
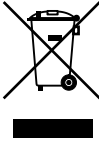




Advisor Advanced ATSx500A(-IP) Installation and Programming Manual

Copyright	© 16SEP16 UTC Fire & Security Americas Corporation, Inc. All rights reserved.
Trademarks and patents	<p>Interlogix, Advisor Advanced AT5x500A(-IP) name and logo are trademarks of UTC Fire & Security.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	<p>UTC Fire & Security Americas Corporation, Inc. 3211 Progress Drive, Lincolnnton, NC, 28092, USA</p> <p>Authorized EU manufacturing representative: UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands</p>
Version	<p>This document applies to the following Advisor Advanced firmware versions:</p> <p>AT5x500A(-IP): MR_3.0</p>
Certification	<p></p> <p>EN 50131-1 System requirements EN 50131-3 Control and indicating equipment EN 50131-6 Power Supplies EN 50136-1-1 Alarm systems -Alarm Transmission systems</p> <p>AT51500A(-IP): Security Grade 2, Environmental class II AT53500A(-IP): Security Grade 3, Environmental class II AT54500A-IP: Security Grade 3, Environmental class II</p> <p>Note: AT51500A(-IP) is upgradable to Security Grade 3 using the AT5-MM-TK (MM enclosure) or the AT5-SM-TK (SM enclosure) tamper kit.</p> <p>Tested and certified by VdS Schadenverhütung GmbH</p> <p>Important: To comply with the above standards, it is required to configure the system according to settings listed in Chapter 8 “Regulations” on page 301 onwards.</p> <p>This product has not been designed to comply with EN 50134 and EN 54 norms.</p>
European Union directives	<p>UTC Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of one or more of the Directives 2014/30/EU and 2014/35/EU. For more information see www.utcfireandsecurity.com or www.interlogix.com.</p>
	<p>2002/96/EC (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: www.utcfsecurityproducts.eu/recycle/</p>
Contact information	www.utcfireandsecurity.com or www.interlogix.com
Customer support	www.utcfsecurityproducts.eu

Content

	Important information	iii
Chapter 1	Quick installation and programming	1
	Quick installation	2
	Quick programming	4
Chapter 2	Installation	7
	General installation information	8
	Maintenance	16
	Mounting	18
	Earthing	20
	Shielding	21
	Cabling	22
	Configuration	30
	Specifications	35
Chapter 3	System functions	41
	Function list	43
	Zones	45
	Areas	50
	Set and unset	51
	Inhibit and isolate	53
	Keys	54
	Bus devices	58
	Users	60
	User groups	62
	PIN	66
	Outputs	67
	Access control	68
	Condition filters	74
	Triggers	76
	Calendar	77
	Events	79
	Tests and diagnostics	80
	Alarm reporting	84
	User programmable functions	88
	Autoset	91
	Wireless device programming	92
	Using cameras	98
	Engineer reset	102
	Timed unset / ATM	103
Chapter 4	Programming	105
	The Advisor Advanced menu	106

	How to program the options	108
	Remote access	113
	Initial start-up	114
Chapter 5	Menu reference	117
	1 Service menu	120
	2 Device menu	142
	3 User menu	162
	4 Zones and areas	171
	5 Door menu	196
	6 Outputs and filters	217
	7 Calendar	225
	8 System option menu	232
	9 Dialler menu	258
Chapter 6	Software	287
	Programming Advisor Advanced via configuration software	288
	Upgrading Advisor Advanced firmware	290
Chapter 7	Troubleshooting	295
	Recovery procedure	296
	Device troubleshooting	297
Chapter 8	Regulations	301
	Options affected by EN 50131 regulations	302
	Options affected by other regulations	308
Appendix A	Advisor Advanced events	311
Appendix B	Advisor Advanced reporting codes	327
	Glossary	337
	Index	343
	Programming map	351

Important information

This document includes an overview of the product and detailed instructions explaining how to install your Advisor Advanced 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 Advisor Advanced and Advisor Advanced-IP control panels in all variations. “Advisor Advanced control panel” refers to any variant of the Advisor Advanced control panels, unless specifically stated otherwise.

List of panel variants

Table 1: List of ATsx500A(-IP) panel variants

Model	Enclosure	Dimensions (mm)	Weight (kg)
ATS1500A-MM	Metal	MM, 315 x 388 x 85	5.2
ATS1500A-IP-MM	Metal	MM, 315 x 388 x 85	5.2
ATS1500A-SM	Metal	SM, 250 x 250 x 86	2.8
ATS1500A-IP-SM	Metal	SM, 250 x 250 x 86	2.8
ATS1500A-LP	Plastic	LP, 257 x 400 x 112	2.6
ATS1500A-IP-LP	Plastic	LP, 257 x 400 x 112	2.6
ATS3500A-MM	Metal	MM, 315 x 388 x 85	5.2
ATS3500A-IP-MM	Metal	MM, 315 x 388 x 85	5.2
ATS3500A-LP	Plastic	LP, 257 x 400 x 112	2.6
ATS3500A-IP-LP	Plastic	LP, 257 x 400 x 112	2.6
ATS4500A-IP-MM	Metal	MM+, 315 x 445 x 88	5.4
ATS4500A-IP-LM	Metal	LM, 475 x 460 x 160	10.9

Notes

- Not all variants may be available.
- Weight does not include batteries.

Limitation of liability

To the maximum extent permitted by applicable law, in no event will UTCFS 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 UTCFS 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 UTCFS 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, UTCFS assumes no responsibility for errors or omissions.

Advisory messages

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

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

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

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



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

Chapter 1

Quick installation and programming

Summary

The chapter contains basic steps of connection and programming of the Advisor Advanced control panel and auxiliary devices.

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

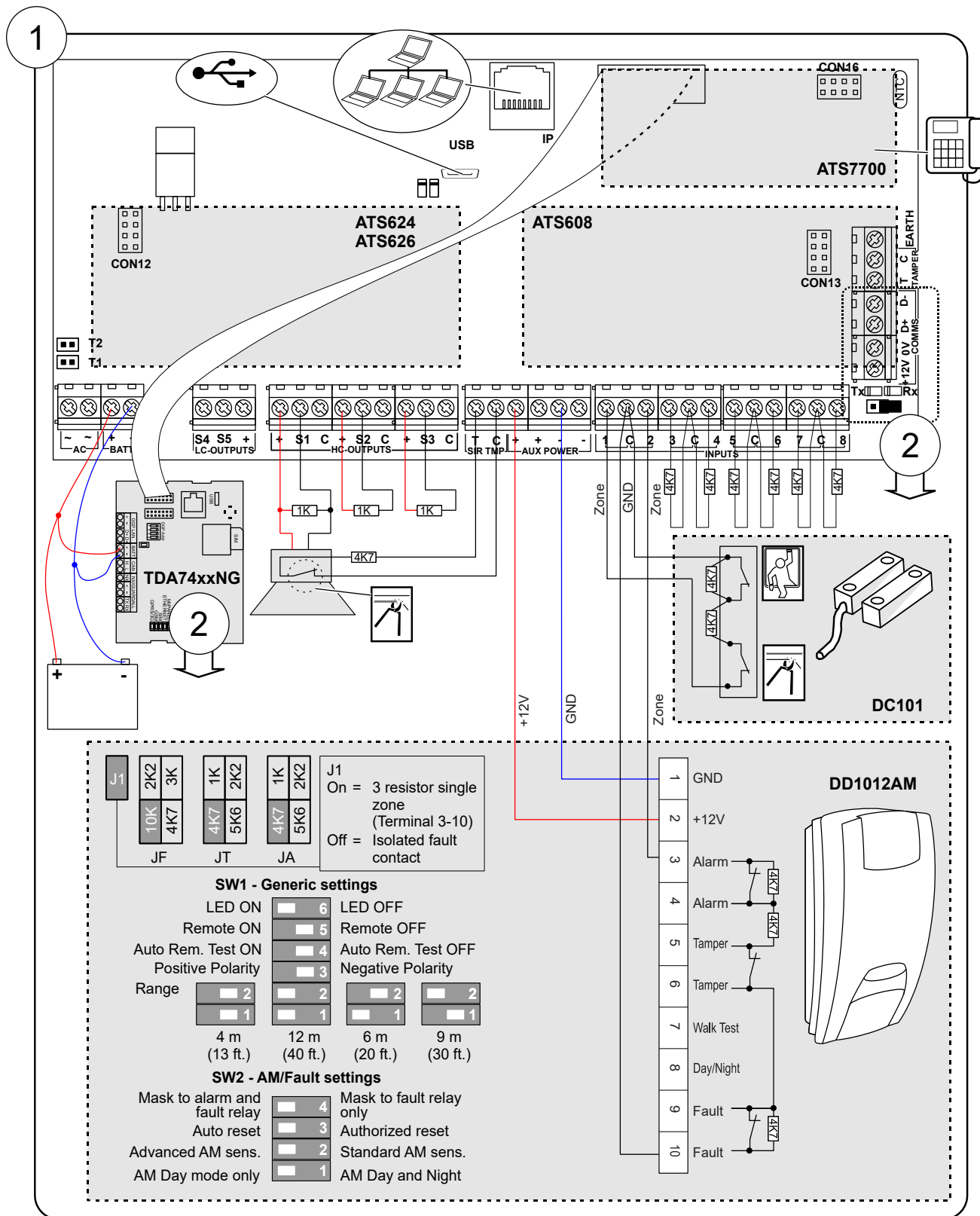
For details on programming, see Chapter 4 “Programming” on page 105 and Chapter 5 “Menu reference” on page 117.

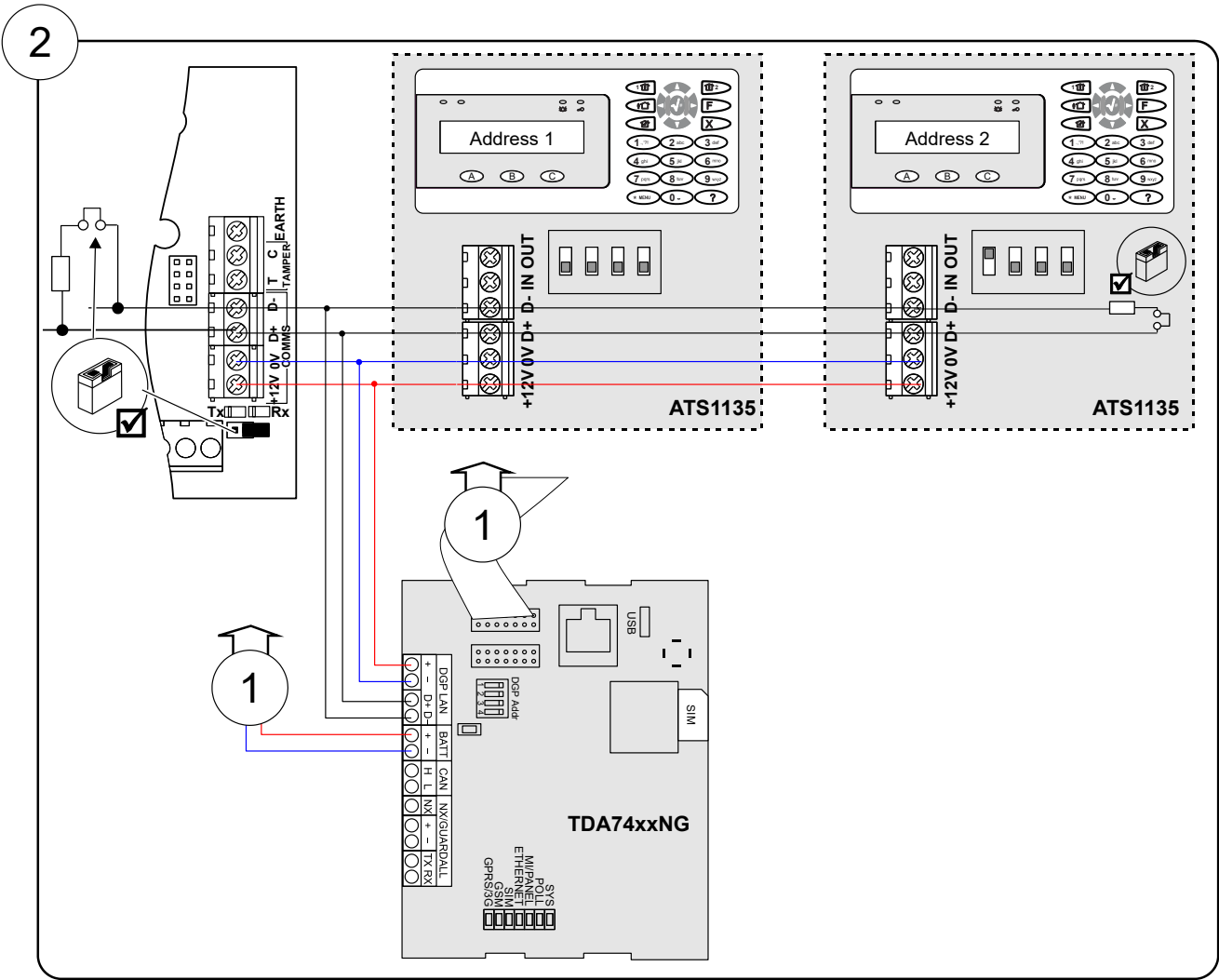
Content

Quick installation 2

Quick programming 4

Quick installation





Quick programming

Initial start-up

Note: See “The Advisor Advanced menu” on page 106 for menu explanation. For more information on editing options, see “How to program the options” on page 108.

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 English.
2>Defaults	Choose EN 50131 Grade 3.
4>PIN length	Enter 6.
5>Time&date	Set current time and date.
6 Install >Cancel<	Choose OK
Installer PIN:127800	Press Enter to continue.
Supervisor PIN:112200	Press Enter to continue.

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

UTC F&S THU 05 Mar 12:21	Press 112200, 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

UTC F&S THU 05 Mar 12:21	Press 127800, Menu
-----------------------------	--------------------

Inh reports >No<	Press Enter to continue.
---------------------	--------------------------

Inh tampers Unset areas	
----------------------------	--

1>Service menu 2 Device menu	
---------------------------------	--

The installer menu is displayed.

Changing installer PIN

Go to 3.1.n.2.1 Change PIN (see page 163).

1>Change PIN *****	Press Enter.
-----------------------	--------------

New PIN >_	Enter the new installer PIN.
---------------	------------------------------

Configuring zones

Go to 4.1 Zone menu (see page 171).

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 4.1.n.1 Zone name (page 172).

01 Zone name >1 Zone 1 <	
-----------------------------	--

Next, set its zone type in 4.1.n.2 Zone type (see page 172).

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

Adding users

Go to menu 3.1 Users (see page 162).

```
0>Add user          Press Enter to add a user.
1 Installer
```

```
INFO
User added
```

```
01>User name       Press Enter.
                User 3
```

```
01 User name      Enter a new user name.
>User 3          <
```

Configure other options of the user:

- 3.1.n.2 PIN (page 162)
- 3.1.n.3 User card (page 163)
- 3.1.n.6 User groups (page 164), etc.

Repeat for other users.

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

```
Lock user data?   Choose OK and confirm.
>Cancel<
```

Configuring areas

Go to 4.2 Areas (see page 185).

Change the area name in 4.2.n.1 Area name (see page 185).

```
1 Area name       Enter a new area name
>Area 1          <
```

Configure other options of the area:

- 4.2.n.2 Exit time (see page 186)
- 4.2.n.3 Entry time (see page 186), etc.

Caution: Before enabling 4.2.n.5.4 Dual unset (see page 189), make sure to add users that can assist the unset. See “Adding users” above.

Configuring Central Station

Configure the communication path in 9.3 Path options (page 267).

```
1>PSTN
3 GSM/SMS/GPRS
```

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

Next, go to menu 9.1 Central station (page 258).

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

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

- 9.1.n.1 CS name (page 258)
- 9.1.n.2 Transm path (page 259)
- 9.1.n.3 Protocol (page 259)
- 9.1.n.5 Accounts (page 259)
- Other options, depending on the communication path used.

Test the communication using menu 1.2.6.n.6 Man. test call (page 131), 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 301 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 Advisor Advanced system.

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

Content

General installation information	8
Advisor Advanced housings	8
Advisor Advanced layout	12
Keypads and readers	13
Maintenance	16
Mains power connection	16
Battery replacement	16
Mounting	18
General installation guidelines	18
Earthing	20
Shielding	21
Cabling	22
System databus preferred wiring	22
System databus connection	22
Zone connection	23
Values for end-of-line resistors	24
EOL connection types	27
Siren connection	28
Other connections	28
Configuration	30
Defaulting the panel	30
Zone configuration	30
Outputs	30
Zone and output addressing	31
Specifications	35
Auxiliary current and battery capacity	39

General installation information

Advisor Advanced housings

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: Small metal housing (-SM)

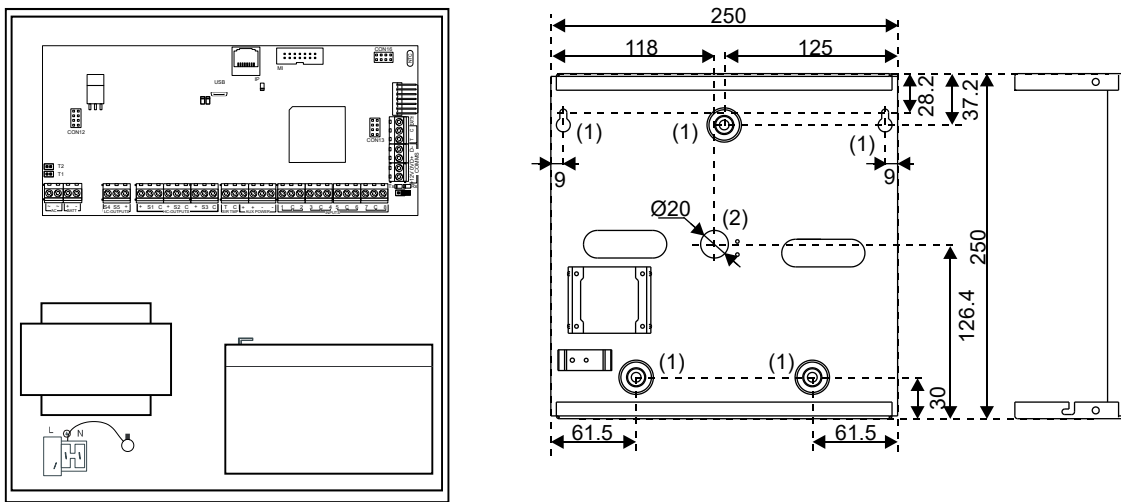


Figure 2: Medium metal housing (-MM)

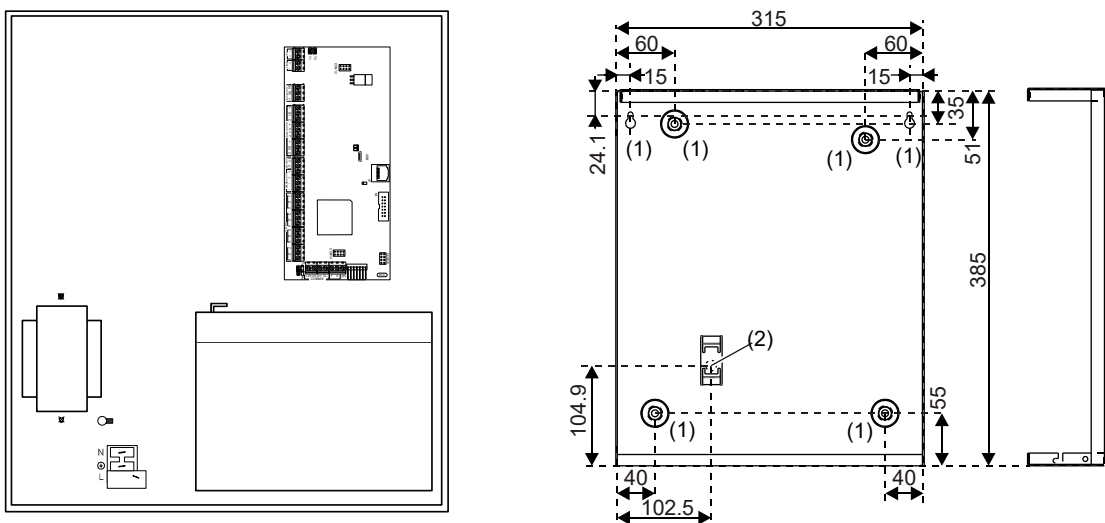


Figure 3: Large polycarbonate housing (-LP)

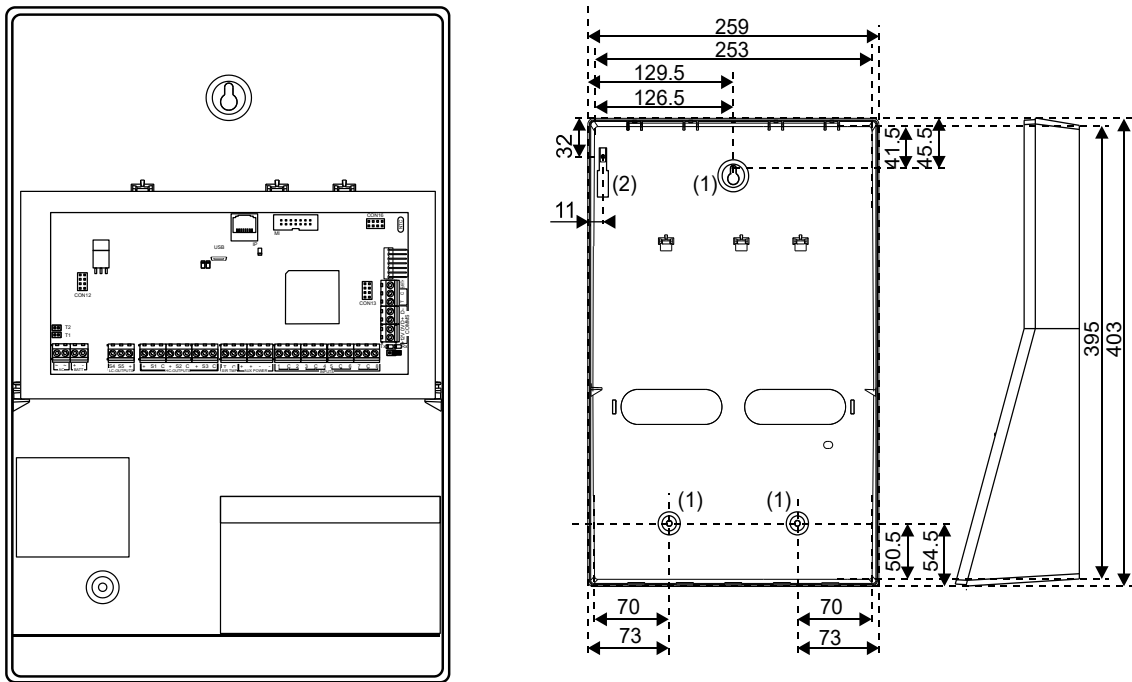


Figure 4: Medium metal housing (-MM+)

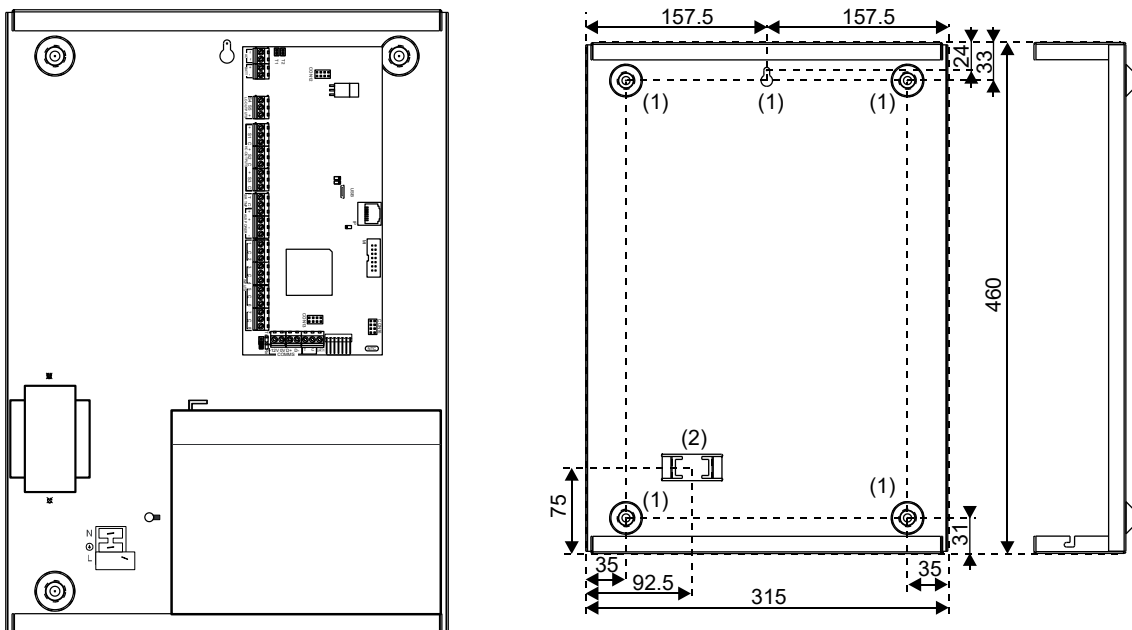
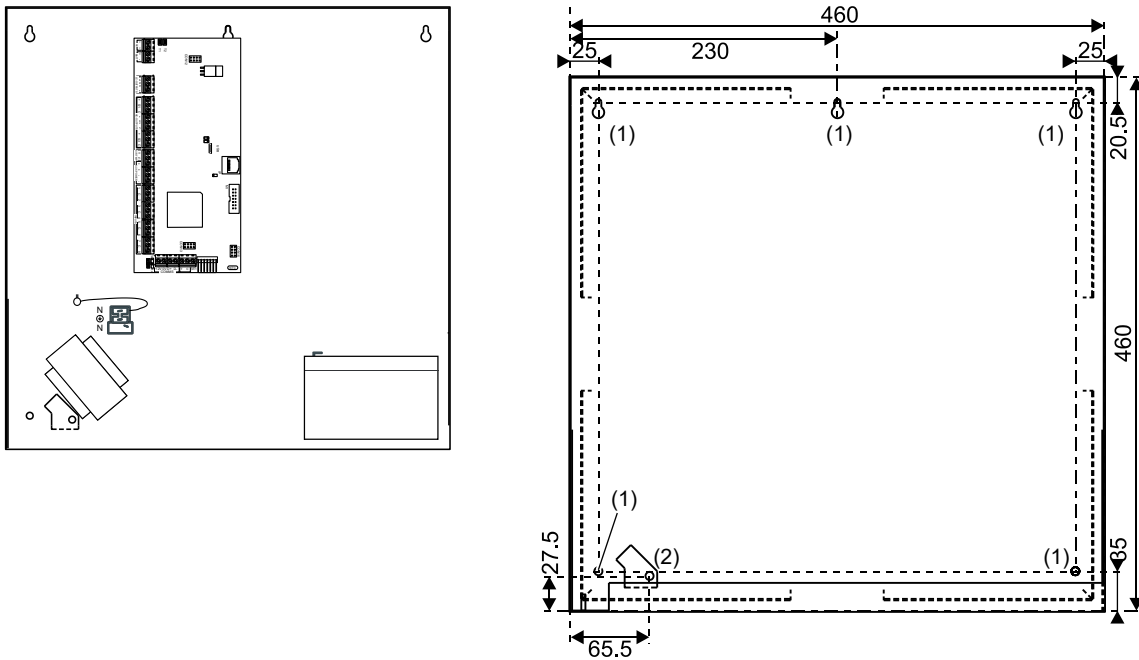


Figure 5: Large metal housing (-LM)



For more details on connections and connecting devices to the Advisor Advanced, see “Cabling” on page 22.

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

Pry-off tamper mounting

For small housing (SM), follow the steps in Figure 6 on page 11 to install pry-off tamper. For medium (MM and MM+), and large housings (LM), follow the steps in Figure 7 on page 11. For large plastic housing (LP), follow the steps in Figure 8 on page 12.

Figure 6: Small housing (SM) pry-off tamper mount

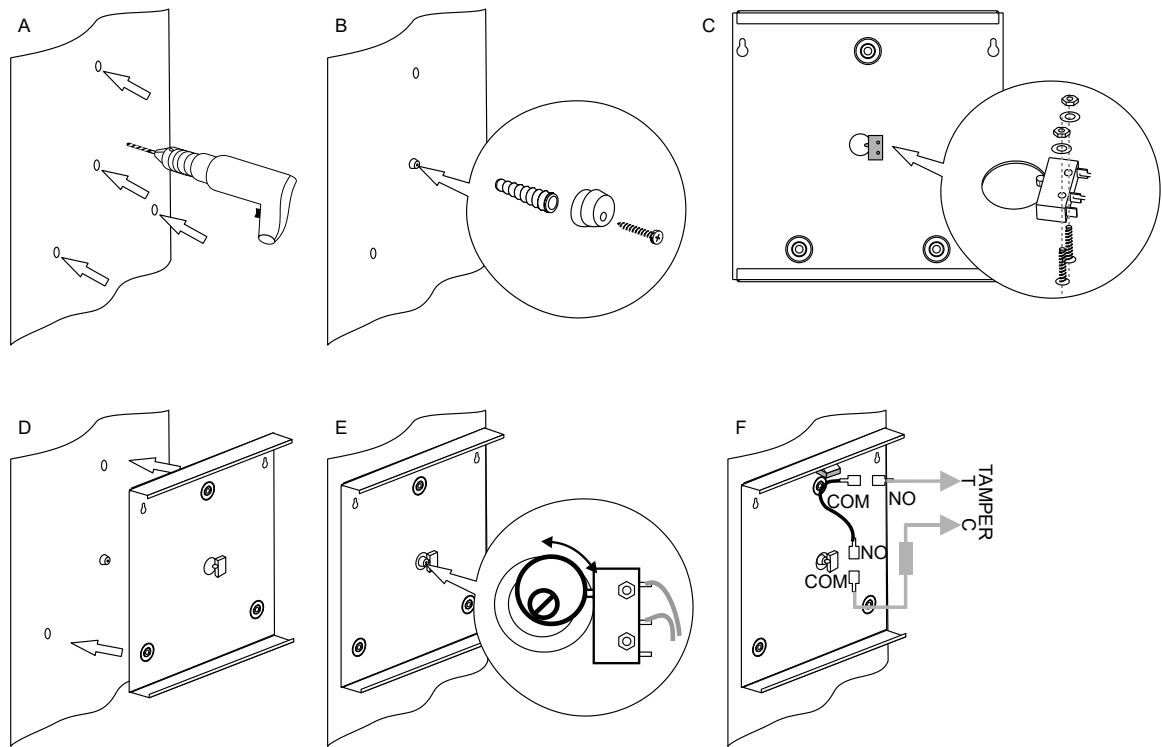


Figure 7: Medium (MM and MM+) and large housing (LM) pry-off tamper mount

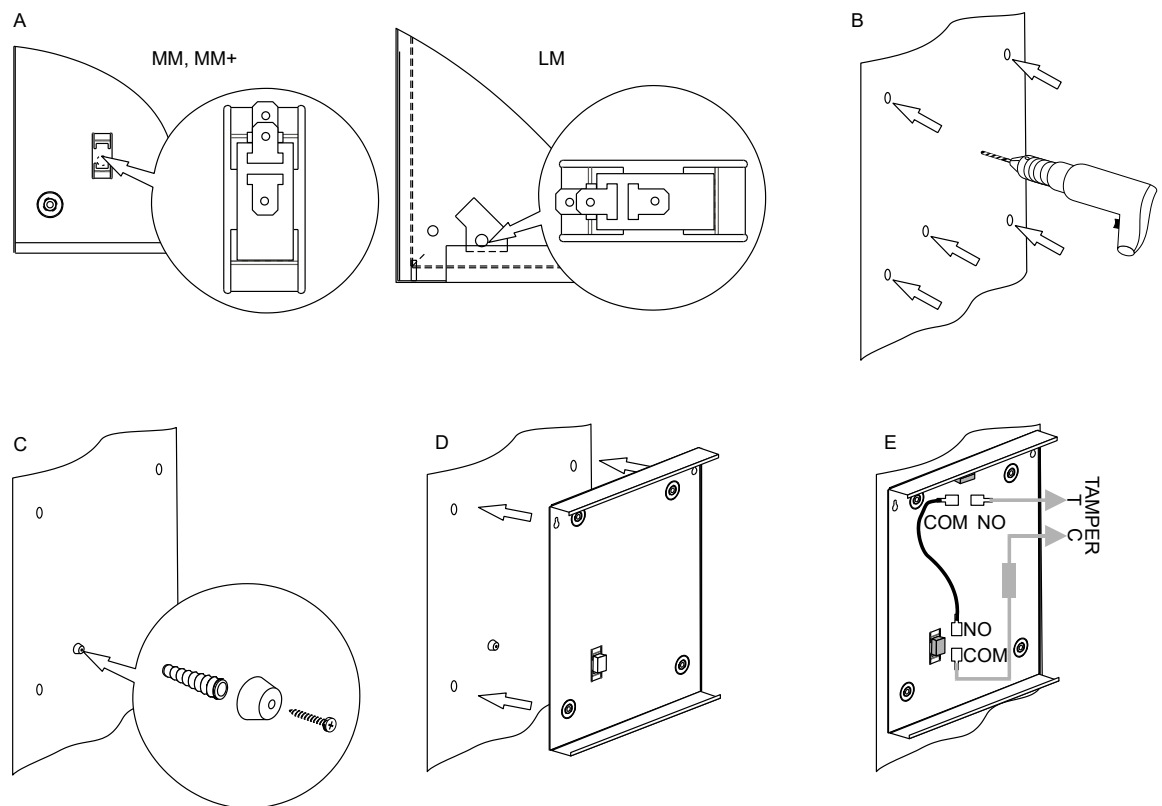
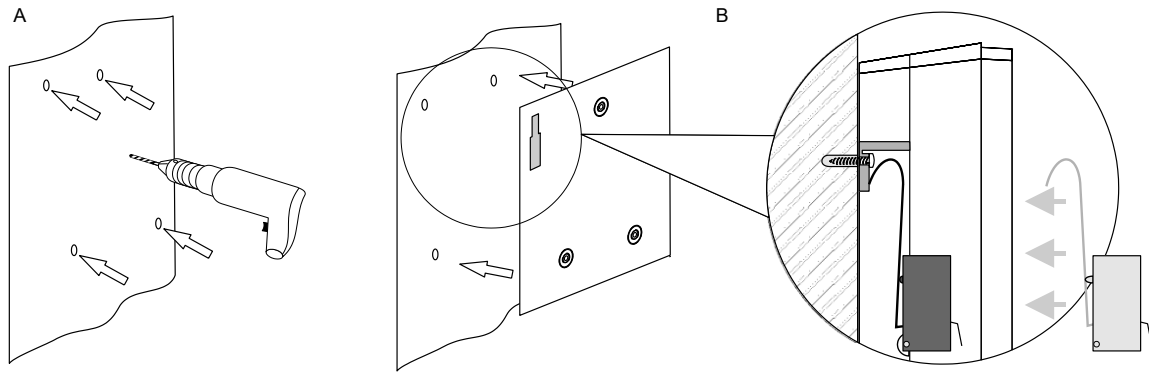
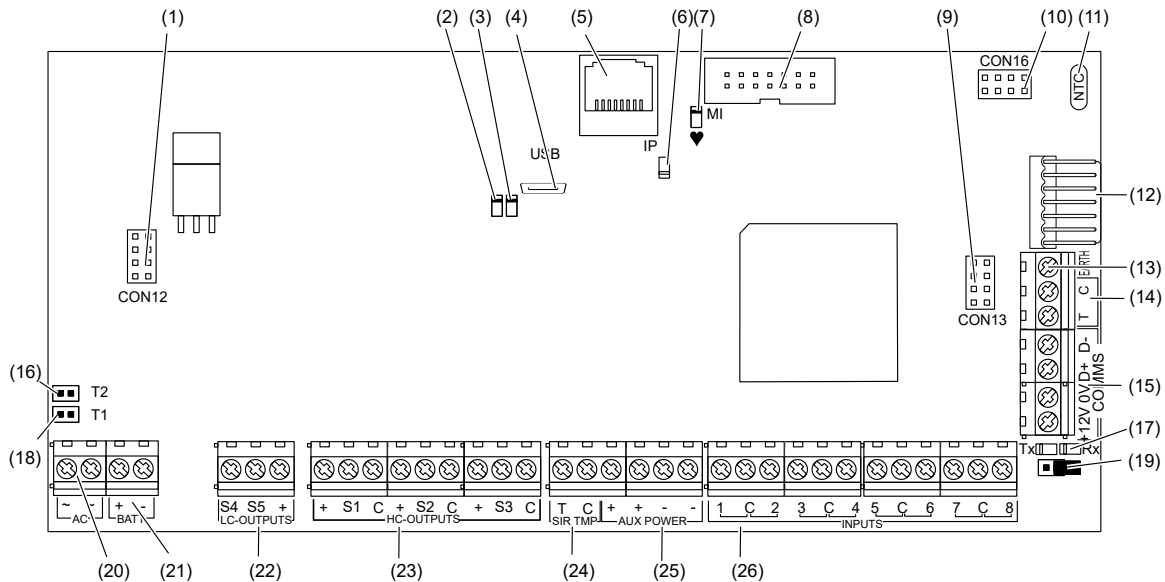


Figure 8: Large plastic housing (LP) pry-off tamper mount



Advisor Advanced layout

Figure 9: Advisor Advanced ATsx500A(-IP) PCB layout



- | | |
|---|---|
| (1) Interface to output expander | (15) RS-485 system databus connections |
| (2) USB fault LED | (16) T2: Device firmware upgrade mode (DFU) |
| (3) USB power LED | (17) RS-485 system databus communication LEDs |
| (4) USB connector (micro-A/B type) | (18) T1: Restores installer default PIN |
| (5) Ethernet RJ-45 connector (ATS-IP only) | (19) System databus termination jumper |
| (6) IP communication LED (ATS-IP only) | (20) AC power supply terminal |
| (7) Heartbeat LED | (21) Battery connection |
| (8) MI-bus connector for MI devices | (22) Low current (OC) outputs |
| (9) Interface to input expander | (23) High current outputs |
| (10) Interface to PSTN module | (24) Siren tamper switch |
| (11) Optional: enclosure ambient temperature sensor | (25) 12 VDC auxiliary power output |
| (12) ATsx670 databus expander connector | (26) Zone inputs |
| (13) Panel earth terminal | |
| (14) External tamper switch | |

Keypads and readers

Figure 10: AT5111xA keypad

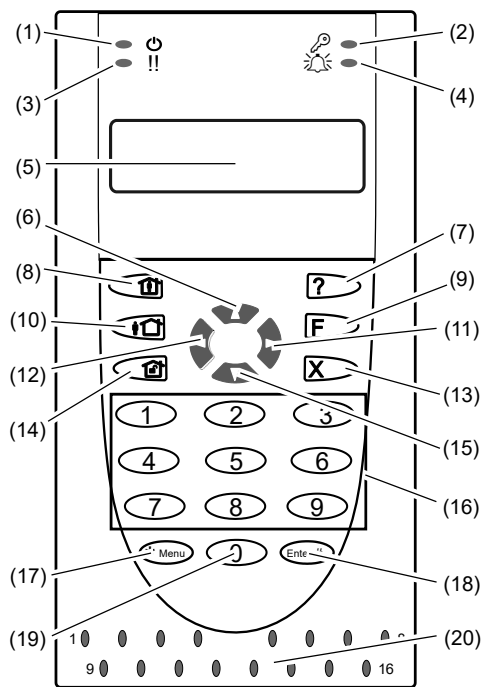
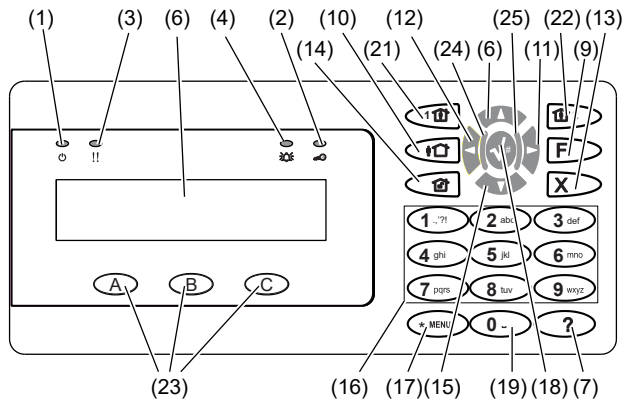


Figure 11: AT51135 keypad



(1)	AC mains LED	Green on: AC mains supply on
(2)	Access LED	Blue flashes: card read
(3)	Fault LED	Yellow on: system fault active Yellow flashing: general alert (EN 50131)
(4)	Alarm LED	Red on: alarm condition active
(5)	LCD display	Displays messages
(6)	▲ / Up	Scroll up in the menus Change value Delete
(7)	? / Help	Show help Scroll text (ATS113x only)
(8)	Partset	Part set an area Scroll text (ATS111x only)
(9)	F / Function	Show active zones / faults Function key modifier Scroll text (ATS113x only)
(10)	On	Full set an area
(11)	► / Right	Enter the selected menu Move cursor right
(12)	◀ / Left	Return to the previous menu Move cursor left
(13)	X / Clear	Exit the current user function Volume control modifier
(14)	Off	Unset an area

(15)	▼ / Down	Scroll down in the menus Change value Backspace
(16)	Alphanumeric keys	Keys 1 to 9, alphanumerical data. See “Keypad layout” on page 112.
(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 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

Figure 12: ATS1190/ATS1192 readers

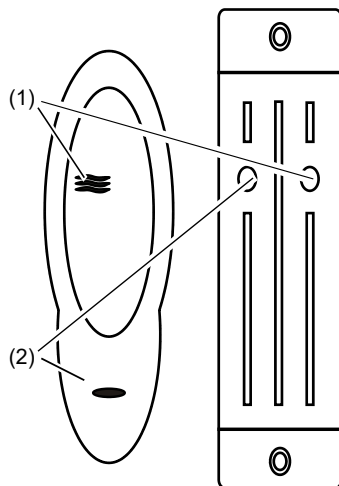


Figure 13: ATS1197 reader with keypad

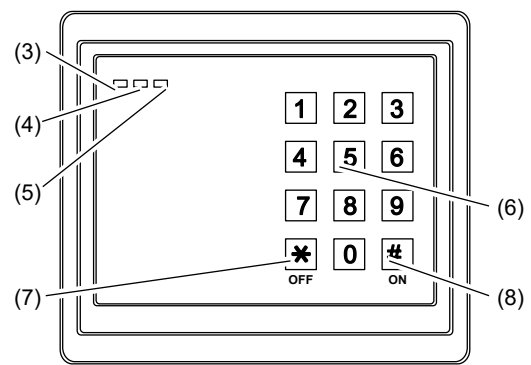
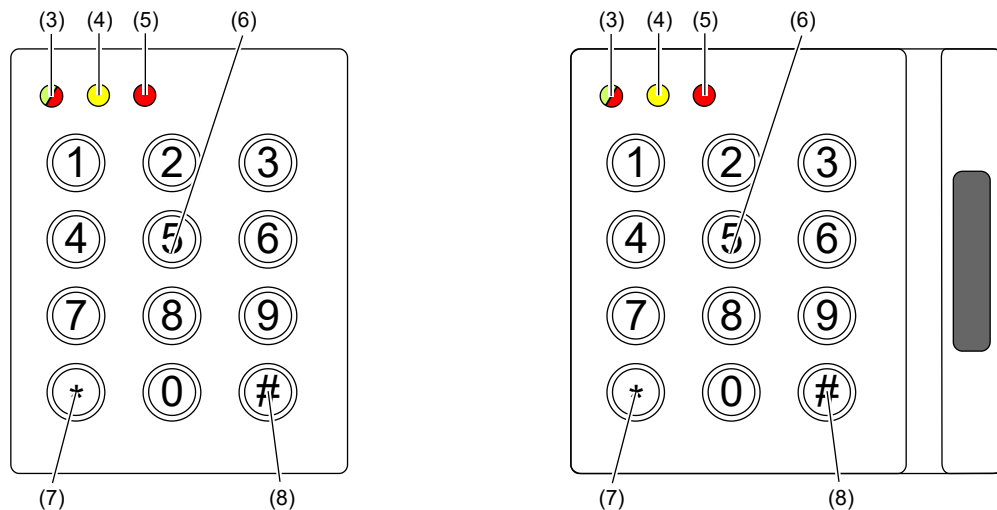


Figure 14: ATS1151/ATS1156 readers



(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 Green flashing: AC mains supply off, or unlocked while unset Red on: all areas set Red flashing: unlocked while set
(4)	Yellow LED	On: All zones are in normal state Flashing: general alert (EN 50131)
(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



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.

For metal housing, the screw is already installed out of the box. For plastic housing, the screw, available inside housing, should be mounted before first time use.



Mains power connection

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 circuit breaker in the power distribution network. In all cases the mains connection must comply with local regulations.

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. 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 replacement

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

To remove a battery:

1. Make sure that your product settings allow you to open the cover without starting the tamper alarm.
2. Switch off the mains power, if necessary, and remove the cover.

3. Disconnect the battery. Note that depending on the battery model the connectors may be located differently.
4. Remove the battery from the holder.

In case a battery BS131 (12 V / 18 Ah) in an ATS1640 housing is used in combination with ATS7700 PSTN expander board, it is required to have double insulation in place. Use adequately insulated wires for PSTN cabling, and make use of heat shrink.

Dispose of the battery as required by local ordinances or regulations.

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

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.

General installation guidelines

The Advisor Advanced 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 Advisor Advanced 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 bipolar 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 (e.g. a 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 relay output expansion (for example, ATS624 four-relay expander).
- The minimum clearance between equipment closures is 50 mm (between equipment vents).
- Only use these units in a clean environment and not in humid air. Environmental requirements are given in “Specifications” on page 35.
- 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.

If a device is placed in a plastic housing the earth lug of the device does not have to be connected.

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

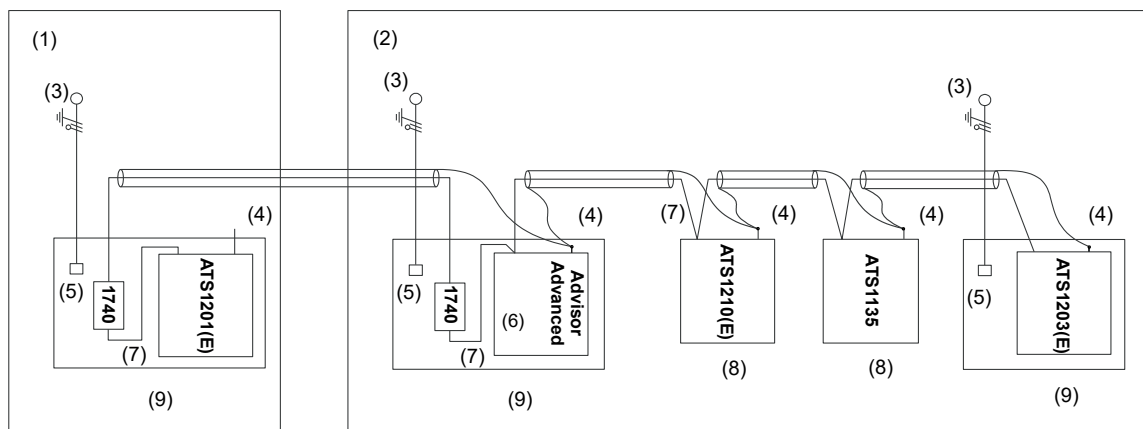
If the wiring extends to separate buildings, more than one common earth system will be used. Use ATS1740 isolator/repeaters to isolate the system databus. In this way the system is protected against variations in earth potential.

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 15 below). If a shielded databus 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 15: System shielding



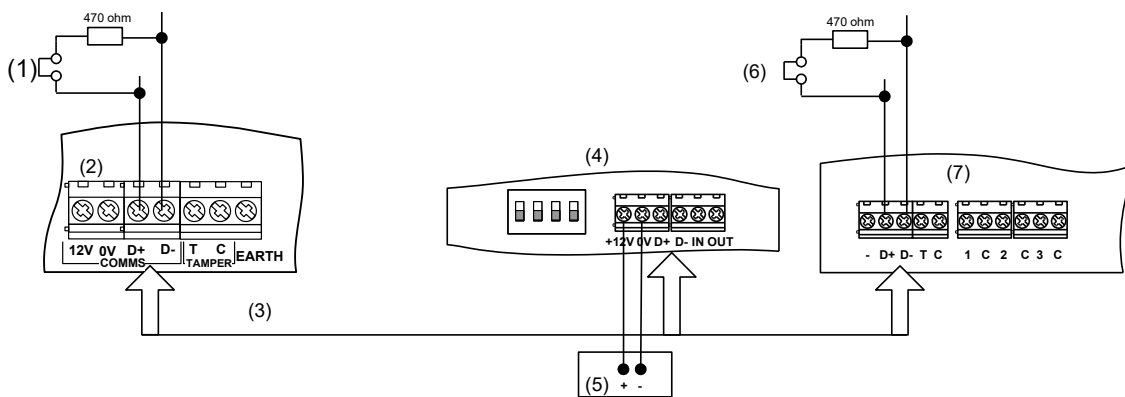
- | | |
|----------------------------------|------------------------------------|
| (1) Building 1 | (6) Advisor Advanced control panel |
| (2) Building 2 | (7) System databus |
| (3) Mains power with local earth | (8) Device in plastic housing |
| (4) Earth and shielding | (9) Device in metal housing |
| (5) Mains power connector | |

Cabling

System databus preferred wiring

The terminator jumper (also called TERM link), or DIP switch must be ON, or a 470 Ω resistor must be fitted at each of the devices at the extreme ends of the daisy chained databus. In a star-wiring configuration, the TERM link is only fitted on the devices at the ends of the two longest system databus cable runs.

Figure 16: System databus wiring



- (1) TERM link fitted (first device on local databus).
- (2) Advisor Advanced control panel variants.
- (3) Preferred data cable type is WCAT 52 (two twisted pairs).
- (4) Advisor LCD keypad (TERM switch is set to OFF).
- (5) 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 databus).
- (6) TERM link fitted (last device on local databus).
- (7) Any remote expander like ATS1201(E) or ATS1210(E).

System databus connection

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

Keypads and remote expanders must be connected via a shielded data cable with two twisted-pairs from the system databus 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.

If the keypad is powered with a separate power supply, do not connect "+" from the system databus. Connect "+" of the local power supply to "+" on the keypad, and connect 0 volts from the power supply and 0 volts from the system databus

to the keypad terminal marked “-”. The maximum number of devices allowed on the databus is given in “General features” on page 36.

Two system databuses

Particular panel variants allow you to connect more bus devices by using a second system databus. To install another system databus, use ATS670 second RS485 LAN extension module.

System addresses of devices connected to the additional bus (BUS2) are determined by adding 16 to keypad physical addresses, and 15 to expander addresses. So, BUS1 handles keypads 1 to 16 and expanders 1 to 15, while BUS2 — keypads 17 to 32 and expanders 16 to 30.

Note: Door controllers can only be installed on BUS1.

Zone connection

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

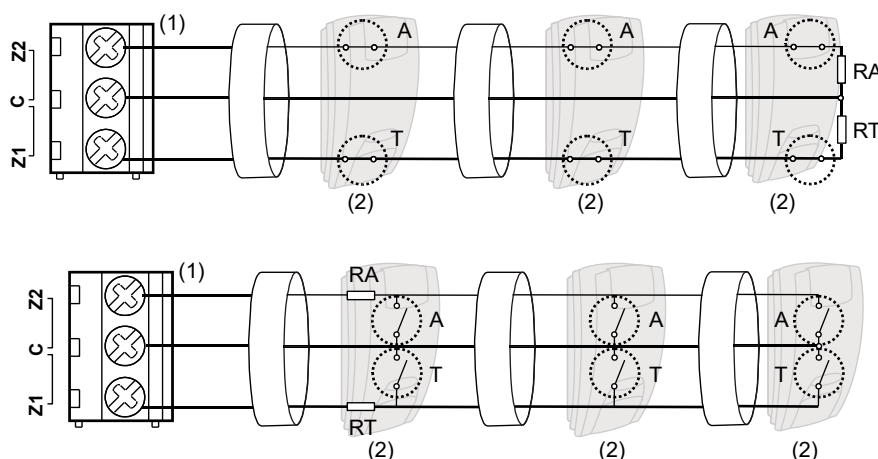
Depending on the detector model, do the following to set up zones:

- Choose your EOL connection type. See “EOL connection types” on page 27.
- Program input mode. See “8.6.1 Input mode” on page 248 for the panel, or “2.2.2.n.4.4 Input mode” on page 152 for expanders.
- Set end-of-line resistor values. See “8.6.2 EOL” on page 248 for the panel, or “2.2.2.n.4.5 EOL” on page 152 for expanders.
- Configure anti-masking option. See “4.1.n.6.7 Anti mask” on page 175.

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 17: Single loop examples



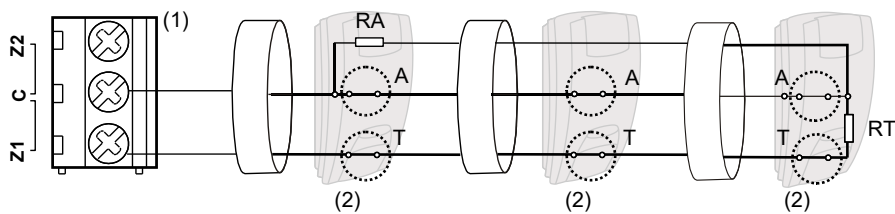
- | | |
|-------------------|----------------|
| (1) Zone terminal | (2) Detector |
| C Common terminal | A Alarm relay |
| Z1 Zone 1 input | T Tamper relay |
| Z2 Zone 2 input | |

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 18: Dual loop example



- | | |
|-------------------|----------------|
| (1) Zone terminal | (2) Detector |
| C Common terminal | A Alarm relay |
| Z1 Zone 1 input | T Tamper relay |
| Z2 Zone 2 input | |

Possible EOL connections are listed in “EOL connection types” on page 27.

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)	—	—	>44.70	<44.70	—	—
		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	—
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	—
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	—
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
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	—
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	—
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	—

EOL	Connection details [1]	Measure [2]	Zone state					
			Short	Masking	Normal	Alarm	Fault	Open
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	—
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	—
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	—
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	—
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	—
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
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	—
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

[1] Refer to Figure 19 on page 27.

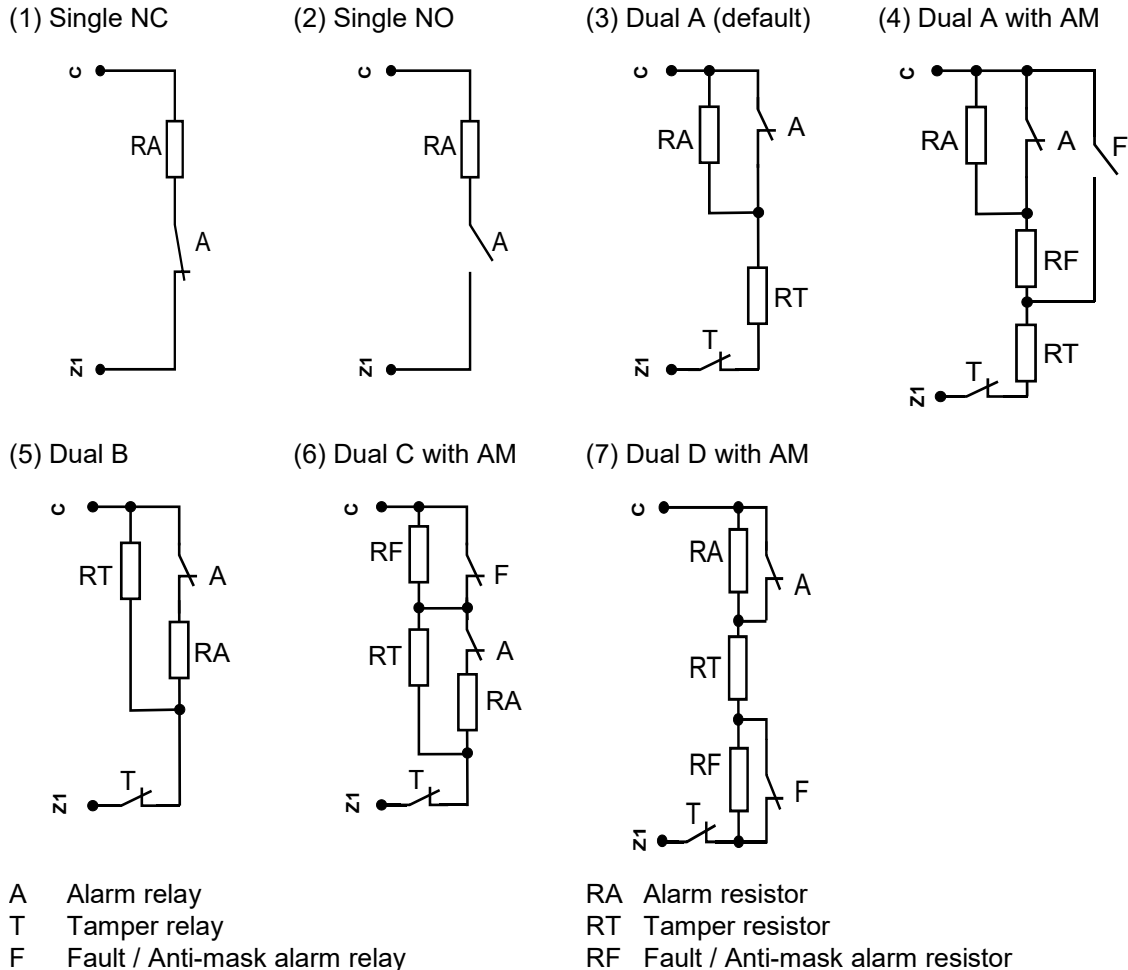
[2] Zone resistance R (kΩ), zone voltage U (V).

— 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 24 for more details.

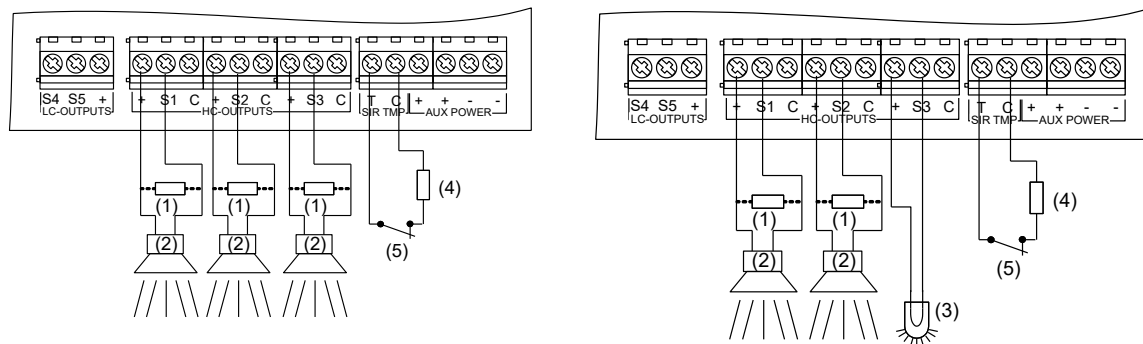
Figure 19: Connection type



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 “4.1.n.6.7 Anti mask” on page 175.

Siren connection

Figure 20: Siren connection examples



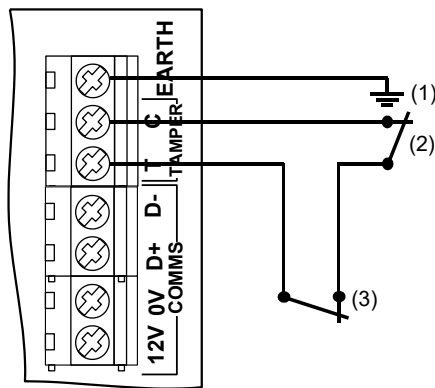
- (1) Siren EOL resistor (1 kΩ). It must be installed if siren does not contain a built-in resistor.
- (2) Siren.
- (3) Beacon.
- (4) Siren tamper EOL resistor.
- (5) Siren tamper (normally closed).

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 31 and “Outputs” on page 67.

Other connections

Tamper connection

Figure 21: Earthing and tamper connection in ATsx500A(-IP)



- (1) Earthing
- (2) External tamper (normally closed)
- (3) Optional pry-off tamper (normally closed) required by EN 50131 Grade 3 and VdS-C regulations

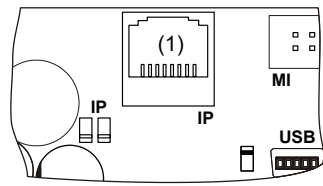
PSTN connection

To connect PSTN in ATsx500A(-IP) control panels, use ATs7700 PSTN module. See *ATs7700 PSTN Module Installation Sheet* for details.

Caution: If the PSTN line is provided via the ADSL network, make sure that at least ADSL splitter/filter is used, otherwise the PSTN communication quality may be too low for a reliable reporting.

Ethernet connection

Figure 22: Ethernet connection



(1) Ethernet RJ45

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 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 114.

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

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 36.

External expansion

Expanders can be used to expand the Advisor Advanced control panels with external zones. The maximum zone number for each control panel is listed in “Specifications > General features” on page 36.

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 36.

Outputs

There are 5 outputs on the panel PCB. Output expander can be used to add another 16 outputs inside the panel.

Output controllers are used to expand the number of outputs on an expander. An expander output controller expands the outputs by 8. An expander can have two output controllers connected, increasing the outputs to a maximum of 16 per 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 36.

Notes

- Low current output S4 is active when the system is ready to set. Low current output S5 is active when the system is armed.
- Set keypad output 7 to activate continuous keypad buzzer sound, or output 8 to activate intermittent sound.

Siren outputs

The siren outputs on the Advisor Advanced control panel have addresses starting from 1 (see Table 2 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 67 for more details.

Default output assignments

The default output assignments are shown in Table 2 below.

Table 2: 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 S1 VdS: External siren output S2
Panel 3	S3	High current output	EN 50131 Grade 3: Programmable siren output VdS: External strobe output S3
Panel 4	S4	Low current output	A1 ready to set
Panel 5	S5	Low current output	A1 set
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 3 on page 32 shows the zone and output addressing in the Advisor Advanced 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 “8.7.9 Object scheme” on page 253.

Table 3: Zone and output numbering

Device	Zones	Outputs	Device	Zones	Outputs
Panel	1–8	1–8	2X ATS1810 relay cards	—	17–24 [1]
Input expander (ATS608)	9–16	N/A	Output expander (ATS62x)	—	9–16 [2]
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 [3]	465–496	Keypad 15	—	1113–1120
Expander 16 [4]	497–528	497–528	Keypad 16	—	1121–1128
Expander 17	529–560	529–560	Keypad 17 [4]	—	1129–1136
Expander 18	561–592	561–592	Keypad 18	—	1137–1144
Expander 19	593–624	593–624	Keypad 19	—	1145–1152
Expander 20	625–656	625–656	Keypad 20	—	1153–1160
Expander 21	657–688	657–688	Keypad 21	—	1161–1168
Expander 22	689–720	689–720	Keypad 22	—	1169–1176
Expander 23	721–752	721–752	Keypad 23	—	1177–1184
Expander 24	753–784	753–784	Keypad 24	—	1185–1192
Expander 25	785–816	785–816	Keypad 25	—	1193–1200
Expander 26	817–848	817–848	Keypad 26	—	1201–1208
Expander 27	849–880	849–880	Keypad 27	—	1209–1216
Expander 28	881–912	881–912	Keypad 28	—	1217–1224
Expander 29	913–944	913–944	Keypad 29	—	1225–1232
Expander 30	945–976	945–976	Keypad 30	—	1233–1240
			Keypad 31	—	1241–1248
			Keypad 32	—	1249–1256

[1] Output 17 to 24 states are duplicated on ATS1810 relays and Expander 1 outputs.

- [2] When using ATS624 relay card with the ATS1810 expander attached, expander output 8 state is inverted.
- [3] Inputs 17 to 32 of Expander 15 cannot be used.
- [4] You cannot connect more than 15 expanders and 16 keypads to one system databus. To connect more bus devices to a panel, it is necessary to install ATS670 second RS485 LAN extension module. See also “Two system databuses” on page 23.

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 Advisor Advanced control panel system databuses are used for simple access control functions.

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

See “Doors” on page 68 for more details.

Table 4 below shows the door, zone and output numbering for door controllers.

Table 4: 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 5 below shows the default zone and output assignment for door controllers.

Table 5: 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
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 6 below shows the default assignment of door controller local databus readers to specific doors.

Table 6: 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 ±10%
Current consumption at 230 VAC:	
ATS1500A(-IP)	300 mA max.
ATS3500A(-IP), ATS4500A-IP	500 mA max.
Transformer output:	
ATS1500A(-IP)-SM/LP	20 VAC, 31 VA
ATSx500A(-IP)-MM/MM+/LM	23 VAC, 58 VA
ATS3500A(-IP)-LP	22 VAC, 53 VA

Power supply specifications

Power supply type	Type A per EN 50131-6 Type I per VdS 2115
Power supply voltage [1]	13.8 V $\overline{=}$ ±0.2 V
Power supply current:	
ATS1500A(-IP)	1.10 A max. at 13.8 V $\overline{=}$ ±0.2 V
ATS3500A(-IP)	2.10 A max. at 13.8 V $\overline{=}$ ±0.2 V
ATS4500A-IP	2.65 A max. at 13.8 V $\overline{=}$ ±0.2 V
Main board consumption:	
ATSx500A	100 mA at 13.8 V $\overline{=}$ ±0.2 V
ATSx500A-IP	150 mA at 13.8 V $\overline{=}$ ±0.2 V
Maximum system current available [2]:	
ATS1500A	1000 mA at 13.8 V $\overline{=}$ ±0.2 V
ATS1500A-IP	950 mA at 13.8 V $\overline{=}$ ±0.2 V
ATS3500A	2000 mA at 13.8 V $\overline{=}$ ±0.2 V
ATS3500A-IP	1950 mA at 13.8 V $\overline{=}$ ±0.2 V
ATS4500A-IP	2500 mA at 13.8 V $\overline{=}$ ±0.2 V
Auxiliary power output (AUX. POWER) [3]	13.8 V $\overline{=}$ ±0.2 V, 1 A max.
Battery power output (BAT) [4]	13.8 V $\overline{=}$ ±0.2 V, 2.5 A max.
Battery type	Lead acid rechargeable: [5] 7.2 Ah, 12 V nom. (BS127N) 12 Ah, 12 V nom. (BS130N) 18 Ah, 12 V nom. (BS131N) 26 Ah, 12 V nom. (BS129N) 36 Ah, 12 V nom. (BS134N)

Maximum voltage at power supply, auxiliary power output and battery power output	14.5 V _{DC}
Battery low condition	From 9.5 to 10.5 V _{DC}
Battery test level [6]	11.2 V _{DC}
Minimum voltage (battery recharging) at power supply, auxiliary power output and battery power output [7][8]	9.45 V _{DC}
Maximum ripple voltage V, p-p [9]	100 mV typical, 300 mV max.
Overvoltage trigger value [10]	15.5 V _{DC} min.

[1] The power supply voltage is monitored according EN 50131 Grade 3 and VdS-C regulations.

[2] Current available for auxiliary power and battery charge outputs.

[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 39.

[4] Battery output provides battery shortcut protection (according to VdS requirements).

[5] The housings applicable for particular batteries are specified in “Auxiliary current and battery capacity” on page 39.

[6] If during a manual or a programmed battery test the battery voltage drops below this threshold, the battery test fails.

[7] 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.

[8] A specific fail message is generated when any output fails.

[9] Max ripple voltage only when empty battery is charging.

[10] 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.

General features	ATS1500A(-IP)	ATS3500A(-IP)	ATS4500A-IP
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, 3.3 kΩ, 3.74 kΩ, 4.7 kΩ (default), 5.6 kΩ, 6.8 kΩ, 8.2 kΩ, 10 kΩ		
Onboard zones	8 (expandable to 16 with 1X ATS608)		
Maximum zone number	32	128	512
Onboard outputs	5 (expandable to 9 with 1X ATS624, or to 21 with 1X ATS626). See “Standard onboard outputs” on page 37.		
Maximum output number	128		
Areas	4	8	64
Area groups	—	—	64
Maximum keypad / RAS number	8	16	32 [1]
Maximum expander / DGP number	7	15	30 [1]

[1] It is necessary to install ATS670 second RS485 LAN extension module to connect more than 16 RASes and 15 DGPs.

Maximum user number (for users with SMS and voice reporting functionality)	50	200	1000
User groups	16	64	128
Inhibit / isolate / shunt limit, max.	32	128	512
Schedules	24		
Time frames	4 per schedule		
Special days	8		
Actions per schedule	20		
Event log capacity Note: See also “Events” on page 79.	15500, which includes: - 1000 mandatory events - 1500 non-mandatory events - 10000 access events - 1000 installer events - 1000 dialler events - 1000 extended events		
Data retention (log, program settings)	20 years		
Access control features	ATS1500A(-IP)	ATS3500A(-IP)	ATS4500A-IP
Door controllers supported	7	12	12
Standard doors	4	8	16
Intelligent doors	28	48	48
Regions	256		
Door groups	128		
Maximum user number (with door controllers connected)	2000 17488 (with ATS1831 IUM installed) 64532 (with ATS1832 IUM installed)		

Note: SMS and voice 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 36.

Ethernet connection (IP only)

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 V \approx
S4, S5 [1]	Low current electronic output, rating: 50 mA at 13.8 V \approx

[1] Maximum cable length for low current output connection may not exceed 30 m. For longer distances, use relay output expansion (for example, ATS624 four-relay expander).

Environmental	
Operating temperature	0 to +40°C
Tested temperature according EN 50131	-10 to +55°C
Humidity	95% noncondensing
IP protection grade	IP31
Colour	Beige
Dimensions	See “List of panel variants” on page iii
EN 50131 grade and class	ATS1500A(-IP): Grade 2, Class II ATS3500A(-IP): Grade 3, Class II ATS4500A-IP: Grade 3, Class II Note: ATS1500A(-IP)-MM can be upgraded to an EN Grade 3 setup with the use of the ATS-MM-TK tamper kit. ATS1500A(-IP)-SM can be upgraded to an EN Grade 3 setup with the use of the ATS-SM-TK tamper kit.
Safety class	Class I
Enclosure type	Enclosure (meets UL94V-0)
Overvoltage category	Category II
Maximum altitude, or minimum air pressure	2000 m above mean sea level

Fuses

Battery	ATS1500A(-IP), ATS3500A(-IP): 2 A, resettable ATS4500A(-IP): 3 A, resettable
12 V aux	1 A, resettable
System databus	1 A, resettable
Siren 1, high current output S1	1 A, resettable
Siren 2, high current output S2	1 A, resettable
Siren 3, high current output S3	1 A, resettable
Mains, mains fuse:	
ATS1500A(-IP)	315 mA, fast 20x5
ATS3500A(-IP), ATS4500A-IP	630 mA, fast 20x5

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

WARNING: Before removing the mains fuse, mains power must be disconnected (see “Mains power connection” on page 16).

Auxiliary current and battery capacity

Table 7: ATS1500A(-IP) maximum available auxiliary current

Battery capacity, Ah			7.2	12	18
Applicable housing			SM, MM, LP	LP	MM
Security approval / Grade	Discharge time, h	Charge time, h	Auxiliary current, mA		
EN Grade 2	12	72	450	750	750
INCERT	24	24	150	350	400
EN Grade 3, VdS-B	30	24	90	250	350
NF&A2P Grade 2 (EN+RTC)	36	72	—	180	350
NF&A2P Grade 3 (EN+RTC), VdS-C	60	24	—	—	150

Table 8: ATS3500A(-IP) maximal available auxiliary current

Battery capacity, Ah			7.2	12	18
Applicable housing			MM, LP	LP	MM
Security approval / Grade	Discharge time, h	Charge time, h	Auxiliary current, mA		
EN Grade 2	12	72	450	850	1350
INCERT	24	24	150	350	600
EN Grade 3, VdS-B	30	24	90	250	450
NF&A2P Grade 2 (EN+RTC)	36	72	—	180	350
NF&A2P Grade 3 (EN+RTC), VdS-C	60	24	—	—	150

Table 9: ATS4500A-IP maximal available auxiliary current

Battery capacity, Ah			7.2	12	18	25	36
Applicable housing			MM+, LM	LM	MM+, LM	LM	LM
Security approval / Grade	Discharge time, h	Charge time, h	Auxiliary current, mA				
EN Grade 2	12	72	450	850	1350	1600	1600
INCERT	24	24	150	350	600	875	900
EN Grade 3, VdS-B	30	24	90	250	450	675	700
NF&A2P Grade 2 (EN+RTC)	36	72	—	180	350	540	850
NF&A2P Grade 3 (EN+RTC), VdS-C	60	24	—	—	150	260	450

Note: 18 Ah battery blocks some entry holes in the MM housing.

Example for ATS1500A(-IP) EN Grade 2

When using battery backup as specified for EN Grade 2 using a 12 Ah battery, the maximum available auxiliary current is 750 mA.

Example for ATS3500A(-IP) EN Grade 3

When using battery backup as specified for EN Grade 3 using an 18 Ah battery, the maximum available auxiliary current is 450 mA.

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

- Devices on the Advisor Advanced system databus
- Detectors on the auxiliary power output
- Communication devices via MI-bus (e.g. 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]
Battery	Battery low	Battery low voltage [1]
	Battery test fail	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.

Chapter 3

System functions

Summary

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

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

Content

Function list 43

Zones 45

 Zone types 45

Areas 50

Set and unset 51

 Delayed unset 52

Inhibit and isolate 53

 Inhibit 53

 Isolate 53

 Zone shunt 53

 Door shunt 69

Keys 54

 Common key sequences for LCD keypad 54

 Common key sequences for keypad without LCD 55

 Function keys 57

Bus devices 58

 Bus device numbering 58

 Adding keypad with a higher number 58

 Keypads 58

 Expanders 59

Users 60

 Predefined users 60

 User data lock 61

User groups 62

PIN 66

Outputs 67

Condition filters	74
Triggers	76
Calendar	77
Events	79
Log	79
Programming	79
Tests and diagnostics	80
Walk test	80
Other tests	83
Alarm reporting	84
Reporting principles	84
Reporting order	85
Failed to communicate (FTC)	86
User programmable functions	88
Autoset	91
Wireless device programming	92
Learning wireless sensors	92
Learning fobs	94
Two-zone RF sensors	96
Device activation	97
Using cameras	98
Configuration	98
Diagnostics	100
Troubleshooting	100
Engineer reset	102
Timed unset / ATM	103

Function list

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

Table 11: Function list

Function	Reference
Access control	“Access control” on page 68
Areas	“Areas” on page 50
ATM	“Timed unset / ATM” on page 103
Autoset	“Autoset” on page 91
Calendar	“Calendar” on page 77
Cameras	“Using cameras” on page 98
Condition filters	“Condition filters” on page 74
Diagnostics	“Tests and diagnostics” on page 80
Doors	“Doors” on page 68
Events	“Events” on page 79
Expanders / DGPs	“Bus devices” on page 58, “Expanders” on page 59
Inhibit	“Inhibit and isolate” on page 53
Inputs	“Zones” on page 45
Isolate	“Inhibit and isolate” on page 53
Keypads / RASes	“Bus devices” on page 58, “Keypads” on page 58
Keys	„Keys” on page 54
Outputs	“Outputs” on page 67
Part set	“Set and unset” on page 51
PIN	“PIN” on page 66
Reporting	“Alarm reporting” on page 84
Set	“Set and unset” on page 51
Shunt	“Zone shunt” on page 53, “Door shunt” on page 69
Tests	“Tests and diagnostics” on page 80
Timed unset	“Timed unset / ATM” on page 103
Triggers	“Triggers” on page 76
Unset	“Set and unset” on page 51
User groups	“User groups” on page 62
User programmable functions	“User programmable functions” on page 88
Users	“Users” on page 60
Walk test	“Walk test” on page 80

Function	Reference
Wireless devices	"Wireless device programming" on page 92
Zones	"Zones" on page 45

Zones

Zone is an electrical signal from a security device or a group of devices (PIR detector, door contact) to the Advisor Advanced 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 23.

For zone configuration, see “Zone configuration” on page 30.

Zone addressing is described in “Zone, output, and door addressing” on page 31.

Zone programming is done via “4.1 Zone menu” on page 171 (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 “4.2 Areas” on page 185 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 “4.2 Areas” on page 185 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.

5. Panic

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

Example: panic button.

See also “8.8.1 Panic mode” on page 254.

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 “8.1.3.5 Final set delay” on page 235”).

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 “4.1.n.6.16 Key latch” on page 176, “4.1.n.6.17 Key set” on page 176, “4.1.n.6.18 Key unset” on page 177.

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 “4.1.n.6.19 Technical full set” on page 177, “4.1.n.6.20 Technical unset” on page 177.

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.

Example: Fire doors or emergency doors.

See also “4. Fire” on page 46.

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 “8.1.4.5 Key box time” on page 236). 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 “4.2.n.2 Exit time” on page 186” and “4.2.n.3 Entry time” on page 186.

See also “2. Entry/Exit 1” on page 45 for more details.

19. Shunt

Zone activation causes shunt of all area zones that have shunting allowed. Shunt is allowed by the option “4.1.n.6.36 Shunt” on page 181.

See also “Zone shunt” on page 53.

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 path fault	13. Fire door	14. Aux mains fault	15. Aux batt fault	16. Key box	17. Eng. reset	18. Entry/Exit 2	19. Shunt
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 Double knock		-			-		-					-	-	-	-	-				
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 Engineer walk test		+	+	+	+	+	+				+	+	+	+	+	+				+
4.1.n.6.12 User walk test		+	+	+		+	+				+	+		+	+	+				+
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 — full set										-										
4.1.n.6.17 Key set — part set										-										
4.1.n.6.18 Key unset										-										
4.1.n.6.19 Technical full set												+								
4.1.n.6.20 Technical unset												+								
4.1.n.6.21 Technical 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												-	-		-	-				

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 path fault	13. Fire door	14. Aux mains fault	15. Aux batt fault	16. Key box	17. Eng. reset	18. Entry/Exit 2	19. Shunt
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 Stop report		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

Areas

Area is a section of premises that has specific security requirements. The Advisor Advanced system allows any premises to be divided into different areas having different security requirements. Each area has 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 51 for details.

Areas are configured in “4.2 Areas” on page 185 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 “4.3 Area groups” on page 190.

Note: Area group availability depends on the control panel variant. See “Specifications” on page 35 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 “4.2.n.6 Hierarchy” on page 189.

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 50.

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

- By users via a keypad or a reader. See “Users” on page 60 and “Bus devices” on page 58. The available key sequences are listed in “Keys” on page 54.
- By users via SMS command. See *Advisor Advanced SMS Control Reference Manual* for details.
- By operators remotely via management software. See Chapter 6 “Software” on page 287.
- Automatically via the autosest functionality. See “Autosest” on page 91 for details.

How to use part set

When users performs 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 “8.4.3.1 Report BA” (see page 244). 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 “4.2.n.4.3 Unset delay” on page 188.

There is no way to manually override the 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 “8.4.4 Forced set” on page 244 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 time period.

A zone can be shunted in the following ways:

- Manually by the installer. Use menu “1.2.1.9 Shunt zones” on page 124.
- By a schedule. See “Calendar” on page 77 for details.
- By a conditional filter. See “Condition filters” on page 74 for details.
- By a zone with Shunt type. See “Zone types” on page 45 for details.

Caution: There is a limitation of the number of zones that can be shunted simultaneously. The limit is set in “4.2.n.7.3 Shunt limit” on page 190.

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 particular 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.

Keys

The authorization method depends on system settings. See “2.2.1.n.3.7 Control options” on page 145 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	<input type="checkbox"/>	
		On, PIN, Enter	<input type="checkbox"/>	
	Set with PIN	PIN, On	<input type="checkbox"/>	
		Card	<input type="checkbox"/>	
		On, card	<input type="checkbox"/>	
	Set with card	3 x card	<input type="checkbox"/>	
		Set with card and PIN	On, card, PIN, Enter	<input type="checkbox"/>
			Card, PIN, On	<input type="checkbox"/>
	Unset [2][3]	Unset with PIN	Off, PIN, Enter	<input type="checkbox"/>
PIN				
PIN, Off			<input type="checkbox"/>	
Unset with card		Card	<input type="checkbox"/>	
		Off, card	<input type="checkbox"/>	
Unset with card and PIN		Off, card, PIN, Enter	<input type="checkbox"/>	
		Card, PIN, Off	<input type="checkbox"/>	
		Card, PIN		
Part set [2]		Part set with key	Partset	<input type="checkbox"/>
	Partset, PIN, Enter		<input type="checkbox"/>	
	Part set with PIN	PIN, Partset	<input type="checkbox"/>	
		Part set with card	Card	<input type="checkbox"/>
			Partset, card	<input type="checkbox"/>
	3 x card		<input type="checkbox"/>	
	Part set with card and PIN	Partset, card, PIN, Enter	<input type="checkbox"/>	
		Card, PIN, Partset	<input type="checkbox"/>	
	Door access [2][3]	Door access with PIN	PIN, Enter	<input type="checkbox"/>
Door access with card		Card	<input type="checkbox"/>	

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

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

[2] The functionality depends on “2.2.1.n.3.7.1 Card&PIN mode” on page 145.

[3] The functionality depends on “8.7.7 Easy unset” on page 253.

[4] The functionality depends on “8.7.3 Duress method” on page 250.

[5] Panic alarm functionality depends on the “8.8.1 Panic mode” option described on page 254. It also depends on the “2.2.1.n.3.20 1+3 keys” option described on page 149.

[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 “8.3.3 Alarm list” on page 241.

Common key sequences for keypad without LCD

Table 14: Common key sequences for keypad without LCD

Action	Programmed method	Key sequence	[1]
Set [2]	Set with PIN	On, PIN, On	<input type="checkbox"/>
		Set with card	Card
	Set with card and PIN	On, card	<input type="checkbox"/>
		3 x card	<input type="checkbox"/>
		On, card, PIN, On	<input type="checkbox"/>
		Card, PIN, On	<input type="checkbox"/>

Action	Programmed method	Key sequence	[1]
Unset [2][3]	Unset with PIN	Off, PIN, On	<input type="checkbox"/>
		PIN	<input type="checkbox"/>
		PIN, Off	<input type="checkbox"/>
	Unset with card	Card	<input type="checkbox"/>
		Off, card	<input type="checkbox"/>
	Unset with card and PIN	Off, card, PIN, On	<input type="checkbox"/>
		Card, PIN, Off	<input type="checkbox"/>
		Card, PIN	
	Part set	Part set with card	Card
3 x card			<input type="checkbox"/>
Door access [2]	Door access with PIN	Any digit, PIN, On	<input type="checkbox"/>
	Door access with card	Card	<input type="checkbox"/>
		Any digit, card	<input type="checkbox"/>
	Door access with card and PIN	Any digit, card, PIN, On	<input type="checkbox"/>
		Card, PIN, On	<input type="checkbox"/>
Duress [4]	Duress with PIN	Any set key (On / Off), duress code, Enter	<input type="checkbox"/>
		Duress code, any set key	<input type="checkbox"/>
	Duress with card and PIN	Any set key (On / Off), duress code, card, Enter	<input type="checkbox"/>
		Card, duress code, any set key	<input type="checkbox"/>
Panic [5]	Panic alarm	1 + 3	<input type="checkbox"/>

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

[2] The functionality depends on “2.2.1.n.3.7.1 Card&PIN mode” on page 145.

[3] The functionality depends on “8.7.7 Easy unset” on page 253.

[4] The functionality depends on “8.7.3 Duress method” on page 250.

[5] Panic alarm functionality depends on the “8.8.1 Panic mode” option described on page 254.

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 15 below to describe function keys functionality and availability.

See also “2.2.1.n.3.12 Function keys” on page 148.

Table 15: Function keys

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

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

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 68 for details.

Bus device numbering

Devices use DIP switches to set bus address. The Advisor Advanced 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 “2.2.1.n.2 Keypad address” (keypad) and “2.2.2.n.2 Expander address” (expander).

See also Chapter 2 “Installation > Zone, output, and door addressing” on page 31.

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 “2.2.1.n.4 Keypad menu” (described on page 150).
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 “2.2.1 Keypad devices” on page 143 in Chapter 5 “Menu reference”.

Expanders

Expanders are devices that expand number of inputs or outputs in the Advisor Advanced 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 Advisor Advanced 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 “2.2.2 Expander devices” on page 150 in Chapter 5 “Menu reference”.

Users

Users are identified to the Advisor Advanced 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 61 for more details.

For each user, the system records the following:

- Number
- Name
- PIN
- Card ID number
- Phone number
- 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 35.

Note: Connecting door controllers to the Advisor Advanced system increases the maximum user number in the system (see “Specifications > Access control features” on page 37 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 Advisor Advanced 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. The default supervisor PIN is 1122.

Note: If the configured PIN length is configured for more than 4 digits, zeroes are added to the default PIN values. For example, if the system is configured for 6-digit PINs, the supervisor PIN is 112200.

There is always one installer in the system. More than one user can have rights that allow granting access to the installer or service engineer.

See also “User groups” on page 62.

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 *Advisor Advanced User Guide* and *Advisor Advanced Manager Manual* for more details).

After a new user is added via menu “3.1.0 Add user” on page 162, 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 is able to modify own settings.

Otherwise, choose Cancel to return to the user configuration.

User groups

A user group allows users to control the Advisor Advanced 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. This group can be assigned to only one user, the default installer user.

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.

There are the following types of user groups:

- 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 "3.2.n.2 User group type" on page 168.

Table 16 on page 63 denotes default and allowed user group options (user privileges).

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

Table 16: User group types and allowed options [1]

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

#	Option	User group type						Log
		Normal user	Super-visor	Installer	Guard	Timed Unset / ATM	Reset only	
32.	Door control	No	[Yes]	[Yes]	No	No	No	No
33.	Region ctrl	No	[Yes]	[Yes]	No	No	No	No

[value]: Option is read only.

[1] The value may depend on defaults selected during the initial start-up. See “Initial start-up” on page 114 for details.

[2] See “User privilege limitation” below for details.

[3] Allowed keypad numbers depend on the panel variant. For details, see “General features” on page 36.

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 61.

User group options

User group options are set in menu “3.2.n.6 User group options” on page 169.

The following options are available.

Table 17: User group options as user privileges

#	Option	Description
1.	Full set	Set the premises.
2.	Part set 1	Perform a partial set 1.
3.	Part set 2	Perform a partial set 2.
4.	Unset	Unset.
5.	Inhibit	Inhibit zones.
6.	Isolate	Isolate zones, bus devices, cameras etc.
7.	Time and date	Change system time and date.

#	Option	Description
8.	User adding	Create new users (see also “User privilege limitation” on page 64).
9.	Forced set	Perform a forced set. The availability of this option depends on the system configuration.
10.	Change PIN	Change own PIN.
11.	Walk test	Perform a walk test.
12.	Engineer reset	Perform an engineer reset.
13.	Duress code	Use a duress code.
14.	Reporting tests	Make a test call to the particular central station.
15.	Remote connection	Respond to a remote access request.
16.	Cleaner	Leave zones inhibited after the unset.
17.	User group area list	Display the list of areas.
18.	Menu access	Enter the user menu.
19.	Inst. access	Grant the Installer an access to the system configuration.
20.	Logs access	Access the panel logs.
21.	Stop report	Stop reporting in progress.
22.	SMS reporting	Receive SMS reports.
23.	SMS control	Control the system via SMS.
24.	Card and PIN mode	Set the mode for this particular user group (if possible). The following modes are available: <ul style="list-style-type: none"> • PIN only • Card only • Card or PIN
25.	No OP/CL reports	Open/close events generated by users of the user group are not reported
26.	Schedule access	Access to schedule. The following options are available: <ul style="list-style-type: none"> • None: No access • View: Restricted access. Users can view schedule and cancel actions for the present day. • Configure: Full access.
27.	Fob learning	Program a fob.
28.	Remote pics	Enable remote picture triggering.
29.	Pic deletion	Delete pictures.
30.	CS configuration	Configure CS communication.
31.	Shunt	Shunt zones.
32.	Door control	Control door state: lock, unlock, open, timed open, enable and disable.
33.	Region ctrl	Move users between regions.

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 an Advisor keypad as a prerequisite to perform most Advisor Advanced options. In the Advisor Advanced configuration the PIN is associated with a user, which identifies the PIN holder to the system.

The PINs policy in the Advisor Advanced 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 “8.7.5 PIN chg mode” (see page 250).

PIN length is programmed using “8.7.4 PIN length” on page 250. 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 “3.1.n.2 PIN” on page 162 if the user data is not locked. See “User data lock” on page 61 for more information.

See also “Keys” on page 54.

Outputs

Advisor Advanced 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.

Advisor Advanced outputs are assigned to physical outputs and configured in the menu “6 Outputs and filters” described on page 217 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 74 for more details.

Access control

The Advisor Advanced system allows controlling user access to particular 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 badges 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 69 for more information on door shunts.

See also “Doors” below, “Zone shunt” on page 53.

- 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 69.

Door controller

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

One door controller can control up to four intelligent doors.

Currently there are the following door controllers available: ATS1250, ATS125x (ATS1251, ATS1252, ATS1253, ATS1254).

See “Expanders” on page 59 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 69.
- 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 69.

Use menu “5 Door menu” on page 196 to configure doors.

For reader, door zone and lock outputs default addressing, see “Zone, output, and door addressing” on page 31 in Chapter 2 “Installation”.

Note: It is not required to configure triggers to control door locks. The output set in menu “5.1.n.4 Door output” on page 198 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 time period (schedule) when access to different doors may be granted.

Door groups are programmed in “5.2 Door groups” on page 214.

You can assign door groups to users in “3.1.n.8.1 Door group” on page 167.

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 “5 Door menu” on page 196 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 “5.3 Regions” on page 216 to edit regions.

The menu “5.1.n.9.1 Regions” on page 213 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 “5.1.n.9.2 Anti-passback” on page 213 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 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 “5.1.n.9.4 HSU options” on page 214.

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 Advisor Advanced 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 32 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 have to 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 relay needed are taken from the relay specified in menu “5.1 Doors” on page 196. The “5.1.n.4 Door output” on page 198 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 “5.1.n.6.1.1 Door zone” on page 199 and “5.1.n.6.1.2 Second zone” on page 207.

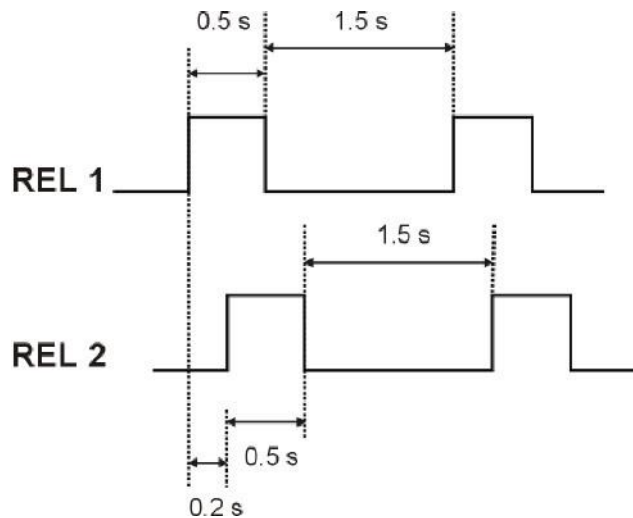
The function is programmed in “5.1.n.6.2.3 Pulsed L&UnL” on page 208.

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 “5.1.n.5.1 Unlock time” described on page 198. If a “Door Unlock” command is sent, this procedure is permanently continued. The procedure continues every 1.5 seconds. See timing diagram in Figure 23 below.

Figure 23

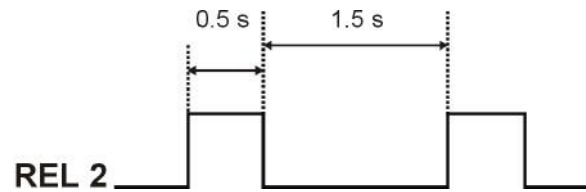


The difference between Door Open and Door Unlock is: The Door Open command only unlocks the door for the Unlock Time, whereas the Door Unlock command opens the door permanently until a Door Lock command is sent. See also “1.2.13 Door control” on page 139.

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 24 on page 73.

Figure 24



Zone monitoring

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

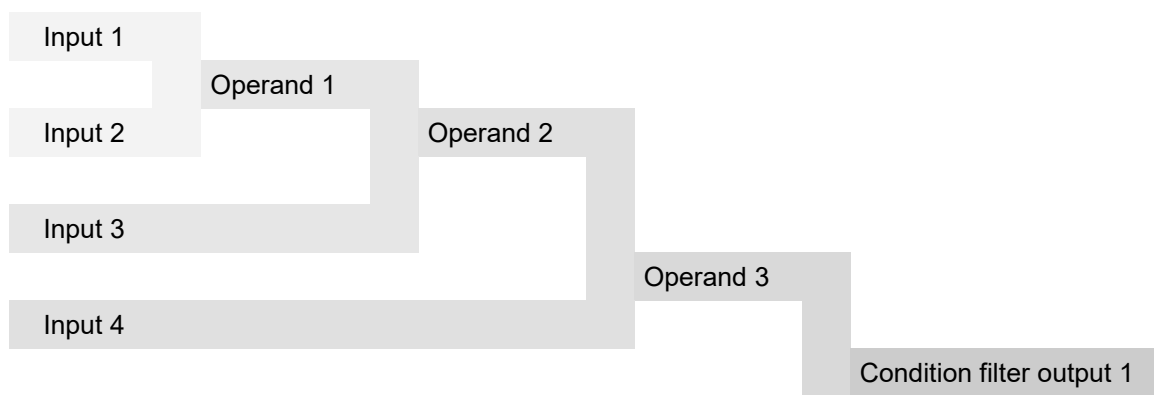
- Door Open or Door Unlock: If the second zone is active and the first zone is normal.
- Door Lock: If the second zone is normal and the first zone is active.

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 have to 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 25: How a condition filter works



You can use a condition filter output as an input for conditional filters that are defined below it in the list. For example, you cannot use condition filter 7 output in conditional filters 2, 3 and 6, but you can use conditional filter 7 output as an event for conditional filter 10.

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 “6.1.n Select filter” on page 217.
2. Change the name of the filter to “Door open” in menu “6.1.n.1 Filter name” on page 217.

3. In menu “6.1.n.2 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 “4 Zones and areas” menu.
4	AND	
5	Area.1.3	Area 1 unset.

4. In menu “6.2 Outputs” on page 219 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.

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 74 for more information.

Each trigger has 7 independent flags that can be set or reset. The flags can be controlled by the following means:

- Advisor Advanced schedule. See “Calendar” on page 77.
- SMS commands. See *Advisor Advanced 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 92 for details.
- Advisor Advanced compatible PC software. Refer to Chapter 6 “Software” on page 287.

See “Events” on page 79 for more information about trigger events.

Calendar

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

The calendar is configured via menu “7 Calendar” on page 225 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 this schedule.

Maximum numbers of schedules, actions, time frames and special days in the system are listed in “Specifications > General features” on page 36.

Schedules are defined by the following parameters.

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

Caution: Time frames should not overlap.

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

If no 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 78.
- **Filter:** A conditional filter that enables the schedule when becomes true. See also “Condition filters” on page 74.

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 88.

Counteractions

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

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

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

Special days in schedules

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

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

Special days are assigned to dates in the menu “7.1 View” on page 225.

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 “8.1.1 Time and date” on page 232.

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 “7.2 Schedules” on page 226.

Note: Available elements and parameters are described in “User programmable functions” on page 88.

Events

Log

All events are recorded in the Advisor Advanced log. The log size is specified in “Specifications” on page 35, Chapter 2 “Installation”.

The log can be viewed using “1.1 Display logs” on page 120.

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 84.

Programming

Advisor Advanced events can be also used for user function programming. See “Condition filters” on page 74 for details. Events and groups of events, available for condition filter programming, are listed in Appendix A “Advisor Advanced events” on page 311.

Tests and diagnostics

The Advisor Advanced system provides a range of test features. Most of them are accessible from “1.2 Test menu” on page 121.

Input and detector tests

To test single inputs or detectors, use “1.2.1 Input tests” on page 121. A single input state can be checked in “1.2.1.7 Zone kOhm” on page 123.

To verify wireless input status, use “1.2.1.3 RF RSSI test” on page 122 and “1.2.1.4 RF diagnostics” on page 122.

Wireless PIR camera range can also be verified in “1.2.1.5 Cam range test” on page 123.

If the detector has an internal test functionality, use “1.2.1.8 Detector test” on page 124 to configure an autotest, or to run it manually.

Test shock sensors via “1.2.2 ShockSens test” on page 125.

Outputs

Test outputs or verify their state using the “1.2.3 Outs&triggers” menu on page 125.

Walk test

Walk test is a working system 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.

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 “1.2.5 Walk test” on page 127 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 “4.1.n.6.11 Engineer walk test” on page 175 enabled.

Configure test parameters using “1.2.5.1 Start” menu on page 127.

After this, run the walk test by “1.2.5 Walk test” on page 127.

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 108 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 “1.2.5.2.9 Reduced walk” on page 129.

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 “4.1.n.6.11 Engineer walk test” on page 175).

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 “8.1.3.3 Walk test time” (see page 234). 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 108).

Single zone walk test

You can also use “1.2.5.3 Single zone WT” on page 129 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 “4.1.n.6.11 Engineer walk test” on page 175 for these zones must be enabled.
- The user privileges in this area must have Walk test allowed. See “3.2 User groups” on page 168 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 “1.2.5.2.7 Frequency” on page 128. If the option “1.2.5.2.8 Need to set” on page 128 is enabled, setting an area without prior user walk test is not allowed.

Note: For walk test purposes Advisor Advanced 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 “1.2.6 Test call opts” on page 130.

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

IP: “1.2.7 IP diagnostic” on page 131

GSM: “1.2.8 GSM diagnostic” on page 133

Battery

Use “1.2.9 Battery test” on page 135 to diagnose the panel battery status. The menu also allows you to configure automatic battery tests.

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 Advisor Advanced reporting features are configured via menu “9 Dialler menu” on page 258 in Chapter 5 “Menu reference”.

Available reporting codes for different protocols are listed in Appendix B “Advisor Advanced reporting codes” on page 327.

Reporting principles

See Appendix B “Advisor Advanced reporting codes” on page 327 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 Advisor Advanced system has defined a particular set of central stations that it can be reported to. It is done via menu “9.2.1 CS mapping” on page 266.

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 exactly 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 “9.2.3 Delayed events” menu on page 267, 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 disarms the area and 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 “9.1.n.9 OP/CL report” on page 262 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 unset 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, Advisor Advanced 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. Advisor Advanced 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.

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 33 on page 327 for event priority values.

Failed to communicate (FTC)

Each central station has the “9.1.n.7 Retry count” described on page 260. 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.

Note: For Voice protocol, there is a possibility to avoid FTC fault using option “9.1.n.8.2.1 Suppress FTC” on page 262.

In FTC condition, the system still tries to re-establish the communication with the central station using test calls that are configured in the “1.2.6 Test call opts” menu described on page 130.

Note: If “1.2.6.n.5 Freq TC if FTC” on page 131 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. Advisor Advanced 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.

User programmable functions

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

Programming menu

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

The list of allowed functions may vary for different menus.

To program a user function:

1 Type
>None<

First, choose an appropriate function type.

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

Next, configure function parameters.

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

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

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

Table 18: Available function types and parameters

Type	Description	Available parameters
None	No function is assigned	None
Set	Set areas [1][2]	1. Areas selection 2. Area groups selection 3. User code requirement
Unset	Unset areas [1]	1. Areas selection 2. Area groups selection
Trigger	Change a trigger state	1. Trigger name 2. State change: Clear, Set, or Toggle
Part set 1	Part set 1 for areas [1][2]	1. Areas selection 2. User code requirement

Type	Description	Available parameters
Part set 2	Part set 2 for areas [1][2]	1. Areas selection 2. User code requirement
Inhibit	Inhibit zones [1][3]	None
Test call	Execute a test call [3][4]	None
PC connection	Establish connection with the PC [1][3]	None
Service in	Allow service in [5]	None
Panic	Activate panic alarm	None
Chime area	Change a chime functionality status in the area	1. Areas 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. Areas selection 2. Area groups selection 3. User code requirement
Fire reset	Reset fire detectors [1]	1. Areas 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 “3.2.n.6 User group options” on page 169 for more details. Note that the user group type must allow this change. See “3.2.n.2 User group type” on page 168 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 time period configured in “8.1.2.1 Activation” on page 233. 2. User code requirement.

Type	Description	Available parameters
Test pic to CS	Take a picture and send it to a central station	1. Camera 2. Central station
Fire	Raise a fire alarm	None
Medical alarm	Raise a medical alarm	None
Show inhibited	Show inhibited zones	None
GSM credit	Check GSM credit	None
UG area access	Change user access to areas	1. UG identifier 2. Areas selection 3. Area groups selection
Prohibit unset	Disable area unset	1. Areas selection 2. State change: On or Off
Shunt	Allow shunt in areas	1. Areas 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 “2.2.1.n.3.11 Quick set” on page 147 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 “4.2.n.4.1 Warning time” on page 187 for more details.

[3] The function is an entry to the appropriate user menu. See *Advisor Advanced 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 78.

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

- Schedule. See “Calendar” on page 77 for more details.
- Function key. See “Function keys” on page 57.
- Fob. See “Wireless device programming” on page 92 for more details.

Autoset

The Advisor Advanced 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 “7 Calendar” on page 225, create an action with Set function. See also “User programmable functions” on page 88.
- Configure an appropriate schedule using the menu “7.2 Schedules” on page 226.
- Enable or disable “4.2.n.5.3 Silent autoset” option on page 188.
- If necessary, set “4.2.n.5.2 Set retry” option on page 188.
If Set retry is allowed, configure “8.4.8 AS user retry” on page 245.
- Set “4.2.n.4.1 Warning time” option on page 187 as well.
- Optionally, configure “8.4.7 AS fault retry” option on page 245.

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 “4.1.0 Add zone” menu described on page 171.

```
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 97 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 “4.1.0 Add zone” menu described on page 171.

```
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 97 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<nnnnnn>”. For example, “Tx H103EB2B” mark identifies a sensor with the ID 103EB2B. See also “4.1.n.7.1 Sensor ID” on page 183 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 96.

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 cameras” on page 98 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 “4.4.0 Add fob” menu described on page 191.

```
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 97 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 “4.4.0 Add fob” menu described on page 191.

```
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
```

- 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 97 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 19 on page 97 for more details.

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

If 1 zone is selected, this zone functionality depends on sensor configuration. See “4.1.n.7.5 Sensor opt” on page 184.

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 19 below lists all compatible devices and their activation methods.

Table 19: Wireless device learning activation

Device type	Learning activation
Door / window sensor	Raise a tamper alarm by opening the housing. Note: For two zones programming in sequential mode, the external contact input must be in open state.
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	<ol style="list-style-type: none"> 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.

Using 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 “4.5.n.2 Pics by zone” on page 193.
In this case camera event type depends on the zone type. See “Camera event types” below.
See also “Zone types” on page 45.
- Activation of a condition filter. The event type is defined for the programmed filter. See “4.5 Cameras” on page 193.
- Activation of a standard reporting event. See “4.5.n.4 Pics by rep ev” on page 194.
- 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 “4.5.n.3.m.2 Event type <n>” on page 194.
- Custom type 2. Generated by conditional filters of this type.

Event type details are listed in Table 20 below.

Table 20: 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 particular 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 “Advisor Advanced reporting codes” on page 327.

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

[4] See “4.5.n.3.m.3 Report as” on page 194 for details.

Each of these types can be configured in “2.2.2.n.4.9.1 Pic settings” on page 155.

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 58 for more details.
2. Program a wireless PIR camera as a wireless PIR detector. See “Wireless device programming” on page 92 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 “4.5 Cameras” on page 193.
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 “4.5.n.2 Pics by zone” on page 193.

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 “4.5 Cameras” on page 193 for details.

6. If necessary, program reporting events that activate the camera. See “4.5 Cameras” on page 193 for details.

Diagnostics

If necessary, use the following menus for diagnostics:

- “1.2.1.3 RF RSSI test” on page 122
- “1.2.1.4 RF diagnostics” on page 122
- “1.2.1.5 Cam range test” on page 123

Troubleshooting

See also Chapter 7 “Troubleshooting” on page 295.

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 request
- 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” above.

OH receiver line trouble when MMS sending

Advisor Advanced 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 “8.2.4.13 Do reset” on page 239.
- 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 “8.2.4.12 System code” on page 239, 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 “4.1.n.2 Zone type” on page 172). 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.

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 “8.9.1 Delay” on page 256.
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 “3.2.n.2 User group type” on page 168 for details.
- Timed unset. The ATM is unset for a programmed time period. This period is defined in “8.9.2 Unset Time” on page 257.

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 “8.9.3 Ext Unset Time” on page 257 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.

Chapter 4

Programming

Summary

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

Content

- The Advisor Advanced menu 106
 - How the menu sections are organized in this manual 106
 - Option availability 107
- How to program the options 108
 - Accessing the installer programming menu 108
 - What the LCD display tells you 109
 - Editing the options 109
 - Confirmation of changes 111
 - Exit from menu 111
 - Keypad layout 112
- Remote access 113
- Initial start-up 114
 - Auto configuration 115

The Advisor Advanced menu

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.

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 “8.2.1 User code required” (see page 237).

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 period set in “8.1.3.6 Installer in-time” on page 235.

The option is enabled in “8.2.6 Challenge code” on page 240.

How the menu sections are organized in this manual

The menu entries are numbered in the Advisor Advanced system. This numbering system is also used in this manual, so menu option 1 “Inhibit zones” is described in section “1 Inhibit zones”.

The menu number also refers to the key sequence you press to enter it. For example, if you want to enter menu 1.4 Walk test, you can press 1, 4 after entering the installer menu.

Option availability

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

- Firmware version
- Panel model (for example, IP or non-IP 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 114 for details.

How to program the options

Accessing the installer programming menu

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

How to access the installer programming menu

1. Start with this LCD display:

```
UTC F&S
TUE 27 May 10:00
```

2. If the option “8.2.1 User code required” (see page 237) 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 period defined in “8.1.3.6 Installer in-time” on page 235.
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.

The following display appears:

```
Inh reports
>Yes<
```

5. 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.
6. Press Enter. The next screen shows whether tampers are inhibited and areas are unset:

```
Inh tampers
Unset areas
```

7. 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
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 “Programming map” on page 351 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
```

Particular 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 112.

- 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 110, enter one of the following:

- An IP address as nnn.nnn.nnn.nnn. For example, 192.168.1.20.
- A host name as a text string. For example, “utc.com”. In this case DNS server must be configured in “9.3.n.5 DNS config” on page 271, 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 “1.2.4 Panel status” on page 126.

Keypad layout

Table 21: AT511xA 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 22: AT5135 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.

Remote access

The panel programming can be accessed remotely via configuration software. A remote access can be gained via IP, GPRS, PSTN or ISDN connection, depending on the available panel hardware configuration and settings.

Note: Connection via USB cable is not a remote connection.

By default, the menu is accessible remotely with the same installer PIN. The remote access PIN can be altered using menu “3.1.n.2.2 Remote PIN” on page 163.

The supervisor have an access to his Remote PIN only if the option “8.7.8.2 Remote PIN” on page 253 allows it.

Cautions

- Once enabled, remote PIN can be neither disabled nor changed locally, and the Remote PIN menu is disabled.
 - If PIN length gets changed (via “8.7.4 PIN length” described on page 250) while remote PIN is enabled, the configuration software will not be able to connect the programmed panel anymore. It will be necessary to delete the panel configuration in the software, and then recreate it.
-

The remote configuration is allowed only if the option “8.7.8.1 Remote config” on page 253 is set to Yes.

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 23: Values set during installation

Option	Default value	Description
1 Panel language	English UK	Defines the language* 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	EN 50131	Defines approval* dependent default values.
3 Duress method	Disabled	Default duress method. See <i>Advisor Advanced Manager Manual</i> for more information.
4 PIN length	4	Default length of PIN (allowed range is from 4 to 10). See "8.7.4 PIN length" on page 250 for more details.
5 Time and date	Depends on the firmware version	Time and date must be set during installation. See also "8.1.1 Time and date" on page 232.
6 Install	Cancel	Run the installation process

* 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. The following messages are displayed:

```
Installer
PIN:1278
```

```
Supervisor
PIN:1122
```

1278 is the default PIN for master installer, and 1122 is the default PIN for a supervisor.

Note: If the PIN length is configured for more than 4 digits, zeroes are added to the default PIN values. For example, if the system is configured for 6-digit PINs, the master installer PIN is 127800.

Confirm each screen with Enter.

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 “8.7 Panel and AB options” (see page 249).

See also “1.5 Default panel” on page 141.

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-?-----
```

```
Rkp 17-32 BUS2
--?-----
```

```
Exp 1-15 BUS1
-?-----
```

```
Exp 16-30 BUS2
-?-----
```

Bus devices are automatically configured in a way that is similar to the configuration via viewing devices menu. See “2.1 Installed remotes” on page 142 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 “2.2.2.n.4.4 Input mode” on page 152 and “8.6.1 Input mode” on page 248.

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 Advisor Advanced control panel.

See “The Advisor Advanced menu” on page 106 for more information about menu organization.

Content

- 1 Service menu 120
 - Test options 121
- 2 Device menu 142
 - 2.1 Installed remotes 142
 - 2.2 Edit Keypad&Exp 143
 - 2.2.1 Keypad devices 143
 - Keypad options 143
 - 2.2.2 Expander devices 150
 - Expander options 150
 - Wireless specific options 153
 - Camera specific options 155
 - Four-door expander specific options 157
 - 2.2.3 DC/LC Exp Rdrs 160
 - Reader options 160
- 3 User menu 162
 - 3.1 Users 162
 - Common options 162
 - Mobile phone options 166
 - Access control options 167
 - 3.2 User groups 168
 - User group settings 168
- 4 Zones and areas 171
 - 4.1 Zone menu 171
 - Zone options 171
 - Adding a wireless sensor 172
 - Common options 172

- Shock sensor options 182
- Wireless sensor options 183
- 4.2 Areas 185
 - Area options 185
- 4.3 Area groups 190
 - Area group options 190
- 4.4 RF fobs 191
 - Fob options 191
- 4.5 Cameras 193
- 5 Door menu 196
 - 5.1 Doors 196
 - Common door options 196
 - Standard door specific options 204
 - Intelligent door specific options 204
 - 5.2 Door groups 214
 - 5.3 Regions 216
- 6 Outputs and filters 217
 - 6.1 Condition filters 217
 - Filter settings 217
 - 6.2 Outputs 219
 - Output settings 219
 - 6.3 Triggers 223
 - Trigger settings 223
- 7 Calendar 225
 - 7.1 View 225
 - 7.2 Schedules 226
 - Schedule settings 227
- 8 System option menu 232
 - 8.1 Timer menu 232
 - 8.2 Engineer options 237
 - 8.3 LCD display options 241
 - 8.4 Set options 242
 - 8.5 Access options 246
 - 8.6 Zone options 248
 - 8.7 Panel and AB options 249
 - 8.8 PA and other 254
 - 8.9 Timed Unset / ATM 256
- 9 Dialler menu 258
 - 9.1 Central station 258
 - Common options 258
 - PSTN and ISDN specific options 263
 - IP and GSM/GPRS specific options 263
 - Photo transmission specific options 265
 - GSM/phone specific options 265
 - 9.2 Event options 266
 - 9.3 Path options 267
 - Common options 268

- PSTN specific options 269
- ISDN specific options 270
- IP specific options 270
- GSM/SMS/GPRS specific options 273
- 9.4 PC connection 282
- Common options 283
- PSTN specific options 285
- IP specific options 285
- GSM specific options 286

1 Service 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.

1.1 Display logs

```
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, engineer reset etc.)
3. Non mandatory: Events other than mandatory events mentioned above
4. Installer: Events caused by an installer (programming mode, PC connection etc.)
5. Access: Access events, like access granted and access denied
6. Dialer: Dialer and communication events

The display shows where the 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

1.2 Test menu

```
1>Input tests
2 ShockSens test
```

The Tests menu gives you access to all testing functions.

1.2.1 Input tests

```
1>Show open zn
2 Nbr of used zn
```

Enter the Input test menu to test inputs.

1.2.1.1 Show open zones

```
0>Zone
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.

1.2.1.2 Number of used zones

```
Zone capacity 64
Zones used 8
```

The Number of used zones menu shows the following system data:

- Zone capacity: Maximum zone number in the Advisor Advanced system
- Zones used: Number of zones currently programmed.

1.2.1.3 RF RSSI test

```
1>Expander 1
2 Expander 5
```

Select the input location first.

Notes

- Only existing RF expanders are displayed.
- The function is not supported in wireless expanders AT51235 with firmware version older than 1.13.

Enter the physical input number on this location. The RSSI is displayed for the selected zone.

```
Zone 1
-44dBm [IIII ]
```

Note: In case of AT51235, 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.

1.2.1.4 RF diagnostics

```
1>Expander 1
2 Expander 5
```

Select the input location first.

Notes

- Only existing RF expanders are displayed.
- The function is not supported in wireless expanders AT51235 with firmware version older than 1.13.

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

1.2.1.5 Cam range test

```
17 Camera 17
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.

1.2.1.6 Inactive days

```
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 “8.1.4.7 Inactive days” on page 236.

1.2.1.7 Zone kOhm

```
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.

1.2.1.8 Detector test

```
1>Duration
      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.

1.2.1.8.1 Duration

```
1 Duration
      >10<
```

Duration defines how long the test signal is active. The allowed range is 10 to 60 seconds.

1.2.1.8.2 Test time

```
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.

1.2.1.8.3 Test when Set

```
3 Test when set
      >Off<
```

Defines whether an automatic test is activated or not when the area with the appropriate detector is set.

1.2.1.8.4 Manual test

```
4 Manual test
      >Cancel<
```

Change the value to OK and press Enter to activate the detector test manually.

1.2.1.9 Shunt zones

```
1>Exit Button
      Shunt Off
```

The menu allows you to shunt zones manually.

1.2.2 ShockSens test

```
1>Panel
2 Input exp
```

Using the ShockSens test 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 “4.1.n.7.2 Gross level” on page 183 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.

1.2.3 Outs&triggers

```
1>Output test
2 Trigger state
```

The Outputs and Triggers menu allows you to test outputs and check trigger states.

1.2.3.1 Output test

```
1>Outputs
2 Keypad LEDs
```

The Output test allows you to check outputs and LEDs.

1.2.3.1.1 Outputs

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.

1.2.3.1.2 Keypad LEDs

```
1>Keypad 1
2 Keypad 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.

1.2.3.2 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
```

1.2.4 Panel status

```
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.

1.2.4.1 View open ZN

```
INFO
View open ZN
```

```
2>Front Door
Zone tamper
```

View abnormal zone states.

All items scroll automatically. Press Enter to exit.

1.2.4.2 Alarms

```
INFO
No alarms
```

View active alarms. Press Enter to exit.

1.2.4.3 Faults

```
INFO
No faults
```

View active system faults. Press Enter to exit.

1.2.5 Walk test

```
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 80 in Chapter 3 “System functions”.

1.2.5.1 Start

Run the engineer walk test.

See “Engineer walk test” on page 80 for details.

1.2.5.2 Walk test opts

```
1>Use int siren
    Yes
```

The Options menu allows setting up the following walk test options.

1.2.5.2.1 Use internal siren

```
1 Use int siren
    >Yes<
```

If the Use internal siren option is set to Yes, each activation of a tested zone is signalled by the internal siren.

1.2.5.2.2 Use buzzers

```
2 Use buzzers?
    >No<
```

If set to Yes, each tested zone activation is signalled by keypad buzzers.

1.2.5.2.3 Log untested

```
3 Log untested
    >Yes<
```

If the Log untested option is set to Yes, untested zones are recorded in the system log.

1.2.5.2.4 Zone tamper

```
4 Zone tamper
    >Yes<
```

If the Zone tamper option is set to Yes, the zone tamper is included into the walk test.

1.2.5.2.5 Rkp/Exp tamper

```
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 have to be tested.

1.2.5.2.6 Siren tamper

```
6 Siren tamper
  >No<
```

If the Siren tamper option is set to Yes, the tamper alarms from sirens assigned to this area also have to be tested.

1.2.5.2.7 Frequency

```
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 Advisor Advanced 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.

1.2.5.2.8 Need to set

```
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.

1.2.5.2.9 Reduced walk

```
9 Reduced walk
  >4h<
```

Reduced walk test period is a time period 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 “1.2.5.1 Start” on page 127 for more details on reduced walk test.

1.2.5.3 Single zone WT

```
With reporting
  >Yes<
```

Before walk test starts, you are asked if the reporting to central stations must be enabled (see “1.2.5.1 Start” on page 127 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 “1.2.5.1 Start” on page 127.

1.2.5.4 Test No Bells

```
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.

1.2.5.5 Active walk test

```
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 82 for more details.

1.2.6 Test call opts

```
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.

1.2.6.n Select CS

```
1>Test call mode
Off
```

Select central station to configure test call options.

1.2.6.n.1 Test call mode

```
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 “1.2.6.n.2 Test call time” below.
- **Period:** Automatic test call triggers once at the time specified in “1.2.6.n.2 Test call time” below, and then repeats with the interval programmed in “1.2.6.n.3 Period” on page 131.

1.2.6.n.2 Test call time

```
2 Test call time
>00:35<
```

If the “1.2.6.n.1 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 “1.2.6.n.1 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 “1.2.6.n.3 Period” on page 131.

Note: If the option “1.2.6.n.4 Extend” on page 131 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.

1.2.6.n.3 Period

```
3 Period
  > <
```

The Period menu defines an interval for test calls that are described in “1.2.6.n.2 Test call time” on page 130.

The allowed range is 1 to 999 hours.

1.2.6.n.4 Extend

```
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.

1.2.6.n.5 Freq TC if FTC

```
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.

1.2.6.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.

1.2.7 IP diagnostic

```
1>ETH
  >>>
```

The IP diagnostic menu provides an access to diagnostic tools for IP connectivity.

1.2.7.n Choose interface

```
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.

1.2.7.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 “9.3.n.7 Firewall” on page 272 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.

1.2.7.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.

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.

1.2.7.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 “9.4 PC connection” menu. See “9.4.1.n.4.3 Ping host” on page 286 for more details. See also “1.2.7.n.2 Ping host” above.

1.2.7.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 “9.1 Central station” menu. See “9.1.n.4.3 Ping host” on page 264 for more details. See also “1.2.7.n.2 Ping host” on page 132.

1.2.7.n.5 NTP status

```
5>NTP status
    Inactive
```

The NTP status screen allows you to check the current 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.

1.2.8 GSM diagnostic

```
1>PIN status
    Normal
```

The GSM diagnostic menu provides an access to diagnostic tools for GPRS and SMS connectivity.

1.2.8.1 PIN status

```
1>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 Advisor Advanced system.

1.2.8.3 GSM net.reg.

```
3>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

1.2.8.4 GPRS net.reg.

```
4>GPRS net.reg.
  Home network
```

The GPRS network registration state can have the same values as described in “1.2.8.3 GSM net.reg.” on page 133.

1.2.8.5 GPRS state

```
5>GPRS net.reg.
  Home network
```

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 “9.3.n.7.8 Disconn.time” on page 280 for more details.
- No data: Unknown error.

1.2.8.6 Network name

```
6>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.

1.2.8.7 Network code

```
7>Network code
```

The network code is the unique identification number of the GSM network in which the GSM dialler is currently registered.

1.2.8.8 RSSI

```
8>RSSI
  23 [IIII ]
```

The Received Signal Strength Indication (RSSI) value is read-only diagnostic information.

The following ranges are available.

Table 24: 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	[IIIII]	Excellent signal

For accurate data transfer, we recommend a RSSI value above 16.

1.2.8.9 Msg sent 24h

```
1>All SMSes
0
```

The Msg sent 24h 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 “9.3.n.6.2 SMS forwarding” on page 278.

1.2.8.10 Battery status

```
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.

1.2.9 Battery test

```
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.

1.2.9.1 Test options

```
1>Panel
3 Exp
```

Use this menu to configure an automatic battery test.
First, select the panel or an expander to test the battery.

1.2.9.1.m Select device type

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

Select the appropriate device group.

1.2.9.1.m.n Select device

```
1>Test time
10
```

Select the appropriate device.

1.2.9.1.m.n.1 Duration

```
1 Duration
> 10<
```

Set duration (in minutes) for battery test.

Allowed range is 2 to 254.

1.2.9.1.m.n.2 Batt.test freq

```
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

1.2.9.2 Man. Bat. test

```
1>Panel
3 Exp
```

The menu allows you to perform a manual test of the device battery.

1.2.9.2.m Select device type

```
1>Exp 1
2 Exp 2
```

Select the appropriate device group.

1.2.9.2.m.n Select device

```
1>Duration [min]
2 Run/Stop test
```

Select the appropriate device.

1.2.9.2.m.n.1 Duration [min]

```
1 Test time
   > 10<
```

Set duration (in minutes) for battery test.

Allowed range is 2 to 254.

1.2.9.2.m.n.2 Run/Stop test

```
2 Run test?
   >Yes<
```

Run battery test.

Test duration is set in “1.2.9.2.m.n.1 Duration [min]” above.

If battery test for this device is already running, you are prompted to stop this test.

1.2.9.3 Battery replaced

```
Confirm?
   >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.

1.2.10 Panel diag

```
1>System V/A
2 Battery V
```

Panel diagnostic allows you to monitor particular electrical data, for example, current and voltage.

1.2.10.1 System V/A

```
System voltage:
   13.8V
```

```
System current:
   0.8A
```

The scrolled screens show the system power supply voltage and current.

1.2.10.2 Battery (V)

```
Battery voltage:  
12.8V
```

The screen shows the battery voltage.

1.2.11 Check card

```
Badge card  
Keypad 1
```

Use the menu to read data from a user card.

Badge card on the keypad indicated on the screen the same way as it is done when user card programming (see “3.1.n.3.1 Assign card” on page 163).

Note: The keypad for user card programming is defined in “8.8.5 Card learn-in” on page 255.

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

```
User 05  
J.Smith
```

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

```
CARD/TAG  
98832665774
```

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

1.2.12 Demo mode

```
1-8 Demo mode  
>1234....<
```

Enable the Advisor Advanced 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 “1.1 Display logs” on page 120.

- 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.

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 “5.1.n.5.1 Unlock time” on page 198.
- 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.

1.3 Software Mgmt

```
1>Software rev
2 Panel language
```

The informational screens provide information on the panel firmware and initial settings.

1.3.1 Software Rev

```
ATS1000A 1.0
TR_008.008.0028
```

The Software Revision menu lets you view information of the version number of the panel firmware.

1.3.2 Panel language

The screen shows panel language set during installation.

See “Initial start-up” on page 114 for details.

1.3.3 Defaults

The screen shows panel defaults set during installation.

See “Initial start-up” on page 114 for details.

1.3.4 USB upgrade

Allows you to write or read the panel firmware or configuration using USB flash drive.

1.3.4.1 FW Upgrade

Allows you to upgrade the panel firmware or configuration with selected file from the USB flash drive.

1.3.4.2 FW Upload

Allows you to read the panel firmware or configuration, and store it as .dfu file on the USB flash drive.

1.4 Bypass panel lid

```
1>Panel lid time
    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 “1.4.1 Panel lid time” value is enough for you to come to the panel, open the housing, and connect the USB cable.
2. Bypass panel lid using menu “1.4.2 Restore lid” below.
3. Open the panel housing and connect the USB cable.

After logging to the panel from the PC, the box tamper is isolated automatically and the box tamper timer is stopped.

1.4.1 Panel lid time

```
1 Panel lid time
    >01'00<
```

The Panel lid timer defines for how long the panel lid is bypassed.

1.4.2 Restore lid

```
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.

1.5 Default panel

```
5 Default panel
   >Cancel<
```

The Default panel menu lets you clear all settings and repeat the initial installation.

Caution: This command deletes all programming settings, including users.

See “Initial start-up” on page 114 for more details.

Caution: After defaulting panel, restart the system by powering it down and up.

1.6 Service in

```
6 Service in
   Disable?
```

The menu lets you disallow the Installer in function before the Installer in-time expires (see “8.1.3.6 Installer in-time” on page 235).

Note: This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 237.

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 “8.2.1 User code required” on page 237.

2 Device menu

```
1>Inst. Remotes
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 58.

For more information on readers, see “Access control” on page 68.

For bus device numbering, see “Bus device numbering” on page 58.

2.1 Installed remotes

```
1>Keypad devices
2 Exp devices
```

The Installed remotes menu shows the status of all connected remote keypads and various system and local expanders.

Note: The maximum number of devices allowed on the databus is given in “General features” on page 36.

Select a device type to display.

2.1.1 Keypad devices

2.1.2 Expander devices

```
Rkp 1-8 BUS1
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
- l : 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.

Note: The second system bus (BUS2) is only available when using the second RS485 LAN extension module. See also “Two system databuses” on page 23.

2.2 Edit Keypad&Exp

```
1>Keypad devices
2 Exp devices
```

Choose what type of device you want to configure.

2.2.1 Keypad devices

```
0>Add keypad
1 Keypad 1
```

Press 0 to add a keypad, or a number to configure an existing one.

Note: The maximum number of devices allowed on the databus is given in “General features” on page 36.

Keypad options

2.2.1.0 Add keypad

```
Keypad number
>_<
```

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.

2.2.1.n Select keypad

Select the keypad number to configure.

2.2.1.n.1 Keypad type

```
1>Keypad type
ATS1115
```

The Keypad type screen is an informational screen. The type is defined by keypad itself.

2.2.1.n.2 Keypad address

```
2>Bus 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.

2.2.1.n.3 Keypad options

```
3>Keypad options
  >>>
```

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.

2.2.1.n.3.1 Keypad name

```
1>Keypad name
  Keypad 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.

2.2.1.n.3.2 Tamper area

```
2>Tamper area
  Area 1
```

The Tamper area option determines which area receives keypad tamper and fault events. To change it, select the area and press Enter.

2.2.1.n.3.3 View areas

```
01-10>View areas
  12.4.....
```

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 110.

Notes

- After changing this list, the control of selected areas is also enabled (see “2.2.1.n.3.5 Control areas” on page 145).

- 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 “5.1.n.6.3 Alarm control” on page 199 instead.

2.2.1.n.3.4 View AG

```
01-10>View AG
    12.4.....
```

Provides the same functionality as in “2.2.1.n.3.3 View areas” on page 144, but for area groups.

See also “Area groups” on page 50.

2.2.1.n.3.5 Control areas

```
5>Control areas
    12.4....
```

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 “2.2.1.n.3.3 View areas” on page 144.

2.2.1.n.3.6 Control AG

```
01-10>Control AG
    12.4.....
```

Provides the same functionality as in “2.2.1.n.3.5 Control areas” above, but for area groups.

See also “Area groups” on page 50.

2.2.1.n.3.7 Control options

```
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 54.

2.2.1.n.3.7.1 Card&PIN mode

```
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 badge 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

2.2.1.n.3.7.2 Logoff time

```
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.

2.2.1.n.3.7.3 1 x set/unset

```
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.

2.2.1.n.3.7.4 3 x badge set

```
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 “2.2.1.n.3.7.1 Card&PIN mode” on page 145 for available modes.
- This functionality is available only if the “2.2.1.n.3.7.3 1 x set/unset” option described above is not configured as Set-Unset.

2.2.1.n.3.8 EE PIN lock

```
8 EE PIN lock
    >No<
```

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 “5.1 Doors > 5.1.n.6.3.4.3 EE PIN lock” on page 201 instead.

2.2.1.n.3.9 Isolate keypad

```
9 Isolate Rkp
>No<
```

Use the Isolate keypad option to isolate the tamper fault events on the selected keypad. The keypad, however, remains functional.

2.2.1.n.3.10 Buzzer silent

```
10 Buzzer silent
>Never<
```

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 E/E: Buzzer remains silent during entry and exit time.

2.2.1.n.3.11 Quick set

```
11 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.

2.2.1.n.3.12 Function keys

```
1>F1 key
2 F2 key
```

Function keys menu allows you to assign a user programmable function to any of available function keys. See “User programmable functions” on page 88 for more details.

Function keys availability depends on the keypad type. See also “2.2.1.n.1 Keypad type” on page 143.

2.2.1.n.3.13 Area ind.LED1

```
13 Area ind.LED1
>.....<
```

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 “2.2.1.n.3.3 View areas” on page 144 and “2.2.1.n.3.5 Control areas” on page 145.

2.2.1.n.3.14 Area ind.LED2

```
14 Area ind.LED2
>.....<
```

Use Area ind.LED2 to program LED 2 indicator in the same way as described in “2.2.1.n.3.13 Area ind.LED1” above.

2.2.1.n.3.15 Status ind.

```
15 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:

- List: The areas are displayed as a vertical list with names and statuses, which requires scrolling.
- Symbolic: All areas are displayed in one screen. Only area numbers and statuses are displayed.
- AG list: The same as list, but for area groups.

- AG symbolic: The same as symbolic, but for area groups.

See *Advisor Advanced User Guide* for more information on area selection.

2.2.1.n.3.16 LCD backlight

```
16 Status ind.
   >Always on<
```

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 particular idle time.
- Excl. entry: LCD backlight is off during the entry time, until a key is pressed.

Note: The backlight timeout depends on the particular keypad firmware.

2.2.1.n.3.17 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 “4.1.n.6.26 ACK on keypad” on page 178 for more details.

2.2.1.n.3.18 EE 1 buzzer

```
18 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 45 for more details.

2.2.1.n.3.19 EE 2 buzzer

```
19 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 47 for more details.

2.2.1.n.3.20 1+3 keys

```
20 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 *Advisor Advanced User Guide* for more details.

This functionality is only available for ATS113x keypads.

2.2.1.n.3.21 Schedule

The shortcut menu allows you to assign up to two schedules to the selected element.

See “Schedule shortcut menu” on page 78 for more information.

2.2.1.n.4 Keypad menu

```
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.

2.2.1.n.5 Delete keypad

```
5 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.

2.2.2 Expander devices

```
0>Add expander
  1 Expander 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 databus is given in “General features” on page 36.

Expander options

2.2.2.0 Add expander

```
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.

2.2.2.n Select expander

Select the expander number to configure.

2.2.2.n.1 Expander type

```
1>Expander type
   AT51201
```

The expander type is an informational screen. The type is set by the expander.

2.2.2.n.2 Expander address

```
2>Exp address
   BUS: 1 ADDR: 1
```

The expander address is an informational screen providing the DIP switch address.

2.2.2.n.3 Expander range

```
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 “2.2.2.n.4.6 Expander mode” on page 154 for more details.

2.2.2.n.4 Exp settings

```
4>Exp settings
   >>>
```

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.

2.2.2.n.4.1 Expander name

```
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.

2.2.2.n.4.2 Tamper area

```
2>Tamper area
   Area 1
```

The Tamper area option determines which area receives expander tamper and fault events. To change it, press Enter and select the area.

2.2.2.n.4.3 Isolate expander

```
3 Isolate exp
   >No<
```

Use the Isolate expander command to isolate the tamper fault events on the selected expander. The expander however remains functional.

2.2.2.n.4.4 Input mode

```
4 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 “8.6.1 Input mode” on page 248.

See “Zone connection” on page 23 for more details on EOL usage.

2.2.2.n.4.5 EOL

```
5 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 “8.6.2 EOL” on page 248.

See “Zone connection” on page 23 for more details on EOL usage.

2.2.2.n.5 Expander menu

```
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 1.13 and newer.

2.2.2.n.6 Delete expander

```
6 Delete exp.
   >Cancel<
```

Use the Delete expander command to remove an expander. Press Enter, select OK and press Enter again. The expander is deleted.

Note: Before removing an expander, you should delete any outputs or condition filters connected to the expander.

Wireless specific options

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

2.2.2.n.4.4.1 Short superv.

```
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.

2.2.2.n.4.4.2 Long superv.

```
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.

2.2.2.n.4.4.3 Smoke superv.

```
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.

2.2.2.n.4.5 R. Sensitivity

```
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.

2.2.2.n.4.6 Expander mode

```
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 1.13 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.

2.2.2.n.4.7 Exp version

```
ATS1238.B008
```

The Expander version screen is an informational screen with the expander version data.

2.2.2.n.4.8 Jamm detection

```
8 Jamm detection  
>Enable<
```

The Jamming detection option must be set to Enable if the wireless expander must detect and report communication jamming attempts.

2.2.2.n.4.11 Default expander

```
11 Default exp  
>No<
```

Reset the wireless expander to the factory settings.

Camera specific 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 cameras” on page 98 for more details.

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 98.

2.2.2.n.4.9.1.1 Burglar settings

```
1>Pic amount
  1
```

Enter the BA settings menu to configure picture settings for burglar alarms.

2.2.2.n.4.9.1.1.1 Pic amount

```
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 “2.2.2.n.4.9.1.1.2 Frame rate” below.

2.2.2.n.4.9.1.1.2 Frame rate

```
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 “2.2.2.n.4.9.1.1.1 Pic amount” above value is larger than 1.

The allowed values are 500 ms, 1 s, 5 s, 15 s, 60 s.

2.2.2.n.4.9.1.1.3 Pic resolution

```
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.

2.2.2.n.4.9.1.2 Fire settings

2.2.2.n.4.9.1.3 Panic settings

2.2.2.n.4.9.1.4 Medical set.

2.2.2.n.4.9.1.5 Tamper set.

2.2.2.n.4.9.1.6 Fault settings

See “2.2.2.n.4.9.1.1 Burglar settings” on page 155

2.2.2.n.4.9.1.7 Custom type 1

2.2.2.n.4.9.1.8 Custom type 2

Custom types are used with condition filters for camera activation.

See “2.2.2.n.4.9.1.1 Burglar settings” on page 155

2.2.2.n.4.9.2 Show pic mem

```
Pictures: 12
Left sp for: 123
```

```
Free sp: 3,0MB
Total sp: 4,0MB
```

The informational screen shows a pictures number currently stored in the wireless PIR camera expander as well as available memory.

2.2.2.n.4.9.3 Pic auto deletion

```
3 Pic autodel
  >1<
```

The value defines whether the pictures stored in the wireless PIR camera expander will be deleted automatically after a chosen period of time (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.

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.

2.2.2.n.4.11 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

2.2.2.n.4.6 Output modules

```
6 Outp. modules
      >0<
```

Enter the number of output controllers fitted to the door controller.

Allowed range is 0 to 32. 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.

2.2.2.n.4.7 Region count limit

```
7 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.

2.2.2.n.4.8 Macro Logic

```
00>Add macro
01 Macro 1
```

Use the menu to program door controller macros.

For more information on macros, see “Door controller macro logic” on page 70.

2.2.2.n.4.8.0 Add macro

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.

2.2.2.n.4.8.m Select macro

Select an existing macro to program.

2.2.2.n.4.8.m.1 Macro name

```
1 Macro name
>Macro 1 <
```

The name identifies the macro for installer, making the programming dependencies clearer.

2.2.2.n.4.8.m.2 Formula

```
1>!Door Open.2
2 OR
```

The Formula menu allows definition of the macro formula. 4 events can be combined in a formula.

2.2.2.n.4.8.m.2.x Select event

Select the appropriate event to configure it.

```
1>Group
Door
```

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, “Advisor Advanced events”, Table 32 on page 322.

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 “Advisor Advanced events”, Table 32 on page 322.

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: Particular events can only be inputs, while some events can be used as outputs only.

2.2.2.n.4.8.m.2.y Select Operator

All events are joined with logical operators. Choose the operator to change it. Valid operators are AND and OR.

2.2.2.n.4.8.m.3 Macro output

```
3>Macro output
  >>>
```

Configure the output of the selected macro.

2.2.2.n.4.8.m.3.1 Output Func.

```
1 Output func.
  >Non-timed<
```

Output functions are described in “Door controller macro logic” on page 70.

2.2.2.n.4.8.m.3.2 Duration

```
2 Duration [s]
  > <
```

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.

2.2.2.n.4.8.m.3.3 Activate

```
1>Group
  Door
```

Select the output event the same way as you configure the input event. See “2.2.2.n.4.8.m.2.x Select event” on page 158 for details.

2.2.2.n.4.8.m.4 Delete macro

```
4 Delete macro
  >Cancel<
```

Use the command to remove a macro from the door controller. To remove the macro, select Ok and press Enter.

2.2.2.n.4.9 Local Devices

The menu is equal to “2.2.3 DC/LC Exp Rdrs”, but applies only to readers connected to the local bus of the selected door controller. Refer to “2.2.3 DC/LC Exp Rdrs” on page 160.

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 databus is given in “General features” on page 36.

Reader options

2.2.3.0 Add reader

```
Reader number
>_<
```

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.

2.2.3.n Select reader

Select the reader number to configure.

2.2.3.n.2 Reader address

```
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.

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.

2.2.3.n.3.1 Reader name

```
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.

2.2.3.n.3.2 LCD

```
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.

2.2.3.n.5 Delete reader

```
5 Delete reader
    >Cancel<
```

To remove the reader, press Enter, select OK and press Enter again. The reader is deleted.

3 User menu

```
1>Users
2 User groups
```

Use the User menu to add, edit, or delete users of the Advisor Advanced system. This menu allows also user groups editing.

3.1 Users

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

The Users menu lets you add, delete and edit system users.

Common options

3.1.0 Add user

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

```
INFO
User added
```

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

3.1.n Select user

Select a user to edit.

The following options can be configured.

3.1.n.1 User name

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

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

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

The name can have up to 16 characters.

3.1.n.2 PIN

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

The menu allows changing user PIN as well as setting up the remote user code.

3.1.n.2.1 Change PIN

```
1 PIN
*****
```

Change the selected user PIN.

See “PIN” on page 66 for details on PIN usage.

3.1.n.2.2 Remote PIN

```
1>Set PIN
*****
```

Remote PIN is a PIN for programming the panel via remote connection. If remote PIN is not set, the installer uses local PIN to log in remotely.

Note: This submenu is available for installer only. If the option “8.7.8.2 Remote PIN” on page 253 allows it, the submenu is also available for the supervisor.

See “Remote access” on page 113 for more details.

3.1.n.2.2.1 Set PIN

```
1>Set PIN
> <
```

Set remote PIN.

To enable remote PIN, use “3.1.n.2.2.2 Enable login” below.

3.1.n.2.2.2 Enable login

```
2>Enable login
>Yes<
```

Use the command to enable remote PIN.

See “3.1.n.2.2 Remote PIN” above for more details.

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 whether a card has been already assigned or not.

3.1.n.3.1 Assign 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.

```
INFO
Badge card
```

Note: This operation is only possible on LCD keypads with integrated readers. The keypad for card learning is defined in System Options. See “8.8.5 Card learn-in” on page 255 for more details. If another keypad is defined as a keypad for card learning, the learning keypad name is prompted, for example:

```
Badge card
Keypad 3
```

Removing a card

If the user has a card assigned, you can remove the assigned card. The following screen appears.

```
1>Remove card
Card set
```

Press Enter.

```
INFO
Card removed
```

The card has been removed from the selected user.

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 4 Zones and areas > 4.4 RF fobs menu described on page 191.

3.1.n.5 Language

```
5>Language
ENGLISH UK
```

The Advisor Advanced system can display menus in the preferred language of each user.

The language is switched after user authorization.

Contact your supplier to get more information about available languages.

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.

```
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 “3.2 User groups” on page 168.

3.1.n.9 Select mode

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

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

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

3.1.n.10 Delete user

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

The display shows:

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

Choose Ok and press Enter. This removes the user.

Repeat 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.

Mobile phone options

3.1.n.7 SMS and Voice

```
1>User phone
    None
```

The SMS and Voice menu contains configuration menus for SMS and voice reporting.

3.1.n.7.1 User phone

```
1 User phone
> <
```

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

This phone number is used if the GSM reporting destination type is set to User or User Group. See "9.1.n.4.1 Type" on page 266.

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

3.1.n.7.2 SMS reporting

```
2 SMS reporting
    Off
```

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

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

This option is editable only if the user belongs to a user group that has the SMS reporting privilege enabled. See "3.2.n.6 User group options" on page 169 for more information.

3.1.n.7.3 SMS control

```
3 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 "3.2.n.6 User group options" on page 169 for more information.

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

Access control options

3.1.n.8 Access options

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

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

3.1.n.8.1 Door group

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

Assign a door group to the selected user.

See Chapter 3 “System functions > Door groups” on page 69 for more information on door groups.

3.1.n.8.2 Trace

```
2 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.

3.1.n.8.3 Privileged

```
2 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.

3.1.n.8.4 Extended access

```
4 Ext. access
    >No<
```

If set to Yes, the selected user has an extended door unlock time granted after badging a valid card or entering PIN. The extended time is set separately for each door. See “5.1.n.5.2 Extended time” on page 198.

3.1.n.8.5 Acc. user type

```
5 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 70 for details.

3.2 User groups

```
0>Add UG
1>Installer Grp
```

The User group program block is used to record information about user groups.

User group settings

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.

3.2.n Select user group

To edit a user group, select a user group first.

The following options can be configured.

3.2.n.1 User group name

```
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.

3.2.n.2 User group type

```
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 62.

3.2.n.3 User group areas

```
01-10>UG areas
  1.....
```

The User group areas option defines which areas the user can control.

3.2.n.4 User group AG

```
01-10>UG AG
  1.....
```

The UG area group option defines which area groups the user can control.

3.2.n.5 User group filter

```
5>UG filter
  Not used
```

When using a filter, the user rights defined by the user group depend on this filter state.

For more information on condition filters, see “6.1 Condition filters” on page 217.

3.2.n.6 User group options

```
6>UG options
  >>>
```

User group options define the user access rights to the particular options.

Available options are listed in “User group options” on page 64.

3.2.n.7 Schedule

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 78 for more information.

3.2.n.8 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:

```
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.

4 Zones and areas

```
1>Zone menu
2 Areas
```

In the Zones and Areas programming section all zone, fob, and area parameters are programmed.

4.1 Zone menu

```
0>Add zone
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

4.1.0 Add zone

```
0>Zone
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, and then select an input.
- 4 Auto-detect: Add a zone assigned to the first unused system input.

See “Zone, output, and door addressing” on page 31 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 “4.1.n.1 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 92.

If the device is a wireless PIR camera, a corresponding camera will be also created in the camera database. See “Using cameras” on page 98.

4.1.n Select zone

```
1>Zone name
   Zone 1
```

Select a zone to program.

Note: Particular options in this menu differ for specific sensors. For specific options, see:

- “Shock sensor options” on page 182
- “Wireless sensor options” on page 183

Common options

4.1.n.1 Zone name

```
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 16 characters.

4.1.n.2 Zone type

```
1>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 45).

4.1.n.3 Isolated

```
3 Isolated
   >No<
```

The Isolated menu allows you to isolate or de-isolate the selected zone.

4.1.n.4 Zone location

```
4>Zone location
   Panel 1.1
```

The Zone location field informs what physical input the zone is connected to.

4.1.n.5 Zone areas

```
5>Areas
   12.....
```

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 has to 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.

4.1.n.6 Zone options

```
6>Zone options
   >>>
```

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 45).

4.1.n.6.1 Inhibit

```
1 Inhibit
   >Yes<
```

If the Inhibit option is set to Yes, this zone can be inhibited by user.

4.1.n.6.2 Isolate

```
2 Isolate
   >Yes<
```

If the Isolate option is set to Yes, this zone can be isolated by users.

4.1.n.6.3 Excl. in PS1

```
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.

4.1.n.6.4 Excl. in PS2

See “4.1.n.6.3 Excl. in PS1” above.

4.1.n.6.5 Double knock

```
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 “8.1.4.2 Double knock open” on page 235) or the zone has to return to normal and trigger again within the Double Knock interval (see “8.1.4.1 Double knock interval” on page 235).

Note: If the option is active, the option “4.1.n.6.30 Held open” on page 179 is not available.

4.1.n.6.6 Swinger shunt

```
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 “8.6.4 Swinger shunt” (see page 249) for one set/unset cycle.

4.1.n.6.7 Anti mask

```
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 23 for more details.

4.1.n.6.8 Zone pairing

```
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.

Note: It is not possible to use this option on the zone assigned to the last input number.

4.1.n.6.9 Chime

```
9 Chime
    >Off<
```

If the Chime option is On, the zone can be switched off and, depending on “8.8.2 Chime menu” setting (see page 254), 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

4.1.n.6.10 Soak test

```
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.

4.1.n.6.11 Engineer walk test

```
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 “1.2.5 Walk test” on page 127 for more details.

4.1.n.6.12 User walk test

```
12 User walk
    >Yes<
```

If the User walk test option is set to Yes, the zone is included in the User walk test. See “1.2.5 Walk test” on page 127 for more details.

4.1.n.6.13 Shock sensor

```
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 “4.1.n.7 Grs&PIs options” (see page 182).

Only the first eight inputs on the control panel and first eight on the input expander support this option.

4.1.n.6.14 Extend EE

```
14 Extend EE
    >No<
```

If the Extend EE option is Yes, the zone activation expands the entry time for the value defined by “4.2.n.4.2 Prealarm time” on page 187.

Note: After entry timer times out, local alarm activates.

4.1.n.6.15 Final door

```
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 “8.1.3.5 Final set delay” on page 235) and the area is set.

4.1.n.6.16 Key latch

```
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).

4.1.n.6.17 Key set

```
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.

4.1.n.6.18 Key unset

```
18 Key unset
    >No<
```

If the Key unset option is set to Yes, the zone is a key switch that unsets an area.

4.1.n.6.19 Technical full set

```
19 Tech full set
    >No<
```

If the Technical full set option is set to No, the technical alarms in this zone are disabled when the area is fully set.

4.1.n.6.20 Technical unset

```
20 Tech unset
    >No<
```

If the Technical unset option is set to No, the technical alarms in this zone are disabled when the area is unset.

4.1.n.6.21 Technical part set

```
21 Tech part set
    >No<
```

If the Technical part set option is set to No, the technical alarms in this zone are disabled when the area is partially set.

4.1.n.6.22 Keypad LCD

```
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.

4.1.n.6.23 Log

```
23 Log
    >No<
```

The Log option determines whether the zone event is recorded in the system log.

4.1.n.6.24 CS report

```
24 CS report
    >No<
```

The CS report option determines whether the zone event is reported to the central station.

4.1.n.6.25 Delay timer

```
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 “8.1.4.4 Input delay” (see page 236).

4.1.n.6.26 ACK on keypad

```
26 ACK on keypad
    >Keypad 1<
```

Acknowledge options are available for keyswitch zone type. They allow you to define a keypad where the particular 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: “4.1.n.6.27 ACK by user” below must be also set for the acknowledgement functionality to work.

4.1.n.6.27 ACK by user

```
27 ACK by user
    >User 3<
```

The option defines the user that is logged in automatically when the selected zone causes an alarm.

Note: “4.1.n.6.26 ACK on keypad” above must be also set for the acknowledgement functionality to work.

See “4.1.n.6.26 ACK on keypad” above for more details.

See also “2.2.1.n.3.17 ACK on keypad” on page 149.

4.1.n.6.28 Sensor type

```
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

Table 25 on page 179 lists events that may be reported for each sensor type.

Table 25: 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
Fire	SIA	FA	FR	FB	FU	FT	FJ
	CID	E110	R110	E570	R570	E373	R373
Generic	SIA	UA	UR	UB	UU	ZS	ZJ
	CID	E150	R150	E570	R570	E381	R381

See also Appendix B “Advisor Advanced reporting codes” on page 327.

4.1.n.6.29 Virtual zone

```
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 67.

4.1.n.6.30 Held open

```
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 “8.1.4.6 Held open time” on page 236.

Note: If the option is active, the option “4.1.n.6.5 Double knock” on page 174 is not available.

4.1.n.6.31 EE set check

```
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.

4.1.n.6.32 Alarm in PS1

```
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 45
- The zone must be included into part set 1. See “4.1.n.6.3 Excl. in PS1” on page 174.
- Zone functionality does not change if the same zone belongs to an area in full set state.

4.1.n.6.33 Alarm in PS2

The same as “4.1.n.6.32 Alarm in PS1” above, but for part set 2.

4.1.n.6.34 Report as

```
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 “Advisor Advanced reporting codes” on page 327 for details.

Notes

- This option is only available for panic type zones. See “Zone types” on page 45.
- The option is only available when Panic mode is set to Silent. Otherwise panic alarm is always reported as PA event. See “8.8.1 Panic mode” on page 254.

4.1.n.6.35 Auto test

```
35 Auto test
    >Yes<
```

If the option is set to yes, the detector will be tested automatically when auto test is active. See also “1.2.1.8 Detector test” on page 124.

4.1.n.6.36 Shunt

```
36 Shunt
    >Yes<
```

If the option is set to Yes, the zone can be shunted.

See “Zone shunt” on page 53 for details.

4.1.n.6.37 View isolated

```
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.

4.1.n.6.38 Stop report

```
38 Stop report
    >No<
```

If the option is set to Yes, zone activation stops voice reporting, if active.

This option is only available for keyswitch type zones.

4.1.n.8 Copy

```
1>Copy params
    >>>
```

Use Copy menu to copy zone parameters.

The following copy methods are available.

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.

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 “4.1.n.7 RF details” on page 183 for more details.

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 “8.7.9 Object scheme” on page 253 for details.

See also “Zone, output, and door addressing” on page 31.

4.1.n.10 Delete zone

```
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 96 for more details.

Shock sensor options

4.1.n.7 Grs&Pls options

```
7>Grs&Pls opts
>>>
```

The Gross and Pulse options are valid if the “4.1.n.6.13 Shock sensor” functionality (see page 176) for this zone is set to Yes.

4.1.n.7.1 Pulse count

```
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.

4.1.n.7.2 Gross level

```
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 “1.2.2 ShockSens test” (see page 125).

Wireless sensor options

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 1.13 or newer, which is online.

4.1.n.7.1 Sensor ID

```
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 26 on page 184.

4.1.n.7.2 Sensor type

```
2>Sensor type
  DWS
```

The screen allows you to view the sensor type. The following sensor types are available:

Table 26: 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*

4.1.n.7.3 Sensor mode

```
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 96 for more details.

4.1.n.7.4 Supervision

```
3 Supervision
  >Off<
```

Enables or disables the wireless device supervision. Supervision of all types becomes active. See “2.2.2.n.4.4 Supervision” on page 153 for more details.

4.1.n.7.5 Sensor opt

```
4 Sensor opt
  >Ignore alarm<
```

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 27: 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

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.

4.2 Areas

```
1>Area 1
2 Area 2
```

The Area menu allows you to configure areas and area groups.

See “Areas” on page 50 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

4.2.n Select area

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

Select an area to program.

4.2.n.1 Area name

```
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 16 characters.

4.2.n.2 Exit time

```
2 Exit time 1
  > <
```

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 “4.1.n.2 Zone type” on page 172) or a zone with the final door option (see “4.1.n.6.15 Final door” on page 176) to complete.

Note: If zones are assigned to more than one area, the longest exit time is used. See “4 Zones and areas” on page 171.

4.2.n.2.1 Exit time 1

4.2.n.2.2 Exit time 2

Configure exit timers for entry/exit 1 and entry/exit 2 zone types. See “4.2.n.2 Exit time” above for details on exit timer programming.

4.2.n.2.3 PS Exit time 1

4.2.n.2.4 PS 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 “4.2.n.2 Exit time” above for details on exit timer programming.

4.2.n.3 Entry time

```
3 Entry time 1
  > <
```

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 particular entry zones. See “4.2.n.4.2 Prealarm time” on page 187 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 “4 Zones and areas” on page 171.

4.2.n.3.1 Entry time 1

4.2.n.3.2 Entry time 2

Configure entry timers for entry/exit 1 and entry/exit 2 zone types. See “4.2.n.3 Entry time” on page 186 for details on entry timer programming.

4.2.n.3.3 PS Entry time 1

4.2.n.3.4 PS 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 “4.2.n.3 Entry time” on page 186 for details on entry timer programming.

4.2.n.4 Other timers

```
1>Warning time
    1
```

The menu groups additional area timers. See submenus below for details.

4.2.n.4.1 Warning time

```
1 Warning time
    > <
```

Warning time is a period of time 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 “4.2.n.5.2 Set retry” on page 188.

The warning timer can be programmed from 1 to 15 minutes.

4.2.n.4.2 Prealarm time

```
2 Prealarm time
    > <
```

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 “4.1.n.6.14 Extend EE” described on page 176.

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 “4 Zones and areas” on page 171.

4.2.n.4.3 Unset delay

```
3 Unset delay
  > <
```

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 52 for more details.

4.2.n.5 Set/unset options

```
1>Entry alarms
  Delayed
```

The menu groups the following setting options.

4.2.n.5.1 Entry alarms

```
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.

4.2.n.5.2 Set retry

```
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 “4.2.n.4.1 Warning time” on page 187). If the autoset has been postponed by a normal user, the system will attempt autoset again after a time period defined in “8.4.8 AS user retry” on page 245.

Note: The privileged users, Installer and Supervisor, can choose the postpone time during the Warning time.

4.2.n.5.3 Silent autoset

```
3 Silent autoset
  >Off<
```

If Silent autoset is on, the keypad buzzer remains silent during the “4.2.n.4.1 Warning time” described on page 187.

4.2.n.5.4 Dual unset

```
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 296 in Chapter 7 “Troubleshooting”.

4.2.n.6 Hierarchy

```
6 Hierarchy
   >Off<
```

Set a hierarchy for the selected area. The area hierarchy can have value from 1 (highest) to 3 (lowest). Hierarchy 0 is means that the functionality is off and this area functions with no restrictions.

See “Area hierarchy” on page 50 for more details.

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 36 in Chapter 2 “Installation”.

See also “Inhibit and isolate” on page 53.

4.2.n.7.1 Inhibit limit

```
1 Inhibit limit
   > <
```

The maximum number of system elements that can be inhibited at any one time.

4.2.n.7.2 Isolate limit

```
2 Isolate limit
   > <
```

The maximum number of system elements that can be isolated at any one time.

4.2.n.7.3 Shunt limit

```
3 Shunt limit
    > <
```

The maximum number of system elements that can be shunted at any one time.

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 78 for more information.

4.3 Area groups

```
1>AG 1
2 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 35 in Chapter 2 “Installation”.

See also “Area groups” on page 50.

Area group options

4.3.n Select area group

```
1>Name
    AG 1
```

Select an area group to program.

4.3.n.1 AG name

```
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.

4.3.n.2 Areas

```
01-10 Areas
.....
```

Assign areas to the selected area group.

4.4 RF fobs

```
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

4.4.0 Add fob

To add a fob, follow one of the procedures described in “Wireless device programming” on page 92.

4.4.n Select fob

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

Select an existing fob to program.

4.4.n.1 Fob name

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

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

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

A fob name can consist of 16 characters.

4.4.n.2 Assigned user

```
2>Assigned user
      User 1
```

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.

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 “4.4.n.2 Assigned user” on page 191 for the button combinations to work.

Table 28 below lists buttons and combinations that are available.

Table 28: 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 2 + 3	—
Buttons 2 + 4	—
Buttons 3 + 4	—

4.4.n.3.1 Select button

```
1>Function
>>>
```

Select a button to assign a user function to it. See “User programmable functions” on page 88 for more details.

4.4.n.4 RF details

```
1>Sensor ID
14232C1
```

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

4.4.n.4.1 Sensor ID

```
1>Sensor ID
14232C1
```

The screen allows you to view the sensor ID.

4.4.n.4.2 Remove RF dev

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

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

4.4.n.5 Remove fob

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

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

4.5 Cameras

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

The menu allows you to configure camera modules in wireless PIR cameras. For more details on cameras, see also “Using cameras” on page 98.

4.5.n Select camera

```
1>Camera name
  Camera 17
```

Select an appropriate camera to configure.

4.5.n.1 Camera name

```
1 Camera name
  >Camera 17  <
```

Enter camera name.

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.

4.5.n.3 Pics by filter

```
1>Filter 1
    >>>
```

Additionally to the zones listed in “4.5.n.2 Pics by zone” on page 193, there can be up to two condition filters that also trigger the camera.

4.5.n.3.m Select filter

```
1>Filter 1
    Not used
```

Select one of two filters to configure.

4.5.n.3.m.1 Choose filter

```
00>Not used
01 Internal sire
```

Choose a filter that activates the selected camera.

4.5.n.3.m.2 Event type <n>

```
2 Event type 1
    >Burglar<
```

Define a type of the condition filter chosen in “4.5.n.3.m Select filter” above.

The available filter types are listed in “Camera event types” on page 98.

4.5.n.3.m.3 Report as

```
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 “Advisor Advanced reporting codes” on page 327 for details.
- Only particular reporting events are available.

4.5.n.4 Pics by rep ev

```
1>Rep. event 1
    Not used
```

The camera can be also triggered by a selected reporting event.

4.5.n.4.m Select event

```
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 “Advisor Advanced reporting codes” on page 327 for details.
- Only particular reporting events are available.

4.5.n.5 Isolated

```
5 Isolated
    >No<
```

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

4.5.n.6 Max pics 24h

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

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

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

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

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

4.5.n.7 Remote pics

```
7 Remote pics
    >Yes<
```

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

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.

5 Door menu

```
1>Doors
2 Door groups
```

Use the Door menu to add, edit, or delete doors, door groups, and regions of the Advisor Advanced system.

5.1 Doors

```
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: Particular options in this menu are specific for different door types. For specific options, see:

- “Standard door specific options” on page 204
- “Intelligent door specific options” on page 204

Common door options

5.1.0 Add door

```
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 31 in Chapter 2 “Installation”.

5.1.n Select door

Select a door to edit.

The following options can be viewed or configured.

5.1.n.1 Door name

```
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.

5.1.n.2 Door location

```
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 “4.1.n.4 Zone location” on page 173.

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 204.

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

5.1.n.4 Door output

```
0>Not used
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 Advisor Advanced system. See “8.5.2.1 Map relays” on page 247 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.

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.

5.1.n.5.1 Unlock time

```
1>Time
0
```

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.

5.1.n.5.2 Extended time

```
1>Time
0
```

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 “3.1.n.8.4 Extended access” on page 167.

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 204.

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.

5.1.n.6.1.1 Door zone

```
0>Not used
17 Zone 17
```

Select a zone with door contact for the selected door.

5.1.n.6.3 Alarm control

```
1>Door areas
    >>>
```

Set alarm control options for the selected door.

5.1.n.6.3.1 Door areas

```
1>Door areas
123456789012345>
```

Select door areas.

In case of an intelligent door, the areas specified here are used for:

- The reader LEDs if the option “5.1.n.3.5.5 LEDs option” described on page 206 is selected to show area status.
- “5.1.n.6.3.4.1 Deny access” when set (described on page 200).
- Option “5.1.n.6.4.3 Dis. when set” on page 209 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 62.

See “How to edit a list” on page 110 for details on the area selection.

Note: “2.2.1.n.3.3 View areas” on page 144 and “2.2.1.n.3.5 Control areas” on page 145 are not available for keypads that are configured as door readers.

5.1.n.6.3.2 Door AGs

```
2>Door AGs
123456789012345>
```

Select door area groups in the same way as areas in “5.1.n.6.3.1 Door areas” on page 199.

5.1.n.6.3.3 When unset

```
1>Low security
No
```

Define the door functionality when the assigned areas are unset.

5.1.n.6.3.3.1 Low Security

```
1 Low security
>No<
```

If set to yes, the door is operating in the low security mode when all door areas are unset, which means the user authorization is changed from Card *and* PIN to Card *or* PIN.

5.1.n.6.3.3.2 Unlock Door

```
2 Unlock Door
>No<
```

If set to yes, the door is unlocked when all door areas are unset.

5.1.n.6.3.4 When set

```
1>Deny access
No
```

Define the door functionality when the assigned areas are set.

5.1.n.6.3.4.1 Deny access

```
1 Deny access
>No<
```

If set to Yes, the door access is denied unconditionally when any of door areas is set.

5.1.n.6.3.4.2 Lock door

```
2 Lock door
>No<
```

If set to Yes, the door is locked when all door areas are set.

5.1.n.6.3.4.3 EE PIN lock

```
3 EE PIN lock
  >No<
```

If the EE PIN lock option is set to Yes, it is not possible to use a PIN during the entry time.

The option is equal to “2.2.1 Keypad devices > 2.2.1.n.3.8 EE PIN lock” on page 146.

5.1.n.6.4 RTE options

```
1 Use RTE
  >>>
```

Configure RTE (Request to exit) functionality options.

5.1.n.6.4.1 Use reader RTE

```
1>Reader IN
2 Reader OUT
```

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 204.

5.1.n.7 Schedule opts

```
1>Door unlocked
  >>>
```

The menu allows you to configure schedule options for the selected door.

5.1.n.7.1 Door unlocked

```
1>Schedule
  >>>
```

Configure schedule options for the door unlock.

5.1.n.7.1.1 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 78 for more information.

5.1.n.8 Shunt options

```
1>Zones
  >>>
```

Use the menu to set up door shunt options for the door.

See also “Door shunt” on page 69 in Chapter 3 “System functions” for shunt functionality description.

For options specific for standard doors, see “Standard door specific options” on page 204. For options related to intelligent doors, see “Intelligent door specific options” on page 204.

5.1.n.8.2 Shunt timers

```
1>Shunt time
    >>>
```

The menu allows you to configure timers assigned to the door shunt. See details below.

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 as submenus:

1. Time: Set the time value from 0 to 127.
2. Resolution: Set units (seconds or minutes) for the time value above.

5.1.n.8.2.1 Shunt time

```
1>Time
    0
```

The amount of time (value and units) for the door zone to be shunted.

5.1.n.8.2.2 Extended time

```
1>Time
    0
```

The extended shunt timer, which is applied if the user has extended time option enabled. See “3.1.n.8.4 Extended access” on page 167 for details.

5.1.n.8.2.3 Warning time

```
1>Time
    0
```

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 88, “Zone shunt” on page 53.

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 204.

5.1.n.8.3.1 Shunting

```
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 “5.1.n.8.2.1 Shunt time” on page 202.
- 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 “5.1.n.6.5.4 Forced door” on page 210 and “5.1.n.6.5.5 DOTL” on page 210.

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.

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 “8.7.9 Object scheme” on page 253 for details.

See also “Zone, output, and door addressing” on page 31.

5.1.n.11 Delete door

```
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

5.1.n.8.3.2 Shunt active

```
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.

5.1.n.8.4 Indication

```
1>Door held open
    No
```

The menu allows you to configure options for indication of particular access control events.

5.1.n.8.4.1 Door held open

```
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.

5.1.n.8.8 EE Shunt

```
8 EE Shunt
    >No<
```

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).

Intelligent door specific options

5.1.n.3.5 Readers opts

```
1>Card and PIN
    >>>
```

Use the menu to configure readers of the selected door.

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.

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 "8.5.1.2 Two cards" on page 246.

The option is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

5.1.n.3.5.3 NoSchedule req

```
1>Reader Out
    No
```

This option extends the exit access for the selected OUT reader.

- Yes: The user has an 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 an 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.

5.1.n.3.5.4 Card format

```
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
- ATS Wiegand 23 bit
- Mag swipe - Aritech format
- Mag swipe - Midas format

5.1.n.3.5.5 LEDs option

```
5 LEDs option
>Door locked<
```

Specifies the status that the reader LEDs indicate (not applicable for PIN readers).

- 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 70.

See also “5.1.n.6.3.1 Door areas” on page 199.

5.1.n.3.5.6 Time&Attendance

```
6 Time&Attendanc
>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.

5.1.n.3.5.7 Disable Duress

```
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.

5.1.n.6.1.2 Second zone

```
0>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 “5.1.n.6.1.1 Door zone” on page 199.

5.1.n.6.1.3 DOTL zone

```
0>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 “5.1.n.6.5.5 DOTL” on page 210.

5.1.n.6.2 Door unlocked

```
1>Lock when CL
  No
```

The menu contains various options for the selected door unlocking process.

5.1.n.6.2.1 Until closed

```
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.

5.1.n.6.2.2 Until opened

```
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 “5.1.n.5.1 Unlock time” on page 198.

5.1.n.6.2.3 Pulsed L&UnL

```
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 71.

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 62 for details.

5.1.n.6.3.6 Control type

```
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. Badging 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.

5.1.n.6.3.7 If PIN sets

```
1>Deny access
   No
```

Configure the door operation if the area is set using PIN.

5.1.n.6.3.7.1 Deny access

```
1>Deny access
   No
```

If set to Yes, the access to the door is denied if the areas were set using PIN.

5.1.n.6.4.2 RTE zone

```
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 “5.1.n.6.4 RTE options” on page 201.

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.

5.1.n.6.4.4 RTE Control

```
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 “5.1.n.5.1 Unlock time” on page 198.
- 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.

5.1.n.6.5 Reporting

```
1>CL & Locked
No
```

Determines when access control events are reported.

5.1.n.6.5.1 CL & Locked

```
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.

5.1.n.6.5.2 OP&Unl as Unl

```
2 OP&Unl as Unl
   >No<
```

If set to yes, the door is reported as unlocked, if it is open and unlocked.

5.1.n.6.5.3 Open/Close

```
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).

5.1.n.6.5.4 Forced door

```
4 Forced door
   >No<
```

If set to Yes, opening of the door without a valid card, PIN or Request To Exit is reported.

5.1.n.6.5.5 DOTL

```
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.

5.1.n.6.5.6 RTE

```
6 RTE
   >No<
```

If set to Yes, Request To Exit zone activation is reported.

5.1.n.6.6 Interlocking

```
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.

5.1.n.7.1.2 After entry

```
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 “5.1.n.7.1 Door unlocked” on page 201.

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 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 78 for more information.

- 2 RdrIn Inh PIN. If set to yes, the IN reader is in the low security mode if the above schedule is active.
- 3 RdrOut Inh PIN, etc.

The functionality is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

5.1.n.7.3 RTE Schedule

```
1>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 78 for more information.

5.1.n.8.1 Zones

```
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 “5.1.n.8 Shunt options” on page 201.

5.1.n.8.4 Indication

```
1>DOTL output
   Not used
```

The menu allows you to assign door controller outputs for indication of the specific access control events.

5.1.n.8.4.2 DOTL output

```
00>Not used
19 Output 17
```

Select an output on the door controller to indicate the Door Open Too Long alarm.

5.1.n.8.4.3 Warning output

```
00>Not used
20 Output 17
```

Select an output on the door controller to indicate the warning before the shunt time or extended shunt time expires. See also “5.1.n.8.2 Shunt timers” on page 202.

5.1.n.8.4.4 Forced door

```
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).

5.1.n.8.5 Until door CL

```
5 Until door CL
   >No<
```

If set to Yes, the door shunt zones remain shunted as long as the door is opened.

5.1.n.8.6 CancelAfterCL

```
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 approx. 2 seconds).

5.1.n.9 Regions & AP

```
1>Regions
    >>>
```

The menu contains door options connected to region control and anti-passback.

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 “5.3 Regions” described on page 216.

See Chapter 3 “System functions > Regions” on page 69 for details.

5.1.n.9.2 Anti-passback

```
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 69 for details.

5.1.n.9.3 Inh Reg 1 Usr

```
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.

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 70 for details.

5.1.n.9.4.1 Req HSU Nr

```
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.

5.1.n.9.4.2 Prewarn. time

```
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.

5.1.n.9.4.3 HS alarm out

```
00>Not used
19 Output 17
```

Select an output on the door controller to indicate an anti-passback or high-security alarm.

5.2 Door groups

```
0>Add Door Gr
1 Door Gr 1
```

Door groups define when a user can have an access to specific doors.

See Chapter 3 “System functions > Door groups” on page 69 for details.

5.2.0 Add Door Gr

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.

5.2.n Select door group

```
1>Door Gr name
   Door Gr 2
```

Select a door group to program.

5.2.n.1 Door Gr name

```
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.

5.2.n.2 Door Gr data

```
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 an 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 78 for more information.

4. Repeat for all doors specific for this door group.

5.2.n.3 Delete Door Gr

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:

```
2 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.

5.3 Regions

```
0>Add region
1 Outside
```

Configure regions.

See Chapter 3 “System functions > Regions” on page 69 for more information.

5.3.0 Add region

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.

5.3.n Select region

```
1>Regionname
Region 2
```

Select a region to program.

5.3.n.1 Region name

```
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.

5.3.n.2 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:

```
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.

6 Outputs and filters

```
1>Cond filters
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.

6.1 Condition filters

```
0>Add filter
1 External Siren
```

A condition filter is an evaluation and a decision-making algorithm. There are 64 pre-programmed filters.

Filter settings

6.1.0 Add filter

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.

6.1.n Select filter

Select an existing filter to program.

6.1.n.1 Filter name

```
1 Filter name
>Filter 52 <
```

The name identifies the filter for installer, making the programming dependencies clearer.

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.

6.1.n.2.0 Add event

```
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.

6.1.n.2.x Select event

Select the appropriate event to configure it.

```
1>Group
    System
```

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 “Advisor Advanced events” on page 311.

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 “Advisor Advanced events” on page 311.

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

6.1.n.2.y Select operator

All events are joined with logical operators. Choose the operator to change it. Valid operators are AND, OR, and XOR.

6.1.n.3 Invert

```
3 Invert
    >No<
```

The Invert option specifies if the condition filter output is inverted.

6.1.n.4 Delete filter

```
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.

6.2 Outputs

```
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

6.2.0 Add output

```
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 31 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 “6.2.n.1 Output name”.

6.2.n Select output

Select an appropriate existing output to program. There are 200 programmable outputs in the system.

6.2.n.1 Output name

```
1 Output name
>Output P1.6 <
```

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.

6.2.n.2 Output location

```
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.

6.2.n.3 Invert output

```
3 Invert output
   >No<
```

The Invert output option determines if the output is inverted.

6.2.n.4 Start filter

```
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 “6.2.n.6 Mode” below.

6.2.n.5 Stop filter

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

Use the Stop filter menu to specify an optional condition filter that deactivates the output.

6.2.n.6 Mode

```
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 “6.2.n.7.1 Delay time” on page 222.

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 “6.2.n.7.1 Delay time” on page 222. After the time passes, the output activates for a time defined in “6.2.n.7.2 Active time” on page 222, and then it switches off.

If the stop condition filter is set, its activation deactivates the output and resets both described timers.

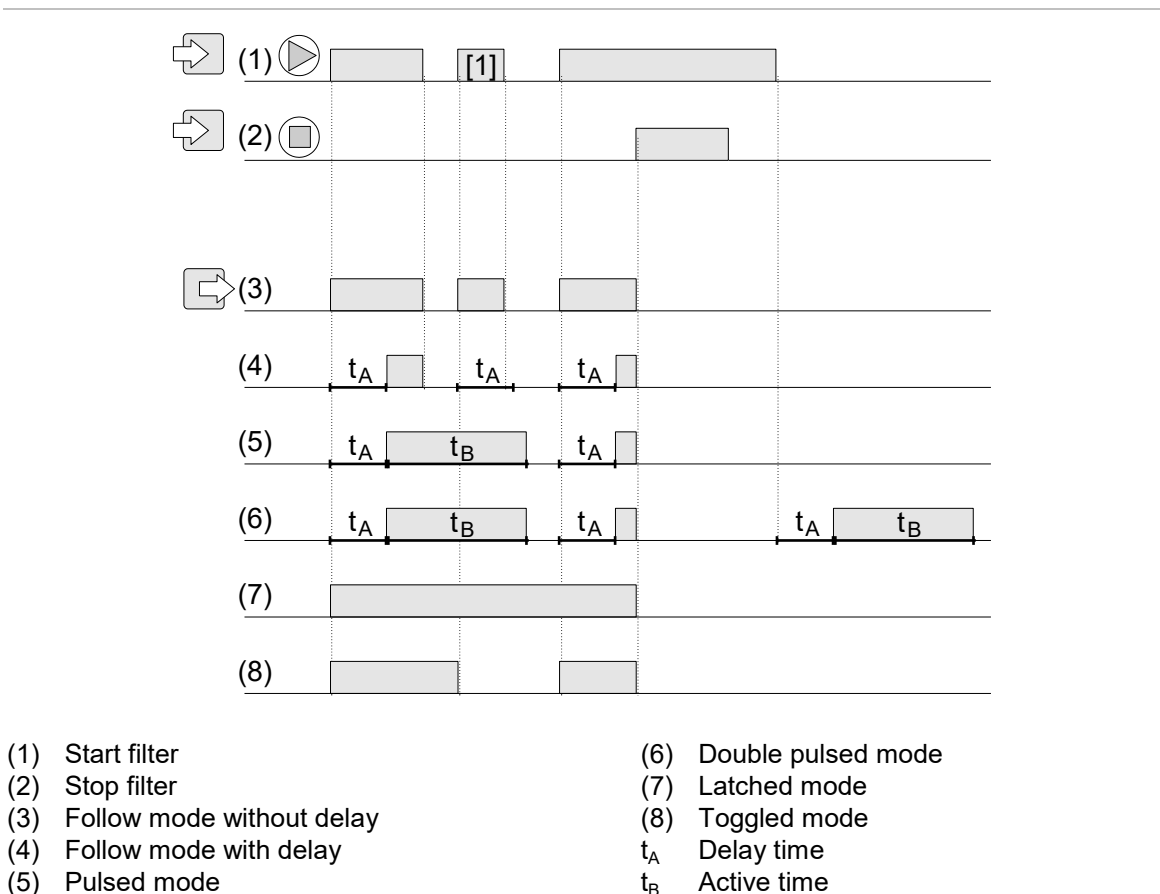
- Double pulsed: Similar to the previous one, except the delay timer is activated by any change of the start condition filter, activation and deactivation.
- Latched: A single activation of the start condition filter switches the output on. The output can be then deactivated only by activating the stop 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 26 below shows examples of described output activation modes.

Figure 26: Output activation mode examples



Note: Full active time t_B is equal to the programmed delay if the option 6.2.n.7.3 Retriggerable is set to No. Otherwise, the timer is restarted when start filter goes active [1] and the active time is prolonged. See “6.2.n.7.3 Retriggerable” on page 222 for more details.

6.2.n.7 Parameters

```
1>Delay time
   00:00'00
```

Set the appropriate parameters for the functions described above.

6.2.n.7.1 Delay time

```
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.

6.2.n.7.2 Active time

```
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 “6.2.n.6 Mode” on page 220.

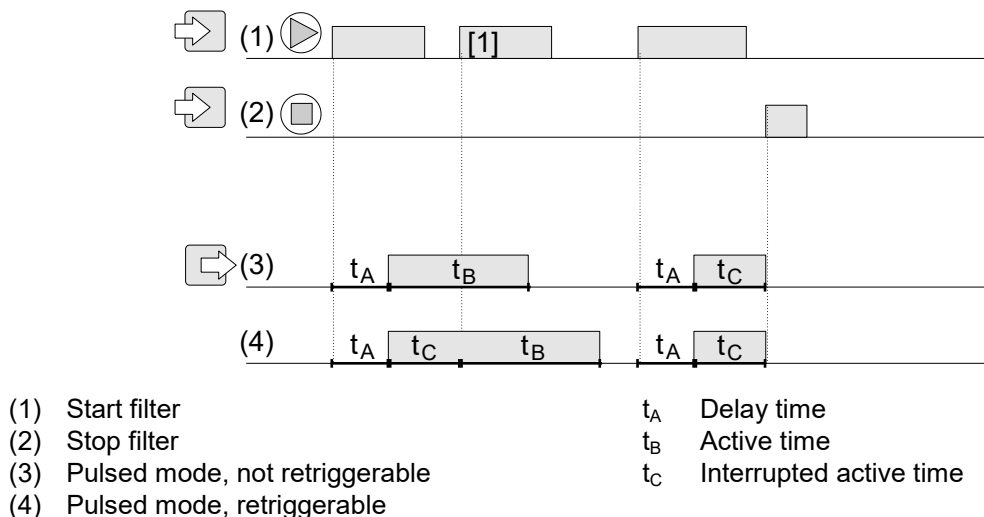
6.2.n.7.3 Retriggerable

```
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 27 below shows the output retriggering when the start filter is reactivated [1].

Figure 27: Output examples



6.2.n.8 Log limit

```
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.

6.2.n.9 Delete output

```
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.

6.3 Triggers

```
0>Add trigger
1 Trigger 1
```

The Triggers menu allows you to configure system triggers.

Trigger settings

6.3.0 Add trigger

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.

6.3.n Select trigger

```
1>Name
   Trigger 1
```

Select a trigger to program.

6.3.n.1 Trigger name

```
1 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.

6.3.n.2 Schedule

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 78 for more information.

6.3.n.3 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:

```
3 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.

7 Calendar

```
1>View
2 Schedules
```

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 77 in Chapter 3 “System functions” the detailed functionality description.

7.1 View

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

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

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

7.1.n Date

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

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

7.1.n.1 Auto setting

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

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

Select All areas, or choose the appropriate area.

7.1.n.2 By object

```
1>Area
2 Rkp
```

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 88.

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 78.

7.1.n.3.1 Day type

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

Choose a type for the selected day:

- Normal day: A normal day. A special day time frame is not valid.
- Holiday, Special day 2 etc.: The day is one of special days defined in “7.2.n.6 Special days” on page 230.

7.1.n.3.2 Recurring

```
2 Recurring
   >Yes<
```

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

7.1.n.3.3 Until date

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

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

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

7.2 Schedules

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

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

The maximum schedule number in the system is given in “General features” on page 36.

For more information on schedules see “Schedules” on page 77 in Chapter 3 “System functions”.

Schedule settings

7.2.0 Add schedule

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

```
INFO
Schedule added
```

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

7.2.n Select schedule

```
1>Name
Schedule 1
```

Select a schedule to program.

7.2.n.1 Schedule name

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

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

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

7.2.n.2 Active

```
2 Active
>No<
```

If set to Yes, the schedule is currently active.

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.

7.2.n.4 Time

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

Define time frames when the schedule activates.

7.2.n.4.0 Add time frame

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

```
INFO
Time frame added
```

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

Caution: Time frames should not overlap.

7.2.n.4.m Select time frame

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

Select a time frame to program.

7.2.n.4.m.1 Start time

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

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

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

7.2.n.4.m.2 End time

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

Provide the time of the day in 24-hour HH:MM format when the selected time frame ends. The value 00:00 means that the end time is not set, and therefore the counteraction is not performed. See Chapter 3 “System functions > Counteractions” on page 78 for more information.

7.2.n.4.m.3 Week days

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

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

If no 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 77.

7.2.n.4.m.4 Delete time frame

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

The display shows:

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

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

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

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 36.

7.2.n.5.0 Add action

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

```
INFO
Action added
```

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

7.2.n.5.m Select action

```
1>Name
   Action 1
```

Select an action to program.

7.2.n.5.m.1 Action name

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

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

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

7.2.n.5.m.2 Object type

7.2.n.5.m.3 Function

7.2.n.5.m.4 Parameters

Available functions and parameters are described in “User programmable functions” on page 88.

7.2.n.5.m.5 Delete action

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

The display shows:

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

Choose Ok and press Enter. This removes the action.

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

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

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 36.

7.2.n.6.0 Add special day

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

```
INFO
Sp day added
```

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

7.2.n.6.m Select special day

```
1>Name
   Holiday
```

Select a special day to program.

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

```
1 Name
>Holiday <
```

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

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

Note: Special day names are common for all schedules.

7.2.n.6.m.2 Start time

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

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

7.2.n.6.m.3 End time

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

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

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

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

The display shows:

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

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

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

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 “6.1 Condition filters” on page 217 for more details.

7.2.n.8 Delete schedule

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

The display shows:

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

Choose Ok and press Enter. This removes the schedule.

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

8 System option menu

```
1>Timer menu
2 Engineer opt
```

Use the System menu to program the global system options including timers.

8.1 Timer menu

```
1>Time&date
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.

8.1.1 Time and date

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

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

The following options are available.

- 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 78 for information on daylight saving time change on programmed actions.

8.1.2 Siren options

```
1>Activation
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.

8.1.2.1 Activation

```
1>Internal siren
00:03'00
```

The Activation menu allows you to set the activation time both for internal and external siren.

8.1.2.1.1 Internal siren

8.1.2.1.2 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).

8.1.2.1.3 F/P/M internal

8.1.2.1.4 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).

8.1.2.2 Delay time

```
1>Internal siren
00:00'00
```

The Delay time menu allows you to set the delay time before an internal or external siren is activated.

8.1.2.2.1 Internal siren

8.1.2.2.2 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.

8.1.3 System misc opts

The System misc options menu allows you to set up all system programmable timers.

8.1.3.1 Armed display

```
1 Armed display
   >00'30<
```

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.

8.1.3.2 Card and PIN

```
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.

8.1.3.3 Walk test time

```
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 “1.2.5 Walk test” on page 130.

8.1.3.4 Mains reporting delay

```
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.

8.1.3.5 Final set delay

```
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.

8.1.3.6 Installer in-time

```
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 “8.2.1 User code required” on page 237). 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.

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.

8.1.4 Zone timer menu

```
1>DblKnock int
    10'00
```

The Zone timer menu allows you to set up all programmable zone timers.

8.1.4.1 Double knock interval

```
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.

8.1.4.2 Double knock open

```
2 DblKnock open
    >00'05<
```

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.

8.1.4.3 Soak test

```
3 Soak test
   > <
```

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 “4.1.n.6.10 Soak test” on page 175) for a zone has been set to Yes. During the soak test period the zone does not trigger alarms.

8.1.4.4 Input delay

```
4 Input delay
   > <
```

The Input delay value represents the delay between an input and appropriate zone activation. The allowed range is 0 to 255 seconds.

8.1.4.5 Key box time

```
5 Key box time
   > <
```

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.

8.1.4.6 Held open time

```
6 Held open time
   >00:00'00<
```

The options define the time period of held open, after which the zone raises “open too long” flag, which can be used for filter programming.

See “4.1.n.6.30 Held open” on page 179.

8.1.4.7 Inactive days

```
7 Inactive days
   > <
```

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 “1.2.1.6 Inactive days” menu described on page 123.

8.2 Engineer options

```
1>User Code Req
    Yes
```

The Engineer options are options that apply to maintenance and installation functions.

8.2.1 User code required

```
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 *Advisor Advanced User Guide* for more information on Installer option.

8.2.2 Tamper required

```
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.

8.2.3 Engineer lockout

```
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 (jumper T1 set during power-up).

Caution: If this option is enabled, it is impossible to run the system recovery procedure. See “Recovery procedure” on page 296 for more information.

8.2.4 Engineer reset

```
1>Alarm
    No
```

The Engineer reset menu lets you define which conditions require an engineer reset, and also lets you perform this reset.

8.2.4.1 Alarm

```
1 Alarm
    >No<
```

If the Alarm option is set to Yes, the area in which the alarm occurred can not be set until an engineer reset has been performed, provided engineer reset prevents setting (see “8.4.1 RTS options”, page 242).

This option is ignored in case AB alarm confirmation is enabled. For more information see “8.2.4.4 Confirmed alarm” on page 238.

8.2.4.2 Tamper

```
2 Tamper
    >No<
```

If the Tamper option is set to Yes, tamper alarms require an engineer reset.

8.2.4.3 Panic

```
3 Panic
    >No<
```

If the Panic option is set to Yes, panic alarms require an engineer reset.

8.2.4.4 Confirmed alarm

```
4 Conf. alarm
    >Off<
```

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.

8.2.4.5 Battery fail

```
5 Battery fail
    >Off<
```

If the Battery fail option is set to Yes, battery faults require an engineer reset.

8.2.4.6 Aux fuse

```
6 Aux fuse
    >Off<
```

If the Aux fuse option is set to Yes, auxiliary fuse faults require an engineer reset.

8.2.4.7 Mains fail

```
7 Mains fail
    >Off<
```

If the Mains fail option is set to Yes, mains supply faults require an engineer reset.

8.2.4.8 Siren fault

```
8 Siren fault
    >Off<
```

If the Siren fault option is set to Yes, siren faults require an engineer reset.

8.2.4.9 Interconn fault

```
9 Intconn fault
    >Off<
```

If the Interconnection fault option is set to Yes, interconnection faults require an engineer reset.

8.2.4.10 Auto reset

```
10 Auto reset
    >Off<
```

If the Auto reset option is set to Yes, the engineering reset is performed automatically upon the installer log in.

8.2.4.11 Dis by service

```
11 Dis by servi>
    >Off<
```

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 “8.2.1 User code required” on page 237.

8.2.4.12 System code

```
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 102 for more information.

8.2.4.13 Do reset

```
13 Do reset
    >Cancel<
```

The Do reset command is used to perform the engineer reset.

8.2.4.14 Custom text

```
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 102.

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 102 for more information.

8.2.5 Service in

```
5 Service in
  Disable?
```

The menu lets you disallow the Installer in function before the Installer in time expires (see “8.1.3.6 Installer in-time” on page 235).

Note: This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 237.

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 106.

8.2.6 Challenge code

```
6 Challenge code
  Disable
```

Use this menu to activate challenge code functionality. See “Challenge code requirement” on page 106 for more details.

Caution: Once activated, this option cannot be deactivated by software settings.

8.2.7 Inspection

```
1>Date
  31.12.2099
```

Set up a periodic inspection reminder.

8.2.7.1 Date

```
1 Date
  >31.12.2099<
```

Enter the date of the next inspection.

8.2.7.2 Custom msg

```
2 Custom msg
  >Need inspectio<
```

Enter the message for the inspection reminder.

8.3 LCD display options

```
1>Arm display
   Always
```

The LCD options menu contains options that can be set for LCDs and menus.

8.3.1 Armed display

```
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 “8.1.3.1 Armed display” (see page 234).

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.

8.3.2 Custom message

```
2 Custom msg
   >UTC F&S <
```

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.

8.3.3 Alarm list

```
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 54.
- **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 “8.3.1 Armed display” on page 241 for details.

8.3.4 Indicate faults

```
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.

8.3.5 View EE timer

```
5 View EE timer
  >Off<
```

The option defines if the entry and exit timers are displayed during setting and unsetting the system.

8.4 Set options

```
1>RTS options
2 Inhibit incl
```

Options on the Set options menu define the set conditions.

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

8.4.2 Inhibit includes

```
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

8.4.3 Part set

```
1>Report BA
   Yes
```

The Part set menu allows you to configure the part set options.

8.4.3.1 Report BA

```
1 Report BA
   >Yes<
```

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.

8.4.3.2 Access to EE

```
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.

8.4.3.3 EE full set

```
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 “4.2.n.2 Exit time” on page 186 must be longer than 0.

8.4.3.4 PS1 name

8.4.3.5 PS2 name

```
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 *Advisor Advanced User Manual* for more details on partial setting.

8.4.4 Forced set

```
3 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.

8.4.5 Forced set options

```
4 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.

8.4.6 Pending alarms

```
5 Pending alarms
  >Enable<
```

If set to Enable, the Pending alarms option requires all alarms and faults to be acknowledged.

Enable EN Gr3 is equal to Enable except that faults and tampers can only be acknowledged by level 3 user (installer).

When disabled, it does not require alarm acknowledgement. During unsetting or resetting the area, the alarm is acknowledged automatically. However, each alarm and fault is shown 3 times on the keypad screen.

8.4.7 AS fault retry

```
6 AS fault retry
  >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 91 for more details.

8.4.8 AS user retry

```
8 AS user retry
  >15 minutes<
```

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 91 for more details.

The user must have a privilege for full setting to be allowed to postpone the autoset. See “3.2.n.6 User group options” on page 169 for more details.

8.5 Access options

```
1>Access timers
2 DGP options
```

The menu contains various access control options.

8.5.1 Access timers

```
1>Card to PIN
127
```

The menu contains access timer settings.

Note: All timers are programmed in seconds. The allowed ranges are 0 to 127 s.

8.5.1.1 Card to PIN

```
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.

8.5.1.2 Two cards

```
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.

8.5.1.3 Multiple badge

```
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.

8.5.1.4 Re-lock delay

```
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.

8.5.2 DGP options

```
1>Map relays
  No
```

The menu contains door controller settings.

8.5.2.1 Map relays

```
1 Map relays
  >No<
```

Defines whether door controller unlock outputs can be controlled as standard outputs.

- Yes: Door unlock outputs can be controlled by the control panel as its outputs.
- No: Door unlock outputs can only be activated by door controller when using door unlock user menu, or upon presenting a valid card.

8.5.2.2 Map panel LEDs

```
2 Map panel LEDs
  >No<
```

When this option is set to Yes, LEDs in door readers connected to the door controller will represent the same status as LEDs in keypads connected directly to the panel.

8.6 Zone options

```
1>Input mode
  Dual loop
```

The Input options menu defines options of zone inputs.

8.6.1 Input mode

```
1 Input mode
  >Dual loop<
```

The Input mode option determines the configuration of 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 “8.6.2 EOL” below, normal state for Single NO zone is open.
- **Single NC:** Similar to Single NO above, but If EOL is disabled in “8.6.2 EOL” below, 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 “8.6.2 EOL” below. See “Zone connection” on page 23 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 only. For expanders, see “2.2.2.n.4.4 Input mode” on page 152.

8.6.2 EOL

```
2 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 “8.6.1 Input mode” option above.

See “Zone connection” on page 23 for more details on EOL usage.

This is a setting for panel only. For expanders, see “2.2.2.n.4.5 EOL” on page 152.

8.6.3 Siren tamper EOL

```
3 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 “8.6.2 EOL” on page 248.

8.6.4 Swinger shunt

```
4 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 “4.1.n.6.6 Swinger shunt” option enabled (see page 174).

8.6.5 Report restore

```
5 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.

8.7 Panel and AB options

```
1>Panel name
   Panel
```

The Panel and AB options menu allows you to change particular system values. See also “Initial start-up” on page 114.

If particular 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 111.

8.7.1 Panel name

```
1 Panel name
   >Panel <
```

The Panel name menu lets you change the panel name.

8.7.2 Panel language

```
2 Panel language
  >ENGLISH UK<
```

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 114, and “Predefined users” on page 60.

8.7.3 Duress method

```
3 Duress method
  >Disabled<
```

The Duress method menu allows you to change the duress entering method.

See *Advisor Advanced User Guide* for more information on available duress methods.

8.7.4 PIN length

```
4 PIN length
  > <
```

The PIN length menu allows you to change the PIN length. See “3.1.n.2.1 Change PIN” on page 163 for more information about PINs.

Caution: If PIN length is changed when remote PIN is set, the configuration software will not be able to connect the panel with the programmed data anymore. See “3.1.n.2.2 Remote PIN” on page 163 for details.

8.7.5 PIN chg mode

```
5 PIN chg mode
  >Custom<
```

The PIN change mode option allows you to choose the appropriate PIN change mode. See “3.1.n.2.1 Change PIN” on page 163 for more details.

8.7.6 Alarm confirm

```
6>AB mode
  >>>
```

The Alarm confirm menu allows you to set a various options connected to the alarm verification.

8.7.6.1 AB mode

```
1>Area 1
  Off
```

The AB mode option enables the AB alarm confirmation feature for particular areas. When set to On, the first alarm is reported as a standard burglar alarm (A-

alarm). A second input has to 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.

8.7.6.2 AB time

```
1>Intr. AB time
      1
```

The menu allows you to configure the maximum delay between A and B alarms.

8.7.6.2.1 Intrusion AB time

```
1 Intr. AB time
      > <
```

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.

8.7.6.2.2 Holdup AB time

```
2 Holdup AB time
      > <
```

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 “8.7.6.2.1 Intrusion AB time” above.

8.7.6.3 System confirm

```
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.

8.7.6.4 EE confirm

```
4 EE confirm
      >No<
```

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.

8.7.6.5 Access to EE

```
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.

8.7.6.6 TA confirm

```
6 TA confirm
  >No<
```

If the TA confirm option is set to Yes, tamper alarm (TA) can report a B-alarm for burglary alarm (BA), and vice versa.

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 “8.7.6.1 AB mode” on page 250.

8.7.6.8 Call CS message

```
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.

8.7.6.9 Reporting delayed

```
9 Rep. delayed
  >Yes<
```

Enable a 30-second delay before alarm reporting required by ACPO regulations.

8.7.7 Easy unset

```
7 Easy unset
  >Yes<
```

If enabled, you can unset premises entering a PIN or badging a valid card without pressing any other keys.

8.7.8 Remote options

```
1>Remote config
  Yes
```

Set remote configuration options.

8.7.8.1 Remote config

```
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.

8.7.8.2 Remote PIN

```
2 Remote PIN
  Yes
```

If the option is set to Yes, the supervisor is allowed to change his Remote PIN. See “Remote access” on page 113 for details.

8.7.9 Object scheme

```
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 31 in Chapter 2 “Installation”.

8.8 PA and other

```
1>Panic mode
   Silent
```

The menu allows you to configure panic alarm mode, chime, and buzzer options, etc.

8.8.1 Panic mode

```
1 Panic mode
   >Silent<
```

Panic mode can be one of the following.

- Silent: The panic alarm is silent (no siren activation)
- Audible: The panic alarm is standard (with siren activation)
- Audible alarm if line fault: The panic alarm is audible only if a Line Fault (LF) or a Failed To Communicate (FTC) fault is present

8.8.2 Chime menu

```
1>Chime in PS
   No
```

The Chime menu allows you to set up chime options.

8.8.2.1 Chime in part set

```
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.

8.8.2.2 Latched chime

```
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.

8.8.3 System tamper areas

```
3 SysTamp areas
  >1.....<
```

The System tamper areas option allows assigning system tampers and faults to the specified areas. At least one area must be selected.

8.8.4 Siren retrigger

```
4 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.

8.8.5 Card learn-in

```
5 Card learn-in
  >Keypad 1<
```

Choose a keypad for user card learning. See also “3.1.n.3 User card” on page 163.

8.8.6 Test inputs

```
6 Test inputs
  >All<
```

The Test inputs option defines what inputs should be accessible when performing input tests as described in “1.2.1 Input tests” on page 121. The following options are available:

- All: All inputs are visible.
- If used: Only the inputs assigned to the existing zones are visible.

8.8.7 Buzzer mode

```
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.

8.8.8 Mon 3 HC out

```
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 30 for details.

8.8.9 Card number

```
9 Card number
  >Basic<
```

Select the way the card number is represented in the control panel.

- Basic. The card number is represented in the standard Advisor Advanced format.
- Titan. The card number is represented in the extended Titan format.

8.8.10 Anonymize Log

```
10 Anonymize Log
  > <
```

The menu allows you to set a time 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 30 days.

8.9 Timed Unset / ATM

```
1>Delay
  0
```

The menu allows you to configure the ATM (automated teller machine) interface.

8.9.1 Delay

```
1 Delay
  > <
```

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.

8.9.2 Unset Time

```
2 Unset Time
  > <
```

The maximum allowed unset time of the ATM. The allowed range is 1 to 255 minutes.

8.9.3 Ext Unset Time

```
3 Ext Unset Time
  > <
```

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.

8.9.4 Uns Warn Time

```
4 Uns Warn Time
  > <
```

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.

9 Dialler menu

```
1>CS
2 Event options
```

The menu is used to program all system-wide communication options.

9.1 Central station

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

The Advisor Advanced system lets you program up to 16 central stations.

9.1.0 Add CS

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.

9.1.n Select central station

```
01>CS name
CS 1
```

Select a central station to program.

Note: Particular options in this menu differ for specific transmission paths. For specific options, see:

- “PSTN and ISDN specific options” on page 263
- “IP and GSM/GPRS specific options” on page 263
- “Photo transmission specific options” on page 265
- “GSM/phone specific options” on page 265

Common options

9.1.n.1 CS name

```
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.

9.1.n.2 Transm path

```
1>PSTN
4 IP
```

The transmission path defines the type of connection for reporting alarms to the central station. Paths are defined in menu “9.3 Path options” on page 267.

9.1.n.3 Protocol

```
3 Protocol
> (X) SIA<
```

Choose the appropriate communication protocol.

Depending on the settings in “9.1.n.2 Transm path” above, the following protocols can be available:

- SIA
- (X)SIA
- VOICE
- CID
- OH+SIA
- OH+XSIA
- OH+CID
- SMS TEXT
- SMS+CID
- SMS+SIA
- SMS+XSIA
- VOICE+SMS
- SMS+MMS
- OHPHOTO+CID
- OHPHOTO+SIA
- OHPHOTO+XSIA
- PHOTO+XSIA

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.

Note: When using voice reporting, account codes are used to identify if alarms for an area should be reported. The account code is not transmitted.

In case a few areas have the same account numbers, and “9.1.n.9 OP/CL report” option on page 262 is set to Yes, a special operation takes place for SIA/XSIA reporting of opening/closing depending on the area modifier setting (see “9.1.n.8.1 XSIA”, page 261).

- 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.

9.1.n.5.m Select area

```
1 Area 1
  > <
```

Set account numbers for each area.

9.1.n.6 Mode

```
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 “9.1 Central station” on page 258). 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 84 for more information.

9.1.n.7 Retry count

```
7 Retry count
  >1<
```

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 86 for more information.

The value ranges from 0 to 14. The default value is 1.

9.1.n.8 Protocol opt

```
1> (X) SIA
2 VOICE
```

It is possible to customize the communication protocol parameters using the Protocol opt menu.

9.1.n.8.1 XSIA

```
1>Area modifier
      Off
```

The XSIA menu allows you to set options for the SIA and XSIA protocol.

9.1.n.8.1.1 Area modifier

```
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 “9.1.n.5 Accounts” on page 259.

9.1.n.8.1.2 Name chars

```
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.

9.1.n.8.1.3 Event number

```
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.

9.1.n.8.1.4 Subev coding

```
4 Subev coding
      >Decimal<
```

The Subev coding value defines whether the subevent number is reported to the CS in hexadecimal (hex) or decimal format.

9.1.n.8.1.5 SIA frequency

```
5 SIA frequency
  >Bell<
```

The SIA frequency menu allows you to select one of two standards for modem communication regarding transmitted/received frequencies used by transmitter/receiver.

This option allows you to select between CCITT and BELL.

9.1.n.8.2 VOICE

```
1>Suppress FTC
  No
```

The VOICE menu allows you to configure voice reporting options listed below.

9.1.n.8.2.1 Suppress FTC

```
1 Suppress FTC
  >No<
```

If the Suppress FTC option is set to Yes, no FTC fault is activated for this central station when the voice protocol is used.

9.1.n.8.2.2 Without ACK

```
2 Without ACK
  >No<
```

If the Without ACK option is set to Yes, a recipient of a voice message does not need to acknowledge the message.

Otherwise, he must acknowledge it by pressing a phone key using tone dialing mode. The panel tries to retransmit the message until it is acknowledged.

9.1.n.9 OP/CL report

```
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 “9.1.n.8.1.1 Area modifier” on page 261).

Note: When (X)SIA protocol is selected, separate reporting works only when SIA area modifier is enabled.

See “9.1.n.5 Accounts” on page 259 for more details.

9.1.n.11 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:

```
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.

PSTN and ISDN specific options

9.1.n.4 Phone

```
4 Phone
> <
```

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

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

Note: To enter a character, press the corresponding key twice.

IP and GSM/GPRS specific options

9.1.n.4 Destination/IP

```
1>Type
    Phone
```

The Destination menu contains the configuration of the reporting receiver.

9.1.n.4.1 Dest name

```
1 Dest name
> <
```

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 111.

9.1.n.4.2 Dest port

```
2 Dest port
    > <
```

The destination port is used to report to the host selected in “9.1.n.4.1 Dest name” on page 263.

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 a 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 “1.2.7.n.2 Ping host” described on page 132 to send ping to another host.

9.1.n.8.3 OH 2000

```
1>Version
    OH V1.9.3
```

The OH 2000 menu allows you to set up a few OH 2000 protocol options that are listed below.

9.1.n.8.3.1 Version

```
1 Version
    >OH V1.9.3<
```

The following versions of the OH 2000 protocol can be used for Osborne-Hoffman receiver communication:

- OH V1.9.3
- OH V2
- OH V3

See an appropriate receiver’s manual for more details.

9.1.n.8.3.2 Heartbeat time

```
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.

9.1.n.8.3.3 Receiver nbr

```
3 Receiver nbr
   >0001<
```

A receiver identifier used in central stations with multiple receivers. The allowed value is a hexadecimal number from 0001 to FFFF.

9.1.n.8.3.4 Line nbr

```
4 Line nbr
   >0001<
```

A line identifier used in central stations with multiple receiving lines. The allowed value is a hexadecimal number from 0001 to FFFF.

9.1.n.8.3.5 Freq. HB time

```
5 Freq. HB time
   >00:01'00<
```

If the primary CS communication fails, the backup CS heartbeat time is switched from normal to frequent.

See also “9.1.n.8.3.2 Heartbeat time” on page 264.

Photo transmission specific options

Additionally to “IP and GSM/GPRS specific options” described on page 263, it is necessary to set the options below.

9.1.n.4.4 Encryption

```
4 Encryption
   >No<
```

If the Encryption option is set to Yes, the pictures are sent encrypted with AES algorithm.

9.1.n.4.5 Vid dest port

```
5 Vid dest port
   >9000<
```

The destination port is used to send the pictures to a host set up in “9.1.n.4.1 Dest name” on page 263.

GSM/phone specific options

9.1.n.4 Destination

```
1>Type
   Phone
```

The Destination menu contains the configuration of the reporting receiver.

9.1.n.4.1 Type

```
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 “9.1.n.4.2 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 “9.1.n.4.2 Phone/User/UG” below.
- User Group: The report is sent to all users that belong to the user group that is set via menu “9.1.n.4.2 Phone/User/UG” below.

User and user group reporting require the following:

- Users must have their phone numbers set in “3.1.n.7.1 User phone” on page 166.
- The SMS reporting must be enabled for these users. See “3.1.n.7.2 SMS reporting” on page 166.
- At least one of the user groups must allow these users to receive SMS reports. See “3.2.n.6 User group options” on page 169).

9.1.n.4.2 Phone/User/UG

```
2 Phone  
> <
```

This menu depends on the Type value set for the reporting recipient. See menu “9.1.n.4.1 Type” above for parameters description.

9.2 Event options

```
1>CS mapping  
2 Voice mapping
```

The Event options menu contains event options.

See “Reporting principles” on page 84 for more details on event reporting.

9.2.1 CS mapping

```
01>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 A “Advisor Advanced events” on page 311.

9.2.2 Voice mapping

```
01>AN Msg number
    0
```

The Voice mapping menu allows you to assign a particular voice message (0 to 14) to each system event. 0 means that no message is assigned.

The list of events is shown in Appendix A “Advisor Advanced events” on page 311.

9.2.3 Delayed events

```
0>Delay timer
    0
```

The Delayed events menu allows you to set a delay for particular 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 particular events. If the option is On, the delay is applied.

```
01>AN Delayed
    Off
```

For the list of events, see Appendix A “Advisor Advanced events” on page 311.

9.3 Path options

```
1>PSTN
  4 IP
```

The Path options menu allows you to configure options for available transmission paths.

9.3.n Select path

```
1>Path name
    PSTN
```

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:

- PSTN
- ISDN
- GSM
- TDA74xx

Note: Particular options in this menu differ for specific transmission paths. For specific options, see:

- “PSTN specific options” on page 269
- “ISDN specific options” on page 270
- “IP specific options” on page 270
- “GSM/SMS/GPRS specific options” on page 273

Common options

9.3.n.1 Path name

```
1 Path name
   >PSTN<
```

Use the path name screen to enter or change the transmission path name. The name can consist of up to 16 characters.

9.3.n.2 Line fault

```
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.

9.3.n.4 Expander menu

```
4 Expander menu
   >>>
```

Particular diallers have their internal menus. Enter Expander menu to set internal dialler options.

The menu content depends on the equipment.

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.

9.3.n.8.1 Ring count

```
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.

9.3.n.8.2 Omit 1st call

```
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 “9.3.n.8.1 Ring count” on page 268, and answers immediately to the second incoming call received within 30 seconds after the first one.

If set to No, the panel answers after a number of incoming rings programmed in “9.3.n.8.1 Ring count”.

9.3.n.9 Encryption

```
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 “9.4.3 Encryption key” on page 284.

Note: IP connection is always encrypted. USB communication does not use encryption.

PSTN specific options

9.3.n.3 Line fault delay

```
3 LF delay
   >0<
```

Line fault delay defines the time period after which the PSTN line 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.

9.3.n.4 Transm path

```
3 Transm path
   PSTN
```

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

9.3.n.5 Dial tone

```
5 Dial tone
   >Default<
```

The Dial tone menu allows you to choose an appropriate dial tone standard for PSTN paths.

One of the following dial tone options can be selected:

- None
- Default (CTR21)
- UK
- Other (Netherlands)

9.3.n.6 Dialing

```
6 Dialing
  >DTMF<
```

The Dialing menu allows you to select the PSTN dial mode: pulse or tone (DTMF).

ISDN specific options

9.3.n.6 Point to Point

```
6 Point to Point
  >No<
```

The option must be set to Yes if the ISDN dialler uses point-to-point connection, otherwise it should be set to No.

Contact your ISDN provider for details on the service.

9.3.n.7 MSN

```
7 MSN
```

The MSN option lets you enter the ISDN MSN number.

IP specific options

9.3.n.3 Transm path

```
3 Transm path
  ETHERNET
```

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

9.3.n.4 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.

9.3.n.4.1 IP config

```
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.

9.3.n.4.2 IP address

```
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 “9.3.n.4.1 IP config” menu above, this value shows the dynamic IP address that is assigned by the DHCP server and cannot be changed.

9.3.n.4.3 Subnet mask

```
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 “9.3.n.4.1 IP config” menu above, this value shows the dynamic IP subnet mask that cannot be changed.

9.3.n.4.4 Gateway

```
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 “9.3.n.4.1 IP config” menu above, this value shows the dynamic gateway address that cannot be changed.

9.3.n.5 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.

9.3.n.5.1 DNS config

```
1 DNS config
   >Static<
```

If the IP configuration in menu “9.3.n.4 IP config” on page 270 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.

9.3.n.5.2 DNS server

```
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 “9.3.n.4.1 IP config” menu on page 271.

9.3.n.6 NTP config

```
6 NTP config
>Static<
```

The NTP config menu is used to configure the NTP (Network Time Protocol) server.

The following options are configurable in this menu.

9.3.n.6.1 NTP config

```
1 NTP config
>Static<
```

If the IP configuration in menu “9.3.n.4 IP config” on page 270 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.

9.3.n.6.2 NTP server

```
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 “9.3.n.4.1 IP config” menu on page 271.

9.3.n.7 Firewall

```
1>Firewall
On
```

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 “9.4.1.n.4 Destination/IP” on page 285.

The following options are configurable in this menu.

9.3.n.7.1 Firewall

```
1 Firewall
   >On<
```

Use the Firewall menu to enable (On) or disable (Off) the built-in firewall.

9.3.n.7.2 Reply on PING

```
2 Reply on PING
   >No<
```

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.

9.3.n.8 Link speed

```
8 Link speed
   >10 MB<
```

The Link speed menu allows you to choose the Ethernet link speed. The allowed options are:

- 10 MB
- 100 NB
- Auto

9.3.n.9 MAC address

```
9>MAC address
   0051DB3D7E73
```

MAC address of the Ethernet controller is a read-only value.

9.3.n.10 Max Pics 24h

```
10 Max Pics 24h
   > <
```

You can limit the maximum number of pictures sent to users via GPRS or 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.

GSM/SMS/GPRS specific options

9.3.n.4 Transm path

```
4 Transm path
   ETHERNET
```

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

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 “9.3.n.6.1 SMS Center num” on page 278 for more details.

9.3.n.5.1 SIM card PIN

```
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 “1.2.8.1 PIN status” on page 133 for more detailed explanation for these messages.

This menu does not have any functionality if the PIN is not required for this SIM card.

9.3.n.5.2 Networks

```
1>Net.selection
    Automatic
```

The Networks menu lets you configure the GSM network settings.

9.3.n.5.2.1 Net.selection

```
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.

9.3.n.5.2.2 Sel.net.only

```
2 Sel.net.only
    >No<
```

If the Selected network only option is set to Yes, only the network selected in the “9.3.n.5.2.1 Net.selection” above is allowed for the communication. Otherwise,

the system automatically selects another network, if the configured network is unavailable.

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]”.

9.3.n.5.2.3.0 Rescan nets

```
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.

9.3.n.5.2.3.m Select a network

```
1>Network name
MyGSM
```

Select a network to see more options.

9.3.n.5.2.3.m.1 Network name

```
1>Network name
MyGSM
```

The Network name is the name of the GSM network. Refer to “1.2.8.6 Network name” on page 134 for more details.

9.3.n.5.2.3.m.2 Network code

```
2>Network code
21999
```

The Network code is the unique code of the GSM network. Refer to “1.2.8.7 Network code” on page 134 for more details.

9.3.n.5.2.3.m.3 Availability

```
3>Availability
   Connected
```

The Availability values are described in “9.3.n.5.2.3 Net.scanning” on page 275.

9.3.n.5.2.3.m.4 RSSI

```
4>RSSI
   -35 dBm [IIII ]
```

The Received Signal Strength Indication (RSSI) value is diagnostic information. See also “1.2.8.8 RSSI” on page 134.

9.3.n.5.2.3.m.5 Use this net.

```
5>Use this net.
   -----
```

Enter Use this network menu to connect the selected GSM network. This replaces the network selected in “9.3.n.5.2.1 Net.selection” on page 274.

9.3.n.5.3 Credit

```
1>Check now
   >>>
```

The Credit menu lets you configure and perform GSM account checking.

9.3.n.5.3.1 Check now

```
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.

9.3.n.5.3.2 Check mode

```
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 “9.3.n.5.3.3 Check number” on page 277.

9.3.n.5.3.3 Check number

```
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 “9.3.n.5.3.2 Check mode” on page 276.

9.3.n.5.3.4 Request code

```
4 Request code
  > <
```

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.

9.3.n.5.3.5 Check period

```
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 “9.3.n.6.2 SMS forwarding” on page 278 is enabled, otherwise the account state response will be lost.

9.3.n.5.3.6 Check time

```
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 “9.3.n.5.3.5 Check period” above.

9.3.n.5.4 Jamm detection

```
1>Jamm detection
  Off
```

The menu allows you to configure GSM jamming detection parameters.

9.3.n.5.4.1 Jamm detection

```
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 AT57310 GSM dialler with firmware version V01.08 or later.

9.3.n.5.4.2 Jamming threshold

```
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).

9.3.n.6 SMS Setup

```
1>SMS Center num
   None
```

The SMS Setup menu lets you change various SMS settings.

9.3.n.6.1 SMS Center num

```
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.

9.3.n.6.2 SMS forwarding

```
0>Off
-----
```

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 “3.2.n.6 User group options” on page 169)
- Have their phone numbers configured (see “3.1.n.7.1 User phone” on page 166)

9.3.n.6.3 Max Msg 24h

```
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.

9.3.n.6.4 SMS header msg

```
4 SMS header msg
> <
```

The SMS header message identifies the Advisor Advanced 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 “9.1.n.3 Protocol” on page 259

9.3.n.6.5 User PIN req.

```
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 *Advisor Advanced SMS Control Reference Manual* for more information.

9.3.n.6.6 Ext.charset

```
6 Ext.charset
>No<
```

The Extended charset (UCS2) option has an influence on the SMS messages sent by the Advisor Advanced 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.

9.3.n.7 GPRS Setup

```
1 APN
None
```

The GPRS Setup menu lets you change various GPRS settings.

9.3.n.7.1 APN

```
1 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.

9.3.n.7.2 User name

```
2 User name
> <
```

The User name must be specified by the GPRS provider.

9.3.n.7.3 User password

```
3 User pass
> <
```

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.

9.3.n.7.4 IP config

See “9.3.n.4 IP config” on page 270.

9.3.n.7.5 DNS config

See “9.3.n.5 DNS config” on page 271.

9.3.n.7.6 Firewall

See “9.3.n.7 Firewall” on page 272.

9.3.n.7.7 Line fault

```
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.

9.3.n.7.8 Disconn.time

```
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.

9.3.n.7.9 Max Pics 24h

See “9.3.n.10 Max Pics 24h” on page 273.

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.

9.3.n.10.1 MMS Center

```
1 MMS center
> <
```

The MMS center number is the address for the MMS service.

9.3.n.10.2 APN

See “9.3.n.7.1 APN” on page 279 for details.

9.3.n.10.3 User name

See “9.3.n.7.2 User name” on page 280 for details.

9.3.n.10.4 User password

See “9.3.n.7.3 User password” on page 280 for details.

9.3.n.10.5 Proxy

```
5 Proxy
> <
```

Enter the MMS proxy server address.

9.3.n.10.6 Proxy port

```
6 Proxy port
> <
```

Enter the proxy server port number for the proxy server configured in “9.3.n.10.5 Proxy” above.

9.3.n.10.7 Max MMS 24h

```
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.

9.3.n.11 Module info

```
1>Module version
    731000V01
```

The informational screens contain GSM dialer firmware version, modem type, etc.

9.4 PC connection

```
1>Connections
    >>>
```

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.

9.4.1 Connections

```
0>Add PC conn
1 PC conn 1
```

It is possible to define up to 16 different PC connections.

9.4.1.0 Add PC conn

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.

9.4.1.n Select PC connection

Select the connection to configure.

Note: Particular options in this menu differ for specific transmission paths. For specific options, see:

- “PSTN specific options” on page 285
- “IP specific options” on page 285
- “GSM specific options” on page 286

Common options

9.4.1.n.1 Name

```
1 Name
>PC conn 1 <
```

The connection name can consist of up to 16 characters.

9.4.1.n.2 Transm path

```
2>Transm path
PSTN
```

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. The text in square brackets identifies the transmission path that the option is applicable to.

9.4.1.n.4 Phone number

```
4 Phone number
> <
```

The Phone number menu defines the Up/Download telephone number 1. The phone number can contain up to 20 digits. The following special characters are available:

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

Note: To enter a character, press the corresponding key twice.

9.4.1.n.5 Retry limit

```
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.

9.4.1.n.6 Delete PC conn

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.

The display shows:

```
6 Delete PC conn
>Cancel<
```

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.

9.4.2 PC callback

```
1>Primary
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 is only possible for modem connection.

9.4.2.1 Primary

9.4.2.2 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.

```
0>Off
1 PC conn 1
```

Upon a callback request Advisor Advanced attempts to connect to the primary callback destination. The number of attempts is defined in “9.4.1.n.5 Retry limit” on page 283. After the retry limit exceeds, the panel connects to the backup callback destination.

9.4.3 Encryption key 1

9.4.4 Encryption key 2

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

The Advisor Advanced 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 000000000000000000000000 (24 zeroes).

Note: A PC connection via IP transmission path is always encrypted. An encryption of PSTN and ISDN connection is optional. It is set via menu “9.3.n.9 Encryption” on page 269. USB communication is never encrypted.

9.4.5 Listening port

```
4 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 “9.3.n.7.8 Disconn.time” on page 280 for more details.

9.4.6 Panel ID

```
6 Panel ID
  > <
```

Use Panel ID to distinguish between a few panels when using them in one facility with Downloader connection.

PSTN specific options

9.4.1.n.3 Modem protocol

```
3 Modem protocol
  >V.21<
```

The Modem protocol option allows you to select one of the following modem protocols: Bell-103, V.21, V.22 or V.22bis.

IP specific options

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.

9.4.1.n.4.1 Dest. name

```
1 Dest name/IP
  > <
```

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 111.

9.4.1.n.4.2 Destination port

```
2 Dest port
  > <
```

The Destination port defines which IP port is used to establish the selected PC connection.

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 a number of packets sent and received.

GSM specific options

9.4.1.n.3 Conn. type

```
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.

Chapter 6

Software

Summary

The chapter describes how to connect Advisor Advanced control panel to PC for programming and firmware upgrading.

Content

Programming Advisor Advanced via configuration software 288

Upgrading Advisor Advanced firmware 290

 Installing AAFIash on the PC 290

 Connecting Advisor Advanced to the PC 290

 Archiving current firmware and settings 291

 Upgrading Advisor Advanced firmware 291

 Upgrading bootloader 292

Programming Advisor Advanced via configuration software

There are different PC configuration and administration tools that are designed to make Advisor Advanced 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 Advisor Advanced 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 Advisor Advanced 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 Advisor Advanced 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 “9.4.3 Encryption key 1” on page 284 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 “8.2.1 User code required” is On (see page 237). In this case the following steps must be performed:

1. The authorized user enters the User menu and activates “Service In” option. See *Advisor Advanced 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 “8.1.3.6 Installer in-time” described on page 235) expires, a new user authorization is required.

Upgrading Advisor Advanced firmware

The Advisor Advanced 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.

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 Advisor Advanced to the PC

To connect the panel to the PC for an upgrade:

1. Disconnect the mains power supply from the panel.
2. Open the panel housing and disconnect the battery.
3. Put on the T2 jumper.
4. Reconnect mains supply.
RX and TX diodes must start blinking. If they don't, disconnect the power and then reconnect again.
5. Plug a USB cable plug into the Advisor Advanced PCB main board.
See "General installation information" on page 8 for more information.

After that, the USB LED turns on, the TX LED turns off, and the RX LED continues blinking.

If this is the first DFU connection, the system prompts you to find Advisor Advanced USB DFU drivers to install. Choose the driver located in the subdirectory “Driver” or the AAFflash 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 Advisor Advanced panel, run AAFflash 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 Advisor Advanced firmware

To upgrade the panel firmware:

1. While connected to the Advisor Advanced panel, run AAFflash 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.

After the firmware is upgraded, the TX LED blinks to indicate that the panel is ready to leave the firmware upgrade mode.

Caution: If firmware upgrade procedure fails, restore the latest archived firmware.

4. Disconnect the USB cable from the panel main board, and then remove the T2 jumper.

The TX LED stops blinking. The panel is automatically restarted.

Upgrading bootloader

Particular 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 Advisor Advanced 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 290.

2. Run the panel in DFU mode.

- a. Disconnect the mains power and batteries from the panel.

- b. Put in the T2 jumper and plug a mini-B USB cable into the panel PCB.

- c. Reconnect mains power supply.

The panel is running in DFU mode now, RX LED is blinking.

If RX and TX LEDs are blinking alternately, the connected PC does not have the required driver installed. In this case, the system prompts you to find Advisor Advanced 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. *Remove T2 jumper 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. Insert T2 jumper 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 Advisor Advanced firmware” on page 291.

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 296

Device troubleshooting 297

 Advisor Advanced control panel 297

 LCD keypads 298

 Remote expanders — Models ATS1201, ATS1210, ATS1211, ATS1220 298

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:

1. Remove mains and battery power from the panel.
2. Set jumper T1.
3. Apply power to the panel.

During the next 3 minutes, it will be possible to access the installer menu using the default code. No user is required to provide access to installer programming mode.

This procedure is logged.

Note: The recovery procedure is not allowed if the “8.2.3 Engineer lockout” option is set to Yes.

Caution: After the recovery procedure keypad 1 access limitations are reset, which allows you to view and control all areas from this keypad. See “2.2.1.n.3.3 View areas” on page 144 and “2.2.1.n.3.5 Control areas” on page 145 for more details.

Device troubleshooting

Advisor Advanced 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.
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 22.
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 22.
The panel is not reporting to the central station	The telephone line connections may be wired incorrectly. See "Cabling" on page 22. The central station receiver does not support the programmed protocol. The account number in "9.1.n.5 Accounts" on page 259 may be programmed incorrectly. The phone number for the central station receiver is wrong. No central station is programmed to report the event. See "9.1 Central station" on page 258. The zone is not programmed to be reported. See "4.1.n.6.24 CS report" on page 177".

LCD keypads

Condition	Possible cause
All the LEDs on the keypad are flashing	<p>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).</p> <p>The system data bus line may be connected incorrectly.</p> <p>The keypad is not being polled (it may not have been included in keypads to be polled when programming keypads).</p>
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 22.
An error is indicated when a code is entered on the keypad (seven beeps)	<p>An invalid PIN may have been used.</p> <p>The keypad may not have been programmed with an alarm group.</p> <p>The alarm group of the PIN may not permit access at this keypad.</p>

Remote expanders — Models ATS1201, ATS1210, ATS1211, ATS1220

Condition	Possible cause
The Tx LED on the expander is not flashing	<p>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).</p> <p>The system data bus cable may be connected incorrectly.</p> <p>The expander is not programmed to be polled.</p>
Tx and Rx LEDs are not operating	<p>No power or low power.</p> <p>The system data bus cable may be connected incorrectly or the power supply is faulty (mains or battery).</p>
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 22.

Condition	Possible cause																				
Some or all expander zones are permanently in tamper (or permanently in alarm if “8.6.1 Input mode” on page 248 is set to Single NO or Single NC).	<p>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 30.</p> <p>The end-of-line resistors are wrong or the wrong resistor value is programmed in “8.6.2 EOL” (see page 248).</p> <p>There is a problem with wiring the zones. To check the voltage or resistor values, see “Zone connection” on page 23.</p> <p>The ATS1202 expansion modules (if fitted) have the DIP switches incorrectly set.</p> <table data-bbox="756 645 1278 869"> <thead> <tr> <th data-bbox="756 645 986 674">Expansion module:</th> <th data-bbox="1043 645 1082 674">1st</th> <th data-bbox="1139 645 1177 674">2nd</th> <th data-bbox="1235 645 1273 674">3rd</th> </tr> </thead> <tbody> <tr> <td data-bbox="756 689 906 719">DIP switch 1</td> <td data-bbox="1043 689 1082 719">On</td> <td data-bbox="1139 689 1177 719">Off</td> <td data-bbox="1235 689 1273 719">Off</td> </tr> <tr> <td data-bbox="756 734 906 763">DIP switch 2</td> <td data-bbox="1043 734 1082 763">Off</td> <td data-bbox="1139 734 1177 763">On</td> <td data-bbox="1235 734 1273 763">Off</td> </tr> <tr> <td data-bbox="756 779 906 808">DIP switch 3</td> <td data-bbox="1043 779 1082 808">Off</td> <td data-bbox="1139 779 1177 808">Off</td> <td data-bbox="1235 779 1273 808">On</td> </tr> <tr> <td data-bbox="756 824 906 853">DIP switch 4</td> <td colspan="3" data-bbox="1043 824 1145 853">not used</td> </tr> </tbody> </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.																				

Chapter 8

Regulations

Summary

These pages describe settings and actions required by particular regulations and norms.

Content

Options affected by EN 50131 regulations	302
EN 50131 Grade 2	302
EN 50131 Grade 3	303
EN 50136 policy	305
Transmitter polling interval requirements	305
EN 50131 Grade 3 certified components	306
EN 50131 compliance precautions	307
Options affected by other regulations	308
ACPO policy	308
INCERT policy	308
SES policy	308
SBSC policy	309

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.

- 1.2.6.n.3 Period, see “Transmitter polling interval requirements” on page 305.
- 2.2.1.n.3.3 View areas and 2.2.1.n.3.5 Control areas settings are identical
- 2.2.1.n.3.10 Buzzer silent, never
- 2.2.1.n.3.11 Quick set, off
- 2.2.1.n.3.12 Function keys, all set to None
- 2.2.1.n.3.17 ACK on keypad, set to None for non-LCD keypads
- 3.1.n.7.3 SMS control, disabled for all users
- 3.2.n.6 User group options, 25. No OP/CL reports option set to No
- 4.1.n.6.1 Inhibit, set to No for all zones with type 5. Panic, 6. 24H
- 4.1.n.6.6 Swinger shunt, set to Yes for all zones
- 4.1.n.6.26 ACK on keypad, set to None for all zones with type 9. Keypad
- 4.2.n.3 Entry time, 45 s maximum
- 4.2.n.5.1 Entry alarms, Instant
- 7.2.n.2 Active, set to No for all schedules.
- 8.1.2.1 Activation, external siren 90 to 900 s
- 8.1.2.2 Delay time, external siren 600 s maximum
- 8.1.3.1 Armed display, 30 s maximum
- 8.1.3.4 Mains reporting delay, 3600 s maximum
- 8.2.1 User code required, enabled
- 8.3.1 Armed display, always
- 8.3.3 Alarm list, disabled
- 8.4.1 RTS options, all enabled except zone technical alarm, which is optional
- 8.4.2 Inhibit includes, all allowed except engineer reset, which must be disabled
- 8.4.6 Pending alarms, enabled
- 8.6.4 Swinger shunt ≥ 3
- 8.6.5 Report restore, on ACK
- 8.7.8.1 Remote config, No
- 9.3.n.2 Line fault, enabled per path used
- 9.3.n.3 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:

- Advisor Advanced series control panel
- AT51238 Advanced Wireless DGP
- TX-2344-03-1 Wireless PIR Camera
- AT57310 GSM/GPRS Module

These PIR camera settings have no influence on EN 50131 compliance:

- 2.2.2.n.4.9.1.1.2 Frame rate for all event types
- 2.2.2.n.4.9.1.1.3 Pic resolution for all event types
- 2.2.2.n.4.9.3 Pic auto deletion
- 4.5 Cameras
- 9.1.n.4.5 Vid dest port
- 9.3.n.10 Max Pics 24h, 9.3.n.7.9 Max Pics 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 302).
- PIN length should be 6 digits minimum. See also “8.7.4 PIN length”.
- 3.2.n.6 User group options, set (6) Isolate, (22) SMS reporting, (23) SMS control to No for all user groups except Installer.
- 4.1.n.6.7 Anti mask, set to Yes for all I&HAS movement detectors
- 8.1.3.1 Armed display, set to 00’00
- 8.3.5 View EE timer, set to Off
- 8.4.1 RTS options, set Zone masking condition to Yes
- 8.4.2 Inhibit includes, set Zone masking condition to Access Level 2
- Battery test should be performed daily. See “1.2.9 Battery test” on page 135 for details.

The following features are not allowed (not evaluated):

- Keyswitch zone types to set and unset the system. See “Zone types” on page 45.
- Presetting indication and any automatic override of set prevention.

Refer to Table 29 below for all supported options for notification requirements.

Table 29: EN 50131-1:2006 options

Notification equipment (Alarm reporting)	Grade 3 options			
	A	B	C	D
Remotely powered audible WD	2	Optional	Optional	Optional
Self-powered audible WD	Optional	1	Optional	Optional
Main ATS [1]	ATS 4	ATS 4	ATS 4	ATS 5
Additional ATS [1]	Optional	Optional	ATS 3	Optional
ATS [2]	SP3	SP3	DP3 [3]	SP4

[1] Requirement according to EN 50136:2010

[2] Requirement according to EN 50136:2012

[3] Primary Path — SP4, backup path — SP2

Legend:

- ATS: Alarm transmission system
- SP: Single path alarm transmission system
- DP: Dual path alarm transmission system

The key variations of cards and keys are the following:

Both

- ATS1471 (1 pc.) and ATS1477 (10 pcs.) tags as well as
- ATS1475 (10 pcs.) card badges

have a number of key variations of 67 million minimum.

Both 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) is able to 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.

- 2.2.1.n.3.7.1 Card&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.
- 2.2.1.n.3.7.3 1 x set/unset: Off
- 2.2.1.n.3.7.4 3 x badge set: Set
- 2.2.1.n.3.11 Quick set: Off
- 4.1.n.6.18 Key unset: Off

- 8.4.4 Forced set: Off
- 8.4.7 AS fault retry: 15 minutes
- 8.4.8 AS user retry: Disable

See also the appropriate RAS manual for more details.

EN 50136 policy

Required settings:

- “9.1.n.7 Retry count”: 1
- “9.1.n.8.3.2 Heartbeat time”: According Table 30 below.
- “9.1.n.8.3.5 Freq. HB time”: According Table 30 below.
- “9.3.n.7.1 Firewall”: Yes
- “9.3.n.7.2 Reply on PING”: No
- “9.3.n.7.6.1 Firewall”: Yes
- “9.3.n.7.6.2 Reply on PING”: No
- “9.3.n.9 Encryption”: Yes
- “9.4.3 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 (ATS). Table 30 below lists all required settings for the appropriate standards and diallers.

Table 30: Transmitter polling settings

Standard and category	Required polling interval	Comm. path and dialler	Option	Required value
EN 50136:2012				
SP2	25 h	PSTN via ATS7700 and GPRS (backup) via ATS7310	1.2.6.n.3 Period	24
SP3	30 min	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	00:29'00
SP4	3 min	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	00:02'30
SP5	90 s	IP built-in	9.1.n.8.3.2 Heartbeat time	00:01'00
SP6	20 s	IP built-in	9.1.n.8.3.2 Heartbeat time	00:00'10
EN 50136:2010				
ATS2 (T2), ATS3 (T2)	25 h	PSTN via ATS7700 and GPRS (backup) via ATS7310	1.2.6.n.3 Period	24
ATS4 (T3)	300 min	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	04:55'00

Standard and category	Required polling interval	Comm. path and dialler	Option	Required value
ATS5 (T4)	180 s	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	00:02'30
ATS6 (T6)	20 s	IP built-in	9.1.n.8.3.2 Heartbeat time	00:00'10
LPS1277: Issue 3.0				
ATS4Plus	10 min	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	00:09'00

EN 50131 Grade 3 certified components

The Advisor Advanced EN 50131 Grade 3 system exists out the following components.

Intrusion control panels

- ATS3500A(-IP): Control panel

Note: In case of ATS1500A(-IP) panel, the system with peripherals listed below will be Grade 2 certified.

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).

- ATS1135: LCD keypad
- ATS1190/1192: Smart Card reader
- ATS1151/ATS1156: Keypad

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
- ATS1203E: 8 to 32 zone DGP expander with 3 A PSU, medium 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.

- AT57310: GSM communication device
- AT57440: IP/GPRS alarm dialer
- AT57700: PSTN interface board

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” below.

EN 50131 compliance precautions

Installation

In order 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 306 for more details.

Programming

Make sure that all system settings are in line with regulatory compliance guidelines. See “EN 50131 Grade 3” on page 303 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 306.
- All settings are done according to “EN 50131 Grade 3” on page 303.

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

ACPO policy

Required settings are all EN 50131 Grade 2 settings with the following modifications:

- 4.2.n.5.1 Entry alarms, Delayed
- 8.2.4 Engineer reset, tamper enabled
- 8.7.6 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

Required settings:

- Isolate for End Users option disabled in 3.2.n.6 User group options
- Full Set/Part Set/Unset/Forced Set for Installer disabled in 3.2.n.6 User group options
- 8.2.4 Engineer reset, tamper enabled
- 8.4.1 RTS options, all enabled except FTC, Pending Alarms, and Zone technical alarm, that are optional
- RTS for Battery Fault enabled in 8.4.1 RTS options
- Inhibit for Battery Fault disabled in 8.4.2 Inhibit includes
- PIN length should be 6 digits minimum. See also “8.7.4 PIN length”.

SES policy

Depending on the SES default chosen, the following SES settings are required on top of EN 50131 Grade 2 / Grade 3.

- Take care that a proper dedicated panic button is used (which cannot be pushed by accident).
- Automatic unsetting is not allowed.

- For SES Grade 3 is not allowed to program GPRS communication as primary CS, it is only allowed in Grade 2.
- The table below indicates the required polling intervals for SES Grade 2 and Grade 3.

		Primary CS (IP)				
		AÜA-B25 25 h	AÜA-B5 5 h	AÜA-S180 180 sec	AÜA-S20 20 sec	
Back-up CS (GPRS)	AÜA-B25	25 h	2	2, 3	2, 3	2, 3
	AÜA-B5	5 h	2	2, 3	2, 3	2, 3

* 2, 3: EN-CH Grade of the system

- The following options must be set:

Standard and category	Required polling interval	Comm. path and dialler	Option	Required value
SES CHD.07 (V3 / 01.01.2011)				
AÜA-B25	25 h	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	24
AÜA-B5	5 h	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	4
AÜA-S180	180 s	IP built-in, or GPRS via ATS7310	9.1.n.8.3.2 Heartbeat time	00:02'30
AÜA-S20	20 s	IP built-in	9.1.n.8.3.2 Heartbeat time	00:00'10

SBSC policy

Larmklass 1

Required settings are all EN 50131 Grade 2 settings with the following modifications:

- 4.2.n.5.1 Entry alarms: Instant
- 8.7.6.9 Reporting delayed: No

See also "EN 50131 Grade 2" on page 302.

Larmklass 2

Required settings are all EN 50131 Grade 3 settings with the following modifications:

- 4.2.n.5.1 Entry alarms: Instant
- 8.7.6.9 Reporting delayed: No

See also "EN 50131 Grade 3" on page 303.

Appendix A

Advisor Advanced events

For Advisor Advanced system events, see Table 31 below. For access control events, used to program door controllers, see Table 32 on page 322.

Table 31: Advisor Advanced events

Group	Event	#	Event description	Notes
Zone	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 short
	SVLONG	8	Zone supervision long	Zone in short supervision state long
	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	

Group	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
Group	Event	#	Event description	Notes
Area	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

Group	Event	#	Event description	Notes
	FTCPANIC	23	Panic and FTC	A panic alarm active while FTC present
	MEDICAL	24	Medical alarm	A medical alarm active
	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

Group	Event	#	Event description	Notes
	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
	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

Group	Event	#	Event description	Notes
	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.
	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
	UNSETEXTTIME	88	ATM extended unset time	Extended ATM unset time is active
	AREA DSHUNT	89	Door shunt	A zone in the area is shunted

Group	Event	#	Event description	Notes
	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	

Group	Event	#	Event description	Notes
Keypad	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	Badged card	A card is badged 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	Event	#	Event description	Notes
Expander	OFFLINE	1	Expander is offline	Active if device is offline
	MAINSFAULT	2	Mains fail	

Group	Event	#	Event description	Notes
	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	

Group	Event	#	Event description	Notes
Panel	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
	LFPSTN	7	PSTN line fault	PSTN line fault detected
	LFISDN	8	ISDN line fault	ISDN line fault detected
	LFGSM	9	GSM line fault	GSM line fault detected
	FTC	10	Failed To Communicate	Failed to deliver an alarm message
	MIFFAULT	11	Line fault PSTN	MI Bus communication fault
	MIFISDN	12	Line fault ISDN	ISDN dialler fault
	MIFGSM	13	Line fault GSM	GSM dialler fault
	MIFVOICE	14	Failed To Communicate	Voice module fault
	NTPFAULT	15	NTP server connection fault	NTP server connection fault
	LFETH	16	Ethernet line fault	Ethernet connection fault
	LFIP	17	IP fault	Ethernet IP is not configured
	LFGPRS	18	GPRS line fault	GPRS connection fault
	LFIPGPRS	19	GPRS IP fault	GPRS IP is not configured
	LFTDA	20	TDA line fault	TDA module line fault
	LFTDAGPRS	21	TDA GPRS fault	TDA module line fault (GPRS)
	LFTDAETH	22	TDA ETH fault	TDA module line fault (ETH)
	MIFTDA	23	TDA MI fault	Panel MI device fault (TDA)

Group	Event	#	Event description	Notes
	GSMJAMMING	24	GSM jamming	GSM jamming detected
	POWER UNIT FA	25	Panel PSU fail	
	BTESTACTV	26	Panel battery test active	
	BTESTFAIL	27	Panel battery test fail	
	DLRBATTFault	28	Dialer battery fault	
	MODRESET	29	Dialer module reset	
	DEVTAMPERINH	30	Panel tamper inhibited	
	SIRTAMPERINH	31	Siren tamper inhibited	

Group	Event	#	Event description	Notes
User	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	Event	#	Event description	Notes
Output	ACTIVE	1	Output active	Specified output activates
	ON	2	Output on	Physical output activates
	FORCED	3	Door forced output	

Group	Event	#	Event description	Notes
Filter	ACTIVE	1	Condition true	The selected filter condition is true / valid.

Group	Event	#	Event description	Notes
User group	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	Event	#	Event description	Notes
System	ALLSET	1	All set	All areas in the system are set
	AUTOANS	2	Auto Answer	Auto answer procedure started (1 min)
	RCONNECTV	3	Remote connection	Remote connection active
	RCONNFAIL	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)
	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	

Group	Event	#	Event description	Notes
Door	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
	TUNLOCKED	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

Group	Event	#	Event description	Notes
	FORCED	7	Door forced	Door zone has been activated without unlocking
	DOTL	8	Door DOTL	Door zone active after shunt time
	SHUNTING	9	Door shunting	Door zone has been shunted
	READER FAULT	10	Door reader fault	Door reader communication problem
	READER TA	11	Door reader tamper	Door reader tamper is active
	UNSECURED	12	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	13	Door input	Door zone is in active/tamper state

Group	Event	#	Event description	Notes
CS	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	Event	#	Event description	Notes
Trigger	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 (ATS1235)	7	Trigger is activated by a fob	

Group	Event	#	Event description	Notes
Calendar	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

Group	Event	#	Event description	Notes
	Thursday	6	Thursday	Active on Thursdays
	Friday	7	Friday	Active on Fridays
	Saturday	8	Saturday	Active on Saturdays
	Sunday	9	Sunday	Active on Sundays

Group	Event	#	Event description	Notes
Fob ATS1235+	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	Event	#	Event description	Notes
Camera	Pic captured	1	Picture has been taken	Active for 3 seconds
	Pic limit exc	2	Picture limit has been exceeded	

Group	Event	#	Event description	Notes
Area group	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

Group	Event	#	Event description	Notes
	ALARM	7	An alarm state	At least one area is in alarm
	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	Event	#	Event description	Notes
Schedule	SCH ACTIVE	1	Schedule active	

Group	Event	#	Event description	Notes
Special day	SP DAY ACTIVE	1	Special day is active	

Group	Event	#	Event description	Notes
Reader	OFFLINE	1	Reader is offline	
	TAMPER	2	Reader tamper	

Table 32: Door controller events

Group	Event	#	Event description	Notes
Door	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
	2 card outside	11		Two Card access is required at the "OUT" reader

Group	Event	#	Event description	Notes
	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	Event	#	Event description	Notes
Door access	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 badged once
	Granted 2badge	7		Door access has been granted when badged twice
	Granted 3badge	8		Door access has been granted when badged 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.

Group	Event	#	Event description	Notes
	Anti-psbck dis	13	Anti-passback disable	Disable anti-passback for selected door

Group	Event	#	Event description	Notes
Region	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	Event	#	Event description	Notes
Faults	D.reader fault	1	Door reader fault	
	D.lock fault	2	Door lock fault	
	RAS offline	3		RAS on door controller local databus is offline (16 events, 1 per RAS address)
	DGP offline	4		DGP on ATS1260 local databus 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 fit	7	Door controller fuse fail	Fuse Fail condition exists on the door controller
	DGP siren fit	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 Advisor Master

Group	Event	#	Event description	Notes
Other	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

Advisor Advanced reporting codes

Table 33 below shows descriptions of SIA, CID, and VdS reporting codes used in Advisor Advanced.

Table 34 on page 332 lists allowed values for the appropriate reporting codes.

Table 33: SIA, CID, and VdS reporting code descriptions

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
1.	AN	0xB0	R393	Detector dirty restore		Low
2.	AR	0xB2	R301	AC restore		Low
3.	AS	0x30	E393	Detector dirty		Low
4.	AT	0x32	E301	AC trouble		Medium
5.	BA	0x22	E130	Burglary alarm	Alarm / input in mask / trouble when set	Medium
6.	BB	0x51	E570	Burglary bypass	Alarm inhibit	Low
7.	BC	0x52	E406	Burglary cancel	Cancel alarm by user / key / remotely	Low
8.	BJ	0xB0	R381	Detector supervision restore		Low
9.	BR	0xA2	R130	Burglary restore		Low
10.	BT	0x30	E380	Burglary trouble	Input in mask / trouble when unset	Low
11.	BU	0xD1	R570	Burglary unbyypass	Alarm uninhibit	Low
12.	BV	0x00	E139	Alarm confirm	ACPO	Medium
13.	BW	0x80	R139	Restore confirmed alarm	ACPO	Low
14.	BZ	0x30	E381	Detector supervision		Low
15.	CF	0x51	E408	Forced closing	Set by user / by key	Low
16.	CG	0x62	E456	Part set	Part set by user / by key / remotely	Low

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
17.	CL	0x61	R401	Closing normal	Set by user	Low
			R407	Closing normal	Set remotely	Low
			R409	Closing normal	Set by key	Low
18.	EE	0x30	E374	Exit error	Exit fault	Medium
19.	ER	0xB0	R143	Expansion restore	Expander / keypad trouble restore	Low
			R300	Expansion restore	Expander fuse restore	Low
			R330	Expansion restore	Expander / keypad communication restore	Low
20.	ET	0x30	E143	Expansion trouble	Expander / keypad trouble	Low
			E300	Expansion trouble	Expander fuse failure	Low
			E330	Expansion trouble	Expander / keypad communication fault	Low
21.	FA	0x10	E110	Fire alarm		High
22.	FB	0x51	E570	Fire bypass	Fire inhibit	Low
23.	FJ	0xA3	R373	Fire trouble restore		Low
24.	FR	0x90	R110	Fire restore		Low
25.	FT	0x23	E373	Fire trouble		Low
26.	FU	0xD1	R570	Fire unbyypass	Fire uninhibit	Low
27.	FW	0x30	–	Fire long supervision		Low
28.	HA	0x24	E121	Holdup alarm	Duress	High
29.	HR	0xA4	R121	Holdup restore	Duress restore	Low
30.	JP	0x63	E466	Service in		Low
31.	JR	0xE3	R466	Service out		Low
32.	JT	0x55	E625	Time changed		Low
33.	LB	0x01	E627	Local programming begin		Low
34.	LR	0xBA	R351	Line restore		Low
35.	LS	0x81	R628	Local programming stop		Low
36.	LT	0x3A	E351	Line fault		Low
37.	MA	0x48	E100	Medical alarm		High
38.	MB	0x51	E570	Medical bypass		Low
39.	MJ	0xB0	–	Medical long supervision restore		Low
40.	MR	0xC8	R100	Medical restore		Low
41.	MS	0x30	–	Medical long supervision		Low
42.	MU	0xD1	R570	Medical unbyypass		Low

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
43.	OP	0xE1	E401	Unset normal	Unset by user	Low
			E407	Unset normal	Unset remotely	Low
			E409	Unset normal	Unset by key	Low
44.	OR	0xE1	E406	Unset from alarm	Unset by user / key / remotely	Low
45.	PA	0x21	E120	Panic alarm		High
46.	PB	0x51	E570	Panic bypass		Low
47.	PJ	0xA1	R375	Panic trouble restore		Low
48.	PR	0xA1	R120	Panic restore		Low
49.	PT	0x21	E375	Panic trouble		Low
50.	PU	0xD1	R570	Panic unbypass		Low
51.	RB	0x74	E416	Remote programming begin		Low
52.	RP	—	E602	Automatic test / ring-in test		Low
53.	RR	0x53	E305	Power up	System power-up	Low
54.	RS	0xF4	R416	Remote programming success		Low
55.	RU	0x55	R416	Remote programming fail		Low
56.	RX	—	E601	Manual CS test		Low
57.	TA	0x23	E144	Tamper alarm	Zone tamper	Medium
			E145	Tamper alarm		Medium
			E320	Tamper alarm	Expander siren tamper	Medium
58.	TB	0x51	E570	Tamper bypass		Low
59.	TR	0xA3	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	E370	KeyBox zone active		High
61.	TU	0xD1	R570	Tamper unbypass		Low
62.	UB	0x51	E570	Expander / keypad / zone bypassed	Expander / keypad / zone isolated	Low
63.	UU	0xD1	R570	Expander / keypad / zone unbypassed	Expander / keypad / zone de-isolated	Low
64.	WF	0xF6	E612	Walk test fail		Low
65.	WP	0x76	E611	Walk test pass		Low
66.	XH	0xB0	R344	RF jamming restore		Low
67.	XQ	0x30	E344	RF jamming		Low

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
68.	XR	0xB0	R384	Detector or fob low battery restore		Low
69.	XT	0x30	E384	Detector or fob low battery		Low
70.	YC	0x37	E350	Communications fail	ISDN / GSM / voice / audio device fail	Low
71.	YK	0xB9	R354	Communications restore	ISDN / GSM / voice / audio device restore	Low
72.	YR	0xB3	R302	System battery / fuse restore	Expander / dialler battery / fuse restore	Low
73.	YS	0x39	E354	Communication trouble	Fail To Communicate (FTC)	Low
74.	YT	0x33	E302	System battery / fuse trouble	Expander / dialler battery low / fuse fault	Low
75.	ZA	0x40	E152	Technical alarm — low temperature	Low temperature detector alarm	Medium
76.	ZB	0x51	E570	Technical bypass — low temperature	Low temperature detector inhibit	Low
77.	ZJ	0xB0	R381	Technical long supervision restore — low temperature	Low temperature detector long supervision restore	Low
78.	ZR	0xC0	R152	Technical restore — low temperature	Low temperature detector restore	Low
79.	ZS	0x30	E381	Technical long supervision — low temperature	Low temperature detector long supervision alarm	Low
80.	ZU	0xD1	R570	Technical unbyypass — low temperature	Low temperature detector uninhibit	Low
81.	YA	0x23	E321	Siren fault		Low
82.	YH	0xA3	R321	Siren restore		Low
83.	NC	0x34	E356	CS polling fail	Heartbeat inactive	Low
84.	NR	0xB4	R356	CS polling restore	Heartbeat active	Low
85.	CP	0x61	R403	Auto set	Set by schedule	Low
86.	OA	0xE1	E403	Auto unset	Unset by schedule	Low
87.	OT	0x61	E608	Late close	Postponed auto set	Low
88.	OK	0x61	R608	Early open	Manually unset before auto unset	Low
89.	IA	0x63	E313	Engineer reset request		Low
90.	IR	0xE3	R313	Engineer reset restore		Low
91.	GA	0x73	E151	Technical alarm — gas	Gas detector alarm	High
92.	GR	0xF3	R151	Technical restore — gas	Gas detector restore	High

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
93.	GB	0x51	E570	Technical bypass — gas	Gas detector inhibit	Low
94.	GU	0xD1	R570	Technical unbyypass — gas	Gas detector uninhibit	Low
95.	GS	0x30	E381	Technical long supervision — gas	Gas detector long supervision alarm	Low
96.	GJ	0xB0	R381	Technical long supervision restore — gas	Gas detector long supervision restore	Low
97.	KA	0x12	E158	Technical alarm — high temperature	High temperature detector alarm	Medium
98.	KR	0x92	R158	Technical restore — high temperature	High temperature detector restore	Medium
99.	KB	0x51	E570	Technical bypass — high temperature	High temperature detector inhibit	Low
100.	KU	0xD1	R570	Technical unbyypass — high temperature	High temperature detector uninhibit	Low
101.	KS	0x30	E381	Technical long supervision — high temperature	High temperature detector long supervision alarm	Low
102.	KJ	0xB0	R381	Technical long supervision restore — high temperature	High temperature detector long supervision restore	Low
103.	WA	0x75	E154	Technical alarm — water	Water detector alarm	Medium
104.	WR	0xF5	R154	Technical restore — water	Water detector restore	Medium
105.	WB	0x51	E570	Technical bypass — water	Water detector inhibit	Low
106.	WU	0xD1	R570	Technical unbyypass — water	Water detector uninhibit	Low
107.	WS	0x30	E381	Technical long supervision — water	Water detector long supervision alarm	Low
108.	WJ	0xB0	R381	Technical long supervision restore — water	Water detector long supervision restore	Low
109.	ES	0x23	E145	Tamper alarm	Expander / keypad tamper alarm	Medium
110.	EJ	0xA3	R145	Tamper restore	Expander / keypad tamper restore	Medium
111.	HV	0x21	E129	Hold-up alarm confirm		Medium
112.	HW	0xA1	R129	Confirmed hold-up alarm restore		Low
113.	UA	0x20	E150	Technical zone — general alarm		Medium

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
114.	UR	0xA0	R150	Technical zone — general alarm restore		Medium
115.	TS	0x71	E607	Single zone walk test start	Start of single zone test, also for multiple zones selected	High
116.	TE	0xF1	R607	Single zone walk test end	End of single zone test, also for multiple zones selected	Low
117.	LU	0x55	R628	Local programming fail		Low
118.	YP	0x32	E301	Power Supply Trouble		Low
119.	YQ	0xB2	R301	Power Supply Restored		Low
120.	CI	—	E455	Autoset fail		Low
121.	DD	—	E421	Access denied	Card is unknown	Low

Table 34: SIA and CID reporting code values

#	SIA code	Subevent type and range	CID code	Group range	Point range
1.	AN	Zone (1–128, 257–368)	R393	Area (1–8)	Zone (1–128, 257–368)
2.	AR	Expander (299–307)	R301	System (0)	Expander (65–72)
3.	AS	Zone (1–128, 257–368)	E393	Area (1–8)	Zone (1–128, 257–368)
4.	AT	Expander (299–307)	E301	System (0)	Expander (65–72)
5.	BA	Zone (1–128, 257–368)	E130	Area (1–8)	Zone (1–128, 257–368)
6.	BB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
7.	BC	System (0), User (1–50)	E406	Area (1–8)	User (0), User (1–50)
8.	BJ	Zone (1–128, 257–368)	R381	Area (1–8)	Zone (1–128, 257–368)
9.	BR	Zone (1–128, 257–368)	R130	Area (1–8)	Zone (1–128, 257–368)
10.	BT	Zone (1–128, 257–368)	E380	Area (1–8)	Zone (1–128, 257–368)
11.	BU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
12.	BV	Zone (1–128, 257–368)	E139	Area (1–8)	Zone (1–128, 257–368)
13.	BW	Zone (1–128, 257–368)	R139	Area (1–8)	Zone (1–128, 257–368)
14.	BZ	Zone (1–128, 257–368)	E381	Area (1–8)	Zone (1–128, 257–368)
15.	CF	User (1–50) Zone (1–128, 257–368)	E408	System (0) Area (1–8)	User (1–50) Zone (1–128, 257–368)
16.	CG	User (1–50), Zone (1–128, 257–368)	E456	System (0) Area (1–8)	User (1–50) Zone (1–128, 257–368)
17.	CL	Keypad (401–408)	–	–	–
		User (1–50)	R401	Area (1–8)	User (1–50)
		System (0)	R407	System (0)	
		Zone (1–128, 257–368)	R409	Area (1–8)	Zone (1–128, 257–368)

#	SIA code	Subevent type and range	CID code	Group range	Point range
18.	EE	Zone (1–128, 257–368)	E374	Area (1–8)	Zone (1–128, 257–368)
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)
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)
21.	FA	System (0)	E110	System (0)	Keypad (1–8)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
22.	FB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
23.	FJ	Zone (1–128, 257–368)	R373	Area (1–8)	Zone (1–128, 257–368)
24.	FR	Zone (1–128, 257–368)	R110	Area (1–8)	Zone (1–128, 257–368)
25.	FT	Zone (1–128, 257–368)	E373	Area (1–8)	Zone (1–128, 257–368)
26.	FU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
27.	FW	Zone (1–128, 257–368)	–	–	–
28.	HA	User (1–50)	E121	Area (1–8)	User (1–50)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
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)	E100	System (0)	Keypad (1–8)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
38.	MB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
39.	MJ	Zone (1–128, 257–368)	–	–	–
40.	MR	Zone (1–128, 257–368)	R100	Area (1–8)	Zone (1–128, 257–368)
41.	MS	Zone (1–128, 257–368)	–	–	–
42.	MU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
43.	OP	User (1–50)	E401	Area (1–8)	User (1–50)
		System (0)		E407	System (0)

#	SIA code	Subevent type and range	CID code	Group range	Point range
		Zone (1–128, 257–368)	E409	Area (1–8)	Zone (1–128, 257–368)
44.	OR	User (1–50)	E406	System (0)	User (1–50)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
45.	PA	System (0)	E120	System (0)	Keypad (1–8)
		User (1–50)		Area (1–8)	User (1–50)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
46.	PB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
47.	PJ	Zone (1–128, 257–368)	R375	Area (1–8)	Zone (1–128, 257–368)
48.	PR	Zone (1–128, 257–368)	R120	Area (1–8)	Zone (1–128, 257–368)
49.	PT	Zone (1–128, 257–368)	E375	Area (1–8)	Zone (1–128, 257–368)
50.	PU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
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 (1–128, 257–368)	E144	Area (1–8)	Zone (1–128, 257–368)
		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 (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
59.	TR	Zone (1–128, 257–368)	R144	Area (1–8)	Zone (1–128, 257–368)
		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 (1–128, 257–368)	E370	Area (1–8)	Zone (1–128, 257–368)
61.	TU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
62.	UB	Expander (299–307), keypad (401–408)	E570	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–128, 257–368)	–	–	–
63.	UU	Expander (299–307), keypad (401–408)	R570	System (0)	Expander (65–72), keypad (1–8)
		Zone (1–128, 257–368)	–	–	–
64.	WF	Area (1–8)	E612	Area (1–8)	Area (1–8)
65.	WP	Area (1–8)	E611	Area (1–8)	Area (1–8)
66.	XH	Expander (299–307)	R344	System (0)	Expander (65–72)

#	SIA code	Subevent type and range	CID code	Group range	Point range
		Communication path (0–6) [1]			
67.	XQ	Expander (299–307) Communication path (0–6) [1]	E344	System (0)	Expander (65–72)
68.	XR	Zone (1–128, 257–368) Fob (1–112)	R384	Area (1–8)	Zone (1–128, 257–368)
69.	XT	Zone (1–128, 257–368) Fob (1–112)	E384	Area (1–8)	Zone (1–128, 257–368)
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)
73.	YS	System (0)	E354	System (0)	–
74.	YT	Expander (299–307) Zone (1–128, 257–368)	E302	System (0)	Expander (65–72)
75.	ZA	Zone (1–128, 257–368)	E152	Area (1–8)	Zone (1–128, 257–368)
76.	ZB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
77.	ZJ	Zone (1–128, 257–368)	R381	Area (1–8)	Zone (1–128, 257–368)
78.	ZR	Zone (1–128, 257–368)	R152	Area (1–8)	Zone (1–128, 257–368)
79.	ZS	Zone (1–128, 257–368)	E381	Area (1–8)	Zone (1–128, 257–368)
80.	ZU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
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 (1–128, 257–368)	E151	Area (1–8)	Zone (1–128, 257–368)
92.	GR	Zone (1–128, 257–368)	R151	Area (1–8)	Zone (1–128, 257–368)
93.	GB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
94.	GU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
95.	GS	Zone (1–128, 257–368)	E381	Area (1–8)	Zone (1–128, 257–368)
96.	GJ	Zone (1–128, 257–368)	R381	Area (1–8)	Zone (1–128, 257–368)
97.	WA	Zone (1–128, 257–368)	E154	Area (1–8)	Zone (1–128, 257–368)

#	SIA code	Subevent type and range	CID code	Group range	Point range
98.	WR	Zone (1–128, 257–368)	R154	Area (1–8)	Zone (1–128, 257–368)
99.	WB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
100.	WU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
101.	WS	Zone (1–128, 257–368)	E381	Area (1–8)	Zone (1–128, 257–368)
102.	WJ	Zone (1–128, 257–368)	R381	Area (1–8)	Zone (1–128, 257–368)
103.	KA	Zone (1–128, 257–368)	E158	Area (1–8)	Zone (1–128, 257–368)
104.	KR	Zone (1–128, 257–368)	R158	Area (1–8)	Zone (1–128, 257–368)
105.	KB	Zone (1–128, 257–368)	E570	Area (1–8)	Zone (1–128, 257–368)
106.	KU	Zone (1–128, 257–368)	R570	Area (1–8)	Zone (1–128, 257–368)
107.	KS	Zone (1–128, 257–368)	E381	Area (1–8)	Zone (1–128, 257–368)
108.	KJ	Zone (1–128, 257–368)	R381	Area (1–8)	Zone (1–128, 257–368)
109.	ES	Expander (299–307), keypad (401–408)	R145	System (0)	Expander (65–72), keypad (1–8)
110.	EJ	Expander (299–307), keypad (401–408)	E145	System (0)	Expander (65–72), keypad (1–8)
111.	HV	Zone (1–128, 257–368)	E129	Area (1–8)	Zone (1–128, 257–368)
112.	HW	Zone (1–128, 257–368)	R129	Area (1–8)	Zone (1–128, 257–368)
113.	UA	Zone (1–128, 257–368)	E150	Area (1–8)	Zone (1–128, 257–368)
114.	UR	Zone (1–128, 257–368)	R150	Area (1–8)	Zone (1–128, 257–368)
115.	TS	Area (1–8)	E607	Area (1–8)	Area (1–8)
116.	TE	Area (1–8)	R607	Area (1–8)	Area (1–8)
117.	LU	System (0)	R628	Area (1–8)	Area (1–8)
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 (1–8)	User (1–50)
121.	DD	Keypad (401–408) Card	E421	System (0)	Keypad (1–8)

[1] Communication path is one of the following:

- 1: PSTN
- 2: ISDN
- 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 Advisor Advanced system allows any premises to be divided into different areas having different security requirements. Each area has its zones. Each area is identified by a number or a name. For example, area 1, Workshop, etc.
Armed	See Set.
Armed display	Armed display activates on a keypad after particular idle time. In this mode, the information displayed on LCD and LED is very limited for security reasons. A user intervention is necessary for return to a normal display mode.
Arming station (RAS)	See Keypad.
Autoset	An automatic setting of the premises started by a schedule. See Schedule.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.

Central station	A company that monitors whether an alarm has occurred in a security system. The central station is located away from the premises/area it monitors.
Condition filter	A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.
Control panel	An electronic device that is used to gather all data from zones on the premises. Depending on programming and status of areas, it generates alarm signals. If required, alarms and other events can be reported to the central station.
Cursor	A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.
Detector test	Alarm system function for detectors with a dedicated test input. After the detector test input is activated, the panel checks if proper alarm signal is provided by the detector to the system. This functionality allows testing detectors that are difficult to access.
DGP	Data gathering panel. See Expander.
Dialler	An electronic device that allows the Advisor Advanced system to transmit alarms and other events to a central station. Can also be used to perform up/download.
Disarmed	See Unset.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control of doors. Part of access control features.
Door controller	A 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 Advisor Advanced duress facility allows a signal to be activated (for example, notification to a central station) by the user. This is done by entering a duress digit in conjunction with a PIN.
Engineer	Personnel from an installer that is able to install and service the control panel.
Expander	A device that collects data from other security devices within an area, and transfers it to the Advisor Advanced control panel.
Fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
Fob	A personal wireless device, which is used to perform programmed functions, for example, set or unset premises, open doors.

High Security Region (HSR)	<p>High security regions (HSR) require a certain number of high security users (HSU) present in them to allow any normal users inside. If a high security user leaves the region causing too few HSU present in it, an alarm is raised, preceded by prewarning time.</p> <p>The system does not allow the normal user to stay in the HSR without HSU inside, therefore the last high security user will not be permitted to leave the high security area if there are normal users inside.</p>
High Security User (HSU)	See High Security Region.
History	A list of past alarm and access control events stored in memory that can be viewed on an LCD keypad or through PC connections.
Hold-up	A (silent) alarm that is triggered by a hold-up button. Normally it does not trigger any siren, only sends a message to a central station. Sometimes also referred to as Panic button.
Inhibit	See Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault.
Installer	A company that installs and services security equipment.
Intelligent door	<p>There are two types of doors in the ATS system:</p> <ul style="list-style-type: none"> - Intelligent door: A door controlled by a door controller. This door can be used for advanced access control. - Standard door: A door controlled by the control panel. It only allows basic access control functions.
Inverted walk test	A test based on counting days of inactivity for each zone.
Key switch	A device using a switch to arm or disarm areas. The switch needs a key to switch.
Keypad	A device that is the user control panel for security options for areas or for access points (doors). The keypad can be a console (LCD keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as set/unset, open doors, etc.
LCD	Liquid crystal display. The part of a keypad where messages are displayed.
LED	Light emitting diode. A light indicator on a keypad which conveys a condition. For example, area in alarm, communication fault, etc.
Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault	<p>Describes the condition of a zone.</p> <ul style="list-style-type: none"> • Normal: The zone is <i>not</i> activated. For example, fire exit door closed. • Active: The zone is activated. For example, fire exit door open. • Tamper: The zone is open or short-circuited. Someone may have tried to tamper the security device. • Inhibited: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system for particular time. However, tampers are still monitored. • Isolated: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system permanently. • Masked: Detector is masked. • Fault: Detector reports an internal fault.

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

Special day	A date when alternative time frames in an active schedule are valid.
Tamper	A situation where a zone, a keypad, control panel, expander or associated wiring are tampered with, or accidentally damaged. The Advisor Advanced tamper facility activates a signal when tamper occurs. Tamper alarms from zones are called zone tampers.
Trigger	Triggers are system variables that can be used in condition filters to control outputs remotely. Each trigger has 7 independent flags that can be set or reset. The flags can be controlled by the various means, for example: schedule, SMS command, 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 Advisor Advanced system or change parameters in the system either local or remote.
User	Anybody making use of the Advisor Advanced system. Users are identified to the Advisor Advanced system by a unique number that is associated with the user'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 Advisor Advanced system. Each device is identified by a zone number or a name. For example, zone 14, Fire Exit Door.

Index

A

- access control, **68**
 - reporting, 209
- access denied, 200, 208
- access options, 246
- access zone, 45
- account, 276
- action, **77, 225, 229**
 - creating, 229
 - deleting, 230
 - name, 229
- action list, 77
- actions
 - view, 225
- active walk test, 82, 129
- add
 - action, 229
 - central station, 258
 - door, 196
 - door group, 214
 - event, 218
 - expander, 150
 - filter, 217
 - fob, 94, 191
 - keypad, 143
 - macro, 158
 - output, 219
 - PC connection, 282
 - reader, 160
 - region, 216
 - schedule, 227
 - special day, 230
 - time frame, 228
 - trigger, 223
 - user, 162
 - user group, 168
 - zone, 171
- adding a central station, 258
- adding a door group, 214
- adding a door to the system, 196
- adding a filter to the system, 217
- adding a macro to the system, 158
- adding a PC connection, 282
- adding a region, 216
- adding a schedule, 227
- adding a special day, 230
- adding a time frame, 228
- adding a trigger, 223
- adding a user group, 168
- adding a user to the system, 162
- adding an action, 229
- addressing, 31, 253
- alarm, 126
 - restore, 249
- alarm confirmation, 250
- alarm control, 199
- alarm history, 120
- alarm reporting, 84
- alarm restore, 249
- anti-mask, 175
- anti-passback, **69, 213**
- APN, 279
- area, **50, 173, 185**
 - entry/exit time, 186
 - hierarchy, 50, 189
 - prealarm time, 187
 - selection mode, 165
 - unset delay, 188
 - warning time, 187
- area group, **50, 190**
 - assign areas, 191
 - name, 190
- area indicator, 148
- area modifier, 260, 262
- area selection mode, 165
- area shunt, 203
- area status, 148
- arm, 51
- armed display, 241
 - timeout, 234
- ATM, **103, 256**
 - delay, 256
 - extended unset time, 257
 - unset time, 257
 - unset warning time, 257
- auto configuration, **4, 115**
- auto test, 181
- automatic battery test, **136**
- autoset, **91, 187, 188**

B

battery
 status, 135
 battery replacement, 16, 137
 battery test, **135**
 automatic test, 136
 battery replacement, 137
 duration, 136, 137
 frequency, 136
 bus device, 58
 bus devices, **142**
 buzzer, 255

C

calendar, **77**, 225
 callback, 284
 camera, **98**, **193**
 filter, 194
 isolate, 195
 taking picture, 195
 zone list, 193
 camera diagnostics, 100
 camera range test, 123
 card
 assign, 164
 check, 138
 remove, 164
 card & PIN mode, 145
 card and PIN, 205
 card and PIN timeout, 234
 card format, 205
 card reader, **14**
 card to PIN time, 246
 central station, 258
 backup, 86
 creating, 258
 deleting, 263
 mapping, 84
 primary, 85
 challenge code, 240
 change PIN, 163
 changing a door, 197
 changing a user, 162
 changing user group, 168
 check card, 138
 chime, 175, 254
 CID codes, 327
 classic addressing scheme, 253
 code tamper, 54, 106
 combined reporting, 85
 communication, **258**
 account code, 259
 auto-answer, 284
 callback, 284
 central station, 258
 destination name, 263, 285
 destination port, 264, 286
 Downloader, 288

encryption, 265
 events, 266
 frequent heartbeat, 265
 GSM, 274
 GSM network, 274, 275
 heartbeat, 264
 line number, 265
 PC connection, 282
 phone number, 263
 protocol, 259, 261
 receiver number, 265
 subevents, 261
 test, 83
 Titan, 288
 transmission path, 259, 267
 video port, 265
 condition filter, 74, 231
 condition filters, **217**, 220
 configuration software, 288
 configure
 area, 185
 area group, 190
 condition filter, 217
 door, 197
 event, 158, 218
 expander, 150
 fob, 191
 input, 248
 keypad, 143
 macro, 158
 macro output, 159
 output, 219
 part set, 243
 reader, 160
 user, 162
 zone, 172, 248
 confirmed alarm test, 82, 129
 creating a central station, 258
 creating a door, 196
 creating a door group, 214
 creating a filter, 217
 creating a macro, 158
 creating a PC connection, 282
 creating a region, 216
 creating a schedule, 227
 creating a special day, 230
 creating a time frame, 228
 creating a trigger, 223
 creating a user, 162
 creating a user group, 168
 creating an action, 229
 credit, 276
 custom LCD message, 241

D

date, 232
 daylight saving time, 232
 default, 141

- default values, 30
- defaulting panel, 30
- defaults, 114, 249
- de-isolate, 173, 174
- delayed unset, 52
- delete
 - door, 204
 - expander, 152
 - filter, 218
 - keypad, 150
 - macro, 159
 - output, 223
 - reader, 161
 - zone, 182
- deleting a central station, 263
- deleting a door group, 215
- deleting a PC connection, 283
- deleting a region, 216
- deleting a schedule, 231
- deleting a special day, 231
- deleting a time frame, 228
- deleting a trigger, 224
- deleting a user, 165
- deleting a user group, 169
- deleting an action, 230
- demo, 138
- deny access, 208
- detector test, 124
 - auto test, 181
 - duration, 124
 - manual test, 124
 - time, 124
- device states, 142
- DHCP, 271
- dialler
 - battery, 135
- disable door, 139
- disable duress, 207
- disarm, 51
- DNS, 271
- door, **68, 196**
 - alarm control, 208
 - anti-passback, 213
 - area groups, 200
 - areas, 199
 - changing, 197
 - control, 139
 - creating, 196
 - delete, 204
 - deny access, 200, 208
 - disable RTE, 209
 - DOTL output, 212
 - DOTL reporting, 210
 - DOTL zone, 207
 - EE PIN lock, 201
 - extend unlock time until opened, 207
 - extended time, 198
 - forced door, 210, 212
 - group, 69, 214
 - indication, 204, 212
 - intelligent door, 68
 - interlock, 210
 - location, 197
 - lock, 200
 - lock when closed, 207
 - low security, 200, 211
 - move, 203
 - name, 197
 - open and close reporting, 210
 - output, 198, 214
 - outside user, 213
 - pulsed lock and unlock, 71, 208
 - reader options, 204
 - readers, 197
 - region, 213
 - reporting, 209
 - RTE, 201
 - RTE control, 209
 - RTE reporting, 210
 - RTE schedule, 211
 - RTE zone, 209
 - schedule, 201
 - second zone, 207
 - shunt, 69, 201
 - standard door, 68
 - time, 198
 - unlock, 200, 201
 - user group, 208
 - warning output, 212
 - zone, 199
- door control, 139
- door controller, **68**
 - options, 247
 - outputs, 212
- door group, **69, 214**
 - creating, 214
 - deleting, 215
- door group
 - name, 215
- door held open, 204
- door shunt, **69, 201, 204**
 - entry/exit, 204
 - extended time, 202
 - time, 202
 - warning, 202
 - zones, 211
- door shunt time, 202
- door shunt warning, 202
- DOTL
 - output, 212
- DOTL zone, 207
- double knock, 174
 - timers, 235
- Downloader, **288**
- DST, 232
- dual loop, 152
- dual unset, 189

duress
 disable, 207

E

earthing, 20
EN 50131 requirements, 61
enable door, 139
encryption, 265, 269
 key, 284
end time, 228, 231
engineer lockout, 237
engineer reset, **102**, 237
 auto reset, 239
 disable when service in, 239
engineer walk test, 80, 127, 175
entry
 extend time, 176
entry alarms, 188
entry time, 176, 186
entry timer, 242
entry/exit, 45, 47, 180
 access, 244
 full set, 244
 PIN lock, 146
entry/exit door shunt, 204
entry/exit time, 186
entry/exit zone, 149
EOL, 24, 152, 248
event, 79
event list, 311
events, **266**
 mapping, 266
exit terminator, 46, 176, 235
exit time, 186
exit timer, 242
expander, **59**, 142, **150**
 dual loop, 152
 EOL, 152
 input mode, 152
 isolate, 152
 name, 151
 resistor values, 152
 settings, 151
 single zone, 152
 troubleshooting, 298
extend entry timer, 176
extend test call, 131
extended door shunt time, 202
extended time, 198
extended unset time, 257

F

failed to communicate, 86
fault, 126
fault indication, 242
filter, **217**
 creating, 217
 delete, 218

final door, 176
final set, 235
firewall, 272
firmware, 290
flash, 290
flexible addressing scheme, 253
fob, 164, **191**
 add, 94, 191
 assigned user, 191
 buttons, 192
 name, 191
 remove, 193
forced set, 244
formula, 158, 217
frame rate, 155
frequent heartbeat, 265
frequent test call, 131
FTC, 86
function key, 57, 148

G

gateway, 271
glossary, 337
GPRS, 279
 disconnection time, 280
 line fault, 280
 password, 280
 picture limit, 273
 user name, 280
GPRS network
 registration, 134
 state, 134
gross level, 183
GSM, 274
 battery status, 135
 reporting, 266
GSM network, 274
 availability, 275
 code, 134
 diagnostic, 133
 PIN status, 133
 registration, 133
 scan, 275
 signal strength, 134

H

HDR, 122
heartbeat, 264
 frequent, 265
held open alarm, 179
 time, 236
hierarchy, 189
high current output, 256
high security, 189
high security region, **70**, 214
high security user, **70**, 214
 prewarning time, 214
housing, **8**

HSR, **70**, 214

HSU, **70**, 214

I

IN reader, 197

inactive days, 123, 236

inhibit, **53**, 174

inhibit limit, 189

input, 171

 delay, 236

 options, 248

 resistance, 123

 test, 121

input mode, 152

input state, 121, 126

inspection, 240

 date, 240

installation, **114**

installer, **60**

 in-time, 235

 user confirmation, 237

installer code, 114, 115

installer in, 240

intelligent door, 68

interlock, 210

invert output, 220

inverted walk test, 123

 timer, 236

IP

 picture limit, 273

IP address, 270

IP diagnostic, 131

IP interface, 132

IP statistics, 132

ISDN

 point to point, 270

isolate, **53**, 173, 174

 camera, 195

 keypad, 147

isolation limit, 189

K

key, **54**, 176

key box

 time, 236

key switch, 46, 176

keypad, **13**, **58**, 142, **143**

 buzzer, 255

 troubleshooting, 298

keypad layout, 112

keypad lockout, 54, 106

L

LAN device, 58

LCD

 EE timer, 242

LCD backlight, 149

LCD message, 241

LCD options, 241

LCD reader, 161

LDR, 122

learn card, 164

LED, 206

LED test, 125

line number, 265

link speed, 273

listing open zones, 121

lock door, 139, 200

lock user data, 61

lock when closed, 207

lockout, 54, 106

log, 120

logic, 74

logout, 141, 240

low security, 200

M

MAC, 273

macro, 157

 creating, 158

 delete, 159

mains fail reporting delay, 234

manual test, 124, **131**

map door controller relays, 247

map panel LEDs, 248

menu entries, 241

 accessing, 108

 confirmation of changes, 111

 exit, 111

 explanation of the LCD display, 109

 how to edit host address, 111

 how to edit list, 110

 how to edit text, 110

 how to program values, 109

 how to program Yes/No options, 110

 programming, 109

 scrolling the list of menus, 109

 unauthorized access, 106

 using PIN, 106

menu tree, 351

MMS, 281

 limit, 281

 proxy, 281

monitor output 3, 256

move a door, 203

multiple badge time, 247

N

need acceptance, 108

need to set, 128

NTP, 133, 272

O

OH 2000, 264
 omit first call, 269
 open door, 139
 open zones, 121
 OUT reader, 197
 output, 30, **67**, 214, **217**
 active time, 222
 add, 219
 alarm, 214
 delay, 222
 delete, 223
 DOTL, 212
 edit, 219
 forced door, 212
 mode, 220
 name, 219
 siren, 256
 test, 125
 warning, 212
 outside user, 213

P

panel diagnostics, 137
 panel ID, 285
 panel information, 139
 panel lid, 140
 panel status, 126
 panel version, 139
 panic alarm, 149, 254
 part set, 51, 180
 name, 244
 options, 243
 PC connection, 282, 288
 creating, 282
 deleting, 283
 host, 285
 port, 286
 PCB, 12
 picture auto deletion, 156
 picture frame rate, 155
 picture options, 155
 picture quality, 156
 picture settings, 155
 PIN, **66**, 162, 274
 ping, 132, 264, 273, 286
 point to point, 270
 prealarm time, 187
 predefined user, 60
 prepaid, 276
 privilege limitation, 64
 programmable functions, 88
 programming, 74, 351
 programming cameras, 98
 programming map, 351
 programming users, 162
 programming wireless devices, 92
 protocol, 259, 261

pry-off tamper, 10
 PUK, 133, 274
 pulse count, 183
 pulsed lock and unlock, 71
 door lock procedure, 72
 door open procedure, 72

Q

quick installation, **2**
 quick programming, **4**
 quick set, 147

R

range test, 123
 reader, **160**, 197
 card and PIN, 205
 card format, 205
 LED, 206
 schedule, 205
 two cards, 205
 reader options, 204
 ready to set, 242
 receiver number, 265
 reduced walk test, 129
 region, **69**, 213
 count limit, 157
 creating, 216
 deleting, 216
 name, 216
 region count limit, 157
 regulations, 302
 reinstall, 141
 re-lock delay, 247
 remote configuration, 253
 remote login, 163
 remote options, 253
 remote PIN, **163**, 253
 remove
 fob, 193
 RF device, 185, 193
 replacing battery, 16
 reporting, 84
 account code, 259
 phone numbers, 263
 request to exit, 179
 resistance, 123
 resistor values, 152, 248, 249
 resolution, 156
 RF device
 configuration, 183, 192
 remove, 185, 193
 supervision, 184
 RF state, 122
 ring setup, 268
 RSSI, 122

RTE, 179, 201
 control, 209
 disabled when areas set, 209
 schedule, 211
 RTE zone, 209
 RTS, 242

S

schedule, **77**, 205
 action list, 229
 active schedule, 227
 condition filter, 231
 creating, 227
 date, 227
 deleting, 231
 door unlock, 201
 name, 227
 RTE, 211
 special day, 230
 time, 227
 time frame, 228
 scheme, 31, 253
 sensor type, 178
 service, **120**
 time, 235
 user confirmation, 237
 service in, 108, 141, 240
 set, **51**
 set options, 242
 shielding, 21
 shock sensor, 125, 176, 182
 sensitivity, 183
 shunt, 47, **53**, 124, 181
 door, 69, 201
 time, 202
 type, 202
 zone, 53
 shunt limit, 190
 shunt zones, 211
 SIA codes, 327
 SIA frequency, 262
 silent set, 188
 SIM, 274
 single zone, 152
 single zone walk test, 129
 siren, 28
 siren EOL, 249
 siren output, 256
 siren timers, 233
 SMS, 278
 center, 278
 charset, 279
 control, 65, 166
 counter, 135
 forwarding, 278
 header, 279
 messages limit, 278
 PIN, 279

reporting, 65, 166
 soak test, 175
 time, 236
 software revision, 139
 special day, 225, 230
 creating, 230
 deleting, 231
 end time, 231
 name, 230
 start time, 231
 special walk test mode, 129
 standard door, 68
 standard walk test, 127
 start filter, 220
 start time, 228, 231
 status, 126
 stop filter, 220
 stop voice reporting, 181
 subevents, **261**
 supervision, 184
 suppress FTC, 262
 swinger shunt, 174, 249
 system bus, 22
 system code, 239
 system options, **232**

T

tamper area, 144
 technical alarm, 177
 technical zone sensor, 178
 telephone number, 263
 test, 121
 battery, 135
 communication, 83
 test call, 130, 131
 extend test call, 131
 frequent test call, 131
 FTC, 131
 test duration, 124
 test time, 124
 testing system, **80**
 time and attendance, 206
 time and date, 232
 time frame, 225
 creating, 228
 deleting, 228
 end, 228
 start, 228
 week days, 228
 time zone, 232
 timed open, 139
 timed unset, 256
 delay, 256
 extended time, 257
 time, 257
 warning time, 257
 timers, **232**
 Titan, 288

transmission path, 259, 267

trigger, **76, 217**

creating, 223

deleting, 224

name, 223

state, 126

troubleshooting, **297**

data gathering panels, 298

LCD keypads, 298

two cards, 205

two cards time, 246

U

uninhibit, 174

unlock door, 139, 200

output, 198

unset, **51**

delayed unset, 52

unset delay, 188

upgrade, 290

user, **60, 162**

area selection mode, 165

card, 163

changing, 162

creating, 162

deleting, 165

language, 164

PIN, 162, 163

programming, 162

user group, 168

user card, 163

user confirmation, 237

user data lock, 61

user group, **62, 168, 208**

changing, 168

creating, 168

deleting, 169

functions, 62

name, 168

options, 169

privilege limitation, 64

type, 168

user group type, 62

user LCD message, 241

user management, 162

user name, **162**

user phone, 166

user privilege, 168

user programmable functions, 88

user walk test, 127, 128, 175

using cameras, 98

V

VdS codes, 327

version, 290

video port, 265

virtual zone, 179

W

walk test, **80, 82, 127, 129, 175**

active walk test, 82, 129

confirmed alarm, 82, 129

frequency, 128

reduced walk test, 129

single zone, 129

standard walk test, 127

timeout, 234

walk test mode, 82, 129

warning time, 187, 257

week days, 228

wireless device, **92, 183, 192**

supervision, 184

wireless sensor, 92

Z

zone, **45, 171**

access, 180

area, 173

auto test, 181

connection, 23

copy, 181

de-isolate, 173, 174

delete, 182

entry/exit, 180

entry/exit time, 186

held open alarm, 179

inhibit, 174, 243

isolate, 173, 174, 181

move, 182

name, 172

open too long, 179, 236

options, 173, 248

part set, 51

prealarm time, 187

report as duress, 180

report as panic, 180

reporting, 177

resistance, 123

RTE, 209

shunt, 47, 53, 124, 181

stop voice reporting, 181

type, 45, 172

uninhibit, 174

warning time, 187

zone acknowledgement, 178

zone delay, 178

zone expansion, 30

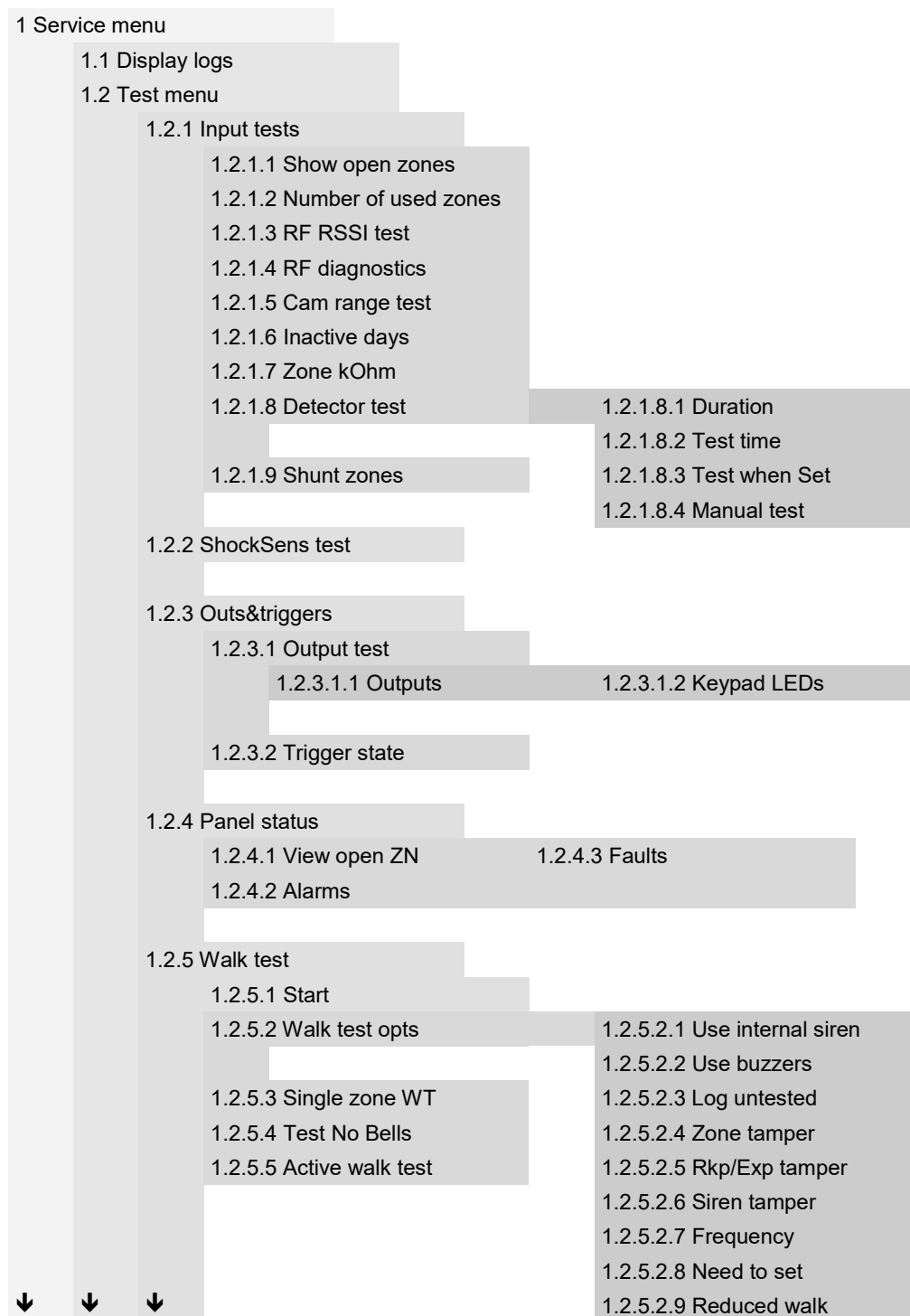
zone options, 173

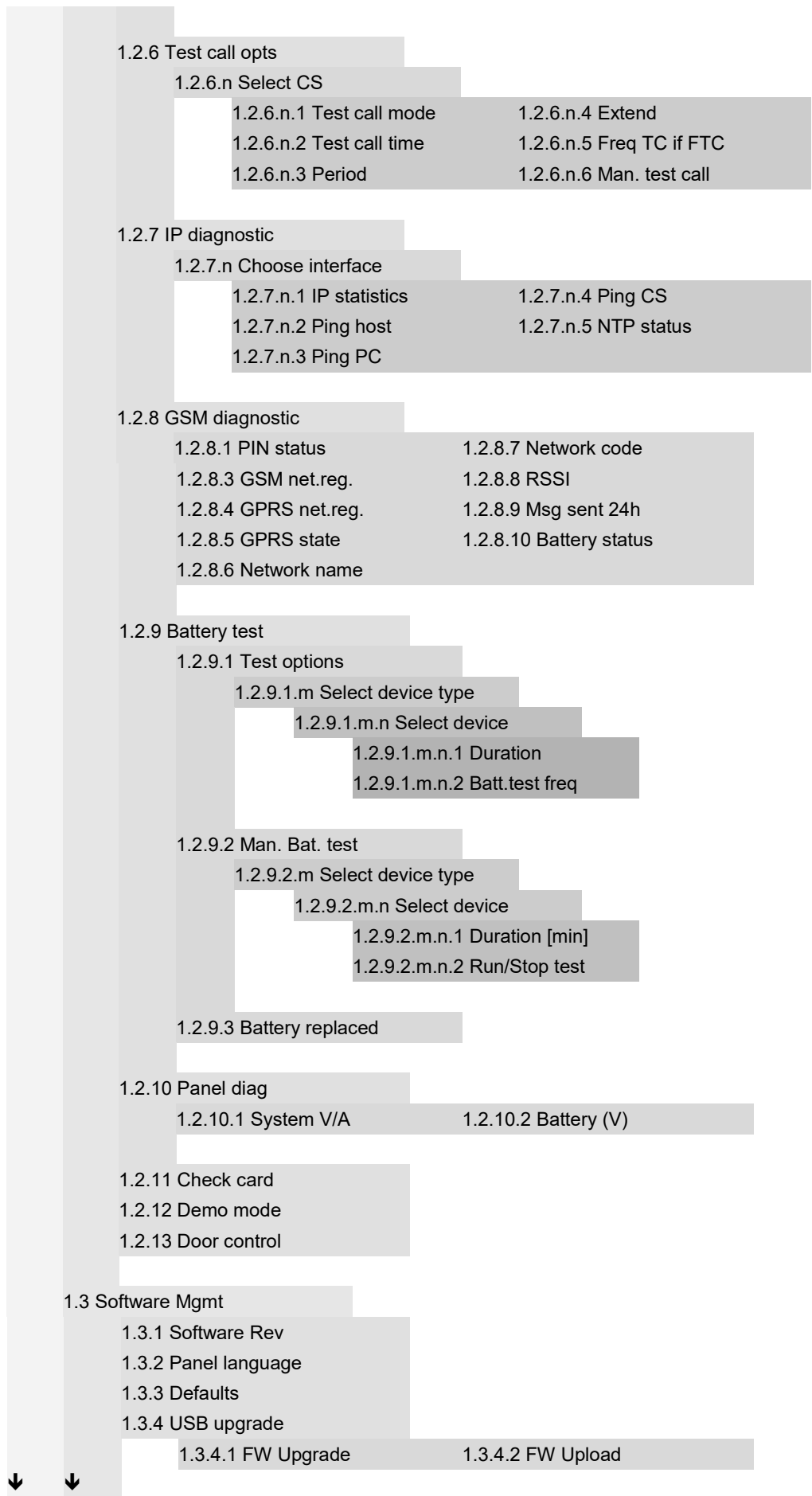
zone pairing, 175

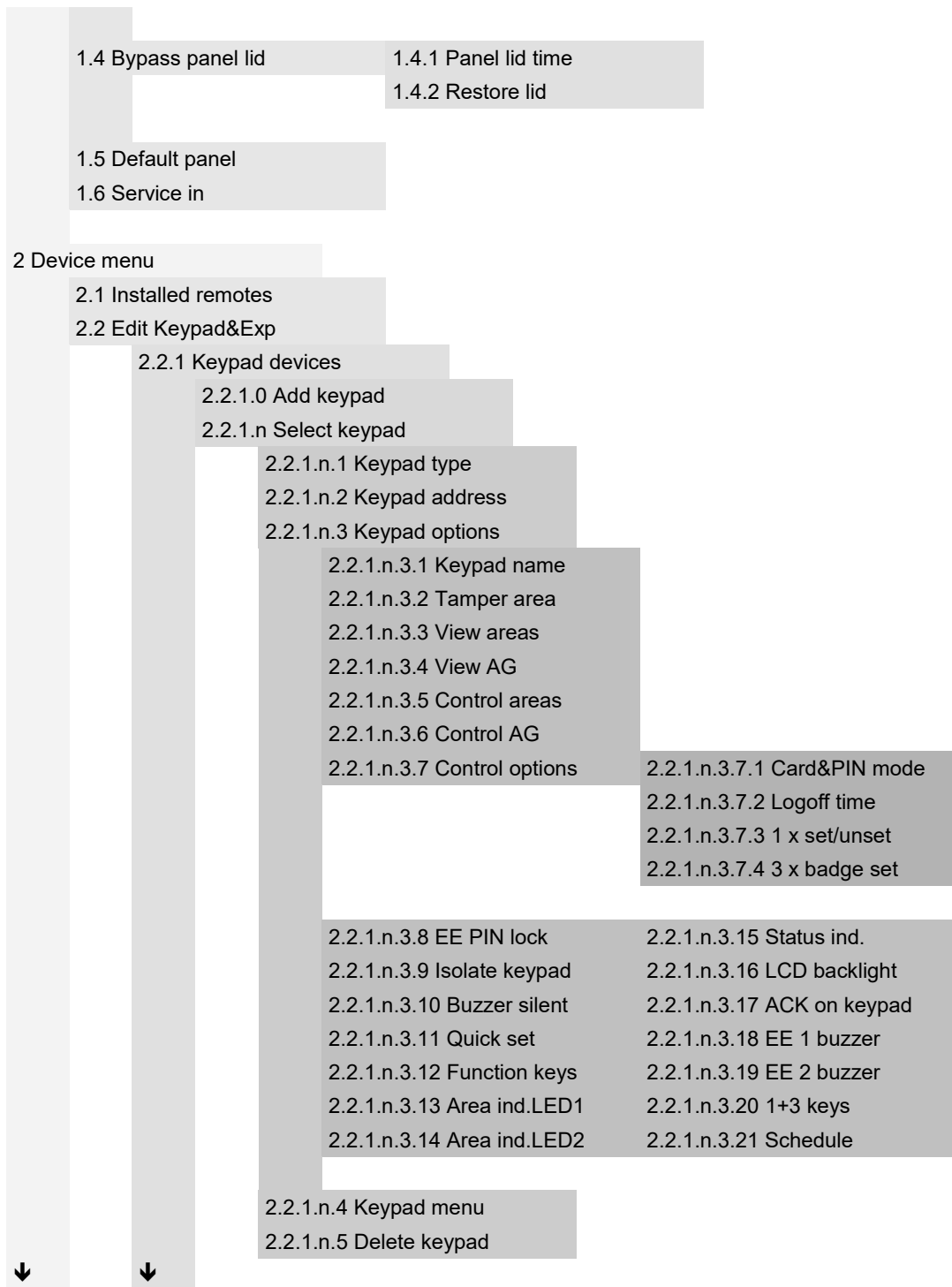
zone shunt, 203

zone type, 45, 172

Programming map

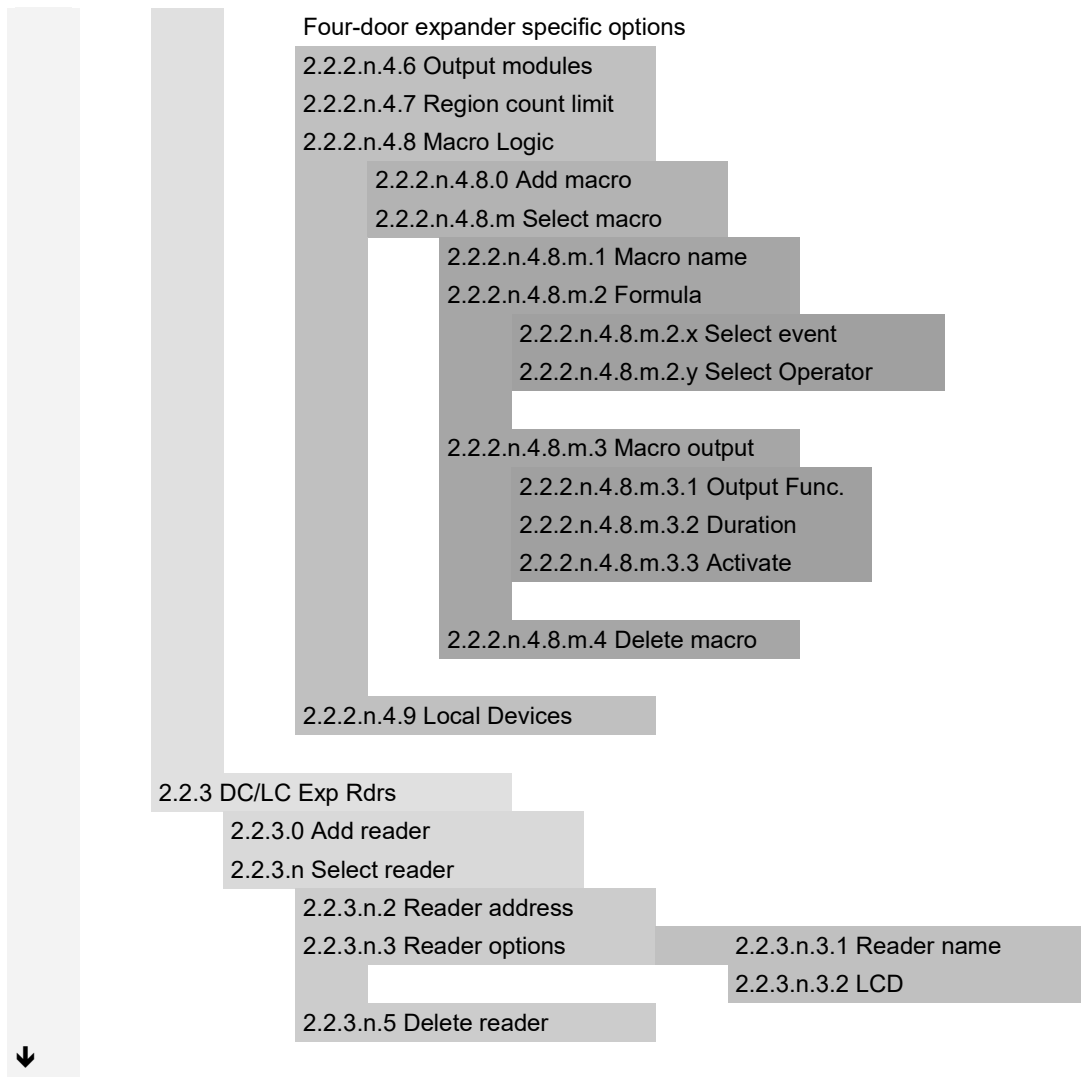


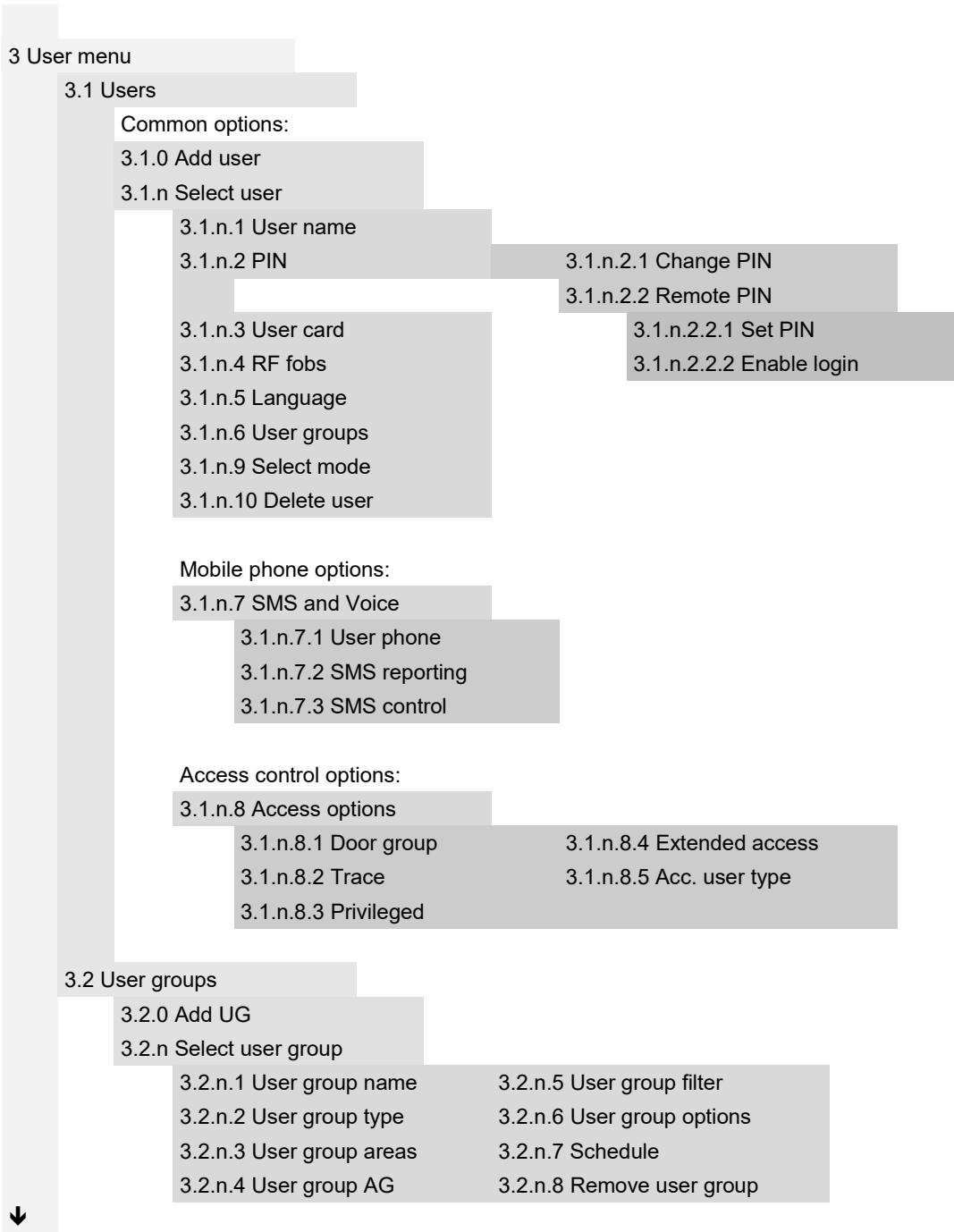




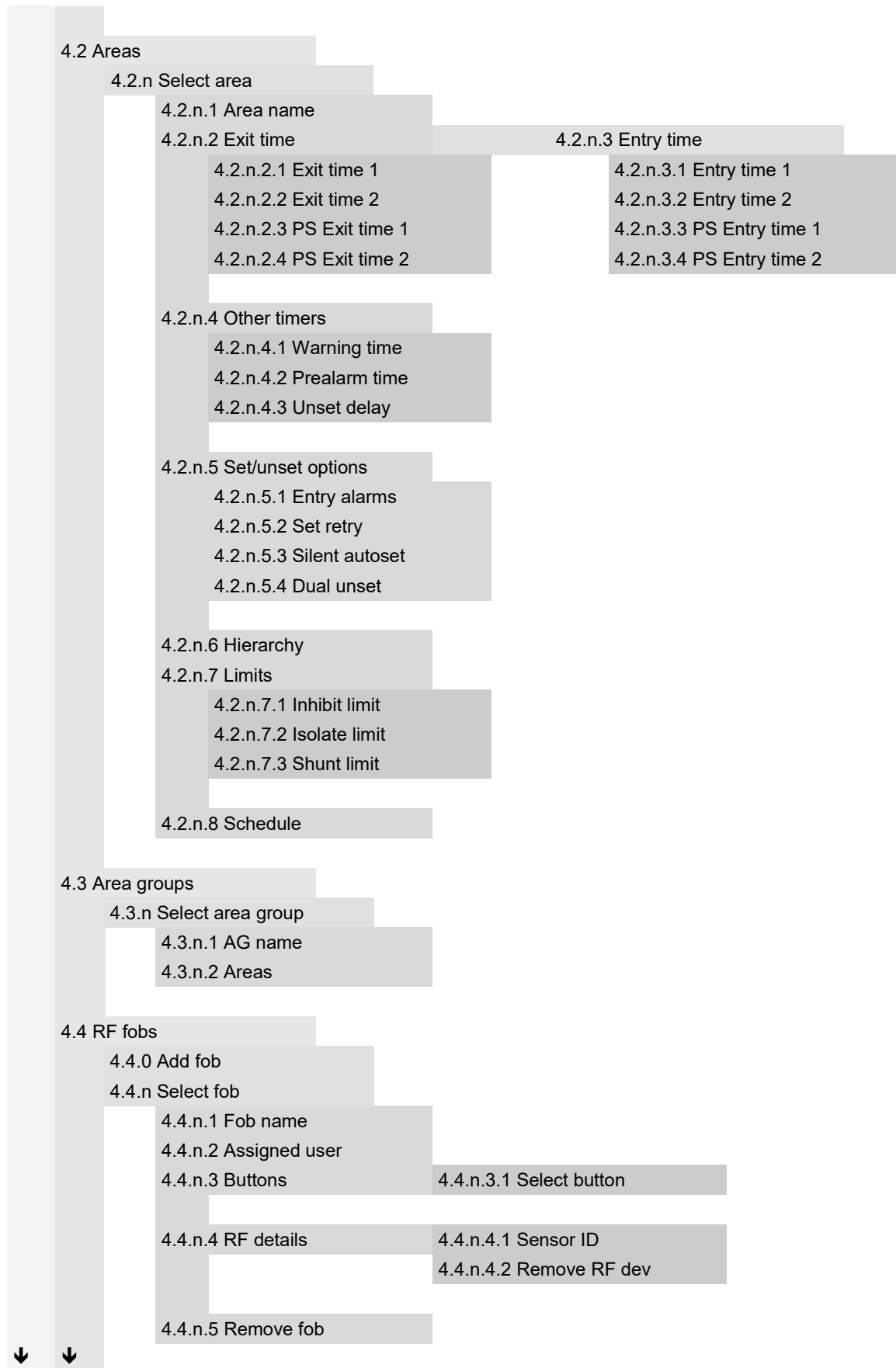
- 2.2.2 Expander devices
 - 2.2.2.0 Add expander
 - 2.2.2.n Select expander
 - 2.2.2.n.1 Expander type
 - 2.2.2.n.2 Expander address
 - 2.2.2.n.3 Expander range
 - 2.2.2.n.4 Exp settings
 - 2.2.2.n.4.1 Expander name
 - 2.2.2.n.4.2 Tamper area
 - 2.2.2.n.4.3 Isolate expander
 - 2.2.2.n.4.4 Input mode
 - 2.2.2.n.4.5 EOL
 - 2.2.2.n.5 Expander menu
 - 2.2.2.n.6 Delete expander
 - 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 Jamm detection
 - 2.2.2.n.4.11 Default expander
 - 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 settings
 - 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
 - 2.2.2.n.4.9.1.2 Fire settings
 - 2.2.2.n.4.9.1.3 Panic settings
 - 2.2.2.n.4.9.1.4 Medical set.
 - 2.2.2.n.4.9.1.5 Tamper set.
 - 2.2.2.n.4.9.1.6 Fault settings
 - 2.2.2.n.4.9.1.7 Custom type 1
 - 2.2.2.n.4.9.1.8 Custom type 2
 - 2.2.2.n.4.9.2 Show pic mem
 - 2.2.2.n.4.9.3 Pic auto deletion
 - 2.2.2.n.4.9.4 Total pic cnt
 - 2.2.2.n.4.11 Delete pics

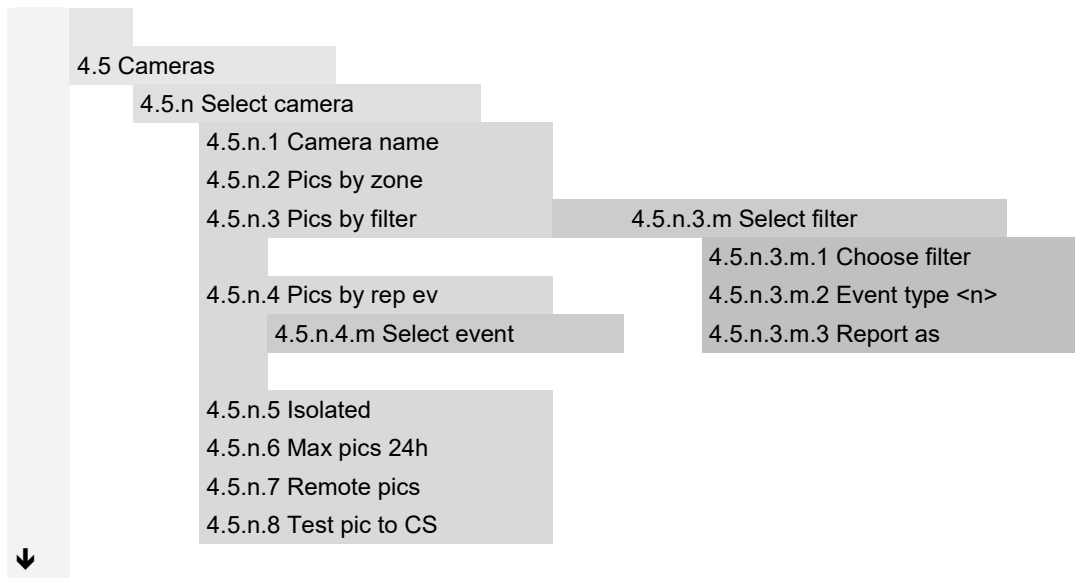


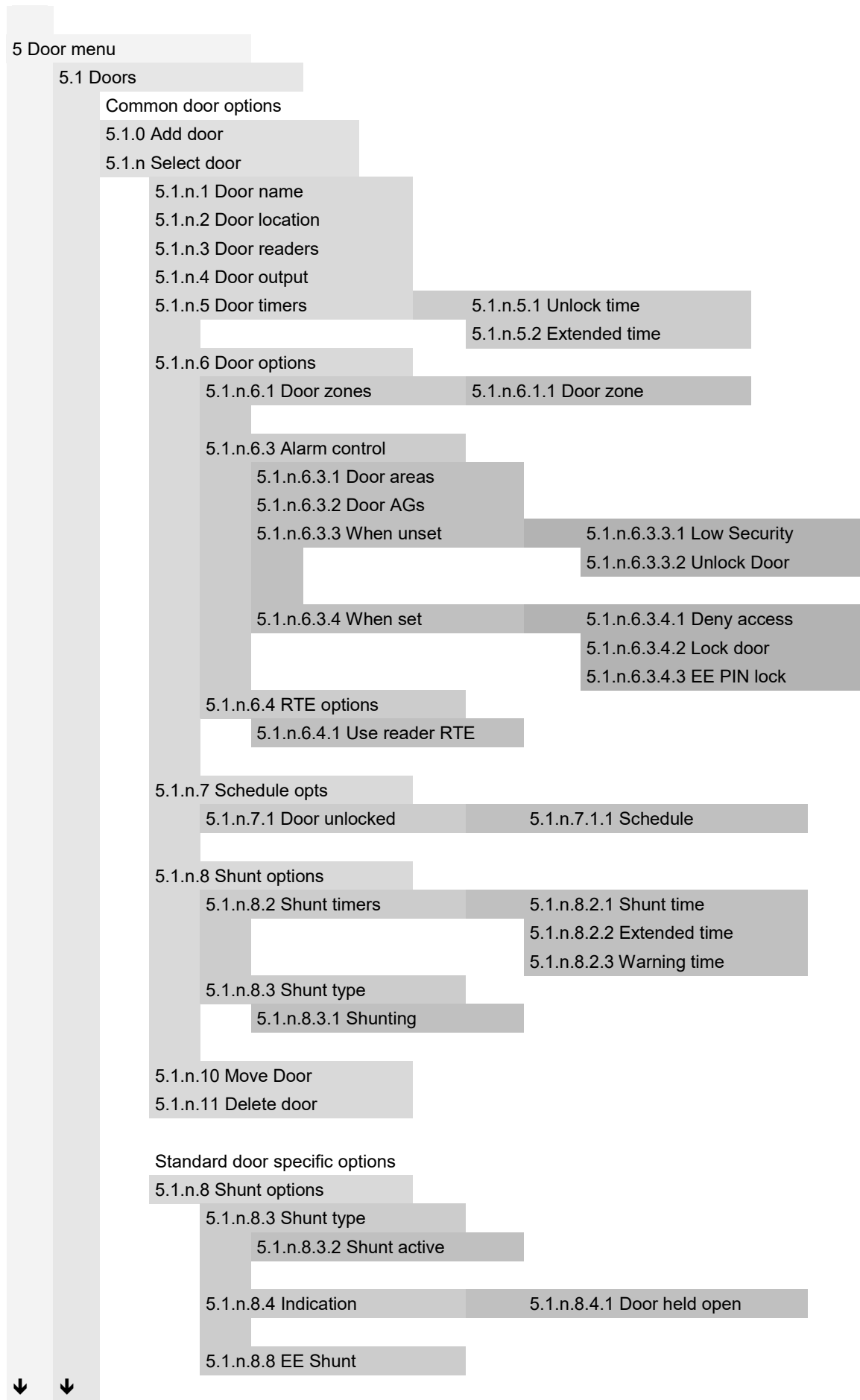




- 4 Zones and areas
 - 4.1 Zone menu
 - 4.1.0 Add zone
 - 4.1.n Select zone
 - Common options
 - 4.1.n.1 Zone name
 - 4.1.n.2 Zone type
 - 4.1.n.3 Isolated
 - 4.1.n.4 Zone location
 - 4.1.n.5 Zone areas
 - 4.1.n.6 Zone options
 - 4.1.n.6.1 Inhibit
 - 4.1.n.6.2 Isolate
 - 4.1.n.6.3 Excl. in PS1
 - 4.1.n.6.4 Excl. in PS2
 - 4.1.n.6.5 Double knock
 - 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 Engineer walk test
 - 4.1.n.6.12 User walk test
 - 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 Technical full set
 - 4.1.n.6.20 Technical unset
 - 4.1.n.6.21 Technical 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 Stop report
 - Shock sensor options
 - 4.1.n.7 Grs&PIs options
 - 4.1.n.7.1 Pulse count
 - 4.1.n.7.2 Gross level
 - 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
 - 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







Intelligent door specific options

5.1.n.3 Door readers

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&Attendance
- 5.1.n.3.5.7 Disable Duress

5.1.n.6 Door options

5.1.n.6.1 Door zones

- 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 Alarm control

- 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 RTE options

- 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 Schedule opts

- 5.1.n.7.1 Door unlocked
- 5.1.n.7.1.2 After entry
- 5.1.n.7.2 Low Security
- 5.1.n.7.3 RTE Schedule

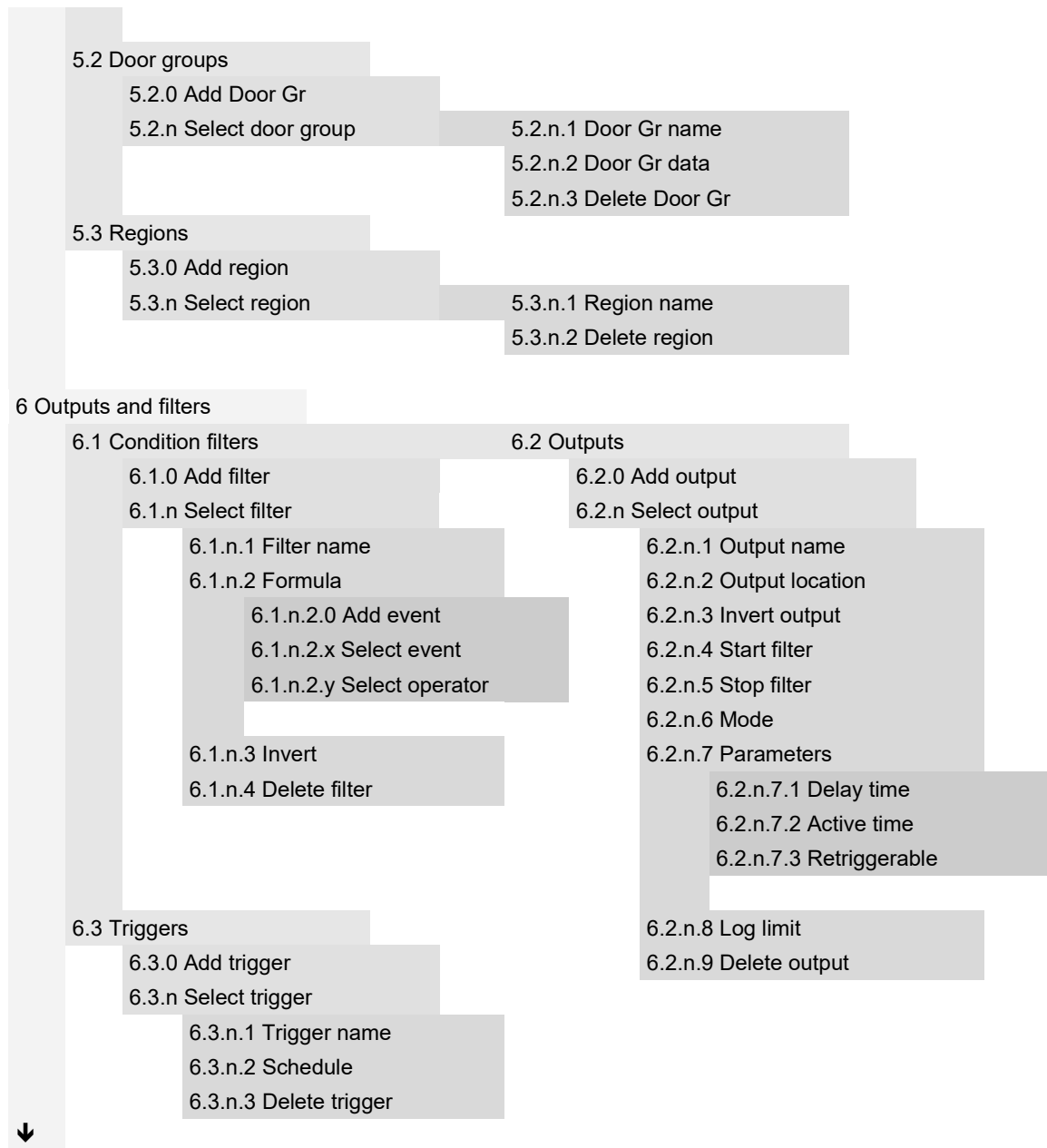
5.1.n.8 Shunt options

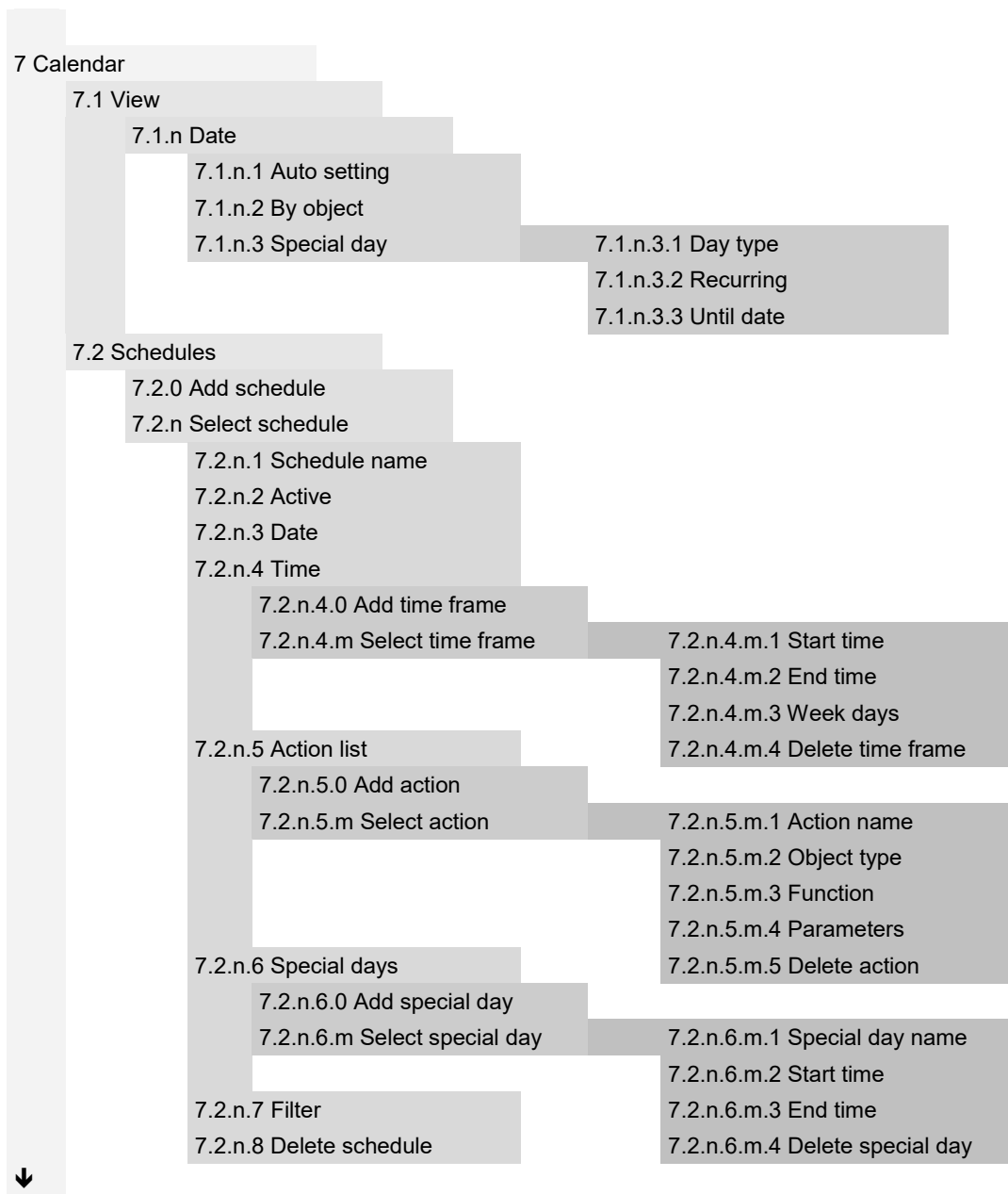
- 5.1.n.8.1 Zones
- 5.1.n.8.4 Indication
- 5.1.n.8.4.2 DOTL output
- 5.1.n.8.4.3 Warning output
- 5.1.n.8.4.4 Forced door
- 5.1.n.8.5 Until door CL
- 5.1.n.8.6 CancelAfterCL

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

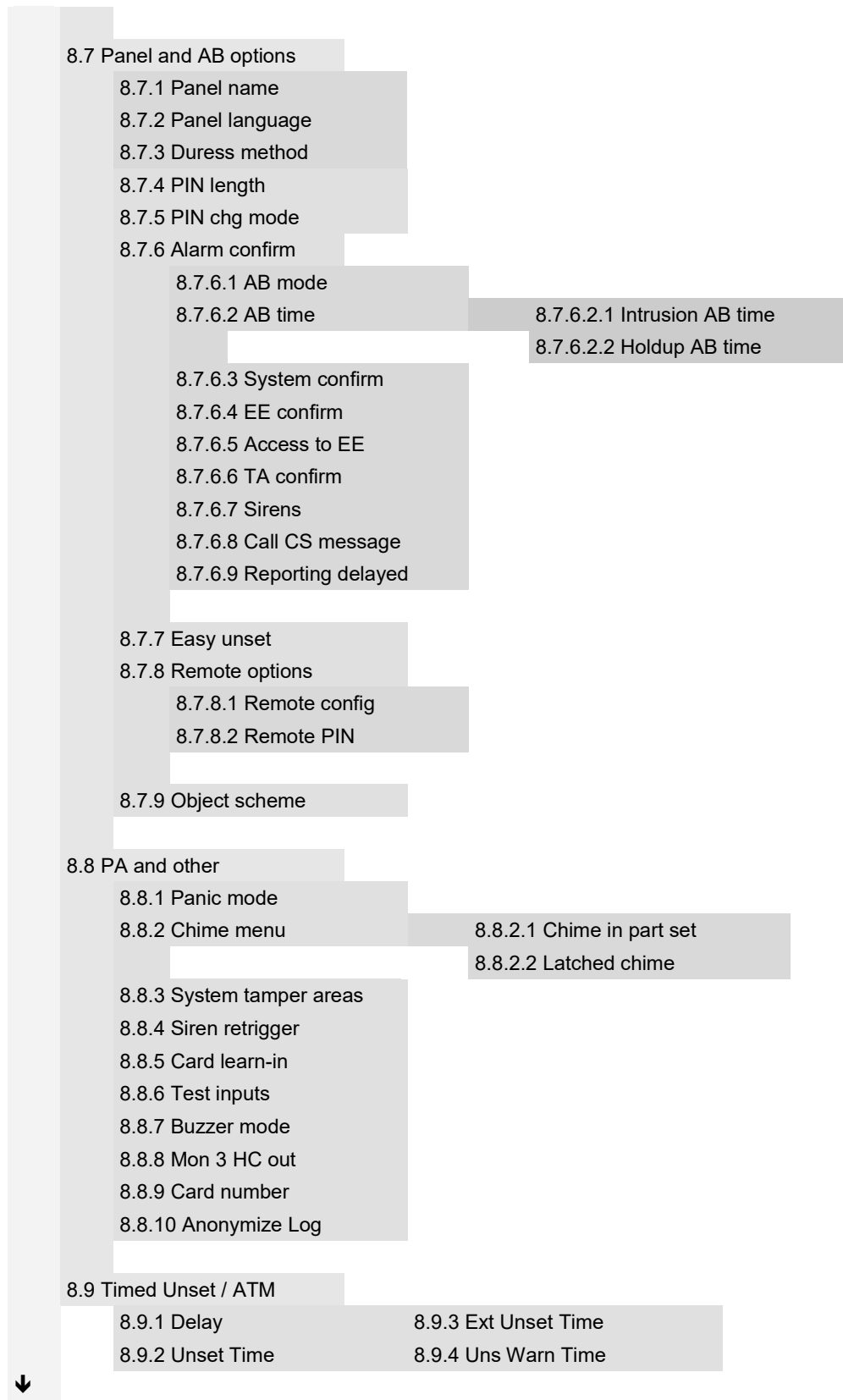


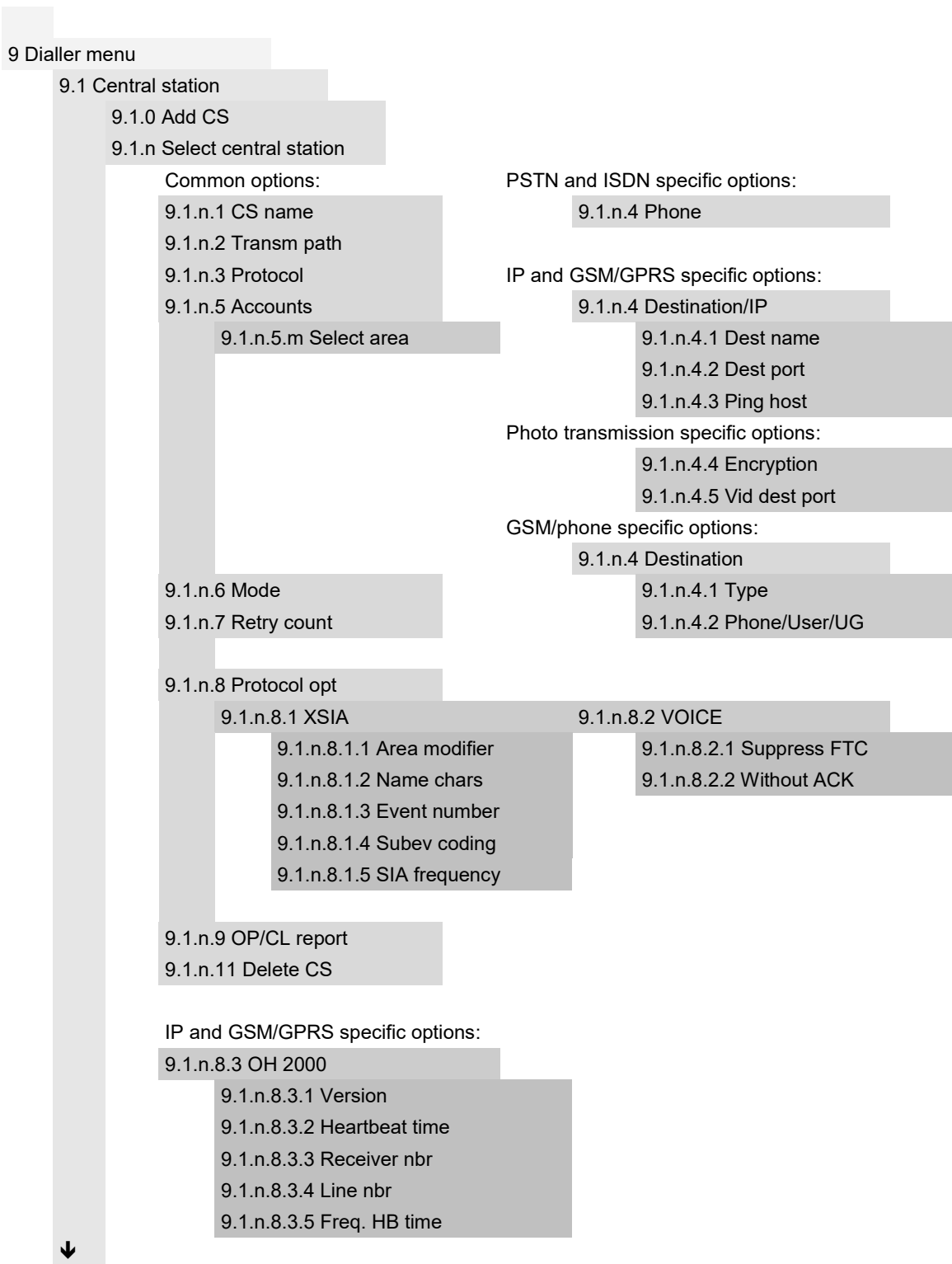




8 System option menu	
8.1 Timer menu	
8.1.1 Time and date	
8.1.2 Siren options	
8.1.2.1 Activation	8.1.2.2 Delay time
8.1.2.1.1 Internal siren	8.1.2.2.1 Internal siren
8.1.2.1.2 External siren	8.1.2.2.2 External siren
8.1.2.1.3 F/P/M internal	
8.1.2.1.4 F/P/M external	
8.1.3 System misc opts	
8.1.3.1 Armed display	8.1.3.4 Mains reporting delay
8.1.3.2 Card and PIN	8.1.3.5 Final set delay
8.1.3.3 Walk test time	8.1.3.6 Installer in-time
8.1.4 Zone timer menu	
8.1.4.1 Double knock interval	8.1.4.5 Key box time
8.1.4.2 Double knock open	8.1.4.6 Held open time
8.1.4.3 Soak test	8.1.4.7 Inactive days
8.1.4.4 Input delay	
8.2 Engineer options	
8.2.1 User code required	
8.2.2 Tamper required	
8.2.3 Engineer lockout	
8.2.4 Engineer reset	
8.2.4.1 Alarm	8.2.4.8 Siren fault
8.2.4.2 Tamper	8.2.4.9 Interconn fault
8.2.4.3 Panic	8.2.4.10 Auto reset
8.2.4.4 Confirmed alarm	8.2.4.11 Dis by service
8.2.4.5 Battery fail	8.2.4.12 System code
8.2.4.6 Aux fuse	8.2.4.13 Do reset
8.2.4.7 Mains fail	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
8.3 LCD display options	
8.3.1 Armed display	8.3.4 Indicate faults
8.3.2 Custom message	8.3.5 View EE timer
8.3.3 Alarm list	
↓	↓

8.4 Set options	
8.4.1 RTS options	
8.4.2 Inhibit includes	
8.4.3 Part set	
8.4.3.1 Report BA	8.4.3.4 PS1 name
8.4.3.2 Access to EE	8.4.3.5 PS2 name
8.4.3.3 EE full set	
8.4.4 Forced set	
8.4.5 Forced set options	
8.4.6 Pending alarms	
8.4.7 AS fault retry	
8.4.8 AS user retry	
8.5 Access options	
8.5.1 Access timers	
8.5.1.1 Card to PIN	8.5.1.3 Multiple badge
8.5.1.2 Two cards	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
8.6 Zone options	
8.6.1 Input mode	8.6.4 Swinger shunt
8.6.2 EOL	8.6.5 Report restore
8.6.3 Siren tamper EOL	
↓	↓





9.2 Event options

- 9.2.1 CS mapping
- 9.2.2 Voice mapping
- 9.2.3 Delayed events

9.3 Path options

9.3.n Select path

Common options:

- 9.3.n.1 Path name
- 9.3.n.2 Line fault
- 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.3 Transm path
- 9.3.n.4 IP config
 - 9.3.n.4.1 IP config
 - 9.3.n.4.2 IP address
 - 9.3.n.4.3 Subnet mask
 - 9.3.n.4.4 Gateway
- 9.3.n.5 DNS config
 - 9.3.n.5.1 DNS config
 - 9.3.n.5.2 DNS server
- 9.3.n.6 NTP config
 - 9.3.n.6.1 NTP config
 - 9.3.n.6.2 NTP server
- 9.3.n.7 Firewall
 - 9.3.n.7.1 Firewall
 - 9.3.n.7.2 Reply on PING
- 9.3.n.8 Link speed
- 9.3.n.9 MAC address
- 9.3.n.10 Max Pics 24h

PSTN specific options:

- 9.3.n.3 Line fault delay
- 9.3.n.4 Transm path
- 9.3.n.5 Dial tone
- 9.3.n.6 Dialing

ISDN specific options

- 9.3.n.6 Point to Point
- 9.3.n.7 MSN

↓

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 Select a network

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.5.3.4 Request code

9.3.n.5.3.2 Check mode

9.3.n.5.3.5 Check period

9.3.n.5.3.3 Check number

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 Jamming threshold

9.3.n.6 SMS Setup

9.3.n.6.1 SMS Center num

9.3.n.6.4 SMS header msg

9.3.n.6.2 SMS forwarding

9.3.n.6.5 User PIN req.

9.3.n.6.3 Max Msg 24h

9.3.n.6.6 Ext.charset

9.3.n.7 GPRS Setup

9.3.n.7.1 APN

9.3.n.7.6 Firewall

9.3.n.7.2 User name

9.3.n.7.7 Line fault

9.3.n.7.3 User password

9.3.n.7.8 Disconn.time

9.3.n.7.4 IP config

9.3.n.7.9 Max Pics 24h

9.3.n.7.5 DNS config

9.3.n.10 MMS Setup

9.3.n.10.1 MMS Center

9.3.n.10.5 Proxy

9.3.n.10.2 APN

9.3.n.10.6 Proxy port

9.3.n.10.3 User name

9.3.n.10.7 Max MMS 24h

9.3.n.10.4 User password

9.3.n.11 Module info



