction with door groups (see “Door groups” above).

Floor groups are programmed in “Floor groups” on page 278.

You can assign floor groups to users in “Floor group” on page 224.

Basic access control functions

Door shunt

Door shunt is a procedure that inhibits an open door, which could cause an alarm, for a set time.

A door can be shunted by a keypad or a reader, or a door controller. See “Doors Menu” on page 256 for details on door shunting.

Advanced access control functions

Regions

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.

Note that region 1 is “outside” region.

Use menu “Region” on page 276 to edit regions.

The menu “Regions” on page 273 allows you to assign specific door readers to regions.

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.

The following anti-passback types are available:

- Soft anti-passback: A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
- Hard anti-passback. A valid card or PIN *does not* open the door when used to enter the region a second time without leaving first. An attempt to do so generates a report.
- Regions anti-passback. A valid card or PIN *does not* open the door when used to leave a region other than the one entered previously. For example, if the user had entered region 3 from region 2, he will be denied when trying to enter region 2 from region 1. An attempt to do so generates a report.

Use menu “Anti-passback” on page 273 program the anti-passback for the selected door.

High security

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

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

Set HSU options in “High Security User options” on page 274.

Door controller macro logic

Every door controller may be programmed with macro logic to control its outputs depending on inputs and flags.

Note that this macro logic structure is different from AXON control panel condition filter programming.

These pages explain the door control macro logic principles.

Caution: It is very important to plan the macro logic carefully on paper, noting all details, and the origin of every zone and/or event flags, before attempting to program.

Macros

A macro is an evaluation and a decision-making device. It has up to four inputs and one output. There are 48 macros available for each door controller.

The four inputs may be individually configured to activate the output when active (OR) or, collectively joined (AND) so two or more inputs must activate to operate the output.

Notes

- All inputs may be optionally individually inverted using the NOT function.
- Any unused inputs should be set to OR.

The macros timers

The output has many timed and a latched option. Each of the timed options may be programmed in minutes or seconds within the range of 1 to 255.

- Disabled: Macro is disabled.
- Non-timed: Follows the result of the logic equation only. If a macro input (an event flag or an output) for this macro changes, the logic equation will be calculated again.
- On pulse [s]: Activates for the programmed time (in seconds) or the active period of the logic result, whichever is the shortest.
- On pulse [m]: Activates for the programmed time (in minutes) or the active period of the logic result, whichever is the shortest.
- On timed [s]: Activates for the programmed time (in seconds) regardless of the macro output changing.
- On timed [m]: Activates for the programmed time (in minutes) regardless of the macro output changing.
- On delay [s]: Activates after the programmed time period (in seconds) unless the result of the logic equation is no longer valid.
- On delay [m]: Activates after the programmed time period (in minutes) unless the result of the logic equation is no longer valid.
- Off delay [s]: Follows the result of the logic equation, but remains active for the time (in seconds) programmed after the result of the logic equation is no longer active.
- Off delay [m]: Follows the result of the logic equation, but remains active for the time (in minutes) programmed after the result of the logic equation is no longer active.

- **Latched:** Activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input. Any programmed AND / OR function is not used.

Note: In the Latched mode, the reset input 4 will not reset the macro's output while any of the inputs (1, 2, or 3) are active.

Pulsed lock and unlock

This function is only used on special electronic locks that require two separate relays to be pulsed at different times for it to open, and two separate zones for monitoring.

The two relays needed are taken from the relay specified in menu “Doors” on page 256. The “Door output” on page 257 specifies one relay, and door controller takes the next sequential relay number for the second relay it needs to operate the lock. For example, if output 17 is entered as an Unlock output number and this option is set to Yes, then outputs 17 and 18 are used for the lock.

Two zones are also needed for this operation to work. One for the normal door open contact (for example, reed switch) and one for the monitoring of the door lock status that comes from the electronic lock. The two zones needed are taken from options “Door zone” on page 259 and “Second zone” on page 267.

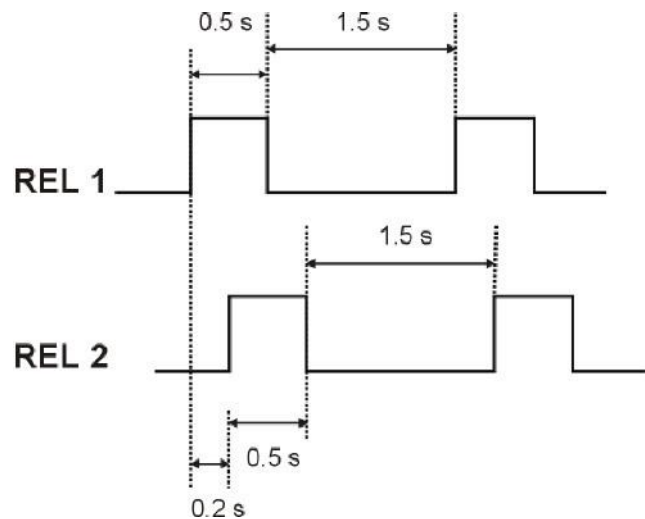
The function is programmed in “Pulsed Lock and Unlock” on page 268.

The specific operation is as follows.

Door Open procedure

On presenting a valid user at this reader, the second relay will pulse on for 0.5 s. After 0.2 s of the second relay switching on, the first relay will pulse on for 0.5 s. If according to the zone monitoring (explained below) the door has not opened, it will continue this procedure for the “Unlock time” described on page 258. If a “Door Unlock” command is sent, this procedure is permanently continued. The procedure continues every 1.5 seconds. See timing diagram in Figure 18 on page 84.

Figure 18

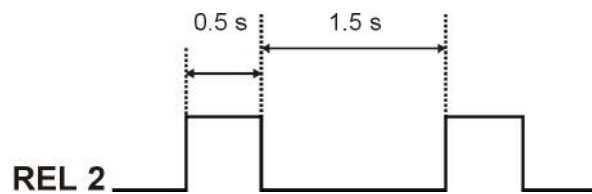


The difference between Door Open and Door Unlock is: The Door Open command only unlocks the door for the Unlock Time, whereas the Door Unlock command opens the door permanently until a Door Lock command is sent. See also “Door control” on page 189.

Door Lock procedure

The second relay will pulse on for 0.5 s. If according to the zone monitoring (explained below) the door has not closed, this procedure will continue until it does. See timing diagram in Figure 19 below.

Figure 19



Zone monitoring

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

- Door Open or Door Unlock: If the second zone is active and the first zone is normal.
- Door Lock: If the second zone is normal and the first zone is active.

Menu reference

The following menus are applicable for access control.

Menu	Page	Description
Door control	189	Send a direct command to a specific door.

Menu	Page	Description
Expander devices	205	Configure door controllers.
Door Control/Lift Control Expander Readers	217	Configure keypads and readers, connected to a door controller local bus.
Access options	224	Configure access control options for the selected user.
Doors Menu	256	Add, edit, or delete doors, door groups, and regions.
Access options	311	Various access control options.

Condition filters

A condition filter can be used to control outputs or user groups. Each filter has up to four inputs, and one output.

Four inputs may be individually configured to activate the filter when active (OR), or collectively joined (AND), so two or more inputs must activate to operate the output. A condition filter input can be an area, a zone, an event, or another condition filter output, etc. All dependencies are then calculated in turn.

Figure 20: How a condition filter works



Example of a condition filter use

Required action: when Area 1 is disarmed, entering the correct PIN or activating the keylock opens the door.

1. Select an appropriate condition filter using menu “Select filter” on page 280.
2. Change the name of the filter to “Door open” in menu “Filter name” on page 280.
3. In menu “Formula” program the condition filter as below:

#	Event or operand	Description
1>	Keypad.1.7	Correct PIN, entered on keypad 1.
2	OR	
3	Zone.10.1	Active Zone 10, which is connected to the key switch and set up in “Zones and areas” menu.
4	AND	
5	Area.1.3	Area 1 unset.

4. In menu “Outputs” on page 282 set the following values:
 - Select filter “Door open” for output 10. Output 10 can then be used to unlock a door.
 - Select Pulsed mode.

- Set Delay time to 00:00'00.
- Set Active time to 00:00'05 s.

Menu reference

The following menus are applicable for condition filters.

Menu	Page	Description
Pictures by filter	253	Configure condition filters that trigger the camera.
Condition filters	280	Add, edit, and delete condition filters.
Start filter	283	Specify a condition filter that activates the output.
Stop filter	283	Specify an optional condition filter that deactivates the output.
Filter	294	Assign an optional conditional filter, which enables the schedule.

Triggers

There can be up to 255 triggers in the system. They can be used in condition filters to control outputs remotely. See “Condition filters” on page 86 for more information.

Each trigger has a few independent flags that can be set or reset. These flags can be controlled by different means, for example:

- Schedule. See “Calendar” on page 89.
- SMS commands. See *SMS Control Reference Manual* for more information.
- Keyfobs. The keyfobs can be assigned to triggers in the wireless expander settings. See “Wireless device programming” on page 109 for details.
- AXON compatible PC software. Refer to Chapter 6 “Software” on page 363.
- Mobile application. See “Mobile Application” on page 125 for details.

Note: A trigger can only be controlled by users from the user group that is assigned to this trigger.

For the complete list of events that can change particular flags, see Appendix A “AXON events” on page 421, group “Trigger”.

See “Events” on page 92 for more information about trigger events.

Menu reference

The following menus are applicable for triggers.

Menu	Page	Description
Trigger state	176	Manually change trigger flag states.
Triggers	286	Add, edit, and delete triggers.

Calendar

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

The calendar is configured via menu “Calendar” on page 288 in Chapter 5 “Menu reference”.

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.

Maximum numbers of schedules, actions, time frames and special days in the system are listed in “Specifications > General features” on page 39.

Schedules are defined by the following parameters.

- **Date:** Start date and end date determine a 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.

Caution: Always define end time when using the time frame with one of the following: Access Enabled period, RTE On period, Low Security On period, and Unlocked period. Undefined end time (00:00) can lead to unspecified behaviour.

If no week day 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 90.
- **Filter:** A conditional filter that enables actions in the schedule when becomes true. See also “Condition filters” on page 86.

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 104.

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 toggling 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 week days selected and are repeated annually.

Special days are assigned to dates in the menu “View” on page 288.

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 rewound.

For more information on daylight saving programming, see “Time and date” on page 296.

Schedule shortcut menu

Most of system elements have schedule shortcut menu entry that allows you to quickly assign up to two schedules to the selected system element, for example, area, user group, etc.

```
1>Sel schedule 1
    Not used
```

Selecting a schedule brings you to a list of schedules defined in the system.

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

When you select a schedule for the selected element, or create a new one, the system adds an action to the selected schedule. The action contains the selected element.

To edit schedules, use menu “Schedules” on page 289.

Note: Available elements and parameters are described in “User programmable functions” on page 104.

Menu reference

The following menus are applicable for calendar and schedules.

Menu	Page	Description
Schedule	204	Assign schedules to the selected keypad.
Schedule	227	Assign schedules to the selected user group.
Schedule	249	Assign schedules to the selected area.
Schedule options	261	Configure schedule options for the selected door.
No schedule required	266	Extend the exit access for the selected OUT reader.
Schedule	286	Assign schedules to the selected trigger.
Calendar	288	Configure an automatic execution of specific actions at certain time and date.
Inspection	304	Set up a periodic inspection reminder.

Events

Log

All events are recorded in the AXON log. The log size is specified in “Specifications” on page 38, Chapter 2 “Installation”.

The log can be viewed using “Display logs” on page 170.

Note: The mandatory event log limits the number of repeating events to 3 within one set/unset cycle. The excessive events are stored in the extended event log instead.

See also “Alarm reporting” on page 98.

Programming

Events can be also used for user function programming. See “Condition filters” on page 86 for details. Events and groups of events, available for condition filter programming, are listed in Appendix A “AXON events” on page 421.

Menu reference

The following menus are applicable for events.

Menu	Page	Description
Display logs	170	Review alarm details
Log untested	177	If set to Yes, zones untested during walk test are recorded in the system log.
Log	235	Determine whether the zone event is recorded in the system log.
Pictures by reporting event	254	Allow the camera to be triggered by a selected reporting event.
Reporting	270	Determine when access control events are reported.
Condition filters	280	Configure condition filters activated by events.
Log limit	285	Limit recording of activating and restoring events from the selected output to three per one set cycle.
Rep. restore	314	Determine if the restore event is reported to the central station when a user acknowledges an alarm.
Call central station message	318	Display a message with advice for the user to call the central station when a report has been sent.
Reporting delayed	318	Enable a 30-second delay before alarm reporting required by ACPO regulations.
PD6662	318	Disable a delay for the specific case of the entry/exit zone reporting. This is required by ACPO regulations.
Anonymize Log	324	Set a period, after which the user details are removed from a log entry.

Menu	Page	Description
Central station	329	Configure central stations and reporting options.
Event options	338	Assign events to central stations and program the reporting delay.

Tests and diagnostics

The AXON system provides a range of test features. Most of them are accessible from “Test menu” on page 170.

Input and detector tests

To test single inputs or detectors, use “Input tests” on page 171. A single input state can be checked in “Zone kOhm” on page 173.

To verify wireless input status, use “RF RSSI test” on page 171 and “RF diagnostics” on page 172.

Wireless PIR camera range can also be verified in “RF Range test for Camera” on page 172.

If the detector has an internal test functionality, use “Detector test” on page 174 to configure an autotest, or to run it manually.

Test shock sensors via “ShockSens test” on page 174.

Outputs

Test outputs or verify their state using the “Outs&triggers” menu on page 175.

Walk test

Walk test is a working system test performed by a user or installer. To pass the test, the user or installer must walk past detectors to activate these. The intention is to test the functionality of the security system.

The zone passes the test when switching its state from normal to active, and then from active to normal. In walk test mode each zone state change is signalled by the keypad buzzer or an internal bell.

The menu “Walk test menu” on page 176 allows you to run the test manually (engineer walk test), as well as define conditions when the user has to perform the walk test, including a required walk test before setting an area (user walk test).

The menu also allows you to run a walk test for a single zone, as well as a general walk test, which is required by a central station operator to verify all alarm system features, including set and unset, entry and exit, tampers, etc.

Engineer walk test

The walk test initiated and executed by the service engineer.

The walk test applies to all zones that have option “Engineer walk test” on page 232 enabled.

Configure test parameters using “Walk test start” menu on page 177.

After this, run the walk test by “Walk test menu” on page 176.

Before walk test starts, you are asked if the reporting to central stations must be enabled.

```
With reporting
>Yes<
```

Choose Yes if all corresponding events must be reported to the central station. These include test events, walk test events, as well as activated zone list. If set to No, only a walk test result event is sent.

Note: If the reporting has been inhibited during installer logging in, the walk test reporting is disabled as well. See “Accessing the installer programming menu” on page 133 for more details.

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.

Note: The time period is programmed in “Reduced walktest” on page 178.

Choose a walk test scope and press Enter.

The Walk test start command starts the engineer walk test for zones that have the engineer walk test option enabled (see “Engineer walk test” on page 232).

The tested areas need to be unset.

Note: If zones that generate alarms regardless to the area state, for example, 24H type, are included in the walk test, they are suspended during the test, and do not cause an alarm. However, their activation is reported even if reporting is disabled during test start.

While the test is running, the list of untested zones scrolls automatically. The LCD displays a zone and the condition that must be achieved. For example, the screen below shows that zone 1 should be activated.

```
Zone 1
Need active
```

Zones disappear from the displayed list as they are tested.

When all zones are tested successfully, the following message is displayed.

```
Walk test OK
Press ENTER
```

The test is cancelled if the Clear key is pressed. There is also a maximum time limit on the test, set in “Walk test time” (see page 298). The test fails if this timer expires. If engineer reset fails and inhibit reporting has not been enabled when accessing the programming mode then a message is sent to the central station

to indicate that the test failed (see “Accessing the installer programming menu” on page 133).

Single zone walk test

You can also use “Single zone WT” on page 179 to perform a single zone walk test on the same rules as the engineer walk test described above.

Walk test mode

A special walk test mode allows verification of the whole alarm system functionality. In this mode, a service engineer or a guard must perform as many actions on the operating alarm system as possible. This may include set and unset, entry and exit, activating all detectors and tampers. The system operates as usual, sending all alarm and tamper events to the central station, except none of system sirens is active.

This allows the central station operator to review all received alarms and verify if appropriate system functions are working properly.

Active walk test

Active walk test allows you to test alarm reporting in case of a confirmed alarm simulation (required by ACPO).

Choose zone A for A-alarm, and zone B for B-alarm.

First, activate zone A, and then zone B.

The panel will simulate a confirmed alarm and send all appropriate reporting events to the central station.

Notes

- The tested zones must be one of the following types: 1. Alarm, 4. Fire, 5. Panic, 6. 24H, 7. Tamper, 13. Fire door.
- Options “Engineer walk test” on page 232 for these zones must be enabled.
- The user privileges in this area must have Walk test allowed. See “User groups” on page 226 for more details.

User walk test

If the user walk test is configured and enabled, the user is requested to perform the user walk test prior to setting an area. The frequency of this request is defined in “Frequency” on page 178. If the option “Need to set” on page 178 is enabled, setting an area without prior user walk test is not allowed.

Note: For walk test purposes AXON stores information on any zone activation for 4 hours. Therefore, if the zone was activated during the last 4 hours before walk test, it is not included into the list of zones required to test. If each walk test zone was activated during this time, the walk test is not requested.

Other tests

Communication

To configure automatic communication test or run it manually, use “Test call opts” on page 179.

Use the following menu to diagnose appropriate communication paths (if available):

- IP: “IP diagnostic” on page 181
- GSM: “GSM diagnostic” on page 183

Battery

Use “Battery test” on page 186 to diagnose the panel battery status. The menu also allows you to configure automatic battery tests.

UltraSync connectivity test

See “UltraSync > UltraSync path connectivity test” on page 124.

Menu reference

The following menus are applicable for testing.

Menu	Page	Description
Test menu	170	Access to all testing functions.
Soak test	232	Enable the soak test mode for the selected zone.
Engineer walk test, User walk test	232	Enable engineer and user walk tests for the selected zone.
Test picture to CS	255	Take picture and send it to a selected central station.
Soak test	300	Specify the number of days the soak test for a zone is active.
Test inputs	323	Define what inputs should be accessible when performing input tests.
Module info	353	Display GSM dialler firmware version, modem type, etc.

Alarm reporting

Alarm reporting is a procedure to transmit alarm events or other events to the central station by means of a dialler or other device, and a set of rules called a protocol.

The reporting features are configured via menu “Communication” on page 329 in Chapter 5 “Menu reference”.

Available reporting codes for different protocols are listed in Appendix B “AXON reporting codes” on page 437.

Reporting principles

See Appendix B “AXON reporting codes” on page 437 for a list of events that can be reported to central stations.

When a new event occurs, the system performs a few checks below before it is reported to central stations.

Is it mapped to any central station?

Every event in the AXON system has defined a particular set of central stations that it can be reported to. It is done via menu “CS mapping” on page 338.

For example, central station 1 is the Fire Brigade Station. All fire events then can be mapped to CS 1. CS 3 is a security company, which monitors burglar alarms. Burglar events as well as tamper alarms are mapped to it.

If the event is not mapped, is not reported anywhere.

Is this event already waiting for reporting?

If the same event (from the same area and source) is already waiting for reporting, such event will be reported only once.

Are there restored events?

There are two possible situations when two consecutive events are ignored during reporting:

- The new event is a restoring event for the other one, which is already waiting for reporting.
- The new event is an event, which restoring event is already waiting for reporting.

If the first complementary event is configured as a delayed one in “Delayed events” menu on page 338, both events are excluded from reporting.

For example, burglar alarm (BA) from area 1 is a delayed event, and the delay time is 30 seconds. The event is mapped to CS 1, as well as burglar restore event (BR). When there is an alarm in area 1, the event is waiting for reporting. When the user acknowledges the alarm, the burglar restore event occurs. If the

user does it before 30-second delay times out, no information is sent to the central station 1.

Note: The events do not exclude each other if they are mapped to different central stations.

Is this event a part of the combined OP/CL reporting?

If “OP/CL report” on page 333 is set to combined, only the initial area disarming (opening) and the final area arming (closing) in the group of areas with the same account code is reported to the central station. Other area set and unset events are not reported.

For example, premises include areas 1, 2, and 4 (that have the same account code). The owner unsets areas 1, 2, and then 4 on morning, and sets them in the same order on evening. The event is sent to the central station only when he unsets area 1 and sets area 4.

After all abovementioned conditions are met, the event is waiting to be reported. The possible reporting delay depends on whether it is a delayed event, what communication paths are available, and how many events with higher priority are already waiting for reporting.

Reporting order

If there are a few events waiting for reporting, and there are a few central stations to report to, the following principles are applied.

Connect to primary central stations

From all primary central stations that need to be communicated due to existing events and their mapping, the system starts establishing connection from the lower CS numbers to the higher ones.

For example, if there are events to report to primary central stations 1, 3, and 6, the system tries to contact the CS 1 first.

Note: The first connection attempt is always performed twice. The same applies backup central stations.

If the communication attempt fails, the system tries to contact CS 3, and then CS 6. If the CS 6 connection is also unavailable, the system starts with CS 1 again.

If there are configured the same delays and connection attempt numbers, AXON attempts to report to central stations in the following order:

1, 1, 3, 3, 6, 6, 1, 3, 6, 1, 3, 6, etc.

Use the backup central stations

In case the primary central station reporting fails, the system tries to send the event to the appropriate backup central station. For example, if there are primary central stations CS 1 and CS 4, and there are central stations CS 2 and CS 3,

which are backup stations for CS 1. AXON tries to report to central stations in the following order:

1, 1, 4, 4, 2, 2, 4, 3, 3, 4, 1, 4, 2, 4, 3, 4, 1, etc.

Note: To keep reporting order transparent, always program event mapping to backup central stations the same as mapping to primary central station.

Caution: Backup central station always applies to the previous one in the list. Be careful when deleting a primary central station, which has a backup central station. If you delete primary central station CS 1 in the example above, the control panel will immediately try to communicate backup central station CS 2, because the primary central station is not accessible anymore. See also “Mode” on page 331.

Report all necessary events to the central station

Once the communication to the central station is established, the system reports all active events that are mapped to this central station.

After all necessary events are successfully reported to the central station, the system closes the communication and tries to contact the next central station, which the active events need to be reported to.

Event priority

In the queue of events waiting for the central station reporting, events with higher priority are transmitted first. See Table 35 on page 437 for event priority values.

Failed to communicate (FTC)

Each central station has the “Retry count” described on page 331. When the unsuccessful communication attempts reached this limit, the system stops to try to report to this central station, and generates FTC fault for this station.

In FTC condition, the system still tries to re-establish the communication with the central station using test calls that are configured in the “Test call opts” menu described on page 179.

Note: If “Frequent test calls in case of FTC” on page 181 is set to Yes, the test call is attempted every hour until FTC fault restores.

If there are new events for this central station, the system starts communication attempts over again.

If due to retry limits the panel is unable to deliver an event to any of the central stations it is mapped to, the Global FTC fault is generated.

For example, there is the primary central station CS 1, and its backup central stations CS 2 and CS 3. The retry counter is set to four. AXON tries to report to central stations in the following order:

1, 1, 2, 2, 3, 3, 1, 2, 3, 1, <FTC 1 occurs>, 2, <FTC 2 occurs>, 3, <FTC 3 occurs>, <Global FTC occurs>.

When Global FTC occurs, unreported events are deleted from the reporting queue.

An event, which occurs after Global FTC, resets all reporting counters.

VdS channel reporting

If the VdS reporting is used, the control panel can report events using channels for block reporting.

In this case, each SIA event code is assigned to one of 26 event types, which are mapped to one or more of 16 reporting channels. The report contains the event name, a list of active channels, area number, event source, account number, etc.

The following event types are reported via VdS reporting.

Table 19: Channel mapping for VdS reported events

#	Description	Default channel
Input events		
1	Medical	10
2	Fire	1
3	Panic	2
4	Burglary	3
5	General	5
6	Test call	No channel is activated / restored
7	Technical Alarm 24 H	Not reported
8	Tamper events	4
9	Inhibit events	Not reported
10	Open/Close	8
System events		
1	RAS Code attempts	Not reported
2	Expander Offline	14
3	DGP Mains Fail	7
4	DGP Low Battery	6
5	DGP Tamper	4
6	Duress Code	9
7	Company Specific 1	Not reported
8	Company specific 2	Not reported
9	Company specific 3	Not reported
10	Sensor Fault	14
11	System Fault	14
12	System Restart	15

#	Description	Default channel
13	System Messages	14
14	Transmission Path 1 Fault	12
15	Transmission Path 2 Fault	13
16	Communication Fault	11
Area events		
1	Area 1	1 to 16
2	Area 2	Not reported
...		
64	Area 64	Not reported

Note: You need to assign a particular area to appropriate reporting channels to be able to receive events from this area. For example, the open/close event (channel 8) will be reported from area 2 only if Area 2 event is mapped to channel 8. By default, all input and system events are mapped to Area 1 only. Event types without a channel number assigned are not reported, except Test call event, which is always reported.

Channels can be remapped in the “VdS channels” menu described on page 338.

To activate VdS channel reporting, set the following options:

1. Set protocol to VdS. See “Protocol” on page 330.
2. Set Encryption key number and value. This information must be provided by the central station operators. See “Encryption key number” and “Encryption key value” on page 337.
3. Enable the “Send block status” on page 361.
4. If necessary, change VdS channel mapping. See “VdS channels” on page 338.

Menu reference

The following menus are applicable for alarm reporting.

Menu	Page	Description
Test call opts	179	Define the automatic test call interval, and perform a test call on demand.
IP diagnostic	181	Diagnostic tools for IP connectivity.
Remote options	222	Configuration menus for remote access.
CS report	235	Determine whether the zone event is reported to the central station.
Report as	254	Assign a SIA reporting event to the selected camera conditional filter.
Mains reporting delay	298	Define the delay time before a mains fail is reported to the central station.

Menu	Page	Description
Report BA	308	If set to Yes, in the part set the system reports burglar alarms triggered during part set to the central station.
Rep. restore	314	Report the restore event to the central station when a user acknowledges an alarm.
Call central station message	318	Allow the keypad to display a message with advice for the user to call the central station when an alarm report is sent.
Reporting delayed	318	Enable a 30-second delay before alarm reporting required by ACPO regulations.
Communication	329	Program all system-wide communication options.

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 certain types parameters are disabled.

Note: Certain functions require user code entering. To disable it, switch off the User code required option, if allowed. See “User code requirement” on page 133 for details.

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

Table 20: 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 group selection 3. User code requirement
Unset	Unset areas [1]	1. Area selection 2. Area group 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

Type	Description	Available parameters
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
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 group 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. See “User group options” on page 227 for more details. Note that the user group type must allow this change. See “User group type” on page 226 for details.
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. These outputs are switched on simultaneously for the longest period configured in “Activation” on page 297. 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

Type	Description	Available parameters
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 group selection
Prohibit unset	Disable area unset. Note: If unset is prohibited, it is only possible to unset using a Downloader Command and Control session.	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
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. See “Quick set mode” on page 200 for more details.
- [2] Set and part set function start time is the time when the warning timer is started. The warning time must be taken into account. See “Autoset warning time” on page 246 for more details.
- [3] The function is an entry to the appropriate user menu. See *AXON Control Panel Manager Manual* for more details.
- [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 Chapter 3 “System functions > Counteractions” on page 90.

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

- Schedule. See “Calendar” on page 89 for more details.
- Function key. See “Function keys” on page 65.
- Fob. See “Wireless device programming” on page 109 for more details.

Menu reference

The following menus are applicable for user programmable functions.

Menu	Page	Description
Function keys	201	Assign a user programmable function to any of available function keys.
Buttons	251	Assign an appropriate function to a button or a button combination.
Action list	289	Select actions that must be performed by the system according to the selected schedule.

Autoset

The AXON system allows autoset configuration. The system can be set automatically via schedule.

The following options must be considered when providing an autoset facility.

- Using menu “Calendar” on page 288, create an action with Set function. See also “User programmable functions” on page 104.
- Configure an appropriate schedule using the menu “Schedules” on page 289.
- Enable or disable “Autoset silent mode” option on page 248.
- If necessary, set “Autoset retry” option on page 247.

If Set retry is allowed, configure “Autoset user retry” on page 310.

- Set “Autoset warning time” option on page 246 as well.
- Optionally, configure “Autoset retry on system fault” option on page 310.

Menu reference

The following menus are applicable for autoset.

Menu	Page	Description
Autoset warning time	246	Period during which the automatic set procedure can be postponed.
Autoset retry	247	Define whether users can postpone or cancel an autoset.
Autoset silent mode	248	The keypad buzzer remains silent during the warning time.
Calendar	288	Configure an automatic setting at certain time and date.
Autoset retry on system fault	310	Define if and when the system repeats an attempt to set automatically in if a system fault has made an autoset impossible.
Autoset user retry	310	Define a time for which a normal user can postpone an autoset.

Wireless device programming

To add a wireless device, follow one of the following procedures.

Learning wireless sensors

There are two modes available for learning a wireless device, sequential and manual.

Sequential mode

In sequential mode, you can quickly learn a range of wireless sensors.

To learn sensors in sequential mode:

1. Go to the “Add zone” menu described on page 228.

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

2. Select zone location.

```
Learn mode
>Sequential<
```

3. Choose Sequential mode and press Enter.

```
INFO
Tamper RF 1
```

4. Activate the wireless device. See “Device activation” on page 114 for more information about activation.

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

Example:

```
ERROR
RF duplicate
```

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

If the device is programmed successfully, the keypad beeps twice.

If there are more wireless devices to program, and the consecutive wireless zones are available in the wireless expander, repeat activating another wireless device.

```
INFO
Tamper RF 2
```

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

If next zones are already occupied on the wireless expander, the learning process is over.

Proceed with the zone configuration.

Manual mode

In manual mode, you can learn and configure a wireless sensor.

To learn a sensor in manual mode:

1. Go to the “Add zone” menu described on page 228.

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

2. Select zone location.

```
Learn mode
>Manual<
```

3. Choose Manual mode and press Enter.

```
Tamper RF 1
Press # for ID
```

4. Activate the device, or press Enter to enter the wireless device identifier manually. See “Device activation” on page 114 for more information about activation.

```
Sensor ID
> <
```

Note: Learning a wireless PIR camera by entering its identifier is not supported.

The sensor ID is printed on a barcode sticker on the sensor box in the following format: “Tx H<nnnnnnnn>”. For example, “Tx H103EB2B” mark identifies a sensor with the ID 103EB2B. See also “Sensor identifier” on page 242 for more details on sensor identification.

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

```
INFO
RF exists
```

Next you are asked if you want to replace the programmed wireless device.

```
Replace RF dev?
>No<
```

Note: If the programmed device has two inputs capacity, the system asks should the device occupy two zones. See “Two-zone RF sensors” on page 113.

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

```
INFO
RF learned
```

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

```
Edit zone?
      >No<
```

Chose Yes and press Enter to edit zone settings.

Otherwise you are asked if you want to learn another wireless device.

```
Next zone?
      >No<
```

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

Note: If learned wireless device is a wireless PIR camera, you are also asked to edit settings of the created camera.

```
Edit camera?
      >No<
```

See “Using wireless cameras” on page 116 for more details.

Learning fobs

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 “Add fob” menu described on page 250.

```
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 “Device activation” on page 114 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 “Add fob” menu described on page 250.

```
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 “Device activation” on page 114 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<
```

Choose Yes and press Enter to edit fob settings.

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

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

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

Two-zone RF sensors

Particular RF devices, for example, door/window sensors and shock sensors, have two inputs on-board. If both inputs are enabled in the device, during the configuration process the system asks if two zones should be used to report these inputs states.

Note: For two zones to be visible upon device learning process, the device must have an appropriate configuration during the activation. See Table 21 on page 114 for more details.

```
1 or 2 zones
  >2<
```

If 1 zone is selected, this zone functionality depends on sensor configuration. See “Sensor options” on page 243.

If 2 zones are selected, the device must occupy two consecutive zones.

If the second zone has been already programmed, there is an error displayed.

ERROR
Not possible

Device activation

Depending on the device type, the learning activation of this device can differ. Table 21 below lists all compatible devices and their activation methods.

Table 21: Wireless device learning activation

Device type	Learning activation
Door / window sensor	Raise a tamper alarm by opening the housing. Notes - For two zones programming in sequential mode, the external contact input must be in open state. - Two zones programming in sequential mode is not possible with LoNa door / window sensor. The second zone must be added manually.
Shock sensor	Raise a tamper alarm by opening the housing. Note: For two zones programming in sequential mode, the reed contact must be enabled and closed with the magnet.
Smoke detector	Raise a tamper alarm by removing the detector head from the base.
PIR camera	Raise a tamper alarm by removing the PIR camera from its mounting plate.
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.

See the appropriate wireless device manual for more information about the device functionality.

Menu reference

The following menus are applicable for wireless devices.

Menu	Page	Description
RF RSSI test	171	Display received signal strength indicator (RSSI).
RF diagnostics	172	Display wireless device status.
RF Range test for Camera	172	Verify wireless PIR camera signal reception.
Expander devices	205	Configure wireless expanders.

Menu	Page	Description
RF fobs	221	Configure the selected user fobs.
RF details	242	Program a wireless device manually or remove it from the wireless expander.
RF fobs	250	Configure fobs.
Cameras	252	Configure camera modules in wireless PIR cameras.

Using wireless cameras

A wireless PIR camera is a wireless PIR detector with a camera built in. The camera can be programmed to take pictures in case of activation of associated zones, conditional filters, as well as by manual activation or remote requests.

After an alarm the associated pictures are sent to a central station via IP/GPRS. Pictures can also be viewed from configuration software.

Configuration

The system with a wireless PIR camera expander can have up to 8 wireless PIR cameras programmed. Each camera can be activated in case of the following events:

- Activation of one of 4 assigned zones. Zones are assigned in menu “Pictures by zone” on page 253.

In this case camera event type depends on the zone type. See “Camera event types” below.

See also “Zone types” on page 49.

- Activation of a condition filter. The event type is defined for the programmed filter. See “Cameras” on page 252.
- Activation of a standard reporting event. See “Pictures by reporting event” on page 254.
- User command.
- Remote request from configuration software.

The number and the quality of pictures taken depend on the camera event type.

Camera event types

There are the following camera event types available.

- Burglar alarm. Generated by alarm, entry/exit, access, 24 H, fire door and keybox type zones.
- Fire alarm. Generated by fire zones.
- Panic alarm. Generated by panic zones.
- Medical alarm. Generated by medical zones.
- Tamper alarm. Generated by tamper zones.
- Fault. Generated by technical, transmission fault, aux mains fault and aux battery fault type zones.
- Custom type 1. Generated by conditional filters of this type.
The types are assigned to conditional filters in “Event type <n>” on page 253.
- Custom type 2. Generated by conditional filters of this type.

Event type details are listed in Table 22 on page 117.

Table 22: Camera events and reporting codes

Event type	Activated by zone type [1]	SIA code [2]
Burglar alarm	1. Alarm, 2. Entry/Exit 1, 3. Access, 6. 24H, 13. Fire door, 16. Key box, 18. Entry/Exit 2	BA
Fire alarm	4. Fire	FA
Panic alarm	5. Panic	PA
Medical alarm	10. Medical	MA
Tamper alarm	7. Tamper	TA
Fault	11. Technical, 12. Transmission path fault, 14. Aux mains fault, 15. Aux batt fault	UA
Custom type 1	Not allowed [3]	Selectable [4]
Custom type 2	Not allowed [3]	Selectable [4]

[1] Zones of certain types do not activate camera. These are 8. Exit terminator, 9. Keyswitch, 17. Eng. reset. When an assigned zone is one of the listed types, it is ignored when active.

[2] If the camera has been activated by a standard reporting event, another event caused by camera activation does not occur. Detailed codes and subevent values are described in Appendix B “AXON reporting codes” on page 437.

[3] Custom type events can only be activated by condition filters.

[4] See “Report as” on page 254 for details.

Each of these types can be configured in “Pic settings” on page 211.

Depending on camera event type, the camera can be programmed to take a single picture or a series of pictures, in low or high resolutions.

How to program a camera:

1. Program the wireless PIR camera expander. See “Bus devices” on page 67 for more details.
2. Program a wireless PIR camera as a wireless PIR detector. See “Wireless device programming” on page 109 for more details.

If the detector is programmed successfully, the appropriate camera is created automatically. The created camera number is equal to the zone number of the wireless PIR detector.

3. Program the camera options. See “Cameras” on page 252.
4. Assign zones to the camera. Choose up to four zones. The camera is useful if its field of view covers these zones or possible burglar escape paths from there. See “Pictures by zone” on page 253.

By default, the first assigned zone is the zone of the wireless detector built in the configured wireless PIR camera.

5. If necessary, program conditional event filters that activate the camera. See “Cameras” on page 252 for details.
6. If necessary, program reporting events that activate the camera. See “Cameras” on page 252 for details.

Diagnostics

If necessary, use the following menus for diagnostics:

- “RF RSSI test” on page 171
- “RF diagnostics” on page 172
- “RF Range test for Camera” on page 172

Menu reference

The following menus are applicable for wireless PIR cameras.

Menu	Page	Description
RF RSSI test	171	Display received signal strength indicator (RSSI).
RF diagnostics	172	Display wireless device status.
RF Range test for Camera	172	Verify wireless PIR camera signal reception.
Expander devices	205	Configure wireless expanders.
RF details	242	Program a wireless device manually or remove it from the wireless expander.
Cameras	252	Configure camera modules in wireless PIR cameras.
Central station	329	Set photo transmission options.

Troubleshooting

See also Chapter 7 “Troubleshooting” on page 371.

Camera busy message

Camera busy message may appear when a camera or a wireless expander does not respond to a request because one of the following operations is currently in progress:

- Erasing picture memory on the wireless expander
- Running RSSI test
- Running RF diagnostic test
- Running range test
- Setting camera mode (for example, unsetting the system)
- Taking pictures according to other requests
- Running walk test
- Learning in camera
- Updating current state (occurs for 2 to 3 s every 17 minutes)

Solution: repeat the request after a delay of a few seconds.

Camera error message

Camera error message appears due to one of the following states:

- Processing another request for longer than 20 s (for example, reporting pictures for previous request for this camera)
- Communication failed

Solutions:

- Repeat the request in a few minutes
- Verify power supply
- Verify communication quality

See also “Diagnostics” on page 118.

OH receiver line trouble when MMS sending

AXON control panel provides an option to send pictures from PIR cameras to an Osborne-Hoffman NetRec receiver, and MMS to users in parallel.

When control panel is sending MMS, the heartbeat message is suspended. If this delay is longer than the supervision period, for example, due sending multiple MMS, the receiver generates a fault.

Solution: The supervision period in OH receiver should be longer than it can take to send 10 pictures (VGA) and extended by a time necessary for APN switch. This period is approximately 7 minutes. Note that weak GSM network conditions may extend this time.

Engineer reset

Some events can be set to require an engineer reset to be performed. The engineer reset can be done in one of the following ways:

- The engineer (installer) performs an engineer reset from the Engineer menu. See “Do reset” on page 303.
- The user enters a reset code.

In case an engineer reset is required, an engineer code is displayed.

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

In this case the user contacts the engineer (installer) and gives him the engineer code displayed. Using this code and the system code defined in the menu “System code” on page 303, the installer calculates a reset code, which he gives to the user. The user enters the calculated code and performs an engineer reset after logging in.

Note: If System code is not defined, the engineer reset by user is not available.

- The reset is performed by an activation of the special Engineer reset zone type (see “Zone type” on page 229). This is used in systems using RedCare transmitters, where the central station operator can switch an output that is wired back into the panel to perform an engineer reset.

Menu reference

The following menus are applicable for the engineer reset.

Menu	Page	Description
Engineer reset	301	Define which conditions require an engineer reset, perform the reset.

Timed unset / ATM

ATM (automatic teller machine) is secured with an additional functionality that includes the following:

- Double code unset. The ATM user must enter the code, and then enter it again after the programmed delay period.
The delay is set in “Delay” on page 327.
After this delay, the user is prompted to enter the code again.
The user must belong to a user group with Timed unset / ATM type. See “User group type” on page 226 for details.
- Timed unset. The ATM is unset for a programmed time period. This period is defined in “Unset Time” on page 327.

The keypad displays the remaining unset time.

```
Time left 11 min
```

- Extended time. The user can extend the unset time for an additional time period, if this period is set in “Extended Unset Time” on page 327 as longer than 0.

```
Time left 11 min
* to extend time
```

Press * to extend the unset time. The unset time can be extended only once.

Note: The Timed unset / ATM functionality is only available on LCD keypads.

Menu reference

The following menus are applicable for the timed unset.

Menu	Page	Description
Timed Unset / ATM	327	Configure the ATM (automated teller machine) interface options, for example, unset delay and extended unset delay.

UltraSync

UltraSync is a secure cloud solution, connecting alarm devices to remote application via a managed web portal, supported by a service model. The UltraSync connectivity can be enabled in the control panel, Advisor Advanced Pro mobile application (IOS/Android), and the ATS85xx software.

Path communication to the UltraSync cloud can be single or dual: via the on-board Ethernet connection, and GSM/GPRS communicator (ATS73x0) connected to the panel.

The events can be delivered via push notification to the mobile devices of maximum 16 users.

Note: A push notifications can only be received if the phone is switched on when the notification is being sent, and the mobile application is running. The UltraSync cloud does not store the notifications after sending it to the push notification service provider, so there is no way to ensure that the notification reaches the smartphone, as it only depends on a connection quality between your smartphone and the push notification service provider.

Caution: When the panel is registered in the UltraSync cloud, all security cloud reporting is configured remotely from the cloud. In this case, account code settings are disabled for this central station.

The panel is identified in the UltraSync cloud by its unique serial number. The serial number is shown in the “SID number” screen described on page 358.

It is necessary to set an UltraSync password to be able to connect the panel remotely using Downloader or Mobile Application via UltraSync secure cloud.

Caution: The Internet connection is necessary to activate UltraSync functionality. Ensure that the panel IP and DNS addresses are valid. See “IP specific options” on page 341, “GSM/SMS/GPRS specific options” on page 345, and “IP diagnostic” on page 181.

UltraSync connection uses port 443 and the following addresses: at1.zerowire.com and at1.ultraconnect.com. Ensure that your firewall allows this. The addresses may change in the future. Contact your security service provider to find out what addresses must be allowed by firewall.

Service model

There are two models of the service provided by UltraSync security cloud:

- Basic Service model
- Portal Service model

In the Basic Service model, you use the unique serial number in the Mobile Application and Downloader to connect in an easy way. This model includes smartphone push messages. The alarm reporting must be configured by the

installer to an OH Receiver using Ethernet or a GSM module for communication. When you use the mobile connection, you need to use your own SIM card.

In the Portal Service model, you use all features of the Basic model, and additionally you can gain access to the UltraSync Web portal. This portal allows you to register panels in order to link them to a central station of choice, and run reports or view statistics on all your connected panels. As a part of the model an UltraSync SIM card can be applied for the cellular connection. To gain access to the Web portal, you need to request access via the KGS sales office and sign an UltraSync order form.

Registering the panel in UltraSync cloud

Registering the panel in the UltraSync portal is linked to a monthly service cost.

Unregistered panel does not support UltraSync SIM cards. Also, the UltraSync communication path monitoring is not supported.

Web portal and diagnostic functions are not available when the panel is connected to the UltraSync cloud using a third-party SIM card.

UltraSync SIM card

ATS734x-SIM is an ATS734x GSM module with a preinstalled UltraSync SIM card. This module and its SIM card should be used for UltraSync functionality only when the panel is registered in the UltraSync portal. *Registering the panel in the UltraSync portal is linked to a monthly service cost.*

KGS reserves the right to check if the UltraSync SIM card is used in the correct modem. Improper use of the modem or SIM card can result in the product to stop operating with the UltraSync infrastructure.

Note: UltraSync SIM card does not support SMS and GPRS OH reporting.

Caution: When using UltraSync SIM card, ensure that the APN name is empty. See “APN” on page 351.

Configuring a control panel from mobile application

See “Mobile Application” on page 125 for information.

Creating a site in Web portal

Each panel is represented as a site in Web portal. To add your site in the UltraSync Web portal, do the following:

1. Ensure that your panel is connected to the secure cloud via Ethernet or GPRS.
2. Sign in on Web portal using the URL address and credentials obtained from the manufacturer.
3. On the list of available sites (panels), click New Site.
4. Select your central station (defined by the manufacturer), or choose Self-Monitoring.

5. Provide your site name, which identifies your site in Web portal.
6. Enter the site address and contact information, if necessary.
7. Enter your panel serial ID number, which can be found on the package box, or in the “SID number” screen described on page 358.
8. Select your time zone.
9. Choose a reporting channel (VFNN).
10. Enter the account number.

Note: Web portal allows only one account number per panel to be defined.

11. Enter the required service grade.

Service grade defines security grade and reporting communication path, which can be IP (Ethernet), cellular (GPRS), or dual path (IP primary reporting and cellular backup reporting).

12. Select the reporting format, required by the central station.
13. Click Create.

Your site is now created.

For its monitoring and control, see the appropriate Web portal manual.

UltraSync path connectivity test

The monitoring station should be notified before a test is carried out.

If the panel is connected to UltraSync via dual path, the test must be carried out for each type of connection, Ethernet, and GSM.

It can be done by removing the other connection:

- To verify the Ethernet connection, remove the SIM card.
- When testing the GSM connection, disconnect the Ethernet cable.

To conduct the test, use the following menus.

- Installer: Man. test call
- Supervisor: 8.3 Manual test call

Menu reference

The following menus are applicable for the UltraSync functionality.

Menu	Page	Description
Transm path	330	Set the central station communication to UltraSync Cloud.
UltraSync options	358	Configure UltraSync communication.

Mobile Application

Advisor Advanced Pro mobile application allows users to monitor and control your AXON 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. If you want to use the walk-test functionality of the application, please collaborate with the supervisor.

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 option “Allow remote access to configuration by Supervisor” on page 319 must be set to Yes.

Menu reference

The following menus are applicable for the mobile application functionality.

Menu	Page	Description
User menu	219	Add, edit, or delete users and user groups.
Cameras	252	Configure camera modules in wireless PIR cameras.
Outputs and filters	280	Configure outputs.
Allow remote access to configuration by Supervisor	319	Enable remote supervisor access
Communication	329	Program all system-wide communication options.

Site Manager

Introduction

The application allows users in real-time, updated information about their installations, ensuring a seamless experience.

From site provisioning to future detector configuration, the UltraSync Site Manager App redefines convenience and efficiency for UltraSync users.

Key features

- Site provisioning
- SIM provisioning
- Panel remote access
- Event history
- Sensor configuration for future products
- Search and filter on the installations, easy and accessible overview
- Easy login procedure – similar to the UltraSync web portal login

Installation

To install Site Manager on your smartphone, go to the UltraSync Site Manager webapp address: <https://webportal.ultraconnect.com/pro>.

Alternatively, download the application directly from the stores using one of the following links:

- UltraSync Site Manager in Google Play:
<https://play.google.com/store/apps/details?id=com.aritech.ngms>
- UltraSync Site Manager in App Store:
<https://apps.apple.com/se/app/ultrasync-site-manager/id6504744039>

Refer to *Site Manager User Manual* for more information.

See also “UltraSync” on page 122.

Menu reference

The following menus are applicable for the Site Manager functionality.

Menu	Page	Description
User menu	219	Add, edit, or delete users and user groups.
Communication	329	Program all system-wide communication options.

Securing card data

The card data can be secured when using secure devices with smart cards. To secure the data, the following functions must be activated:

- **Secure mode:** The card data sent from a smart card to a secure device is secured using AES encryption.

The following devices support this mode: ATS118x, ATS1125, ATS1136, ATS1140.

- **Secure channel:** The data sent from a secure device to the control panel through the data bus is secured with AES encryption.

The following devices support this mode: ATS118x, ATS1125, ATS1136, ATS1140, CDC4(-EN).

Secure mode

In secure mode, the card is identified by the data encrypted and recorded on it instead of its serial number. The card data can be read only if the secure key programmed in the panel is correct.

The secure mode is enabled in menu “Secure mode” on page 325.

Note: This is a system wide setting. If the feature is enabled, it is applied for these devices automatically.

The secure key is programmed in menu “Application key” on page 325.

Application name and file ID

In the secure mode the smart user card may contain multiple data for various applications.

The control panel, which grants the access to the user with a card, is identified as one of applications and application file numbers defined on this card. The system application name is set in “Application name” on page 325, its file number is set in “Application file ID” on page 325.

There can be up to 32 files for each application. Application file IDs are hexadecimal numbers from 00 to 1F.

You can use one smart card in more systems or control panels by using different application names and file IDs. For example, a card can have access to six control panels with file IDs from 01 to 06 for application “555443”, which covers security systems.

Note: Each file is encrypted with its own application key. See also “Application key” on page 325.

Secure channel

Secure channel is used for communication between secure devices and the control panel through the data bus. If the secure channel is enabled, the data sent is AES encrypted.

Note: This is a system wide setting. The secure channel is enabled automatically if the device supports this functionality. The encryption key for the secure channel is negotiated between the device and the control panel, and is not accessible for users.

Caution: Your system data bus must be physically secured against unauthorized access when the secure channel encryption key is reset, for example, during the following processes:

- System installation and commissioning
 - Panel defaulting (see “Default panel” on page 193 and “Default” on page 326)
 - Initial start-up (see “Initial start-up” on page 163)
 - The recovery procedure (see “Recovery procedure” on page 372)
 - The communication key reset (see “Reset comm. key” on page 205)
-

If an existing device is replaced by a new one, the new device does not know the encryption key and therefore the communication between the device and the panel cannot be established. Use menu “Reset comm. key” on page 205 to reset the encryption, so the panel and the device can negotiate a new encryption key.

Caution: The encryption keys should only be reset when replacing an existing device (for example, faulty one) without reconfiguring it. This operation uses the default encryption key. You should only reset encryption key when the system is fully secured against a physical intervention and its data bus is protected.

This also applies when defaulting control panel if there are secure channel devices used.

Configuration card

Secure devices like ATS118X readers and ATS1136 keypads with readers can be programmed sequentially using a configuration card.

To prepare the configuration card, follow the steps below:

1. Program all reader security settings using menu “RDR security” on page 324.
2. Program the configuration card with the same configuration key, as set in the control panel.

Use menu “Config card” on page 192 to suspend polling of new devices for 30 minutes, which will make possible to sequentially program each of them.

Note: You can reset the secure key in the secure reader ATS118X using the configuration card. To do this, disconnect the communication wires from the reader and badge the configuration card on the reader when it is powered up. This functionality is available in secure readers with firmware version 0.3 or newer.

Troubleshooting

Secure communication is only secure between two devices when both devices agree on proper secure keys. If these are not aligned, the communication fails, for example, the LCD keypad shows System Fault, and it cannot be polled by the control panel. This requires a reset on one or on both devices.

This may happen when:

- The control panel is replaced, but secure devices (CDC4(-EN), keypad, reader) remain
- Installing a device, which was previously used on another control panel or CDC4(-EN) door controller
- A device is replaced by a new device of the same type

In general, this requires actions on both device and panel side.

To reset the secure channel key on the device:

CDC4(-EN) door controller. Set test link 1 for a few seconds, then remove.

ATS1125 keypad. Follow these steps:

1. Remove the keypad from the mounting plate.
2. Perform the keypad power cycle. To do this, pull the terminal block out of the keypad to disconnect the power, then plug it back again.
3. Right after restoring the power, press and hold the MENU button until the keypad shows the Keypad internal installation menu.
4. Once the internal installation menu is displayed, use the Up and Down keys to select the Reset menu option. Then, use the Left and Right keys to select the SC key. Finally, press Enter to confirm the security channel key reset.
5. Press X / Clear to exit the menu.

The keypad is restarted.

6. Close the device housing and mount the device on its mounting plate.
7. Confirm the tamper alarm in the panel if necessary.

ATS1140 Touchscreen interface. Follow these steps:

1. Perform the interface power cycle. To do this, pull the terminal block out of the interface to disconnect the power, then plug it back again.
2. Right after restoring the power, click Set Address on the Settings > Info Screen.
3. Do not change the current address. Click CHANGE.

This resets the secure channel key. The device will restart.

See also “Programming the system using Touchscreen” on page 140.

ATS118x series reader. Follow these steps:

1. Disconnect the D+ and D– wires from the reader and wait until the reader enters error mode.
2. Present the ATS1482 address cards. The reader should provide feedback by sounding the selected address.
3. Connect the D+ and D– wires to the reader.

Note: ATS1136 does not require an action for security keys reset. If it indicates System Fault, refer to Chapter 7 “Troubleshooting” on page 371.

AXON control panel. To reset the control panel side there are two possible options:

- If the problem occurs on keypad 1, press the PIN bypass push button on the panel board for a few seconds. See Figure 3 on page 10 for the PIN bypass push button position.
- For any other device, enter the installer programming menu, and then go to “Device menu > Edit Keypad&Exp” on page 195. Next, select RKP or EXP whichever is required, and the address of the device to reset. Select “Reset comm. key” on page 205 to reset.

Menu reference

The following menus are applicable for the secure mode and secure channel functionality.

Menu	Page	Description
Config card	192	Suspend polling of new devices for sequential programming with a configuration card.
Linked Reader	199	Link a reader to the selected keypad.
Reset comm. key	205	Reset the encryption between the panel and the device.
RDR security	324	Reader security settings.

Chapter 4

Programming

Summary

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

Content

Programming methods 132

The AXON menu 133

- Accessing the installer programming menu 133

Programming the system using LCD keypad 135

- How to access the installer programming menu using LCD keypad 135

- What the LCD display tells you 136

- Editing the options 136

- Confirmation of changes 138

- Exit from menu 138

- Keypad layout 139

Programming the system using Touchscreen 140

- Introduction 140

- Main screen 140

- Authorization 142

- Emergency alarms 142

- Function keys 143

- Idle screen 143

- Set / Unset 144

- Main menu 146

- Internal menu 153

- Terminal mode 154

- Settings 154

- Initial installation 158

- Reinstallation and defaulting 158

Programming the system using WebApp 159

- Secure connection (SSL) 159

Remote access 162

Initial start-up 163

- Auto configuration 165

Programming methods

Once your devices have been cabled and installed, there are the following ways to access and program your system:

- Using an LCD keypad. The LCD keypad offers a programming menu allowing full system configuration. This manual will assist you in navigating the menus.
- Using a touchscreen keypad. The touchscreen provides a graphical user interface for system control and programming. See “Programming the system using Touchscreen” on page 140 for more information.
- Using Downloader software. All features can be programmed using a PC with Microsoft Windows 7, 8 and 10. Downloader allows easier programming of complex sites as the graphical interface can show all options from multiple menus simultaneously. See also Downloader Online help.
- Via a built-in WebApp. All features can be accessed from a web browser. No software installation is required. This allows access to most commonly accessed features for basic programming or minor changes. See also “Programming the system using WebApp” on page 159.

The AXON menu

PIN authorization

If you attempt to select an option that is not authorized for your PIN (for example, user menus), the display shows the message:

ERROR
Access denied

Note: When an incorrect PIN is entered three times the keypad is locked for 120 seconds.

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)
- Panel variant configured during the initial start-up. See “Initial start-up” on page 163 for details.

Accessing the installer programming menu

The AXON system is programmed from the installer programming menu. Before accessing the programming menu, the system administrator must unset the areas that will be configured. Depending on the system settings, you also can be prompted to open the panel housing prior to configuring the system.

User code requirement

The system can be configured to prevent the installer from accessing the menus without permission from the manager. This is required, for example, by EN 50131 regulations. This is set in the menu “User code required” (see page 301).

Challenge code requirement

The system can be configured to prevent the installer from accessing the menus without permission from the central station operator. In this case the installer gets a 10-digit request code displayed on LCD when entering the menu. He must call the central station and provide this request code to the operator. Next, the central station operator generates a unique challenge code and provides it to the installer. The installer then uses this challenge code to access the programming menus.

This code is valid during the time set in “Inst in-time” on page 299. The option is enabled in “Challenge code” on page 304.

Area selection

If the option “Config in set state” described on page 327 is set to No, the system can be programmed only after all areas are unset and put in the service mode. In this mode, no alarms and faults occur.

If the option “Config in set state” is set to Yes, the installer is prompted to choose unset areas, where the service mode will be activated, when entering the programming menu. The area selection list is the same as the set/unset area list. See *AXON Control Panel User Manual* for details.

The selected areas will be excluded from normal operation. Users will not be able to control these selected areas until the installer exits the programming mode.

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

Programming the system using LCD keypad

The complete programming map is shown in “Keypad programming map” on page 388.

How to access the installer programming menu using LCD keypad

1. Start with this LCD display:

```
Aritech
TUE 27 May 10:00
```

2. If the option “User code required” (see page 301) is set to Yes, the engineer access must be granted by the manager first. The manager must log in, activate the “Service In” option, and logout. Now the installer can login within the time defined in “Inst in-time” on page 299.
3. Press Menu. The display shows:

```
Enter card/code
>_
```

4. Enter your PIN and then press Enter.
Alternatively, and if configured, you may also present a card to the reader.
5. Select the areas that service mode will be activated in, and press Enter. See “Area selection” on page 134 for details.

The following display appears:

```
Inh reports
>Yes<
```

6. Select Yes if you want to inhibit all reports during system programming. Reports include reporting to central station as well as reporting events in the logs.
7. Press Enter. The next screen shows whether tampers are inhibited, and areas are unset:

```
Inh tampers
Unset areas
```

8. Press Enter again. You are now in the programming menu. The following display appears:

```
1>Service menu
2 Device menu
```

From this display you can now:

Option	Action	Result
Change selection	Press Up or Down	Select previous or next menu entry

Option	Action	Result
Enter the menu entry	Enter menu entry number, or Press Enter or Right to enter the selected one	Jump to a specific menu entry
Show help	Press Help	The description of the selected menu entry is displayed (if available)
Exit the menu entry	Press Left or Clear	Exit the menu entry

You can now select the menu option you want to program. See “Keypad programming map” on page 388 for a diagram of all the menu entries available in the programming menu.

What the LCD display tells you

The LCD display on the keypad has two lines of characters.

A programming option occupies both lines:

```
Expander number
>_<
```

A menu command usually occupies one line. Two commands of a menu are shown below:

```
1>Keypad devices
2 Exp devices
```

Certain menu entries occupy the whole screen, and the line “>>>” indicates a submenu.

```
3>Keypad options
>>>
```

Editing the options

Once you have selected the menu option you want to program, most options can be programmed using the standard procedure shown in “How to program” below.

How to program

The method of programming depends on the options to be programmed. Some options require a value, others require a Yes/No setting.

How to program values

```
3 Entry time
>_<
```

- 1 to 0: Enter the new information
- Enter: Confirm the entry
- Clear: Exit without changes

How to program Yes/No options

```
01 Zone alarm
    >Yes<
```

- Up and Down arrow keys: Toggle between options
- Enter: Confirm the entry

How to edit text

```
1 Area name
>Area 1 <
```

Keys 1 to 9 have alphabetical characters printed above them. To enter a letter, press the key the number of times relative to the position of the letter. Both upper- and lower-case letters are available as well as numerical values and spaces. See “Keypad layout” on page 139.

- 1 to 0: Enter a character
- Up: Delete a character
- Down: Backspace
- Left and Right: Move the cursor
- Function, and then Left: delete text backwards
- Function, and then Right: delete text onwards
- Enter: Confirm the entry
- Clear: Exit without changes

How to edit a list

```
5 Areas
    >12_4....<
```

- Up and Down: Toggle the value under cursor
- 0: Include or exclude all values in the list
- Left and Right: Move the cursor to a specific item
- Enter: Confirm the entry
- Clear: Exit without changes

If the number of allowed list elements is higher than 16, the list elements are grouped, for example:

```
01-10 Areas
    >12.4.....<
```

In this case, select a group first, and then edit the selected group as described above.

How to edit a host address

```
Host name
>      <
```

Using the same rules as described in “How to edit text” on page 137, enter one of the following:

- An IP address as nnn.nnn.nnn.nnn. For example, 192.168.1.20.
Note: Each IP number can be entered in decimal, octal, or hexadecimal notation. Octal notation requires a leading zero, and hexadecimal notation uses 0x prefix. For example, decimal address 192.168.1.20 is equal to 0300.0xA8.0x1.024.
- A host name as a text string. For example, “hostname.com”. In this case DNS server must be configured in “DNS options” on page 342, and must be available.

Confirmation of changes

If particular settings are changed, you are prompted to confirm those changes when you exit from the current menu. The following screen appears:

```
Apply settings?
>No<
```

Changing of other settings that affect user configuration, like PIN length, Duress method, etc., requires all user database reset. In this case you are prompted to confirm all user removal.

```
Reset users?
>No<
```

If you want to keep the changes, choose “Yes” and press Enter, otherwise the changes are cancelled.

Exit from menu

You must confirm your decision to exit from the menu system. The appropriate prompt appears. Choose “Yes” and press Enter to exit from the menu.

```
Goodbye?
>No<
```

Alternatively, choose “Engineer mode”. In this case the panel remains in the service in mode, while the installer logs off the keypad. It lets the installer to log in another keypad without leaving the programming mode.

If any faults or any open inputs are present, they are listed the same way as in the menu “Panel status” on page 176.

Keypad layout

Table 23: ATS111xA keypad layout for entering text

Key	Character sequence
1	a b c A B C 1
2	d e f D E F 2
3	g h i G H I 3
4	j k l J K L 4
5	m n o M N O 5
6	p q r P Q R 6
7	s t u S T U 7
8	v w x V W X 8
9	y z Y Z 9
0	Space . , + - * % 0

Table 24: ATS113x keypad layout for entering text

Key	Character sequence
1	. , ' ? ! - & % * / _ < > @ 1
2	a b c A B C 2
3	d e f D E F 3
4	g h i G H I 4
5	j k l J K L 5
6	m n o M N O 6
7	p q r s P Q R S 7
8	t u v T U V 8
9	w x y z W X Y Z 9
0	Space 0

The keypad layout, as well as the menu text, depends on the language programmed for the user currently logged in.

The layout may change depending on the context of the edited value. For example, digits are entered prior to characters when editing phone numbers.

Programming the system using Touchscreen

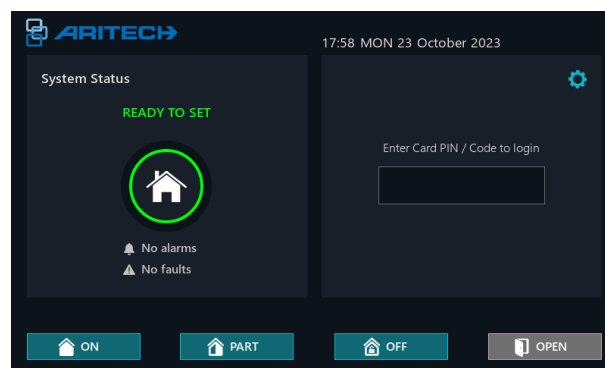
Introduction

ATS1140 is an intuitive graphical touchscreen interface for security system users. It provides simple fingertip control via its touchscreen with user-friendly graphic icons. See also “Common key sequences for Touchscreen” on page 62.

Additionally, it provides the classic panel terminal mode with two-line text interface, which offers all the system features as available on LCD keypads. See “Terminal mode” on page 154 for more information.

See also “Programming the system using LCD keypad” on page 135.

Main screen



The following main screen elements are available:

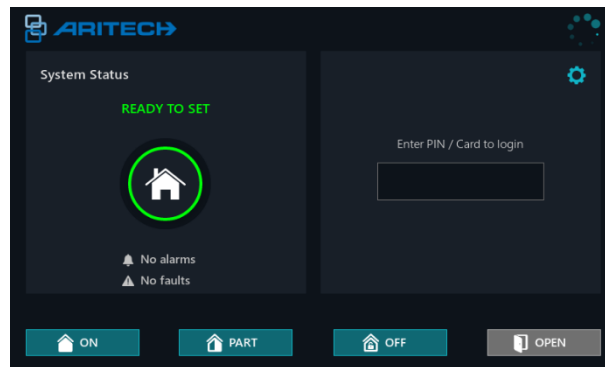
-  System status indication: Shows the current system state (if allowed by the configuration).
Single click on the system status indication shows the current state of the areas. Second click displays currently open zones.
- Authorization field: Touch to log in to the device or panel menus. It requires user authorization. See “Authorization” on page 142.
After the successful authorization, the main menu opens. See “Main menu” on page 146.
-  ON: Set button. Tap to set areas (may require authorization). See “Set / Unset” on page 144.
-  PART: Partset button. Tap to part set areas (may require authorization). See “Set / Unset” on page 144.
-  OFF: Unset button. Tap to unset areas, and acknowledge alarm and fault messages (requires authorization). See “Set / Unset” on page 144.
-  OPEN: Open door button. Tap to unlock the door assigned to the touchscreen device (if configured).

-  Internal menu: Tap the gear icon to enter the internal touchscreen menu. See “Internal menu” on page 153 for more information.

Note: If the Function keys in the menu “Settings > Display settings > Idle screen”, described on page 156, is enabled, then the Function keys screen becomes the default screen. In this case, the main screen is available after clicking on the empty parts of the display. See also “Function keys” on page 143.

Loading configuration

Main screen may show the rotating wheels animation  in the top-right corner.



This means the touchscreen is downloading the configuration from the panel. It happens on every system start-up and after significant changes in the panel configuration (for example, when the database has been loaded from the Downloader software).

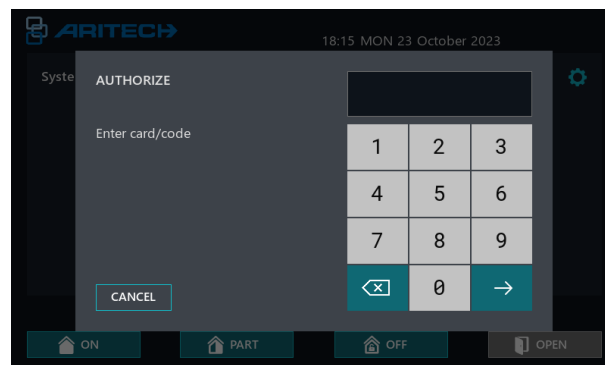
Depending on the system size, number of touchscreen devices on the bus and the scope of the configuration change, the database loading may take from few seconds up to 30 minutes.

When the configuration is being loaded, the touchscreen may be normally used for controlling the system and checking the status with the following exceptions:

- The Devices menu is not accessible.
- If the EN 50131 standard is enabled, the alarm/fault confirming while setting/unsetting is shown in a simplified form (one event a time, instead of the whole list).
- User may experience minor reduction of device responsiveness.

Authorization

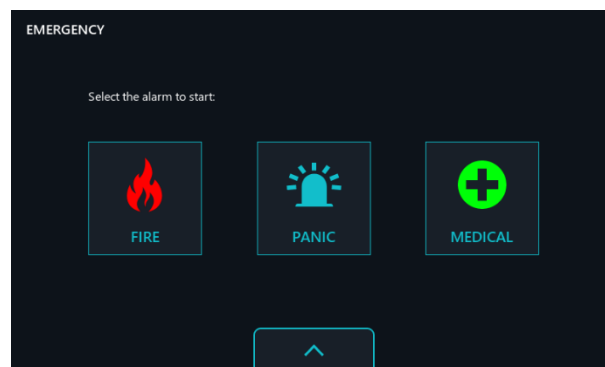
Most of the system functions require user authorization. Pressing on one of the buttons on the main screen may cause the PIN entry window to appear:



Enter your PIN code using the digit buttons and press ➔ Enter (right arrow icon) to confirm. Alternatively, present the card if the system is configured for card authorization. See also “Common key sequences for Touchscreen” on page 62.

Emergency alarms

User can trigger Fire, Panic or Medical alarms without the authorization, if configured by system installer. To trigger one of the emergency alarms, slide the screen down (touch at the top of the screen and pull down). The emergency screen appears:



Touch one of the icons to trigger respective alarm. Additional confirmation is required on another screen.

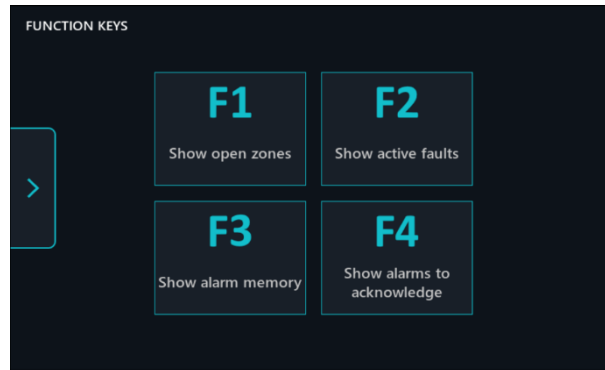
Emergency alarm screen hides automatically after a few seconds. Alternatively, it can be dismissed by sliding the screen up.

Note: Emergency alarm screen can be opened only from the main screen.

Availability of this screen and particular alarm buttons can be set up by the Installer in the menu “Settings > Display settings > Emergency keys” described on page 156.

Function keys

User can trigger one of the four function keys programmed by the installer (F1 to F4). Function keys can be triggered on a function key screen, which shows up after sliding the screen left.



Touch one of the icons to trigger the required function. Certain functions may require authorization.

Function key screen hides automatically after few seconds. Alternatively, it can be dismissed by sliding the screen right.

Function keys are configured in the menu “Function keys” described on page 201.

The installer may use the Downloader software to upload custom images that will replace default F1 to F4 function key descriptions.

See also “Function keys” on page 65.

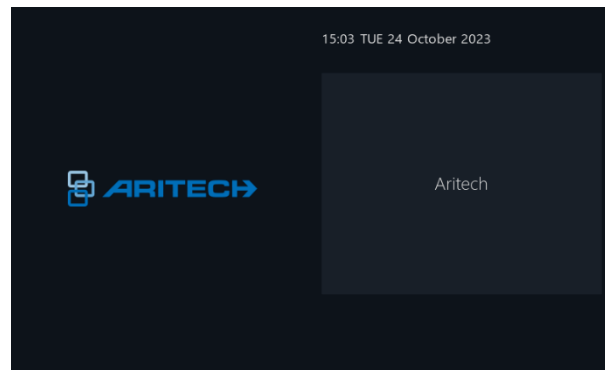
Note: Function key screen can be opened only from the main screen. It can also be the default screen, if the option Function keys is enabled in the menu “Settings > Display settings > Idle screen” described on page 156.

Idle screen

Depending on the system configuration, the touchscreen may enter idle mode after certain period of user inactivity.

This results in dimming the screen and entering the idle screen. The idle screen may contain a combination of the following elements:

- Logo (Aritech or customer defined uploaded via Downloader).
- Date and time
- System custom message



When the idle screen is displayed, tap the screen to return to the Main screen. See “Main screen” on page 140.

If the screen is dimmed, or the idle screen appeared, tap the screen to wake up the device. If the proximity sensor is enabled, the device wakes up automatically if the user presence is detected.

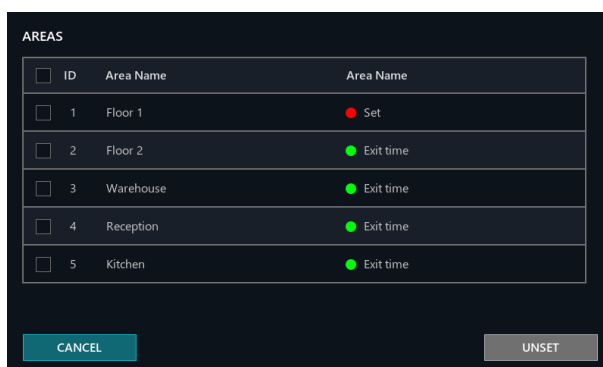
The idle screen is configured in “Settings > Display settings > Idle screen” on page 156.

Set / Unset

Setting and unsetting can be triggered from the main screen only. Press one of the dedicated buttons (ON / PART / OFF) to control the system.

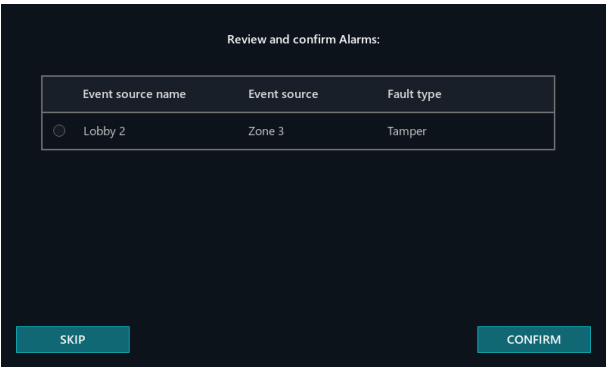
Depending on the system configuration and state, the setting/unsetting process may consist of the following stages:

- User authorization. See “Authorization” on page 142.
- Partset type selection. See also “How to use part set” on page 57.
- Area selection. Select the areas from the list, press the operation button in the bottom-right corner. See also “Area selection” on page 134.

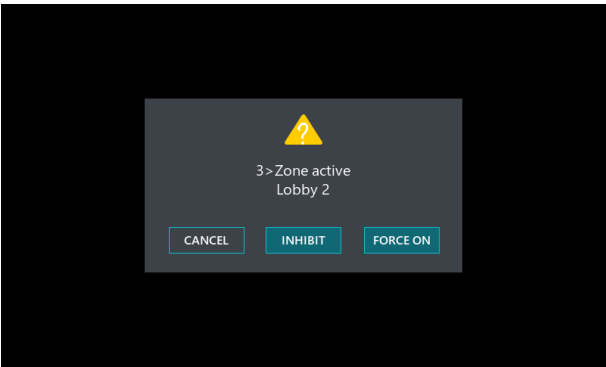


- Alarm confirmation. Select the alarm or fault from the list, then tap CONFIRM.
Note: If the alarm condition still persists, the relevant message appears, and the alarm remains on the list.

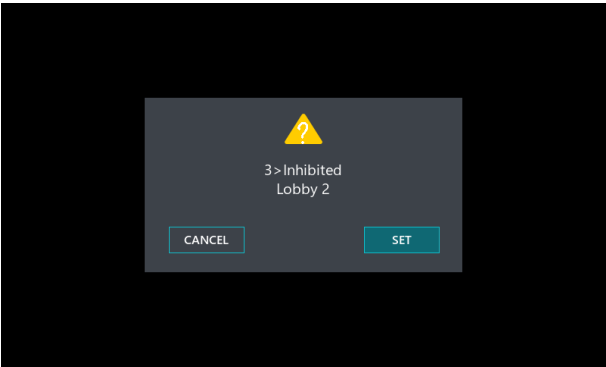
Confirmation may be finished at any time by tapping SKIP. The outstanding alarms and faults remain unconfirmed.



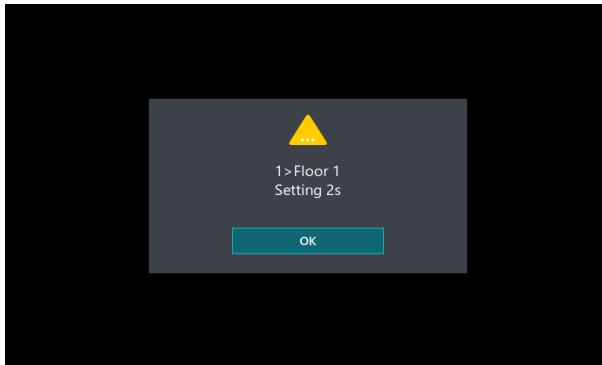
- Inhibiting open zones / forced set. If any zones are open, which makes setting the system impossible, they can be inhibited by tapping INHIBIT. Alternatively, forced setting may be activated if this is allowed by system configuration. See also “Inhibit and isolate” on page 59.



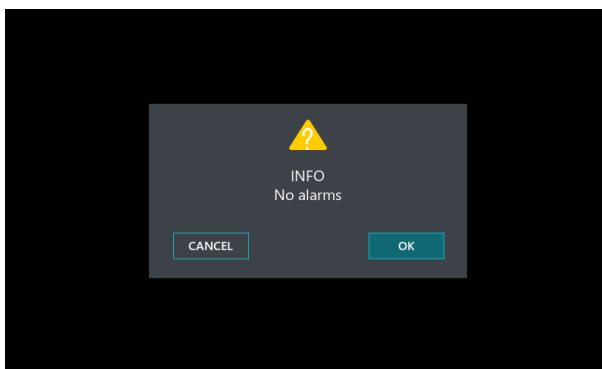
- Reviewing of all inhibited zones when setting. If any zones were inhibited while setting, they are shown before finalizing the setting process. Tap SET to confirm setting.



- Set progress information. Information screen can be dismissed by tapping OK.



- Reviewing alarms and faults while unsetting.



Main menu

Main menu can be entered from the initial screen by pressing the login bar, then entering the PIN code and/or presenting the card. See also “Authorization” on page 142.

Menu items are listed along the left side of the screen. Press the icon to move to the selected menu.

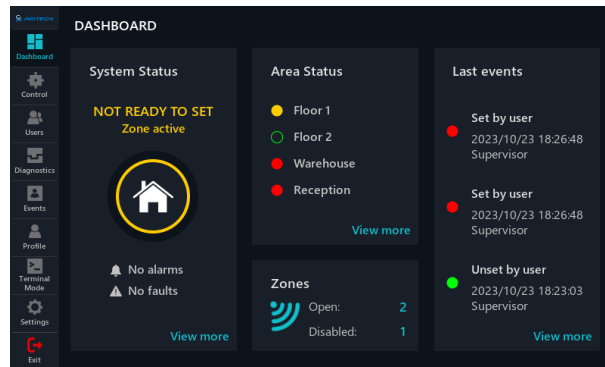
Exit button is located at the left bottom corner of the screen. Tap it to return to the main screen.

Note: The 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.

The following pages describe particular menu items and screens.

Dashboard

Dashboard screen is a default screen that is shown after opening main menu.

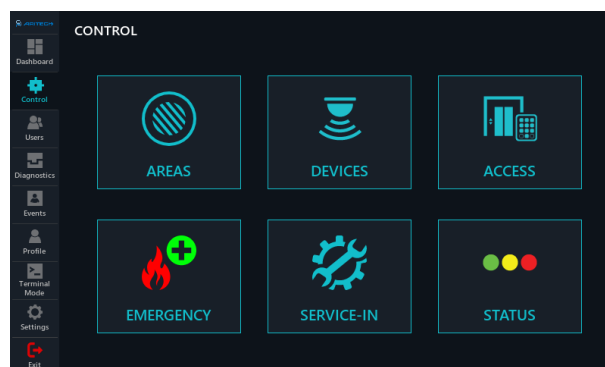


Dashboard shows an overview of the current system state. Tapping on a particular widget moves to relevant submenus. The following widgets are available:

- **System status:** Overall status of all user's areas. Tap to move to Control > Status menu. See "Control" below for details.
- **Area status:** States of areas. Tap to move to the Control > Areas menu. See "Control" below for details.
- **Zones:** Number of open/inhibited zones is shown. Tap to move to the Control > Devices menu. See "Control" below for details.
- **Last events:** Up to 3 recent events from the Mandatory event log, generated during the past 24 hours.

Control

Screen groups sub-menus and functions related to system control and status checking.



Note: Certain functions switch the view to the Terminal mode. See "Terminal mode" on page 154 for more information.

- Areas: List of all areas available to the user with their current state.

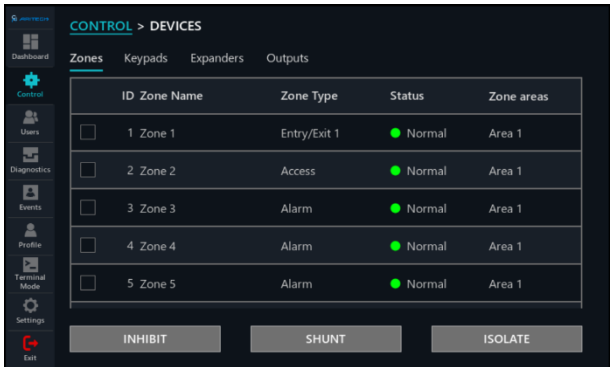


The screenshot shows the 'CONTROL > AREAS' screen. On the left is a sidebar with icons for Dashboard, Control, Users, Diagnostics, Events, Profile, Terminal Mode, Settings, and Exit. The main area contains a table with the following data:

ID	Area Name	Area Name
1	Floor 1	● Not ready to set
2	Floor 2	○ Ready to set
3	Warehouse	● Set
4	Reception	● Set
5	Kitchen	○ Ready to set

- Devices: Lists of zones, keypads, expanders, and outputs, with their current state. Device category can be selected by tapping at the tabs at the top of the list.

Depending on user privileges and device category, certain operations may be possible by tapping one of the buttons at the bottom of page (select the device first, one at a time).



The screenshot shows the 'CONTROL > DEVICES' screen with tabs for Zones, Keypads, Expanders, and Outputs. The 'Zones' tab is selected, showing a table with the following data:

ID	Zone Name	Zone Type	Status	Zone areas
☐	1 Zone 1	Entry/Exit 1	● Normal	Area 1
☐	2 Zone 2	Access	● Normal	Area 1
☐	3 Zone 3	Alarm	● Normal	Area 1
☐	4 Zone 4	Alarm	● Normal	Area 1
☐	5 Zone 5	Alarm	● Normal	Area 1

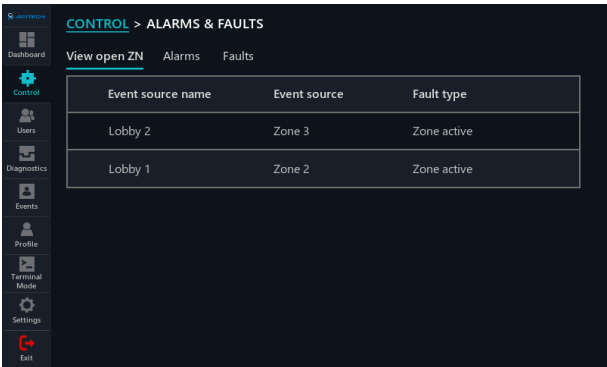
At the bottom of the screen are three buttons: INHIBIT, SHUNT, and ISOLATE.

- Access: Tapping the button switches to the Terminal mode and enters Door control menu. See “Door control” on page 189.
- Emergency: The emergency alarm screen. See “Emergency alarms” on page 142.

Note: Availability of this menu and particular alarm buttons can be set up by the installer in the menu “Settings > Display settings > Emergency keys” described on page 156.

- Service in: Switches off the system accessibility for installer. Pressing the button switches to the Terminal mode and enters Service in option. See “Service in” on page 192 and “Service in” on page 304.

- Status: Lists open zones, alarms, and faults. Depending on system settings and user privileges alarm and fault tabs may allow you to confirm alarms and faults. Select the item, then tap the CONFIRM button.

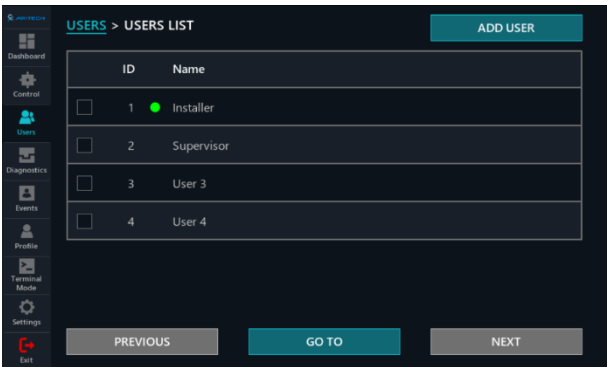


Users

The menu shows the list of users. The green dot indicates the user currently logged in.

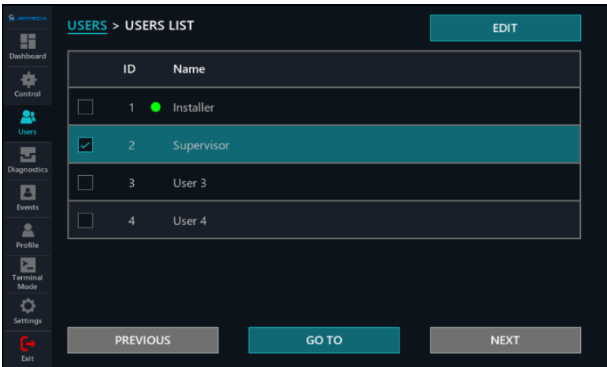
The screen also allows you to:

- Add a new user. To do that, tap the ADD USER button.

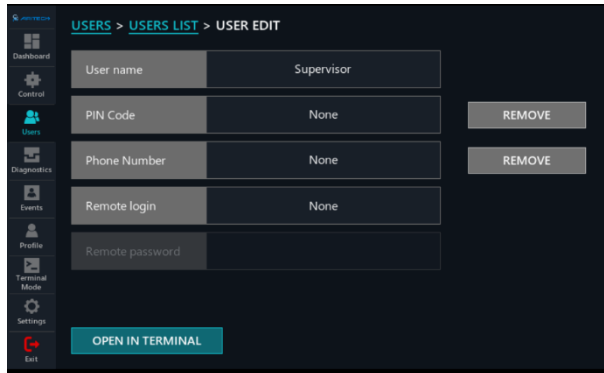


The panel user management menus will be opened in the terminal mode, with the “Add user” process started. See “Add user” on page 219.

- Edit existing user from the list. To do that, select a user, and then tap the EDIT button.



The user edit screen will be opened:



The screen allows you to change PIN, phone number, remote login and remote password of the selected user, if allowed by system settings and the logged-in user privileges.

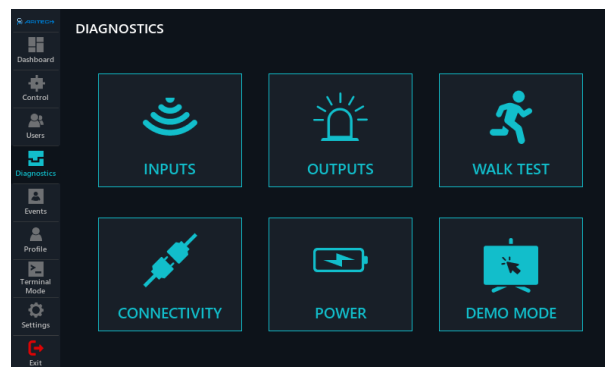
Additionally, tapping the OPEN IN TERMINAL button switches to the relevant menu in the terminal mode, which allows you to view or change other parameters of the selected user.

Note: Use the “Profile” menu described on page 152 to edit your own user data.

See also “Users” on page 69.

Diagnostics

Screen groups sub-menus and functions related to system diagnostics.



- Inputs: Input or sensor tests. Tapping the button switches to the Terminal mode and enters the Input test menu. See “Input tests” on page 171.
- Outputs: Output tests. Tapping the button switches to the Terminal mode and enters Output test menu. See “Output test” on page 175.

- Walk test: Walk test mode. First, select walk test type (total or reduced).

Next, the walk test window is shown:



The list shows the sensors to be walk-tested (top of the list, red icons) and the sensors already passed (bottom of the list, green icons). The number of sensors required for the test is shown at the top of the screen.

Walk test finishes:

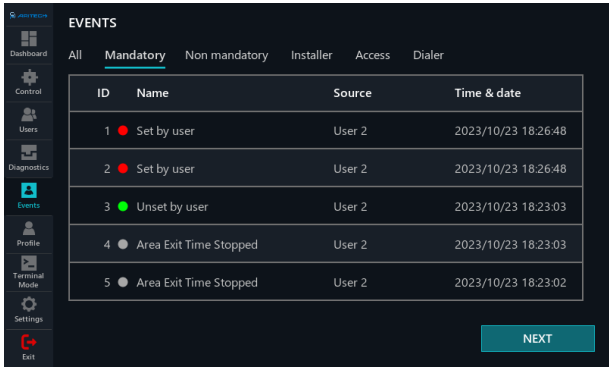
- When all sensors have been positively tested (walk test success).
- When the walk test timeout passed (walk test fail).
- When the user presses END button or switches to the other menu item (walk test cancel).

See “Walk test” on page 94 for more information.

- Connectivity: Shows the screen with the following buttons:
 - Test call. See “Test call opts” on page 179.
 - IP diagnostics. See “IP diagnostic” on page 181.
 - GSM diagnostics. See “GSM diagnostic” on page 183.
- Power. Shows the screen with the following buttons:
 - Panel diag. See “Panel Diagnostic” on page 188.
 - Battery test. See “Manual Battery Test” on page 187.
 - Replace. Allows you to confirm the battery replacement. See “Battery replaced” on page 187.
- Demo mode. See “Demo mode” on page 189.

Events

The screen shows the panel event log. The log is divided into subcategories, selectable by tapping the tabs at the top of screen.



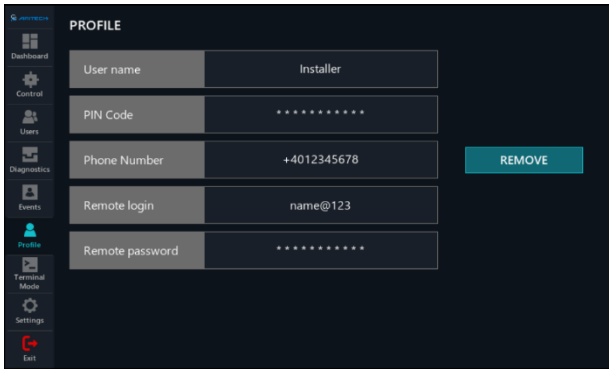
The screen shows the most recent events in every category. The user may pass to the older/newer events by tapping NEXT/PREVIOUS buttons at the bottom of the screen.

Note: The list is *not* refreshed instantly if there are new events generated. Instead, a REFRESH button appears. Tapping the button reloads the list, starting at the most recent event. REFRESH button may appear only when the first event on the list is currently displayed.

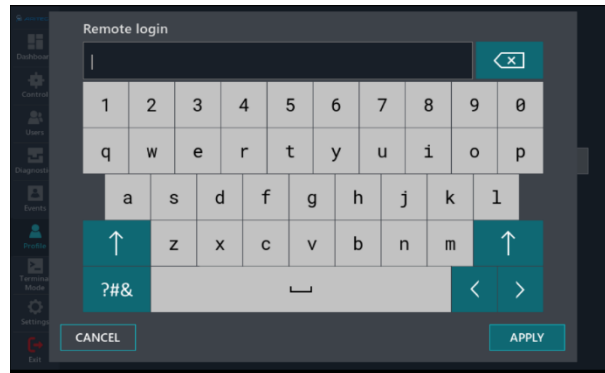
See also “Events” on page 92.

Profile

The screen allows the user to change his own PIN code, phone number, remote login and remote password. Tap the black bar with stars/phone number to change the value. Tap the REMOVE button to remove the value.



Remote login and remote password is entered using the popup alphanumeric keyboard.



Use the following special keys:

- Alt button (?#&): Switch to special characters
- Shift: Switch to uppercase
- Left/Right arrow: Change the cursor position
- Cancel: Discard the changes
- Apply: Accept the changes

Internal menu

The user can enter the internal menu without authorization by pressing the Internal menu icon  on the main screen.

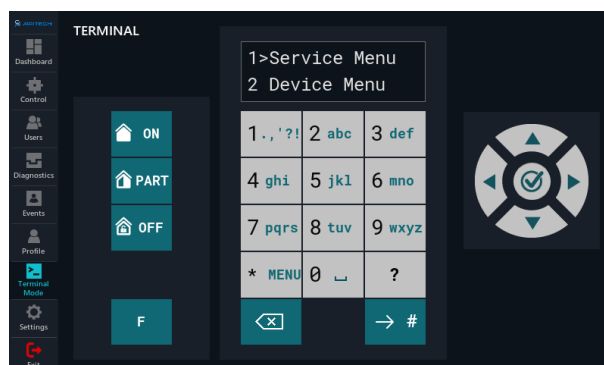
The menu contains the following functions:

- Terminal mode. See “Terminal mode” on page 154.
- Settings. See “Settings” on page 154.

If the user logs into the panel using Terminal mode, then the main menu items appear, as if entered the menu from the main screen. See “Main menu” on page 146 for more information.

Terminal mode

The screen allows you to interact with the system in a classic way. It behaves as an LCD keypad device (ATS113x/ATS111x) and exposes all the features of the panel.

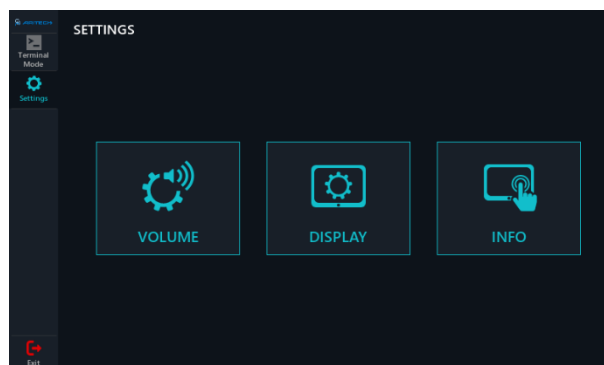


See “Programming the system using LCD keypad” on page 135.

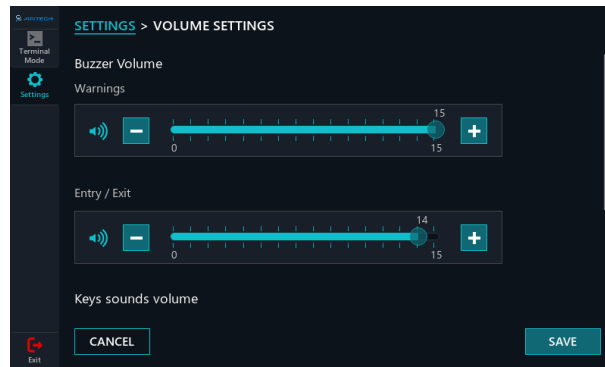
This screen is available also from the Internal menu. See “Internal menu” on page 153.

Settings

Screen groups submenus for the touchscreen information, volume, and display settings.



Volume settings



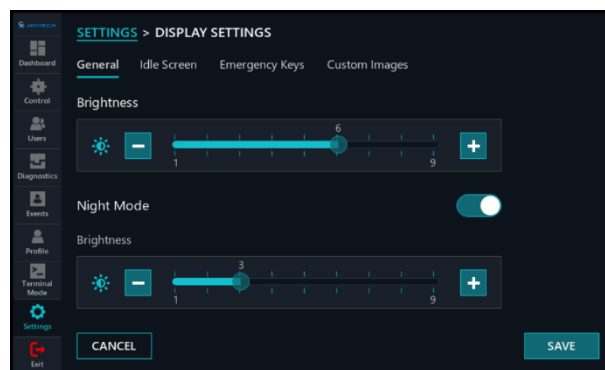
The following internal buzzer volume settings can be adjusted:

- Warning signal volume
- Entry/exit signal volume
- Screen tap volume
- Buzzer tone pitch
- Buzzer silent mode enable
- Entry/exit signal enable

Tap SAVE button to apply changes.

Note: Slide screen up and down to access all the options.

Display settings

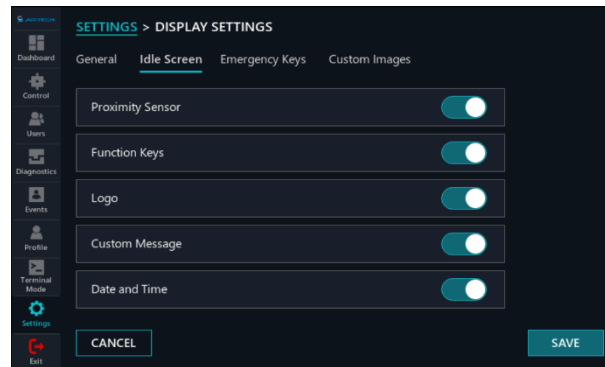


The following display categories can be changed.

General

- Brightness
- Night mode (idle) brightness (if programmed)
- Night mode enable

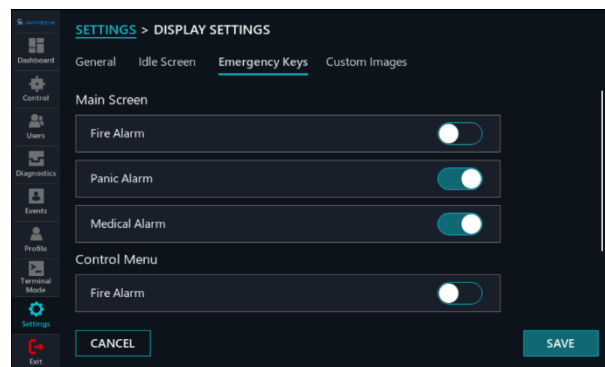
Idle screen



The following idle screen settings can be changed:

- Proximity sensor enables: Enables/disables the user presence detection.
- Function keys enable, Logo enable, Custom Message enable, Date and Time enable. **Note:** If none of these elements is selected, the idle screen does not appear.

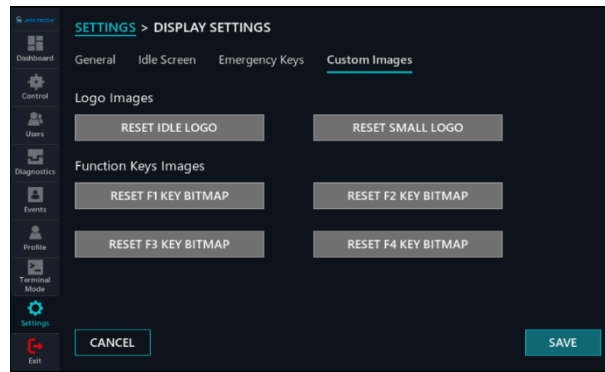
Emergency keys



Enable or disable the emergency alarm buttons without authorization for the main screen and the Control menu.

Note: By default, all emergency keys are disabled. It is recommended to verify these settings after updating the touchscreen firmware, because certain keys may have been enabled by default in earlier touchscreen versions.

Custom images

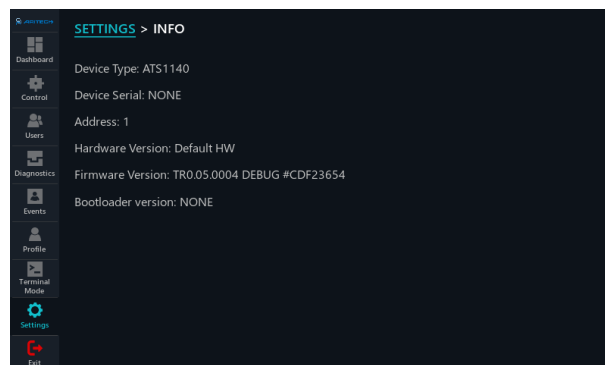


Custom Images allows you to reset custom images and bitmaps, uploaded from the Downloader software, to the default ones.

Info screen

The screen shows the information about the device firmware version, serial number, and the assigned address.

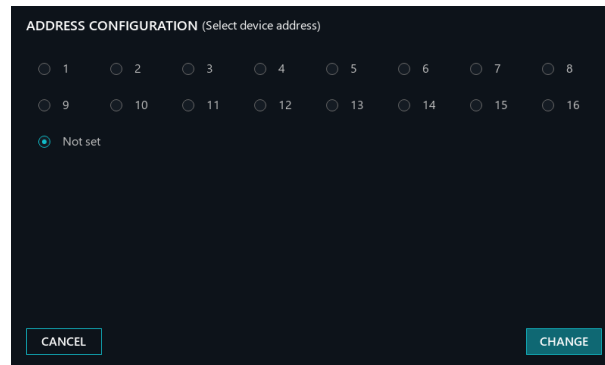
Within 1 minute after powering up the screen will be shown with the following additional buttons.



- **Set Address.** It allows you to set the device address, if for any reason change is needed after initial installation. See “Address configuration” on page 158.
- **Factory Reset.** Resets all internal settings of the touchscreen, including volume, brightness, proximity sensor, emergency alarms, etc. See also “Settings” on page 154.

Address configuration

Set the device address.

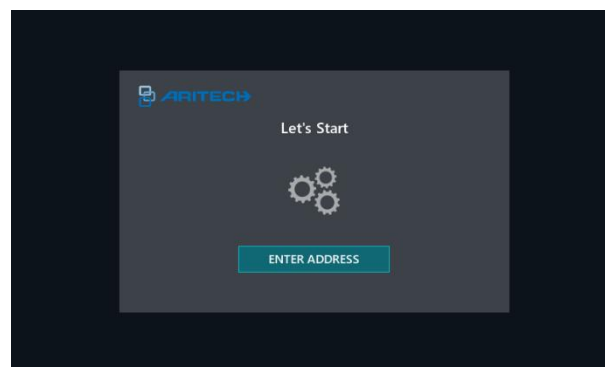


Select the desired address and press CHANGE button. The device will restart to apply changes.

Caution: Tapping CHANGE button on the address selection screen resets the secure channel encryption key in the device to factory default value even if the device address has not been changed.

Initial installation

The device, when powered for the very first time, shows the initial installation screen:



Press ENTER ADDRESS button to pass to address setting screen. See “Address configuration” above.

Reinstallation and defaulting

To access maintenance/defaulting options, the following procedure should be followed:

- Power cycle the device
- Within the 1 minute after powering up enter the Info screen.

See “Info screen” on page 157 for more information.

Programming the system using WebApp

You can control your system and program its basic functions using the built-in web application (WebApp).

WebApp meets the Web Content Accessibility Guidelines (WCAG) 2.1 requirements, which provides a better user experience.

The following options must be set before you can use WebApp:

- Configure the remote access. See “Remote access” on page 162 for details.
- Enable Direct IP connection in “Access options for webserver” on page 319.
- Activate HTTP connection in “Direct IP Protocol” on page 319.
- If mDNS is supported, set mDNS to be able to connect to the panel via LAN. See menu “mDNS enabled” described on page 344.
 - Enable mDNS using “mDNS enabled” menu on page 344.
 - If the custom panel address is not set in “Host name prefix” on page 344, use the default panel address “SID.local”, where SID is the panel serial identifier. SID may be obtained from the label on the panel PCB or using the menu “SID number” described on page 358.

Using web browser, go to your panel local address.

Note: The following web browsers in the newest versions support the WebApp functionality: Chrome, Firefox, Edge, Safari, iOS built-in browser, Android built-in browser.

For panel programming, see “WebApp programming map” on page 413.

Caution: Do not leave the WebApp session unattended. After your session log out immediately. Unattended session may critically compromise your site security.

Secure connection (SSL)

The control panel supports SSL networking protocol for WebApp connection. This protocol encrypts the data transmitted between a user's browser and the build-in web server. This means that even if the data is intercepted, it remains unreadable to unauthorized parties. SSL certificates authenticate the identity of the website, ensuring that users are not sending their information to a fraudulent site. SSL also ensures that the information, such as PINs and personal data, remains accurate and unaltered during the transmission.

The SSL connection requires a valid SSL certificate, which must be provided by your local network administrator. This certificate is generated for the specified connection. The certificate file must be in #PKCS8 format. This file contains the server certificate and encrypted, password protected server private key.

To activate the secure communication with the control panel, follow the steps below.

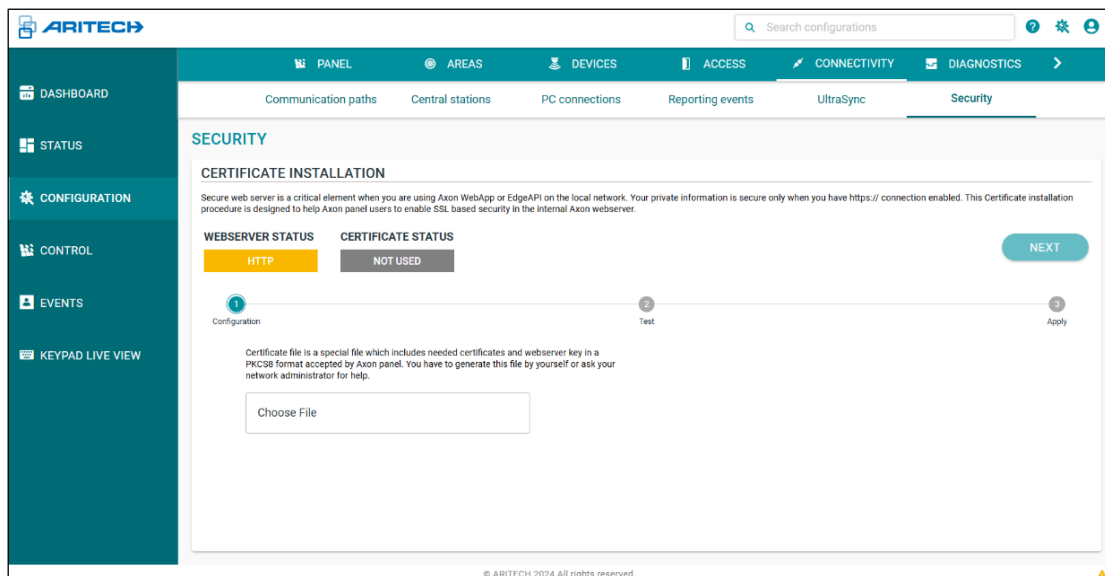
- Using a keypad or configuration software, set the following control panel settings:
 - “Access options for webserver” on page 319: Enable Direct IP connection.
 - “Direct IP Protocol” on page 319: Activate HTTP connection.
- Connect to your panel WebApp using insecure http connection, for example:
`http://SID.local` (control panel host name)

— or —

`http://nnn.nnn.nnn.nnn` (control panel IP address)

- In Webapp, go to CONFIGURATION > SECURITY.

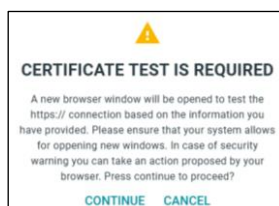
Note: If the connection is insecure, a warning icon  is shown in the right bottom corner of the Webapp window.



You will be prompted to install an SSL certificate.

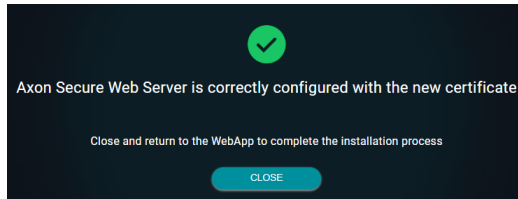
- Click the Choose File button and choose the SSL certificate, generated for this connection by your local network administrator.
- When the certificate file is loaded, enter the certificate password provided by your local network administrator. Click NEXT to initiate the certificate test.

The test requirement popup window is displayed.



6. Click CONTINUE.

If the test is successful, the confirmation is displayed.



7. Click CLOSE.

8. Apply the new SSL certificate by clicking APPLY in the popup window.

The WebApp connection will be restarted in secure mode. The address will change to the secure one, for example:

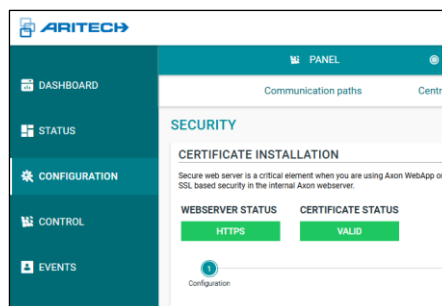
`https://SID.local` (control panel host name)

— or —

`https://nnn.nnn.nnn.nnn` (control panel IP address)

If the connection is secure, CONFIGURATION > SECURITY window will display WEBSERVER STATUS: HTTPS and CERTIFICATE STATUS: VALID.

Note: If the option “Direct IP Protocol” described on page 319 was set to HTTP only, it automatically switches to HTTPS, so the insecure HTTP protocol is disabled.



Note: Depending on certificate type and network configuration web browser may show a warning message, which should be confirmed. In this case the communication is encrypted, but the browser cannot fully verify the authenticity of the panel web server.

Remote access

A remote access can be gained via IP or GPRS connection, depending on the available panel hardware configuration and settings.

Note: Connection via USB cable is not a remote connection.

Every remote access requires the remote login and password to be set. To do so, use menu “Remote options” described on page 222.

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

The remote configuration is allowed only if the option “Remote configuration access” on page 319 is set to Always or When Service In. If this option is set to When Service In, the additional authorization is necessary. See “The AXON menu” on page 133 for details.

The supervisor is allowed to configure the panel remotely only if the option “Allow remote access to configuration by Supervisor” on page 319 allows it.

Notes

- After 10 unauthorized access attempts via Downloader or mobile application the remote login is locked for 90 seconds.
- After 3 unauthorized access attempts via WebApp the remote login is locked for 90 seconds.

Initial start-up

When switched on first time, the system prompts you to perform an installation.

INFO
Inst required

Caution: It is only possible to perform the initial system installation from keypad 1.

It is necessary to set appropriate default values for this particular system prior to programming. The following settings can be defined during installation.

Table 25: Values set during installation

Option	Description
1 Panel language	Defines the language [1] of the panel menus. This language is used for messages when no user is logged in. After login the language is switched to the one assigned to the logged user (set by system manager).
2 Defaults	Defines approval dependent default values [1]. Note: The default values of particular programming options may depend on this selection. This manual shows default values set for the EN Grade 3 defaults.
3 Time and date	Time and date must be set during installation. See also “Time and date” on page 296.
4 UltraSync	UltraSync options. See “UltraSync” on page 122 for details.
1 Connectivity	Enable or disable the UltraSync cloud connection. See also “Cloud connectivity” on page 358.
2 Password	The UltraSync password is necessary to connect to the panel remotely via UltraSync cloud. See also “UltraSync password” on page 358.
5 Other options	
1 Duress method	Default duress method. See <i>AXON Control Panel Manager Manual</i> for more information. See also “Duress method” on page 315.
2 PIN length	Default length of PIN (allowed range is from 4 to 10). See “PIN length” on page 315 for more details.
3 PIN change mode	PIN change mode. See “PIN” on page 76 for details on PIN usage. See also “PIN change mode” on page 316.
5 Batt capacity	Battery capacity. The option allows the system to optimize battery recharge pattern and prolong battery life.
6 Remote options	Provide a remote login and password for the installer user to enable access through the web application. Enable Direct IP Protocol is you want to use WebApp for programming. See also “Programming the system using WebApp” on page 159.
7 Install	Run the installation process

[1] Contact your supplier for a list of available languages and approved versions.

Set the appropriate options and run the installation, then choose OK and press Enter.

Next, you are prompted to change the installer and the supervisor PINs.

```
Change PIN
  Installer
```

Press Enter.

```
New PIN
> _
```

```
Verify
> _
```

Provide the new installer PIN of the required length, and press Enter. Next, enter the PIN again to verify it.

If the PIN is changed successfully, the following message appears.

```
INFO
PIN changed
```

If the provided PIN is shorter than required, or the new PIN is the same as the previous one, the warning is displayed.

```
WARNING
Wrong PIN
```

If the PIN confirmation fails, the following warning is displayed.

```
WARNING
PIN NOT changed
```

Repeat the above steps for the supervisor PIN.

```
Change PIN
  Installer
```

After both PINs are successfully set, the panel continues the installation process.

The display shows the installation progress percentage complete.

After the installation is complete, the panel restarts.

Note: You can change most of these values later using menu “Panel and AB options” (see page 315).

See also “Default panel” on page 193.

Caution: After defaulting panel, restart the system by powering it down and up.

Auto configuration

During the second system start, the panel prompts to activate an automatic system configuration.

```
Auto Config?
  >Yes<
```

Select No and press Enter to cancel.

Select Yes and press Enter to run the automatic configuration process.

The system configures the following elements:

1. Keypads and expanders.

```
Rkp 1-16 BUS1
R-?-----
```

```
Exp 1-15 BUS1
-?-----
```

Bus devices are automatically configured in a way that is similar to the configuration via viewing devices menu. See “Install remotes” on page 194 for details.

2. Zones.

Zones are configured according to the number of installed internal and external expanders, as well as the number of physical inputs in a state, which is equal to the normal state of the zone.

Note: Normal zone state depends on “Input mode” on page 207 and “End of line resistor” on page 207.

After the configuration is complete, the number of configured elements is displayed.

```
Added
R:1 D:0 Z:8
```

The following elements are displayed: R – remote keypads (or RASes), D – remote expanders (DGPs), Z – zones.

Caution: After the installation and the auto configuration you automatically enter to the programming menu. Next time you will need an authorization to enter the menu.

Chapter 5

Menu reference

Summary

This chapter contains descriptions of all programming menu entries of AXON control panel.

See “The AXON menu” on page 133 for more information about menu organization.

Content

Service 170

- Test options 170

Device menu 194

- Install remotes 194

- Edit Keypad&Exp 195

- Keypad devices 195

- Keypad options 195

- Expander devices 205

- Expander options 206

- Wireless specific options 209

- Camera specific options 211

- Four-door expander specific options 213

- Door Control/Lift Control Expander Readers 217

- Reader options 217

User menu 219

- Users 219

- User groups 226

- User group settings 226

Zones and areas 228

- Zone menu 228

- Zone options 228

- Adding a wireless sensor 229

- Common options 229

- Shock sensor options 242

- Wireless sensor options 242

- Areas 244

- Area options 244
- Area groups 249
- Area group options 250
- RF fobs 250
- Fob options 250
- Cameras 252
- Doors Menu 256
 - Doors 256
 - Common door options 256
 - Standard door specific options 264
 - Intelligent door specific options 265
 - Door groups 275
 - Region 276
 - Floors 277
 - Floor groups 278
- Outputs and filters 280
 - Condition filters 280
 - Filter settings 280
 - Outputs 282
 - Output settings 282
 - Triggers 286
 - Trigger settings 286
- Calendar 288
 - View 288
 - Schedules 289
 - Schedule settings 290
- System options 296
 - Timer menu 296
 - Engineer options 301
 - LCD Display opt 305
 - Set options 307
 - Access options 311
 - Zone options 314
 - Panel and AB options 315
 - PA and other 321
 - Timed Unset / ATM 327
- Communication 329
 - Central station 329
 - Common options 330
 - IP and GSM/GPRS specific options 333
 - Photo transmission specific options 335
 - GSM/phone specific options 336
 - UltraSync specific options 337
 - VdS specific options 337
 - Event options 338
 - Path options 339
 - Common options 339

IP specific options	341
GSM/SMS/GPRS specific options	345
PC connection	354
Common options	354
IP specific options	357
GSM specific options	357
UltraSync options	358
VdS options	361

Service

```

1 Service Menu
2 Device Menu
  
```

→

```

1 Display logs
2 Test menu
  
```

The Service menu provides an installer with options for commissioning and maintenance such as hardware overview, logs listing, etc.

Display logs

```

1. 1 Display logs
    2 Test menu
  
```

→

```

1 All
2 Mandatory
  
```

The View logs menu is a fast and easy way to review where alarms have happened. This information is useful when you have had to reset an alarm without initially checking its cause.

You can select one of the following message types:

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

The display shows where the alarm occurred.

```

1>Access granted
    User 3
  
```

You can now:

- Scroll through the alarm list. Press Up or Down.
- View details. Press Enter.

```

05May08 15:04:54
    Keypad 1
  
```

If there is additional information, it is scrolled automatically.

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

Test options

Test menu

```

1. 2 Test menu
    3 Panel inf
  
```

→

```

01 Input tests
02 ShockSens tes
  
```

The Tests menu gives you access to all testing functions.

Input tests

1.2. **01 Input tests** → 1 Show open Zn
02 ShockSens tes 2 Nbr of used Zn

Enter the Input test menu to test inputs.

Show open zones

1.2.01. **1 Show open Zn** → 0>Zone
2 Nbr of used Zn 1 Panel

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.

Number of used zones

1.2.01. **2 Nbr of used Zn** → Zones used
3 RF RSSI test 8/512

The Number of used zones menu shows the following system data:

- Zones used: Number of zones currently programmed.
- Zone capacity: Maximum zone number in the AXON system.

RF RSSI test

1.2.01. **3 RF RSSI test** → 1>Expander 1
4 RF diagnostics 2 Expander 5

Select the input location first.

Notes

- Only existing RF expanders are displayed.
- The function is not supported in wireless expanders ATS1235 with firmware version older than 1.20.

Enter the physical input number on this location. The RSSI is displayed for the selected zone.

```
Zone 1
-44dBm [IIII ]
```

Note: In case of ATS1235, the value is updated automatically each time the selected zone is activated.

If the wireless detector is equipped with two wireless transmitters, LDR (Low Data Rate) and HDR (High Data Rate), the screen above shows LDR data.

Press Right to toggle between LDR and HDR receiver data or wait 2 seconds for the screen to scroll automatically.

```
Zone 1
QI=50% [III ]
```

For more information on the communication quality, refer to the appropriate wireless expander manual.

RF diagnostics

```
1.2.01. 4 RF diagnostics → 1>Expander 1
          5 Cam range test    2 Expander 5
```

Select the input location first.

Notes

- Only existing RF expanders are displayed.
- The function is not supported in wireless expanders ATS1235 with firmware version older than 1.20.

Enter the physical input number on this location. The RF state is then displayed, for example:

```
Zone 1
LB D
```

The device can report the following states:

- RF state OK: The RF device is working properly
- No data: No data received from the RF device
- LB: Low battery fault
- SS: Short supervision fault
- LS: Long supervision alarm
- D: Fire sensor is contaminated

RF Range test for Camera

```
1.2.01. 5 Cam range test → 17 Camera 17
          6 Inactive days    18 Camera 18
```

Range test allows you to verify wireless PIR camera signal reception.

Select a camera to activate range test.

```
Camera 17
In range test
```

In this mode, selected wireless PIR cameras show the reception quality with alarm LED colour:

- Green: Good signal
- Orange: Medium signal
- Red: Weak signal

The LED follows the weakest communication link of LDR and HDR.

For more information on the communication quality, refer to the appropriate wireless PIR camera expander manual.

Inactive time

```
1.2.01. 6 Inactive days
        7 Zone kOhm      → 0>Reset Timers
                               >>>
```

The inverted walk test function is performed by watching all zones inactive timers and deciding whether a long inactivity is caused by a detector fault.

The menu allows you to view inactive day timers for each zone, and to reset all zone timers.

Every time a zone becomes active, the inactive day timer is reset for this zone. The timer range is 0 to 127 days.

Press 0 to reset all inactive day timers.

Choose a zone to view its timer.

```
1>Zone 1
108
```

See also “Inactive days” on page 300.

Zone kOhm

```
1.2.01. 7 Zone kOhm
        8 Detector test  → 1 Panel
                               2 Input exp
```

The menu allows you to monitor zone resistances.

Select the input location first (panel or internal expander). Then enter the (physical) input number on this location.

The zone resistance is displayed.

```
Panel 1.1
4.6kOhm
```

Values above 65 kΩ are considered as open state.

You can now scroll through the list of inputs by pressing Up or Down.

Note: External expanders (DGP) do not support this functionality.

Detector test

1.2.01. 8 Detector test → 1>Duration
9 Shunt zones 10

Detector test functionality allows remote tests of detectors with a dedicated input test. The menu allows you to configure automatic detector test parameters, or to run the test manually.

Detector Test Duration [sec]

1.2.01.8. 1 Duration [sec]
>10<

Duration defines how long the test signal is active. The allowed range is 10 to 60 seconds.

Detector Test Time

1.2.01.8. 2 Test time
>00:00<

The time of day the system activates an automatic detector test on.

The allowed range is 00:00 to 23:59, while 00:00 is equal to Off and means that the automatic test is disabled.

Detector Test when Set

1.2.01.8. 3 Test when set
>Off<

Defines whether an automatic test is activated or not when the area with the appropriate detector is set.

Manual test

1.2.01.8. 4 Manual test
>Cancel<

Change the value to OK and press Enter to activate the detector test manually.

Shunt zones

1.2.01. 9 Shunt zones → 1>Exit Button
----- Shunt Off

The menu allows you to shunt zones manually.

ShockSens test

1.2. 02 ShockSens te> → 1>Panel
03 Outs&triggers 2 Input exp

Using the menu, you can test shock sensor sensitivity.

Select the input location first (panel, internal or external expander). Then enter the (physical) input number on this location.

The input state is displayed.

```
Panel 1.1
normal 0
```

Apply shocks to the structure. The menu shows the input state and the shock gross level (see “Gross level” on page 242 for more information).

The correct setting for gross attacks can be set to the value + 1 as an alarm should only be activated when exceeding the test attack.

Outs&triggers

```
1.2. 03 Outs&triggers → 1 Output test
      04 Panel status    2 Trigger state
```

The Outputs and Triggers menu allows you to test outputs and check trigger states.

Output test

```
1.2.03. 1 Output test → 1 Outputs
         2 Trigger state 2 Keypad LEDs
```

The Output test allows you to check outputs and LEDs.

Outputs

```
1.2.03.1. 1 Outputs → 1 Panel
           2 Keypad LEDs 2 Expander 01
```

Use the Outputs menu to test system outputs.

Select the output location first (panel, internal or external expander, or keypad). Then enter the output number on this location.

The current output state is displayed.

```
Panel 1.1
Off
```

You can now:

- Toggle its state using the Enter button.
- Scroll through the list of outputs. Press Up or Down.
- Exit output test. On exit, the output returns to its original state. Press Clear.

Keypad LEDs

```
1.2.03.1. 2 Keypad LEDs → 1 Rkp 1
           -----      2 Rkp 2
```

Use the Keypad LEDs menu to test keypad and reader LEDs.

Choose the keypad and press Enter.

You can now:

- Switch all keypad LEDs to the on or off state using the Enter button.

- Exit keypad LED test. Press Clear to exit from test and restore the LED states.

Trigger state

1.2.03. **2 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

Panel status

1.2. **04 Panel status**
05 Walk test me> → 1 View open ZN
2 Alarms

The Panel status menu provides an overview of all abnormal zone states, alarms and faults present in the system.

Select the required state to view.

View open zones

1.2.04. **1 View open ZN**
2 Alarms → 2 Front Door
Zone tamper

View abnormal zone states.

All items scroll automatically. Press Enter to exit.

Alarms

1.2.04. **2 Alarms** → INFO
No alarms

View active alarms. Press Enter to exit.

Faults

1.2.04. **3 Faults**
----- → INFO
No faults

View active system faults. Press Enter to exit.

Walk test menu

1.2. **05 Walk test me>**
06 Test call opt → 1 Start
2 Walk test opts

The Walk test menu allows testing of zones. The zone passes the test when switching its state from normal to active, and then from active to normal. In walk

test mode each zone state change is signalled by the keypad buzzer or an internal bell.

See also “Walk test” on page 94 in Chapter 3 “System functions”.

Walk test start

```
1.2.05.  1 Start
          2 Walk test opts
```

Run the engineer walk test.

See “Engineer walk test” on page 94 for details.

Walk test opts

```
1.2.05.  2 Walk test opts
          3 Singlezone WT  →  1 Use int siren
                               Yes
```

The menu allows you to set up the following walk test options.

Use internal siren

```
1.2.05.2.  1 Use int siren
            >No<
```

If the Use internal siren option is set to Yes, each activation of a tested zone is signalled by the internal siren.

Use buzzers

```
1.2.05.2.  2 Use buzzers?
            >Yes<
```

If set to Yes, each tested zone activation is signalled by keypad buzzers.

Log untested

```
1.2.05.2.  3 Log untested
            >Yes<
```

If the Log untested option is set to Yes, untested zones are recorded in the system log.

Zone tamper

```
1.2.05.2.  4 Zone tamper
            >Yes<
```

If the Zone tamper option is set to Yes, the zone tamper is included into the walk test.

Keypad/Expander tamper

```
1.2.05.2.  5 Rkp/Exp tamper
            >No<
```

If the Keypad/expander tamper option is set to Yes, the tamper alarms from keypads and expanders assigned to this area also must be tested.

Siren tamper

1.2.05.2. 6 Siren tamper
>No<

If the Siren tamper option is set to Yes, the tamper alarms from sirens assigned to this area also must be tested.

Frequency

1.2.05.2. 7 Frequency
>Never<

The Frequency setting defines, how often the user is requested to perform the user walk test prior to setting an area. The following options are available:

- Never: User walk test is not requested
- Every set: User is asked to perform the walk test prior to each set
- 1st set of day: User is asked to perform the walk test prior to the first set each day
- 1st set of week: User is asked to perform the walk test prior to the first set each week
- 1st set of month: User is asked to perform the walk test prior to the first set each month

Note: For walk test purposes AXON stores information on any zone activation for 4 hours. Therefore, if the zone was activated during the last 4 hours before walk test, it is not included into the list of zones required to test. If each walk test zone was activated during this time, the walk test is not requested.

Need to set

1.2.05.2. 8 Need to set
>Off<

If Need to set option is set to On, the requested user walk test is obligatory. The area cannot be set until the walk test is passed.

Reduced walktest

1.2.05.2. 9 Reduced walk
>4h<

Reduced walk test period is a time before reduced walk test start, in which particular zone activation excludes this zone from the list of zones being tested. The following options are available:

- 4h: Reduced walk test only includes zones that were not active during last 4 hours.
- Set2set: Reduced walk test only includes zones that were not active since the last set.

See “Walk test start” on page 177 for more details on reduced walk test.

Single zone WT

```
1.2.05.  3 Single zone WT
         4 Test No Bells      →  With reporting
                                   >Yes<
```

Before walk test starts, you are asked if the reporting to central stations must be enabled (see “Walk test start” on page 177 for details).

Select the input location first (panel, internal or external expander). Then enter the (physical) input number on this location.

Proceed with walk test for this particular zone the same way as for all zones in a standard walk test. See “Walk test start” on page 177.

Test No Bells

```
1.2.05.  4 Test No Bells
                                   >No<
```

A special walk test mode allows verification of the whole alarm system functionality. In this mode, a service engineer or a guard must perform as many actions on the operating alarm system as possible. This may include set and unset, entry and exit, activating all detectors and tampers. The system operates as usual, sending all alarm and tamper events to the central station, except none of system sirens is active.

This allows the central station operator to review all received alarms and verify if appropriate system functions are working properly.

Active WT

```
1.2.05.  5 Active WT
         -----      →  Zone A
                                   >>>
```

Active walk test allows you to test alarm reporting in case of a confirmed alarm simulation (required by ACPO).

See “Active walk test” on page 96 for more details.

Test call opts

```
1.2.  06 Test call op>
      07 IP diagnostic      →  1>CS 1
                               2 CS 2
```

The Test call menu allows you to define the automatic test call interval, and to perform a test call on demand.

Select CS

```
1.2.06.  1 CS 1
         2 CS 2      →  1>Test call mode
                        Off
```

Select central station to configure test call options.

Test call mode

1.2.06.n. 1 Test call mode
>Off<

Select test call mode. The following modes are available:

- Off: Automatic test call functionality is disabled.
- Time: Automatic test call triggers every day at the time of the day programmed in “Test call time” below.
- Period: Automatic test call triggers once at the time specified in “Test call time” below, and then repeats with the interval programmed in “Period” below.

Test call time

1.2.06.n. 2 Test call time
>00:35<

If the “Test call mode” above is set to Time, the menu allows you to define the time of the day for test calls to the central station.

If the “Test call mode” above is set to Period, the menu allows you to define the time of the day for *the first* test call to the central station. Once the time is defined in this menu, the panel starts sending the event RP (Automatic test/ring-in test) report to the appropriate central stations. The event is sent periodically, the period is defined in the menu “Period” below.

Note: If the option “Extend” below is set to Yes, the real time of the test call can vary depending on other events reported to the central station.

This start time is used by the panel when one of the following occurs:

- The panel is reset
- One of the test call options is changed by installer

The test call time is set in 24 h format, as HH:MM.

Period

1.2.06.n. 3 Period
> <

The Period menu defines an interval for test calls that are described in “Test call time” above.

The allowed range is 1 to 999 hours.

Extend

1.2.06.n. 4 Extend
>No<

The Extend option defines whether the test call interval is counted from the previous test call or from the last successful event report.

If this option is set to Yes, after an event transmitted to the central station the test call delay is extended and the next test call is postponed.

If this option is set to No, the next test call occurs in a test call period after the previous test call, regardless of other reported events.

Frequent test calls in case of FTC

```
1.2.06.n.  5 Freq TC if FTC
           >No<
```

If this option is set to Yes, during the communication fault (FTC) the panel tries to establish a communication by initiating a test call every hour. Otherwise, the test call is attempted as usual.

Caution: Enable this function only for primary central station.

Man. test call

```
1.2.06.n.  6 Man. test call  →  Calling CS 1...
           >>>                Ready
```

The Manual test call option lets you 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.

RSSI in report

```
1.2.06.n.  7 RSSI in report
           >No<
```

If the option is set to Yes, test call reports (RP, RX) contain GSM RSSI level as a subevent.

Panel Identifier

```
1.2.06.n.  8 Panel ID
           0001 0001 000000
```

Panel Identifier should be passed to Central Station when making phone call to confirm Authentication Code.

Authentication code

```
1.2.06.n.  9 Auth. code
           None
```

OH V4 key exchange authentication code.

IP diagnostic

```
1.2.  07 IP diagnostic  →  1>ETH
    08 GSM diagnost>    >>>
```

The IP diagnostic menu provides an access to diagnostic tools for IP connectivity.

Choose interface

```
1.2.07. 1>ETH          >>> → 1>IP statistics
                                     >>>
```

Choose an interface for diagnostic. Depending on the panel firmware and hardware, the following interfaces may be available:

- ETH: Ethernet
- GPRS: GPRS via GSM module
- TDA74xx: External dialler

IP statistics

```
1.2.07.n. 1 IP statistics  >>> → 1>TX packets
                                     5
```

The IP statistics menu allows viewing of the statistics listed below.

- 1 TX packets: Number of packets sent.
- 2 RX packets: Number of packets received.
- 3 Rej. packets: Number of packets that are rejected by built-in firewall. See “Firewall options” on page 343 for more information.
- 4 TX bytes: Number of bytes sent.
- 5 RX bytes: Number of bytes received.
- 6 Clear stat: This command clears the data described above.

Ping host

```
1.2.07.n. 2 Ping host      >>> → Host name
                                     > <
```

The Ping host command allows you to send a ping to the specified network address. This command is used to check if the specified host is present and accessible from the panel in the network.

If the selected interface provides several communication paths, you will be prompted to select one path, which should be used for ping.

```
1>ETH
2 GPRS
```

Note: The ping command must be acceptable by the remote host. Make sure its firewalls and routers allow ping requests and replies. This applies to all ping commands.

Ping PC

```
1.2.07.n. 3 Ping PC        >>> → 1>PC conn 1
                                     -----
```

The Ping PC command allows you to send a ping to the specified PC if it is configured as a PC connection via IP. This function is identical to the one in the “PC connection” menu. See “Ping host” on page 357 for more details. See also “Ping host” above.

Ping CS

```
1.2.07.n.  4 Ping CS      →  2>CS 2
                                     -----
                                     >>>
```

The Ping CS command allows you to send a ping to the specified central station if it is configured as a CS connection via IP. This function is identical to the one in the “Central station” menu. See “Ping host” on page 334 for more details. See also “Ping host” on page 182.

NTP status

```
1.2.07.n.  5 NTP status
                                     Inactive
```

The NTP status screen allows you to check the status of the Network Time Protocol server configured. Possible server statuses are listed below.

- Inactive: The NTP server is not queried yet. This status is usually present after panel restart or NTP configuration.
- Unknown: The query was sent, but no answer from NTP server was received yet.
- Fail: No answer from NTP server.
- OK: NTP server answered the query.
- Link error: Faulty Ethernet line.

GSM diagnostic

```
1.2.  08 GSM diagnost> → 1>PIN status
      09 Battery test      Normal
```

The GSM diagnostic menu provides an access to diagnostic tools for GPRS and SMS connectivity.

PIN status

```
1.2.08.  01 PIN status
                                     Normal
```

The PIN status is an informational screen that lets you verify the PIN acceptance status. The status can be one of the following:

- Normal: Accepted by the SIM.
- Unknown: The status is unknown.
- One trial left! The SIM card provides the last attempt for the correct PIN.
- PUK required! The SIM card is locked after three unsuccessful PIN entering attempts, until the PUK will be provided.

You can only unlock the SIM card by inserting it in a standard cell phone and providing the PUK. There is no possibility to enter the PUK in the AXON system.

GSM net.reg.

1.2.08. 03 GSM net.reg.
Home network

The GSM network registration state can be one of the following:

- Inactive: The dialler has not registered in the network, and is not searching nor connecting
- Home network: Registered in the home network
- Searching: Searching for the network to register
- Reg. denied: Registration to the network has been denied
- Unknown: Registration state is unknown
- Roaming: Registered to a network in roaming

GPRS net.reg.

1.2.08. 04 GPRS net.reg.
Home network

The GPRS network registration state can have the same values as described in “GSM net.reg.” above.

GPRS state

1.2.08. 05 GPRS state
Not available

The GPRS network state can be one of the following:

- Not available: GPRS functionality is not available.
- No network: GPRS functionality is available, but no network is present (for example, SIM card is absent).
- Not established: GPRS functionality is available, but connection is not established (IP parameters are not assigned).
- Configured: GPRS functionality is available, and connection is established.
- Stopped: GPRS functionality is available, but connection is stopped due to the disconnection time expiration. See “Disconn.time” on page 352 for more details.
- No data: Unknown error.

Network name

1.2.08. 06 Network name
MyGSM

Network name is the name of the GSM network that the GSM dialler is currently registered in. This is read-only information. The name can be “unknown”, if the network code is not recognized by the communication module.

Network code

1.2.08. 07 Network code

The network code is the unique identification number of the GSM network in which the GSM dialler is currently registered.

RSSI

1.2.08. 08 RSSI
23 [IIII]

The Received Signal Strength Indication (RSSI) value is read-only diagnostic information.

The following ranges are available.

Table 26: RSSI ranges

RSSI	Signal level	Bar indicator	Description
0	<-112 dBm	[]	No signal
1 to 7	-111 to -99 dBm	[I]	Insufficient signal
8 to 12	-97 to -89 dBm	[II]	Mediocre signal
13 to 20	-87 to -73 dBm	[III]	Good signal
21 to 26	-71 to -61 dBm	[IIII]	Excellent signal
27 to 31	>-60 dBm	[IIIIII]	Excellent signal

For accurate data transfer, we recommend a RSSI value above 16.

Msg sent 24h

1.2.08. 09 Msg sent 24h → 1>All SMSes
0

The menu lists the SMS messages sent since midnight (00:00). The following submenus are available.

- 1 All SMSes: All messages.
- 2 Report SMSes: Reporting messages.
- 3 Unknown SMSes: User SMS control messages that were not recognized and therefore forwarded to the Supervisor.

Note: This counter works only if the SMS forwarding is enabled. See “SMS forwarding” on page 349.

Battery status

1.2.08. 10 Battery stat.
OK

The informational screen shows the GSM module battery status.

Battery status should be OK. If the battery is faulty or missing, the battery status is Fail.

Battery test

```
1.2. 09 Battery test
10 Panel diag → 1>Test options
                2 Man. bat. test
```

This menu allows you to perform a manual battery test as well as configure an automatic test for batteries in the panel or an expander.

Notes

- This functionality is available only in specific devices, for example, ATS120xE expanders.
- Battery test works only if there is no mains fault present.

Test options

```
1.2.09. 1 Test options
          2 Man. bat. test → 1>Panel
                              3 Exp
```

Use this menu to configure an automatic battery test.

First, select the panel or an expander to test the battery.

Select device type

```
1.2.09.1. 1>Panel
           3 Exp → 1>Expander 1
                   2 Expander 2
```

Select the appropriate device group.

Select device

```
1.2.09.1.n 1>Expander 1
            2 Expander 2 → 1>Duration [min]
                              10
```

Select the appropriate device.

Duration [min]

```
1.2.09.1.n.m. 1 Duration [min]
                > <
```

Set duration (in minutes) for battery test.

Allowed range is 2 to 254.

Battery test frequency

```
1.2.09.1.n.m. 2 Batt.test freq
                >Disabled<
```

Set automatic battery test frequency. The following values are available:

- Disabled
- Every working day

- Every Monday
- First Monday of month
- Everyday

Manual Battery Test

```
1.2.09.  2 Man. Bat. test      → 1>Panel
          3 Bat. replaced      3 Exp
```

The menu allows you to perform a manual test of the device battery.

Select device type

```
1.2.09.2. 1>Panel           → 1>Exp 1
          3 Exp              2 Exp 2
```

Select the appropriate device group.

Select device

```
1.2.09.2.m. 1 Exp 1         → 1>Duration [min]
              2 Exp 2         2 Run/Stop test
```

Select the appropriate device.

Duration [min]

```
1.2.09.2.m.n. 1 Duration [min] → 1 Duration [min]
                2 Run/Stop test    2
```

Set duration (in minutes) for battery test.

Allowed range is 2 to 254.

Run/Stop test

```
1.2.09.2.m.n. 2 Run/Stop test → >BTESTOK<
                -----        >Run test?<
```

Run battery test.

Test duration is set in “Duration [min]” above.

If battery test for this device is already running, you are prompted to stop this test.

Battery replaced

```
1.2.09.  3 Bat. replaced      → Confirm?
          4 Batt capacity      >No<
```

After replacing the battery the installer should confirm this by using the Battery replaced menu.

Select Yes and press Enter. The confirmation is displayed for 3 seconds.

```
INFO
Bat. confirmed
```

The battery replacement is recorded in the control panel event log.

Battery capacity

1.2.09. 4 Batt capacity
>7.2 Ah<

Set the capacity of the installed battery. The option allows the system to optimize battery recharge pattern and prolong battery life.

Panel Diagnostic

1.2. 10 Panel diag
11 Check card → 1>System V/A
2 Battery V

Panel diagnostic allows you to monitor electrical data, for example, current and voltage.

System V/A

1.2.10. 1 System V/A → System voltage: 13.8V → System current: 0.8A
2 Battery V

The scrolled screens show the system power supply voltage and current.

Battery Voltage

1.2.10. 2 Battery V → Battery voltage: 12.8V

The screen shows the battery voltage.

Check card

1.2. 11 Check card → Badge card
>>> Keypad 1

Use the menu to read data from a user card.

Read card on the keypad indicated on the screen the same way as it is done when user card programming (see “Assign card” on page 220).

Note: The keypad or the door for the user card programming is selected in “Card learn-in” on page 323.

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
48.111.2.3.146.>

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

Demo mode

1.2. 12 Demo mode
Disabled → 1-10 Demo mode
>1234.....<

Enable the demo mode.

Select areas where demo mode will be active.

In this mode the system operates with following limitations:

- All keypads assigned to selected areas display the following message:

DEMO MODE
Enabled

- Only access and entry/exit zones are operational.
- No mandatory events are reported to a central station and recorded in the event log. The demo mode switching is not reported either.

See also “Display logs” on page 170.

- Engineer reset is disabled.
- Walk test is disabled.
- Internal and external siren outputs are disabled.

The demo mode is cancelled:

- Automatically after 15 minutes
- When the option is switched off
- When the system is restarted

The mode can be only activated via keypad.

Note: The demo mode should be activated only when all areas are unset.

Door control

1.2. 13 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 period configured for this door. See “Unlock time” on page 258.
- 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.

Notification test

```
1.2. 14 Notif. test → 1>Notification 1
      >>>           2 Notification 2
```

The menu allows you to send a test push notification.

Select a notification to send a test push notification to the recipient of the selected one.

The test result is displayed.

```
Notification
sent succesfully
```

Panel info

```
1. 3 Panel info → 01>Software rev
    4 Bypass Pan.Lid 02 Panel langua>
```

The informational screens provide information on the panel firmware and initial settings.

Software Rev

```
1.3. 01 Software rev → ATS1000A 1.0
      02 Panel langua> TR_008.008.0028
```

The Software Revision menu lets you view information of the version number of the panel firmware.

Panel language

```
1.3. 02 Panel langua>
      English
```

The screen shows panel language set during installation.

See “Initial start-up” on page 163 for details.

Defaults

```
1.3. 03 Defaults
      Grade 2
```

The screen shows panel defaults set during installation.

See “Initial start-up” on page 163 for details.

Sys fault info

```
1.3. 05 Sys fault in> → Sys fault R 3
      06 HW variant 01JUN19 15:22:56
```

The menu allows you to see the information about the last critical system fault. The following information is displayed: unique identification number (UID) of the fault, its date and time. A letter indicator (R) is displayed if the fault has been reported to the technical support service.

HW variant

```
1.3. 06 HW variant
      Default HW
```

The screen shows the panel hardware variant, default or VdS.

PCB Serial Number

```
1.3. 07 HW Serial Nbr    → 23234-R56-1070-
      08 CDC Mode         02-010
```

The screen shows the panel PCB serial number.

CDC Mode

```
1.3. 08 CDC Mode
      standard
```

The screen shows the CDC4(-EN) door controller mode.

See also *CDC4(-EN) Door Controller Installation and Programming Manual*.

OH/IRIS Reporting enabling from cloud

```
1.3. 09 OH/IRIS Repo>
      Enabled
```

The screen shows the status of OH/IRIS reporting, which is controlled by UltraSync.

The following statuses are available:

- Enabled: OH/IRIS reporting is enabled in cloud
- Disabled: OH/IRIS reporting is disabled in cloud
- Not configured: OH/IRIS reporting not configured in cloud

ATS Lan Errors

```
1.3. 10 ATSLan Errors    → 1 Clear stat
      -----           2 Keypad devices
```

The menu allows you to see the communication error statistics for the selected devices connected to the system data bus. The following submenus are available.

- 1 Clear stat: Clear all data bus communication error counters.
- 2 Keypad devices: Select a keypad to display the data bus communication error counter.
- 3 Exp devices: Select a keypad to display the data bus communication error counter.

Bypass panel lid

```
1. 4 Bypass Pan.Lid → 1>Panel lid time
   5 Config card      01'00
```

The Bypass panel lid option lets you connect a PC without initiating the panel tamper alarm. The following menus allow setting the isolating timer and running the connection process.

To connect a USB cable to the panel:

1. Ensure the “Panel Lid time” value is enough for you to come to the panel and open the housing.
2. Bypass panel lid using menu “Restore lid” below.

The lid tamper is now isolated and the panel lid timer starts.

3. Open the panel housing and connect the USB cable.

The box tamper timer is stopped and the panel lid is isolated as long as it remains open.

Panel Lid time

```
1.4. 1 Panel lid time
      >01'00<
```

The Panel lid timer defines for how long the panel lid is bypassed.

Restore lid

```
1.4. 2 Restore lid
      Yes
```

Enter the Restore lid menu to bypass the panel lid. The panel lid tamper timer starts timing.

If the panel lid is already bypassed, entering this menu unbypasses it.

Config card

```
1. 5 Config card
   >Disabled<
```

The menu allows the installer to enable reader programming by a configuration card. When enabling the configuration card, all added secure devices are not polled for 30 minutes, so the installer can configure each device using the configuration card. When the option is disabled, all devices are polled normally.

See “Securing card data > Configuration card” on page 128 for details.

Service in

```
1. 6 Service in
   Disable?
```

The menu lets you disallow the Installer in function before the Installer in-time expires (see “Inst in-time” on page 299).

Note: This option is only valid if the installer requires a user authorization. See “User code required” on page 301.

Use this function after the panel programming is complete. To disable service in, go to this menu and press Enter. Next, log out. After this, the installer log in requires another user confirmation.

See also “User code required” on page 301.

Default panel

```
1.  7 Default panel  →  7 Default panel
      >>>                >Cancel<
```

The Default panel menu lets you clear all settings and repeat the initial installation.

Cautions

- This command deletes all programming settings, including users.
 - When the security channel is used, use this option only if your system data bus is physically secured against unauthorized access. See Chapter 3 “System functions > Secure channel” on page 127 for more information.
 - After defaulting panel, restart the system by powering it down and up.
-

See “Initial start-up” on page 163 for more details.

Device menu

```
2 Device Menu      → 1>Inst. remotes
3 User Menu        2 Edit Rkp&Exp
```

Device menu allows you to view and configure bus devices: keypads (RASes), expanders (DGPs), and readers.

For more information on keypads and expanders, see Chapter 3 “System functions > Bus devices” on page 67.

For more information on readers, see “Access control” on page 79.

For bus device numbering, see “Bus device numbering” on page 67.

Install remotes

```
2. 1 Inst. Remotes → 1>Keypad devices
   2 Edit Rkp&Exp   2 Exp devices
```

The Installed remotes menu shows the status of all connected remote keypads, various system and local expanders.

Note: The maximum number of devices allowed on the data bus is given in “General features” on page 39.

Select a device type to display.

Keypad devices

Expander devices

```
2.1. 1>Keypad devices → >Rkp 1-16 BUS1
     2 Exp devices     R-?-----
```

The bottom line has a list of device states; each device state is shown as one character, which can be one of the following.

- ? : Device is currently being read
- x : Device is offline or not supported
- I : Device is configured but isolated
- R : Keypad is online and configured (polled)
- r : Keypad is online, but not configured (new)
- D : Expander is online and configured (polled)
- d : Expander is online, but not configured (new)
- M : MI bus expander is online and configured (polled)
- m : MI bus expander is online, but not configured (new)
- c : MI bus expander is online, but its address is in conflict with another expander
- O : AT574xx series IP/GPRS dialler is online and configured (polled)
- — : No device

Note: For expander local devices, select the expander address first, and then select the local device type.

Press Clear to exit from this view.

Press Enter, then select OK and confirm the new configuration. In this case all new devices are added, and missing devices are removed from the system.

Edit Keypad&Exp

```

2.  2 Edit Rkp&Exp      →  1>Keypad devices
    3 Databus EOL      2 Exp devices
  
```

Choose what type of device you want to configure.

Keypad devices

```

2.2.  1 Keypad devices  →  0>Add keypad
    2 Exp devices      1 Rkp 1
  
```

Press 0 to add a keypad, or a number to configure an existing one.

Note: The maximum number of devices allowed on the data bus is given in “General features” on page 39.

Keypad options

Add keypad

```

2.2.1.  0 Add keypad   →  Keypad number
    1 Rkp 1           >_<
  
```

On the Add keypad menu, enter the number for this new keypad and press Enter to confirm or Clear to exit without adding a device.

After the device is added, the keypad configuration options are shown.

Select keypad

```

2.2.1.  1 Rkp 1      →  1 Keypad type
    2 Rkp 2          ATS1136
  
```

Select the keypad number to configure.

Keypad type

```

2.2.1.n.  1 Keypad type
          ATS1136
  
```

The Keypad type screen is an informational screen. The type is defined by keypad itself.

Keypad address

2.2.1.n. 2 Keypad address
BUS 1 ADDR 0

The bus address is an informational screen showing the bus address set by DIP switches or programmed within the keypad.

Note: If the keypad communicates with the panel using a secure channel, it is marked by the “SC” indicator, for example: “SC BUS 1 ADDR 0”. See also “Securing card data” on page 127.

Keypad options

2.2.1.n. 3 Keypad options
>>> → 1>Keypad name
Rkp 1

The Keypad options menu contains the shown below, which are necessary to configure the selected keypad.

Note: The available options depend on the keypad type.

Keypad name

2.2.1.n.3. 01 Keypad name
Rkp 1

Use the Keypad name option to enter a name that identifies the keypad to the end-user.

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

A keypad name can consist of 16 characters.

Tamper area

2.2.1.n.3. 02 Tamper area
Area 1 → 01 Area 1
02 Area 2

The Tamper area option determines which area receives keypad tamper and fault events. To change it, select the area and press Enter.

Detect tamper

2.2.1.n.3. 03 Detect tamper
>On<

If set to Off, the tamper alarms are not reported by the selected keypad to the panel.

View areas

2.2.1.n.3.

04 View areas 1.....>	→	01-10>View areas 1.....
---------------------------------	---	----------------------------

The View areas menu lets you specify which area will display information on this keypad without a user authorization. The areas are displayed as a list. To change the selection, press Enter and select the appropriate areas.

Note: After an authorization the area view depends on the user privileges and system state.

How to select areas to view

See “How to edit a list” on page 137.

Notes

- After changing this list, the control of selected areas is also enabled (see “Control areas” below).
- You cannot select an area to view and control using this option, if this area is assigned to a door. To do so, use the menu “Alarm control” on page 259 instead.

View Area Group

2.2.1.n.3. 05 View AG → 01-10>View AG

Provides the same functionality as in “View areas” above, but for area groups.

See also “Area groups” on page 55.

Control areas

2.2.1.n.3. 06 Ctrl areas → 01-10>Ctrl areas
1.....> 1.....

The Control areas menu allows you to select areas that can be controlled by this keypad. The areas are displayed as a list. To change the selection, press Enter or Right, and select the appropriate areas.

See also “View areas” above.

Control Area Group

2.2.1.n.3. 07 Control AG → 01-10>Control AG

Provides the same functionality as in “Control areas” above, but for area groups.

See also “Area groups” on page 55.

Control options

2.2.1.n.3. 08 Control opt → 1>Card&PIN mode
>>> Card or PIN

The menu contains a set of options connected to the selected keypad control functions.

See also “Keys” on page 61.

Card and PIN mode

2.2.1.n.3.08. 1 Card&PIN mode
>Card or PIN<

The Card and PIN mode option allows you to select one of the following control methods.

- PIN only: Only the PIN is necessary to set and unset areas
- Card only: A single card unsets areas
- Card and PIN unset: Both card and PIN are required to unset areas
- Card and PIN always: Both card and PIN are required to set or unset areas
- Card or PIN: Either a PIN or a card is required to set or unset

Logoff time

2.2.1.n.3.08. 2 Logoff time
>3<

A time period (in minutes) of the keypad inactivity before the user is automatically logged off.

Allowed range is 1 to 255 minutes. Default value is 3.

One time badge to set/unset

2.2.1.n.3.08. 3 1xset/unset
>Off<

One-time badge to set/unset defines if the selected keypad allows you to set or unset areas with one badge. The following values are available:

- Off: One badge does not cause any set or unset action.
- Unset: One badge unsets areas.
- Set-Unset: One badge sets or unsets areas.
- Part set 1-unset / Part set 2-unset: One badge partially sets or unsets areas.

Three time badge to set

2.2.1.n.3.08. 4 3xbadge set
>Off<

Three-time badge to set defines if the selected keypad allows you to set areas with triple badge. The following values are available:

- Off: Triple badge does not cause any action.
- Set: Triple badge sets areas.

- Partset1 / Partset 2: Triple badge partially sets areas.

Notes

- This functionality works only if areas can be set with a card. See “Card and PIN mode” on page 198 for available modes.
- This functionality is available only if the “One time badge to set/unset” option described on page 198 is not configured as Set-Unset.

Key/Card Sequence Mode

2.2.1.n.3.08. 5 Key/Card Mode
>Alarm&Access<

The option defines how the card reader handles conflicting key sequences that may be used both for door access and alarm control (for example, card + PIN + Off on a card reader without LCD). The following values are available:

- Alarm&Access: The conflicting key sequence opens the door and sets or unsets the system.
- Access: The key sequence only opens the door.

Note: If the option is set to Access, the option One time badge to set/unset is not available.

See also “Keys” on page 61.

Card tamper lock

2.2.1.n.3.08. 6 Card Tamp.Lock
>Off<

If the option is set to On, the card reader and the keypad lock for 120 seconds when an unauthorized card is presented three times.

Note: The option only applies cards. Incorrect PINs will cause the keypad lockout regardless the option status.

Linked Reader

2.2.1.n.3.08. 7 Linked Reader
>Not set<

Use the menu to link a reader to the selected LCD keypad, so information from this reader is displayed on the keypad, and the reader is used for user authorization.

EE PIN lock

2.2.1.n.3. 09 EE PIN lock
>Yes<

If the EE PIN lock option is set to Yes, it is not possible to use a PIN during the entry time.

Note: If the keypad is configured as a reader, using this option is not allowed and causes a warning:

```
WARNING
Check door conf
```

In this case program this option using menu “Doors > EE PIN lock” on page 260 instead.

Isolate keypad

```
2.2.1.n.3. 10 Isolate Rkp
>No<
```

Use the Isolate keypad option to isolate the tamper fault events on the selected keypad. The keypad, however, remains functional.

Buzzer silent

```
2.2.1.n.3. 11 Buzzer silent
>During PS Exit<
```

It is possible to disable the keypad buzzer for particular events. The following options are available:

- Never: Buzzer operates normally. It is impossible to mute the buzzer using X + Left volume control.
- During PS exit: Buzzer does not sound when part setting. The manual volume control is available without limitations.
- Always: Buzzer is disabled. The manual volume control is available without limitations.
- During EE: Buzzer remains silent during entry and exit time.

Quick set mode

```
2.2.1.n.3. 12 Quick set
>Off<
```

The Quick set option allows setting areas without providing user PIN or card. If this functionality is on, the premises are set after pressing On without user authorization.

The following options are available:

- Off: Quick set is disabled
- Without list: All areas assigned to the keypad are set after pressing On
- With list: After On is pressed, the system prompts to choose areas from those assigned to the keypad.

This option affects part setting as well.

Function keys

2.2.1.n.3. **13 Function keys** → 1>A key
>>> 2 B key

Function keys menu allows you to assign a user programmable function to any of available function keys. See “User programmable functions” on page 104 for more details.

Function keys availability depends on the keypad type. See also “Keypad type” on page 195.

Area indication for LED 1

2.2.1.n.3. **14 Area ind.LED1** → 01-10>Area ind.>
1.....> 1.....

Area ind.LED1 allows you to assign areas to the programmable LED 1 of the keypad. The indicator is green when all areas assigned are ready to set. It turns red when any area assigned is set or part set. The red indicator is flashing when there is an alarm in an area assigned to it.

Note: This functionality is different when only one area is assigned to both indicators. In this case the combination of two indicators shows another two states of this area:

- LED 1 is red, LED 2 is off: The area is in part set 1 state.
- LED 1 is off, LED 2 is red: The area is in part set 2 state.

This indication requires the selected keypad to be assigned only to this particular area both for view and control. See “View areas” on page 197 and “Control areas” on page 197.

Area indication for LED 2

2.2.1.n.3. **15 Area ind.LED2** → 01-10>Area ind.>
1.....> 1.....

Use Area ind.LED2 to program LED 2 indicator in the same way as described in “Area indication for LED 1” above.

Status indication mode

2.2.1.n.3. **16 Status ind.**
>List<

Status indication defines how the area status list is displayed. The following options may be available, depending on panel variant and keypad model:

- Area list: The areas are displayed as a vertical list with names and statuses, which requires scrolling.
- Area symbolic: All areas are displayed in one screen. Only area numbers and statuses are displayed.
- Area group list: The same as list, but for area groups.

- Area group symbolic: The same as symbolic, but for area groups.

See *AXON Control Panel User Manual* for more information on area selection.

LCD backlight behavior

2.2.1.n.3. 17 LCD backlight
>Normal<

LCD backlight option defines when the keypad display backlight is lit. There are the following options available:

- Always on: LCD backlight never switches off.
- Normal: LCD backlight switches off after the certain idle time.
- Excluding entry time: LCD backlight is off during the entry time, until a key is pressed.

Note: The backlight timeout depends on the keypad firmware.

ACK on keypad

2.2.1.n.3. 18 ACK on keypad → 1>Rkp 1
2 Rkp 2

The ACK on keypad option allows you to select an additional LCD keypad that displays an acknowledgement prompt after the system is unset using the selected non-LCD keypad or reader.

Note: This option is only available for non-LCD keypads and card readers.

See also “ACK on keypad” on page 235 for more details.

EE 1 buzzer

2.2.1.n.3. 19 EE 1 buzzer
>Yes<

If the option is set to Yes, the buzzer of the selected keypad is active during entry/exit time 1.

See “2. Entry/Exit 1” on page 49 for more details.

EE 2 buzzer

2.2.1.n.3. 20 EE 2 buzzer
>Yes<

If the option is set to Yes, the buzzer of the selected keypad is active during entry/exit time 2.

See “18. Entry/Exit 2” on page 51 for more details.

1+3 keys

2.2.1.n.3. 21 1+3 keys
>Yes<

If the option is set to Yes, the combination of 1 and 3 keys allows you to raise a panic alarm.

See *AXON Control Panel User Manual* for more details.

This functionality is only available for ATS113x keypads.

RTE

2.2.1.n.3. 22 RTE
>On<

If the option is set to On, the request to exit input of the selected keypad is enabled.

Backlight

2.2.1.n.3. 23 Backlight
>On<

If the option is set to On, the key backlight of the selected keypad is always active. If set to Off, the backlight lights up only for 30 seconds after pressing a key or presenting a card.

Nightlight

2.2.1.n.3. 24 Nightlight
>On<

If the option is set to On, the key nightlight of the selected keypad activates in 30 seconds after pressing a key or presenting a card. Note that the “Backlight” option described above must be set to Off for the Nightlight to activate.

Card beep option

2.2.1.n.3. 25 Card beep opt
>On<

If the option is set to On, the beep sounds when a card is badged on the keypad reader.

Idle screen

2.2.1.n.3. 26 Idle scr opt → 1>Logo
>>> 2 Custom msg

The menu contains a set of options for the keypad idle screen.

Logo

2.2.1.n.3.26. 1 Logo >On<

If the option is set to On, the logo is shown when the idle screen is active.

Custom message

2.2.1.n.3.26. 2 Custom msg >On<

If the option is set to On, the custom message configured in the panel settings is shown when the idle screen is active.

See also “Custom message” on page 306.

Time and date

2.2.1.n.3.26. 3 Time and date >On<

If the option is set to On, time and date are shown when the idle screen is active.

Text background

2.2.1.n.3.26. 4 Text bkgd >On<

If the option is set to On, the custom message as well as time and date is shown on the background when the idle screen is active.

Text color

2.2.1.n.3.26. 5 Text color >White<

Select the color of the text for the custom message, time, and date displayed when the idle screen is active. The following values are available:

- White
- Black

Schedule

2.2.1.n.3. 27 Schedule >>> → 1>Sel schedule 1
Not used

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

Keypad menu

2.2.1.n. 4 Keypad menu
>>>

The keypad menu provides access to the programming menu built-in to the keypad. For more information, see the appropriate keypad manual.

Reset comm. key

2.2.1.n. 5 Reset Comm Key
>Cancel<

The menu allows you to reset an encryption key used for the secure channel communication between the selected secure device and the control panel. Use this menu to recover the secure channel in case of the device replacement, or a system bus communication fault.

Caution: When the security channel is used, use this option only if your system data bus is physically secured against unauthorized access.

See Chapter 3 “System functions > Secure channel” on page 127 for more information.

Delete keypad

2.2.1.n. 6 Delete keypad
>Cancel<

To remove the keypad, press Enter, select OK and press Enter again. The keypad is deleted.

Note: Before removing a keypad, you should remove any outputs or condition filters connected to the keypad.

Expander devices

2.2. 2 Exp devices → 0>Add expander
3 DC/LC Exp Rdrs 1 Exp 1

On the Expander devices menu, press 0 to add an expander, or a number to configure an existing one.

Note: The maximum number of devices allowed on the data bus is given in “General features” on page 39.

Expander options

Add expander

```
2.2.2. 0 Add expander
        1 Expander 1    → Expander number
                           >_<
```

On the Add expander menu, enter the number for the new expander and press Enter to confirm, or Clear to exit without adding a device.

After the device is added, the expander configuration options are shown.

Select expander

```
2.2.2. 1 Exp 1
        2 Exp 2    → 1>Expander type
                           ATS1201
```

Select the expander number to configure.

Expander type

```
2.2.2.n. 1 Expander type
                           ATS1201
```

The expander type is an informational screen. The type is set by the expander.

Expander address

```
2.2.2.n. 2 Exp address
                           BUS: 1 ADDR: 1
```

The expander address is an informational screen providing the DIP switch address.

Expander range

```
2.2.2.n. 3 Expander range
                           113-128
```

Expander range is an informational screen. It shows zone range available for this expander.

Note: In case of 32-zone devices there are two zone ranges.

```
3 Expander range
  113-128 353-368
```

See “Expander mode” on page 210 for more details.

Expander settings

```
2.2.2.n. 4 Exp settings    → 01>Expander name
                           >>> Exp 1
```

The Expander settings menu contains menus shown below, which are necessary to configure the selected expander.

Note: The available settings depend on the expander type.

Expander name

2.2.2.n.4. 1 Expander name
>Expander 1 <

Use the Expander name option to enter a name that identifies the expander to the end-user.

When an expander is created, it is given the default name “Expander <n>”, where <n> is the expander address. Enter this menu to edit the current name.

An expander name can consist of 16 characters.

Tamper area

2.2.2.n.4. 2 Tamper area
Area 1 → 01>Area 1
02 Area 2

The Tamper area option determines which area receives expander tamper and fault events. To change it, press Enter and select the area.

Detect tamper

2.2.2.n.4. 3 Detect tamper
>On<

If the option is set to Off, the device tamper detection is disabled.

Isolate expander

2.2.2.n.4. 4 Isolate Exp
>No<

Use the Isolate expander command to isolate the tamper fault events on the selected expander. The expander, however, remains functional.

Input mode

2.2.2.n.4. 5 Input mode
>Dual loop<

The Input mode option determines the configuration of zone inputs in the expander. This setting is similar to the panel zone input mode, which is described in “Input mode” on page 239.

See “Zone connection” on page 27 for more details on EOL usage.

End of line resistor

2.2.2.n.4. 6 EOL
>4k7<

The End of line resistor menu allows you to define an end-of-line resistor value for expander zone inputs. This setting is similar to the panel zone input EOL, which is described in “End of line resistor” on page 240.

See “Zone connection” on page 27 for more details on EOL usage.

Expander menu

2.2.2.n. 5 Expander menu
>>>

The menu provides an access to the programming menu built-in to the expander. For more information, see the appropriate expander manual.

Note: This menu is not available in wireless expanders ATS1235 with firmware version 1.20 and newer.

Delete expander

2.2.2.n. 7 Delete Exp >>> → 0>Delete all
1 Delete zone

Use the Delete expander command to delete an expander, or certain system elements assigned to it, for example, zones or outputs.

Depending on the expander type, the following options may be available:

- 0 Delete all: Delete expander and all elements assigned to it.
- 1 Delete zone: Delete zones assigned to the selected expander.

```
465>Zone 465
466 Zone 466
```

The list of assigned zones is shown.

Select a zone and press Enter to delete it.

```
Delete zone
>Cancel<
```

Select OK and press Enter to confirm.

- 2 Delete fob: Delete fobs assigned to the selected expander.
- 3 Delete output: Delete outputs assigned to the selected expander.

If no elements are assigned to the selected expander, you can only delete the expander itself.

```
Delete expander
>Cancel<
```

Select OK and press Enter to confirm. The expander is deleted.

Note: Before removing an expander, you should delete any condition filters connected to the expander.

Wireless specific options

Supervision

2.2.2.n.4. **4 Supervision** >>> → 1>Short superv. 20

The supervision is used to disable arming if the wireless expander does not receive a supervision message from a sensor within the short supervision time.

A programmable supervision function checks the state of the devices in the field. The supervision timers in the sensors are “dithered” by a small time so that transmissions occur on a random basis with the effect of minimizing collisions in larger installations.

Notes

- Two- and four-button fobs don’t transmit supervision signals
- Supervision time cannot be set for individual sensors, only for individual wireless expanders

Short supervision time

2.2.2.n.4.4. **1 Short superv.** >20<

Short supervision is used to disable arming if the wireless expander does not receive a supervision message from a sensor within the short supervision time.

The allowed range is 20 to 1920 minutes.

Long supervision time

2.2.2.n.4.4. **2 Long superv.** >20<

Long supervision sets an alarm condition in the panel for a sensor which supervision timer expired. Program the supervision time to control how often the wireless expander checks the sensor is communicating and in range of the wireless expander.

The allowed range is 20 to 1920 minutes.

Smoke supervision time

2.2.2.n.4.4. **3 Smoke superv.** >65<

Smoke supervision sets a fault condition in the panel when a detector supervision timer expired. Program the supervision time to control how often the wireless expander checks that the sensor is communicating and in range of the wireless expander.

The allowed range is 65 to 1920 minutes.

Receiver Sensitivity

2.2.2.n.4. 5 R.Sensitivity
>Normal<

Use the Receiver Sensitivity menu to decrease the wireless expander sensitivity. Changing the value from Normal to Low reduces the sensitivity by 6 dB.

After exit from the programming mode the sensitivity returns to Normal.

Expander mode

2.2.2.n.4. 6 Expander mode
>16 inputs<

Choose one of the following modes for the expander:

- 16 inputs: The expander is fitted with 16 zones.
- 32 inputs: The expander is fitted with 32 zones.

Notes

- 32 inputs mode is only available in the wireless expander with firmware version 1.20 or newer.
- Zones assigned to inputs 17–32 are not adjacent with those assigned to inputs 1–16 of the expander. For example, first 16 inputs are assigned to panel zones 113 to 128, and inputs 17 to 32 are assigned to zones 353 to 368.

Expander version

2.2.2.n.4. 7 Exp version
>>> → AT51238.B008

The Expander version screen is an informational screen with the expander version data.

Jamming menu

2.2.2.n.4. 8 Jamming menu
>>> → 1>Jamm detection
Enable

Use the menu to set the jamming detection options.

Jamming detection

2.2.2.n.4.8. 1 Jamm detection
>Enable<

The Jamming detection option must be set to Enable if the wireless expander must detect and report communication jamming attempts.

A jamming condition occurs if the jamming is present within any one minute for a longer period than it is set in “Jamming Seconds” on page 211. The required jamming threshold is set in “Jamm Threshold” on page 211.

Note: The above-mentioned menus are only available for ATS1235 firmware version V1.20 and newer. In older versions the values are set using the internal expander menu.

Jamming Seconds

2.2.2.n.4.8. 2 Jamming Sec
30

The jamming period can be configured from 10 to 50 seconds. Default value is 30 seconds.

Jamm Threshold

2.2.2.n.4.8. 3 Jamm Thresh
44.8%

The jamming threshold can be configured from 25.0 to 75.0%. The default threshold value is 44.8%.

Default expander

2.2.2.n.4. 11 Default exp
>No<

Reset the wireless expander to the factory settings.

Camera specific options

Pic options

2.2.2.n.4. 9 Pic options >>> → 1>Pic settings >>>

This menu is specific for systems with wireless PIR camera expanders. See “Using wireless cameras” on page 116 for more details.

Pic settings

2.2.2.n.4.9. 1 Pic settings >>> → 1>Burglar set. >>>

The menu allows you to configure photo recording options separately for the following camera event types:

- Burglar alarms
- Fire alarms
- Panic alarms
- Medical alarms
- Tamper alarms
- Faults: Device faults and technical alarms
- Custom type 1: User programmable type 1
- Custom type 2: User programmable type 2

See also “Camera event types” on page 116.

Burglar settings

2.2.2.n.4.9.1. 1 Burglar set. >>> → 1>Pic amount 1

Enter the BA settings menu to configure picture settings for burglar alarms.

Pic amount

2.2.2.n.4.9.1.1. 1 Pic amount >1<

Set the number of pictures taken after an event of the selected type occurs.

Allowed range is 1 to 30. The delay between pictures is set in “Frame rate” below.

Frame rate

2.2.2.n.4.9.1.1. 2 Frame rate >500 ms<

The menu defines a frequency of taking pictures on an event of the selected type.

The menu is only available if “Pic amount” above value is larger than 1.

The allowed values are 500 ms, 1 s, 5 s, 15 s, 60 s.

Picture resolution

2.2.2.n.4.9.1.1. 3 Pic resolution >QVGA<

The option defines resolutions of pictures taken upon an event of the selected type. The following options are available:

- QVGA: 320 x 240 pixels
- VGA: 640 x 480 pixels
- QVGA and VGA: Two pictures at once, one in low resolution, and one in high.

Fire settings

Panic settings

Medical settings

Tamper settings

Fault settings

See “Burglar settings” above

Custom type 1

Custom type 2

Custom types are used with condition filters for camera activation.

See “Burglar settings” on page 212

Show picture memory

2.2.2.n.4.9. 2 Show pic mem → Pictures: 12 → Free sp: 3,0MB
 3 Pic autodel Left sp for: 123 Total sp: 4,0MB

The informational screen shows a pictures number currently stored in the wireless PIR camera expander as well as available memory.

Pic auto deletion

2.2.2.n.4.9. 3 Pic autodel → 3 Pic autodel
 4 Total pic cnt >1<

The value defines whether the pictures stored in the wireless PIR camera expander will be deleted automatically after a chosen period (in days).

The allowed range is 1 to 120 days. 0 or Off mean that pictures are never deleted automatically. Users must control the available memory and remove pictures manually.

Total picture counter

2.2.2.n.4.9. 4 Total pic cnt → Total pic cnt:
 ----- 12

The Total picture counter shows how many pictures were stored on the PIR camera expander flash memory since the beginning of its lifetime.

Delete pictures

2.2.2.n.4.9. 11 Delete pics → 11 Delete pics
 ----- >Cancel<

Choose OK and press Enter to remove all stored pictures from the wireless PIR camera expander.

Four-door expander specific options

Output modules number

2.2.2.n.4. 7 Outp. modules
 >0<

Enter the number of output controllers fitted to the door controller.

Allowed range is 0 to 32 (ATS125x) or 0 to 16 (CDC4). 0 means no clocked output card connected. Note that there are four open collector outputs available on the door controller for a 4-way relay card.

Region count limit

2.2.2.n.4. 8 Reg cnt limit
>65534<

When the number of users reaches this limit, the door controller sets an internal flag (region count limit) that can be used in the door controller macro logic. You may activate events when a certain number of users are in a region.

The allowed range is 0 to 65534.

Examples:

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

Macro Logic

2.2.2.n.4. 9 Macro Logic → 00>Add macro
10 Local Devices 01 Macro 1

Use the menu to program door controller macros.

For more information on macros, see “Door controller macro logic” on page 81.

Add macro

2.2.2.n.4.9. 00 Add macro
01 Macro 1

Access the Macro filter menu option to add a macro. If the macro is created successfully, the following message appears:

INFO
Macro added

The new macro is given the default name “Macro N” and placed on the end of the macro list. You can now start editing its details.

Select macro

2.2.2.n.4.9. 01 Macro 1
02 Macro 2

Select an existing macro to program.

Macro name

2.2.2.n.4.9.m. 1 Macro name
>Macro 1 <

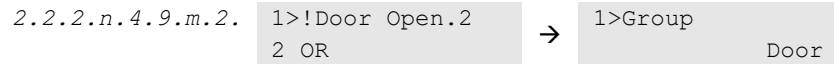
The name identifies the macro for installer, making the programming dependencies clearer.

Formula



The Formula menu allows definition of the macro formula. 4 events can be combined in a formula.

Select event



Select the appropriate event to configure it.

To choose an appropriate event, you must define the source of the event first. The source is defined by a group of objects, and an object within this group. Available groups are listed in Appendix A “AXON events”, Table 34 on page 432.

When the group and the object (if available) are selected, select the appropriate event. The available selection depends on the selected source. The full event list with sources is shown in Appendix A “AXON events”, Table 34 on page 432.

The following functions are available for the selected event:

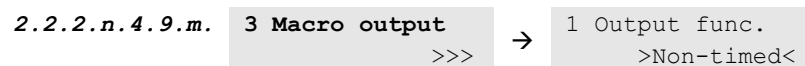
1. Group: Select group.
2. Input flag: Select an input flag from the group above.
3. Item: Select an item for the Input flag above.
4. Inversion: Invert the selected event. If inverted, it is marked with '!' in the formula.

Note: Certain events can only be inputs, while some events can be used as outputs only.

Select Operator

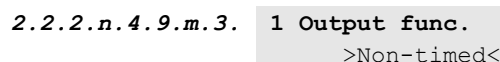
All events are joined with logical operators. Choose the operator to change it. Valid operators are AND and OR.

Macro output



Configure the output of the selected macro.

Output function



Output functions are described in “Door controller macro logic” on page 81.

Duration

2.2.2.n.4.9.m.3. 2 Duration > <

Provide the duration for the output function from the previous menu.

Units are shown in the menu title. The allowed range is 1 to 255.

Activate

2.2.2.n.4.9.m.3. 3 Activate → 1>Group Door

Select the output event the same way as you configure the input event. See “Select event” on page 215 for details.

Delete macro

2.2.2.n.4.9.m. 4 Delete macro >Cancel<

Use the command to remove a macro from the door controller. To remove the macro, select Ok and press Enter.

Local Devices

2.2.2.n.4. 10 Local Devices >>>

The menu is equal to “Door Control/Lift Control Expander Readers”, but applies only to readers connected to the local bus of the selected door controller. Refer to “Door Control/Lift Control Expander Readers” on page 217.

Device version

2.2.2.n.4. 11 Dev version → 1250.0000.11MIUM

The informational screen shows the door controller firmware version.

Synchronize

2.2.2.n.4. 12 Synchronize >Cancel<

The menu allows you to synchronize control panel and door controller settings.

Select OK and press Enter to synchronize. The following data will be sent from the control panel to the selected door controller, depending on its model: users, schedules, settings.

The synchronization process start is confirmed on the LCD screen.

INFO
Sync started

Door Control/Lift Control Expander Readers

2.2. 3 DC/LC Exp Rdrs → 0>Add reader
1 Reader 1

Keypads and readers, connected to one of door controller local buses, can be configured as intelligent system readers to provide access control functions.

Press 0 to add a reader, or a number to configure an existing one.

Note: The maximum number of devices allowed on the data bus is given in “General features” on page 39.

Reader options

Add reader

2.2.3. 0 Add reader → Reader number
1 Reader 1 >_<

On the Add reader menu, enter the number for this new reader and press Enter to confirm or Clear to exit without adding a device.

After the device is added, the reader configuration options are shown.

Select reader

2.2.3. 1 Reader 1
2 Reader 2

Select the reader number to configure.

Reader address

2.2.3.n. 2 Reader address
Exp: 1 ADDR: 0

The information screen showing the reader address. The address is set by DIP switches or programmed within the keypad or reader menu.

Reader options

2.2.3.n. 3 Reader options → 1>Reader name
Reader 1

The Reader options menu contains the shown below, which are necessary to configure the selected Reader.

Reader name

2.2.3.n.3. 1 Reader name
>Reader 1<

Use the Reader name option to enter a name that identifies the reader to the end-user.

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

A reader name can consist of 16 characters.

LCD

2.2.3.n.3. 2 LCD
>Yes<

The LCD option determines whether the selected reader has LCD.

Note: If the door controller recognizes the model of the selected reader, this value will be read-only.

Delete reader

2.2.3.n. 5 Delete reader
>Cancel<

To remove the reader, press Enter, select OK and press Enter again. The reader is deleted.

Databus EOL termination

2. 3 Databus EOL
----- → 1>BUS#1 EOL
Off

The menu allows you to activate built-in 470 Ω termination EOL for each system data bus. Select the data bus first, then set On to activate termination of this bus.

See “System data bus preferred wiring” on page 26 for more information.

User menu

3 User menu	→	1>Users
4 Zones&Areas		2 User groups

Use the User menu to add, edit, or delete users of the AXON system. This menu also allows user groups editing.

Users

3.	1 Users	→	0 Add user
	2 User groups		1 Installer

The Users menu lets you add, delete and edit system users.

Add user

3.1.	0 Add user	→	Add mode
	1 Installer		>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 read the new user card.

Badge card Rkp 1

Read the card on the reader or the door programmed in System Options. See “Card learn-in” on page 323 for more details.

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 read 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

Select user

Select a user to edit.

The following options can be configured.

User name

```
3.1.n. 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.

PIN

```
3.1.n. 2 PIN code → 1>Change PIN
>>>
```

The menu allows changing user PIN as well as setting up the remote user code.

Change PIN

```
3.1.n.2. 1 Change PIN
*****
```

Change the selected user PIN.

See “PIN” on page 76 for details on PIN usage.

Remove PIN

```
3.1.n.2. 2 Remove PIN
*****
```

Remove the selected user PIN.

User card

```
3.1.n. 3 User card → 1>Assign card
>>> Card not set
```

The User card menu lets you assign or delete a user card.

The content of the menu depends on whether a card has been already assigned or not.

Assign card

```
3.1.n.3. 1 Assign card → INFO
Card not set Badge card
```

If the user has no card assigned, the menu lets you enter a user card number.

Press Enter and present the card at the keypad within 10 seconds.

Note: This operation is only possible on keypads with integrated readers. The keypad or the door for card learning is defined in System Options. See “Card learn-in” on page 323 for more details. If another keypad or door is selected for card learning, the learning keypad or door name is prompted, for example:

```
Badge card
Keypad 3
```

Remove card

If the user has a card assigned, you can remove the assigned card. The following screen appears.

```
3.1.n.3. 1 Remove card
          Card set
```

Press Enter.

```
INFO
Card removed
```

The card has been removed from the selected user.

RF fobs

```
3.1.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.

The menu contents are similar to the Zones and areas > RF fobs menu described on page 250.

Language

```
3.1.n. 5 Language
          ENGLISH UK
```

The AXON system can display menus in the preferred language of each user. Contact your supplier to get more information about available languages.

User groups

```
3.1.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 8 user groups assigned. User groups define the options and areas available for users.

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.

```
2>Supervisor Grp
3 Area 1
```

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

If the selected slot already contains a user group assigned, you are moved to the “Change User Group” menu.

```
3.1.n.6. 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 choose the appropriate group.
- Remove the assigned group: Press 2, or go the next menu entry and press Enter.

Note: The Installer user group can only be assigned to the installer.

For more information on user groups, see “User groups” on page 226.

Remote options

```
3.1.n. 7 Remote opts  → 1>Remote login
          >>>          None
```

The menu contains configuration menus for remote access.

Login for remote access

```
3.1.n.7. 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.

Change password

```
3.1.n.7. 2 Chg rem passwd  → New passwd
          *****          >
```

Use the menu to change the user remote password.

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

INFO
Password changed

Mobile number

3.1.n.7. 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. See "Type" on page 336.

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

SMS reporting

3.1.n.7. 4 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 the user belongs to a user group that has the SMS reporting privilege enabled. See "User group options" on page 227 for more information.

SMS control

3.1.n.7. 5 SMS control
Disable

The SMS control menu lets you enable or disable SMS control for the selected user.

This option can be changed only if the user belongs to a user group that has the SMS control privilege enabled. See "User group options" on page 227 for more information.

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.

Access options

3.1.n. 8 Access opts >>> → 1>Door group
Not used

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

Door group

3.1.n.8. 1 Door group > → 0>Not used
Not used 1 Door group 1

Assign a door group to the selected user.

See Chapter 3 “System functions > Door groups” on page 80 for more information on door groups.

Floor group

3.1.n.8. 2 Floor group > → 0>Not used
Not used 1 Floor group 1

Assign a floor group to the selected user.

See Chapter 3 “System functions > Floor groups” on page 80 for more information on floor groups.

Trace

3.1.n.8. 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.

Privileged

3.1.n.8. 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.

Extended access

3.1.n.8. 5 Ext. access >No<

If set to Yes, the selected user has an extended door unlock time and shunt time granted after reading a valid card or entering PIN. The extended time is set separately for each door. See “Extended time” on page 258.

Access user type

3.1.n.8. 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. See “High security” on page 81 for details.

Select mode

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

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:

3.1.n. 10 Delete user
>Cancel<

Choose Ok and press Enter. This removes the user.

Repeat the command 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.

User groups

```
3.  2 User groups
-----
    → 00>Add UG
       01 Installer Grp
```

The User group program block is used to record information about user groups.

User group settings

Add user group

```
3.2.  0 Add UG
```

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

```
INFO
UG added
```

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

Select user group

To edit a user group, select a user group first.

The following options can be configured.

User group name

```
3.2.n.  1 UG name
        >User group 6  <
```

Use the UG name option to set the user group name. Press Enter to edit the name, or Clear to exit.

The user group name can have up to 16 characters.

User group type

```
3.2.n.  2 UG type
        >Normal user<
```

Choose a type of the selected user group.

For detailed user group type description and available user group types, see “User group types” on page 71.

User group areas

```
3.2.n.  3 UG areas
    → 01-10>UG areas
       1.....
```

The User group areas option defines which areas the user can control.

User group area group

3.2.n. 4 UG AG
.....> → 01-10>UG AG
1.....

The UG area group option defines which area groups the user can control.

User group filter

3.2.n. 5 UG filter
Not used → 0>Not used
1 External Siren

When using a filter, the user rights defined by the user group depend on this filter state.

For more information on condition filters, see “Condition filters” on page 280.

User group options

3.2.n. 6 UG options
>>> → 1>Full set
Yes

User group options define the user access rights to the particular options.

Available options are listed in “User group options” on page 73.

Schedule

3.2.n. 7 Schedule
>>> → 1>Privileges
2 Area access

Select schedules for the selected user group.

The shortcut menu allows you to assign up to two schedules to each of the following elements:

- 1 Privileges
- 2 Area access

See “Schedule shortcut menu” on page 90 for more information.

Remove user group

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

The display shows:

3.2.n. 8 Remove UG
>Cancel<

Choose Ok and press Enter. This removes the user group.

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

Note: You cannot delete a user group if you have users, actions or central stations assigned to it.

Zones and areas

4 Zones&Areas → 1>Zones Menu
2 Areas

In the Zones and Areas programming section all zone, fob, and area parameters are programmed.

Caution: Select the required object numbering scheme before programming zones. See “Object scheme” on page 320 for details.

Zone menu

4. 1 Zones Menu → 0>Add zone
2 Areas 1 Zone 1

This menu lets you see all programmed zones, select an existing zone, or create a new one.

Each zone can be a physical input on the control panel, an expander, or a plug-in expander, or a wireless device programmed in the wireless expander.

Zone options

Add zone

4.1. 0 Add zone → 0>Zone
1 Zone 1 1 Panel

Use the Add zone menu to add a new zone. When adding a zone, select one of the following options:

- 0 Zone: Add a zone assigned to the specific system input.
- 1 Panel: Add a zone assigned to the specific panel input.
- 2 Panel exp.: Add a zone assigned to the specific panel expander input.
- 3 Exp.: Add a zone assigned to the specific expander input. Select an expander first.

If the selected expander supports both wired and wireless zones, you are prompted to choose the appropriate option.

Sensor device
>Wireless<

For wired zone, select an input on the expander.

For wireless devices, refer to “Adding a wireless sensor” on page 229.

- 4 Auto-detect: Add a zone assigned to the first unused system input.

See “Zone, output, and door addressing” on page 34 for available zone addresses.

If the chosen zone already exists, a warning is displayed.

If the zone is created successfully, you are moved to the menu “Zone name”.

Adding a wireless sensor

If the selected expander is a wireless expander, adding zone results in learning the wireless sensor by the wireless expander.

Wireless sensor learning is described in “Wireless device programming” on page 109.

If the device is a wireless PIR camera, a corresponding camera will be also created in the camera database. See “Using wireless cameras” on page 116.

Select zone

```
4.1.  1 Zone 1
      2 Zone 2      →  1>Zone name
                       Zone 1
```

Select a zone to program.

Note: Certain options in this menu differ for specific sensors. For specific options, see:

- “Shock sensor options” on page 242
- “Wireless sensor options” on page 242

Common options

Zone name

```
4.1.n.  1 Zone name
        >Zone 1    <
```

Use the Zone name option to set a zone name. The zone name identifies the zone to the end-user for alarm reporting or for display of status or error message. Without a proper name, the end-user would not be able to resolve problems that arise in a particular zone.

When a zone is created, it is given the default name “Zone n”.

Enter this menu to edit the current name.

A zone name can consist of 30 characters.

Zone type

```
4.1.n.  2 Zone type
        Alarm
```

Use the Zone type menu to set the zone type for a specific zone. The zone type determines exactly how the zone functions in given circumstances. Each zone type behaves differently.

Notes

- Available zone options depend on the zone type.
- Zone type for a wireless device is initially defined by the device type during the device learning. For example, the zone with a panic button is set by default with type “Panic”.

All available zone types and their options are listed in “Zone types” (see page 49).

Isolate

```
4.1.n.  3 Isolated
                >No<
```

The option allows you to isolate or de-isolate the selected zone.

Zone location

```
4.1.n.  4 Zone location
                Panel 1.1
```

The field informs what physical input the zone is connected to.

Zone areas

```
4.1.n.  5 Zone areas
1.....> → 01-10>Zone areas
                1.....
```

The zone needs an area to be able to send alarm information to the central station, and to be able to reset when an alarm occurs. Use the Areas menu to assign the area to the zone that must alarm when the zone is activated, and the area status (set or unset) meets the requirement for the zone type.

In case multiple areas are selected, the alarm is reported to the lowest area number assigned. The alarm occurs depending on the zone type and only if all assigned areas are set.

The function of the zone depends on the zone type selected during programming.

The screen shows a list of areas that the zone is assigned to. For example, the screen above shows that the zone is assigned to areas 1 and 2.

Zone options

```
4.1.n.  6 Zone options
                >>> → 1>Inhibit
                        No
```

The Zone options menu contains all zone settings. These settings are described below.

Note: Not all options may be available. The available options depend on the zone type (see “Zone types” on page 49).

Inhibit

4.1.n.6. 1 Inhibit
>No<

If the Inhibit option is set to Yes, this zone can be inhibited by users.

Isolate

4.1.n.6. 2 Isolate
>Yes<

If the Isolate option is set to Yes, this zone can be isolated by users.

Exclude in part set 1

4.1.n.6. 3 Excl. in PS1
>No<

When a zone is programmed for excluding while part set (the Exclude in part set option is set to Yes), it is excluded when the assigned area is part set. The normal unset conditions, if relevant, continue to be monitored (tamper, masking, etc). If the Exclude in part set option is set to No, the zone is set in both part set and full set modes.

There are two independent part sets available, PS1 and PS2.

Exclude in part set 2

4.1.n.6. 4 Excl. in PS2
>No<

See “Exclude in part set 1” above.

Double knock

4.1.n.6. 5 DblKnock
>No<

If the Double knock option is set to Yes, the zone requires two parameters to be present in order to generate an alarm. If the zone becomes active and would normally trigger an alarm, either the zone needs to remain active for the programmed Double Knock open time (see “Double knock open” on page 299) or the zone has to return to normal and trigger again within the Double Knock interval (see “Double knock interval” on page 299).

Note: If the option is active, the option “Zone held open” on page 237 is not available.

Swinger shunt

4.1.n.6. 6 Swinger shunt
>No<

If the Swinger shunt option is set to Yes, the number of alarms from this zone is limited to the number set in “Swinger shunt” (see page 314) for one set/unset cycle.

Anti mask

4.1.n.6. 7 Anti mask
>No<

When the Anti-mask option is set to Yes, the lower alarm window, nominally half of the EOL, is monitored for a detector masking condition.

See “Zone connection” on page 27 for more details.

Zone pairing

4.1.n.6. 8 Zone pairing
>No<

If the Zone pairing option is set to Yes, this zone is considered as active only when two inputs activate: the assigned (n) and the next to the assigned (n+1).

The zone assigned to the next input (n+1) must exist in the system. This zone alarm is not logged if both zones are assigned to the same area.

Note: It is not possible to use this option on the zone assigned to the last input number.

Only zones of specific zone types can be paired. See Table 12 on page 52 for details.

Chime

4.1.n.6. 9 Chime
>Off<

If the Chime option is On, the zone can be switched off and, depending on “Chime menu” setting (see page 321), can activate a short signal on:

- The keypad buzzers on all keypads assigned to the related areas
- The internal siren assigned to the related areas

Soak test

4.1.n.6. 10 Soak test
>No<

The zone can be set in Soak test mode, which is useful for diagnostic purposes. The zone in soak test does not generate alarms on the system but its activation is logged. This zone is not checked during setting.

Note: If this option is active in an entry/exit zone, the entry/exit functionality is disabled, and entry/exit timers are not activated.

Engineer walk test

4.1.n.6. 11 Eng walk test
>No<

If the Engineer walk test option is set to Yes, the zone is included in the Engineer walk test. See “Walk test menu” on page 176 for more details.

User walk test

4.1.n.6. 12 User walk
>Yes<

If the User walk test option is set to Yes, the zone is included in the User walk test. See “Walk test menu” on page 176 for more details.

Shock sensor

4.1.n.6. 13 Shock sensor
>No<

The Shock sensor option activates the shock sensor functionality. If this option is set to Yes, the zone operates according to the settings configured in “Gross and Pulse options” (see page 242).

Only the internal panel inputs and the ATS608 expander inputs support this option.

Extend EE

4.1.n.6. 14 Extend EE
>No<

If the Extend EE option is Yes, the zone activation expands the entry time for the value defined by “Prealarm time” on page 247.

Note: After entry timer times out, local alarm activates.

Final door

4.1.n.6. 15 Final door
>No<

When the Final door option is set to Yes, the zone has the exit terminator functionality. If the zone is activated during the exit time, the exit timer is terminated after the Final Set delay has expired (see “Final set delay” on page 298) and the area is set.

Key latch

4.1.n.6. 16 Key latch
>No<

If the Key latch option is set to Yes, the key switch zone input is latching. If the zone state is active, the area is set. If the zone changes to normal, the area is unset.

If set to No, the input needs both states to toggle between set and unset (pulse key switch).

Key set

4.1.n.6. 17 Key set
>Off<

The Key set option defines the zone as a key switch for area set. The following options are available:

- Off: the area set is not affected by the zone.
- Key part set: zone is a key switch for area part set.
- Key full set: zone is a key switch for area full set.

Key unset

4.1.n.6. 18 Key unset
>No<

If the Key unset option is set to Yes, the zone is a key switch that unsets an area.

Technical full set

4.1.n.6. 19 Tech full set
>No<

The option defines how technical alarms are shown when the area is set:

- No: Technical alarms in this zone are disabled. They are neither indicated nor reported.
- Warning: Technical alarms are indicated as faults.
- Alarm: Technical alarms cause that fault LED is on, and the zone in alarm flag is raised.

If set to Warning or Alarm, technical alarms are reported with events listed in Table 27 on page 236.

Technical unset

4.1.n.6. 20 Tech unset
>No<

The option defines how technical alarms are shown when the area is unset:

- No: Technical alarms in this zone are disabled. They are neither indicated nor reported.
- Warning: Technical alarms are indicated as faults.
- Alarm: Technical alarms cause that fault LED is on, and the zone in alarm flag is raised.

If set to Warning or Alarm, technical alarms are reported with events listed in Table 27 on page 236.

Technical part set

4.1.n.6. 21 Tech part set
>No<

The option defines how technical alarms are shown when the area is part set:

- No: Technical alarms in this zone are disabled. They are neither indicated nor reported.
- Warning: Technical alarms are indicated as faults.
- Alarm: Technical alarms cause that fault LED is on, and the zone in alarm flag is raised.

If set to Warning or Alarm, technical alarms are reported with events listed in Table 27 on page 236.

Keypad LCD

4.1.n.6. 22 Keypad LCD
>No<

If the Keypad LCD option is set to Yes, when the zone activates, the zone name is displayed on the keypad LCD on all keypads, related to the area.

Log

4.1.n.6. 23 Log
>No<

The Log option determines whether the zone event is recorded in the system log.

CS report

4.1.n.6. 24 CS report
>No<

The CS report option determines whether the zone event is reported to the central station.

Delay timer

4.1.n.6. 25 Delay timer
>No<

A delay timer is activated for this zone if the Delay timer option is set to Yes. The delay timer is set in “Input delay” (see page 300).

ACK on keypad

4.1.n.6. 26 ACK on keypad → 0>Not set
Rkp 1 1 Rkp 1

Acknowledge options are available for keyswitch zone type. They allow you to define a keypad where the user is logged in automatically. This causes that an alarm and fault information is displayed instantly on the selected keypad.

The ACK session opens for 2 minutes. During this time you can acknowledge the alarm on the programmed keypad.

Note: “ACK by user” below must be also set for the acknowledgement functionality to work.

ACK by user

```
4.1.n.6. 27 ACK by user → 0>Not set
          >User 3<       1 Installer
```

The option defines the user that is logged in automatically when the selected zone causes an alarm.

Note: “ACK on keypad” on page 235 must be also set for the acknowledgement functionality to work.

See “ACK on keypad” on page 235 for more details.

See also “ACK on keypad” on page 202.

Sensor type

```
4.1.n.6. 28 Sensor type
          >Low temp.<
```

The events reported by a technical zone depend on the type of the sensor connected. The Sensor type option specifies what the sensor is and what events it should report. The following sensor types are available:

- Low temperature detector
- High temperature detector
- Gas detector
- Water detector
- Fire alarm
- Generic
- Custom

Table 27 below lists events that may be reported for each sensor type.

Table 27: Sensor types and reported events

Sensor Type	Code	Alarm	Alarm restore	Bypass	Unbypass	Supervision long	Supervision restore
Low temp.	SIA	ZA	ZR	ZB	ZU	ZS	ZJ
	CID	E152	R152	E570	R570	E381	R381
Gas	SIA	GA	GR	GB	GU	GS	GJ
	CID	E151	R151	E570	R570	E381	R381
High temp.	SIA	KA	KR	KB	KU	KS	KJ
	CID	E158	R158	E570	R570	E381	R381
Water	SIA	WA	WR	WB	WU	WS	WJ
	CID	E154	R154	E570	R570	E381	R381

Sensor Type	Code	Alarm	Alarm restore	Bypass	Unbypass	Supervision long	Supervision restore
Fire	SIA	FA	FR	FB	FU	FT	FJ
	CID	E110	R110	E570	R570	E373	R373
Ext. module fail	SIA	ET	ER	UB	UU	ZS	ZJ
	CID	E333	R333	E570	R570	E381	R381
	VdS	0x30	0xB0	0x51	0xD1	0x30	0xB0
Ext. module tamper	SIA	ES	EJ	UB	UU	ZS	ZJ
	CID	E341	R341	E570	R570	E381	R381
	VdS	0x23	0xA3	0x51	0xD1	0x30	0xB0
Generic	SIA	UA	UR	UB	UU	ZS	ZJ
	CID	E150	R150	E570	R570	E381	R381
Custom	SIA	Selectable [1]	Selectable [1]	UB	UU	ZS	ZJ
	CID	Selectable [1]	Selectable [1]	E570	R570	E381	R381

[1] For custom sensor type, the zone activation event reporting code can be selected. See “Reporting code” on page 240 for more information.

See also Appendix B “AXON reporting codes” on page 437.

Virtual zone

4.1.n.6. 29 Virtual zone
Not set → 1>Outputs
2 Rkp

The menu allows mapping the selected zone to an existing output or a keypad.

If an output or a keypad is not set, the zone state follows the state of the physical input assigned.

- If an output is selected, the zone becomes a virtual zone that is active when the selected output is active. In this case the physical input has no effect on the zone.
- If a keypad is selected, the zone becomes a virtual zone, which is active when the selected keypad has request to exit state (RTE) active.

See also “Outputs” on page 78.

Zone held open

4.1.n.6. 30 Held open
>No<

The menu defines if this zone raises a “zone open too long” alarm while held open longer than for a defined period.

The held open period is defined in “Held open time” on page 300.

Note: If the option is active, the option “Double knock” on page 231 is not available.

EE set check

4.1.n.6. 31 EE set check
>No<

If set to yes, entry/exit or access zone must be in a normal state when setting the area. Otherwise, the user is not allowed to set premises until the problem is solved.

The option is only available for entry/exit and access type zones.

Alarm in PS1

4.1.n.6. 32 Alarm in PS1
>No<

If the option is set to yes, entry/exit zone becomes an alarm zone during part set 1.

Notes

- The option is only available for entry/exit type zones. See “Zone types” on page 49.
- The zone must be included into part set 1. See “Exclude in part set 1” on page 231.
- Zone functionality does not change if the same zone belongs to an area in full set state.

Alarm in PS2

4.1.n.6. 33 Alarm in PS2
>No<

The same as “Alarm in PS1” above, but for part set 2.

Report as

4.1.n.6. 34 Report as
>Panic (PA)<

Defines how panic alarm is reported to central stations.

- Report as panic: PA event is reported.
- Report as duress: HA event is reported.

See Appendix B “AXON reporting codes” on page 437 for details.

Notes

- This option is only available for panic type zones. See “Zone types” on page 49.

- The option is only available when Panic mode is set to Silent. Otherwise panic alarm is always reported as PA event. See “Panic mode” on page 321.

Detector Auto Test

4.1.n.6. 35 Auto test
>Yes<

If the option is set to yes, the detector will be tested automatically when auto test is active. See also “Detector test” on page 174.

Shunt

4.1.n.6. 36 Shunt
>Yes<

If the option is set to Yes, the zone can be shunted.

See “Zone shunt” on page 59 for details.

View isolated

4.1.n.6. 37 View isolated
>On<

If the option is set to On, users are warned about this zone being isolated when attempting to set or unset the appropriate area.

Limit reports

4.1.n.6. 38 Limit reports
>Off<

If the option is set to On, the reporting from the zone is limited with the time frame defined in “Limit reports” on page 314.

Input mode

4.1.n.6. 39 Input mode
>Dual loop<

The Input mode option determines the configuration of the zone inputs in the panel. The following values can be set:

- Single NO: In the single zone mode the panel can only detect an alarm from the zone. In the single input mode normal state depends on the EOL value. If this value is set to “No EOL” in “End of line resistor” on page 240, normal state for Single NO zone is open.
- Single NC: Similar to Single NO above, but If EOL is disabled in “End of line resistor” on page 240, normal state for zone is short.
- Dual loop: For dual loop to operate, every zone needs two or three EOL resistors. This enables the panel to detect multiple zone states, including alarm, tamper, masking etc., depending on connection type and EOL value set in “End of line resistor” on page 240. See “Zone connection” on page 27 for more details on EOL usage.

In the Dual loop mode, open or short input state causes zone tamper.

This is a setting for panel zone only. For expanders, see “Input mode” on page 207.

End of line resistor

4.1.n.6. 40 EOL
>4k7<

The menu allows you to define end-of-line resistor values. For different input modes the following values can be available: 1k0, 1k5, 2k, 2k2, 2k2+4k7, 3k3, 3k74, 4k7, 5k6, 6k8, 8k2, 10k, No EOL.

Note: Available EOL values depend on “Input mode” option described on page 239.

See “Zone connection” on page 27 for more details on EOL usage.

This is a setting for panel zone only. For expanders, see “End of line resistor” on page 207.

Indication

4.1.n.6. 41 Indication
>Off<

If the option is set to On, a technical alarm is indicated when the technical zone becomes active.

Reporting code

4.1.n.6. 42 Report code
UA → 113>UA
118 YP

If the technical zone is custom sensor type, use the menu to assign a SIA reporting code for this zone. This event is reported to the Central Station if the zone is activated.

For more information, see “Sensor type” on page 236.

Note: It is only possible to select a code of an event that has an appropriate restore code.

For a complete list of event activation and restore codes, see Appendix B “AXON reporting codes” on page 437.

Copy

4.1.n. 8 Copy
>>> → 1>Copy par. from
>>>

Use Copy menu to copy zone parameters.

The following copy methods are available.

Copy par. from

4.1.n.8. 1 Copy par. from → Zone 1
>>> Zone 2

Use the menu to import all zone parameters from a particular zone to the selected one.

Choose the zone which parameters must be copied to the selected one, and press Enter.

INFO
Params copied

All settings except the name are copied.

Block assign

4.1.n.8. 2 Block assign → Start input
>>>

Use the Block assign menu to copy all selected zone parameters to a range of inputs, creating the appropriate zones.

Select a start and the end of device input range.

The system creates or modifies the existing zones with parameters equal to the selected zone (except names that are default).

Note: Copying zone parameters does not copy a wireless device. The device must be programmed separately. See “RF details” on page 242 for more details.

Move zone

4.1.n. 9 Move zone → 004>Not used
>>> 009 Not used

Allows you to move the selected zone to other available zone number.

This option is only available in a flexible zone numbering scheme. See “Object scheme” on page 320 for details.

See also “Zone, output, and door addressing” on page 34.

Delete zone

4.1.n. 10 Delete zone
>Cancel<

Use the Delete zone command to remove a zone from the system. To remove the zone, select Ok and press Enter. The zone is deleted.

Notes: In case of a wireless device, the device is also removed from the wireless expander database.

Caution: If the zone is assigned to a two-zone RF device, both zones are deleted. See “Two-zone RF sensors” on page 113 for more details.

Shock sensor options

Gross and Pulse options

4.1.n. 7 Grs&Pls opts → 1>Pulse count
>>> 0

The Gross and Pulse options are valid if the “Shock sensor” functionality (see page 233) for this zone is set to Yes.

Pulse count

4.1.n.7. 1 Pulse count
0

Set the number of pulses within a time window that will activate the zone.

The following values are applicable:

- 1 to 9: number of pulses within 30 seconds that activates the zone. Only 1 count per second is taken into account.
- 0: the counter functionality is disabled.

Gross level

4.1.n.7. 2 Gross level
0

Use the Gross level option to set the level for a single pulse that activates the zone. The following values are applicable:

- 1 to 9: Gross attack level where 1 means high sensitivity, and 9 means low sensitivity
- 0: Gross level is disabled

Gross level can be checked in menu “ShockSens test” (see page 174).

Wireless sensor options

RF details

4.1.n. 7 RF details → 1>Sensor ID
>>> 10EBA9E

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

Note: This menu is only available for a wireless expander ATS1235 with firmware version 1.20 or newer, which is online.

Sensor identifier

4.1.n.7. 1 Sensor ID
10EBA9E

The screen allows you to view the sensor ID.

Note: First two digits of the sensor identifier also define the sensor type. See Table 28 below.

Sensor type

4.1.n.7. 2 Sensor type
DWS

The screen allows you to view the sensor type. The following sensor types are available:

Table 28: Wireless sensor types

Type	Description	ID
Repeater	Wireless signal repeater	0A*
CO	Carbon monoxide sensor	0D*
DWS	Door/Window sensor	10*
Smoke sensor	Smoke sensor	11*
PIR	Passive infrared detector	12*
2 button panic	2 button panic sensor	14*
Shock sensor	Shock sensor	18*
Sound sensor	Glass break sound sensor	1A*
PIR camera sensor	Wireless PIR camera	23*

Sensor mode

4.1.n.7. 3 Sensor mode
Single

The informational screen allows you to see if the sensor operates in two-zone mode. The following values are available:

- Single: Single zone sensor.
- Master: The selected zone is the first zone of a two-zone sensor.
- Slave: The selected zone is the second zone of a two-zone sensor.

See “Two-zone RF sensors” on page 113 for more details.

Supervision

4.1.n.7. 4 Supervision
>Off<

Enables or disables the wireless device supervision. Supervision of all types becomes active. See “Supervision” on page 209 for more details.

Sensor options

4.1.n.7. 5 Sensor opt
>Ignore tamper<

Sensor options depend on the type of the wireless device.

See an appropriate RF device manual for more information on available options. The following options may be available.

Table 29: Wireless sensor options

Option	Sensor type	Description
Reed and contact	Door/window sensor	Report alarms from both sources
Contact	Door/window sensor	Ignore reed alarms
Reed and shock	Shock sensor	Report alarms from both sources
Shock sensor	Shock sensor	Ignore reed alarms
Reed	Door/window sensor, shock sensor	Only report reed alarms
Notice tamper	Smoke sensor	Control housing tamper alarms
Ignore tamper	Smoke sensor	Ignore housing tamper alarms

Remove RF device

4.1.n.7. **6 Remove RF dev** → Remove RF dev?
>>> >Cancel<

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

Areas

4. **2 Areas** → 1>Area 1
3 Area groups 2 Area 2

The Area menu allows you to configure areas.

See “Areas” on page 55 in Chapter 3 “System functions” for details.

Each area can be programmed with a number of options, like the area name, entry and exit times etc. Before going any further, select the area to program.

Area options

Select area

4.2. 1>Area 1 → 1>Area name
2 Area 2 Area 1

Select an area to program.

Area name

4.2.n. **1 Area name**
>Area 1 <

Every area can be programmed with a name to identify the area.

Use the Area name screen to enter or edit the area name. The area name can contain up to 30 characters.

Exit time

4.2.n. 2 Exit time >>> → 1 Exit time 1
infinity

Every area has its own exit timers. Exit timers allow users that set an area, to leave the premises without generating an alarm (using access or entry/exit zones). Only after the exit timers have expired can an alarm occur.

Each area can be programmed with two exit times, one for entry/exit 1 zone type, another one for entry/exit 2 zone. Select an appropriate timer and set the time.

The exit timers can be programmed from 0 to 255 seconds. 0 means the timer is not engaged and the area is set immediately. 255 means the timer remains active and requires an exit terminator (see “Zone type” on page 229) or a zone with the final door option (see “Final door” on page 233) to complete.

Note: If zones are assigned to more than one area, the longest exit time is used. See “Zones and areas” on page 228.

Exit time 1

Exit time 2

Configure exit timers for entry/exit 1 and entry/exit 2 zone types. See “Exit time” above for details on exit timer programming.

Part set exit time 1

Part set exit time 2

Configure part set exit timers for entry/exit 1 and entry/exit 2 zone types.

Part set exit timers are configured the same way as full set exit timers. See “Exit time” above for details on exit timer programming.

Remote exit time

4.2.n.2. 5 Rem exit time > <

The timer is used in case of a remote set initiated by configuration or management software, or a mobile application. Activation of any zone, including entry/exit and access zones, during the remote exit time generates an E/E fault.

If the value is set to 0, the exit time programmed in “Exit time 1” above is used.

Entry time

4.2.n. 3 Entry time >>> → 1 Entry time 1
00'30

Every area has its own entry timer. When entering the premises via an entry/exit zone, the entry time starts. A user can unset the area while the entry time is

running without generating an alarm provided only entry/exit zones or access zones are activated.

Note: The entry time can be extended for certain entry zones. See “Prealarm time” on page 247 for more details.

Each area can be programmed with two entry times, one for entry/exit 1 zone type, another one for entry/exit 2 zone. Select an appropriate timer and set the time.

The entry timers can be programmed from 0 to 255 seconds. 0 means the timer is not engaged and the alarm is activated immediately when entering the armed premises. 255 and more means the time is infinite.

Note: If zones are assigned to more than one area, the longest entry and exit time is used. See “Zones and areas” on page 228.

Entry time 1

Entry time 2

Configure entry timers for entry/exit 1 and entry/exit 2 zone types. See “Entry time” on page 245 for details on entry timer programming.

Part set entry time 1

Part set entry time 2

Configure part set entry timers for entry/exit 1 and entry/exit 2 zone types.

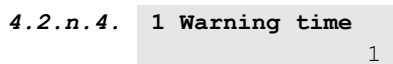
Part set entry timers are configured the same way as full set entry timers. See “Entry time” on page 245 for details on entry timer programming.

Other timers



The menu groups additional area timers. See submenus below for details.

Autoset warning time



Warning time is a period, during which the automatic set procedure can be postponed. After the warning time expires, the system is set.

The set postponing must be allowed in “Autoset retry” on page 247.

The warning timer can be programmed from 1 to 15 minutes.

Prealarm time

4.2.n.4. 2 Prealarm time
00'00

Every area has its own prealarm timer. When an alarm is triggered, it only generates a local alarm, and the prealarm timer is started. If the local alarm is not acknowledged during the prealarm time, the alarm is reported.

Note: The entry zone must have activated option “Extend EE” described on page 233.

Use the PreAlarm time screen to set the prealarm time for the area. Each area can be programmed with one prealarm time.

The prealarm timers can be programmed from 0 to 255 seconds.

Note: If zones are assigned to more than one area, the longest prealarm time is used. See “Zones and areas” on page 228.

Unset delay

4.2.n.4. 3 Unset delay
Off

Set a delay for authorized unset (in minutes). The allowed range is 1 to 30 min. 0 means that no delay is applied. See “Delayed unset” on page 58 for more details.

Set/unset options

4.2.n. 5 Set/unset opts → 1>Entry alarms
>>> Delayed

The menu groups the following setting options.

Entry alarms

4.2.n.5. 1 Entry alarms
Delayed

The Entry alarms option defines whether the entry fail alarm is reported immediately. The following values are applicable:

- Delayed: The alarm activates 30 s after the entry time passed.
- Instant: The alarm activates immediately.

Autoset retry

4.2.n.5. 2 Set retry
Off

Set retry defines whether users can postpone or cancel an autoset. If this option is set to On, you can postpone autoset during the Warning time (see “Autoset warning time” on page 246). If the autoset has been postponed by a normal user, the system will attempt autoset again after a time period defined in “Autoset user retry” on page 310.

Note: The privileged users, Installer and Supervisor, can choose the postpone time during the Warning time.

Autoset silent mode

4.2.n.5. 3 Silent autoset
Off

If Silent autoset is on, the keypad buzzer remains silent during the “Autoset warning time” described on page 246.

Dual unset

4.2.n.5. 4 Dual unset
Off

If the option is set to yes, two valid user authorization is necessary to unset the area.

Note: The users must authorize on the same keypad.

Caution: Before switching this option on, or applying defaults that have this option enabled, add at least one user, otherwise you will lose an access to the programming menu. See also “Recovery procedure” on page 372 in Chapter 7 “Troubleshooting”.

Confirm alarm

4.2.n.5. 5 Confirm alarm
After unset

The option defines when an alarm can be confirmed by a user. The following values are available:

- After unset: An alarm can be confirmed only when the area is unset.
- Without unset: An alarm can be confirmed when the area is set or unset.

See *AXON Control Panel User Manual* for more details on alarm confirmation.

Hierarchy level

4.2.n. 6 Hierarchy
Off

Set a hierarchy for the selected area. The area hierarchy can have value from 1 (highest) to 3 (lowest). Hierarchy 0 means that the functionality is off and this area functions with no restrictions.

See “Area hierarchy” on page 55 for more details.

Limits

4.2.n. 7 Limits >>> → 1>Inhibit limit
128

Limits the number of system elements that can be isolated or inhibited at any one time.

Allowed ranges depend on the panel variant. See “General features” on page 39 in Chapter 2 “Installation”.

See also “Inhibit and isolate” on page 59.

Inhibit limit

4.2.n.7. 1 Inhibit limit
512

The maximum number of system elements that can be inhibited at any one time.

Isolate limit

4.2.n.7. 2 Isolate limit
512

The maximum number of system elements that can be isolated at any one time.

Shunt limit

4.2.n.7. 3 Shunt limit
512

The maximum number of system elements that can be shunted at any one time.

Schedule

4.2.n. 8 Schedule >>>

Select schedules for the selected area.

The shortcut menu allows you to assign up to two schedules to each of the following elements:

- 1 Set
- 2 Shunt
- 3 Prohibit unset
- 4 Chime area

See “Schedule shortcut menu” on page 90 for more information.

Area groups

4. 3 Area groups → 01>AG 1
4 RF Fobs 02 AG 2

Area group menu allows you to assign areas to area groups.

Note: Area group availability depends on the control panel variant. See “Specifications” on page 38 in Chapter 2 “Installation”.

See also “Area groups” on page 55.

Area group options

Select area group

```
4.3.  01>AG 1
      02 AG 2      →  1>Name
                        AG 1
```

Select an area group to program.

Area group name

```
4.3.n.  1 Name
        >AG 1      <
```

Every area group can be programmed with a name to identify the area.

Use the Area group name screen to enter or edit the area group name. The area group name can contain up to 16 characters.

Area group areas

```
4.3.n.  2 Areas
        .....>    →  01-10 Areas
                        .....
```

Assign areas to the selected area group.

RF fobs

```
4.  4 RF fobs
    5 Cameras Menu  →  0>Add fob
                        1 Fob 1
```

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

Fob options

Add fob

```
4.4.  0 Add fob
      1 Fob 1
```

To add a fob, follow one of the procedures described in “Wireless device programming” on page 109.

Select fob

```
4.4.  1 Fob 1
      2 Fob 2      →  1>Fob name
                       Fob 1
```

Select an existing fob to program.

Fob name

```
4.4.n.  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.

Assigned user

```
4.4.n.  2 Assigned user
        User 1      →  1>User 1
                       2 User 2
```

Assign an existing user to the selected fob.

Note: One user can have a few fobs assigned. However, one fob can be assigned only to one user.

Buttons

```
4.4.n.  3 Buttons
        >>>      →  1>Button 1
                       2 Button 2
```

Use the Buttons menu to assign an appropriate function to a button or a button combination.

Note: A user must be assigned in “Assigned user” above for the button combinations to work.

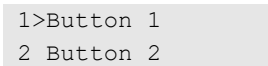
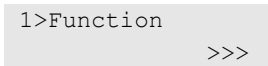
Table 30 below lists buttons and combinations that are available.

Table 30: Fob buttons and combinations

Buttons	Function
Button 1	Set all areas
Button 2	Unset all areas
Button 3	Part set 1 all areas
Button 4	Toggle trigger 99
Buttons 1 + 2	—
Buttons 1 + 3	—
Buttons 1 + 4	—

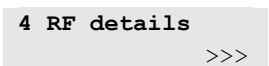
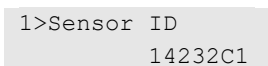
Buttons	Function
Buttons 2 + 3	—
Buttons 2 + 4	—
Buttons 3 + 4	—

Select button

4.4.n.3.  → 

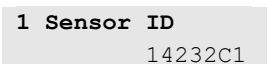
Select a button to assign a user function to it. See “User programmable functions” on page 104 for more details.

RF details

4.4.n.  → 

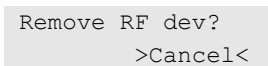
The RF device menu allows you to program a wireless device manually, or remove it from the wireless expander.

Sensor identifier

4.4.n.4. 

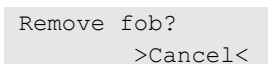
The screen allows you to view the sensor ID.

Remove RF device

4.4.n.4.  → 

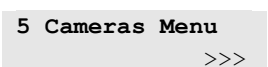
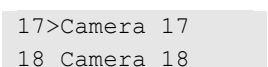
Select Ok and press Enter to remove the wireless device from the wireless expander database.

Remove fob

4.4.n.  → 

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

Cameras

4.  → 

The menu allows you to configure camera modules in wireless PIR cameras. For more details on cameras, see also “Using wireless cameras” on page 116.

Select camera

```
4.5. 17>Camera 17
      18 Camera 18
```

→

```
1>Camera name
   Camera 17
```

Select an appropriate camera to configure.

Camera name

```
4.5.n. 1 Camera name
        >Camera 17  <
```

Enter camera name.

Pictures by zone

```
4.5.n. 2 Pics by zone
        >>>
```

→

```
1>Zone 17
2 Zone 2
```

Choose 1 to 4 zones that can trigger the camera when active.

By default, the first zone assigned is the zone with PIR detector of this wireless PIR camera.

Choose a zone position to assign a zone, or an existing zone to remove it from the associated zone list.

Pictures by filter

```
4.5.n. 3 Pics by filter
        >>>
```

→

```
1>Filter 1
        >>>
```

Additionally to the zones listed in “Pictures by zone” above, there can be up to two condition filters that also trigger the camera.

Select filter

```
4.5.n.3. 1 Filter 1
          >>>
```

→

```
1>Filter 1
   Not used
```

Select one of two filters to configure.

Choose filter

```
4.5.n.3.m. 1 Filter 1
            Not used
```

→

```
00>Not used
01 Internal sire
```

Choose a filter that activates the selected camera.

Event type <n>

```
4.5.n.3.m. 2 Event type 1
            >Burglar<
```

Define a type of the condition filter chosen in “Select filter” above.

The available filter types are listed in “Camera event types” on page 116.

Report as

4.5.n.3.m. 3 Report as
>Not used<

If the filter has a custom type, it is necessary to assign a reporting event, which occurs when the filter becomes active.

Notes

- After you leave this menu, the event is shown as a reporting code in SIA format. See Appendix B “AXON reporting codes” on page 437 for details.
- Only particular reporting events are available.

Pictures by reporting event

4.5.n. 4 Pics by rep ev → 1>Rep. event 1
Not used Not used

The camera can be also triggered by a selected reporting event.

Select event

4.5.n.4. 1 Rep. event 1
>Not used<

Select one of two reporting events to configure.

Choose an event that activates the selected camera.

Notes

- After you leave this menu, the event is shown as a reporting code in SIA format. See Appendix B “AXON reporting codes” on page 437 for details.
- Only particular reporting events are available.

Isolated

4.5.n. 5 Isolated
>No<

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

Max pics 24h

4.5.n. 6 Max pics 24h
>Infinity<

Maximum picture number defines how many pictures can be taken by the camera during 24-hour 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.

Remote pics

```
4.5.n.  7 Remote pics
        >Yes<
```

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

Test picture to CS

```
4.5.n.  8 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.

Doors Menu

```
5 Doors Menu
6 Outs&filters    →    1 Doors
                   2 Door groups
```

Use the menu to add, edit, or delete doors, door groups, and regions of the AXON system.

Doors

```
5. 1 Doors
    2 Door groups    →    0>Add door
                       1 Door 1
```

Use the Door menu to add, edit, or delete doors.

The menu allows you to configure doors of both types, standard and intelligent.

Note: Certain options in this menu are specific for different door types. For specific options, see:

- “Standard door specific options” on page 264
- “Intelligent door specific options” on page 265

Common door options

Add door

```
5.1. 0 Add door
      1 Door 1    →    0>Door
                       1 Panel
```

Access the Add door menu option to add a door.

Choose one of the following locations:

- 0: Door. Add a door providing the system address of this door. If the address is valid, the panel displays the physical door location to confirm.

```
Exp 3.2
      >OK<
```

Select OK to confirm, or Cancel to exit, and then press Enter.

- 1: Panel. Add a standard door providing its number on the control panel.
- 2: DC/LC Exp. Add an intelligent door selecting the door controller, and entering a number of the door on this door controller.

If the door is created successfully, the following message appears:

```
INFO
Door added
```

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

For reader, door zone and lock outputs default addressing, see “Zone, output, and door addressing” on page 34 in Chapter 2 “Installation”.

Select door

Select a door to edit.

The following options can be viewed or configured.

Door name

```
5.1.n.  1 Door name
        >Door 1<
```

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

The default door name is “Door N”, where N is the door number.

The name can have up to 16 characters.

Door location

```
5.1.n.  2 Door location
        Exp 3.2
```

The read-only screen that shows the physical door location of the selected door.

The door location is shown in the same format as zone location. See “Zone location” on page 230.

Door readers

```
5.1.n.  3 Door readers  →  1>IN reader
                          >>> Reader 1
```

The menu allows you to assign entry (IN) and exit (OUT) readers to the selected door.

Note: Standard doors can only have one IN reader and one OUT reader. Additional door readers can be only assigned to an intelligent door. For options related to intelligent doors, see “Intelligent door specific options” on page 265.

The following submenus are available for all doors:

- 1 Reader IN: Select an entry reader
- 2 Reader OUT: Select an exit reader

The following submenus are available only for intelligent doors:

- 3 Reader IN 2: Select an additional entry reader
- 4 Reader OUT 2: Select an additional exit reader

Door output

```
5.1.n.  4 Door output  →  0>Not used
                          Output 17 17 Output 17
```

Select unlock door output.

For intelligent doors, the output must belong to the appropriate door controller outputs range.

You can also select an output that cannot be directly controlled from the AXON system. See “Map relays” on page 313 for details.

You cannot select outputs that are already assigned to Forced door, Warning, DOTL or other output.

It is recommended to use one of first four door controller outputs for door unlock.

Door timers

5.1.n. 5 Door timers >>> → 1>Unlock time >>>

Use the menu to configure various timers for the selected door.

Note: For standard doors, the timer value is set in minutes and seconds in mm:ss format, for example, 01'30.

In case of intelligent doors, use two options placed as submenus:

1. Time: Set the time value from 0 to 127.
2. Resolution: Set units (seconds or minutes) for the time value above.

Unlock time

5.1.n.5. 1 Unlock time >>> → 1>Time 5

Program the amount of time (value and units) for the door to unlock when a user enters a valid card or PIN at the door reader.

Extended time

5.1.n.5. 2 Extended time >>> → 1>Time 10

Program the amount of time (value and units) for the door to unlock when a user, with the “Extended access” option enabled, presents a valid card or PIN at the door reader. See also “Extended access” on page 224.

Door options

5.1.n. 6 Door options >>> → 1>Door zones >>>

The menu contains various options for the selected door.

For options related to intelligent doors, see “Intelligent door specific options” on page 265.

Door zones

5.1.n.6. 1 Door zones >>> → 1>Door zone
Not used

Use the menu to assign required zones to the selected door.

In case of standard door, there can be only one door zone indicating door opening.

Note: It is not possible to assign a zone to a particular door function if this zone is already used for other door function. Only unassigned zones are displayed.

Door zone

5.1.n.6.1. 1 Door zone >>> → 0>Not used
Not used 17 Zone 17

Select a zone with door contact for the selected door.

Alarm control

5.1.n.6. 3 Alarm control >>> → 1>Door areas
1.....>

Set alarm control options for the selected door.

Door areas

5.1.n.6.3. 1 Door areas >>> → 01-10>Door areas
1.....> 1.....

Select door areas.

In case of an intelligent door, the areas specified here are used for:

- The reader LEDs if the option “LEDs option” described on page 266 is selected to show area status.
- “Deny access” when set (described on page 260).
- Option “Disable when Set” on page 269 is set to Yes for IN readers.

Although the areas are *not* used for area control, the door controller *does* need to identify the status of these areas to know whether to send an arm or disarm command to the control panel. This is *only* when using cards by themselves for set/unset, for example, alarm control on 1st or 3rd badge. Remember that the User group determines the areas allowed to be set or unset by a user, not the areas listed here. See also “User groups” on page 71.

See “How to edit a list” on page 137 for details on the area selection.

Note: “View areas” on page 197 and “Control areas” on page 197 are not available for keypads that are configured as door readers.

The option is equal to “Keypad devices > EE PIN lock” on page 199.

RTE options

```
5.1.n.6. 4 RTE options  >>> → 1 Use RTE >>>
```

Configure RTE (Request to exit) functionality options.

Use reader RTE

```
5.1.n.6.4. 1 Use RTE >>> → 1>Reader IN No
```

Specify if the Request to Exit input is enabled on the reader.

First, select the appropriate IN or OUT reader. Next, set Yes or No to configure the option for the specified reader.

For options related to intelligent doors, see “Intelligent door specific options” on page 265.

Schedule options

```
5.1.n. 7 Schedule opts >>> → 1>Door unlocked >>>
```

The menu allows you to configure schedule options for the selected door.

Door unlocked

```
5.1.n.7. 1 Door unlocked >>> → 1>Schedule >>>
```

Configure schedule options for the door unlock.

Schedule

Select schedules for the door unlock.

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

Shunt options

```
5.1.n. 8 Shunt options >>> → 2>Shunt timers >>>
```

Use the menu to set up door shunt options for the door.

See also “Door shunt” on page 80 in Chapter 3 “System functions” for shunt functionality description.

For options specific for standard doors, see “Standard door specific options” on page 264. For options related to intelligent doors, see “Intelligent door specific options” on page 265.

Shunt timers

5.1.n.8. 2 Shunt timers >>> → 1>Shunt time >>>

The menu allows you to configure timers assigned to the door shunt.

The following options are available:

- 1 Time: Set the time value from 0 to 127.
- 2 Resolution: Set units (seconds or minutes) for the time value above.

Shunt time

5.1.n.8.2. 1 Shunt time >>> → 1>Time 60

The amount of time (value and units) for the door zone to be shunted.

Extended time

5.1.n.8.2. 2 Extended time >>> → 1>Time 90

The extended shunt timer, which is applied if the user has extended time option enabled. See “Extended access” on page 224 for details.

Warning time

5.1.n.8.2. 3 Warning time >>> → 1>Time 15

The warning time is the time period of door shunt warning before shunt time (or extended shunt time) expires.

Appropriate warning event flags, which are active during this time, can be used for in user programmable function. See also “User programmable functions” on page 104, “Zone shunt” on page 59.

Shunt type

5.1.n.8. 3 Shunt type >>> → 1>Shunting
Zone shunting

The menu contains parameters that define the effect of the shunt.

For options specific for standard doors, see “Standard door specific options” on page 264.

Shunting

5.1.n.8.3. 1 Shunting
>Zone shunting<

The option defines the object of the shunt. The following options are available:

- No shunting. The door is not shunted.

- Zone shunting. The door is shunted. It generates a standard alarm, based on the zone type settings, if left open longer than the programmed shunt time. See “Shunt time” on page 262.
- Zone shunting & DOTL. The door is shunted and generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time. Enables Forced Door and DOTL to be reported on separate zone numbers as programmed in “Forced door” on page 270 and “DOTL” on page 271.

Note: This option is only available for intelligent doors.

- Auto shunting & DOTL. If the area assigned to the door is unset, shunting of the door commences when the door zone is active (no code or card required). A DOTL (Door Open Too Long) alarm is generated if it is left open longer than the programmed shunt time. Forced Door and DOTL are reported on separate zone numbers as above.

Note: This option is only available for intelligent doors.

Until door close

5.1.n.8. 5 Until door CL
>No<

If set to Yes, the door shunt zones remain shunted as long as the door is opened.

Cancel after close

5.1.n.8. 6 CancelAfterCL
>No<

For security reasons, it may be required to limit the shunt period as much as possible. If the option is set to Yes, the door shunt zones are shunted until the door is closed. Opening the door again within the shunt time is not possible, as this will generate an alarm (there is always a debounce time of approximately 2 seconds).

Move Door

5.1.n. 10 Move Door >>> → 5 Not used
6 Not used

The menu allows you to move the selected door to another physical location. The new location must be unused.

If the door is moved successfully, the following message appears:

INFO
Door moved

Note: The door name is changed only if it set by default, for example, Door 5 becomes Door 17. If the door has a custom name, it does not change.

This option is only available in a flexible numbering scheme. See “Object scheme” on page 320 for details.

See also “Zone, output, and door addressing” on page 34.

Disable door

```
5.1.n. 11 Disable door
                               No → Disable door
                                       Yes
```

The command allows you to disable or enable the selected door.

When a door is disabled, access to this door is denied and no door control commands are allowed.

Delete door

```
5.1.n. 12 Delete door
                               >Cancel<
```

Use the Delete door command to remove the door from the system. To remove the door, select Ok and press Enter. The door is deleted.

Standard door specific options

Shunt active

```
5.1.n.8.3.2. 2 Shunt active
                               >Always<
```

Allows you to choose system status when the door shunt is activated.

- Always: The door shunt activates in every system state.
- Set: The door shunt is active only if the areas with the selected door are set.
- Unset: The door shunt is active only if the areas with the selected door are unset, or set partially.

Indication

```
5.1.n.8. 4 Indication
                               >>> → 1>Door held open
                                       No
```

The menu allows you to configure options for indication of certain access control events.

Door held open

```
5.1.n.8.4. 1 Door held open
                               >No<
```

If the option is set to yes, the keypad emits an intermittent signal when the door is held open longer than the shunt timer (or extended shunt timer) allows it.

EE Shunt

5.1.n.8. 7 EE Shunt
>Off<

If entry/exit shunt is set to E/E 1 or E/E 2, the shunted zone becomes an entry/exit zone, and door shunt starts the entry/exit 1 timer (or entry/exit 2 timer).

Shunt start

5.1.n.8. 8 Shunt start
>Access granted<

The option defines the moment when the door shunt starts.

- Access granted: The door shunt starts when door access is granted.
- Door opened: The door shunt starts after door access is granted and the door opens (the zone activates).

Intelligent door specific options

Readers options

5.1.n.3. 5 Readers opts → 1>Card and PIN
>>> >>>

Use the menu to configure readers of the selected door.

Card and PIN

5.1.n.3.5. 1 Card and PIN → 1>Reader In
>>> No

Specify what method is required to open the door from the selected reader.

- Yes: Unlock the door by presenting a valid card to the reader and entering a PIN on the reader's keypad.
- No: Unlock the door by presenting a valid card to the reader or a valid PIN on the reader's keypad.

The option is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

Two cards

5.1.n.3.5. 2 Two cards → 1>Reader In
>>> No

Defines if two user cards or PINs are required to gain access. If set to yes, two different users need to present their card and/or PIN within the programmed time for the door to unlock.

The time is set in "Two cards time" on page 312.

The option is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

No schedule required

5.1.n.3.5. **3 NoSchedule req** → 1>Reader In
 >>> No

This option extends the exit access for the selected OUT reader.

- Yes: The user has access to the door from the OUT reader side even if his schedule has already expired. But he must have assigned any schedule for the door in his door group — users without schedule do not have access to the door.
- No: Valid schedule is required for the user to exit.

The option is configured separately for each door OUT reader. After selecting the option, choose the appropriate reader, and then set the option value.

Card format

5.1.n.3.5. **4 Card format**
 >Wiegand 27 bit<

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

- Wiegand 27 bit
- 27-bit Tecom ASP
- K 32 bit
- Wiegand 26 bit (ID=16, FC=8)
- Indala ASC 27 bit
- Indala ASC 26 bit
- Wiegand 32 bit
- C 36 bit
- ATS Wiegand 23 bit
- Mag swipe - Aritech format
- Mag swipe - Midas format

LEDs option

5.1.n.3.5. **5 LEDs option**
 >Door locked<

Specifies the status that the reader LEDs indicate (only applicable for door controller readers connected to Wiegand interface).

- Door locked. LED 1 is on when the door is locked.
- Door unlocked. LED 1 is on when the door is unlocked.
- Area set. LED 1 indicates if the area assigned to the door is set. If more than one area is assigned, all areas assigned to the door must be set before LED changes state.
- Area unset. LED 1 indicates if the area assigned to the door is unset. If more than one area is assigned, all areas assigned to the door must be unset before LED changes state.

- Area set/unset. Readers with dual LED control indicate the area unset and set with different LED colours.
- Valid/Void. Readers with dual LED control indicate User Valid or Void using different LED colours.
- LEDs disabled. No LED control.

Note: On readers with dual LED control, LED 2 may also be programmed to indicate other conditions using door controller macro logic programming. See “Door controller macro logic” on page 81.

See also “Door areas” on page 259.

Time and Attendance

5.1.n.3.5. **6 Time&Attendance**
>No<

If set to Yes, the reader function as a time and attendance reader. It causes that user access events occurring on this reader are sent from the door controller to the control panel and may be used for user attendance control.

Disable Duress

5.1.n.3.5. **7 Disable Duress**
>No<

This option is used to disable duress codes from functioning. If set to Yes, no duress function is available at this door.

Second zone

5.1.n.6.1. **2 Second zone** → 0>No
No 17 Zone 17

The door controller allows the system to monitor two door contacts for a single intelligent door. Select a second zone with door contact for the selected door. If there is only one door contact, select No.

See also “Door zone” on page 259.

DOTL zone

5.1.n.6.1. **3 DOTL zone** → 0>Not used
Not used 17 Zone 17

Specify the zone that reports the DOTL (door open to long) alarm condition for the selected door.

Note: DOTL reporting must be enabled in Shunt options. See “DOTL” on page 271.

Door unlocked

```
5.1.n.6. 2 Door unlocked  >>>  →  1>Until closed
                                         No
```

The menu contains various options for the selected door unlocking process.

Door unlocked until closed

```
5.1.n.6.2. 1 Until closed
                        >No<
```

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

- Yes: The door lock will not re-lock until the door is closed. This is used where the lock mechanism, when locked, will stop the door closing.
- No: The door lock will re-lock (after the unlock time has expired, etc.) regardless of the door being open or closed.

Until opened

```
5.1.n.6.2. 2 Until opened
                        >No<
```

For security reasons, it is possible for the door to re-lock at the moment it opens. The door stays unlocked until opened, and the door relay is deactivated after the door opens.

The door remains unlocked as long as the unlock time is counting, or the door stays closed, whichever is longer. See also “Unlock time” on page 258.

Pulsed Lock and Unlock

```
5.1.n.6.2. 3 Pulsed L&UnL
                        >No<
```

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

The functionality is described in details in Chapter 3 “System functions > Pulsed lock and unlock” on page 83.

User group

```
5.1.n.6.3. 5 User group  >>>  →  1>Installer grp
                                         2 Supervisor grp
```

Select a user group for the selected door.

See “User groups” on page 71 for details.

Control type

5.1.n.6.3. **6 Control type**
>No control<

Specify what type of alarm control is available for the selected door.

- No control: Reader has no alarm control. It is not possible to set or unset areas using the readers.
- On 1st badge: Presentation of a valid card at a door reader will unset the areas in the user group on first badge. Reading three times will set the areas.
- On 3rd badge: Presentations of a valid card three times sets or unsets the areas in the user group.
- Always: Presentation of a valid card at the IN reader unsets the areas in the user group. Presentation of a valid card at the OUT reader arms the areas in the user group.

If PIN sets

5.1.n.6.3. **7 If PIN sets** >>> → 1>Deny access
No

Configure the door operation if the area is set using PIN.

Deny access

5.1.n.6.3.7. **1 Deny access**
No

If set to Yes, the access to the door is denied if the areas were set using PIN.

RTE zone

5.1.n.6.4. **2 RTE zone** Not used → 0>Not used
19 Zone 19

Select a zone operating as an RTE input for an intelligent door.

Note: It is not possible to choose a zone, which is already used in the door controller (for example, DOTL or door zone, etc.)

See also “RTE options” on page 261.

Disable when Set

5.1.n.6.4. **3 Dis. when set** >>> → 1>IN reader
2 OUT reader

Specify if the RTE functionality is disabled if any of door areas are set.

First, select the appropriate IN or OUT reader. Next, set Yes or No to configure the option for the specified reader.

RTE Control

5.1.n.6.4. **4 RTE Control**
>Timed door OP<

Defines the operation of the Request to Exit button.

- Timed door open. When the RTE button is pressed, the door unlocks for the programmed unlock time. See “Unlock time” on page 258.
- Hold door open. Allows the door to be held unlocked for as long as the RTE button is pressed or for the programmed unlock time, whichever is longer.
- Shunt only. When the RTE button is pressed, the zone is shunted, but no access is granted.

Reporting

5.1.n.6. **5 Reporting** >>> → 1>CL & Locked
No

Determines when access control events are reported.

Closed and Locked

5.1.n.6.5. **1 CL & Locked**
>No<

If set to yes, the door is reported when closed and locked (lock command sent, and zone status is normal).

Note: There is no event specified in the control panel. This function can only be used in conjunction with next options.

Report Open/Unlocked as Unlocked

5.1.n.6.5. **2 OP&Unl as Unl**
>No<

If set to yes, the door is reported as unlocked, if it is open and unlocked.

Open/Close

5.1.n.6.5. **3 Open/Close**
>No<

If set to yes, opening or closing door is reported. Otherwise, there is no reporting unless an alarm occurs (depending on the zone type).

Forced door

5.1.n.6.5. **4 Forced door**
>No<

If set to Yes, opening of the door without a valid card, PIN or Request to Exit is reported.

DOTL

5.1.n.6.5. 5 DOTL >No<

Report when the door is open too long. If set to Yes and the zone assigned to the door is in the DOTL state (for example, still open after the shunt timer expires), the DOTL event is reported.

RTE

5.1.n.6.5. 6 RTE >No<

If set to Yes, Request to Exit zone activation is reported.

Interlocking

5.1.n.6. 6 Interlocking
1234567890123456

This menu stipulates the zone numbers on the door controller that prevents the doors being accessed at the same time. Numbers must be zone numbers on the same door controller.

To interlock with a door on another door controller, a contact from that door must be wired to a spare zone on the first door controller, and vice versa. In this case, if a zone is being used for interlocking and no door on the door controller has that zone as its “Door Contact”, then the door controller automatically inserts a 2 second delay before a door opens. This is to allow for settling times across the door controllers. Please remember that this two-second delay only occurs when a zone is being used for interlocking, and that zone comes from another door not on this door controller.

To activate or deactivate interlocking, toggle a local zone number.

After entry

5.1.n.7.1. 2 After entry >No<

Select if the override takes effect immediately the schedule commences, or after a user has entered.

- Yes: Before the schedule will unlock the door, a user needs to enter the area.
- No: Automatic unlock starts at the schedule start time.

See also “Door unlocked” on page 261.

Low Security

5.1.n.7. **2 Low Security** >>> → 1>LS Schedule
Not used

Use the menu to configure Low Security functionality of the door. The door low security mode means that the user authorization is changed from Card *and* PIN to Card *or* PIN.

The following submenus are available:

- 1 LS Schedule (Low Security Schedule). Select schedules for low security functionality.

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

- 2 RdrIn Inh PIN (IN reader inhibit PIN if timezone). If set to yes, the IN reader is in the low security mode if the above schedule is active.
- 3 RdrOut Inh PIN (OUT reader inhibit PIN if timezone), etc.

The functionality is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

RTE Schedule

5.1.n.7. **3 RTE Schedule**
Not used

Select schedules for Request to Exit input.

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

Zones

5.1.n.8. **1 Zones**
1234567890123456

Select zones that must be shunted on the door opening.

To activate or deactivate shunting, toggle a local zone number.

See also “Shunt options” on page 261.

Indication

5.1.n.8. **4 Indication** >>> → 2>DOTL output
Not used

The menu allows you to assign door controller outputs for indication of the specific access control events.

DOTL output

5.1.n.8.4.	2 DOTL output Not used	→	00>Not used 19 Output 17
------------	---------------------------	---	-----------------------------

Select an output on the door controller to indicate the Door Open Too Long alarm.

Warning output

5.1.n.8.4. 3 Warning output → 00>Not used
Not used 19 Output 17

Select an output on the door controller to indicate the warning before the shunt time or extended shunt time expires. See also “Shunt timers” on page 262.

Forced door

5.1.n.8.4.	4 Forced door Not used	→	00>Not used 19 Output 17
------------	---------------------------	---	-----------------------------

Select an output on the door controller to indicate that the door is forced (opened without a successful authorization).

Regions & AP

```
5.1.n. 9 Regions & AP      → 1>Regions
                                     >>>                                     >>>
```

The menu contains door options connected to region control and anti-passback.

Regions

5.1.n.9. 1 Regions → 1>Reader In

Use the menu to assign regions to readers.

First, select the appropriate reader. Next, choose a region the reader belongs to.

```
0>Add region
1 Outside
```

The list of regions allows you to add a new region. The add region menu is equal to the menu in “Region” described on page 276.

See Chapter 3 “System functions > Regions” on page 80 for details.

Anti-passback

5.1.n.9. 2 Anti-passback
>No AP<

Controls the operation of the door if a card or PIN is used to attempt to enter the region that the user is currently assigned to. The following options are available:

- No AP: No control of passback.

- Soft anti-passback: A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
- Hard anti-passback. A valid card or PIN *does not* open the door when used to enter the region a second time without leaving first. An attempt to do so generates a report.
- Regions anti-passback. A valid card or PIN *does not* open the door when used to leave a region other than the one entered previously. For example, if the user had entered region 2 from region 1, he will be denied when trying to enter region 1 from region 0. An attempt to do so generates a report.

See Chapter 3 “System functions > Anti-passback” on page 81 for details.

Inhibit Region 1 User

```
5.1.n.9. 3 Inh Reg 1 Ustr    → 1>Reader In
          >>>                >>>
```

For users in region 1 (on most occasions is “outside”), a special security feature is available to provide access only via another region. If the option is set to yes, any user in region 1 will be denied access. To access, the user first has to be in another region.

The functionality is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

High Security User options

```
5.1.n.9. 4 HSU options      → 1>Req HSU Nr
          >>>                0
```

The menu contains high security options.

See Chapter 3 “System functions > High security” on page 81 for details.

Required HSU Number

```
5.1.n.9.4. 1 Req HSU Nr
            >0<
```

The value defines how many High Security Users (HSU) must be present in the region assigned to the selected door.

Prewarning time

```
5.1.n.9.4. 2 Prewarn. time
            > <
```

The value defines time (in seconds) for the prewarning timer to run. When there are too few high security users in a high security region, a prewarning timer starts, and when it expires, an alarm is raised and the alarm output activates.

HS Alarm output

5.1.n.9.4.	3 HS Alarm out Not used	→	00>Not used 19 Output 17
------------	----------------------------	---	-----------------------------

Select an output on the door controller to indicate an anti-passback or high-security alarm.

Door groups

5. **2 Door groups** → 0>Add Door Gr
3 Region 1 Door Gr 1

Door groups define when a user can have access to specific doors.

See Chapter 3 “System functions > Door groups” on page 80 for details.

Add Door Gr

```
5.2. 0 Add Door Gr
    1 Door Gr 1
```

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

INFO
Door Gr added

The new door group is given the default name “Door Gr N” and placed on the end of the door list.

Select door group

```
5.2. 2 Door Gr 2
      3 Door Gr 3
```

→

```
1>Door Gr name
      Door Gr 2
```

Select a door group to program.

Door Group name

```
5.2.n. 1 Door Gr name
>Door Gr 2    <
```

Every door group can be programmed with a name to identify it.

Use the Door Gr name screen to enter or change the door group name. The name can contain up to 16 characters.

Door Group Doors

```
5.2.n. 2 Door Gr Doors    → 0>Add door
      >>>                -----
```

Program the user access for the selected door group.

To configure a door group:

1. Add a door to the group if necessary. The default schedule (Always) is automatically assigned to every added door.
2. Select a door, to which a user with the assigned door group can have an access.
3. Assign up to two schedules that define, when users with this door group have access to this door.

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

4. Repeat for all doors specific for this door group.

Delete Door Group

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

The display shows:

```
5.2.n.  3 Delete Door Gr
        >Cancel<
```

Choose Ok and press Enter. This deletes the door group.

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

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

Region

```
5.  3 Region
    4 Floors      →  0>Add region
                    1 Outside
```

Configure regions.

See Chapter 3 “System functions > Regions” on page 80 for more information.

Add region

```
5.3.  0 Add region
      1 Outside
```

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

```
INFO
Region added
```

The first region is given the name “Outside”, while subsequent regions are named “Region 2”, “Region 3”, etc.

Select region

```
5.3.  2>Region 2
      3 Region 3      →  1>Region name
                        Region 2
```

Select a region to program.

Region name

```
5.3.n.  1 Region name
        >Region 2  <
```

Every region, except region 1 “Outside”, can be programmed with a name to identify it.

Use the Region name screen to enter or change the region name. The name can contain up to 16 characters.

Delete region

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

The display shows:

```
5.3.n.  2 Delete region
        >Cancel<
```

Choose Ok and press Enter. This deletes the region.

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

Note: You cannot delete region 1.

Floors

```
5.    4 Floors
      5 Floor groups      →  0>Add floor
                           1 Floor 1
```

Use the Floor menu to add, edit, or delete floors.

Add floor

```
5.4.  0 Add floor
      1 Floor 1
```

Access the Add floor menu option to add a floor.

If the floor is created successfully, the following message appears:

```
INFO
Floor added
```

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

Select floor

```
5.4.  1 Floor 1
      2 Floor 2
```

Select a floor to edit.

The following options can be viewed or configured.

Floor name

```
5.4.n. 1 Floor name
        >Floor 1<
```

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

The default floor name is “Floor N”, where N is the floor number.

The name can have up to 30 characters.

Delete floor

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

The display shows:

```
5.4.n. 2 Delete floor
        >Cancel<
```

Choose Ok and press Enter. This deletes the floor.

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

Floor groups

```
5.  5 Floor groups
-----  →  0>Add Floor Gr
              1 Floor Gr 1
```

Floor groups define when a user can have access to specific floors.

See Chapter 3 “System functions > Floor groups” on page 80 for details.

Add Floor Group

```
5.5.  0 Add Floor Gr
      1 Floor Gr 1
```

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

```
INFO
Floor Gr added
```

The new floor group is given the default name “Floor Gr N” and placed on the end of the floor list.

Select floor group

```
5.5.  2 Floor Gr 2
      3 Floor Gr 3      →  1>Floor Gr name
                           Floor Gr 2
```

Select a floor group to program.

Floor Group name

```
5.5.n.  1 Floor Gr name
        >Floor Gr 2  <
```

Every floor group can be programmed with a name to identify it.

Use the Floor Gr name screen to enter or change the floor group name.

The name can contain up to 30 characters.

Floor Group Floors

```
5.5.n.  2 Floor Gr Fls      →  0>Add floor
                                1 Floor 1
                                >>>
```

Program the user access for the selected floor group.

To configure a floor group:

1. Add a floor to the group if necessary. The default schedule (Always) is automatically assigned to every added floor.
2. Select a floor, to which a user with the assigned floor group can have an access.
3. Assign a schedule that defines when users with this floor group have access to this floor.

See “Schedule shortcut menu” on page 90 for more information.

4. Repeat for all floors specific for this floor group.

Delete Floor Group

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

The display shows:

```
5.5.n.  3 Delete Fl Gr
        >Cancel<
```

Choose Ok and press Enter. This deletes the floor group.

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

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

Outputs and filters

```
6 Outs&filters      → 1>Cond filters
7 Calendar          2 Outputs
```

In this programming section outputs, filters and triggers, and their options are programmed. Outputs on panel or expander as well as system triggers can be activated.

Condition filters

```
6. 1 Cond filters    → 0>Add filter
   2 Outputs          1 External Siren
```

A condition filter is an evaluation and a decision-making algorithm. There are 64 pre-programmed filters.

Filter settings

Add filter

```
6.1. 0 Add filter
      1 External Siren
```

Access the Add filter menu option to add a condition filter. If the filter is created successfully, the following message appears:

```
INFO
Filter added
```

The new filter is given the default name “Filter N” and placed on the end of the condition filter list. You can now start editing its details.

Select filter

Select an existing filter to program.

Filter name

```
6.1.n. 1 Filter name
        >Filter 52  <
```

The name identifies the filter for installer, making the programming dependencies clearer.

Formula

```
6.1.n. 2 Formula      → 0>Add event
                        >>> -----
```

The Formula menu allows definition of the filter formula. Up to 4 events can be combined in a formula.

Add event

6.1.n.2. 0 Add event
1 System.0.1

Use the Add event command to add an operand to the current formula. Press Add event to add the operand.

This menu entry is not available if the formula already contains 4 events.

The next steps depend on whether you select an event or an operator for the formula.

Select event

6.1.n.2.x. 1>Group
System

Select the appropriate event to configure it.

To choose an appropriate event, you must define the source of the event first. The source is defined by a group of objects, and an object within this group. Available groups are listed in Appendix A “AXON events” on page 421.

When the group and the object (if available) are selected, select the appropriate event. The available selection depends on the selected source. The full event list with sources is shown in Appendix A “AXON events” on page 421.

The following functions are available for the selected event:

1. Group: Select group
2. Element: Select an element (or all elements) from the group above
3. Event: Select an event for the element above
4. Invert: Invert the selected event. If inverted, it is marked with '!' in the formula
5. Remove event: Remove the selected event

Select operator

6.1.n.2.y. 1>Operator
OR

All events are joined with logical operators. Choose the operator to change it. Valid operators are AND, OR, and XOR.

Invert

6.1.n. 3 Invert
>No<

The Invert option specifies if the condition filter output is inverted.

Delete filter

6.1.n. **4 Delete filter**
>Cancel<

Use the screen to remove a condition filter from the system. To remove the filter, select OK and press Enter again. The filter is deleted.

Outputs

6. **2 Outputs**
3 Triggers → 0>Add output
1 Int. Siren

The Outputs menu lets you to see all programmed outputs, select an existing output, or create a new one.

Output settings

Add output

6.2. **0 Add output**
1 Ext. siren → 1>Panel
2 Output exp

When adding a new output, use the Add output menu to select whether the output is located on the panel PCB, output expander, remote expander, or keypad.

See “Zone, output, and door addressing” on page 34 for available output addresses.

If the chosen output already exists, a warning is displayed.

If the output is created successfully, you are moved to the menu “Output name”.

Select output

Select an appropriate existing output to program. There are 200 programmable outputs in the system.

Output name

6.2.n. **1 Output name**
>Output Pl.6 <

Use the Output name screen to create or edit the output name. The name identifies the output to the end-user when an output is activated.

When an output is created, it is given the default name “Output Xy.z”, where <X> defines a device type, <y> is the device number, and <z> is a device output number. Device type <X> can be one of the following:

- P: panel
- O: output expansion module
- R: Keypad
- E: Expander

For example, default output name “Output E3.7” is given to the output assigned to physical output 7 on Expander 3.

Output location

6.2.n. 2 Output loc
Panel 1.6

The Output location is a read-only field that is a physical identification of the output in a format “<device> <y>.<z>”, where <device> can be a panel, an expander, or a keypad, <y> is the device number, and <z> is a device output number.

Invert output

6.2.n. 3 Invert output
>No<

The Invert output option determines if the output is inverted.

Start filter

6.2.n. 4 Start filter
Ext. siren → 00>Not used
01 Internal Sire

Use the Start filter menu to specify a condition filter that activates the output. The output behaviour depends on the output activation mode, described in “Mode” below.

Stop filter

6.2.n. 5 Stop filter
Not used → 00>Not used
01 Internal Sire

Use the Stop filter menu to specify an optional condition filter that deactivates the output.

Mode

6.2.n. 6 Mode
Follow

The following modes are available:

- Follow: The output state is equal to the start condition filter state, unless the stop conditional filter becomes valid.

The start of the output activation depends on the delay programmed in “Delay time” on page 285.

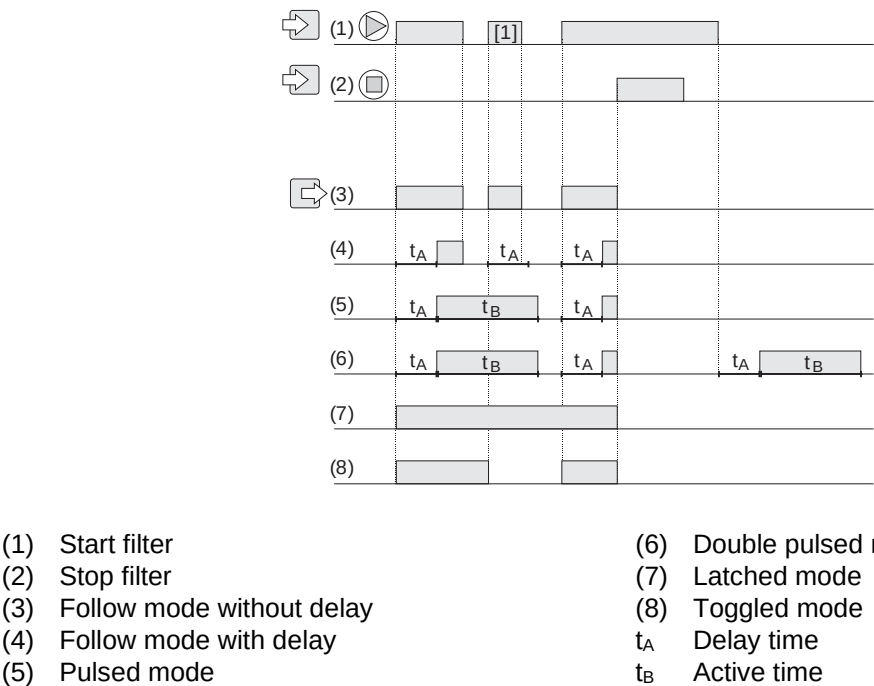
If the delay is programmed to 0, the output activates immediately. Otherwise, the output activates only after the start condition filter has been active for the time programmed.

When the stop condition filter activates, the output immediately becomes passive.

- Pulsed: Switching the start condition filter on causes starting the delay timer set in “Delay time” on page 285. After the time passes, the output activates for a time defined in “Active time” on page 285, and then it switches off.
If the stop condition filter is set, its activation deactivates the output and resets both described timers.
- Double pulsed: Similar to the previous one, except the delay timer is activated by any change of the start condition filter, activation and deactivation.
- Latched: A single activation of the start condition filter switches the output on. The output can be then deactivated only by activating the stop condition filter.
If the stop condition filter is not set, the output will always remain active.
- Toggled: A single activation of the start condition filter switches the output state to the opposite.

Figure 21 below shows examples of described output activation modes.

Figure 21: Output activation mode examples



Note: Full active time t_B is equal to the programmed delay if the option Retriggerable is set to No. Otherwise, the timer is restarted when start filter goes active [1] and the active time is prolonged. See “Retriggerable” on page 285 for more details.

Parameters

6.2.n. 7 Parameters >>> → 1>Delay time 00:00'00

Set the appropriate parameters for the functions described above.

Delay time

6.2.n.7. 1 Delay time
>00:00'00<

Delay time defines the time between an activation of the condition and switching the output on. Allowed range is 00:00'00 to 12:00'00. 00:00'00 means that the output is activated with no delay.

Active time

6.2.n.7. 2 Active time
>00:00'01<

Active time defines the time of an activation of the output. Allowed range is 00:00'01 to 12:00'00.

This option is available only if Pulsed or Double pulsed mode is selected in "Mode" on page 283.

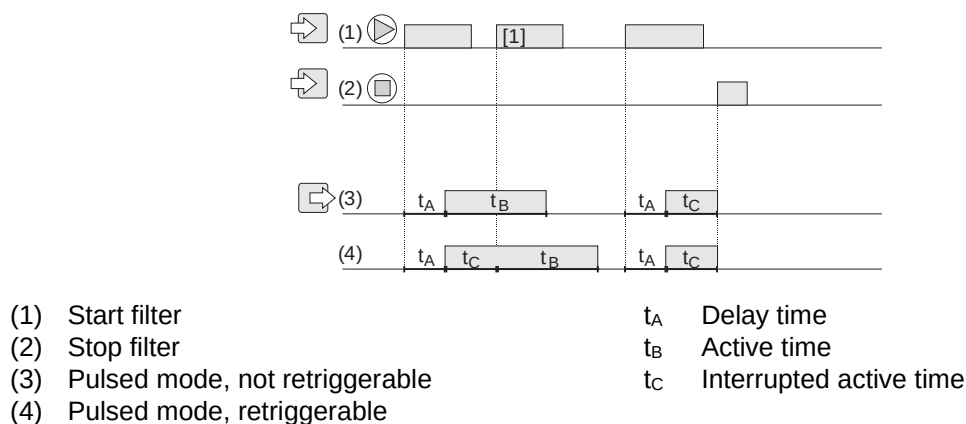
Retriggerable

6.2.n.7. 3 Retriggerable
>No<

Note: The Retriggerable option is only valid for Pulsed and Double pulsed outputs.

If this option is set to Yes, the active timer is restarted when the starting condition becomes valid again during the active state, so the active time is prolonged. Figure 22 below shows the output retriggering when the start filter is reactivated [1].

Figure 22: Output examples



Log limit

6.2.n. 8 Log limit
>Enable<

If the Log limit option is set to Enable, only 3 pairs of activating (opening) and restoring (or closing) events coming from a single output are recorded in the log during one set/unset cycle.

Delete output

```
6.2.n.  9 Delete output
        >Cancel<
```

Use the Delete output screen to remove an output from the system. To remove the output, select OK and press Enter again. The output is deleted.

Triggers

```
6.  3 Triggers
-----  →  0>Add trigger
              1 Trigger 1
```

The menu allows you to configure system triggers.

Trigger settings

Add trigger

```
6.3.  0 Add trigger
        1 Trigger 1
```

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

```
INFO
Trigger added
```

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

Select trigger

```
6.3.  1 Trigger 1
        2 Trigger 2  →  1>Name
                        Trigger 1
```

Select a trigger to program.

Trigger name

```
6.3.n.  1 Trigger name
        >Trigger 1  <
```

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

Use the Trigger name screen to enter or change the trigger name. The trigger name can contain up to 16 characters.

Schedule

```
6.3.n.  2 Schedule
        >>>  →  1>Sel schedule 1
                  Not used
```

Select schedules for the trigger.

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 90 for more information.

User group

```
6.3.n.  3 User group
        Not used    →  00>Not used
                       01 Installer grp
```

Select a user group for the selected trigger.

See “User groups” on page 71 for details.

Delete trigger

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

The display shows:

```
6.3.n.  4 Delete trigger
        >Cancel<
```

Choose Ok and press Enter. This deletes the trigger.

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

Calendar

```
7 Calendar → 1>View
8 Sys.opts Menu >>>
```

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 schedules.

See “Calendar” on page 89 in Chapter 3 “System functions” the detailed functionality description.

View

```
7. 1 View → 1>10-03-2023
>>> 2 11-03-2023
```

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.

Select date

```
7.1. 1>10-03-2023 → 1>Auto Set
2 11-03-2023 >>>
```

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

Auto setting

```
7.1.n. 1 Auto Set → 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.

By object

```
7.1.n. 2 By object → 0>All
>>> 1 Area
```

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

Select object name or type. The available objects are described in “User programmable functions” on page 104.

Special day

7.1.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 Chapter 3 “System functions > Special days in schedules” on page 90.

Day type

7.1.n.3. 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 “Special days” on page 293.

Recurring

7.1.n.3. 2 Recurring
>Yes<

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

Until date

7.1.n.3. 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

7. 2 Schedules >>> → 0>Add Schedule
1 Always

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

The maximum schedule number in the system is given in “General features” on page 39.

For more information on schedules see “Schedules” on page 89 in Chapter 3 “System functions”.

Schedule settings

Add schedule

```
7.2. 0 Add Schedule
      1 Always
```

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.

Select schedule

```
7.2. 1 Schedule 1
      2 Schedule 2 → 1>Name
                        Schedule 1
```

Select a schedule to program.

Schedule name

```
7.2.n. 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.

Schedule activation

```
7.2.n. 2 Active
        >No<
```

If set to Yes, the schedule is currently active.

Schedule Date

```
7.2.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.

Time

```
7.2.n. 4 Time
        >>> → 0>Add time frame
                1 Time frame 1
```

Define time frames when the schedule activates.

Add time frame

```
7.2.n.4.  0 Add time frame
          1 Time frame 1
```

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

```
INFO
TimeFr 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.

Select time frame

```
7.2.n.4.  1 Time frame 1
          2 Time frame 2    →  1>Start time
                               00:00
```

Select a time frame to program.

Start time

```
7.2.n.4.m. 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.

End time

```
7.2.n.4.m. 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 Chapter 3 “System functions > Counteractions” on page 90 for more information.

Week days

```
7.2.n.4.m. 3 Week days
              >M.WT...<
```

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

If no week day 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 Chapter 3 “System functions > Schedules” on page 89.

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:

```
7.2.n.4.m.  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.

Action list

```
7.2.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.

The maximum action number for each schedule is given in “General features” on page 39.

Add action

```
7.2.n.5.  0 Add Action
          1 Action 1
```

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.

Select action

```
7.2.n.5.  1 Action 1  →  1>Name
          2 Action 2      Action 1
```

Select an action to program.

Action name

```
7.2.n.5.m.  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.

Object type

Function

Parameters

Available functions and parameters are described in “User programmable functions” on page 104.

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:

```
7.2.n.5.m.  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.

Special days

```
7.2.n.      6 Special days
              >>> → 0>Add sp day
                   1 Holiday
```

Configure special days associated with this schedule.

The maximum number of special days for each schedule is given in “General features” on page 39.

Add special day

```
7.2.n.6.    0 Add sp day
              1 Holiday
```

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.

Select special day

```
7.2.n.6.    1 Holiday 1
              2 Holiday 2
              → 1>Name
                  Holiday
```

Select a special day to program.

Special day name

```
7.2.n.6.m. 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.

Start time

```
7.2.n.6.m. 2 Start time
             >00:00<
```

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

End time

```
7.2.n.6.m. 3 End time
             >00:00<
```

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

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:

```
7.2.n.6.m. 4 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.

Filter

```
7.2.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.

See “Condition filters” on page 280 for more details.

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:

7.2.n. 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.

System options

```
8 Sys.opts Menu    → 1>Timer menu
>>>                2 Engineer opt
```

Use the System menu to program the global system options including timers.

Timer menu

```
8. 1 Timer menu    → 1>Time&date
   2 Engineer opt   2 Siren options
```

Use the Timer menu to program all system wide timers in this section.

Notes

- Timers are accurate to ± 1 of the value entered. So a timer set for 20 seconds, ends somewhere between 19 and 21 seconds. Consequently, avoid using values of 1 second or 1 minute.
- If a timer is set to 0, that timer is not used.

Time and date

```
8.1. 1 Time&date    → 1>Time zone
     2 Siren options  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.

- 1 Time zone. The system time zone.
- 2 Date. Date format is DD-MM-YYYY.
- 3 Time. Time format is 24 hours.
- 4 DST start mth. The DST start month.
- 5 DST start wk. The DST start week. The available options are: 1st week, 2nd week, 3rd week, 4th week, last week.
- 6 DST end mth. See above.
- 7 DST end wk. See above.
- 8 Set correction. Allows configuring time correction if necessary.

- 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 90 for information on daylight saving time change on programmed actions.

Siren options

```
8.1.  2 Siren options    → 1>Activation
      3 Syst Misc opts   2 Delay
```

The Siren options menu allows you to set timers applicable to internal and external sirens.

Select whether you want to change activation time or siren delay.

Activation

```
8.1.2. 1 Activation      → 1>Internal siren
      2 Delay              00:03'00
```

The Activation menu allows you to set the activation time both for internal and external siren.

Internal siren

External siren

Enter the activation time for the internal / external siren. The input format is hh:mm:ss. The allowed range is from 00:00'00 to 06:00'00. The value 00:00'00 means that the siren does not activate. The value 06:00'00 is equal to infinite time (the siren is active until unset or reset).

F/P/M internal

F/P/M external

Enter the activation time for the internal / external siren in case of fire, panic, and medical alarms. The input format is hh:mm:ss. The allowed range is from 00:00'00 to 06:00'00. The value 00:00'00 means that the siren does not activate. The value 06:00'00 is equal to infinite time (the siren is active until unset or reset).

Delay

```
8.1.2. 2 Delay          → 1>Internal siren
      -----           00:00'00
```

The Delay menu allows you to set the delay time before an internal or external siren is activated.

Internal siren

External siren

Enter the delay time for the internal / external siren. The input format is hh:mm:ss. The allowed range is from 00:00'00 to 06:00'00.

Caution: In an unset condition the internal siren delay is ignored, and the siren activates instantly.

System misc opts

```
8.1. 3 Syst Misc opts → 1 Armed display
      4 Zn timers menu    >00'00<
```

The System misc options menu allows you to set up all system programmable timers.

Armed display

```
8.1.3. 1 Armed display
        >00'00<
```

The Armed display delay is a delay before the armed display is activated on the keypad LCD when it enters the idle state. The input format is mm:ss. The allowed range is from 00'00 to 10'00.

Card and PIN

```
8.1.3. 2 Card&PIN
        >00'10<
```

The Card and PIN menu lets you set the maximum delay time between presenting the card and entering the PIN (default is 10 seconds). The input format is mm:ss. The allowed range is from 00'00 to 05'00.

Walk test time

```
8.1.3. 3 Walk test time
        00'00
```

The Walk test time menu option defines the maximum time for the walk test (0 to 30 minutes). A value of 00'00 means no limitation, in this case the walk test is ended only by the user, or when completed successfully. For more information, see “Walk test menu” on page 179.

Mains reporting delay

```
8.1.3. 4 Mains rep dly
        >00:00'00<
```

The Mains reporting delay option defines the delay time (0 to 4 hours) before a mains fail is reported to the central station. Enter a value of “0” for immediate reporting.

Final set delay

```
8.1.3. 5 Final set dly
        > <
```

The Final set delay option defines the delay time between the completion of an area being set by an exit terminator or final door set and the area being armed.

The period allows for devices connected to inputs to return to normal state. The allowed range is 0 to 255 seconds.

Inst in-time

8.1.3. 6 Inst in-time
>00:01'00<

The Installer in-time menu allows you to configure the time in which an engineer is allowed to access when granted by a user (see “User code required” on page 301). This time starts when the user activates the option “Installer in”. During this time the installer can enter the installer menu and set or unset the system.

Note: Any system set or unset will cancel the installer in time.

When the installer is in the installer menu, this time has no effect on how long the installer can stay logged.

The allowed range is 00 h 01 min to 11 h 59 min. A value of 12 h 00 min is equivalent to infinite access.

Zone timer menu

8.1. 4 Zn timers menu → 1>DblKnock int
----- 10'00

The Zone timer menu allows you to set up all programmable zone timers.

Double knock interval

8.1.4. 1 DblKnock int
>00'00<

If enabled for a particular zone, Double knock interval specifies the maximum permitted time between two pulses that will register an alarm. If this value is set to 0, an alarm condition is not determined by the interval between two pulses, but determined solely by Double knock open time. The allowed range is 0 to 15 minutes.

Double knock open

8.1.4. 2 DblKnock open
>01'00<

If enabled for a particular zone, Double knock open specifies the time for which the zone may remain active. If the zone remains active after this time exceeded, an alarm is generated without waiting for a second activation.

The input format is mm'ss. The allowed range is from 00'00 to 15'00.

Soak test

8.1.4. 3 Soak test 14

The Soak test option defines the number of days the soak test for a zone is active. The allowed range is 0 to 30 days.

Soak test is activated as soon as the zone option Soak test (see “Soak test” on page 232) for a zone has been set to Yes. During the soak test period the zone does not trigger alarms.

Input delay

8.1.4. 4 Input delay 0

The Input delay value represents the delay between an input and appropriate zone activation. The allowed range is 0 to 255 seconds.

Key box time

8.1.4. 5 Key box time 1

The Key box time extends the exit time. Immediately after the exit timer expires, the key box timer starts for duration of the defined time. Before this timer expires, the zone must be closed. If it is not closed, a full alarm is triggered again even if the previous trigger was also an alarm. During operation of the exit timer and key box timer, openings and closings are not registered and do not cause an alarm.

The allowed range is 0 to 99 minutes.

Held open time

8.1.4. 6 Held open time >00:00'00<

The options define the period of held open, after which the zone raises “open too long” flag, which can be used for filter programming.

See “Zone held open” on page 237.

Inactive days

8.1.4. 7 Inactive days 0

If a zone is inactive for longer than a time programmed in this menu (in days), an appropriate inactive days event is activated for zone.

Allowed range is 0 to 127, 0 disables the timer for the zone.

Zone inactive day timers can be viewed and reset using “Inactive time” menu described on page 173.

Engineer options

8. 2 Engineer opt
3 LCD Dsply opts → 1>User Code Req
Yes

The Engineer options are options that apply to maintenance and installation functions.

User code required

8.2. 1 User code req
>Yes<

If the User code required option is set to Yes, a user is required to grant the installer an access to the programming menu. See *AXON Control Panel User Manual* for more information on Installer option.

Tamper required

8.2. 2 Tamper req
>No<

If the Tamper required option is set to Yes, the installer must open the panel housing (initiating the tamper alarm) to be able to enter the programming menu.

Engineer lockout

8.2. 3 Eng. lockout
>Disable<

If the Engineer lockout option is set to Enable, it is no longer possible to enter programming mode during power-up using the default installer code (DIP switch 1 is set to On during power-up).

Caution: If this option is enabled, it is impossible to run the system recovery procedure. See “Recovery procedure” on page 372 for more information.

Engineer reset

8.2. 4 Engineer reset → 1>Alarm
>>> No

The Engineer reset menu lets you define which conditions require an engineer reset, and lets you perform this reset.

Alarm

8.2.4. 01 Alarm
>No<

If the Alarm option is set to Yes, the area in which the alarm occurred cannot be set until an engineer reset has been performed, provided engineer reset prevents setting (see “Ready to set options”, page 307).

This option is ignored in case AB alarm confirmation is enabled. For more information see “Confirmed alarm” on page 302.

Tamper

8.2.4. 02 Tamper
>No<

If the Tamper option is set to Yes, tamper alarms require an engineer reset.

Panic

8.2.4. 03 Panic
>No<

If the Panic option is set to Yes, panic alarms require an engineer reset.

Confirmed alarm

8.2.4. 04 Conf. alarm
>No<

The Alarm confirm menu defines which AB alarm requires an engineer reset. The available options are A-ALARM, B-ALARM, or Off (disabled). This option works only when AB alarm confirmation is enabled.

Battery fail

8.2.4. 05 Battery fail
>No<

If the Battery fail option is set to Yes, battery faults require an engineer reset.

Aux fuse

8.2.4. 06 Aux fuse
>No<

If the Aux fuse option is set to Yes, auxiliary fuse faults require an engineer reset.

Mains fail

8.2.4. 07 Mains fail
>No<

If the Mains fail option is set to Yes, mains supply faults require an engineer reset.

Siren fault

8.2.4. 08 Siren fault
>No<

If the Siren fault option is set to Yes, siren faults require an engineer reset.

Interconnection fault

8.2.4. 09 Intconn fault
>No<

If the Interconnection fault option is set to Yes, interconnection faults require an engineer reset.

Automatic reset

8.2.4. 10 Auto reset
>No<

If the Auto reset option is set to Yes, the engineering reset is performed automatically upon the installer log in.

Disable when SERVICE IN

8.2.4. 11 Dis by servi>
>No<

If the Disable when service in option is set to Yes, an engineer reset request is not issued while the installer is authorized to access the system.

Note: This option is only valid if the installer requires a user authorization. See “User code required” on page 301.

System code

8.2.4. 12 System code
> <

The System code menu allows you to set the system code for engineer reset. The code can have up to 5 digits.

The default value 0 means that the code is not set. In this case the remote reset code generation is disabled.

If the code is set, its value and the engineering code value are used in a special calculation to generate the reset code. See “Engineer reset” on page 120 for more information.

Do reset

8.2.4. 13 Do reset
>Cancel<

The Do reset command is used to perform the engineer reset.

Custom text

8.2.4. 14 Custom text
> <

Use custom text to program a prompt displayed when an engineer reset is required.

If the custom text is not set, the standard prompt will be displayed as described in “Engineer reset” on page 120.

Otherwise, the prompts will be the following, depending on a user code display or warning message:

<custom text>
Code:23353

WARNING
<custom text>

See “Engineer reset” on page 120 for more information.

Service in

8.2. 5 Service in
Disable?

The menu lets you disallow the Installer in function before the Installer in time expires (see “Inst in-time” on page 299).

Note: This option is only valid if the installer requires a user authorization. See “User code required” on page 301.

Use this function after the panel programming is complete. To cancel the service in, go to this menu and press Enter. Next, log out. After this, the installer log in requires another user confirmation.

See also “User code requirement” on page 133.

Challenge code

8.2. 6 Challenge code
Disable

Use this menu to activate challenge code functionality. See “Challenge code requirement” on page 133 for more details.

Caution: Once activated, this option cannot be deactivated by software settings.

Inspection

8.2. 7 Inspection >>> → 1>Date
31.12.2099

Set up a periodic inspection reminder.

Date

8.2.7. 1 Date
>31.12.2099<

Enter the date of the next inspection.

Custom message

8.2.7. 2 Custom msg
>Need inspectio<

Enter the message for the inspection reminder.

Installer group

```
8.2.  8 Installer grp  → 1>Many installe>
      >>>                No
```

The menu contains the options that configure Installer user group.

Many installers

```
8.2.8. 1 Many installe>
        >No<
```

If the option is set to Yes, the system can contain more than one Installer user.

Note: The option can be disabled only after all additional installers are removed from the panel database.

Management software access

```
8.2.8. 2 Mgmt SW
        >No<
```

If the option is enabled, editing installers is possible from a keypad, configuration software (ATS85xx), and remotely by the management software (ATS8600).

If the option is disabled, editing installers is only possible from a keypad and configuration software (ATS85xx).

Note: The option is only available if “Many installers” above is set to Enable.

Caution: If the option is enabled, be careful when writing user data from the management software to the control panel. Do not overwrite active installers.

LCD Display opt

```
8.    3 LCD Dsply opts  → 1>Arm display
      >>>                Always
```

The LCD options menu contains options that can be set for LCDs and menus.

Arm display

```
8.3.  1 Arm display
      >Always<
```

If the Armed display mode is Always, the armed display activates after the programmed idle time. The armed display timeout is programmed in “Armed display” (see page 298).

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

You can select one of the following armed display options:

- Off: Armed display is disabled.

- If set: Armed display activates only when the area is set. No status information is displayed on keypad LCD and LEDs (except mains LED and Alert message).
- Always: Armed display always activates. No status information is displayed on keypad LCD and LEDs (except mains LED and Alert message).
- Without code: Armed display always activates. No area LED is lit.

Note: This mode also allows you to deactivate the armed display pressing the Clear key.

Custom message

```
8.3.  2 Custom msg
      >Aritech  <
```

The Custom message menu allows you to define a keypad welcome message.

This records 16 characters of customized text that is displayed on the top line of LCD keypads instead of the default text. Characters include numbers, spaces, or punctuation.

Alarm list

```
8.3.  3 Alarm list
      >Disable<
```

The option defines how zone alarms and faults can be viewed on LCD by an unlogged user.

- Disable: Zone alarms and faults are not shown.
- Enable: The alarm list option allows users to list active zones and faults as well as alarms.

See “Keys” on page 61.

- Instant: Additionally to the alarm list option above, alarms are shown instantly.

Note: Alarms and faults are not shown if Armed display is active. See “Arm display” on page 305 for details.

Indicate faults

```
8.3.  4 Indicate fault
      >Always<
```

The option defines when faults are indicated on LEDs. The following options are available:

- Always: Faults are always shown.
- On set: Faults are displayed only during system setting attempt.

View EE timer

```
8.3.  5 View EE timer
      >Off<
```

The option defines if the entry and exit timers are displayed during setting and unsetting the system.

Note: The appropriate entry/exit timer is displayed on a keypad only if the option for entry/exit buzzer is enabled for this keypad. See “EE 1 buzzer” on page 202 and “EE 2 buzzer” on page 202 for details.

Set options

```
8.  4 Set options
    5 Access opts  →  1>RTS options
                     >>>
```

Options on the Set options menu define the set conditions.

Ready to set options

```
8.4.  1 RTS options
      >>>  →  1>Zone alarm
               Yes
```

The RTS options menu defines conditions that can prevent setting. If a particular condition below has this option set to Yes, its state affects the “Ready to Set” state. The system does not allow for areas to set if any of the conditions are true.

For conditions related to areas, the condition is tested for those areas. For example, Zone 5 assigned to area 1 only affects the setting of area 1.

The following options are available.

- 1 Zone alarm: Active zone
- 2 Zone panic: Hold-up device active
- 3 Zone masking: Masking / fault state on input
- 4 Zone fault: Intrusion detector fault
- 5 Zone tamper: Tamper in zone
- 6 Interconnection fault: A critical error caused by communication trouble between internal panel components
- 7 Mains fault: Mains fault, including external fault
- 8 Battery fault: Battery fault, including external fault
- 9 FTC (Failed to Communicate): Alarm reporting has failed to deliver events
- 10 Siren fault: Siren output fault
- 11 Zone technical: Technical zone status
- 12 Keypad fault: A fault reported by keypad
- 13 Expander fault: A fault reported by remote expander
- 14 Comms fault: All transmission paths are down (no communication)
- 15 Engineer reset: Engineer reset requirement
- 16 Alarms pending: Unacknowledged alarms

Inhibit includes

8.4. 2 Inhibit incl → 1>Zone panic
>>> Access level 3

The menu defines which conditions a user with particular access level is allowed to inhibit. If a particular condition below has this option set to Access level 2 or Access level 3, a user with this access level can inhibit it using an inhibit menu or during set.

The following options are available.

- 1 Zone panic: Holdup device active
- 2 Zone masking: Masking / fault state on input
- 3 Zone fault: Intrusion detector fault
- 4 Zone tamper: Tamper in zone
- 5 Interconnection fault: A critical error caused by communication trouble between internal panel components
- 6 Mains fault: Mains fault, including external fault
- 7 Battery fault: Battery fault, including external fault
- 8 FTC (Failed to Communicate): Reporting attempts are failed
- 9 Siren fault: Siren output fault
- 10 Zone technical: Technical zone status
- 11 Keypad fault: A fault reported by keypad
- 12 Expander fault: A fault reported by remote expander
- 13 Comms fault: All transmission paths are down (no communication)
- 14 Engineer reset: Engineer reset requirement

Part set

8.4. 3 Part set → 1>Report BA
4 Forced set No

The Part set menu allows you to configure the part set options.

Report BA

8.4.3. 1 Report BA
>No<

If the Report BA option is set to Yes, in the part set the system reports burglar alarms triggered during part set to the central station.

Access to EE

8.4.3. 2 Access to EE
>No<

If the Access to EE option is set to Yes, Access zones become Entry/Exit zones during part set. Users being inside the premises will then trigger the entry timer making them aware that the area is set, and an unset procedure is required.

EE full set

8.4.3. 3 EE full set
>No<

If the option is set to Yes and the user exits premises during part set exit time (which causes activation of entry/exit zone), part set state changes to full set.

Note: The functionality works only if there is exit time defined for part set. It means that area part set exit time defined in “Exit time” on page 245 must be longer than 0.

Part set 1 name

Part set 2 name

8.4.3. 4 PS1 name
> <

Use these menus to change the default part set prompts “Part set 1” and “Part set 2”. Empty string is equal to the default prompt.

See *AXON User Manual* for more details on partial setting.

Forced set

8.4. 4 Forced set
>Off<

The Forced set option enables the forced set feature. The forced set options are configured below.

Forced set is an option where active zones can automatically be inhibited when setting an area.

Note: This option should be used with care. Users may not be aware which zones are inhibited.

Forced set options

8.4. 5 Forced set opt
>Inh unset<

The Forced set options menu defines when the forced set is possible. The following options are available.

- Inhibit till unset: Zone is inhibited until the area is unset.
- Inhibit exit: Zone is inhibited until the exit time expires.
- Inhibit close: Zone is inhibited until its state changes to normal.

Pending alarms

8.4. 6 Pending alarms
>Enable<

The menu defines which alarms may prevent system set. The following options are available:

- Enable. If set to Enable, the Pending alarms option requires all alarms to be acknowledged.
- Enable EN 50131. The value is equal to Enable, but all faults and tampers must be also acknowledged.

User level for users that are allowed to acknowledge, depends on the panel defaults. See “Initial start-up” on page 163 for details.

- When disabled, it does not require alarm acknowledgement. During unsetting or resetting the area, the alarm is acknowledged automatically. However, each alarm and fault are shown 3 times on the keypad screen.

Autoset retry on system fault

8.4. 7 AS fault ret>
>15 minutes<

The Autoset retry on system faults option defines if and when the system repeats an attempt to set automatically in if a system fault has made an autoset impossible. The following options are available:

- Off
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours

See “Autoset” on page 108 for more details.

Autoset user retry

8.4. 8 AS user retry
>Disabled<

The Autoset user retry option defines a time for which a normal user can postpone an autoset. The following options are available:

- Disabled (autoset postponing is not allowed)
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours

See “Autoset” on page 108 for more details.

The user must have a privilege for full setting to be allowed to postpone the autoset. See “User group options” on page 227 for more details.

Exit fault

```
8.4. 9 Exit fault
      >Alarm<
```

The menu defines what is happening if the entry/exit zone is still active when the exit time expires. The following options are available:

- Alarm: Exit error fault is generated and the system remains unset.
- Entry: The system is set and the entry timer starts immediately.

Report exit fault

```
8.4. 10 Rep. EE fault
      EE Fault
```

The option defines how the exit fault from entry/exit or access zone is reported to the Central Station.

- EE Fault: Only entry/exit fault is reported.
- EE Fault + Alarm: Two events are reported, EE fault and Burglary Alarm.

Access options

```
8. 5 Access opts
   6 Zone options → 1>Access timers
                   >>>
```

The menu contains various access control options.

Access timers

```
8.5. 1 Access timers → 1>Card to PIN
      >>>                8
```

The menu contains access timer settings.

Note: All timers are programmed in seconds. The allowed ranges are 0 to 127 s.

Card to PIN time

```
8.5.1. 1 Card to PIN
        > <
```

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

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

Two cards time

8.5.1. 2 Two cards > <

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

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

Multiple badge time

8.5.1. 3 Multiple badge > <

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

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

Re-lock delay

8.5.1. 4 Re-lock delay > <

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

This feature is provided for Drop Bolts and Maglocks etc. where the door must be closed before the unlock relay locks the door.

The Re-lock delay time is the amount of time between the door being closed and the unlock relay deactivating (re-lock). This allows a settling time to ensure that the lock mechanisms are aligned.

DGP options

8.5. 2 DGP options >>> → 1>Map relays On

The menu contains door controller settings.

Map relays

8.5.2. 1 Map relays
>On<

Defines whether door controller unlock outputs can be controlled as standard outputs.

- On: Door unlock outputs can be controlled by the control panel as its outputs.
- Off: Door unlock outputs can only be activated by door controller when using door unlock user menu, or upon presenting a valid card.

Map panel LEDs

8.5.2. 2 Map panel LEDs
>On<

When this option is set to On, LEDs in door readers connected to the door controller will represent the same status as LEDs in keypads connected directly to the panel.

Use 27bitTecom format for 27bit cards

8.5. 3 Use 27bitTecom
>Yes<

When the option is set to Yes, 27-bit cards badged on panel system data bus readers will be identified using 27-bit Tecom format calculation. This allows you to use cards compatible with ATS Master control panels as well as ATS125x and CDC4(-EN) door controllers.

System fault beep

8.5. 4 SysFault beep
>Auto<

If the communication between the keypad and the panel is lost and a system fault occurs, the buzzer is activated until any key is pressed. The setting Auto enables this VdS required feature automatically depending on the system defaults. The setting can also be set to On or Off. The default setting is Auto.

Valid card indication

8.5. 5 Valid card ind
>On<

If the option is set to On, the blue LED activates when the valid card is badged on the reader.

If set to Off, the blue LED only indicates if access is granted.

Zone options

8. **6 Zone options** → 1>Swinger shunt
7 Panel&AB opts 4k7

The Input options menu defines options of zone inputs.

Swinger shunt

8.6. **1 Swinger shunt**
> <

The Swinger shunt value defines the number of alarms from a zone until it is shunted. The default value is 2, the maximum number is 4.

This zone must have the “Swinger shunt” option enabled (see page 231).

Rep. restore

8.6. **2 Rep.restore**
>On ACK<

If the Report restore option is set to On ACK, the restore event is reported to the central station when a user acknowledges an alarm.

If the option is set to On input close, the restore event is reported when the zone returns to the normal state.

Limit reports

8.6. **3 Limit reports**
>120<

The option is the idle time (in seconds), which must elapse after an alarm before the next alarm from the same zone is reported to the central station. This time allows you to limit the reporting of multiple alarms from the same zone.

Note: Alarms from the same zone occurring within this time are not reported, but the events are stored in the log. Every new alarm from this zone restarts the timer.

The allowed range is 0 to 255 s. The default value is 120 s, 0 means the limit is disabled.

See also “Limit reports” on page 239.

Long supervision as TA

8.6. **4 LongSup as TA**
>Off<

If the option is set to On, long supervision fault from an alarm zone is indicated, logged, and reported as tamper fault (TA).

Panel and AB options

```

8. 7 Panel&AB opts      → 1>Panel name
   8 PA & Other          Panel

```

The Panel and AB options menu allows you to change certain system values. See also “Initial start-up” on page 163.

If certain settings are changed in this menu, you are prompted to confirm those changes while trying to leave this menu. See “Confirmation of changes” on page 138.

Panel name

```

8.7. 1 Panel name
      >Panel      <

```

The Panel name menu lets you change the panel name.

Panel language

```

8.7. 2 Panel language
      >ENGLISH<

```

The Panel language menu lets you change the panel language.

Caution: Changes of the following authorization options will cause deleting of all user PINs, and setting default PINs of two predefined users. See also “Initial start-up” on page 163, and “Predefined users” on page 69.

Duress method

```

8.7. 3 Duress method
      >Disabled<

```

The Duress method menu allows you to change the duress entering method.

Note: If CDC4(-EN) Door Controller is connected to the panel, the option is read-only, and its value can be changed only during panel installation. See “Initial start-up” on page 163 for more information.

See *AXON Control Panel User Manual* for more information on available duress methods.

PIN length

```

8.7. 4 PIN length
      > <

```

The PIN length menu allows you to change the PIN length. See “Change PIN” on page 220 for more information about PINs.

PIN change mode

8.7. 5 PIN chg mode
>Custom<

The PIN change mode option allows you to choose the appropriate PIN change mode. See “PIN” on page 76 for details on PIN usage.

Alarm confirm

8.7. 6 Alarm confirm >>> → 6>AB mode >>>

The Alarm confirm menu allows you to set a various options connected to the alarm verification.

AB mode

8.7.6. 1 AB mode >>> → 1>Area 1 Off

The AB mode option enables the AB alarm confirmation feature for certain areas. When set to On, the first alarm is reported as a standard burglar alarm (A-alarm). A second input must alarm within a certain period to report a confirmed alarm (B-alarm), provided the first alarm in the area did not occur in an entry/exit zone.

The verification mode is programmable per area.

AB time

8.7.6. 2 AB time >>> → 1>Intr. AB time 30

The menu allows you to configure the maximum delay between A and B alarms.

Intrusion AB time

8.7.6.2. 1 Intr. AB time 30

The maximum time (0 to 255 minutes) that the system allows for a second intrusion alarm to occur to report a confirmed alarm.

If the second alarm happens within this time, it is reported as a confirmed alarm (B-alarm). When the AB time has expired, any next alarm is again an unconfirmed alarm (A-alarm). If the zone that created the initial A-alarm is still active, it is inhibited.

Holdup AB time

8.7.6.2. 2 Holdup AB time 12:00

The maximum time (8 to 20 hours) that the system allows for a second holdup alarm to occur to report a confirmed alarm.

See also “Intrusion AB time” above.

System confirm

8.7.6. 3 System confirm
No

The System confirmation option defines if the AB alarm confirmation works in separate areas only, or if it allows for system-wide validity. If this option is set to Yes, an A-alarm in one area can be confirmed by a B-alarm in another area. Otherwise, the A-alarm can only be confirmed by a B-alarm in the same area.

EE confirm

8.7.6. 4 EE confirm
Yes

The EE confirmation option configures the AB alarm confirmation during entry time.

If the option is set to Yes, alarm confirmation is suspended during entry time. If no B-alarm was present, all alarms during the entry time are A-alarms. When the entry time has expired, alarm confirmation is enabled. However: entry/exit and access zones cannot generate B-alarms.

If this option is set to No, the start of the entry timer disables any alarm confirmation until the area is set again.

Access to EE

8.7.6. 5 Access to EE
Entry/Exit

The Access to EE option defines the functionality of the access zone in the area (if available) when an entry/exit (EE) zone is inhibited at the end of the AB time (auto-inhibit function). The following values are allowed:

- Entry/Exit: an access zone acts as an entry/exit zone, if the entry/exit zone is inhibited.
- Access: an access zone does not change its functionality and causes an alarm when activated while no EE timer is running.

TA confirm

8.7.6. 6 TA confirm
Yes

If the TA confirm option is set to Yes, tamper alarm (TA) can report a B-alarm for burglary alarm (BA), and vice versa.

Sirens

8.7.6. 7 Sirens >>> → 1 Area 1 >A-ALARM<

The Sirens menu allows you to select per area when the siren is activated: on A-alarm or on B-alarm.

Note: Option B-alarm is valid only if AB mode is enabled. See “AB mode” on page 316.

Call central station message

8.7.6. 8 Call CS msg
No

If the Call central station message option is set to Yes, in case of alarm the keypad displays a message with advice for the user to call the central station when a report has been sent.

Reporting delayed

8.7.6. 9 Rep. delayed
Yes

Enable a 30-second delay before alarm reporting required by ACPO regulations.

PD6662

8.7.6. 10 PD6662
Yes

If set to Yes, the reporting delay, enabled by the option “Reporting delayed” above), is *disabled* for the specific case of the entry/exit zone reporting. This is required by ACPO / PD6662 standard.

Easy unset

8.7. 7 Easy unset
Yes

If enabled, you can unset premises entering a PIN or reading a valid card without pressing any other keys.

Note: if the option is set to Yes, PIN only option for door access is not supported. See also “Card and PIN mode” on page 198.

Remote configuration options

8.7. 8 Rem cfg opt → 1>Remote config
9 Object Scheme Yes

Set remote configuration options.

See “Remote access” on page 162 for details.

Remote configuration

8.7.8. 1 Remote config
Yes

If the option is set to Yes, remote operators can modify user PINs and phone numbers when areas are set. If set to No, user PINs and phone numbers are possible to change by remote operators only when all areas are unset.

Allow remote access to configuration by Supervisor

8.7.8. 2 **Superv config**
No

If the option is set to Yes, the supervisor is allowed to configure the panel remotely.

Remote configuration access

8.7.8. 3 **Rem cfg access**
When ServiceIn

The option defines when system remote configuration is allowed.

The following options are available:

- Never: The system cannot be configured remotely.
- Always: The system can be configured remotely.
- When option Service In is enabled: The system can be configured remotely only when Service In function is active.

Webserver options

8.7.8. 4 **WebApp** → 1>WebApp Access
----- Direct IP & US

The menu contains configuration options for the built-in webserver.

Access options for webserver

8.7.8.4. 1 **WebApp Access**
>Direct IP & US<

The option defines the allowed access to the built-in web server (WebApp). The following values are available:

- Off: The access to WebApp is disabled
- Direct IP only: WebApp can only be accessed via direct IP
- UltraSync only: WebApp can only be accessed by UltraSync
- Direct IP & UltraSync: WebApp can be accessed by both direct IP and UltraSync. This is the default value.

Direct IP Protocol

8.7.8.4. 2 **Direct IP Prot**
HTTP & HTTPS

The option defines, which protocol is used for the WebApp communication. The following values are available:

- Off: Direct IP access is disabled.
- HTTP: Insecure protocol only.
- HTTPS: Secure protocol only.

- HTTP & HTTPS: Both protocols are allowed.

See also “Programming the system using WebApp > Secure connection (SSL)” on page 159.

Remote session timeout

8.7.8.4. **3 Idle timeout**
02:00

The option defines the idle time, after which the remote webserver session will be terminated. The allowed range is 2 to 24 hours. The default value is 2 h.

Object scheme

8.7. **9 Object scheme**
Classic

Choose one of the following object (zone, input, output and door) numbering schemes:

- Classic. In the classic numbering scheme, the object default identifiers depend on physical input or output locations, for example, Zone 1 is assigned to the input located on Panel 1.1, Zone 18 is assigned to the input located on Expander 1.2.
- Flexible. In the flexible numbering scheme, default identifiers are independent. When adding a new object, the object is created in the first available database position, regardless of the specific input or output physical location.

When attempting to toggle the scheme, the confirmation is displayed.

Cautions

- Changing of numbering scheme will require system reboot. After this, the reporting event values will change object numbers according to the new numbering.
 - After changing the scheme from classic to flexible, all programmed object dependencies (for example, condition filters, cameras, etc.) will be unavailable. The appropriate parameters will be set to “Not exist” instead of previously programmed objects, until the scheme is changed back.
-

See also “Zone, output, and door addressing” on page 34 in Chapter 2 “Installation”.

Allow Supervisors to Edit Guard Users

8.7. **10 Spv edit Grd**
On

If enabled, the supervisor can modify Guard users. Otherwise, only the installer can modify Guard users. Guard users are not listed on the supervisor’s user list.

See also Chapter 3 “System functions > User groups” on page 71.

PA and other

```

8.  8 PA & other          → 1 Panic mode
    9 TimedUnset/ATM      Silent
  
```

The menu allows you to configure panic alarm mode, chime, and buzzer options, etc.

Panic mode

```

8.8. 1 Panic mode
      Silent
  
```

Panic mode can be one of the following.

- **Silent:** The panic alarm is silent (no siren activation). Until the first panic alarm is restored, subsequent non-panic alarms are also silent.

In this mode, LED and LCD indication for panic alarm is also disabled.

- **Silent PA:** The panic alarm is silent (no siren activation). Subsequent alarms are audible.
- **Sil PA no eSir:** The panic alarm is silent (no siren activation). Until the first panic alarm is restored, subsequent non-panic alarms are audible except external sirens are not activated.
- **Sil PA no Sir:** The panic alarm is silent (no siren activation). Until the first panic alarm is restored, subsequent non-panic alarms are audible except no sirens are activated.
- **Audible:** The panic alarm is standard (with siren activation).
- **Audible LF:** The panic alarm is audible only if a Line Fault (LF) or a Failed to Communicate (FTC) fault is present.

Chime menu

```

8.8. 2 Chime menu      → 1>Chime in PS
    >>>                No
  
```

The Chime menu allows you to set up chime options.

Chime in part set

```

8.8.2. 1 Chime in PS
        No
  
```

The Chime in part set option defines whether the chime option is active when the area is in the part set mode.

Latched chime

```
8.8.2.  2 Latched chime
        Yes
```

If the Latched chime option is set to Yes, disabling the chime only affects the chime functionality until the next time the area is unset. Otherwise, it should be enabled manually.

System tamper areas

```
8.8.    3 SysTamp areas
        12345678
```

The System tamper areas option allows assigning system tampers and faults to the specified areas. At least one area must be selected.

Siren options

```
8.8.    4 Siren options
        5 Card learn-in    →    1 Sir tamper mod
                                Silent
```

The menu allows you to configure various siren options.

Siren tamper input mode

```
8.8.4.  1 Sir tamper mod
        >Single NC<
```

The menu determines the configuration of the siren tamper input in the control panel. The following values can be set:

- Single NO: In the NO input mode the normal state depends on the EOL value. If this value is set to “No EOL” in “Siren tamper EOL” below, normal state for NO input is open.
- Single NC: Similar to NO above, but if the EOL is disabled in “Siren tamper EOL” below, normal state for the input is short.
- Dual loop: For dual loop to operate, the input needs two EOL resistors. This enables the panel to detect both tamper states, short and open circuit.

See also:

- “Siren connection” on page 32
- “Zone connection” on page 27

Siren tamper EOL

```
8.8.4.  2 Sir tamper EOL
        >4k7<
```

The Siren tamper end of line resistor menu allows you to define an end-of-line resistor value for the siren. The available values are the same as in “End of line resistor” on page 240.

Siren retrigger

8.8.4. 3 Siren retrigger.
No

If there are multiple alarms, and the Siren retrigger option is set to Yes, the external siren activates every time an alarm occurs. Otherwise, the external siren activates only after the first alarm.

Report siren fault

8.8.4. 4 Siren report
Fault (YA)

The option defines how the siren fault is reported to the central station. The following values are available:

- Fault (YA): The siren fault is reported as a fault.
- Tamper (TA): The siren fault is reported as a tamper alarm.

Card learn-in

8.8. 5 Card learn-in → 1 Keypad learnin
>>> Rkp 1

Choose a keypad or a door for user card learning. See also “User card” on page 220.

Keypad learn-in

8.8.5. 1 Keypad learnin
Rkp 1

Select a keypad for user card learning.

Door learn-in

8.8.5. 2 Door learn-in
>Not set<

Select a door for user card learning.

Test inputs

8.8. 6 Test inputs
All

The Test inputs option defines what inputs should be accessible when performing input tests as described in “Input tests” on page 171. The following options are available:

- All: All inputs are visible.
- If used: Only the inputs assigned to the existing zones are visible.

Buzzer mode

8.8. 7 Buzzer mode
Continuous

The Buzzer mode menu defines how the keypad buzzer works during the exit time. The following options are available:

- Continuous: The keypad buzzer emits a continuous sound that switches to an intermittent during an entry/exit or access zone activity.
- Intermittent: The keypad buzzer emits a continuous sound and switches to an intermittent 10 seconds before the exit time expires.

Monitor 3rd High Current Output

8.8. 8 Mon. 3 HC out
Enable

Monitor 3rd high current output option defines whether high current output 3 is monitored or not.

Output 3 mode depends on the panel model. See “Outputs” on page 33 for details.

Card number

8.8. 9 Card number
Titan

Select the way the card number is represented in the control panel.

- Basic. The card number is represented in the standard AXON format.
- Titan. The card number is represented in the extended Titan format.

Anonymize Log

8.8. 10 Anonymize Log
Disabled

The menu allows you to set a period, after which the user details are removed from a log entry.

The allowed range is 0 to 60 days, 0 means the functionality is disabled. The default value is 0.

RDR security

8.8. 11 RDR security >>> → 1>Secure mode
On

The menu contains various secure mode settings for secure devices (keypads and readers) in the alarm system.

Note: Not all settings may be available for all devices supporting secure channel functionality.

See Chapter 3 “System functions > Securing card data” on page 127 for more information.

Secure mode

8.8.11. 1 Secure mode
Yes

If set to On, the card readers operate in the secure mode. In this mode the card user is identified by the smart card data instead of the card serial number. See also “Secure mode” on page 127.

Configuration key

8.8.11. 2 Config. key

The menu allows you to set the configuration card encryption key.

The key consists of 16 two-digit hexadecimal numbers (00 to FF).

See “Securing card data > Configuration card” on page 128 for more information.

Application key

8.8.11. 3 App. key

The menu allows you to set the smart card encryption key.

The key consists of 16 two-digit hexadecimal numbers (00 to FF).

Application name

8.8.11. 4 App. name
555443

The menu allows you to set the application name for the smart card data.

The name consists of 3 two-digit hexadecimal numbers (00 to FF). The default value is “55 54 43”.

See “Application name and file ID” on page 127 for more information.

Application file ID

8.8.11. 5 App. file ID
01

The menu allows you to change the file number for application selected in “Application name” above.

See “Application name and file ID” on page 127 for more information.

Reset keys on tamper

8.8.11. 6 Tamp reset key
No

If the option is set to Yes, all encryption keys are erased from the reader memory when a tamper alarm occurs on this reader.

Caution: If the keys are erased, the reader must be reinstalled.

Card Number Bit Limit

8.8.11. 7 Card Bit Lmt
No limit

The option defines if the length of the card number is limited. The following values are available:

- No limit: Card number length is not limited (default value).
- 48-bit: Card number length is limited to 48 bits.

The option is only available if the secure mode is Off. It is used for backward compatibility with older reader models.

Default

8.8.11. 8 Default
>Cancel<

The menu allows you to restore all secure mode settings to the default values.

Choose OK and press Enter to default the secure mode settings.

Note: After the values are set to default, set your own values to secure your system.

Caution: Secure channel keys must be also reset on all devices supporting secure channel communication (for example, CDC4, ATS118x, ATS1125).

Non LCD RAS Orange LED Indication

8.8. 12 RAS OrangeLED
AllZonesNormal

The menu allows you to configure the functionality of the middle orange LED in non-LCD readers and keypads. The following options are available:

- AllZonesNormal: The middle orange LED on a non-LCD keypad or reader is on when all zones in assigned areas are in normal state.
- Fault: The orange LED is on in case of a system fault.

Config in set state

8.8. 13 Config in set
No

If set to Yes, the system can be programmed without unsetting it.

If set to No, the system must be unset before you can configure it.

See also “Area selection” on page 134.

Clocked outputs

8.8. 14 Clocked out
Off

Set the option to On to support clocked outputs for the output module (for example, ATS1811, ATS1820).

Timed Unset / ATM

8. 9 TimedUnset/ATM → 1>Delay
----- 0

The menu allows you to configure the ATM (automated teller machine) interface.

Delay

8.9. 1 Delay
0

The option value is the time between the first and the second ATM user code entering. At the end of the programmed delay period the ATM user is be prompted to re-enter the code.

The allowed range is 0 to 15 minutes. 0 means that the ATM user code can be entered twice without any delay. The default value is 0.

Unset Time

8.9. 2 Unset Time
15

The maximum allowed unset time of the ATM. The allowed range is 1 to 255 minutes.

Extended Unset Time

8.9. 3 Ext Unset Time
0

The maximum allowed extended unset time of the ATM. The allowed range is 0 to 255 minutes.

Note: The user can extend the unset time only once.

Warning Time before set

8.9.	4 Uns Warn Time	10
------	-----------------	----

Warning time is a time before the ATM time runs out, when a warning signal is raised.

The allowed range is 1 to 14 minutes, while the default value is 10 minutes.

Communication

```

9 Communication
-----
→ 1 CS
   2 Event options

```

The menu is used to program all system-wide communication options.

Central station

```

9. 1 CS
   2 Event options
→ 0 Add CS
   1 CS 1

```

The AXON system lets you program up to 16 central stations.

Add CS

```

9.1. 0 Add CS
      1 CS 1

```

Access the menu to add a central station.

If the central station is created successfully, the following message appears:

```

INFO
CS added

```

The new central station is given the default name “CS N” and placed on the end of the central station list.

You can now start editing the central station details for the new central station.

Select CS

```

9.1. 1 CS 1
      2 CS 2
→ 1 CS name
   CS 1

```

Select a central station to program.

Note: Certain options in this menu differ for specific transmission paths. For specific options, see:

- “IP and GSM/GPRS specific options” on page 333
- “Photo transmission specific options” on page 335
- “GSM/phone specific options” on page 336
- “UltraSync specific options” on page 337
- “VdS specific options” on page 337

Common options

CS name

9.1.n. 1 CS name
CS 1

Use the CS name screen to enter or change the central station name. Central station name can consist of up to 16 characters.

Transm path

9.1.n. 2 Transm path
IP

The transmission path defines the type of connection for reporting alarms to the central station. Paths are defined in menu “Path options” on page 339.

Protocol

9.1.n. 3 Protocol
(X) SIA

Choose the appropriate communication protocol.

Depending on the settings in “Transm path” above, the following protocols can be available:

- OH+SIA
- OH+XSIA
- OH+CID
- SMS TEXT
- SMS+CID
- SMS+MMS
- OHPHOTO+CID
- OHPHOTO+SIA
- OHPHOTO+XSIA

Note: OH reporting can be enabled or disabled by UltraSync operators via the UltraSync portal. Current reporting status can be checked in “OH/IRIS Reporting enabling from cloud” on page 191”.

The menu is not available for UltraSync communication path. See “UltraSync” on page 122 for details.

Accounts

9.1.n. 5 Accounts >>> → 1 Area 1
None

Account numbers identify alarm systems reporting to central stations. Account numbers are 4 to 6 digits long (depending on the type of protocol). If set to None, the reporting for the selected area is disabled.

In case a few areas have the same account numbers, and “OP/CL report” option on page 333 is set to Yes, a special operation takes place for SIA/XSIA reporting

of opening/closing depending on the area modifier setting (see “XSIA”, page 332).

- Area modifier off: Closing is reported when all areas with the same account number have been set. The area that was set last is reported. The first to disarm sends the opening signal for the area to be opened.
- Area modifier on: Opening and closing signals are reported separately. The Area Modifier is used to identify the correct area.

Note: System events, as well as Area 1 events, are always reported using Account 1.

The menu is not available for UltraSync communication path. See “UltraSync” on page 122 for details.

Select area

9.1.n.5. 1 Area 1
> <

Set account numbers for each area.

Mode

9.1.n. 6 Mode
Primary CS

The following modes are available for CS.

- Primary CS: The primary central station must unconditionally receive all addressed events.
- Backup CS: The central station can be a backup CS for the previous CS in the central station list (see “Central station” on page 329). This means that the panel reports to this central station only if the primary CS reporting fails.

For example, if CS 1 and CS 2 are primary CS, and CS 3 and CS 4 are backup CS, it means that CS 1 has no backup, CS 3 is a backup central station for CS 2, and CS 4 is a backup for central station 3.

See “Reporting principles” on page 98 for more information.

Retry count

9.1.n. 7 Retry count
14

The Retry count value is the number of retries to make a successful call to the central station. If the limit is reached, the FTC is generated.

The counter is zeroed when a new event occurs in Global FTC condition. See “Failed to communicate (FTC)” on page 100 for more information.

The value ranges from 0 to 14. The default value is 14.

Protocol opt

9.1.n. 8 Protocol opt → 1 (X) SIA
 >>> 2 OH 2000

It is possible to customize the communication protocol parameters using the Protocol opt menu.

The menu is not available for UltraSync communication path. See “UltraSync” on page 122 for details.

XSIA

9.1.n.8. 1 (X) SIA → 1 Area modifier
 2 OH 2000 Off

The XSIA menu allows you to set options for the SIA and XSIA protocol.

Area modifier

9.1.n.8.1. 1 Area modifier
 Off

If the Area modifier option is set to Yes, the area modifier is added to the SIA and XSIA reports. This allows you to send event from multiple areas using the same account code. See also “Accounts” on page 330.

Name chars

9.1.n.8.1. 2 Name chars
 16

The Name chars value defines the length of the name strings used in the XSIA reporting.

The allowed values are 16 and 30.

Event number

9.1.n.8.1. 3 Event number
 3 digits

The Event number value defines the length of the subevent field (user or point).

The allowed values are 2, 3, and 4 digits.

Subev coding

9.1.n.8.1. 4 Subev coding
 Decimal

The Subev coding value defines whether the subevent number is reported to the CS in hexadecimal (hex) or decimal format.

OP/CL report

9.1.n. 9 OP/CL report
Separate

The OP/CL report option defines if opening and closing is reported for all areas with the same account code, or for each of those. The following options are available:

- Combined: When all areas with the same account code are armed, a closing is reported using the area and user who armed it. An opening is reported only when the first of the areas with the same account code is disarmed.
- Separate: For any of areas with the same account code a closing and an opening is reported. The area modifier indicates the area concerned (see “Area modifier” on page 332).

Note: When (X)SIA protocol is selected, separate reporting works only when SIA area modifier is enabled.

See “Accounts” on page 330 for more details.

The menu is not available for UltraSync communication path. See “UltraSync” on page 122 for details.

Delete CS

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

The display shows:

9.1.n. 10 Delete CS
>Cancel<

Choose Ok and press Enter. This removes the central station.

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

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

IP and GSM/GPRS specific options

Destination/IP

9.1.n. 4 Destination/IP → 1 Type
>>> IP

The Destination menu contains the configuration of the reporting receiver.

Dest. name/IP

9.1.n.4. 1 Dest name
None

Every central station reports to one IP address.

A destination name can be a numeric IP address or an alphabetic domain address. See also “How to edit a host address” on page 138.

Destination port

9.1.n.4. 2 Dest port
9999

The destination port is used to report to the host selected in “Dest. name/IP” above.

Ping host

9.1.n.4. 3 Ping host >>> → Pinging...
Tx/Rx: 2/2

The Ping host command allows you to send a ping to the selected central station. This command is used to check if the central station is present and accessible from the panel in the network.

The Tx/Rx value indicates the number of packets sent and received.

Note: Monitoring station can be configured to not respond to ping requests, thus this feature may not work with every CS IP address. To test the communication path, use menu “Ping host” described on page 182 to send ping to another host.

OH 2000

9.1.n.8. 2 OH 2000
3 VdS → 1>Version
OH V4

The OH 2000 menu allows you to set up a few OH 2000 protocol options that are listed below.

Version

9.1.n.8.2. 1 Version
OH V4

The following versions of the OH 2000 protocol can be used for Osborne-Hoffman receiver communication:

- OH V1.9.3
- OH V2
- OH V3
- OH V3.1
- OH V4

Note: OH version selection is only available if the following options are set:

- Transm path: IP or GSM/GPRS

- Protocol: OH+CID, OH+SIA, OH+XSIA, OHPHOTO+CID, OHPHOTO+SIA, OHPHOTO+XSIA

See an appropriate receiver's manual for more details.

Heartbeat time

9.1.n.8.2. 2 Heartbeat time
00:01'00

The heartbeat time defines how often the panel sends a presence message (heartbeat) to the central station. The range for this value is from every second (00:00'01) to every day (23:59'59). The maximum value 23:59'59 means the heartbeat functionality is disabled.

Receiver nbr

9.1.n.8.2. 3 Receiver nbr
1

A receiver identifier used in central stations with multiple receivers. The allowed value is a hexadecimal number from 0001 to FFFF.

Line nbr

9.1.n.8.2. 4 Line nbr
1

A line identifier used in central stations with multiple receiving lines. The allowed value is a hexadecimal number from 0001 to FFFF.

Frequent Heartbeat time

9.1.n.8.2. 5 Freq. HB time
Disabled

If the primary CS communication fails, the backup CS heartbeat time is switched from normal to frequent.

See also "Heartbeat time" above.

Photo transmission specific options

Additionally to "IP and GSM/GPRS specific options" described on page 333, it is necessary to set the options below.

Encryption

9.1.n.4. 4 Encryption
No

If the Encryption option is set to Yes, the pictures are sent encrypted with AES algorithm.

Picture destination port

9.1.n.4. 5 Pic dest port
9000

The destination port is used to send the pictures to a host set up in “Dest. name/IP” on page 334.

GSM/phone specific options

Destination

9.1.n. 4 Destination >>> → 1 Type
Phone

The Destination menu contains the configuration of the reporting receiver.

Type

9.1.n.4. 1 Type
Phone

The Type submenu defines who receives the reports directed to the specified central station:

- Phone: The report is sent to a specified phone number. Menu “Phone/User/UG” below configures this phone number.
- User: The report is sent to a specified user’s phone number. This user is selected via menu “Phone/User/UG” below.
- User Group: The report is sent to all users that belong to the user group that is set via menu “Phone/User/UG” below.

User and user group reporting require the following:

- Users must have their phone numbers set in “Mobile number” on page 223.
- The SMS reporting must be enabled for these users. See “SMS reporting” on page 223.
- At least one of the user groups must allow these users to receive SMS reports. See “User group options” on page 227).

Phone/User/UG

9.1.n.4. 2 Phone
> <

This menu depends on the Type value set for the reporting recipient. See menu “Type” above for parameters description.

UltraSync specific options

Channel number

9.1.n. 4 Channel no
1

The informational screens contain the channel number used for connection to the UltraSync cloud. The channel is configured in UltraSync Web portal. It defines such settings as reporting format, account number, and polling time.

Caution: When the panel is registered in the UltraSync cloud, all security cloud reporting is configured remotely from the cloud.

See Chapter 3 “System functions > UltraSync” on page 122 for more information on cloud connection.

VdS specific options

VdS

9.1.n.8. 3 VdS → 1 Version
----- VdS 2465

The menu contains various VdS reporting options described below.

Version

9.1.n.8.3. 1 Version
VdS 2465

Select one of the VdS protocol versions supported in the control panel.

Encryption key number

9.1.n.8.3. 2 Enc. key no.
Disable

Select the number of encryption key for VdS protocol encryption.

The number is used for identification in the central station.

0 means no encryption is applied.

Encryption key value

9.1.n.8.3. 3 Enc. key value
>0000000000000000<

Set the value for the selected encryption key used for VdS protocol encryption.

SVCP connection mode

```
9.1.n.8.3. 4 SVCP conn mode
           Disable
```

Enable or disable SVCP connection mode for event reporting to the central station.

Event options

```
9. 2 Event options
   3 Path options      → 1 CS mapping
                        2 Delayed events
```

The Event options menu contains event options.
See “Reporting principles” on page 98 for more details on event reporting.

CS mapping

```
9.2. 1 CS mapping
     2 Delayed events → 001 AN Report to
                       1234.....
```

The CS mapping menu allows you to map reporting events to the specific central stations.
The list of events is shown in Appendix B “AXON reporting codes” on page 437.

Delayed events

```
9.2. 2 Delayed events
     3 VdS channels    → 0 Delay timer
                       0
```

The Delayed events menu allows you to set a delay for selected events.
The first menu entry, “0 Delay timer”, allows you to set the global reporting delay from 0 to 250 sec.
The next menu entries represent the events. If the option is On, the delay is applied.

```
01>AN Delayed
      Off
```

For the list of events, see Appendix B “AXON reporting codes” on page 437.

VdS channels

```
9.2. 3 VdS channels
     -----      → 1>Input events
                       2 System events
```

The menu allows you to map reporting events to the specific VdS reporting channels.
See Chapter 3 “System functions > VdS channel reporting” on page 101 for available VdS reporting events and default channels.

Path options

```

9.  3 Path options
    4 PC connection
    → 1 IP
       -----
  
```

The Path options menu allows you to configure options for available transmission paths.

Select path

```

9.3. 1 IP
      -----
    → 1>Path name
        IP
  
```

Select the appropriate transmission path to configure its options.

Available transmission paths depend on the system configuration. By default, the following transmission paths are available:

- IP

Depending on the hardware configuration, the following transmission paths may also be available:

- GSM
- TDA74xx
- UltraSync

Note: Certain options in this menu differ for specific transmission paths. For specific options, see:

- “IP specific options” on page 341
- “GSM/SMS/GPRS specific options” on page 345

Common options

Path name

```

9.3.n. 1 Path name
        IP
  
```

Use the path name screen to enter or change the transmission path name. The name can consist of up to 16 characters.

Line fault

```

9.3.n. 2 Line fault
        Always
  
```

If the Line fault option is set to Always, the line is tested for line faults. If a line fault is present a fault is generated in the system.

If Line fault is set to “If used”, the line is being tested only if this path is used for any central station communication, and the account number for this station is set.

Line fault delay

9.3.n. 3 LF delay 0

Line fault delay defines the period, after which the path fault is reported to the central station. If the fault restores before this time expires, no fault is reported.

The allowed range is 0 to 255 s.

Expander menu

9.3.n. 4 Expander menu >>>

Certain diallers have their internal menus. Enter Expander menu to set internal dialler options.

The menu content depends on the equipment.

Ring setup

9.3.n. 8 Ring setup >>> → 1>Ring count
2 Omit 1st call

The menu contains ringing configuration options.

Note: This option is not available for IP connection.

Ring count

9.3.n.8. 1 Ring count > <

The Ring count screen lets you enter the number of rings before answering an incoming call. The allowed range is 1 to 15. Higher value is equal to infinity, so incoming calls are not answered at all.

Omit 1st call

9.3.n.8. 2 Omit 1st call >No<

Use this option when sharing a telephone line with other equipment (for example, a fax or an answering machine) that automatically answers incoming rings.

If set to Yes, the panel hangs up after a number of incoming rings programmed in “Ring count” above, and answers immediately to the second incoming call received within 30 seconds after the first one.

If set to No, the panel answers after the number of incoming rings programmed in “Ring count”.

Encryption

9.3.n. 9 Encryption
>No<

If the Encryption option is set to Yes, the communication is encrypted with AES algorithm.

The encryption key is set using menu “Encryption key” on page 356.

Note: IP connection is always encrypted. USB communication does not use encryption.

IP specific options

Transm path

9.3.n. 4 Transm path
ETHERNET

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

IP config options

9.3.n. 5 IP config >>> → 1>IP config
Dynamic

The IP config menu allows you to configure the panel IP address.

The following options are configurable in this menu.

IP config

9.3.n.5. 1 IP config
>Dynamic<

If the IP config is set to Dynamic, the DHCP is enabled. If this value is Static, you must configure the other options in this menu that are described below.

IP address

9.3.n.5. 2 IP address
>000.000.000.00<

You must set the panel IP address prior to use the IP communication, if DHCP is disabled. If DHCP is enabled in “IP config” menu above, this value shows the dynamic IP address that is assigned by the DHCP server and cannot be changed.

Subnet mask

9.3.n.5. **3 Subnet mask**
>255.255.255.00<

You must set the panel IP subnet mask prior to use the OH 2000 communication protocol, if DHCP is disabled. If DHCP is enabled in “IP config” menu on page 341, this value shows the dynamic IP subnet mask that cannot be changed.

Gateway

9.3.n.5. **4 Gateway**
>000.000.000.00<

You must set the gateway IP address prior to use the OH 2000 communication protocol in a WAN, if DHCP is disabled. If DHCP is enabled in “IP config” menu on page 341, this value shows the dynamic gateway address that cannot be changed.

DNS options

9.3.n. **6 DNS config** >>> → 1>DNS config
Static

The DNS server must be configured if you use domain names for the Ethernet reporting.

The following options are configurable in this menu.

DNS config

9.3.n.6. **1 DNS config**
>Static<

If the IP configuration in menu “IP config options” on page 341 is set to Dynamic (DHCP is enabled), you can set the DNS configuration option to Static to override the automatic DNS configuration by DHCP server. Set the DNS address in the menu below. If this option is set to Dynamic, the DHCP is used to obtain the DNS IP address.

If DHCP is disabled, this menu is not available.

DNS server

9.3.n.6. **2 DNS server**
>000.000.000.00<

The DNS server menu allows you to set the DNS address if it is different from the DNS provided by DHCP server, or if DHCP is disabled in menu “IP config” menu on page 341.

NTP options

9.3.n. 07 NTP config >>> → 1 NTP config
Dynamic

The NTP config menu is used to configure the NTP (Network Time Protocol) server.

The following options are configurable in this menu.

NTP config

9.3.n.7. 1 NTP config
Dynamic

If the IP configuration in menu “IP config options” on page 341 is set to Dynamic (DHCP is enabled), you can set the NTP configuration option to Static to override the automatic NTP configuration by DHCP server. Set the NTP address in the menu below. If this option is set to Dynamic, the DHCP is used to obtain the NTP IP address.

If DHCP is disabled, this menu is not available.

NTP server

9.3.n.7. 2 NTP server
>000.000.000.00<

The NTP server menu allows you to set the NTP address if it is different from the NTP provided by DHCP server, or if DHCP is disabled in menu “IP config” menu on page 341.

Firewall options

9.3.n. 8 Firewall >>> → 1 Firewall
Off

The Firewall menu is used to configure the built-in firewall. The firewall allows only communication from hosts that are configured as appropriate PC connections in “Destination/IP” on page 357.

The following options are configurable in this menu.

Firewall

9.3.n.8. 1 Firewall
Off

Use the Firewall menu to enable (On) or disable (Off) the built-in firewall.

Reply on PING

9.3.n.8. 2 Reply on PING
Yes

The Reply on PING defines whether the firewall allows answering to ping requests. If this option is set to No, ping requests are not answered.

MAC address

```
9.3.n. 10 MAC address
      0051DB3D7E73
```

MAC address of the Ethernet controller is a read-only value.

Max IP Picture reports per 24h

```
9.3.n. 11 Max Pics 24h
      > <
```

You can limit the maximum number of pictures sent to users via IP transmission path during a 24-hour period.

If the limit is reached, further picture requests are denied by the system and an appropriate event is recorded in the log.

There is no limit for pictures if this value is set to 0.

Line fault check for WAN connection

```
9.3.n. 12 WAN LF check
      No
```

If the option is set to Yes, the WAN IP communication with UltraSync is tested. If a line fault is present, a WAN fault is generated in the system.

mDNS enabled

```
9.3.n. 13 mDNS enabled
      >>> → 1>mDNS enabled
              No
```

The menu contains options that allow you to connect to the control panel via LAN.

Caution: It is only possible to use mDNS if your local network supports multicast DNS functions. Check with your local IT department or your router manufacturer. If your network does not support multicast, you can connect to the panel only by connecting to its IP address, not via panel SID.

mDNS enabled

```
9.3.n.13. 1 mDNS enabled
          No
```

Enables multicast DNS protocol, which allows you to use your web browser to configure the panel in your LAN.

Host name prefix

```
9.3.n.13. 2 Host name pre>
          None
```

Configure the prefix for your control panel local host name.

If the host prefix is not set, the local host name is “SID.local”, where SID is panel serial number.

GSM/SMS/GPRS specific options

Transm path

9.3.n. 4 Transm path
ETHERNET

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

GSM Setup

9.3.n. 5 GSM Setup >>> → 1 SIM card PIN
0000

The GSM Setup menu lets you set up GSM reporting and control.

Notes

- Before using the SIM card in the system, insert it into a mobile phone and verify its validity, checking the credit and sending a test SMS message.
- Before changing SIM card, delete the SMS center number. Otherwise, the system will overwrite the default SMS center number on the new SIM card with this number. See “SMS Center number” on page 349 for more details.

SIM card PIN

9.3.n.5. 1 SIM card PIN
0000

The SIM card PIN menu lets you configure the PIN of the SIM card.

This menu can also show the following messages:

- PUK required
- One trial left

See “PIN status” on page 183 for more detailed explanation for these messages.

This menu does not have any functionality if the PIN is not required for this SIM card.

Networks

9.3.n.5. 2 Networks >>> → 1>Net.selection
Automatic

The Networks menu lets you configure the GSM network settings.

Network selection

9.3.n.5.2. 1 Net.selection
>Automatic<

The Network selection menu lets you define the preferred GSM network. Enter the GSM network numerical code. If the code is not entered, the network is chosen automatically.

Selected network only

9.3.n.5.2. 2 Sel.net.only
>No<

If the Selected network only option is set to Yes, only the network selected in the “Network selection” above is allowed for the communication. Otherwise, the system automatically selects another network if the configured network is unavailable.

GSM networks scanning

9.3.n.5.2. 3 Net.scanning
>>> → 0>Rescan nets
1 * MyGSM

The Network scanning menu lists all available networks. It also lets you force another scan.

The list contains GSM network names that are preceded by one of the following marks that define the network availability:

- *: The network is currently connected.
- +: The network is allowed for connection.
- -: The network is forbidden for connection.

If the network name is unknown (not recognized by the GSM dialler), the network code in square brackets is displayed instead of the name, for example, “+ [20999]”.

Rescan networks

9.3.n.5.2.3. 0 Rescan nets
1 * MyGSM → Scan in progress
Please wait

The Rescan nets command performs a GSM network scan.

The scan can take a few minutes. You can cancel the scan by pressing Clear.

Select a network

9.3.n.5.2.3. 1 * MyGSM
2 Other GSMNet → 1 Network name
MyGSM

Select a network to see more options.

Network name

9.3.n.5.2.3.m. 1 Network name
MyGSM

The Network name is the name of the GSM network. Refer to “Network name” on page 184 for more details.

Network code

9.3.n.5.2.3.m. 2 Network code
21999

The Network code is the unique code of the GSM network. Refer to “Network code” on page 185 for more details.

Availability

9.3.n.5.2.3.m. 3 Availability
Connected

The Availability values are described in “GSM networks scanning” on page 346.

RSSI

9.3.n.5.2.3.m. 4 RSSI
-35 dBm [IIII]

The Received Signal Strength Indication (RSSI) value is diagnostic information. See also “RSSI” on page 185.

Use this net.

9.3.n.5.2.3.m. 5 Use this net.

Enter Use this network menu to connect the selected GSM network. This replaces the network selected in “Network selection” on page 346.

Credit

9.3.n.5. 3 Credit >>> → 1 Check now >>>

The Credit menu lets you configure and perform GSM account checking.

Check now

9.3.n.5.3. 1 Check now
>>>

The Check now menu lets you manually check your GSM account. When received, the account state is displayed on the LCD.

Prior to this, the credit checking must be configured in the menus described below.

Check mode

9.3.n.5.3. 2 Check mode
Standard

Depending on the GSM network, credit can be checked in a different way. The following modes are available:

- Standard: The credit is checked when contacting the GSM provider using the request code. This mode is used in most GSM networks.
- SMS message: The credit is checked by sending a predefined SMS message on the number given in the “Check number” below.

Check number

9.3.n.5.3. 3 Check number
+48600000000

The Check number is the phone number that is used for sending credit check SMS messages, if this check mode is chosen in “Check mode” above.

Request code

9.3.n.5.3. 4 Request code
*101#

The Request code for the account check must be configured in this menu. It allows you to enter numbers as well as “*” and “#” signs (for example, *101#). Contact your GSM provider to find out how to check your account.

Check period

9.3.n.5.3. 5 Check period
> <

The Check period (in days) defines how often the system automatically checks your account.

Note: When the system performs an automatic account check, the response is treated as an SMS from an unauthorized source, and therefore is forwarded to the Supervisor. Please make sure that option “SMS forwarding” on page 349 is enabled, otherwise the account state response will be lost.

Check time

9.3.n.5.3. 6 Check time
>12:00<

The Check time is the time of day in 24 h format when the system performs the automatic account check described in “Check period” above.

GSM jamming detection options

9.3.n.5. 4 Jamm detection >>> → 1>Jamm detection
Off

The menu allows you to configure GSM jamming detection parameters.

GSM jamming detection

9.3.n.5.4. 1 Jamm detection
>Off<

If set to On, the panel raises tamper alarm when GSM jamming is detected.

Note: The dialler must support jamming detection functionality. The detection is supported in the ATS7310 GSM dialler with firmware version V01.08 or later.

Jamming threshold

9.3.n.5.4. 2 Jamm threshold
>20<

Configure the threshold for jamming detection report. The allowed range is from 1 (–111 dBm) to 31 (–51 dBm). The default value is 20 (–73 dBm).

SMS Setup

9.3.n. 6 SMS Setup >>> → 1>SMS Center num
None

The SMS Setup menu lets you change various SMS settings.

SMS Center number

9.3.n.6. 1 SMS Center num
> <

The SMS Center number is the access number for the SMS service.

If this value is empty, the system uses the default number stored in the SIM card. Use this menu to enter a number other than the provider's default one.

Caution: Delete this number before changing the SIM card. Otherwise, the system will overwrite the default SMS center number on the new SIM card with this number.

SMS forwarding

9.3.n.6. 2 SMS forwarding >>> → 0 Off
1 +48600000000

The SMS forwarding menu lets you choose the phone number to which all unrecognized messages are forwarded (usually the supervisor's or administrator's phone). You can also switch off SMS forwarding using this menu.

The list contains only those users who:

- Have the appropriate privileges to receive SMS messages (see “User group options” on page 227)
- Have their phone numbers configured (see “Mobile number” on page 223)

Max SMS reports per 24h

```
9.3.n.6.  3 Max Msg 24h
          >  <
```

You can limit the maximum number of SMS messages sent to users during a 24-hour period. If this limit is reached, further incoming messages are ignored by the system.

The SMS reports and unrecognized SMS commands have two separate counters. However, the maximum limit defined in this menu is the same for both counters.

There is no limit for messages if this value is set to 0.

Custom SMS header

```
9.3.n.6.  4 SMS header msg
          >  <
```

The SMS header message identifies the AXON system. It is included at the beginning of each text SMS message sent by the system if the reporting format is set to SMS text. See “Protocol” on page 330

User PIN required in SMS

```
9.3.n.6.  5 User PIN req.
          >No<
```

If the User PIN required option is set to Yes, you must start every SMS control message with your PIN, otherwise the command will be rejected. See the *SMS Control Reference Manual* for more information.

Extended character set in SMS

```
9.3.n.6.  6 Ext.charset
          >No<
```

The Extended charset (UCS2) option has an influence on the SMS messages sent by the AXON system to the user. This option must be set to Yes prior to read SMS reports and responses with special and national characters that exceed the standard GSM charset GSM3.38.

Notes

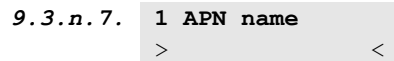
- The extended charset is used only if there is no possibility to send the message in the standard charset.
- Older cell phones may not correctly display messages that use the extended charset.

GPRS Setup



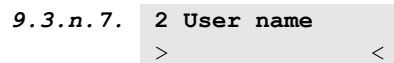
The GPRS Setup menu lets you change various GPRS settings.

APN



The Access Point Name is a configurable network identifier used by a mobile device when connecting to a GSM carrier. It must be specified by the GPRS provider.

User name



The User name must be specified by the GPRS provider.

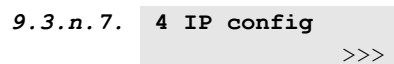
User password



The User password must be specified by the GPRS provider.

Note: The following GPRS configuration menus are equal to appropriate IP configuration menus, except they apply only to the IP connection via the GPRS path.

IP config options



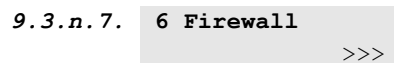
See “IP config options” on page 341.

DNS config options



See “DNS options” on page 342.

Firewall options



See “Firewall options” on page 343.

Line fault

9.3.n.7. 7 Line fault
>No<

If the Line fault option is set to Yes, the line is tested for line faults. If a line fault is present a fault is generated in the system.

Disconn.time

9.3.n.7. 8 Disconn.time
>02:00<

The connection is automatically closed when no data is sent during the Disconnection time. The connection is reinitialised when necessary.

Minimum disconnection time is 5 min. If the time is set to 23:59 or more, it changes to Infinity. In this case the connection never closes.

Caution: If the system should receive requests from PC incoming via GPRS, the disconnection time must be set to infinity for the connection to stay always open.

Note: The option is not used when UltraSync connection is enabled.

Max GPRS Picture reports per 24h

9.3.n.7. 9 Max Pics 24h
> <

See “Max IP Picture reports per 24h” on page 344.

MMS Setup

9.3.n. 10 MMS Setup >>> → 1>MMS center
None

The menu lets you to configure various MMS settings.

Note: Contact your GSM provider to get information on all settings in this menu.

MMS Center

9.3.n.10. 1 MMS center
None

The MMS center number is the address for the MMS service.

APN

9.3.n.10. 2 APN name
> <

See “APN” on page 351 for details.

User name

9.3.n.10. 3 User name
> <

See “User name” on page 351 for details.

User password

9.3.n.10. 4 User pass
> <

See “User password” on page 351 for details.

Proxy

9.3.n.10. 5 Proxy
> <

Enter the MMS proxy server address.

Proxy port

9.3.n.10. 6 Proxy port
> <

Enter the proxy server port number for the proxy server configured in “Proxy” above.

Max MMS 24h

9.3.n.10. 7 Max MMS 24h
> <

You can limit the maximum number of MMS sent to users via GPRStransmission path during a 24-hour period.

If the limit is reached, further MMS requests are denied by the system and an appropriate event is recorded in the log.

Note: This setting affects only one set/unset cycle. When an area changes its state, for example, it is being set, the counter resets.

There is no limit for MMS if this value is set to 0.

Module info

9.3.n. 11 Module info
>>>

The informational screens contain GSM dialer firmware version, modem type, etc.

PC connection

```
9.  4 PC connection      →  1>Connections
    5 UltraSync          >>>
```

A PC connection can be used for:

- Upload / download (U/D)
- Management
- Remote control

The PC connection menu allows you to set up the PC connection parameters.

Connections

```
9.4. 1 Connections      →  0>Add PC conn
    >>>                  1 PC conn 1
```

It is possible to define up to 16 different PC connections.

Add PC conn

```
9.4.1. 0 Add PC conn
        1 PC conn 1
```

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

```
INFO
PC conn added
```

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

Select PC connection

Select the connection to configure.

Note: Certain options in this menu differ for specific transmission paths. For specific options, see:

- “IP specific options” on page 357
- “GSM specific options” on page 357

Common options

Name

```
9.4.1.n. 1 Name
          >PC conn 1  <
```

The connection name can consist of up to 16 characters.

Transm path

9.4.1.n. 2 Transm path
IP

The Transmission path option defines which communication path is used to establish the selected PC connection.

Note: The next options in this menu differ for specific transmission paths.

Retry limit

9.4.1.n. 5 Retry limit
> <

The Retry limit option defines a maximum number of connection attempts. The allowed range is between 0 and 250. The retry counter is reset after each successful connection or any incoming call.

Delete PC conn

9.4.1.n. 6 Delete PC conn
>Cancel<

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

Choose Ok and press Enter. This removes the PC connection.

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

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

PC callback

9.4. 2 PC callback → 1>Primary
3 Encrypt.key 1 2 Backup

The PC callback option defines which PC connection is used as a callback station.

If the PC call back option is set to Off (no connection assigned), then auto-answer is active.

Note: Callback functionality is only used with OH callback option.

Primary

Backup

These menus allow you to configure the primary and the backup callback destination respectively.

Choose a PC connection for a callback, or 0 to disable it.

```
9.4.2. 1>Primary      0>Off
        2 Backup      1 PC conn 1
```

Upon a callback request AXON attempts to connect to the primary callback destination. The number of attempts is defined in “Retry limit” on page 355. After the retry limit exceeds, the panel connects to the backup callback destination.

Encryption key 1

Encryption key 2

```
9.4. 3 Encrypt.key 1
      >00000000000000<

9.4. 4 Encrypt.key 2
      >00000000000000<
```

The AXON control panel requires an encryption key before granting access to the panel using the upload/download PC software. The encryption key can consist of up to 24 characters. The two Encryption key menus represent the first and the second part of the key accordingly. The default key is 0000000000000000000000000000 (24 zeroes).

Caution: It is highly recommended to change the default encryption key.

Note: A PC connection via IP transmission path is always encrypted. USB communication is never encrypted.

Listening port

```
9.4. 5 Listening port
      >      <
```

Listening port is an IP port that is used for receiving uploading/downloading requests from the remote PC. The default listening port is 32000.

Caution: Incoming requests via GPRS are accepted only if the GPRS connection is permanent and never closes automatically. See “Disconn.time” on page 352 for more details.

Panel ID

```
9.4. 6 Panel ID
      >      <
```

Use Panel ID to distinguish between a few panels when using them in one facility with Downloader connection.

IP specific options

Destination/IP

9.4.1.n. 4 Destination/IP >>> → 1 Dest name
None

The Destination menu defines IP details for the selected PC connection. It also allows you to ping the host.

Destination name

9.4.1.n.4. 1 Dest name
> <

The Destination name defines which IP address is used to establish the selected PC connection.

A destination name can be a numeric IP address or an alphabetic domain address. See also “How to edit a host address” on page 138.

Destination port

9.4.1.n.4. 2 Dest port
> <

The Destination port defines which IP port is used to establish the selected PC connection.

Ping host

9.4.1.n.4. 3 Ping host >>> → Pinging...
Tx/Rx: 2/2

The Ping host command allows you to send a ping to the selected PC. This command is used to check if the PC is present and accessible from the panel in the network.

The Tx/Rx value indicates the number of packets sent and received.

GSM specific options

Connection type

9.4.1.n. 3 Conn. type
>CSD<

The Connection type menu defines what GSM connection is used. The following options are available:

- CSD: The modem functionality is used.
- GPRS: The GPRS functionality is used.

UltraSync options

9. **5 UltraSync** → **1>Connectivity**
6 VdS Enable

The menu allows you to configure the UltraSync cloud communication.
See “UltraSync” on page 122 for details.

Cloud connectivity

9.5. **1 Connectivity**
>Enable<

Enable or disable the UltraSync cloud connection.

SID number

9.5. **2 SID number**
084400412454

The informational screen that shows the panel serial number.

Settings

9.5. **3 Settings** >>> → **1 Password**

The menu contains UltraSync connection settings.

UltraSync password

9.5.3. **1 Password**
> <

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

Remote firmware upgrade

9.5.3. **2 FW Upgrade**
>Disabled<

Enable or disable remote firmware upgrade.

Remote configuration

9.5.3. **3 Remote config.**
>Disabled<

Enable or disable remote panel programming.

Notifications

9.5.3. **4 Notifications**
>Enabled<

Enable or disable smartphone push notifications.

Push notifications are configured in “Notifications” on page 359.

GPRS monitoring

9.5.3. 5 GPRS monitor
>Enabled<

Enable or disable UltraSync connection monitoring by control panel.

The panel tries to connect UltraSync every 100 s to monitor the connection.
Disable this option to limit data sent via GPRS.

Servers

9.5.3. 6 US servers → 1 ETH server 1
>>> >192.168.1.1:44>

The menu allows to predefine UltraSync default servers and ports:

- 1 ETH server 1: Default primary Ethernet server
- 2 ETH server 2: Default backup Ethernet server 1
- 3 ETH server 3: Backup Ethernet server 2
- 4 ETH server 4: Backup Ethernet server 3
- 5 Wless server 1: Default primary wireless server
- 6 Wless server 2: Default backup wireless server 1
- 7 Wless server 3: Backup wireless server 2
- 8 Wless server 4: Backup wireless server 3

Notifications

9.5. 4 Notifications → 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.

Select notification

9.5.4. 1>Notification 1 → 1 Name
2 Notification 2 Notification 1

Select a notification to configure it.

Notification name

9.5.4.n. 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.

Identifier

9.5.4.n. 2 Identifier

The informational screen that shows the smartphone notification identifier.

Assigned user

9.5.4.n. 3 User
User 3

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

Sending status

9.5.4.n. 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 “Event types to notify” below.

Event types to notify

9.5.4.n. 5 Notif.events >>> → 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, Tamper, 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

Delete notification

9.5.4.n. 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.

VdS options

9. 6 vds
----- → 1>Block status
Disable

Set the following options to configure the VdS reporting.

Send block status

9.6. 1 Block status
>Disable<

If the option is enabled, the VdS reporting will be based on channels rather than on events.

Send communication path description

9.6. 2 Comm path desc
>Disable<

The option enables sending the communication path description (GPRS or ETH) with the report.

Chapter 6

Software

Summary

The chapter describes how to connect AXON control panel to PC for programming and firmware upgrading.

Content

- Connecting configuration software 364
- Upgrading AXON / SDPRO firmware 366
 - Installing AAFIash on the PC 366
 - Connecting AXON / SDPRO to the PC 366
 - Archiving current firmware and settings 367
 - Upgrading AXON / SDPRO firmware 367
 - Remote firmware upgrade (RFU) 368
 - Upgrading bootloader 369

Connecting configuration software

There are different PC configuration and administration tools that are designed to make AXON system programming fast and simple, without the need for complex commands or strings. All the information is entered directly from your Windows desktop.

For detailed information on these tools and connection see the appropriate online help.

Caution: Ensure that your software version is compatible with your control panel firmware version, otherwise it may be impossible to upload or download panel settings. Contact your local technical support to receive information on version compatibility.

First connection of the AXON panel to the PC:

1. Install the configuration software.
2. Open the panel housing and plug a USB cable into the USB port on the panel PCB. Connect the USB cable to the PC. If this is the first connection, the system prompts you to find AXON USB drivers to install. Install the driver supplied with the configuration software. A new communication port, ATS CDC Communication Port, will be installed in the system.
3. Open the configuration software.
4. Create a new AXON system and select it.
See the appropriate online help.
5. The installer code used is required to gain access to the panel. The access rights are based on the user group options set.
6. If necessary, set the same encryption key parts 1 and 2 as configured in the panel. See “Encryption key 1” on page 356 for more information about panel encryption keys.

The communication between the panel and the configuration software may require an assistance of the user who is allowed to grant service access, if the option “User code required” is On (see page 301). In this case the following steps must be performed:

1. The authorized user enters the User menu and activates “Service In” option. See *AXON Control Panel Manager Manual* for more details. After this he must log off the menu.
2. The installer can perform the uploading or downloading now.
3. Please note that the communication session is closed after data is uploaded / downloaded. This means that after the Service In timer (programmed in “Inst in-time” described on page 299) expires, a new user authorization is required.

Caution: If the USB communication is interrupted during an upload or download operation, exit the configuration software, establish a reliable connection, and wait 10 seconds for connection to be reinitialized. Next, start the configuration software again.

Upgrading AXON firmware

The AXON panel firmware is upgradeable via USB DFU (device firmware upgrade) interface. Use the AAFlash software to do that.

Access level 4 (manufacturer) applies when changing the operating program software and needs to be executed at the local programming site.

Downgrading is not permitted.

To receive the AAFlash software as well as the latest firmware, contact your supplier.

Cautions

- During the firmware upgrade process all functionality of the alarm system is disabled. Certain access control function may also be disabled.
 - Ensure that mains and battery power supply is stable and uninterrupted during the whole upgrading process unless the process requires to disconnect and reconnect the power supply. The system can be damaged if the power supply fails during the upgrade.
 - Ensure that the USB connection is uninterrupted during the whole upgrading process unless the process requires to disconnect and reconnect the USB cable. The firmware can be damaged if the USB connection fails during the upgrade.
-

Installing AAFlash on the PC

If AAFlash is not installed on the PC, follow the steps below to install it.

To install AAFlash:

1. Ensure that Microsoft .Net 3.5 required by AAFlash has been installed on the PC. If not, use Microsoft Update to install it, or download it from the Microsoft web page and install manually.
2. Run Setup.exe from the AAFlash installation package.
3. Choose the installation directory and proceed with the installation by clicking Next, and then Install.
4. Finish the installation process by clicking Finish.

Connecting AXON to the PC

To connect the panel to the PC for an upgrade:

1. Open the panel housing.
2. Connect LCD keypad to the panel.
3. Connect the mains and the battery power supply to the panel.

4. Wait for installation menu.
5. Check if 4. UltraSync menu is available.
If the menu is not available, please contact technical support, otherwise continue.
6. Disconnect the mains and battery power supply from the panel.
7. Set the RESCUE DIP switch to On.
8. Reconnect mains and battery power supply. Data bus LEDs must start blinking red.

Caution: If they don't, and the panel start booting, wait till the Installation menu shows on the keypad, and proceed from step 5.

9. Plug a USB cable plug into the AXON PCB main board. See "General installation information" on page 8 for more information.

After that, the USB LED turns on, the data bus LEDs are still blinking red.

If this is the first DFU connection, the system prompts you to find AXON USB DFU drivers to install. Choose the driver located in the subdirectory "Driver" or the AAFlash program directory (C:\Program Files\AAFlash\driver by default).

A new USB controller, STM Device in DFU Mode, has been installed in the system.

The panel is ready for the firmware upgrade.

Archiving current firmware and settings

Caution: To prevent any potential failure during programming, installing or initializing new firmware or new feature, take care that the actual firmware (including settings) is archived, and can be reprogrammed.

To archive the panel firmware:

1. While connected to the AXON panel, run AAFlash located in the Start > Programs menu.
2. Create filename for the appropriate firmware back-up *.dfu by clicking "..."
(Browse). Enter file name and click Save.
3. Click Upload.

AAFlash uploads existing firmware including settings in dfu-file.

Upgrading AXON firmware

To upgrade the panel firmware:

1. While connected to the AXON panel, run AAFlash located in the Start > Programs menu.

2. Choose the appropriate firmware file *.dfu by clicking “...” (Browse). Select the appropriate file and click Open.
3. Click Upgrade.

AAFlash erases the existing firmware, writes the new one, and then verifies it.

Next, the current firmware verifies already uploaded DFU package. If verification succeeds, upgrade process is started automatically with following steps:

- a. Panel is restarted. PC is detecting disconnecting the DFU device.
- b. Bootloader is upgrading firmware. During the process databus LEDs and battery LED are lit red, power LED is lit green.
- c. The new, already upgraded firmware is upgrading Data base. During the process, databus LEDs are lit red, battery and power LED are dark.
- d. After successful upgrading process, panel will start automatically. Wait for Installation menu. Check if 4. UltraSync menu is available.

If the menu is not available, contact technical support.

Caution: If firmware upgrade procedure fails, restore the latest archived firmware.

4. Disconnect the USB cable from the panel main board, and then switch off the RESCUE DIP switch.

Remote firmware upgrade (RFU)

The panel firmware can be upgraded remotely via UltraSync or Downloader. Contact your UltraSync service provider for details. See also Downloader Online Help for details.

Cautions

- During the firmware upgrade process all functionality of the alarm system is disabled.
 - After the remote firmware upgrade process is done, the system may remain in the System Fault state for up to 3 minutes.
 - All areas become unset after the remote firmware upgrade. Reset the premises if necessary.
 - The event log is erased during the firmware upgrade. Upload the log before the upgrade.
-

Upgrading bootloader

Certain panels with older bootloader firmware cannot be upgraded to a new firmware. In this case an upgrade of bootloader firmware to a newer version is required. Upgrade bootloader firmware as described below.

Caution: Bootloader is a crucial part of the AXON panel. Make sure that the procedure is performed in the right order (steps 5 to 7), and *the power supply is not removed while step 7 is in progress*, otherwise the system can be damaged.

To upgrade bootloader firmware:

1. Install AAFlash version 2.3.0 or higher.

See “Installing AAFlash on the PC” on page 366.

2. Run the panel in DFU mode.

- a. Disconnect the mains power and batteries from the panel.
- b. Switch the RESCUE DIP switch on and plug a mini-B USB cable into the panel PCB.
- c. Reconnect mains power supply.

The panel is running in DFU mode now, data bus LEDs are blinking.

If data bus LEDs are blinking green and red alternately, the connected PC does not have the required driver installed. In this case, the system prompts you to find AXON USB DFU drivers to install. Choose the driver located in the AAFlash program directory (“C:\Program Files(x86)\AAFlash\driver” by default).

3. Run AAFlash (version 2.3.0 or higher), click “...” (Browse), and open *.dfu file with bootloader provided.
4. Click Upgrade Bootloader.
5. *The program prompts to create backup of the existing application firmware and the database. Click Yes and create a new file for the backup, or No to skip this step.*

If you click Yes, you are prompted to enter a name for a dfu file for the backup. Enter a file name and wait for the instructions to display.

6. *Switch off the RESCUE DIP switch and unplug the USB cable.*
7. *Ensure that both mains power supply and the battery are connected.*

The image version is compared with the current bootloader version. If it is the same or older, the upgrade does not perform.

Sectors of internal flash allocated for bootloader are erased and checked.

New bootloader is flashed.

After the operation is completed, the heartbeat LED starts blinking.

8. Switch on the RESCUE DIP switch and plug USB cable.

The panel restarts. It is now running in DFU mode with new bootloader firmware.

If the backup was created in the step 5, the panel starts to restore the existing application firmware and the database. Otherwise, it is now ready for a new firmware upgrade. See also “Upgrading AXON firmware” on page 367.

Chapter 7

Troubleshooting

Summary

The chapter contains information on resolving known hardware and configuration problems. It also describes how to recover the system when the installer access is lost.

Content

Recovery procedure 372

Device troubleshooting 373

AXON / SDPRO control panel 373

LCD keypads 374

Remote expanders — Models ATS1201E, ATS1210(L)E, ATS1211 374

Remote expander — Model ATS1236 375

Remote expander — Model ATS1238 376

Recovery procedure

If the installer PIN is lost, installer access is impossible. In this case the installer can perform a recovery procedure.

To recover installer access, press and hold the PIN bypass push button (Figure 3, item 16) for 3 seconds. Release the PIN bypass push button after green System LED starts blinking fast. See “LEDs” on page 12 for details.

During the next 3 minutes, it will be possible to access the installer menu using the default code 1278 or 127800. No user is required to provide access to installer programming mode.

This procedure is logged.

Note: The recovery procedure is not allowed if the “Engineer lockout” option is set to Yes.

Cautions

- After the recovery procedure keypad 1 access limitations are reset, which allows you to view and control all areas from this keypad. See “View areas” on page 197 and “Control areas” on page 197 for more details.
 - If the keypad 1 communicates with the panel using a secure channel, the recovery procedure resets its encryption keys. See also “Securing card data” on page 127.
-

Device troubleshooting

AXON control panel

Condition	Possible cause
The LCD keypad has all LEDs flashing, and displays the "System Fault" message	The system data bus line may be connected incorrectly. The address links on the keypad may be incorrectly set. A remote firmware upgrade has been performed. Wait up to 3 minutes for the system to restore. See also "Remote firmware upgrade (RFU)" on page 368.
The panel is not communicating with keypads or expanders	The system data bus line may be connected incorrectly. Keypad or expander numbers to be polled may not be programmed, or may not match the addresses set on the units. There is an earth loop in cabling.
The keypads or expanders appear to be going offline and online (indicated by keypad or expander fail LED's)	The system data bus line may be connected incorrectly. The termination may be incorrect. TERM links may not have been removed where necessary. See "Cabling" on page 26.
Zone goes into alarm while the area is unset	The zone is wired incorrectly causing a tamper condition (open circuit or short circuit) instead of active condition. EOL resistors may be installed incorrectly. See "Cabling" on page 26.
The panel is not reporting to the central station	The telephone line connections may be wired incorrectly. See "Cabling" on page 26. The central station receiver does not support the programmed protocol. The account number in "Accounts" on page 330 may be programmed incorrectly. The phone number for the central station receiver is wrong. No central station is programmed to report the event. See "Central station" on page 329. The zone is not programmed to be reported. See "CS report" on page 235. Wrong IP configuration, for example, IP address conflict. See also "LCD keypads" on page 374.

LCD keypads

Condition	Possible cause
All the LEDs on the keypad are flashing	The DIP switches may be incorrectly set (the address set on the keypad may be incorrect and therefore polling to the keypad is not being acknowledged). The system data bus line may be connected incorrectly. The keypad is not being polled (it may not have been included in keypads to be polled when programming keypads).
LEDs do not appear to be indicating the correct condition	The keypad type may have been defined incorrectly: LCD keypad must be set to Yes.
The keypad appears to be going off-line and on-line (indicated by the “Keypad fail” message on the LCD)	The termination may be incorrect. See “Cabling” on page 26.
An error is indicated when a code is entered on the keypad (seven beeps)	An invalid PIN may have been used. The keypad may not have been programmed with an alarm group. The alarm group of the PIN may not permit access at this keypad.
An error “IP conflict” is indicated on the keypad. The IP connection is unavailable.	A wrong IP address is configured. The IP address conflict must be resolved. The state restores in 3 minutes after the conflict is resolved.
An error “WAN fault” is indicated on the keypad.	The connection to UltraSync has been lost.

Remote expanders — Models ATS1201E, ATS1210(L)E, ATS1211

Condition	Possible cause
The Tx LED on the expander is not flashing	The DIP switches may be incorrectly set (the address recorded on the expander may be incorrect and therefore polling to the expander is not being acknowledged). The system data bus cable may be connected incorrectly. The expander is not programmed to be polled.
Tx and Rx LEDs are not operating	No power or low power. The system data bus cable may be connected incorrectly, or the power supply is faulty (mains or battery).
The expander appears to be going off-line and on-line (indicated by “Expander fail” on a LCD keypad)	The termination may be incorrect. See “Cabling” on page 26.

Condition	Possible cause																			
Some or all expander zones are permanently in tamper (or permanently in alarm if “Input mode” on page 207 is set to Single NO or Single NC).	The zone numbers for the expander have been calculated incorrectly, and zone type numbers have therefore been assigned to the wrong zones in the zone database. See “Configuration” on page 33.																			
	The end-of-line resistors are wrong, or a wrong resistor value is programmed in “End of line resistor” on page 207.																			
	There is a problem with wiring the zones. To check the voltage or resistor values, see “Zone connection” on page 27.																			
	The ATS1202 expansion modules (if fitted) have the DIP switches incorrectly set.																			
	<table><tr><td>Expansion module:</td><td>1st</td><td>2nd</td><td>3rd</td></tr><tr><td>DIP switch 1</td><td>On</td><td>Off</td><td>Off</td></tr><tr><td>DIP switch 2</td><td>Off</td><td>On</td><td>Off</td></tr><tr><td>DIP switch 3</td><td>Off</td><td>Off</td><td>On</td></tr><tr><td>DIP switch 4</td><td colspan="3">not used</td></tr></table>	Expansion module:	1st	2nd	3rd	DIP switch 1	On	Off	Off	DIP switch 2	Off	On	Off	DIP switch 3	Off	Off	On	DIP switch 4	not used	
Expansion module:	1st	2nd	3rd																	
DIP switch 1	On	Off	Off																	
DIP switch 2	Off	On	Off																	
DIP switch 3	Off	Off	On																	
DIP switch 4	not used																			
Four-way relay modules (ATS1810) being used with the expander do not function, but some of the LEDs on the module appear to be permanently on	DIP switch B on the expander is set to On (DIP switch B should only be On if 8-way relay (ATS1811) modules or 16 open collector modules (ATS1820) are being used).																			
8-way relay modules (ATS1811) or 16-way open collector modules (ATS1820) connected to the expander do not function	DIP switch B on the expander has not been set to On.																			

Remote expander — Model ATS1236

Condition	Possible cause and solution
“DGP fault” event appears in the control panel log.	Expander configuration got corrupted. In this case the DGP needs to be reconfigured and the wireless devices re-enrolled. To clear the fault, go to Expander settings, “Default expander” (described on page 211).
A wireless device cannot be enrolled	An unsupported device type has been enrolled. If you enroll an unsupported device type into ATS1236 (for example, sirens, key fobs, etc.), ATS1236 will stop accepting sensors from that position onwards. To unblock this state, you need to either remove the unsupported device through ATS85xx configuration software, or default the ATS1236 device.

Remote expander — Model ATS1238

Condition	Possible cause and solution
The expander is offline after it has been remotely added from the Downloader software.	The panel establishes the communication with the ATS1238 expander only during the system start-up.
The expander is not visible by the panel after it has been remotely removed from the Downloader software.	Restart the panel to initiate the communication with the ATS1238 expander.

Chapter 8

Regulations

Summary

These pages describe settings and actions required by particular regulations and norms.

Content

Options affected by EN 50131 regulations	378
EN 50131 Grade 2	378
EN 50131 Grade 3	379
EN 50136 policy	381
Transmitter polling interval requirements	381
EN 50131 Grade 3 certified components	382
EN 50131 compliance precautions	383
Options affected by other regulations	384
ACPO policy	384
INCERT policy	384
SBSC policy	385

Options affected by EN 50131 regulations

EN 50131 Grade 2

Required settings

The following options and values are mandatory for EN 50131-1 Grade 2 regulations.

- Period, see “Transmitter polling interval requirements” on page 381.
- View areas and Control areas settings are identical
- Buzzer silent, never
- Quick set mode, off
- Function keys, all set to None
- ACK on keypad, set to None for non-LCD keypads
- SMS control, disabled for all users
- User group options, 25. No OP/CL reports option set to No
- Zone type, no zones have Fire or Medical types.
- Inhibit, set to No for all zones with type 5. Panic, 6. 24H
- Swinger shunt, set to Yes for all zones
- ACK on keypad, set to None for all zones with type 9. Keyswitch
- Entry time, 45 s maximum
- Entry alarms, Instant
- Schedule activation, set to No for all schedules.
- Activation, external siren 90 to 900 s
- Delay, external siren 600 s maximum
- Armed display, set to 00'00
- Mains reporting delay, 3600 s maximum
- User code required, enabled
- Arm display, always
- Alarm list, disabled
- Ready to set options, all enabled except zone technical alarm, which is optional
- Inhibit includes, all allowed except engineer reset, which must be disabled
- Pending alarms, enable EN50131
- Report exit fault, EE fault
- Swinger shunt ≥ 3
- Rep. restore, on ACK
- Remote configuration, No
- Report siren fault, Fault
- Line fault, enabled per path used
- Line fault delay, 0 s

It is required to apply the following supervision settings for wireless DGPs:

- Short supervision: 20 minutes
- Long supervision: 2 hours
- Smoke supervision: 4 hours

Refer to appropriate sections and manuals.

Caution: When any option, any additional function or any additional zone type in this section does not comply with the EN 50131 requirements, the EN 50131 Grade 2 label must be removed from the system.

Additional functions

The Wireless PIR Camera functionality brings along video verification feature, this additional function is fully available without compromise to standards the system complies to.

The Wireless PIR camera system consists of the following:

- AXON series control panel
- AT51238 Advanced Wireless DGP
- TX-2344-03-1 Wireless PIR Camera
- AT573X0 GSM/GPRS Module

These PIR camera settings have no influence on EN 50131 compliance:

- Frame rate for all event types
- Picture resolution for all event types
- Pic auto deletion
- Cameras
- Picture destination port
- Max IP Picture reports per 24h, Max GPRS Picture reports per 24h

EN 50131 Grade 3

Required settings

The following options and values are mandatory for EN 50131-1 Grade 3 regulations:

- All Grade 2 required settings (see “EN 50131 Grade 2” on page 378).
- PIN length should be 6 digits minimum. See also “PIN length”.
- User group options, set (6) Isolate, (22) SMS reporting, (23) SMS control to No for all user groups except Installer.
- Anti mask, set to Yes for all I&HAS movement detectors
Note: Masking signals are processed as faults as per EN 50131-3
- Exit time 1, ≤ 180 s
- Mains reporting delay, ≤ 1 h
- View EE timer, set to Off
- Ready to set options, set Zone masking condition to Yes
- Inhibit includes, set Zone masking condition to Access Level 2
- Battery test should be performed daily. See “Battery test” on page 186 for details.

The following features are not allowed (not evaluated):

- Keyswitch zone types to set and unset the system. See “Zone types” on page 49.
- Presetting indication and any automatic override of set prevention.

Refer to Table 31 below for all supported options for notification requirements.

Note: The requirements included in each security grade and option represent the minimum requirements. It is permissible to include additional warning device, or to select higher performance alarm transmission system in any security grade or option, for example, to achieve a shorter reporting time.

Table 31: EN 50131-1 options

Notification equipment (Alarm reporting)	Grade 3 options				
	A	B	C	D	E
Remotely powered audible WD (warning device)	2	Optional	Optional	Optional	Optional
Self-powered audible WD (warning device)	Optional	1	Optional	Optional	Optional
Alarm transmission system (according to EN 50136-2)	SP3	SP3	DP2 (primary path SP3, backup SP2)	SP4	DP3 (primary path SP4, backup SP2)

Legend:

- SP: Single path alarm transmission system
- DP: Dual path alarm transmission system

The key variations of cards and keys are the following:

- ATS147x range (used with ATS1135 and ATS119x): 67 million
- ATS145x card range (used with ATS1136, ATS1125, and ATS118x): 280 trillion

The cards make use of 26-bit (to 48-bit) Hitag protocol.

The installer (user level 3) commissions the system with appropriate additional functions.

The end-user (user level 2) can make use of all these functions.

The Installer can only make use of these functions when he has an access granted by end-user.

RAS required setting

The keypad/RAS must be mounted within the secure premises, on the entry/exit route.

Each arming scenario described below meets EN 50131 requirements.

- Card and PIN mode: Card and PIN always
Note: This setting must be applied manually by the installer after the appropriate cards are defined in the system.
- One time badge to set/unset: Off
- Three time badge to set: Set
- Quick set mode: Off
- Key unset: Off
- Forced set: Off
- Autoreset retry on system fault: 15 minutes
- Autoreset user retry: Disable

See also the appropriate RAS manual for more details.

EN 50136 policy

Required settings:

- “Retry count”: 1
- “Heartbeat time”: According Table 32 below.
- “Frequent Heartbeat time”: According Table 32 below.
- “Firewall” (IP): Yes
- “Reply on PING” (IP): No
- “Firewall” (GPRS): Yes
- “Reply on PING” (GPRS): No
- “Encryption”: Yes
- “Encryption key 1” must be set.

See also “Transmitter polling interval requirements” below.

Transmitter polling interval requirements

Transmitter polling interval must be set according to specified requirements for different alarm transmission systems. Table 32 below lists all required settings for the appropriate standards and diallers.

Table 32: Transmitter polling settings

Standard and category	Required polling interval	Comm. path and dialler	Option	Required value
EN 50136-2:2013				
SP3	30 min	IP built-in, or GPRS via ATS73X0	Heartbeat time	00:29'00
SP4	3 min	IP built-in, or GPRS via ATS73X0	Heartbeat time	00:02'30
SP5	90 s	IP built-in, or GPRS via ATS73X0	Heartbeat time	00:00'10
SP6	20 s	IP built-in	Heartbeat time	00:00'10

EN 50131 Grade 3 certified components

The AXON EN 50131 Grade 3 system exists out the following components.

Intrusion control panels

- ATS1700, ATS3700: Control panel

Keypads / readers (RAS, remote arming station)

Panel can support up to 8 or 16 RAS devices at the same time, depending on intrusion panel, regardless of type (independent of other expanders).

- ATS1125: LCD keypad
- ATS1136: LCD keypad
- ATS1190/1192: Smart Card reader
- ATS1151/ATS1156: Keypad
- ATS118x: Smart Card reader series

Remote expanders (DGP, data gathering panel)

Panel can support up to 7 or 15 DGP devices, depending on intrusion panel, regardless of type (independent of other expanders).

- ATS1201E: 8 to 32 zone DGP expander with 3 A PSU, small enclosure, EN 50131 Grade 3
- ATS1204E: 8 to 32 zone DGP expander with 3 A PSU, large enclosure, EN 50131 Grade 3

I/O expanders

Panel can support up to 3 I/O devices depending on the type.

- ATS608: Plug in 8-zone expander
- ATS624: 4 relay board
- ATS626: 16 open collector output board

Reporting devices

Panel can support 1 GSM device connected onto MI bus.

- ATS7310: GSM communication device
- ATS7340: GSM communication device
- ATS7440: IP/GPRS alarm dialer

When any option, any additional function or any additional zone type in this section does not comply with the EN 50131 requirements, the EN 50131 Grade 3 label must be removed from the system. See also “EN 50131 compliance precautions” on page 383.

EN 50131 compliance precautions

Installation

To install an EN 50131 compliant system, please make sure that all system components are EN 50131 compliant. See “EN 50131 Grade 3 certified components” on page 382 for more details.

Programming

Make sure that all system settings are in line with regulatory compliance guidelines. See “EN 50131 Grade 3” on page 379 for more details.

Size of log / event history

For full EN 50131 Grade 3 compliance, the system must store at least 500 events.

Marking

It is only allowed to mark the system with the EN 50131 Grade 3 label, if the following requirements are met:

- All system components are EN 50131 compliant. Refer to “EN 50131 Grade 3 certified components” on page 382.
- All settings are done according to “EN 50131 Grade 3” on page 379.

If any of these two items is not valid, the EN 50131 Grade 3 label must be removed from the system.

Options affected by other regulations

WARNING! Fire alarm and smoke detection products used with AXON 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. KGS accepts no liability for any damages caused by incorrect application of the products.

ACPO policy

Required settings are all EN 50131 Grade 2 settings with the following modifications:

- Entry alarms, Delayed
- Engineer reset, tamper enabled
- Alarm confirm:
 - AB mode, enabled for all relevant areas
 - AB time, 30 min minimum, 60 min maximum
 - EE Confirm, enabled
 - TA confirm, enabled

Note: ACPO policy allows a higher-level manager to become a level 3 user. Also, level 3 user menu access may be allowed without level 2 user authorization if it is provided by appropriate written agreement from the customer.

INCERT policy

The required settings for INCERT Grade 2 are all EN 50131 Grade 2 required settings, and settings for INCERT Grade 3 are all EN 50131 Grade 3 required settings, with the following modifications:

- Battery test frequency: Everyday
- User code required: Enabled
- Alarm list: Disabled
- Ready to set options: FTC and Battery fault set to On
- Inhibit includes: Battery fault must be set to Access level 2
- Pending alarms: Enable EN 50131
- Line fault: Set to If used or On
- Line fault: Set to On

See also “EN 50131 Grade 2” on page 378 and “EN 50131 Grade 3” on page 379.

For INCERT T031 installations the following devices should be mounted in metal housings only: ATS7200E, RC213, ATS1810, ATS1811, ATS1202, ATS1330, ATS1740, ATS1743.

SBSC policy

Larmklass 2

Required settings are all EN 50131 Grade 2 settings with the following modifications:

- Entry alarms: Instant
- Reporting delayed: No

See also “EN 50131 Grade 2” on page 378.

Larmklass 3

Required settings are all EN 50131 Grade 3 settings with the following modifications:

- Entry alarms: Instant
- Reporting delayed: No

See also “EN 50131 Grade 3” on page 379.

Chapter 9

Programming maps

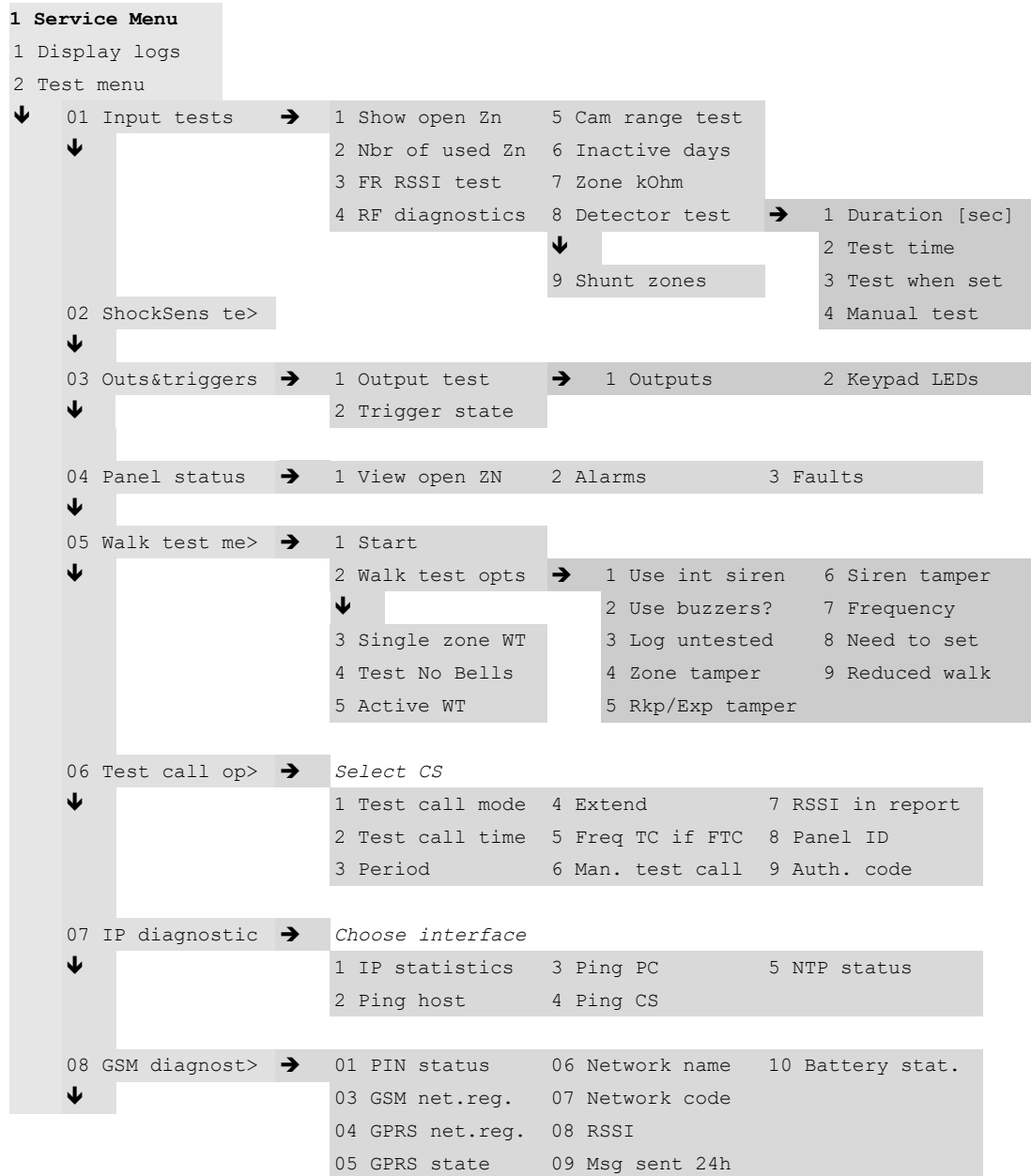
Summary

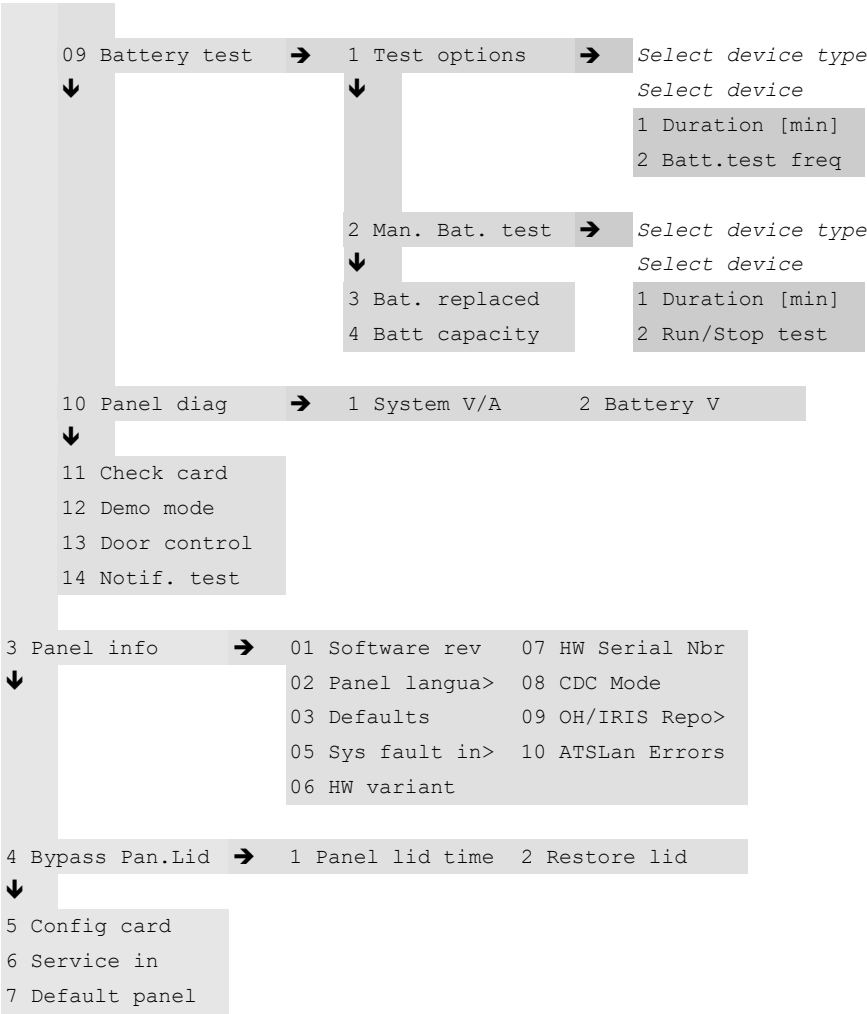
The chapter contains programming maps for different programming methods.
See also “Programming methods” on page 132.

Content

Keypad programming map 388
Keypad programming option list 404
WebApp programming map 413

Keypad programming map





2 Device Menu

1 Inst. Remotes

2 Edit Rkp&Exp

1 Keypad devices

↓ 0 Add keypad

Select keypad

1 Keypad type

2 Keypad address

3 Keypad options →

↓

4 Keypad menu

5 Reset Comm Key

6 Delete keypad

01 Keypad name 05 View AG

02 Tamper area 06 Ctrl areas

03 Detect tamper 07 Control AG

04 View areas 08 Control opt →

↓

09 EE PIN lock 19 EE 1 buzzer

10 Isolate Rkp 20 EE 2 buzzer

11 Buzzer silent 21 1+3 keys

12 Quick set 22 RTE

13 Function keys 23 Backlight

14 Area ind.LED1 24 Nightlight

15 Area ind.LED2 25 Card beep opt

16 Status ind. 26 Idle scr opt →

17 LCD backlight 27 Schedule

18 ACK on keypad

1 Card&PIN mode

2 Logoff time

3 1xset/unset

4 3xbadge set

5 Key/Card Mode

6 Card Tamp.Lock

7 Linked Reader

2 Exp devices

↓ 0 Add expander

Select expander

1 Expander type

2 Exp address

3 Expander range

4 Exp settings 0 →

5 Expander menu

7 Delete Exp

1 Expander name 4 Isolate Exp

2 Tamper area 5 Input mode

3 Detect tamper 6 EOL

1 Logo

2 Custom msg

3 Time and date

4 Text bkgd

5 Text color

3 DC/LC Exp Rdrs

0 Add reader

Select reader

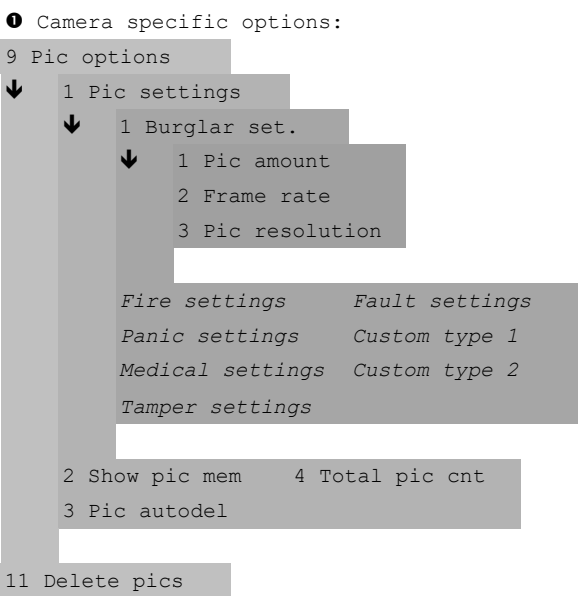
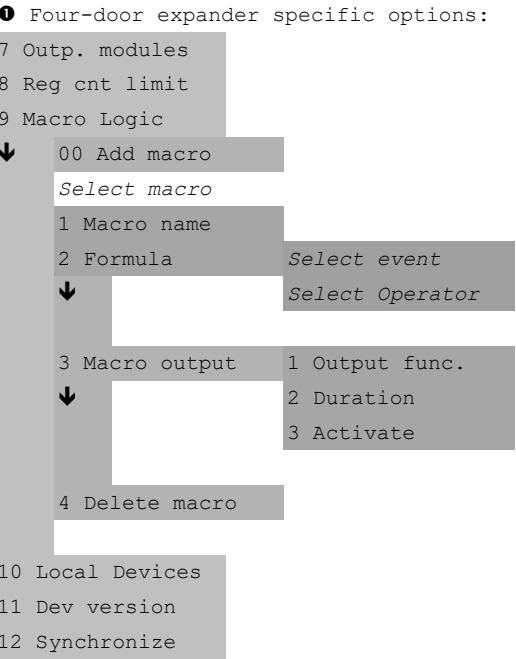
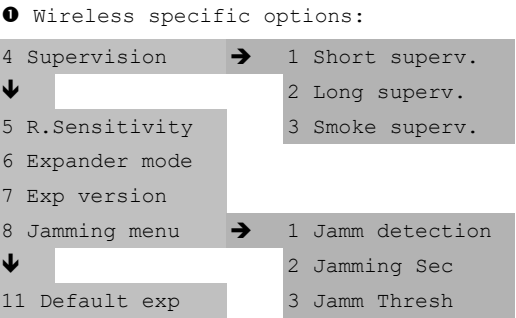
2 Reader address

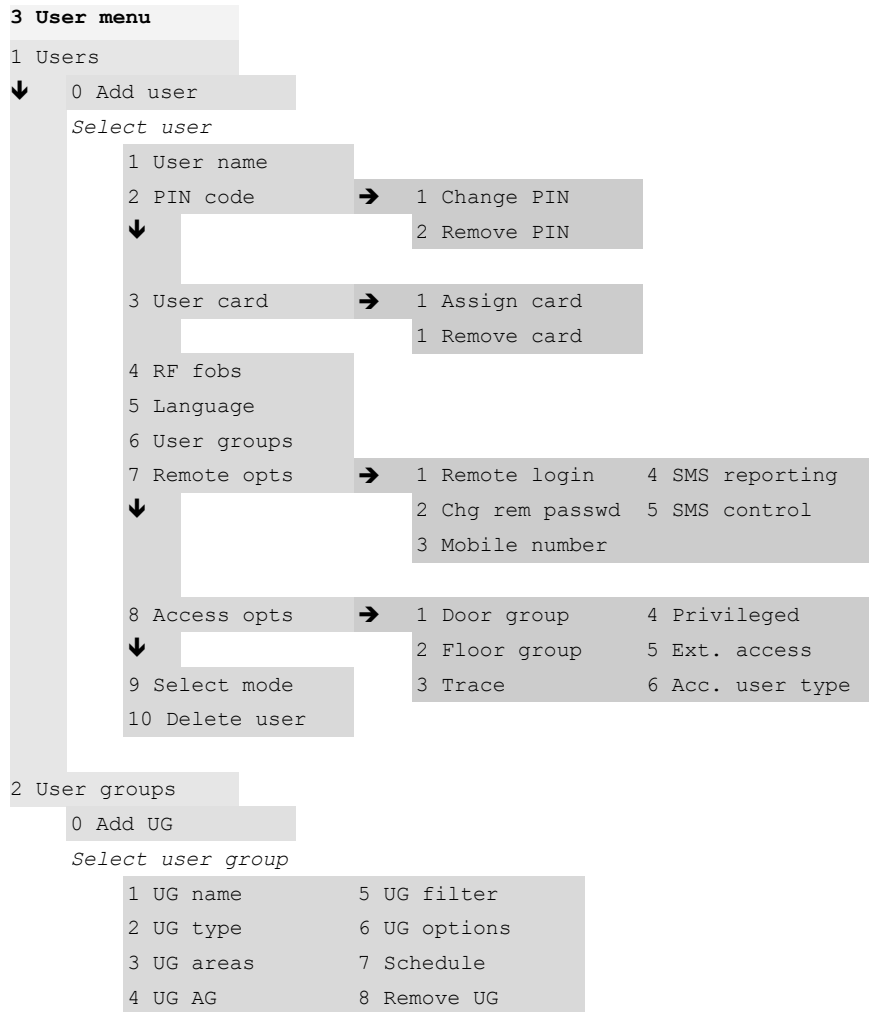
3 Reader options →

5 Delete reader

1 Reader name 2 LCD

3 Databus EOL





4 Zones&Areas**1 Zones Menu****↓ 0 Add zone***Select zone*

Common options

- 1 Zone name
- 2 Zone type
- 3 Isolated
- 4 Zone location
- 5 Zone areas
- 6 Zone options →



- 8 Copy →
 - 1 Copy par. from
 - 2 Block assign



- 9 Move zone
- 10 Delete zone

Shock sensor options

- 7 Grs&Pls opts →
 - 1 Pulse count
 - 2 Gross level

Wireless sensor options

- 7 RF details →
 - 1 Sensor ID
 - 2 Sensor type
 - 3 Sensor mode
 - 4 Supervision
 - 5 Sensor opt
 - 6 Remove RF dev

- 1 Inhibit
- 2 Isolate
- 3 Excl. in PS1
- 4 Excl. in PS2
- 5 DblKnock
- 6 Swinger shunt
- 7 Anti mask
- 8 Zone pairing
- 9 Chime
- 10 Soak test
- 11 Eng walk test
- 12 User walk
- 13 Shock sensor
- 14 Extend EE
- 15 Final door
- 16 Key latch
- 17 Key set
- 18 Key unset
- 19 Tech full set
- 20 Tech unset
- 21 Tech part set
- 22 Keypad LCD
- 23 Log
- 24 CS report
- 25 Delay timer
- 26 ACK on keypad
- 27 ACK by user
- 28 Sensor type
- 29 Virtual zone
- 30 Held open
- 31 EE set check
- 32 Alarm in PS1
- 33 Alarm in PS2
- 34 Report as
- 35 Auto test
- 36 Shunt
- 37 View isolated
- 38 Limit reports
- 39 Input mode
- 40 EOL
- 41 Indication
- 42 Report code

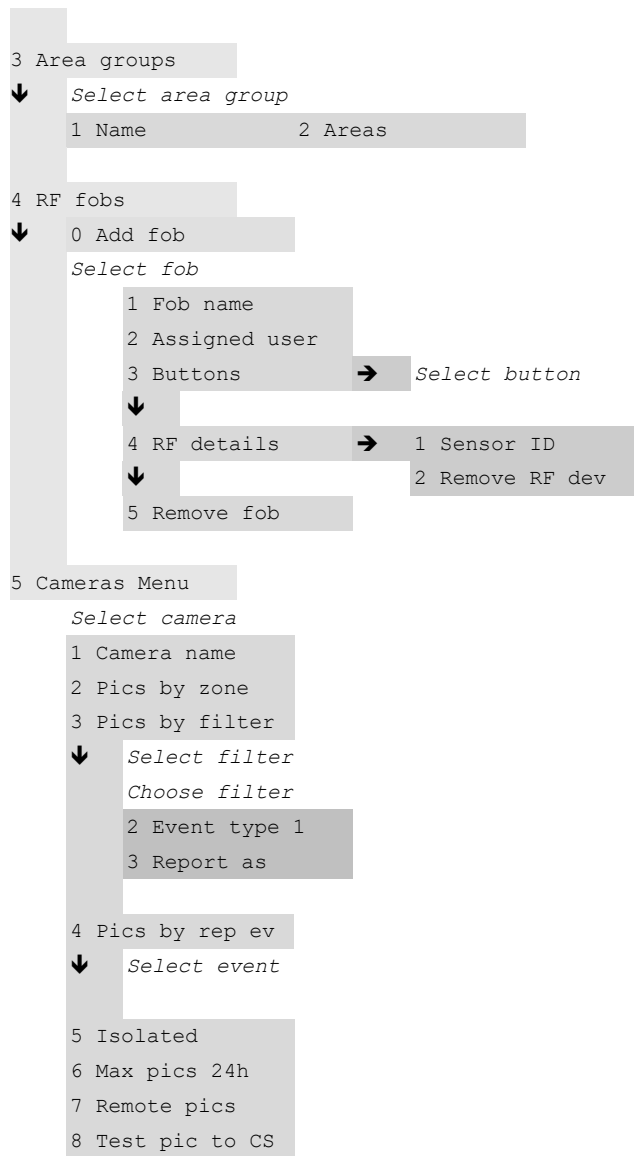
2 Areas**↓ Select area**

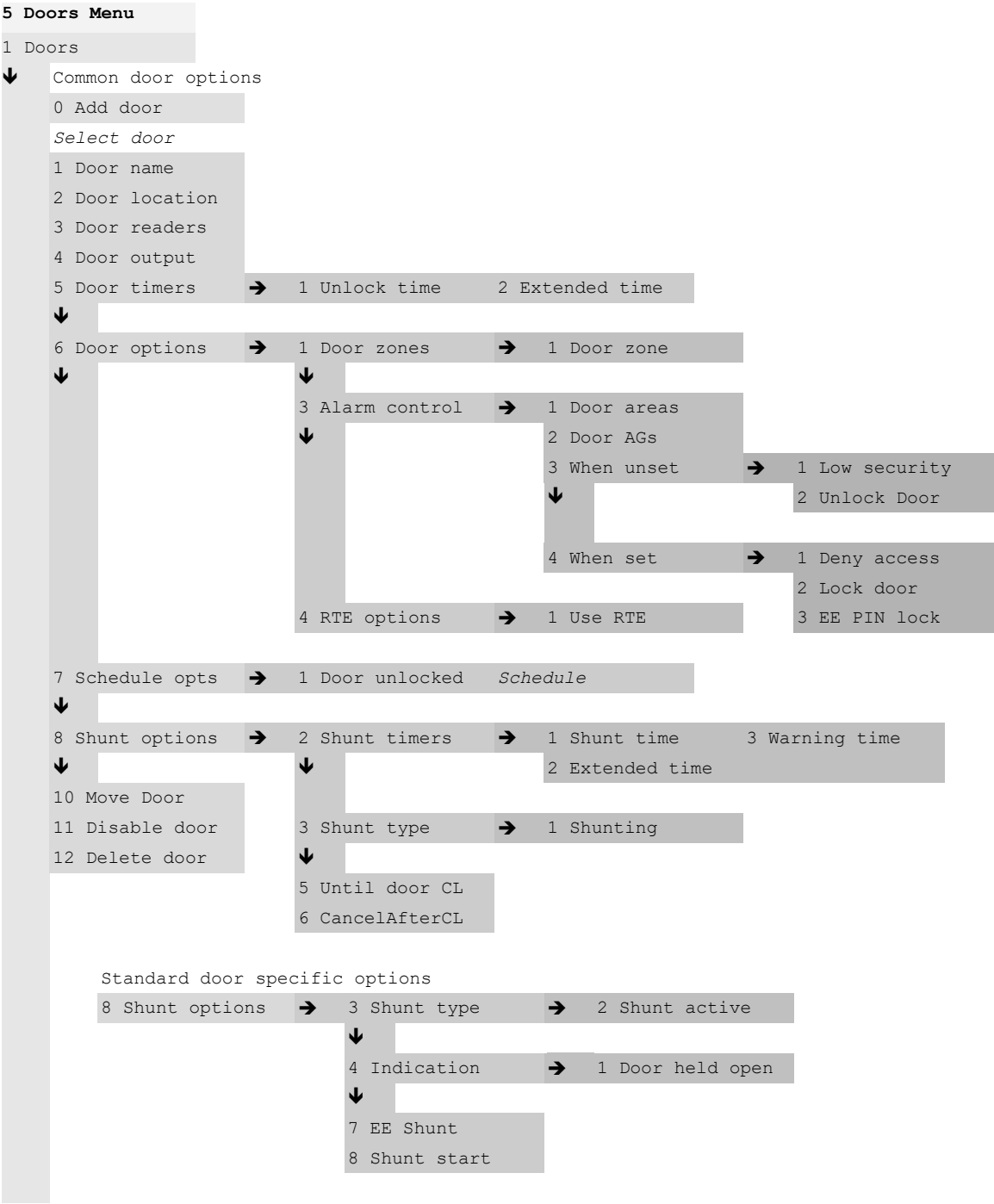
- 1 Area name
- 2 Exit time
- 3 Entry time
- 4 Other timers →
- 5 Set/unset opts →
- 6 Hierarchy
- 7 Limits →
- 8 Schedule

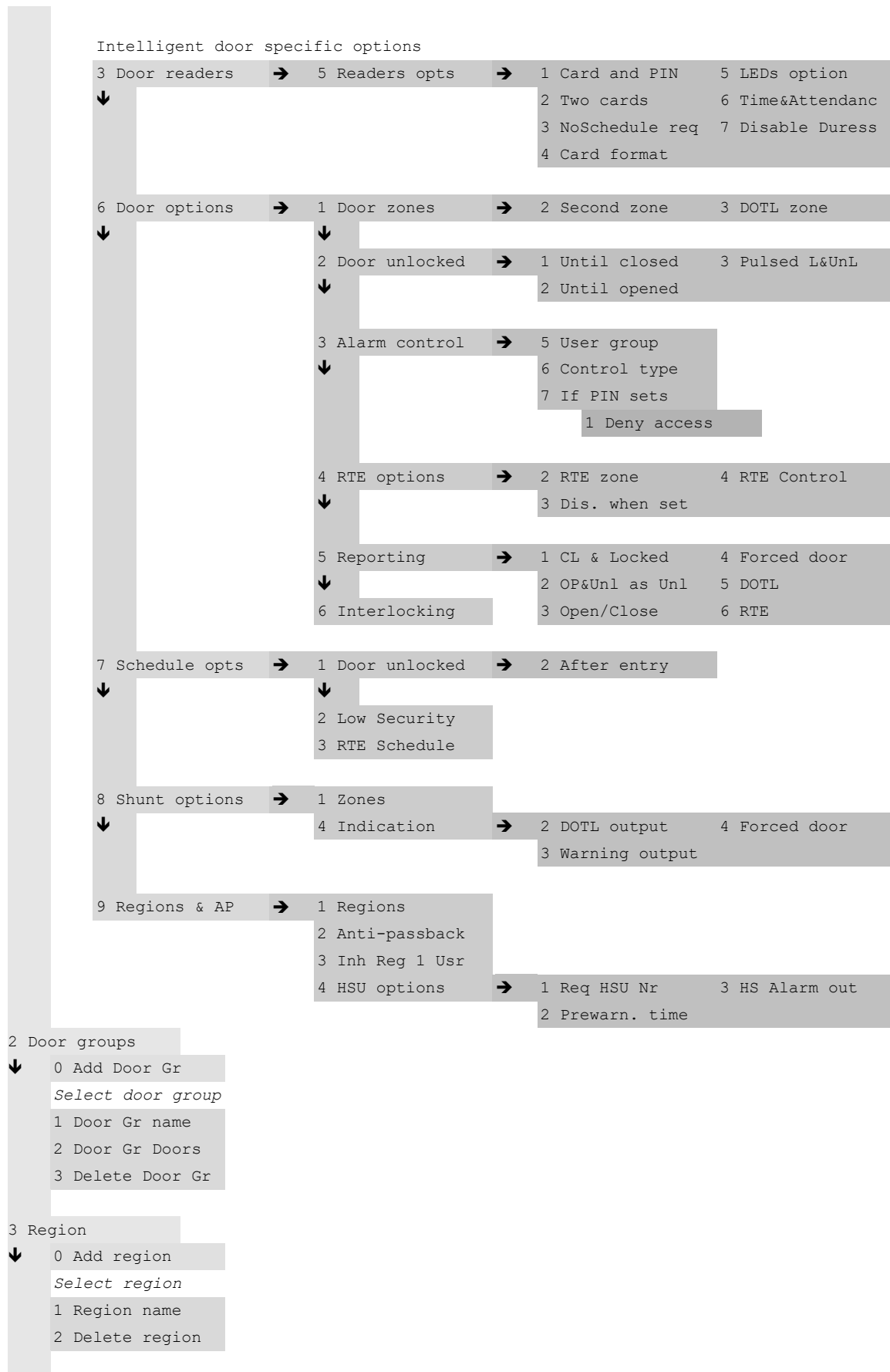
- 1 Warning time
- 2 Prealarm time
- 3 Unset delay

- 1 Entry alarms
- 2 Set retry
- 3 Silent autose
- 4 Dual unset
- 5 Confirm alarm

- 1 Inhibit limit
- 2 Isolate limit
- 3 Shunt limit







4 Floors

↓ 0 Add floor

Select floor

1 Floor name

2 Delete floor

5 Floor groups

0 Add Floor Gr

Select floor group

1 Floor Gr name

2 Floor Gr Fls

3 Delete Fl Gr

6 Outs&filters

1 Cond filters

↓ 0 Add filter

Select filter

1 Filter name

2 Formula → 0 Add event

↓ Select event

3 Invert Select operator

4 Delete filter

2 Outputs

↓ 0 Add output

Select output

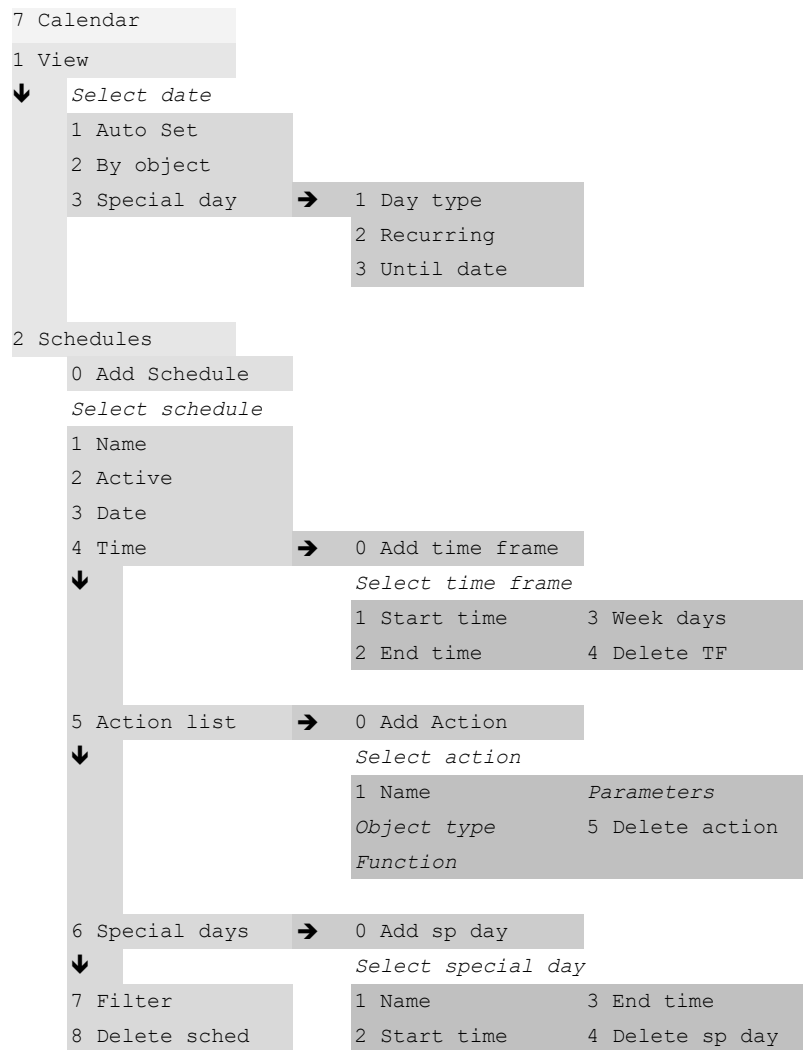
1 Output name	6 Mode	
2 Output loc	7 Parameters	→ 1 Delay time
3 Invert output	8 Log limit	2 Active time
4 Start filter	9 Delete output	3 Retriggerable
5 Stop filter		

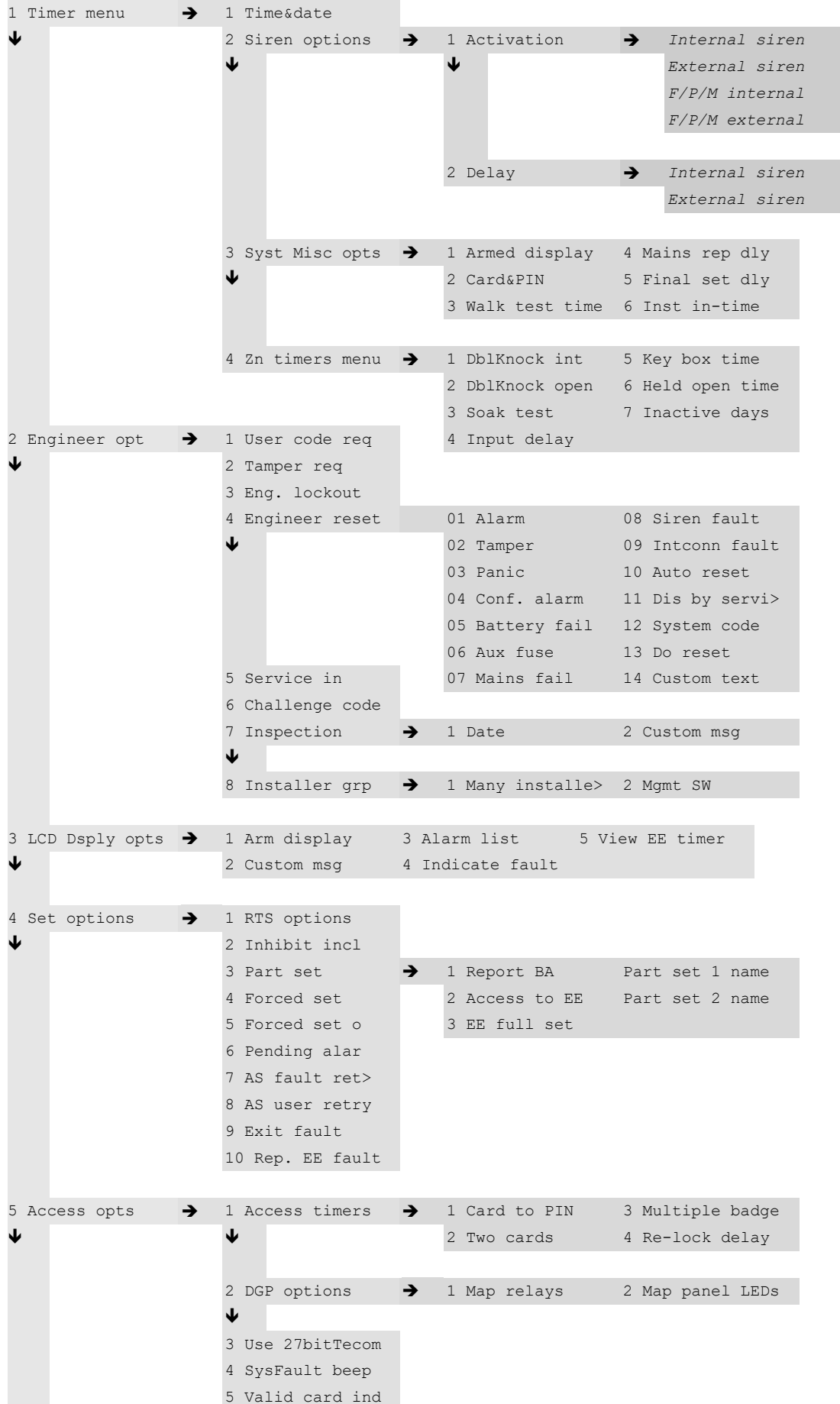
3 Triggers

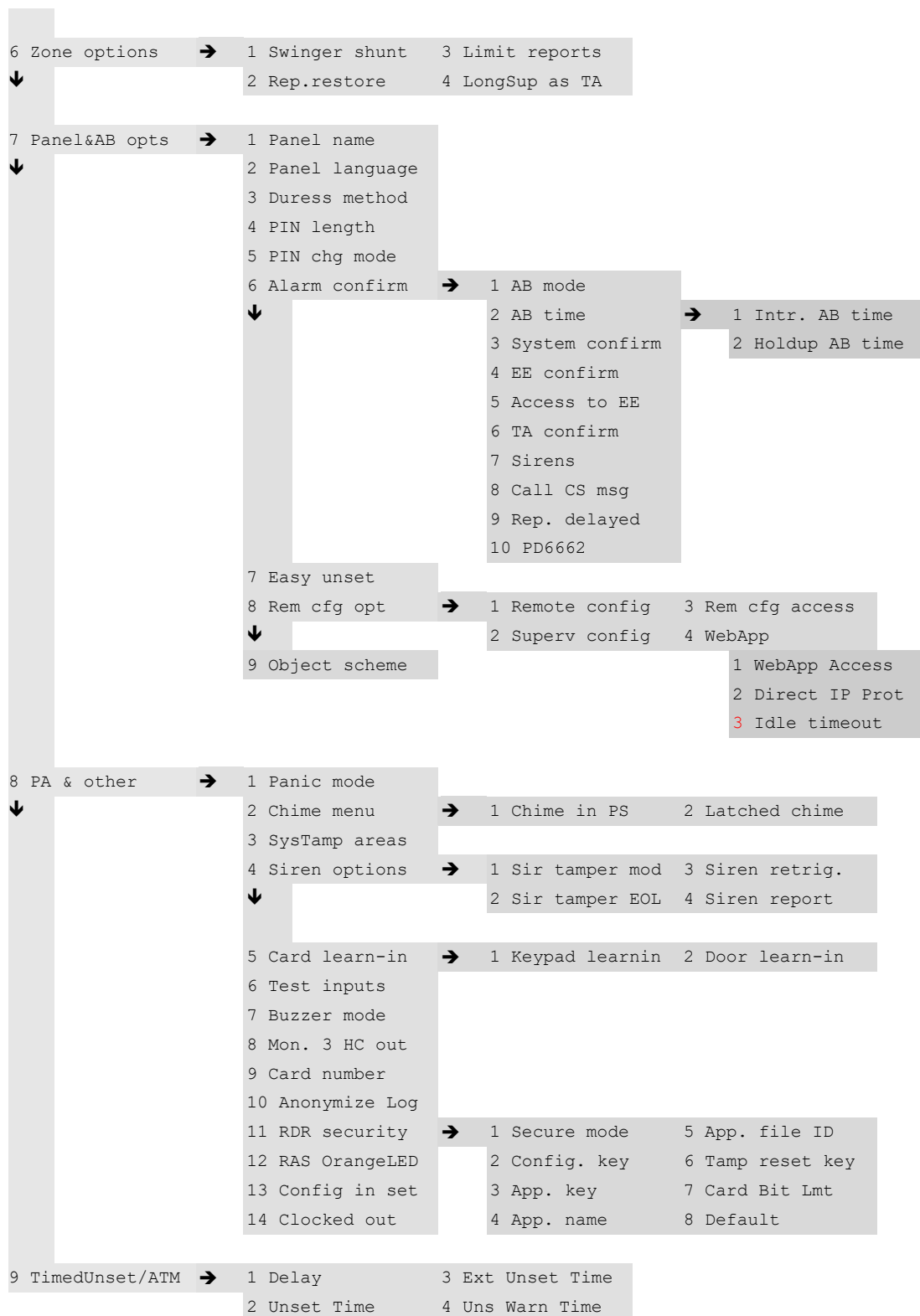
0 Add trigger

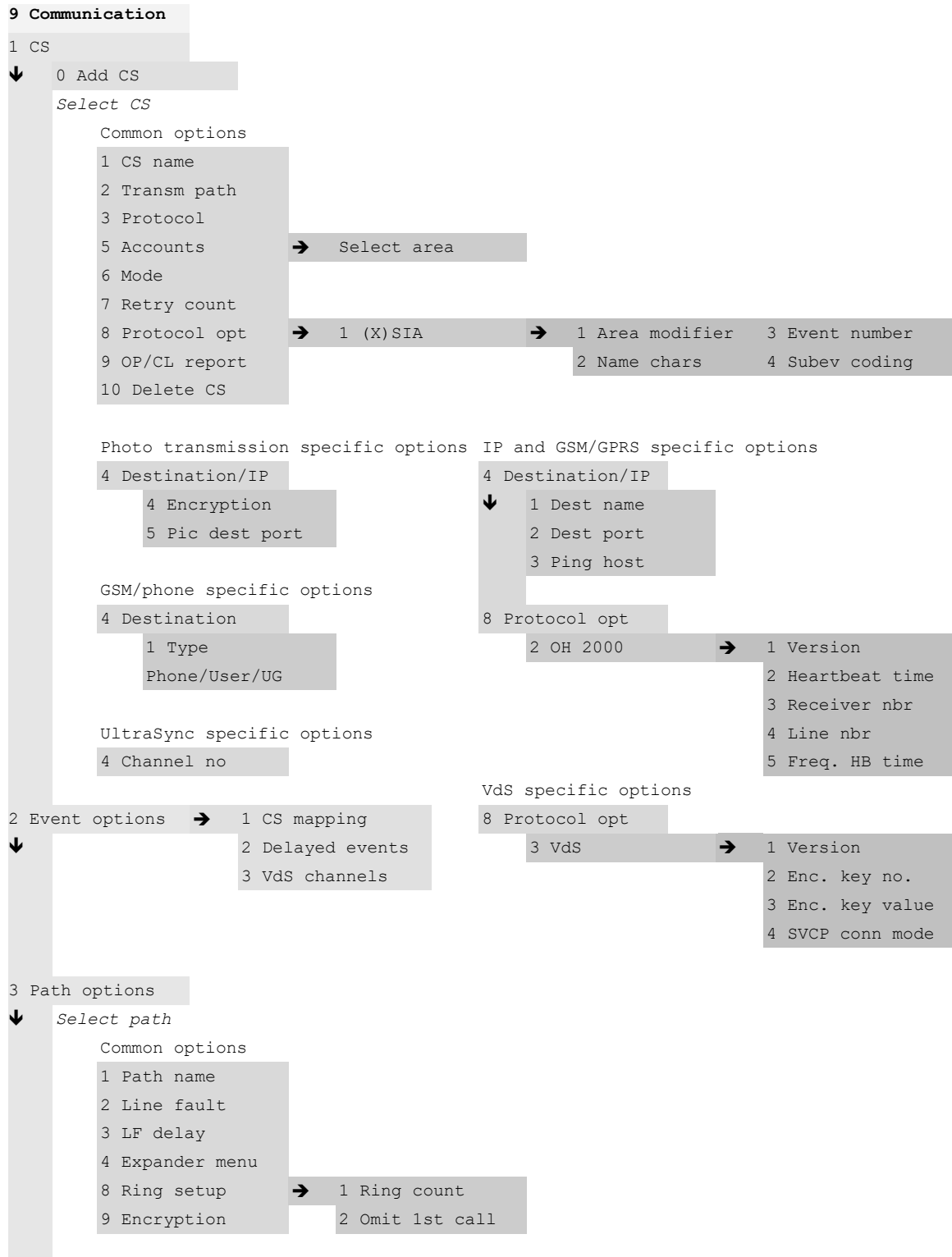
Select trigger

1 Trigger name	3 User group
2 Schedule	4 Delete trigger

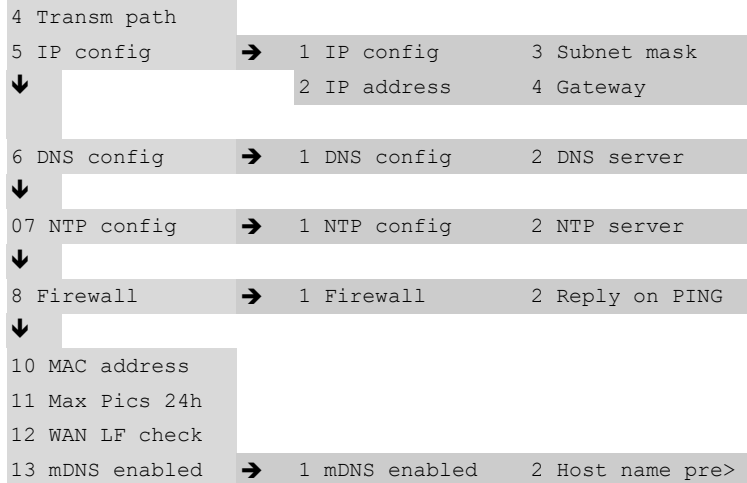


8 Sys.opts Menu



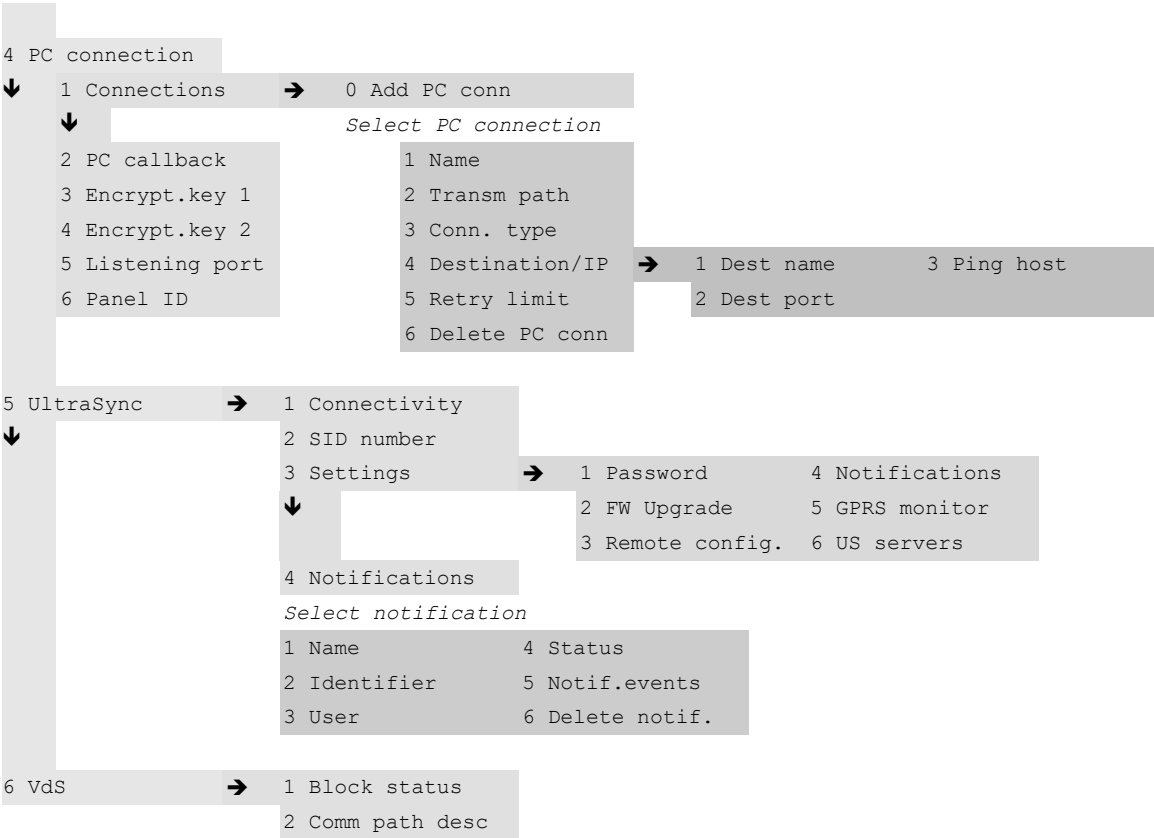


IP specific options



GSM/SMS/GPRS specific options





Keypad programming option list

The programming option list contains all programming options with the key sequences.

1 Service Menu

- 1.1 Display logs
- 1.2 Test menu
 - 1.2.01 Input tests
 - 1.2.01.1 Show open Zn
 - 1.2.01.2 Nbr of used Zn
 - 1.2.01.3 FR RSSI test
 - 1.2.01.4 RF diagnostics
 - 1.2.01.5 Cam range test
 - 1.2.01.6 Inactive days
 - 1.2.01.7 Zone kOhm
 - 1.2.01.8 Detector test
 - 1.2.01.8.1 Duration [sec]
 - 1.2.01.8.2 Test time
 - 1.2.01.8.3 Test when set
 - 1.2.01.8.4 Manual test
 - 1.2.01.9 Shunt zones
 - 1.2.02 ShockSens te>
 - 1.2.03 Outs&triggers
 - 1.2.03.1 Output test
 - 1.2.03.1.1 Outputs
 - 1.2.03.1.2 Keypad LEDs
 - 1.2.03.2 Trigger state
 - 1.2.04 Panel status
 - 1.2.04.1 View open ZN
 - 1.2.04.2 Alarms
 - 1.2.04.3 Faults
 - 1.2.05 Walk test me>
 - 1.2.05.1 Start
 - 1.2.05.2 Walk test opts
 - 1.2.05.2.1 Use int siren
 - 1.2.05.2.2 Use buzzers?
 - 1.2.05.2.3 Log untested
 - 1.2.05.2.4 Zone tamper
 - 1.2.05.2.5 Rkp/Exp tamper
 - 1.2.05.2.6 Siren tamper
 - 1.2.05.2.7 Frequency
 - 1.2.05.2.8 Need to set
 - 1.2.05.2.9 Reduced walk
 - 1.2.05.3 Single zone WT
 - 1.2.05.4 Test No Bells
 - 1.2.05.5 Active WT
 - 1.2.06 Test call op>
 - 1.2.06.n.1 Test call mode
 - 1.2.06.n.2 Test call time
 - 1.2.06.n.3 Period
 - 1.2.06.n.4 Extend
 - 1.2.06.n.5 Freq TC if FTC
 - 1.2.06.n.6 Man. test call
 - 1.2.06.n.7 RSSI in report
 - 1.2.06.n.8 Panel ID
 - 1.2.06.n.9 Auth. code
 - 1.2.07 IP diagnostic
 - 1.2.07.n.1 IP statistics
 - 1.2.07.n.2 Ping host
 - 1.2.07.n.3 Ping PC
 - 1.2.07.n.4 Ping CS
 - 1.2.07.n.5 NTP status
 - 1.2.08 GSM diagnost>
 - 1.2.08.01 PIN status
 - 1.2.08.03 GSM net.reg.
 - 1.2.08.04 GPRS net.reg.
 - 1.2.08.05 GPRS state
 - 1.2.08.06 Network name
 - 1.2.08.07 Network code
 - 1.2.08.08 RSSI
 - 1.2.08.09 Msg sent 24h
 - 1.2.08.10 Battery stat.
 - 1.2.09 Battery test
 - 1.2.09.1 Test options
 - 1.2.09.1.n.m.1 Duration [min]
 - 1.2.09.1.n.m.2 Batt.test freq
 - 1.2.09.2 Man. Bat. test
 - 1.2.09.2.m.n.1 Duration [min]
 - 1.2.09.2.m.n.2 Run/Stop test
 - 1.2.09.3 Bat. replaced
 - 1.2.09.4 Batt capacity
 - 1.2.10 Panel diag
 - 1.2.10.1 System V/A
 - 1.2.10.2 Battery V
 - 1.2.11 Check card
 - 1.2.12 Demo mode
 - 1.2.13 Door control
 - 1.2.14 Notif. test
- 1.3 Panel info
 - 1.3.01 Software rev
 - 1.3.02 Panel langua>
 - 1.3.03 Defaults
 - 1.3.05 Sys fault in>
 - 1.3.06 HW variant
 - 1.3.07 HW Serial Nbr
 - 1.3.08 CDC Mode
 - 1.3.09 OH/IRIS Repo>
 - 1.3.10 ATSLan Errors
- 1.4 Bypass Pan.Lid
 - 1.4.1 Panel lid time

- 1.4.2 Restore lid
- 1.5 Config card
- 1.6 Service in
- 1.7 Default panel

2 Device Menu

- 2.1 Inst. Remotes
- 2.2 Edit Rkp&Exp
 - 2.2.1 Keypad devices
 - 2.2.1.0 Add keypad
 - 2.2.1.n.1 Keypad type
 - 2.2.1.n.2 Keypad address
 - 2.2.1.n.3 Keypad options
 - 2.2.1.n.3.01 Keypad name
 - 2.2.1.n.3.02 Tamper area
 - 2.2.1.n.3.03 Detect tamper
 - 2.2.1.n.3.04 View areas
 - 2.2.1.n.3.05 View AG
 - 2.2.1.n.3.06 Ctrl areas
 - 2.2.1.n.3.07 Control AG
 - 2.2.1.n.3.08 Control opt
 - 2.2.1.n.3.08.1 Card&PIN mode
 - 2.2.1.n.3.08.2 Logoff time
 - 2.2.1.n.3.08.3 1xset/unset
 - 2.2.1.n.3.08.4 3xbadge set
 - 2.2.1.n.3.08.5 Key/Card Mode
 - 2.2.1.n.3.08.6 Card Tamp.Lock
 - 2.2.1.n.3.08.7 Linked Reader
 - 2.2.1.n.3.09 EE PIN lock
 - 2.2.1.n.3.10 Isolate Rkp
 - 2.2.1.n.3.11 Buzzer silent
 - 2.2.1.n.3.12 Quick set
 - 2.2.1.n.3.13 Function keys
 - 2.2.1.n.3.14 Area ind.LED1
 - 2.2.1.n.3.15 Area ind.LED2
 - 2.2.1.n.3.16 Status ind.
 - 2.2.1.n.3.17 LCD backlight
 - 2.2.1.n.3.18 ACK on keypad
 - 2.2.1.n.3.19 EE 1 buzzer
 - 2.2.1.n.3.20 EE 2 buzzer
 - 2.2.1.n.3.21 1+3 keys
 - 2.2.1.n.3.22 RTE
 - 2.2.1.n.3.23 Backlight
 - 2.2.1.n.3.24 Nightlight
 - 2.2.1.n.3.25 Card beep opt
 - 2.2.1.n.3.26 Idle scr opt
 - 2.2.1.n.3.26.1 Logo
 - 2.2.1.n.3.26.2 Custom msg
 - 2.2.1.n.3.26.3 Time and date
 - 2.2.1.n.3.26.4 Text bkgd
 - 2.2.1.n.3.26.5 Text color
 - 2.2.1.n.4 Keypad menu
 - 2.2.1.n.5 Reset Comm Key

- 2.2.1.n.6 Delete keypad
- 2.2.2 Exp devices
 - 2.2.2.0 Add expander
 - 2.2.2.n.1 Expander type
 - 2.2.2.n.2 Exp address
 - 2.2.2.n.3 Expander range
 - 2.2.2.n.4 Exp settings
 - 2.2.2.n.4.1 Expander name
 - 2.2.2.n.4.2 Tamper area
 - 2.2.2.n.4.3 Detect tamper
 - 2.2.2.n.4.4 Isolate Exp
 - 2.2.2.n.4.5 Input mode
 - 2.2.2.n.4.6 EOL
 - 2.2.2.n.5 Expander menu
 - 2.2.2.n.7 Delete Exp

Wireless specific options:

- 2.2.2.n.4.4 Supervision
 - 2.2.2.n.4.4.1 Short superv.
 - 2.2.2.n.4.4.2 Long superv.
 - 2.2.2.n.4.4.3 Smoke superv.
- 2.2.2.n.4.5 R.Sensitivity
- 2.2.2.n.4.6 Expander mode
- 2.2.2.n.4.7 Exp version
- 2.2.2.n.4.8 Jamming menu
 - 2.2.2.n.4.8.1 Jamm detection
 - 2.2.2.n.4.8.2 Jamming Sec
 - 2.2.2.n.4.8.3 Jamm Thresh
- 2.2.2.n.4.11 Default exp

Camera specific options:

- 2.2.2.n.4.9 Pic options
 - 2.2.2.n.4.9.1 Pic settings
 - 2.2.2.n.4.9.1.1 Burglar set.
 - 2.2.2.n.4.9.1.1.1 Pic amount
 - 2.2.2.n.4.9.1.1.2 Frame rate
 - 2.2.2.n.4.9.1.1.3 Pic resolution
- Fire settings, Panic settings, Medical settings, Tamper settings, Fault settings, Custom type 1, Custom type 2:*
See 2.2.2.n.4.9.1.1 Burglar set.
- 2.2.2.n.4.9.2 Show pic mem
 - 2.2.2.n.4.9.3 Pic autodel
 - 2.2.2.n.4.9.4 Total pic cnt
 - 2.2.2.n.4.9.11 Delete pics

Four-door expander specific options:

- 2.2.2.n.4.7 Outp. modules
- 2.2.2.n.4.8 Reg cnt limit
- 2.2.2.n.4.9 Macro Logic
 - 2.2.2.n.4.9.00 Add macro
 - 2.2.2.n.4.9.m.1 Macro name
 - 2.2.2.n.4.9.m.2 Formula
 - 2.2.2.n.4.9.m.3 Macro output
 - 2.2.2.n.4.9.m.3.1 Output func.

- 2.2.2.n.4.9.m.3.2 Duration
- 2.2.2.n.4.9.m.3.3 Activate
- 2.2.2.n.4.9.m.4 Delete macro
- 2.2.2.n.4.10 Local Devices
- 2.2.2.n.4.11 Dev version
- 2.2.2.n.4.12 Synchronize

- 2.2.3 DC/LC Exp Rdrs
- 2.2.3.0 Add reader
- 2.2.3.n.2 Reader address
- 2.2.3.n.3 Reader options
- 2.2.3.n.3.1 Reader name
- 2.2.3.n.3.2 LCD
- 2.2.3.n.5 Delete reader
- 2.3 Databus EOL

3 User menu

- 3.1 Users
- 3.1.0 Add user
- 3.1.n.1 User name
- 3.1.n.2 PIN code
- 3.1.n.2.1 Change PIN
- 3.1.n.2.2 Remove PIN
- 3.1.n.3 User card
- 3.1.n.3.1 Assign card
- 3.1.n.3.1 Remove card
- 3.1.n.4 RF fobs
- 3.1.n.5 Language
- 3.1.n.6 User groups
- 3.1.n.7 Remote opts
- 3.1.n.7.1 Remote login
- 3.1.n.7.2 Chg rem passwd
- 3.1.n.7.3 Mobile number
- 3.1.n.7.4 SMS reporting
- 3.1.n.7.5 SMS control
- 3.1.n.8 Access opts
- 3.1.n.8.1 Door group
- 3.1.n.8.2 Floor group
- 3.1.n.8.3 Trace
- 3.1.n.8.4 Privileged
- 3.1.n.8.5 Ext. access
- 3.1.n.8.6 Acc. user type
- 3.1.n.9 Select mode
- 3.1.n.10 Delete user
- 3.2 User groups
- 3.2.0 Add UG
- 3.2.n.1 UG name
- 3.2.n.2 UG type
- 3.2.n.3 UG areas
- 3.2.n.4 UG AG
- 3.2.n.5 UG filter
- 3.2.n.6 UG options
- 3.2.n.7 Schedule
- 3.2.n.8 Remove UG

4 Zones&Areas

- 4.1 Zones Menu
- 4.1.0 Add zone

Common options

- 4.1.n.1 Zone name
- 4.1.n.2 Zone type
- 4.1.n.3 Isolated
- 4.1.n.4 Zone location
- 4.1.n.5 Zone areas
- 4.1.n.6 Zone options
- 4.1.n.6.1 Inhibit
- 4.1.n.6.2 Isolate
- 4.1.n.6.3 Excl. in PS1
- 4.1.n.6.4 Excl. in PS2
- 4.1.n.6.5 DblKnock
- 4.1.n.6.6 Swinger shunt
- 4.1.n.6.7 Anti mask
- 4.1.n.6.8 Zone pairing
- 4.1.n.6.9 Chime
- 4.1.n.6.10 Soak test
- 4.1.n.6.11 Eng walk test
- 4.1.n.6.12 User walk
- 4.1.n.6.13 Shock sensor
- 4.1.n.6.14 Extend EE
- 4.1.n.6.15 Final door
- 4.1.n.6.16 Key latch
- 4.1.n.6.17 Key set
- 4.1.n.6.18 Key unset
- 4.1.n.6.19 Tech full set
- 4.1.n.6.20 Tech unset
- 4.1.n.6.21 Tech part set
- 4.1.n.6.22 Keypad LCD
- 4.1.n.6.23 Log
- 4.1.n.6.24 CS report
- 4.1.n.6.25 Delay timer
- 4.1.n.6.26 ACK on keypad
- 4.1.n.6.27 ACK by user
- 4.1.n.6.28 Sensor type
- 4.1.n.6.29 Virtual zone
- 4.1.n.6.30 Held open
- 4.1.n.6.31 EE set check
- 4.1.n.6.32 Alarm in PS1
- 4.1.n.6.33 Alarm in PS2
- 4.1.n.6.34 Report as
- 4.1.n.6.35 Auto test
- 4.1.n.6.36 Shunt
- 4.1.n.6.37 View isolated
- 4.1.n.6.38 Limit reports
- 4.1.n.6.39 Input mode
- 4.1.n.6.40 EOL
- 4.1.n.6.41 Indication
- 4.1.n.6.42 Report code

- 4.1.n.8 Copy
- 4.1.n.8.1 Copy par. from
- 4.1.n.8.2 Block assign
- 4.1.n.9 Move zone
- 4.1.n.10 Delete zone

Shock sensor options:

- 4.1.n.7 Grs&Pls opts
- 4.1.n.7.1 Pulse count
- 4.1.n.7.2 Gross level

Wireless sensor options:

- 4.1.n.7 RF details
- 4.1.n.7.1 Sensor ID
- 4.1.n.7.2 Sensor type
- 4.1.n.7.3 Sensor mode
- 4.1.n.7.4 Supervision
- 4.1.n.7.5 Sensor opt
- 4.1.n.7.6 Remove RF dev

4.2 Areas

- 4.2.n.1 Area name
- 4.2.n.2 Exit time
- 4.2.n.3 Entry time
- 4.2.n.4 Other timers
- 4.2.n.4.1 Warning time
- 4.2.n.4.2 Prealarm time
- 4.2.n.4.3 Unset delay
- 4.2.n.5 Set/unset opts
- 4.2.n.5.1 Entry alarms
- 4.2.n.5.2 Set retry
- 4.2.n.5.3 Silent autoreset
- 4.2.n.5.4 Dual unset
- 4.2.n.5.5 Confirm alarm
- 4.2.n.6 Hierarchy
- 4.2.n.7 Limits
- 4.2.n.7.1 Inhibit limit
- 4.2.n.7.2 Isolate limit
- 4.2.n.7.3 Shunt limit
- 4.2.n.8 Schedule

4.3 Area groups

- 4.3.n.1 Name
- 4.3.n.2 Areas

4.4 RF fobs

- 4.4.0 Add fob
- 4.4.n.1 Fob name
- 4.4.n.2 Assigned user
- 4.4.n.3 Buttons
- 4.4.n.4 RF details
- 4.4.n.4.1 Sensor ID
- 4.4.n.4.2 Remove RF dev
- 4.4.n.5 Remove fob

4.5 Cameras Menu

- 4.5.n.1 Camera name

- 4.5.n.2 Pics by zone
- 4.5.n.3 Pics by filter
- 4.5.n.3.m.2 Event type 1
- 4.5.n.3.m.3 Report as
- 4.5.n.4 Pics by rep ev
- 4.5.n.5 Isolated
- 4.5.n.6 Max pics 24h
- 4.5.n.7 Remote pics
- 4.5.n.8 Test pic to CS

5 Doors Menu

5.1 Doors

Common door options:

- 5.1.0 Add door
- 5.1.n.1 Door name
- 5.1.n.2 Door location
- 5.1.n.3 Door readers
- 5.1.n.4 Door output
- 5.1.n.5 Door timers
- 5.1.n.5.1 Unlock time
- 5.1.n.5.2 Extended time
- 5.1.n.6 Door options
- 5.1.n.6.1 Door zones
- 5.1.n.6.1.1 Door zone
- 5.1.n.6.3 Alarm control
- 5.1.n.6.3.1 Door areas
- 5.1.n.6.3.2 Door AGs
- 5.1.n.6.3.3 When unset
- 5.1.n.6.3.3.1 Low security
- 5.1.n.6.3.3.2 Unlock Door
- 5.1.n.6.3.4 When set
- 5.1.n.6.3.4.1 Deny access
- 5.1.n.6.3.4.2 Lock door
- 5.1.n.6.3.4.3 EE PIN lock
- 5.1.n.6.4 RTE options
- 5.1.n.6.4.1 Use RTE
- 5.1.n.7 Schedule opts
- 5.1.n.7.1 Door unlocked
- 5.1.n.8 Shunt options
- 5.1.n.8.2 Shunt timers
- 5.1.n.8.2.1 Shunt time
- 5.1.n.8.2.2 Extended time
- 5.1.n.8.2.3 Warning time
- 5.1.n.8.3 Shunt type
- 5.1.n.8.3.1 Shunting
- 5.1.n.8.5 Until door CL
- 5.1.n.8.6 CancelAfterCL
- 5.1.n.10 Move Door
- 5.1.n.11 Disable door
- 5.1.n.12 Delete door

Standard door specific options:

- 5.1.n.8.3.2.2 Shunt active

- 5.1.n.8.4 Indication
 - 5.1.n.8.4.1 Door held open
- 5.1.n.8.7 EE Shunt
- 5.1.n.8.8 Shunt start
- Intelligent door specific options
 - 5.1.n.3.5 Readers opts
 - 5.1.n.3.5.1 Card and PIN
 - 5.1.n.3.5.2 Two cards
 - 5.1.n.3.5.3 NoSchedule req
 - 5.1.n.3.5.4 Card format
 - 5.1.n.3.5.5 LEDs option
 - 5.1.n.3.5.6 Time&Attendanc
 - 5.1.n.3.5.7 Disable Duress
 - 5.1.n.6.1.2 Second zone
 - 5.1.n.6.1.3 DOTL zone
 - 5.1.n.6.2 Door unlocked
 - 5.1.n.6.2.1 Until closed
 - 5.1.n.6.2.2 Until opened
 - 5.1.n.6.2.3 Pulsed L&UnL
 - 5.1.n.6.3.5 User group
 - 5.1.n.6.3.6 Control type
 - 5.1.n.6.3.7 If PIN sets
 - 5.1.n.6.3.7.1 Deny access
 - 5.1.n.6.4.2 RTE zone
 - 5.1.n.6.4.3 Dis. when set
 - 5.1.n.6.4.4 RTE Control
 - 5.1.n.6.5 Reporting
 - 5.1.n.6.5.1 CL & Locked
 - 5.1.n.6.5.2 OP&Unl as Unl
 - 5.1.n.6.5.3 Open/Close
 - 5.1.n.6.5.4 Forced door
 - 5.1.n.6.5.5 DOTL
 - 5.1.n.6.5.6 RTE
 - 5.1.n.6.6 Interlocking
 - 5.1.n.7.1.2 After entry
 - 5.1.n.7.2 Low Security
 - 5.1.n.7.3 RTE Schedule
 - 5.1.n.8.1 Zones
 - 5.1.n.8.4 Indication
 - 5.1.n.8.4.2 DOTL output
 - 5.1.n.8.4.3 Warning output
 - 5.1.n.8.4.4 Forced door
 - 5.1.n.9 Regions & AP
 - 5.1.n.9.1 Regions
 - 5.1.n.9.2 Anti-passback
 - 5.1.n.9.3 Inh Reg 1 Usr
 - 5.1.n.9.4 HSU options
 - 5.1.n.9.4.1 Req HSU Nr
 - 5.1.n.9.4.2 Prewarn. time
 - 5.1.n.9.4.3 HS Alarm out
- 5.2 Door groups
 - 5.2.0 Add Door Gr

- 5.2.n.1 Door Gr name
- 5.2.n.2 Door Gr Doors
- 5.2.n.3 Delete Door Gr
- 5.3 Region
 - 5.3.0 Add region
 - 5.3.n.1 Region name
 - 5.3.n.2 Delete region
- 5.4 Floors
 - 5.4.0 Add floor
 - 5.4.n.1 Floor name
 - 5.4.n.2 Delete floor
- 5.5 Floor groups
 - 5.5.0 Add Floor Gr
 - 5.5.n.1 Floor Gr name
 - 5.5.n.2 Floor Gr Fls
 - 5.5.n.3 Delete Fl Gr

6 Outs&filters

- 6.1 Cond filters
 - 6.1.0 Add filter
 - 6.1.n.1 Filter name
 - 6.1.n.2 Formula
 - 6.1.n.2.0 Add event
 - 6.1.n.3 Invert
 - 6.1.n.4 Delete filter
- 6.2 Outputs
 - 6.2.0 Add output
 - 6.2.n.1 Output name
 - 6.2.n.2 Output loc
 - 6.2.n.3 Invert output
 - 6.2.n.4 Start filter
 - 6.2.n.5 Stop filter
 - 6.2.n.6 Mode
 - 6.2.n.7 Parameters
 - 6.2.n.7.1 Delay time
 - 6.2.n.7.2 Active time
 - 6.2.n.7.3 Retriggerable
 - 6.2.n.8 Log limit
 - 6.2.n.9 Delete output
- 6.3 Triggers
 - 6.3.0 Add trigger
 - 6.3.n.1 Trigger name
 - 6.3.n.2 Schedule
 - 6.3.n.3 User group
 - 6.3.n.4 Delete trigger

7 Calendar

- 7.1 View
 - 7.1.n.1 Auto Set
 - 7.1.n.2 By object
 - 7.1.n.3 Special day
 - 7.1.n.3.1 Day type
 - 7.1.n.3.2 Recurring
 - 7.1.n.3.3 Until date

- 7.2 Schedules
 - 7.2.0 Add Schedule
 - 7.2.n.1 Name
 - 7.2.n.2 Active
 - 7.2.n.3 Date
 - 7.2.n.4 Time
 - 7.2.n.4.0 Add time frame
 - 7.2.n.4.m.1 Start time
 - 7.2.n.4.m.2 End time
 - 7.2.n.4.m.3 Week days
 - 7.2.n.4.m.4 Delete TF
 - 7.2.n.5 Action list
 - 7.2.n.5.0 Add Action
 - 7.2.n.5.m.1 Name
- Object type, Function, Parameters: See "User programmable functions" on page 104*
- 7.2.n.5.m.5 Delete action
 - 7.2.n.6 Special days
 - 7.2.n.6.0 Add sp day
 - 7.2.n.6.m.1 Name
 - 7.2.n.6.m.2 Start time
 - 7.2.n.6.m.3 End time
 - 7.2.n.6.m.4 Delete sp day
 - 7.2.n.7 Filter
 - 7.2.n.8 Delete sched
- 8 Sys.opts Menu**
- 8.1 Timer menu
 - 8.1.1 Time&date
 - 8.1.2 Siren options
 - 8.1.2.1 Activation
 - 8.1.2.2 Delay
 - 8.1.3 Syst Misc opts
 - 8.1.3.1 Armed display
 - 8.1.3.2 Card&PIN
 - 8.1.3.3 Walk test time
 - 8.1.3.4 Mains rep dly
 - 8.1.3.5 Final set dly
 - 8.1.3.6 Inst in-time
 - 8.1.4 Zn timers menu
 - 8.1.4.1 DblKnock int
 - 8.1.4.2 DblKnock open
 - 8.1.4.3 Soak test
 - 8.1.4.4 Input delay
 - 8.1.4.5 Key box time
 - 8.1.4.6 Held open time
 - 8.1.4.7 Inactive days
 - 8.2 Engineer opt
 - 8.2.1 User code req
 - 8.2.2 Tamper req
 - 8.2.3 Eng. lockout
 - 8.2.4 Engineer reset
 - 8.2.4.01 Alarm
 - 8.2.4.02 Tamper
 - 8.2.4.03 Panic
 - 8.2.4.04 Conf. alarm
 - 8.2.4.05 Battery fail
 - 8.2.4.06 Aux fuse
 - 8.2.4.07 Mains fail
 - 8.2.4.08 Siren fault
 - 8.2.4.09 Intconn fault
 - 8.2.4.10 Auto reset
 - 8.2.4.11 Dis by servi>
 - 8.2.4.12 System code
 - 8.2.4.13 Do reset
 - 8.2.4.14 Custom text
 - 8.2.5 Service in
 - 8.2.6 Challenge code
 - 8.2.7 Inspection
 - 8.2.7.1 Date
 - 8.2.7.2 Custom msg
 - 8.2.8 Installer grp
 - 8.2.8.1 Many installe>
 - 8.2.8.2 Mgmt SW
 - 8.3 LCD Dsply opts
 - 8.3.1 Arm display
 - 8.3.2 Custom msg
 - 8.3.3 Alarm list
 - 8.3.4 Indicate fault
 - 8.3.5 View EE timer
 - 8.4 Set options
 - 8.4.1 RTS options
 - 8.4.2 Inhibit incl
 - 8.4.3 Part set
 - 8.4.3.1 Report BA
 - 8.4.3.2 Access to EE
 - 8.4.3.3 EE full set
 - 8.4.3.4 PS1 name
 - 8.4.4 Forced set
 - 8.4.5 Forced set opt
 - 8.4.6 Pending alar
 - 8.4.7 AS fault ret>
 - 8.4.8 AS user retry
 - 8.4.9 Exit fault
 - 8.4.10 Rep. EE fault
 - 8.5 Access opts
 - 8.5.1 Access timers
 - 8.5.1.1 Card to PIN
 - 8.5.1.2 Two cards
 - 8.5.1.3 Multiple badge
 - 8.5.1.4 Re-lock delay
 - 8.5.2 DGP options
 - 8.5.2.1 Map relays
 - 8.5.2.2 Map panel LEDs
 - 8.5.3 Use 27bitTecom
 - 8.5.4 SysFault beep
 - 8.5.5 Valid card ind
 - 8.6 Zone options
 - 8.6.1 Swinger shunt

- 8.6.2 Rep.restore
- 8.6.3 Limit reports
- 8.6.4 LongSup as TA
- 8.7 Panel&AB opts
 - 8.7.1 Panel name
 - 8.7.2 Panel language
 - 8.7.3 Duress method
 - 8.7.4 PIN length
 - 8.7.5 PIN chg mode
 - 8.7.6 Alarm confirm
 - 8.7.6.1 AB mode
 - 8.7.6.2 AB time
 - 8.7.6.2.1 Intr. AB time
 - 8.7.6.2.2 Holdup AB time
 - 8.7.6.3 System confirm
 - 8.7.6.4 EE confirm
 - 8.7.6.5 Access to EE
 - 8.7.6.6 TA confirm
 - 8.7.6.7 Sirens
 - 8.7.6.8 Call CS msg
 - 8.7.6.9 Rep. delayed
 - 8.7.6.10 PD6662
 - 8.7.7 Easy unset
 - 8.7.8 Rem cfg opt
 - 8.7.8.1 Remote config
 - 8.7.8.2 Superv config
 - 8.7.8.3 Rem cfg access
 - 8.7.8.4 WebApp
 - 8.7.8.4.1 WebApp Access
 - 8.7.8.4.2 Direct IP Prot
 - 8.7.8.4.3 Idle timeout
 - 8.7.9 Object scheme
- 8.8 PA & other
 - 8.8.1 Panic mode
 - 8.8.2 Chime menu
 - 8.8.2.1 Chime in PS
 - 8.8.2.2 Latched chime
 - 8.8.3 SysTamp areas
 - 8.8.4 Siren options
 - 8.8.4.1 Sir tamper mod
 - 8.8.4.2 Sir tamper EOL
 - 8.8.4.3 Siren retrig.
 - 8.8.4.4 Siren report
 - 8.8.5 Card learn-in
 - 8.8.5.1 Keypad learnin
 - 8.8.5.2 Door learn-in
 - 8.8.6 Test inputs
 - 8.8.7 Buzzer mode
 - 8.8.8 Mon. 3 HC out
 - 8.8.9 Card number
 - 8.8.10 Anonymize Log
 - 8.8.11 RDR security
 - 8.8.11.1 Secure mode
 - 8.8.11.2 Config. key

- 8.8.11.3 App. key
- 8.8.11.4 App. name
- 8.8.11.5 App. file ID
- 8.8.11.6 Tamp reset key
- 8.8.11.7 Card Bit Lmt
- 8.8.11.8 Default
- 8.8.12 RAS OrangeLED
- 8.8.13 Config in set
- 8.8.14 Clocked out
- 8.9 TimedUnset/ATM
 - 8.9.1 Delay
 - 8.9.2 Unset Time
 - 8.9.3 Ext Unset Time
 - 8.9.4 Uns Warn Time

9 Communication

9.1 CS

9.1.0 Add CS

Common options:

- 9.1.n.1 CS name
- 9.1.n.2 Transm path
- 9.1.n.3 Protocol
- 9.1.n.5 Accounts
- 9.1.n.6 Mode
- 9.1.n.7 Retry count
- 9.1.n.8 Protocol opt
 - 9.1.n.8.1 (X)SIA
 - 9.1.n.8.1.1 Area modifier
 - 9.1.n.8.1.2 Name chars
 - 9.1.n.8.1.3 Event number
 - 9.1.n.8.1.4 Subev coding
- 9.1.n.9 OP/CL report
- 9.1.n.10 Delete CS

IP and GSM/GPRS specific options:

- 9.1.n.4 Destination/IP
 - 9.1.n.4.1 Dest name
 - 9.1.n.4.2 Dest port
 - 9.1.n.4.3 Ping host
- 9.1.n.8.2 OH 2000
 - 9.1.n.8.2.1 Version
 - 9.1.n.8.2.2 Heartbeat time
 - 9.1.n.8.2.3 Receiver nbr
 - 9.1.n.8.2.4 Line nbr
 - 9.1.n.8.2.5 Freq. HB time

Photo transmission specific options:

- 9.1.n.4.4 Encryption
- 9.1.n.4.5 Pic dest port

GSM/phone specific options:

- 9.1.n.4 Destination
 - 9.1.n.4.1 Type

UltraSync specific options:

9.1.n.4 Channel no

VdS specific options:

9.1.n.8.3 VdS

9.1.n.8.3.1 Version

9.1.n.8.3.2 Enc. key no.

9.1.n.8.3.3 Enc. key value

9.1.n.8.3.4 SVCP conn mode

9.2 Event options

9.2.1 CS mapping

9.2.2 Delayed events

9.2.3 VdS channels

9.3 Path options

Common options:

9.3.n.1 Path name

9.3.n.2 Line fault

9.3.n.3 LF delay

9.3.n.4 Expander menu

9.3.n.8 Ring setup

9.3.n.8.1 Ring count

9.3.n.8.2 Omit 1st call

9.3.n.9 Encryption

IP specific options:

9.3.n.4 Transm path

9.3.n.5 IP config

9.3.n.5.1 IP config

9.3.n.5.2 IP address

9.3.n.5.3 Subnet mask

9.3.n.5.4 Gateway

9.3.n.6 DNS config

9.3.n.6.1 DNS config

9.3.n.6.2 DNS server

9.3.n.07 NTP config

9.3.n.7.1 NTP config

9.3.n.7.2 NTP server

9.3.n.8 Firewall

9.3.n.8.1 Firewall

9.3.n.8.2 Reply on PING

9.3.n.10 MAC address

9.3.n.11 Max Pics 24h

9.3.n.12 WAN LF check

9.3.n.13 mDNS enabled

9.3.n.13.1 mDNS enabled

9.3.n.13.2 Host name pre>

GSM/SMS/GPRS specific options:

9.3.n.4 Transm path

9.3.n.5 GSM Setup

9.3.n.5.1 SIM card PIN

9.3.n.5.2 Networks

9.3.n.5.2.1 Net.selection

9.3.n.5.2.2 Sel.net.only

9.3.n.5.2.3 Net.scanning

9.3.n.5.2.3.0 Rescan nets

9.3.n.5.2.3.m.1 Network name

9.3.n.5.2.3.m.2 Network code

9.3.n.5.2.3.m.3 Availability

9.3.n.5.2.3.m.4 RSSI

9.3.n.5.2.3.m.5 Use this net.

9.3.n.5.3 Credit

9.3.n.5.3.1 Check now

9.3.n.5.3.2 Check mode

9.3.n.5.3.3 Check number

9.3.n.5.3.4 Request code

9.3.n.5.3.5 Check period

9.3.n.5.3.6 Check time

9.3.n.5.4 Jamm detection

9.3.n.5.4.1 Jamm detection

9.3.n.5.4.2 Jamm threshold

9.3.n.6 SMS Setup

9.3.n.6.1 SMS Center num

9.3.n.6.2 SMS forwarding

9.3.n.6.3 Max Msg 24h

9.3.n.6.4 SMS header msg

9.3.n.6.5 User PIN req.

9.3.n.6.6 Ext.charset

9.3.n.7 GPRS Setup

9.3.n.7.1 APN name

9.3.n.7.2 User name

9.3.n.7.3 User pass

9.3.n.7.4 IP config

9.3.n.7.5 DNS config

9.3.n.7.6 Firewall

9.3.n.7.7 Line fault

9.3.n.7.8 Disconn.time

9.3.n.7.9 Max Pics 24h

9.3.n.10 MMS Setup

9.3.n.10.1 MMS center

9.3.n.10.2 APN name

9.3.n.10.3 User name

9.3.n.10.4 User pass

9.3.n.10.5 Proxy

9.3.n.10.6 Proxy port

9.3.n.10.7 Max MMS 24h

9.3.n.11 Module info

9.4 PC connection

9.4.1 Connections

9.4.1.0 Add PC conn

9.4.1.n.1 Name

9.4.1.n.2 Transm path

9.4.1.n.5 Retry limit

9.4.1.n.6 Delete PC conn

Chapter 9: Programming maps

9.4.2 PC callback

9.4.3 Encrypt.key 1

9.4.4 Encrypt.key 2

9.4.5 Listening port

9.4.6 Panel ID

IP specific options:

9.4.1.n.4 Destination/IP

9.4.1.n.4.1 Dest name

9.4.1.n.4.2 Dest port

9.4.1.n.4.3 Ping host

GSM specific options:

9.4.1.n.3 Conn. type

9.5 UltraSync

9.5.1 Connectivity

9.5.2 SID number

9.5.3 Settings

9.5.3.1 Password

9.5.3.2 FW Upgrade

9.5.3.3 Remote config.

9.5.3.4 Notifications

9.5.3.5 GPRS monitor

9.5.3.6 US servers

9.5.4 Notifications

9.5.4.n.1 Name

9.5.4.n.2 Identifier

9.5.4.n.3 User

9.5.4.n.4 Status

9.5.4.n.5 Notif.events

9.5.4.n.6 Delete notif.

9.6 VdS

9.6.1 Block status

9.6.2 Comm path desc

WebApp programming map

Configuration

PANEL	AREAS
DEVICES	ACCESS
CONNECTIVITY	DIAGNOSTICS
USERS	ACTIONS

PANEL

GENERAL

TIME AND DATE SETTINGS

Panel name

Panel language

OBJECT SCHEME

MANY INSTALLERS

ANONYMIZE LOG

DATABUS OPTIONS

DATABUS EOL TERMINATION

DISPLAY AND LEDS

ARM DISPLAY

Custom message

ALARM LIST

INDICATE FAULTS

VIEW EE TIMER

NON LCD RAS ORANGE LED
INDICATION

SOUNDS

BUZZER MODE

CHIME IN PART SET

LATCHED CHIME

TIMERS

SYSTEM TIMERS

ARMED DISPLAY

WALK TEST TIME

MAINS REPORTING DELAY

FINAL SET DELAY

INST IN-TIME

SIREN TIMERS

INTERNAL SIREN

EXTERNAL SIREN

F/P/M INTERNAL

F/P/M EXTERNAL

INTERNAL SIREN

EXTERNAL SIREN

ZONE TIMERS

DOUBLE KNOCK INTERVAL

DOUBLE KNOCK OPEN

SOAK TEST

INPUT DELAY

KEY BOX TIME

HELD OPEN TIME

INACTIVE DAYS

ACCESS TIMERS

CARD AND PIN

CARD TO PIN TIME

TWO CARDS TIME

MULTIPLE BADGE TIME

RE-LOCK DELAY

TIMED UNSET / ATM

DELAY

UNSET TIME

EXTENDED UNSET TIME

WARNING TIME BEFORE SET

AB ALARM TIMERS

INTRUSION AB TIME

HOLDUP AB TIME

CREDENTIALS

DURESS METHOD

PIN LENGTH

PIN CHANGE MODE
USE 27BITTECOM FORMAT FOR
27BIT CARDS
Keypad learn-in
Door learn-in
CARD NUMBER

SET AND UNSET

READY TO SET OPTIONS

INHIBIT INCLUDES

PART SET OPTIONS

ACCESS TO EE

EE FULL SET

Part set 1 name

Part set 2 name

FORCED SET

FORCED SET OPTIONS

PENDING ALARMS

Autoset retry on system fault

Autoset user retry

EXIT FAULT

EASY UNSET

ALARMS AND REPORTING

Panic mode

SYSTEM TAMPER AREAS

SIREN RETRIGGER

AB ALARM OPTIONS

SYSTEM CONFIRM

EE CONFIRM

ACCESS TO EE

TA CONFIRM

CALL CENTRAL STATION

MESSAGE

REPORTING DELAYED

MONITOR 3RD HIGH CURRENT
OUTPUT

SWINGER SHUNT

REPORTING OPTIONS

REPORT BA

REPORT EXIT FAULT

REP. RESTORE

LIMIT REPORTS

SIREN OPTIONS

SIREN TAMPER INPUT MODE

SIREN TAMPER EOL

REPORT SIREN FAULT

ENGINEER OPTIONS

USER CODE REQUIRED

TAMPER REQUIRED

ENGINEER LOCKOUT

ENGINEERING RESET

ALARM

TAMPER

PANIC

BATTERY FAIL

AUX FUSE

MAINS FAIL

SIREN FAULT

INTERCONNECTION FAULT

AUTOMATIC RESET

DISABLE WHEN SERVICE IN

SYSTEM CODE

CUSTOM TEXT

CHALLENGE CODE

INSPECTION

DATE

CUSTOM MESSAGE

MANY INSTALLERS

TEST INPUTS

CONFIG IN SET STATE

ACCESS

MAP RELAYS

MAP PANEL LEDS

REMOTE ACCESS

REMOTE CONFIGURATION

ALLOW REMOTE ACCESS TO

CONFIGURATION BY

SUPERVISOR

REMOTE CONFIGURATION

ACCESS

AREAS

AREAS	AREA GROUPS
-------	-------------

AREAS*Select area*GENERAL

Area name

ZONES ASSIGNED

INHIBIT LIMIT

ISOLATE LIMIT

SHUNT LIMIT

TIMERS

EXIT TIMERS

EXIT TIME 1

EXIT TIME 2

REMOTE EXIT TIME

PART SET EXIT TIME 1

PART SET EXIT TIME 2

ENTRY TIMERS

ENTRY TIME 1

ENTRY TIME 2

PART SET ENTRY TIME 1

PART SET ENTRY TIME 2

PREALARM TIME

UNSET DELAY

AUTOSET WARNING TIME

AREA SET/UNSET

AB MODE

SIREN OPTIONS

ENTRY ALARMS

AUTOSET RETRY

AUTOSET SILENT MODE

DUAL UNSET

CONFIRM ALARM

HIERARCHY LEVEL

AREA GROUPS*Select area group*GENERAL

Area group name

AREA GROUP AREAS

DEVICES

ZONES	KEYPADS
EXPANDERS	OUTPUTS
CAMERAS	FOBS

ZONES*Select zone*GENERAL

Zone name

Zone type

ISOLATE

ZONE AREAS

ANTI MASK

SHOCK SENSOR

SET AND UNSET OPTIONS

INHIBIT

ISOLATE

VIEW ISOLATED

SHUNT

EXCLUDE IN PART SET 1

EXCLUDE IN PART SET 2

EXTEND EE

EE SET CHECK

FINAL DOOR

ALARM AND REPORTING
OPTIONS

DOUBLE KNOCK

SWINGER SHUNT

ZONE PAIRING

LOG

LIMIT REPORTS

ZONE HELD OPEN

ALARM IN PS1

ALARM IN PS2

DIAGNOSTIC OPTIONS

SOAK TEST

ENGINEER WALK TEST

USER WALK TEST

DETECTOR AUTO TEST

SOUND OPTIONS

CHIME

KEYPADS

Select keypad

GENERAL

KEYPAD NAME

DETECT TAMPER

CARD TAMPER LOCK

EE PIN LOCK

ISOLATE KEYPAD

1+3 KEYS

RTE

SOUNDS

BUZZER SILENT

EE 1 BUZZER

EE 2 BUZZER

LED AND DISPLAY

LCD BACKLIGHT BEHAVIOR

AREA INDICATION FOR LED 1

AREA INDICATION FOR LED 2

BACKLIGHT

STATUS INDICATION MODE

CREDENTIALS

CARD AND PIN MODE

ONE TIME BADGE TO SET/UNSET

THREE TIME BADGE TO SET

KEY/CARD SEQUENCE MODE

AREAS ASSIGNED

VIEW AREAS

CONTROL AREAS

VIEW AREA GROUP

CONTROL AREA GROUP

TAMPER AREA

CONTROL OPTIONS

LOGOFF TIME

LINKED READER

ACK ON KEYPAD

QUICK SET MODE

FUNCTION KEYS

USER CODE REQUIRED

EXPANDERS

Select expanders

GENERAL

EXPANDER NAME

ISOLATE EXPANDER

INPUT MODE

END OF LINE RESISTOR

BATTERY TEST FREQUENCY

START TIME

DURATION [MIN]

CONTROL

DETECT TAMPER

TAMPER AREA

OUTPUTS

Select output

GENERAL

OUTPUT NAME

INVERT OUTPUT

START FILTER

STOP FILTER

MODE

DELAY TIME

ACTIVE TIME

RETRIGGERABLE

LOG LIMIT

CAMERAS

FOBS

ACCESS

DOORS

REGIONS

DOORS

Select door

GENERAL

DOOR LOCATION

Door name

Door type

DOOR ZONES

Door zone

DOOR OUTPUTS

Door output

DOOR READERS

TIMERS

UNLOCK TIME

EXTENDED TIME

SHUNT TIME

EXTENDED TIME

WARNING TIME

ASSIGNED AREAS

DOOR AREAS

DOOR AREA GROUPS

INTRUSION OPTIONS

DENY ACCESS

LOCK DOOR

EE PIN LOCK

UNLOCK DOOR

ACCESS OPTIONS

DOOR HELD OPEN

Shunting

SHUNT ACTIVE

EE SHUNT

UNTIL DOOR CLOSE

CANCEL AFTER CLOSE

SHUNT START

DOOR READERS

REGIONS

Select region

Region name

CONNECTIVITY

COMMUNICATION PATHS

PC CONNECTIONS

EVENT
OPTIONS

UltraSync
options

COMMUNICATION PATHS

Select path

GENERAL

Path name

LINE FAULT

LINE FAULT DELAY

ENCRYPTION

FIREWALL

IP

IP CONFIG

IP OPTIONS
IP ADDRESS
SUBNET MASK
GATEWAY

DNS OPTIONS

NTP OPTIONS

REPLY ON PING
LINE FAULT CHECK FOR WAN
CONNECTION

PC CONNECTIONS

Select PC connection

GENERAL

Name
Transm path
RETRY LIMIT
Destination/IP
DESTINATION PORT

EVENT OPTIONS

Select event

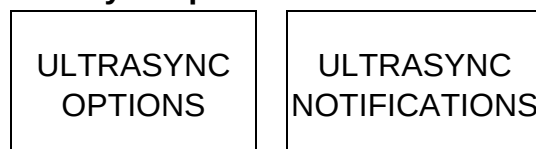
GENERAL

See Appendix A “AXON events” on
page 421.

DELAYED
See Delayed events.

REPORT TO
See CS mapping.

UltraSync options



ULTRASYNC OPTIONS

GENERAL

SID NUMBER
UltraSync password

CLOUD CONNECTIVITY
REMOTE FIRMWARE UPGRADE
REMOTE CONFIGURATION
NOTIFICATIONS
GPRS MONITORING

SERVERS

ULTRASYNC NOTIFICATIONS

DIAGNOSTICS

GENERAL

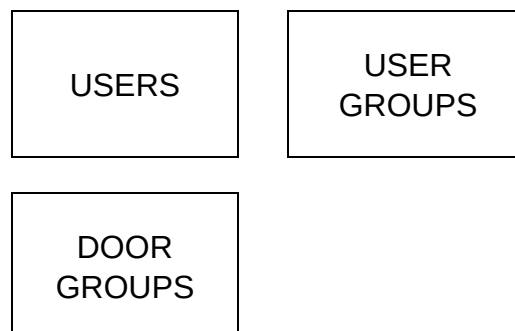
USE INTERNAL SIREN
USE BUZZERS
LOG UNTESTED
ZONE TAMPER
KEYPAD/EXPANDER TAMPER
SIREN TAMPER

Frequency
NEED TO SET
REDUCED WALKTEST

BATTERY TEST

Battery test frequency
DURATION [MIN]

USERS



USERS

Select user
PERSONAL
USER NAME
LANGUAGE
MOBILE NUMBER

CREDENTIALS

CHANGE PIN

REMOTE OPTIONS

Login for remote access

CHANGE PASSWORD

GROUPS

USER GROUPS

DOOR GROUP

FLOOR GROUP

ADVANCED

PRIVILEGED

EXTENDED ACCESS

TRACE

Access user type

RF FOBS

USER GROUPS*Select user group***GENERAL**

User group name

User group type

USER GROUP FILTER

ACCESS POINTS

USER GROUP AREAS

USER GROUP AREA GROUP

PERMISSIONS

See User groups.

DOOR GROUPS**ACTIONS**

FILTERS

TRIGGERS

FILTERS*Select user group***GENERAL**

Filter name

FUNCTION

INVERT

Formula

TRIGGERS*Select trigger***GENERAL**

Trigger name

User group

Appendix A

AXON events

For AXON system events, see Table 33 below. For access control events, used to program door controllers, see Table 34 on page 432.

Table 33: AXON events

Group: Zone

Event	#	Event description	Notes
ACTIVE	1	Zone active	Zone in active state
TAMPER	2	Zone tamper	Zone in tamper state
AM	3	Zone masking	Zone in anti-mask alarm state
BATTFAULT	4	Zone battery fault	Zone in battery fault state
FAULT	5	Zone fault	Zone in fault state
DIRTY	6	Zone dirty	Zone in dirty state
SVSHORT	7	Zone supervision short	Zone in short supervision state
SVLONG	8	Zone supervision long	Zone in short supervision state
INHIBIT	9	Zone inhibited	Zone state changed to inhibited
ISOLATE	10	Zone isolated	Zone state changed to isolated
SOAK	11	Zone in soak test	Soak test is active
SET	12	Zone set	Zone in Part set or Full set mode
ALARM	13	Zone in alarm	Zone in alarm. Restores after alarm acknowledgement.
RF learned	14	Wireless device programmed	Active for 3 seconds after a successful programming
RF signal accept	15	Wireless device found	Active for 3 seconds after device response
Held Open	16	Zone is open too long	Zone is held open
Inactive days	17	Zone inverted walk test failed	Zone has been inactive for longer than inactive day limit
SHUNT	18	Zone shunted	

Event	#	Event description	Notes
SHUNT FAULT	19	Zone shunt fault	Fault — zone is active when unshunt
DOOR SHUNT	20	Door shunt	Zone shunt by door shunt
DSHUNTWARN	21	Door shunt warning	Zone in shunt warning time by door shunt
MAINSFAULT	22	Zone mains fault	
RFJAMFAULT	23	Zone RF Jamming	

Group: Area

Event	#	Event description	Notes
FULLSET	1	Area full set	Area is in full set state
PARTSET1	2	Area part set 1	Area is in part set 1 state
UNSET	3	Area unset	Area is in unset state
ALARM	4	Intrusion alarm	Area Intrusion alarm is active
FSALARM	5	Alarm during full set	Area alarm while in full set
PSALARM	6	Alarm during part set	Area alarm while in part set
USALARM	7	Alarm during unset	Area alarm while unset
FTCALARM	8	Alarm and FTC	Area alarm while FTC present
FIREDOOR	9	Fire door active	A fire door local alarm is active
FSFIREDOOR	10	Fire door during full set	A fire door active while area full set
PSFIREDOOR	11	Fire door during part set	A fire door active while area part set
USFIREDOOR	12	Fire door during unset	A fire door active while area unset
FTCFIREDOOR	13	Fire door and FTC	A fire door active while FTC present
FIRE	14	Fire alarm	A fire alarm active
FSFIRE	15	Fire alarm during full set	A fire alarm active while area full set
PSFIRE	16	Fire alarm during part set	A fire alarm active while area part set
USFIRE	17	Fire alarm during unset	A fire alarm active while area unset
FTCFIRE	18	Fire alarm and FTC	A fire alarm active while FTC present
PANIC	19	Panic alarm	A panic alarm active
FSPANIC	20	Panic during full set	A panic alarm active while area full set
PSPANIC	21	Panic during part set	A panic alarm active while area part set
USPANIC	22	Panic during unset	A panic alarm active while area unset
FTCPANIC	23	Panic and FTC	A panic alarm active while FTC present
MEDICAL	24	Medical alarm	A medical alarm active

Event	#	Event description	Notes
FSMEDICAL	25	Medical during full set	A medical alarm active while area full set
PSMEDICAL	26	Medical during part set	A medical alarm active while area part set
USMEDICAL	27	Medical during unset	A medical alarm active while area unset
FTCMEDICAL	28	Medical and FTC	A medical alarm active while FTC present
TECHNICAL	29	Technical alarm	A technical alarm active
FSTECHNICAL	30	Technical during full set	A technical alarm active while area full set
PSTECHNICAL	31	Technical during part set	A technical alarm active while area part set
USTECHNICAL	32	Technical during unset	A technical alarm active while area unset
FTCTECHNICAL	33	Technical and FTC	A technical alarm active while FTC present
TAMPER	34	Tamper alarm	A tamper alarm active
FSTAMPER	35	Tamper during full set	A tamper alarm active while area unset
PSTAMPER	36	Tamper during part set	A tamper alarm active while area part set
USTAMPER	37	Tamper during unset	A tamper alarm active while area unset
FTCTAMPER	38	Tamper and FTC	A tamper alarm active while FTC present
CHIME	39	Chime	Active for 2 sec when zone with chime option is active
PSCHIME	40	Chime during part set	Active for 2 sec when zone with chime option is active during part set
USCHIME	41	Chime during unset	Active for 2 sec when zone with chime option is active during unset
ZNACTIVE	42	Zone active	At least one zone in the area is in active state
ZNINHIBIT	43	Zone inhibit	At least one zone in the area is inhibited
ZNISOLATE	44	Zone isolate	At least one zone in the area is isolated
ZNFAULT	45	Zone fault	At least one zone in the area is in fault state
ZNAM	46	Zone masking	At least one zone in the area is in anti-mask alarm state
ZNTAMPER	47	Zone tamper	At least one zone in the area is in tamper state
KEYPADTAMPER	48	Keypad tamper	A keypad assigned to the area is in tamper state
KEYPADFAULT	49	Keypad fault	A keypad assigned to the area is in fault state

Event	#	Event description	Notes
EXPANDERTAMPER	50	Expander tamper	An expander assigned to the area is in tamper state
EXPANDERFAULT	51	Expander fault	An expander assigned to the area is in fault state
DURESS	52	Duress	Duress code used in the area
FSDURESS	53	Duress during full set	Duress code used while area full set
PSDURESS	54	Duress during part set	Duress code used while area part set
USDURESS	55	Duress during unset	Duress code used while area unset
FTCDURESS	56	Duress and FTC	Duress code used while FTC present
CODETAMPER	57	Code tamper	Active when a keypad assigned to the area is locked for 2 minutes due to 3 wrong PIN entries
ENTRY	58	Area entry	Area entry time is active
EXIT	59	Area exit	Area exit time is active
EXITFAULT	60	Exit fault	Alarm detected during exit state before changing to part or full set state
RTS	61	Ready to Set	Active when all configured RTS conditions are valid
SETOK	62	Area set OK	Active for 2 s when area set successfully
SETFAULT	63	Area set failed	Active during 30 s after unsuccessful area setting
UNSETOK	64	Area unset OK	Active for 2 sec when area has been unset
ALARMACK	65	Alarms to ACK	Alarms present waiting for acknowledge
FIRERESET	66	Fire reset	For FIRE zone, event active for 10 s after fire alarm acknowledge (also inhibits fire zone for 15 s). Also active for 10 s during fire zone walk test
WALK	67	Walk test	User/Installer Walk test is active
WALKZNACTV	68	Walk test zone active	Zone in walk test is activated
A-ALARM	69	A-Alarm	A-alarm active (unconfirmed alarm), reset after unset or expiration of AB timer and no B-alarm.
B-ALARM	70	B-Alarm	B-alarm active (confirmed alarm). Reset after unset
ISIREN	71	Internal siren	Internal siren. Activated on alarm during the internal siren time. Activation may be delayed by Siren delay time. Can be retriggered by next alarm.

Event	#	Event description	Notes
ESIREN	72	External siren	External siren. Activated on alarm during the external siren time. Activation may be delayed by Siren delay time. This flag can not be retriggered.
STROBE	73	Strobe output	Strobe output. Activated by alarm during Set. Deactivated after unset.
BUZZER	74	Buzzer output	Buzzer output flag
AMRESET	75	AM reset	Activated during set procedure to reset AM detectors
PARTSET2	76	Area part set 2	Area is in part set 2 state.
AS_WARNING	77	Autoset warning	Area in warning state prior to autoset
AUTO_SET	78	Autoset	Autoset procedure is in progress
HA-ALARM	79	A hold-up alarm	Reset after unset
HB-ALARM	80	B hold-up alarm	Reset after unset
ZNINH LIMIT	81	Inhibit limit	Zone inhibit limit is reached
ZNISOL LIMIT	82	Isolation limit	Zone isolation limit is reached
ZNSHT LIMIT	83	Shunt limit	Zone shunt limit is reached
ZNISOL FAULT	84	Faulty zone isolated	
UNSETDELAY	85	ATM unset delay	ATM unset delay is active
UNSETTIME	86	ATM unset time	ATM unset time is active
UNSETWARNTIME	87	ATM unset warning time	ATM unset warning time is active
UNSEXTTIME	88	ATM extended unset time	Extended ATM unset time is active
AREA DSHUNT	89	Door shunt	A zone in the area is shunted
AREA DSHUNTWARN	90	Door shunt warning	A zone in the area is in shunt warning time
UNSETDELAYED	91	Unset delayed	Area unset delayed
PROHIBITUNSET	92	Prohibit unset	User unset prohibited
ZNSHUNT	93	Zone shunted	A zone in the area is shunted
SHUNTFault	94	Faulty zone shunted	A zone in the area is in the shunt fault state
SENSRESET	95	Sensor reset	
SCH ACTIVE	96	Schedule active	
ZNMAINSFAIL	97	Zone mains fail	At least one zone in mains fault
ZNJAMFAIL	98	Zone jamming	At least one zone in jamming
FAULTACK	99	Fault acknowledge	Faults are waiting for acknowledge

Group: Keypad

Event	#	Event description	Notes
OFFLINE	1	Keypad is offline	Active if a keypad is offline
RTE	2	RTE triggered	Keypad RTE input triggered
CODETAMPER	3	Code tamper	Active when a keypad is locked for 2 minutes due to 3 wrong PIN entries
TAMPER	4	Keypad tamper	Keypad tamper
DURESS	5	Duress code	Duress code entered on this keypad
ACTIVE CARD	6	Presented card	A card is read on this keypad, active for 3 s
PIN	7	Valid PIN	Valid PIN entered on this keypad, active for 3 s
DOORACC	8	Valid PIN or card	Valid PIN or card entered on this keypad, active for 3 s
LOCKED	9	Keypad is locked	Code tamper. It restores after the timeout has expired.
ISOLATED	10	Keypad is isolated	
CHIME	11	Keypad chime active	
VALID CARD	12	Valid card	Valid card entered on this keypad, active for 3 s
EXIT STARTED	13	Exit time started	Exit time started during set from the selected keypad
ENTRY STOPPED	14	Entry time stopped	Entry time stopped during unset from the selected keypad
UNKNOWN CARD	15	Card is not recognized	
SCH ACTIVE	16	Schedule active	

Group: Expander

Event	#	Event description	Notes
OFFLINE	1	Expander is offline	Active if device is offline
MAINSFAULT	2	Mains fail	
BATTFAULT	3	Battery fail	
TAMPER	4	Expander tamper	Device tamper
FUSEFAULT	5	Fuse fault	
SIRENFAULT	6	Siren fault	
RCVFAULT	7	Receiver fault	Wireless expander receiver fault
ISOLATED	8	Expander isolated	
BATTLOW	9	Battery low	Expander battery is low
BTESTACTV	10	Battery test active	Expander battery test is active
BTESTFAIL	11	Battery test failed	Expander battery test failed
POWER UNIT FA	12	Expander PSU fail	

Event	#	Event description	Notes
Sync in prog.	13	Synchronization in progress	DGP configuration synchronization in progress
Group: Panel			
Event	#	Event description	Notes
MAINSFAULT	1	Mains fault	Panel mains fault detected
BATTFAULT	2	Battery fault	
TAMPER	3	Panel tamper	
FUSEFAULT	4	Panel fuse fault	
SIRENFAULT	5	Panel siren fault	
LF	6	Line fault	A line fault is detected
LFGSM	7	GSM line fault	GSM line fault detected
FTC	8	Failed To Communicate	Failed to deliver an alarm message
MIFGSM	9	Line fault GSM	GSM dialler fault
NTPFAULT	10	NTP server connection fault	NTP server connection fault
LFETH	11	Ethernet line fault	Ethernet connection fault
LFIP	12	IP fault	Ethernet IP is not configured
LFGPRS	13	GPRS line fault	GPRS connection fault
LFIPGPRS	14	GPRS IP fault	GPRS IP is not configured
LFTDA	15	TDA line fault	TDA module line fault
LFTDAGPRS	16	TDA GPRS fault	TDA module line fault (GPRS)
LFTDAETH	17	TDA ETH fault	TDA module line fault (ETH)
MIFTDA	18	TDA MI fault	Panel MI device fault (TDA)
GSMJAMMING	19	GSM jamming	GSM jamming detected
POWER UNIT FA	20	Panel PSU fail	
BTESTACTV	21	Panel battery test active	
BTESTFAIL	22	Panel battery test fail	
DLRBATTFAULT	23	Dialer battery fault	
MODRESET	24	Dialer module reset	
DEVTAMPERINH	25	Panel tamper inhibited	
SIRTAMPERINH	26	Siren tamper inhibited	
LF WAN	27	Line fault (WAN on ETH)	

Group: User

Event	#	Event description	Notes
CARDPIN	1	Card or PIN presented	Valid Card or PIN presented by the selected user. Active for 3 s after event. Can be used to control door lock for specific users.
SMSCONTROL	2	SMS control active	SMS control is active
SMSCONTROLLOCK	3	SMS control locked	SMS control is disabled by invalid attempts
SMSREPORTING	4	SMS reporting active	SMS reporting is active
SMSREPAFTERSET	5	SMS reporting after set	SMS reporting will be activated after set

Group: Output

Event	#	Event description	Notes
ACTIVE	1	Output active	Specified output activates
ON	2	Output on	Physical output activates
FORCED	3	Door forced output	

Group: Filter

Event	#	Event description	Notes
ACTIVE	1	Condition true	The selected filter condition is true / valid.

Group: User group

Event	#	Event description	Notes
CARDPIN	1	Card or PIN presented	Valid Card or PIN presented by a user from the selected user group. Active for 3 s after event. Can be used to control sirens for specific user groups.
SCH ACTIVE	2	Schedule active	

Group: System

Event	#	Event description	Notes
ALLSET	1	All set	All areas in the system are set
AUTOANS	2	Auto Answer	Auto answer procedure started (1 min)
RCONNACTV	3	Remote connection	Remote connection active
RCONNFALL	4	Remote connection fail	Remote connection fail (1 min)
LPRGACTV	5	Local programming	Local programming active
RPRGACTV	6	Remote programming	Remote programming active
TIMECHG	7	Time Changed	System time changed
SSAVER	8	Armed display	Armed display active
ISIREN	9	Internal siren	Internal siren event flag (system flag)

Event	#	Event description	Notes
ESIREN	10	External siren	External siren event flag (system flag)
STROBE	11	Strobe output	Strobe event flag (system flag)
SYSFAULT	12	Global fault	Global system fault flag
SYSTAMPER	13	Global tamper	Global system tamper flag
SERVICEIN	14	Service in active	Service in is active for the installer
WT MODE ON	15	Walk test mode on	
Detector Test	16	Detector test active	
DT FAILED	17	Detector test failed	
AR HRCHY 1	18	Hierarchy 1	All hierarchy 1 areas are set
AR HRCHY 2	19	Hierarchy 2	All hierarchy 2 areas are set
AR HRCHY 3	20	Hierarchy 3	All hierarchy 3 areas are set
POWERUPREPFAI	21	System power up reporting failure	
Cloud avl.	22	The panel is ready for UltraSync cloud connection	The panel has serial number
Cloud reg.	23	The panel is registered in UltraSync cloud	
UltraSync SIM	24	UltraSync SIM card is present in the GSM module	
RFU in prog.	25	Remote firmware upgrade in progress	
Dev RFU actv	26	Remote device firmware upgrade in progress	
OH/IRIS reporting	27	OH/IRIS reporting enabled from UltraSync web portal	

Group: Door

Event	#	Event description	Notes
Disabled	1	Door disabled	
Unlocked	2	Door unlocked	Door unlocked until locked manually or by a schedule
Unlocked PRD	3	Door unlocked period	Door unlocked automatically
T-unlocked	4	Door timed unlock	Door unlocked for a specified time
Open	5	Door open	Door is unlocked for the time configured in its configuration.
Opened	6	Door opened	Door zone is in active/tamper state
Forced	7	Door forced	Door zone has been activated without unlocking
DOTL	8	Door DOTL	Door zone active after shunt time

Event	#	Event description	Notes
Shunting	9	Door shunting	Door zone has been shunted
Shunt Warning	10	Door shunt warning	
Reader Fault	11	Door reader fault	Door reader communication problem
Reader Tamper	12	Door reader tamper	Door reader tamper is active
Door Unsecure	13	Door unsecured	Door zone is in active/tamper state, or door is unlocked, or the second door zone is in active/tamper state
Door Input	14	Door input	Door zone is in active/tamper state
Output Active	15	Door output active	Door output active state (the flag is activated even if no door output assigned)

Group: CS

Event	#	Event description	Notes
FTC	1	Failed To Communicate	Failed to deliver an alarm message
HB fault	2	OH heartbeat fault	OH protocol heartbeat fault
BUSY	3	CS busy	CS is busy (in use)

Group: Trigger

Event	#	Event description	Notes
S1 1230/34	1	Fob button 1	Toggle state when fob button 1 is pressed
S2 1230/34	2	Fob button 2	Toggle state when fob button 2 is pressed
S1S2 1230/34	3	Fob buttons 1 and 2	Set state when fob button 1 is pressed, reset state when fob button 2 is pressed
REMOTEOUT	4	Remote control	
FUNCTION KEY	5	Function key control	
SCHEDULE	6	Schedule control	
FOB	7	Trigger is activated by a fob	

Group: Calendar

Event	#	Event description	Notes
CALHOUR	1	Every hour	The event flag is toggled every hour at 00 min
CALDAY	2	Every day	The event flag is toggled every day at 00:00
Monday	3	Monday	Active on Mondays
Tuesday	4	Tuesday	Active on Tuesdays
Wednesday	5	Wednesday	Active on Wednesdays
Thursday	6	Thursday	Active on Thursdays
Friday	7	Friday	Active on Fridays

Event	#	Event description	Notes
Saturday	8	Saturday	Active on Saturdays
Sunday	9	Sunday	Active on Sundays

Group: Fob ATS1235+

Event	#	Event description	Notes
Fob learned	1	Fob programmed	Active for 3 seconds after a successful programming
Button 1	2	Button 1 pressed	
Button 2	3	Button 2 pressed	
Button 3	4	Button 3 pressed	
Button 4	5	Button 4 pressed	
Button 1+2	6	Buttons 1 and 2 pressed	
Button 1+3	7	Buttons 1 and 3 pressed	
Button 1+4	8	Buttons 1 and 4 pressed	
Button 2+3	9	Buttons 2 and 3 pressed	
Button 2+4	10	Buttons 2 and 4 pressed	
Button 3+4	11	Buttons 3 and 4 pressed	
FOBBATTLOW	12	Fob battery low	

Group: Camera

Event	#	Event description	Notes
Pic captured	1	Picture has been taken	Active for 3 seconds
Pic limit exc	2	Picture limit has been exceeded	

Group: Area group

Event	#	Event description	Notes
SET	1	All areas set	All areas in area group are set
PSET1	2	All part set 1	All areas in area group are part set 1
PSET2	3	All part set 2	All areas in area group are part set 2
RTS	4	All ready to set	All areas in area group are in Ready to Set state
UNSET	5	All unset	All areas in area group are unset
FULLSET	6	All full set	All areas in area group are in full set state
ALARM	7	An alarm state	At least one area is in alarm

Event	#	Event description	Notes
EXIT	8	An exit state	At least one area is in exit state
NRTS	9	Not ready to set	At least one area in area group is in not Ready to Set state
AREASET	10	An area has been set	Active for 3 s
AREAUNSET	11	An area has been unset	Active for 3 s

Group: Schedule

Event	#	Event description	Notes
SCH ACTIVE	1	Schedule active	

Group: Special day

Event	#	Event description	Notes
SP DAY ACTIVE	1	Special day is active	

Group: Reader

Event	#	Event description	Notes
OFFLINE	1	Reader is offline	
TAMPER	2	Reader tamper	

Table 34: Door controller events**Group: Door**

Event	#	Event description	Notes
Door open	1		Door open command is active (to unlock / start shunt)
Door unlocked	2		Unlock output is active to unlock the door
Door locked	3		Unlock output is deactivated to lock the door
Door override	4		The low security schedule assigned to the door is valid
D.ovr.inhibit	5	Door override inhibit	The low security schedule is inhibited
Door disabled	6		Door is disabled completely (from keypad or computer)
Door enabled	7		
Reader disabld	8		Door reader is disabled
Reader enabled	9		Door reader is enabled
2 card inside	10		Two Card access is required at the "IN" reader

Event	#	Event description	Notes
2 card outside	11		Two Card access is required at the "OUT" reader
Low sec.inside	12	Door low security inside	Card or PIN required to access at the "IN" reader
Low sec.outs.	13	Door low security outside	Card or PIN required to access at the "OUT" reader
Anti-passback	14		Anti-Passback is active
Door shunting	15		Shunt timer is running
Shunt warning	16		Shunt warning timer is running
D. Area armed	17		Area assigned to the door is armed. As a macro output, this event disables a door when "Deny access when set" is set to Yes.
Keypad duress	18		Duress PIN entered at door keypad
DOTL	19		Door contact is active after shunt timer has expired
Forced	20		Door contact is active with no valid door command
LED 1	21		LED 1 output is active
LED 2	22		LED 2 output is active
Buzzer	23		Door buzzer output is active

Group: Door access

Event	#	Event description	Notes
Interlock	1		Interlock zones are active
Intlck.override	2		Interlock has been overridden
Denied	3		Door access has not been allowed
Granted	4		Door access has been allowed
Granted traced	5		Door access has been granted to a user with trace On
Granted 1badge	6		Door access has been granted when read card once
Granted 2badge	7		Door access has been granted when read card twice
Granted 3badge	8		Door access has been granted when read card three times
Granted IN btn	9		Door access has been granted and IN button pressed
Granted OUTbtn	10		Door access has been granted and OUT button pressed
Fire override	11		Secondary override is active
Normal	12		The door is locked and closed.

Event	#	Event description	Notes
Anti-psbck dis	13	Anti-passback disable	Disable anti-passback for selected door

Group: Region

Event	#	Event description	Notes
Limit	1	Region limit	Active when the number of people in any region reaches the present limit (255 events, 1 per region)
Usr to Outside	2	Move users in region to outside region 1	Move users from selected region (1 to 255) to outside region 1 (255 events)
All to Outside	3	Move all users to outside region 1	Move all users to outside region 1
Usr to No Reg	4	Reset users in region to region 256 (no region)	Region value of users in the selected region (1 to 255) is reset to 256 (255 events, 1 per region)
All to No Reg	5	Reset all users regions to 256 (no region)	Region value of all users is reset to 256
Schedule activ	6	Schedule active	Activated if selected schedule is active (24 events, 1 per schedule)

Group: Faults

Event	#	Event description	Notes
D.reader fault	1	Door reader fault	
D.lock fault	2	Door lock fault	
RAS offline	3		RAS on door controller local data bus is offline (16 events, 1 per RAS address)
DGP offline	4		DGP on ATS1260 local data bus is offline
DGP mains fail	5	Door controller mains fail	Mains fail condition exists on the door controller
DGP low batt	6	Door controller low battery	Low battery condition exists on the door controller
DGP fuse flt	7	Door controller fuse fail	Fuse Fail condition exists on the door controller
DGP siren flt	8	Door controller siren fail	Siren fail (siren tamper) condition exists on this door controller
DGP tamper	9	Door controller tamper	Cabinet tamper condition exists on this door controller
DGP offline	10	Door controller DGP offline	Door controller is not communicating with the control panel

Group: Other

Event	#	Event description	Notes
Area disarmed	1	Area disarmed	Area disarmed (16 events, 1 per area)
Area alarm	2	Area alarm	Zones in alarm in area (16 events, 1 per area)
DGP out.active	3	DGP outputs	System output assigned to this DGP is active (16 events, 1 per outputs). First 16 on DGP can also be activated by physical output function
DGP zone active	4	Zones	Zone on this DGP active (16 events, 1 per zone)
Phys.out activ	5	Physical outputs	Output connected to this DGP is active (255 events, 1 per output). Outputs above 16 are only activated by door macro.
DGP bat.t.act	6	Door controller battery test active	The battery test on this door controller is running
DGP bat.t.fail	7	Door controller battery test fail	The battery test failed on this door controller
DGP siren act	8	Door controller siren active	The siren output (16th relay) is active

Appendix B

AXON reporting codes

Table 35 below shows descriptions of SIA, CID, and VdS reporting codes used in AXON.

Table 36 on page 443 lists allowed values for the appropriate reporting codes.

Table 35: SIA, CID, and VdS reporting code descriptions

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
1.	AN	0xB0	14	R393	Detector dirty restore		Low
2.	AR	0xB2	7	R301	AC restore		Low
3.	AS	0x30	14	E393	Detector dirty		Low
4.	AT	0x32	7	E301	AC trouble		Medium
5.	BA	0x22	3	E130	Burglary alarm	Alarm / input in mask / trouble when set	Medium
6.	BB	0x51	11	E570	Burglary bypass	Alarm inhibit	Low
7.	BC	0xA2	3	E406	Burglary cancel	Cancel alarm by user / key / remotely	Low
8.	BJ	0xB0	14	R381	Detector supervision restore		Low
9.	BR	0xA2	3	R130	Burglary restore		Low
10.	BT	0x30	14	E380	Burglary trouble	Input in mask / trouble when unset	Low
11.	BU	0xD1	11	R570	Burglary unbypass	Alarm uninhibit	Low
12.	BV	0x00	5	E139	Alarm confirm	ACPO	Medium
13.	BW	0x80	5	R139	Restore confirmed alarm	ACPO	Low
14.	BZ	0x30	14	E381	Detector supervision		Low
15.	CF	0x61	8	E408	Forced closing	Set by user / by key	Low
16.	CG	0x62	8	E456	Part set	Part set by user / by key / remotely	Low
17.	CL	0x61	8	R401	Closing normal	Set by user	Low

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
				R407	Closing normal	Set remotely	Low
				R409	Closing normal	Set by key	Low
18.	EE	0x30	14	E374	Exit error	Exit fault	Medium
19.	ER	0xB0	14	R143	Expansion restore	Expander / keypad trouble restore	Low
				R300	Expansion restore	Expander fuse restore	Low
				R330	Expansion restore	Expander / keypad communication restore / picture memory released manually	Low
				R333	Expansion restore	External module restore	Low
20.	ET	0x30	14	E143	Expansion trouble	Expander / keypad trouble / picture memory full	Low
				E300	Expansion trouble	Expander fuse failure	Low
				E330	Expansion trouble	Expander / keypad communication fault	Low
				E333	Expansion trouble	External module fail	Low
21.	FA	0x10	1	E110	Fire alarm		High
22.	FB	0x51	11	E570	Fire bypass	Fire inhibit	Low
23.	FJ	0xB0	14	R373	Fire trouble restore		Low
24.	FR	0x90	1	R110	Fire restore		Low
25.	FT	0x30	14	E373	Fire trouble		Low
26.	FU	0xD1	11	R570	Fire unbypass	Fire uninhibit	Low
27.	FW	0x30	14	–	Fire long supervision		Low
28.	HA	0x24	9	E121	Holdup alarm	Duress	High
29.	HR	0xA4	9	R121	Holdup restore	Duress restore	Low
30.	JP	0x63	14	E466	Service in		Low
31.	JR	0xE3	14	R466	Service out		Low
32.	JT	0x53	14	E625	Time changed		Low
33.	LB	0x01	14	E627	Local programming begin		Low
34.	LR	0xBA	12	R351	Line restore		Low
35.	LS	0x81	14	R628	Local programming stop		Low
36.	LT	0x3A	12	E351	Line fault		Low
37.	MA	0x48	10	E100	Medical alarm		High
38.	MB	0x51	11	E570	Medical bypass		Low
39.	MJ	0xB0	14	–	Medical long supervision restore		Low

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
40.	MR	0xC8	10	R100	Medical restore		Low
41.	MS	0x30	14	–	Medical long supervision		Low
42.	MU	0xD1	11	R570	Medical unbypass		Low
43.	OP	0xE1	8	E401	Unset normal	Unset by user	Low
				E407	Unset normal	Unset remotely	Low
				E409	Unset normal	Unset by key	Low
44.	OR	0xE1	8	E406	Unset from alarm	Unset by user / key / remotely	Low
45.	PA	0x21	2	E120	Panic alarm		High
46.	PB	0x51	11	E570	Panic bypass		Low
47.	PJ	0xA1	2	R375	Panic trouble restore		Low
48.	PR	0xA1	2	R120	Panic restore		Low
49.	PT	0x21	2	E375	Panic trouble		Low
50.	PU	0xD1	11	R570	Panic unbypass		Low
51.	RB	0x74	14	E416	Remote programming begin		Low
52.	RP	0x40	0	E602	Automatic test / ring-in test		Low
53.	RR	0x53	15	E305	Power up	System power-up	Low
54.	RS	0xF4	14	R416	Remote programming success		Low
55.	RU	0x55	14	R416	Remote programming fail		Low
56.	RX	0x40	0	E601	Manual CS test		Low
57.	TA	0x23	4	E144	Tamper alarm	Zone tamper	Medium
				E145	Tamper alarm		Medium
				E320	Tamper alarm	Expander siren tamper	Medium
58.	TB	0x51	11	E570	Tamper bypass		Low
59.	TR	0xA3	4	R144	Tamper restore	Zone tamper restore	Low
				R145	Tamper restore		Low
				R320	Tamper restore	Expander siren restore	Low
				R370	Tamper restore	KeyBox tamper restore	Low
60.	TT	0x23	4	E370	KeyBox zone active		High
61.	TU	0xD1	11	R570	Tamper unbypass		Low
62.	UB	0x51	14	E570	Expander / keypad / zone bypassed	Expander / keypad / zone isolated	Low

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
63.	UU	0xD1	14	R570	Expander / keypad / zone unbypassed	Expander / keypad / zone de-isolated	Low
64.	WF	0xF6	13	E612	Walk test fail		Low
65.	WP	0x76	13	E611	Walk test pass		Low
66.	XH	0xB0	14	R344	RF jamming restore		Low
67.	XQ	0x30	14	E344	RF jamming		Low
68.	XR	0xB0	14	R384	Detector or fob low battery restore		Low
69.	XT	0x30	14	E384	Detector or fob low battery		Low
70.	YC	0x37	12	E350	Communications fail	GSM device fail	Low
71.	YK	0xB9	12	R354	Communications restore	GSM device restore	Low
72.	YR	0xB3	6	R302	System battery / fuse restore	Expander / dialler battery / fuse restore	Low
73.	YS	0x39	12	E354	Communication trouble	Fail To Communicate (FTC)	Low
74.	YT	0x33	6	E302	System battery / fuse trouble	Expander / dialler battery low / fuse fault	Low
75.	ZA	0x40	13	E152	Technical alarm — low temperature	Low temperature detector alarm	Medium
76.	ZB	0x51	11	E570	Technical bypass — low temperature	Low temperature detector inhibit	Low
77.	ZJ	0xB0	14	R381	Technical long supervision restore — low temperature	Low temperature detector long supervision restore	Low
78.	ZR	0xC0	13	R152	Technical restore — low temperature	Low temperature detector restore	Low
79.	ZS	0x30	14	E381	Technical long supervision — low temperature	Low temperature detector long supervision alarm	Low
80.	ZU	0xD1	11	R570	Technical unbypass — low temperature	Low temperature detector uninhibit	Low
81.	YA	0x23	4	E321	Siren fault		Low
82.	YH	0xA3	4	R321	Siren restore		Low
83.	NC	0x34	12	E356	CS polling fail	Heartbeat inactive	Low
84.	NR	0xB4	12	R356	CS polling restore	Heartbeat active	Low
85.	CP	0x61	8	R403	Auto set	Set by schedule	Low
86.	OA	0xE1	8	E403	Auto unset	Unset by schedule	Low
87.	OT	0x61	8	E608	Late close	Postponed auto set	Low
88.	OK	0xE1	8	R608	Early open	Manually unset before auto unset	Low

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
89.	IA	0x63	14	E313	Engineer reset request		Low
90.	IR	0xE3	14	R313	Engineer reset restore		Low
91.	GA	0x73	13	E151	Technical alarm — gas	Gas detector alarm	High
92.	GR	0xF3	13	R151	Technical restore — gas	Gas detector restore	High
93.	GB	0x51	11	E570	Technical bypass — gas	Gas detector inhibit	Low
94.	GU	0xD1	11	R570	Technical unbypass — gas	Gas detector uninhibit	Low
95.	GS	0x30	14	E381	Technical long supervision — gas	Gas detector long supervision alarm	Low
96.	GJ	0xB0	14	R381	Technical long supervision restore — gas	Gas detector long supervision restore	Low
97.	KA	0x78	5	E158	Technical alarm — high temperature	High temperature detector alarm	Medium
98.	KR	0xF8	5	R158	Technical restore — high temperature	High temperature detector restore	Medium
99.	KB	0x51	11	E570	Technical bypass — high temperature	High temperature detector inhibit	Low
100.	KU	0xD1	11	R570	Technical unbypass — high temperature	High temperature detector uninhibit	Low
101.	KS	0x30	14	E381	Technical long supervision — high temperature	High temperature detector long supervision alarm	Low
102.	KJ	0xB0	14	R381	Technical long supervision restore — high temperature	High temperature detector long supervision restore	Low
103.	WA	0x72	13	E154	Technical alarm — water	Water detector alarm	Medium
104.	WR	0xF2	13	R154	Technical restore — water	Water detector restore	Medium
105.	WB	0x51	11	E570	Technical bypass — water	Water detector inhibit	Low
106.	WU	0xD1	11	R570	Technical unbypass — water	Water detector uninhibit	Low
107.	WS	0x30	14	E381	Technical long supervision — water	Water detector long supervision alarm	Low
108.	WJ	0xB0	14	R381	Technical long supervision restore — water	Water detector long supervision restore	Low

#	SIA code	VdS code	VdS chan.	CID code	Function	Note	Reporting priority
109.	ES	0x23	4	E145	Tamper alarm	Expander / keypad tamper alarm	Medium
				E341	Tamper alarm	External module tamper	Medium
110.	EJ	0xA3	4	R145	Tamper restore	Expander / keypad tamper restore	Medium
				R341	Tamper restore	External module tamper restore	Medium
111.	HV	0x00	2	E129	Hold-up alarm confirm		Medium
112.	HW	0xA1	2	R129	Confirmed hold-up alarm restore		Low
113.	UA	0x00	5	E150	Technical zone — general alarm		Medium
114.	UR	0x80	5	R150	Technical zone — general alarm restore		Medium
115.	TS	0x71	13	E607	Single zone walk test start / battery test start	Start of single zone test, also for multiple zones selected / battery test start	High
116.	TE	0xF1	13	R607	Single zone walk test end / battery test end	End of single zone test, also for multiple zones selected / battery test end	Low
117.	LU	0x55	14	R628	Local programming fail		Low
118.	YP	0x32	7	E301	Power Supply Trouble		Low
119.	YQ	0xB2	7	R301	Power Supply Restored		Low
120.	CI	0xF9	8	E455	Autoset fail		Low
121.	DD	0xFA	—	E421	Access denied	Card is unknown	Low
122.	JA	0x23	—	R461	Wrong Code Entry	Code tamper	Low
123.	EX	0x54	14	E308	Device fault	System or device fault and reboot	Low
124.	JV	—		E928	PIN changed		Low
125.	JX	—		E928	User deleted		Low
126.	JY	—		E928	User added		Low
127.	RO	0x40	13	E150	Technical alarm — Relay open	Relay open	Low
128.	RC	0xC0	13	R150	Technical alarm — Relay closed	Relay closed	Low

Table 36: SIA and CID reporting code values

#	SIA code	Subevent type and range	CID code	Group range	Point range
1.	AN	Zone (1–512)	R393	Area (1–64)	Zone (1–512)
2.	AR	Expander (299–307)	R301	System (0)	Expander (65–72)
3.	AS	Zone (1–512)	E393	Area (1–64)	Zone (1–512)
4.	AT	Expander (299–307)	E301	System (0)	Expander (65–72)
5.	BA	Zone (1–512)	E130	Area (1–64)	Zone (1–512)
6.	BB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
7.	BC	System (0), User (1–50)	E406	Area (1–64)	User (0), User (1–50)
8.	BJ	Zone (1–512)	R381	Area (1–64)	Zone (1–512)
9.	BR	Zone (1–512)	R130	Area (1–64)	Zone (1–512)
10.	BT	Zone (1–512)	E380	Area (1–64)	Zone (1–512)
11.	BU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
12.	BV	Zone (1–512)	E139	Area (1–64)	Zone (1–512)
13.	BW	Zone (1–512)	R139	Area (1–64)	Zone (1–512)
14.	BZ	Zone (1–512)	E381	Area (1–64)	Zone (1–512)
15.	CF	User (1–50) Zone (1–512)	E408	System (0) Area (1–64)	User (1–50) Zone (1–512)
16.	CG	User (1–50), Zone (1–512)	E456	System (0) Area (1–64)	User (1–50) Zone (1–512)
17.	CL	Keypad (401–408)	–	–	–
		User (1–50)	R401	Area (1–64)	User (1–50)
		System (0)	R407	System (0)	
		Zone (1–512)	R409	Area (1–64)	Zone (1–512)
18.	EE	Zone (1–512)	E374	Area (1–64)	Zone (1–512)
19.	ER	Expander (299–307), keypad (401–408)	R143	System (0)	Expander (65–72), keypad (1–8)
		Expander fuse (316–324)	R300	System (0)	Expander (65–72)
		Expander poll (332–340), keypad poll (465–472)	R330	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512), Expander (299–307), keypad (401–408)	R333	Area (1–64)	Zone (1–512)
20.	ET	Expander (299–307), keypad (401–408)	E143	System (0)	Keypad (1–8), Expander (65–72)
		Expander fuse (316–324)	E300	System (0)	Expander (65–72)
		Expander poll (332–340), keypad poll (465–472)	E330	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512), Expander (299–307), keypad (401–408)	E333	Area (1–64)	Zone (1–512)

#	SIA code	Subevent type and range	CID code	Group range	Point range
21.	FA	System (0) Zone (1–512)	E110	System (0) Area (1–64)	Keypad (1–8) Zone (1–512)
22.	FB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
23.	FJ	Zone (1–512)	R373	Area (1–64)	Zone (1–512)
24.	FR	Zone (1–512)	R110	Area (1–64)	Zone (1–512)
25.	FT	Zone (1–512)	E373	Area (1–64)	Zone (1–512)
26.	FU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
27.	FW	Zone (1–512)	–	–	–
28.	HA	User (1–50) Zone (1–512)	E121	Area (1–64) Area (1–64)	User (1–50) Zone (1–512)
29.	HR	Keypad (401–408)	R121	System (0)	Keypad (1–8)
30.	JP	System (0)	E466	System (0)	–
31.	JR	System (0)	R466	System (0)	–
32.	JT	User (1–50)	E625	–	–
33.	LB	System (0)	E627	–	–
34.	LR	Communication path (0–6) [1]	R351	System (0)	–
35.	LS	System (0)	R628	–	–
36.	LT	Communication path (0–6) [1]	E351	System (0)	–
37.	MA	System (0) Zone (1–512)	E100	System (0) Area (1–64)	Keypad (1–8) Zone (1–512)
38.	MB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
39.	MJ	Zone (1–512)	–	–	–
40.	MR	Zone (1–512)	R100	Area (1–64)	Zone (1–512)
41.	MS	Zone (1–512)	–	–	–
42.	MU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
43.	OP	User (1–50) System (0) Zone (1–512)	E401 E407 E409	Area (1–64) System (0) Area (1–64)	User (1–50) Zone (1–512)
44.	OR	User (1–50) Zone (1–512)	E406	System (0) Area (1–64)	User (1–50) Zone (1–512)
45.	PA	System (0) User (1–50) Zone (1–512)	E120	System (0) Area (1–64) Area (1–64)	Keypad (1–8) User (1–50) Zone (1–512)
46.	PB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
47.	PJ	Zone (1–512)	R375	Area (1–64)	Zone (1–512)
48.	PR	Zone (1–512)	R120	Area (1–64)	Zone (1–512)
49.	PT	Zone (1–512)	E375	Area (1–64)	Zone (1–512)

#	SIA code	Subevent type and range	CID code	Group range	Point range
50.	PU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
51.	RB	Unused (0)	E416	System (0)	–
52.	RP	Unused (0)	E602	–	–
53.	RR	Expander (299–307), keypad (401–408)	E305	System (0)	Expander (65–72), keypad (1–8)
54.	RS	System (0)	R416	System (0)	–
55.	RU	System (0)	–	–	–
56.	RX	System (0)	E601	System (0)	–
57.	TA	Zone (1–512)	E144	Area (1–64)	Zone (1–512)
		Expander (299–307), keypad (401–408)	E145	System (0)	Expander (65–72), keypad (1–8)
		Expander (316–324)	E320	System (0)	Expander (65–72)
58.	TB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
59.	TR	Zone (1–512)	R144	Area (1–64)	Zone (1–512)
		Expander (299–307), keypad (401–408)	R145	System (0)	Expander (65–72), keypad (1–8)
		Expander (316–324)	R320	System (0)	Expander (65–72)
60.	TT	Zone (1–512)	E370	Area (1–64)	Zone (1–512)
61.	TU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
62.	UB	Expander (299–307), keypad (401–408)	E570	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512)	–	–	–
63.	UU	Expander (299–307), keypad (401–408)	R570	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512)	–	–	–
64.	WF	Area (1–64)	E612	Area (1–64)	Area (1–64)
65.	WP	Area (1–64)	E611	Area (1–64)	Area (1–64)
66.	XH	Expander (299–307) Communication path (0–6) [1]	R344	System (0)	Expander (65–72)
67.	XQ	Expander (299–307) Communication path (0–6) [1]	E344	System (0)	Expander (65–72)
68.	XR	Zone (1–512) Fob (1–112)	R384	Area (1–64)	Zone (1–512)
69.	XT	Zone (1–512) Fob (1–112)	E384	Area (1–64)	Zone (1–512)
70.	YC	System (0)	E350	System (0)	–
71.	YK	System (0)	R354	System (0)	–
72.	YR	Expander (299–307)	R302	System (0)	Expander (65–72)

#	SIA code	Subevent type and range	CID code	Group range	Point range
73.	YS	System (0)	E354	System (0)	–
74.	YT	Expander (299–307) Zone (1–512)	E302	System (0)	Expander (65–72)
75.	ZA	Zone (1–512)	E152	Area (1–64)	Zone (1–512)
76.	ZB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
77.	ZJ	Zone (1–512)	R381	Area (1–64)	Zone (1–512)
78.	ZR	Zone (1–512)	R152	Area (1–64)	Zone (1–512)
79.	ZS	Zone (1–512)	E381	Area (1–64)	Zone (1–512)
80.	ZU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
81.	YA	Expander (316–324)	E321	System (0)	Expander (65–72)
82.	YH	Expander (316–324)	R321	System (0)	Expander (65–72)
83.	NC	CS (1–16)	E356	System (0)	CS (1-16)
84.	NR	CS (1–16)	R356	System (0)	CS (1-16)
85.	CP	System (0)	R403		
86.	OA	System (0)	E403		
87.	OT	User (1–50)	E608		
88.	OK	User (1–50)	R608		
89.	IA	System (0)	E313		
90.	IR	User (1–50)	R313		
91.	GA	Zone (1–512)	E151	Area (1–64)	Zone (1–512)
92.	GR	Zone (1–512)	R151	Area (1–64)	Zone (1–512)
93.	GB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
94.	GU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
95.	GS	Zone (1–512)	E381	Area (1–64)	Zone (1–512)
96.	GJ	Zone (1–512)	R381	Area (1–64)	Zone (1–512)
97.	WA	Zone (1–512)	E154	Area (1–64)	Zone (1–512)
98.	WR	Zone (1–512)	R154	Area (1–64)	Zone (1–512)
99.	WB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
100.	WU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
101.	WS	Zone (1–512)	E381	Area (1–64)	Zone (1–512)
102.	WJ	Zone (1–512)	R381	Area (1–64)	Zone (1–512)
103.	KA	Zone (1–512)	E158	Area (1–64)	Zone (1–512)
104.	KR	Zone (1–512)	R158	Area (1–64)	Zone (1–512)
105.	KB	Zone (1–512)	E570	Area (1–64)	Zone (1–512)
106.	KU	Zone (1–512)	R570	Area (1–64)	Zone (1–512)
107.	KS	Zone (1–512)	E381	Area (1–64)	Zone (1–512)

#	SIA code	Subevent type and range	CID code	Group range	Point range
108.	KJ	Zone (1–512)	R381	Area (1–64)	Zone (1–512)
109.	ES	Expander (299–307), keypad (401–408)	R145	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512), Expander (299–307), keypad (401–408)	R341	Area (1–64)	Zone (1–512)
110.	EJ	Expander (299–307), keypad (401–408)	E145	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–512), Expander (299–307), keypad (401–408)	E341	Area (1–64)	Zone (1–512)
111.	HV	Zone (1–512)	E129	Area (1–64)	Zone (1–512)
112.	HW	Zone (1–512)	R129	Area (1–64)	Zone (1–512)
113.	UA	Zone (1–512)	E150	Area (1–64)	Zone (1–512)
114.	UR	Zone (1–512)	R150	Area (1–64)	Zone (1–512)
115.	TS	Area (1–64) Expander (299–307)	E607	Area (1–64)	Area (1–64)
116.	TE	Area (1–64) Expander (299–307)	R607	Area (1–64)	Area (1–64)
117.	LU	System (0)	R628	Area (1–64)	Area (1–64)
118.	YP	Expander (299–307)	E301	System (0)	Expander (65–72)
119.	YQ	Expander (299–307)	R301	System (0)	Expander (65–72)
120.	CI	User (1–50)	E455	Area (1–64)	User (1–50)
121.	DD	Keypad (401–408) Card	E421	System (0)	Keypad (1–8)
122.	JA	Keypad (401–408)	R461	System (0)	Keypad (1–8)
123.	EX	System (0)	E308	System (0)	—
124.	JV	User (1–50)	E928	System (0)	User (1–50)
125.	JX	User (1–50)	E928	System (0)	User (1–50)
126.	JY	User (1–50)	E928	System (0)	User (1–50)
127.	RO	Zone (1–512)	E150	Area (1–64)	Zone (1–512)
128.	RC	Zone (1–512)	R150	Area (1–64)	Zone (1–512)

[1] Communication path is one of the following:

- 3: GSM
- 4: IP
- 5: TDA9xx
- 6: TDA74xx
- 7: TDA75xx
- 61: TDA74xx GPRS virtual port
- 62: TDA74xx ETH virtual port
- 71: TDA75xx GPRS virtual port
- 72: TDA75xx ETH virtual port

Note: SIA reporting range assumes expanders numbering from 0 to 8, where expander 0 is the control panel itself.

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 system allows any premises to be divided into different areas having different security requirements. Each area has its zones. Each area is identified by a number or a name. For example, area 1, Workshop, etc.
Armed	See Set.
Armed display	Armed display activates on a keypad after particular idle time. In this mode, the information displayed on LCD and LED is very limited for security reasons. A user intervention is necessary for return to a normal display mode.
Arming station (RAS)	See Keypad.
Autoset	An automatic setting of the premises started by a schedule. See Schedule.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.

Central station	A company that monitors whether an alarm has occurred in a security system. The central station is located away from the premises/area it monitors.
Condition filter	A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.
Control panel	An electronic device that is used to gather all data from zones on the premises. Depending on programming and status of areas, it generates alarm signals. If required, alarms and other events can be reported to the central station.
Cursor	A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.
Detector test	Alarm system function for detectors with a dedicated test input. After the detector test input is activated, the panel checks if proper alarm signal is provided by the detector to the system. This functionality allows testing detectors that are difficult to access.
DGP	Data gathering panel. See Expander.
Dialler	An electronic device that allows the AXON 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 ATS system with advanced access control functions.
Door group	Door groups specify when access to a specific door is granted. Door groups are assigned to users. Each Door group may have a different time period (schedule) when access to the door may be granted.
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 duress facility allows a signal to be activated (for example, notification to a central station) by the user. This is done by entering a duress digit in conjunction with a PIN.
Engineer	Personnel from an installer that is able to install and service the control panel.
Expander	A device that collects data from other security devices within an area, and transfers it to the AXON control panel.
Fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
Fob	A personal wireless device, which is used to perform programmed functions, for example, set or unset premises, open doors.

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

Nuisance alarm	An alarm that is triggered by a security device, without any burglar. It could be caused by open windows, pets or incorrect projection of security equipment.
Online / offline	Operational/non-operational. A device may be offline due to a malfunction in the device itself or it may be disconnected from the control.
Output expander	A PCB module that connects to the AXON 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 options. In the AXON configuration the PIN is associated with a user number, which identifies the PIN holder to the system.
PIR	Passive infrared detector. A security device used to detect intruders in a certain part of an area or premise. The technique used is based on infrared detection.
PIR camera	See Wireless PIR camera
Poll	An inquiry message continually sent by the AXON 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.
Remote login	The username and the password for the control panel user necessary for the remote access to this panel. The remote access includes access via IP or GPRS communication path, using the mobile application, built-in Web application, configuration or management software. Note: Connection via USB cable is not a remote connection.
Reporting	See Alarm reporting.
Request to Exit zone	A zone that is programmed to open a door using a button or PIR. Used to allow users to exit without using the door reader. Request to exit is often abbreviated to RTE. Also called egress.
Schedule	A timed set of actions.
Screen saver	See Armed display.

Set	The condition of an area where a change in the status of any zone (from normal to active) causes an alarm. An area or premise is only set when it is unoccupied. Some zones (like vaults) can remain armed continually.
Shunt	A procedure that automatically inhibits a zone from generating an alarm when it is activated. For example, shunts stop a door generating an alarm when opened for a short time.
Special day	A date when alternative time frames in an active schedule are valid.
Tamper	A situation where a zone, a keypad, control panel, expander or associated wiring are tampered with, or accidentally damaged. The tamper facility activates a signal when tamper occurs. Tamper alarms from zones are called zone tamperers.
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 system or change parameters in the system either local or remote.
User	Anybody making use of the AXON system. Users are identified to the AXON 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 or a group of devices (PIR detector, door contact) to the AXON system. Each device is identified by a zone number or a name. For example, zone 14, Fire Exit Door.

Index

2

27-bit Tecom format, 313

A

access control, **79**

 reporting, 270

access denied, 260, 269

access options, 311

access zone, 49

account, 347

action, **89, 288**, 292

 creating, 292

 deleting, 293

 name, 292

action list, 89

actions

 view, 288

active walk test, 96, 179

add

 action, 292

 central station, 329

 door, 256

 door group, 275

 event, 281

 expander, 206

 filter, 280

 floor, 277

 floor group, 278

 fob, 111, 250

 keypad, 195

 macro, 214

 output, 282

 PC connection, 354

 reader, 217

 region, 276

 schedule, 290

 special day, 293

 time frame, 291

 trigger, 286

 user, 219

 user group, 226

 zone, 228

adding a central station, 329

adding a door group, 275

adding a door to the system, 256

adding a filter to the system, 280

adding a floor group, 278

adding a floor to the system, 277

adding a macro to the system, 214

adding a PC connection, 354

adding a region, 276

adding a schedule, 290

adding a special day, 293

adding a time frame, 291

adding a trigger, 286

adding a user group, 226

adding a user to the system, 219

adding an action, 292

addressing, 34, 320

Advisor Advanced Pro, **125**

alarm, 176

 confirmation, 248

 restore, 314

alarm confirmation, 248, 316

alarm control, 259

alarm history, 170

alarm reporting, 98

alarm restore, 314

anti-mask, 232

anti-passback, **81**, 273

APN, 351

area, **55**, 230, **244**

 entry/exit time, 245

 hierarchy, 55, 248

 prealarm time, 247

 remote exit time, 245

 selection mode, 225

 unset delay, 247

 warning time, 246

area group, **55**, **249**

 assign areas, 250

 name, 250

area indicator, 201

area modifier, 331, 333

area selection mode, 225

area shunt, 262

area status, 201

arm, 57

armed display, 305

 timeout, 298

ATM, **121**, 327

- delay, 327
- extended unset time, 327
- unset time, 327
- unset warning time, 328
- ATS LAN, 191
- auto configuration, **4**, 165
- auto test, 239
- automatic battery test, **186**, **187**
- autoset, **108**, 246, 247

B

- battery
 - status, 185
- battery capacity, 188
- battery installation, 20
- battery replacement, 20, 187, 188
- battery test, **186**
 - automatic test, 186, 187
 - battery replacement, 187
 - duration, 186, 187
 - frequency, 186
- bus device, 67
- bus devices, **194**
- buzzer, 324

C

- calendar, **89**, **288**
- callback, 355
- camera, **116**, **252**
 - filter, 253, 254
 - isolate, 254
 - taking picture, 255
 - zone list, 253
- camera diagnostics, 118
- camera range test, 172
- card
 - assign, 220
 - check, 188
 - remove, 221
- card & PIN mode, 198
- card and PIN, 265
- card and PIN timeout, 298
- card format, 266
- card indication, 313
- card reader, **17**
- card to PIN time, 311
- CDC mode, 191
- central station, 329
 - backup, 99
 - creating, 329
 - deleting, 333
 - mapping, 98
 - primary, 99
- challenge code, 304
- change PIN, 220
- changing a door, 257
- changing a floor, 278
- changing a user, 219

- changing user group, 226
- check card, 188
- chime, 232, 321
- CID codes, 437
- classic addressing scheme, 320
- cloud, 358
- cloud solution, 122
- code tamper, 61, 133
- combined reporting, 99
- communication, **329**
 - account code, 330
 - auto-answer, 355
 - callback, 355
 - central station, 329
 - cloud, 358
 - destination name, 334, 357
 - destination port, 334, 357
 - Downloader, 364
 - encryption, 335
 - events, 338
 - frequent heartbeat, 335
 - GSM, 345
 - GSM network, 345, 346
 - heartbeat, 335
 - line number, 335
 - PC connection, 354
 - picture port, 336
 - protocol, 330, 332
 - receiver number, 335
 - subevents, 332
 - test, 97
 - Titan, 364
 - transmission path, 330, 339
 - UltraSync, 358
- condition filter, 86, 294
- condition filters, **280**, 283
- configuration software, 364
- configure
 - area, 244
 - area group, 250
 - condition filter, 280
 - door, 257
 - event, 215, 281
 - expander, 206
 - floor, 278
 - fob, 251
 - input, 314
 - keypad, 195
 - macro, 214
 - macro output, 216
 - output, 282
 - part set, 308
 - reader, 217
 - user, 219
 - zone, 229, 314
- confirmed alarm test, 96, 179
- connectors, 11
- creating a central station, 329
- creating a door, 256

- creating a door group, 275
- creating a filter, 280
- creating a floor, 277
- creating a floor group, 278
- creating a macro, 214
- creating a PC connection, 354
- creating a region, 276
- creating a schedule, 290
- creating a special day, 293
- creating a time frame, 291
- creating a trigger, 286
- creating a user, 219
- creating a user group, 226
- creating an action, 292
- credit, 347
- custom LCD message, 306

D

- data bus, 26, 191, 218
- date, 296
- daylight saving time, 296
- default, 193
- default values, 33
- defaulting panel, 33
- defaults, 163, 315
- de-isolate, 230, 231
- delayed unset, 58
- delete
 - door, 264
 - expander, 208
 - filter, 282
 - keypad, 205
 - macro, 216
 - notification, 361
 - output, 286
 - reader, 218
 - zone, 241
- deleting a central station, 333
- deleting a door group, 276
- deleting a floor, 278
- deleting a floor group, 279
- deleting a PC connection, 355
- deleting a region, 277
- deleting a schedule, 294
- deleting a special day, 294
- deleting a time frame, 291
- deleting a trigger, 287
- deleting a user, 225
- deleting a user group, 227
- deleting an action, 293
- demo, 189
- deny access, 269
- detector test, 174
 - auto test, 239
 - duration, 174
 - manual test, 174
 - time, 174
- device states, 194

- DHCP, 341
- dialler
 - battery, 185
- disable door, 189, 264
- disable duress, 267
- disarm, 57
- DNS, 342
- door, **79, 256**
 - alarm control, 269
 - anti-passback, 273
 - area groups, 260
 - areas, 259
 - changing, 257
 - control, 189
 - creating, 256
 - delete, 264
 - deny access, 260, 269
 - disable, 264
 - disable RTE, 269
 - door group, 80
 - DOTL output, 273
 - DOTL reporting, 271
 - DOTL zone, 267
 - EE PIN lock, 260
 - extend unlock time until opened, 268
 - extended time, 258
 - forced door, 270, 273
 - group, 275
 - indication, 264, 272
 - intelligent door, 79
 - interlock, 271
 - location, 257
 - lock, 260
 - lock when closed, 268
 - low security, 260, 272
 - move, 263
 - name, 257
 - open and close reporting, 270
 - output, 257, 275
 - outside user, 274
 - pulsed lock and unlock, 83, 268
 - reader options, 265
 - readers, 257
 - region, 273
 - reporting, 270
 - RTE, 261
 - RTE control, 270
 - RTE reporting, 271
 - RTE schedule, 272
 - RTE zone, 269
 - schedule, 261
 - second zone, 267
 - shunt, 80, 261
 - standard door, 79
 - time, 258
 - unlock, 260, 261
 - unlock time, 258
 - user group, 268
 - warning output, 273

- zone, 259
- door control, 189
- door controller, **79**
 - options, 312
 - outputs, 272
 - synchronization, 216
- door controller mode, 191
- door group, **80**, 275
 - creating, 275
 - deleting, 276
 - doors, 275
 - name, 275
- door held open, 264
- door shunt, **80**, 261, 264
 - entry/exit, 265
 - extended time, 262
 - time, 262
 - warning, 262
 - zones, 272
- door shunt time, 262
- door shunt warning, 262
- DOTL
 - output, 273
- DOTL zone, 267
- double knock, 231
 - timers, 299
- Downloader, **364**
- DST, 296
- dual loop, 207
- dual unset, 248
- duress
 - disable, 267

E

- earthing, 24
- EE fault
 - report, 311
- EN 50131 requirements, 70
- enable door, 189
- encryption, 335, 341
 - key, 356
- encryption key, 205
- encryption key number, 337
- encryption key value, 337
- end time, 291, 294
- end-of-line resistor, 31
- engineer lockout, 301
- engineer reset, **120**, 301
 - auto reset, 303
 - disable when service in, 303
- engineer walk test, 94, 176, 232
- entry
 - extend time, 233
- entry alarms, 247
- entry time, 233, 245, 311
- entry timer, 307
- entry/exit, 49, 51, 238
 - access, 308

- full set, 309
 - PIN lock, 199
- entry/exit door shunt, 265
- entry/exit time, 245
- entry/exit zone, 202
- EOL, 29, 31, 207, 240
- event, 92
- event list, 421
- events, **338**
 - mapping, 338
- exit error, 311
- exit fault, 311
 - report, 311
- exit terminator, 50, 233, 298
- exit time, 245, 311
- exit timer, 307
- expander, **68**, 194, **205**
 - dual loop, 207
 - EOL, 207
 - firmware version, 216
 - input mode, 207
 - isolate, 207
 - name, 207
 - resistor values, 207
 - settings, 206
 - single zone, 207
 - tamper, 207
 - troubleshooting, 374, 375, 376
- extend entry timer, 233
- extend test call, 180
- extended door shunt time, 262
- extended time, 258
- extended unset time, 327

F

- failed to communicate, 100
- fault, 176
- fault indication, 306
- filter, **280**
 - creating, 280
 - delete, 282
- final door, 233
- final set, 298
- fire door, 51, 52
- firewall, 343
- firmware, 366
- firmware upgrade
 - remote, 358
- firmware version, 216
- flash, 366
- flexible addressing scheme, 320
- floor, **80**, **277**
 - changing, 278
 - creating, 277
 - deleting, 278
 - floor group, 80
 - group, 278
 - name, 278

floor group, **80, 278**
 creating, 278
 deleting, 279
 floors, 279
 name, 279
 fob, 221, **250**
 add, 111, 250
 assigned user, 251
 buttons, 251
 name, 251
 remove, 252
 forced set, 309
 formula, 215, 280
 frame rate, 212
 frequent heartbeat, 335
 frequent test call, 181
 FTC, 100
 function key, 65, 201

G

gateway, 342
 glossary, 449
 GPRS, 351
 disconnection time, 352
 line fault, 352
 password, 351
 user name, 351
 GPRS monitoring, 359
 GPRS network
 registration, 184
 state, 184
 gross level, 242
 GSM, 345
 battery status, 185
 reporting, 336
 GSM network, 345
 availability, 346
 code, 185
 diagnostic, 183
 name, 184
 PIN status, 183
 registration, 184
 scan, 346
 signal strength, 185
 guard, 320

H

hardware, 191
 HDR, 172
 heartbeat, 335
 frequent, 335
 held open alarm, 237
 time, 300
 hierarchy, 248
 high current output, 324
 high security, 248
 high security region, **81, 274**
 high security user, **81, 274**

 prewarning time, 274
 host prefix, 344
 housing, **8**
 HSR, **81, 274**
 HSU, **81, 274**
 HTTPS, 319
 HW variant, 191

I

idle screen, 203
 custom message, 204
 logo, 204
 text background, 204
 text color, 204
 time and date, 204
 IN reader, 257
 inactive days, 173, 300
 indication, 240
 inhibit, **59, 231**
 inhibit limit, 249
 input, 228
 delay, 300
 options, 314
 resistance, 173
 test, 171
 input mode, 207
 input state, 171, 176
 inspection, 304
 date, 304
 installation, **163**
 installer, **69**
 in-time, 299
 user confirmation, 301
 installer code, 165
 installer in, 304
 installing battery, 20
 intelligent door, 79
 interlock, 271
 invert output, 283
 inverted walk test, 173
 timer, 300
 IP
 picture limit, 344
 IP address, 341
 IP conflict, 373, 374
 IP diagnostic, 181
 IP interface, 182
 IP statistics, 182
 isolate, **59, 230, 231**
 camera, 254
 keypad, 200
 isolation limit, 249

K

key, **61, 233**
 key box
 time, 300
 key switch, 50, 233

keypad, 14, 67, 194, 195

- backlight, 203
 - buzzer, 324
 - card beep, 203
 - card indication, 313
 - communication fault, 313
 - idle screen, 203
 - nightlight, 203
 - RTE, 203
 - system fault, 313
 - tamper, 196
 - troubleshooting, 374
- keypad layout, 139
- keypad lockout, 61, 133

L

- LAN, 191
- LAN device, 67
- layout, 10
- LCD, 388, 413
 - EE timer, 307
- LCD backlight, 202
- LCD message, 306
- LCD options, 305
- LCD reader, 218
- LDR, 172
- learn card, 220
- LED, 13, 266
- LED test, 175
- limit reports, 239, 314
- line fault
 - WAN, 344
- line number, 335
- listing open zones, 171
- local access, 344
- lock door, 189, 260
- lock user data, 70
- lock when closed, 268
- lockout, 61, 133
- log, 170
- logic, 86
- logout, 192, 304
- long supervision fault, 314
- low security, 260

M

- MAC, 344
- macro, 214
 - creating, 214
 - delete, 216
- mains fail reporting delay, 298
- manual test, 174, **181**
- map door controller relays, 313
- map panel LEDs, 313
- mDNS, 344
- menu entries, 305
 - accessing, 133
 - confirmation of changes, 138

- exit, 138
 - explanation of the LCD display, 136
 - how to edit host address, 138
 - how to edit list, 137
 - how to edit text, 137
 - how to program values, 136
 - how to program Yes/No options, 137
 - programming, 136
 - scrolling the list of menus, 135
 - unauthorized access, 133
 - using PIN, 133
- menu tree, 388, 413
- MMS, 352
 - limit, 353
 - proxy, 353
- mobile application, **125**
- mobile phone number, 223
- monitor output 3, 324
- move a door, 263
- multicast DNS protocol, 344
- multiple badge time, 312

N

- need acceptance, 135
- need to set, 178
- notification, 358
 - delete, 361
 - event, 360
 - identifier, 360
 - name, 359
 - status, 360
 - user, 360
- notification test, 190
- NTP, 183, 343

O

- OH 2000, 334
- omit first call, 340
- open door, 189
- open zones, 171
- OUT reader, 257
- output, 33, **78, 275, 280, 282**
 - active time, 285
 - add, 282
 - alarm, 275
 - delay, 285
 - delete, 286
 - DOTL, 273
 - edit, 282
 - forced door, 273
 - mode, 283
 - name, 282
 - siren, 324
 - test, 175
 - warning, 273
- outside user, 274

P

- panel diagnostics, 188
- panel ID, 356
- panel information, 190
- panel lid, 192
- panel provisioning, 126
- panel status, 176
- panel version, 190
- panic alarm, 203, 321
- part set, 57, 238
 - name, 309
 - options, 308
- PC connection, 354, 364
 - creating, 354
 - deleting, 355
 - host, 357
 - port, 357
- PCB, 10, 191
- picture auto deletion, 213
- picture frame rate, 212
- picture limit, 344
- picture options, 211
- picture port, 336
- picture quality, 212
- picture settings, 211
- PIN, **76**, 220, 345
- ping, 182, 334, 343, 357
- prealarm time, 247
- predefined user, 69
- prepaid, 347
- privilege limitation, 73
- programmable functions, 104
- programming, 86, 388, 413
- programming map, 388, 413
- programming users, 219
- programming wireless cameras, 116
- programming wireless devices, 109
- protocol, 330, 332
- pry-off tamper, 9
- PUK, 183, 345
- pulse count, 242
- pulsed lock and unlock, 83
 - door lock procedure, 84
 - door open procedure, 83

Q

- quick installation, **2**
- quick programming, **4**
- quick set, 200

R

- range test, 172
- reader, **217**, 257
 - card and PIN, 265
 - card beep, 203
 - card format, 266
 - LED, 266

- reset communication key, 205
- RTE, 203
 - schedule, 266
 - secure channel, 205
 - two cards, 265
- reader options, 265
- ready to set, 307
- receiver number, 335
- reduced walk test, 178
- region, **80**, 273, **276**
 - count limit, 214
 - creating, 276
 - deleting, 277
 - name, 277
- region count limit, 214
- regulations, 378
- reinstall, 193
- re-lock delay, 312
- remote configuration, 318, 358
 - direct IP protocol, 319
 - HTTPS, 319
 - service in, 319, 320
 - SSL, 319
 - supervisor, 319
- remote exit time, 245
- remote firmware upgrade, 358
- remote options, 318
- remove
 - fob, 252
 - RF device, 244, 252
- remove PIN, 220
- replacing battery, 20
- report code, 240
- report exit fault, 311
- reporting, 98
 - account code, 330
 - limit reports, 239, 314
 - long supervision, 314
 - tamper, 314
- request to exit, 203, 237
- resistance, 173
- resistor values, 207, 240, 322
- resolution, 212
- RF device
 - configuration, 242, 252
 - remove, 244, 252
 - supervision, 243
- RF state, 172
- ring setup, 340
- RSSI, 171, 181
- RTE, 203, 237, 261
 - control, 270
 - disabled when areas set, 269
 - schedule, 272
- RTE zone, 269
- RTS, 307

S

schedule, **89**, 266
 action list, 292
 active schedule, 290
 condition filter, 294
 creating, 290
 date, 290
 deleting, 294
 door unlock, 261
 name, 290
 RTE, 272
 special day, 293
 time, 290
 time frame, 291
 scheme, 34, 320
 secure channel, 205
 secure cloud, 122
 sensor type, 236
 serial number, 191, 358
 service, **170**
 time, 299
 user confirmation, 301
 service in, 135, 192, 304
 set, **57**
 set options, 307
 shielding, 25
 shock sensor, 174, 233, 242
 sensitivity, 242
 shunt, 51, **59**, 174, 239
 door, 80, 261
 time, 262
 type, 262
 zone, 59
 shunt limit, 249
 shunt zones, 272
 SIA codes, 437
 SID, 358
 silent set, 248
 SIM, 345
 single zone, 207
 single zone walk test, 179
 siren, 32, 322
 siren EOL, 322
 siren output, 324
 siren tamper input EOL, 322
 siren timers, 297
 Site Manager, **126**
 site provisioning, 126
 SMS, 349
 center, 349
 charset, 350
 control, 74, 223
 counter, 185
 forwarding, 349
 header, 350
 messages limit, 350
 PIN, 350
 reporting, 74, 223

soak test, 232
 time, 300
 software revision, 190
 special day, 288, 293
 creating, 293
 deleting, 294
 end time, 294
 name, 294
 start time, 294
 special walk test mode, 179
 SSL, 319
 standard door, 79
 standard walk test, 177
 start filter, 283
 start time, 291, 294
 status, 176
 stop filter, 283
 subevents, **332**
 supervision, 243
 supervisor, 320
 SVCP, 338
 swinger shunt, 231, 314
 synchronization, 216
 system code, 303
 system data bus, 191
 system fault, 190, 313
 system options, **296**

T

tamper
 keypad, 196
 tamper area, 196
 technical alarm, 234
 technical zone sensor, 236
 terminals, 11
 test, 170
 battery, 186
 communication, 97
 test call, 179, 181
 extend test call, 180
 frequent test call, 181
 FTC, 181
 test duration, 174
 test time, 174
 testing system, **94**
 time and attendance, 267
 time and date, 296
 time frame, 288
 creating, 291
 deleting, 291
 end, 291
 start, 291
 week days, 291
 time zone, 296
 timed open, 189
 timed unset, 327
 delay, 327
 extended time, 327

- time, 327
 - warning time, 328
- timers, **296**
- Titan, 364
- transmission path, 330, 339
- trigger, **88, 280, 286**
 - creating, 286
 - deleting, 287
 - name, 286
 - state, 176
 - user group, 287
- troubleshooting, **373**
 - data gathering panels, 374, 375, 376
 - LCD keypads, 374
- two cards, 265
- two cards time, 312

U

- UltraSync, **122**, 358, 359
 - channel, 337
 - password, 358
- uninhibit, 231
- unlock door, 189, 260
 - output, 257
- unset, **57**
 - delayed unset, 58
- unset delay, 247
- upgrade, 366
- user, **69, 219**
 - area selection mode, 225
 - card, 220
 - changing, 219
 - creating, 219
 - deleting, 225
 - language, 221
 - PIN, 220
 - programming, 219
 - user group, 226
- user card, 220
- user confirmation, 301
- user data lock, 70
- user group, **71, 226**, 268, 287
 - changing, 226
 - creating, 226
 - deleting, 227
 - functions, 71
 - name, 226
 - options, 227
 - privilege limitation, 73
 - type, 226
- user group type, 71
- user LCD message, 306
- user management, 219
- user name, **220**
- user phone, 223
- user privilege, 226
- user programmable functions, 104
- user walk test, 176, 178, 233

- using wireless cameras, 116

V

- VdS
 - encryption key number, 337
 - encryption key value, 337
 - SVCP, 338
 - version, 337
- VdS codes, 437
- VdS options, 337
- version, 337, 366
- virtual zone, 237

W

- walk test, **94**, 96, 176, 179, 232
 - active walk test, 96, 179
 - confirmed alarm, 96, 179
 - frequency, 178
 - reduced walk test, 178
 - single zone, 179
 - standard walk test, 177
 - timeout, 298
- walk test mode, 96, 179
- WAN line fault, 344
- warning time, 246, 328
- webserver, 319
 - access, 319
- week days, 291
- wireless camera, **116**
- wireless device, **109**, 242, 252
 - supervision, 243
- wireless sensor, 109

Z

- zone, **49, 228**
 - access, 238
 - area, 230
 - auto test, 239
 - connection, 27
 - copy, 240
 - de-isolate, 230, 231
 - delete, 241
 - entry/exit, 238
 - entry/exit time, 245
 - held open alarm, 237
 - indication, 240
 - inhibit, 231, 308
 - isolate, 230, 231, 239
 - limit reports, 239
 - move, 241
 - name, 229
 - open too long, 237, 300
 - options, 230, 314
 - part set, 57
 - prealarm time, 247
 - report as duress, 238
 - report as panic, 238

- report code, 240
- reporting, 235
- resistance, 173
- RTE, 269
- shunt, 51, 59, 174, 239
- type, 49, 229
- uninhibit, 231
- warning time, 246
- zone acknowledgement, 235, 236
- zone delay, 235
- zone EOL, 31
- zone expansion, 33
- zone options, 230
- zone pairing, 232
- zone shunt, 262
- zone type, 49, 229