Advisor Advanced ATSx000A(-IP) Installation and Programming Manual

P/N 1068970 (EN) • REV H • ISS 28AUG15

Copyright © 2015 UTC Fire & Security Americas Corporation, Inc. All rights reserved.

Trademarks and patents

Interlogix, Advisor Advanced ATSx000A(-IP) name and logo are trademarks of UTC Fire & Security.

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

Manufacturer

UTC Fire & Security Americas Corporation, Inc.
3211 Progress Drive, Lincolnton, NC, 28092, USA

Authorized EU manufacturing representative:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Version

This document applies to the following Advisor Advanced firmware versions:

ATSx000A(-IP): V026.026.130

Certification

CE

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

ATSx000A(-IP): Security Grade 2, Environmental class II

Tested and certified by Telefication B.V.

Important: This product has not been designed to comply to EN 50134 and EN 54 norms.

European Union directives

UTC Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of one or more of the Directives 1999/5/EC, 2014/30/EU and 2014/35/EU. For more information see www.utcfireandsecurity.com or www.interlogix.com.



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.recyclethis.info.

Contact information

www.utcfireandsecurity.com or www.interlogix.com

Customer support

www.utcfssecurityproducts.eu

Content

Preface vi
Typographical conventions vi
Important note vi

General installation information 1
Advisor Advanced housings 1
Advisor Advanced layout 4
Keypads and readers 5

Maintenance 8
Mains power connection 8
Battery replacement 8

Mounting 10
General installation guidelines 10

Earthing 12

Shielding 13

Cabling Advisor Advanced 14
System databus preferred wiring 14
System databus connection 14
Zone connection 15
Values for end-of-line resistors 16
EOL connection types 19
Siren connection 20
Other connections 20

Configuration 22
Defaulting the panel 22
Zone configuration 22
Outputs 22
Zone and output addressing 23

Specifications 25
Auxiliary current and battery capacity 28

Common key sequences 29
Common key sequences for LCD keypad 29
Common key sequences for keypad without LCD 30
Function keys 32

Programming sequence 33
Basic setup 33
Advanced setup 33

Test menus 34

The Advisor Advanced menu 35
How the menu sections are organized in this manual 35
Option availability 36

How to program the options 37
Accessing the installer programming menu 37
What the LCD display tells you 38
Editing the options 38
Confirmation of changes 40
Exit from menu 40
Keypad layout 40
Word library 41
Remote access 42

Initial start-up 43

Service 45
Test options 46

Devices 66
Bus numbering 66
Viewing devices 66
Editing devices 67

Keypads 68
Keypad options 68
Adding keypad with a higher number 68

Expanders 75
Expander options 75
Wireless specific options 77
Camera specific options 79

Users and user groups 82

Users 83
Predefined users 83
User data lock 83
User options 84
Mobile phone options 87

User groups 89
What is a user group? 89
User group options 89
User privilege limitation 93

Zones, fobs, and cameras 94

Zones 95
Zone options 95
Adding a wireless sensor 95
Shock sensor options 104
Wireless sensor options 104
Copying zones 106

Fobs 108
Fob options 108

Cameras 110

Areas 113
Area options 113

Filters, outputs, and triggers 116

Condition filters 117
How condition filter works 117
Filter settings 118

Outputs 120
Output settings 120

Triggers 125
Trigger settings 125

Calendar 127
Viewing calendar 127

Actions 129
Action settings 129

Action lists 131
Action list settings 131

Exceptions 133
Exception validity note 133
Exception settings 133

Schedules 136
Schedule settings 136

System options 138
Timer options 138
Engineer options 142
Engineer reset procedure 143
LCD display options 147
Set options 148

Zones 152
Part set options 153
Panel and AB options 154
Other options 158

Library 161

Communications 162

Central stations 163
Common options 163
PSTN and ISDN specific options 168
IP and GSM/GPRS specific options 168
Photo transmission specific options 170
GSM/phone specific options 170

Events 172

Communication paths 173
Common options 173
PSTN specific options 174
ISDN specific options 175
IP specific options 175
GSM/SMS/GPRS specific options 178

PC connections 188
Common options 188
PSTN specific options 190
IP and GSM/GPRS specific options 191
GSM specific options 192

User programmable functions 193

Autoset 196

Wireless device programming 197
Learning wireless sensors 197
Learning fobs 199
Two-zone RF sensors 201
Device activation 202

Using cameras 203
Configuration 203
Diagnostics 205
Troubleshooting 205

Alarm reporting principles 206
Event conditions 206
Reporting order 207
Failed to communicate (FTC) 208

Programming Advisor Advanced via configuration software 209

Upgrading Advisor Advanced firmware 210
Installing AAFlash on the PC 210
Connecting Advisor Advanced to the PC 210
Archiving current firmware and settings 211
Upgrading Advisor Advanced firmware 211

Troubleshooting 212
Recovery procedure 212
Advisor Advanced control panel 212
LCD keypads 213
Remote expanders — Models ATS1201, ATS1210, ATS1211, ATS1220 213

Advisor Advanced events 215

Reporting codes used in Advisor Advanced 223

Zone types 233

Options affected by EN 50131 regulations 237
EN 50131 Grade 2 237

Options affected by other regulations 239
ACPO policy 239
INCERT policy 239

Glossary 241

Index 245

Programming Map 251

Preface

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.

Typographical conventions

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

Table 1: Notational and typographical conventions

Item	Description
Keys	Capitalized, for example “press Enter”
Note	Notes alert you to information that can save you time and effort
Caution	Cautions identify conditions or practices that may result in damage to the equipment or other property
WARNING	Warnings identify conditions or practices that could result in equipment damage or serious personal injury
❑	Check boxes let you record which options are available for your system.
	Safety sign identifies actions or practices that are required by EN 60950 Safety Standard.

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 2: List of ATSx000A(-IP) panel variants

Model	Enclosure	Dimensions (mm)	Weight (kg)
ATS1000A-SM	Metal	250 x 250 x 86	2.8
ATS1000A-MM	Metal	315 x 388 x 85	5.2
ATS1000A-IP-MM	Metal	315 x 388 x 85	5.2
ATS1000A-LP	Plastic	257 x 400 x 112	2.6
ATS1000A-IP-LP	Plastic	257 x 400 x 112	2.6

Model	Enclosure	Dimensions (mm)	Weight (kg)
ATS2000A-MM	Metal	315 x 388 x 85	5.2
ATS2000A-IP-MM	Metal	315 x 388 x 85	5.2

Notes

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

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)

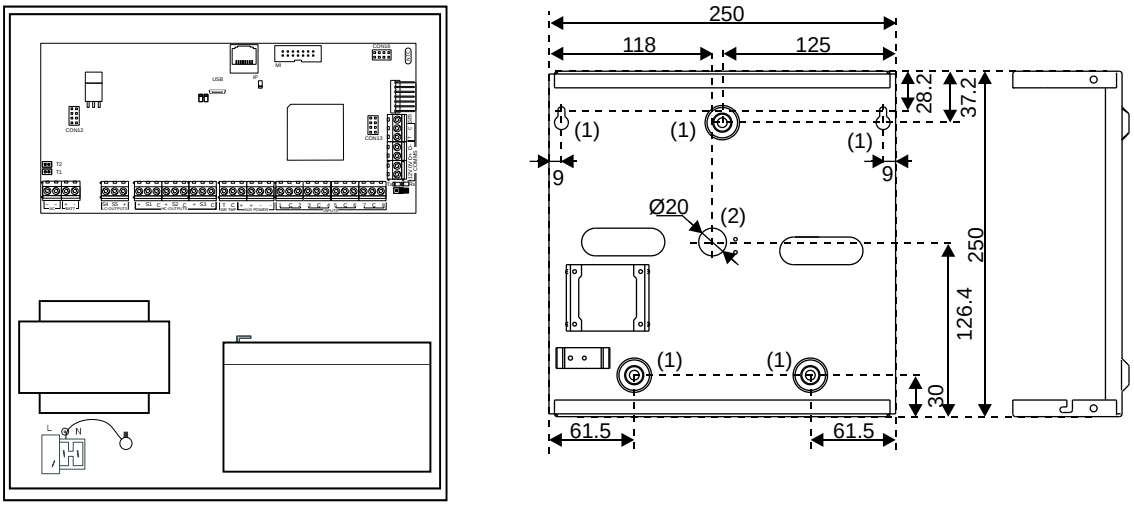


Figure 2: Medium metal housing (-MM)

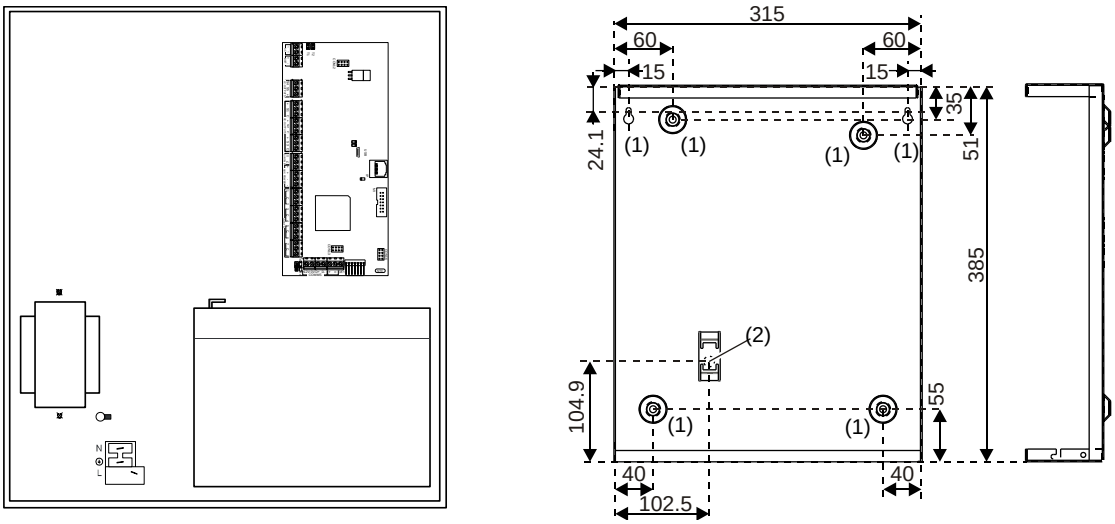


Figure 3: Large polycarbonate housing (-LP)

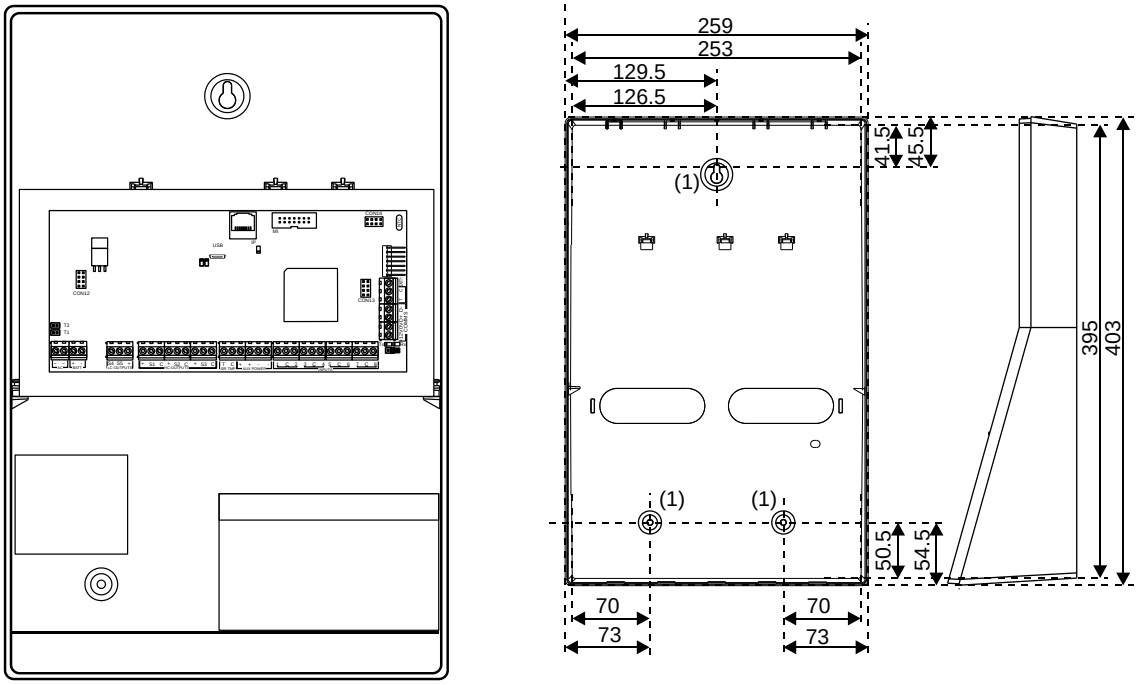
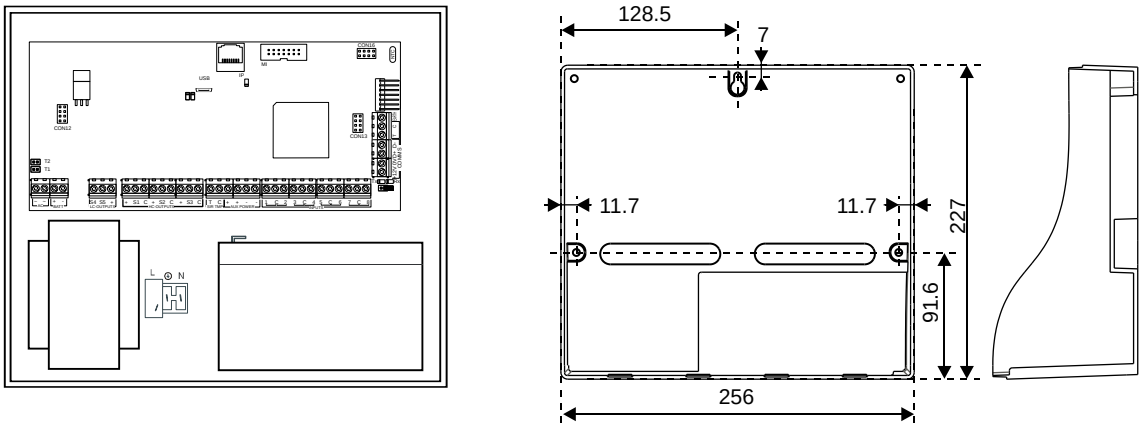


Figure 4: Small polycarbonate housing (-SP)



For more details on connections and connecting devices to the Advisor Advanced, see “Cabling Advisor Advanced” on page 14.

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

Pry-off tamper mounting

For small (-SM) housing, follow the steps in Figure 5 on page 3 to install pry-off tamper. For medium (-MM) housing, follow the steps in Figure 6 on page 3.

Figure 5: Small (-SM) housing pry-off tamper mount

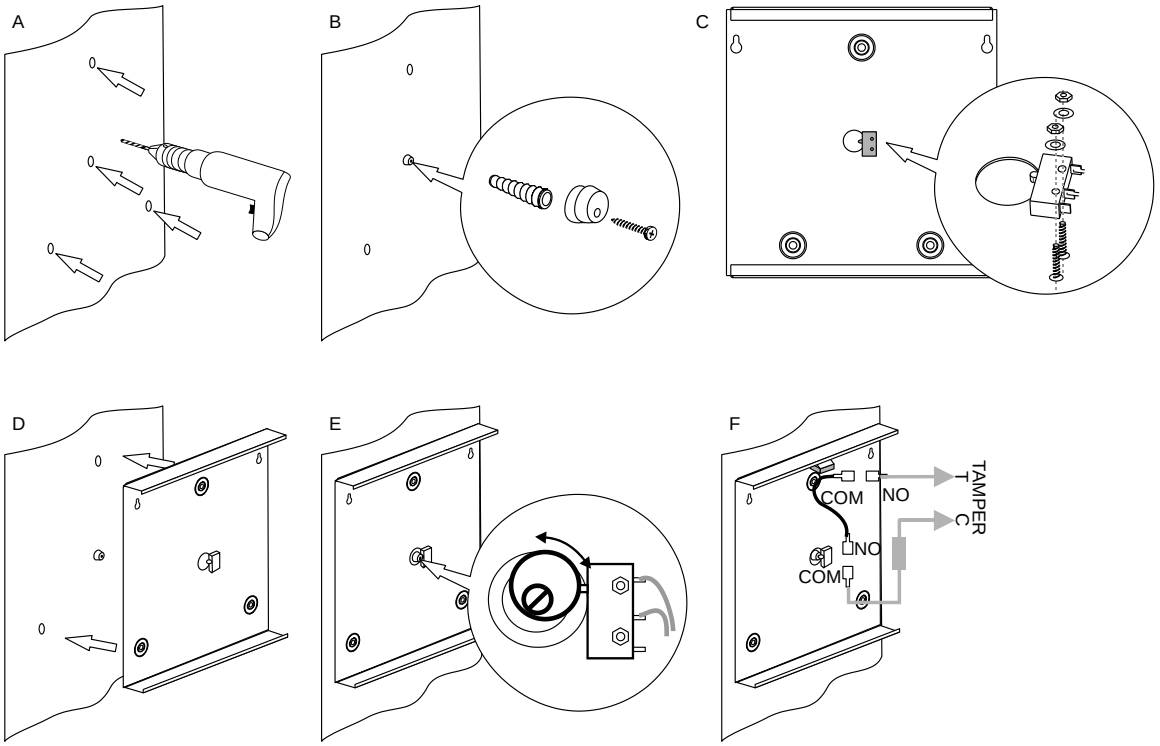
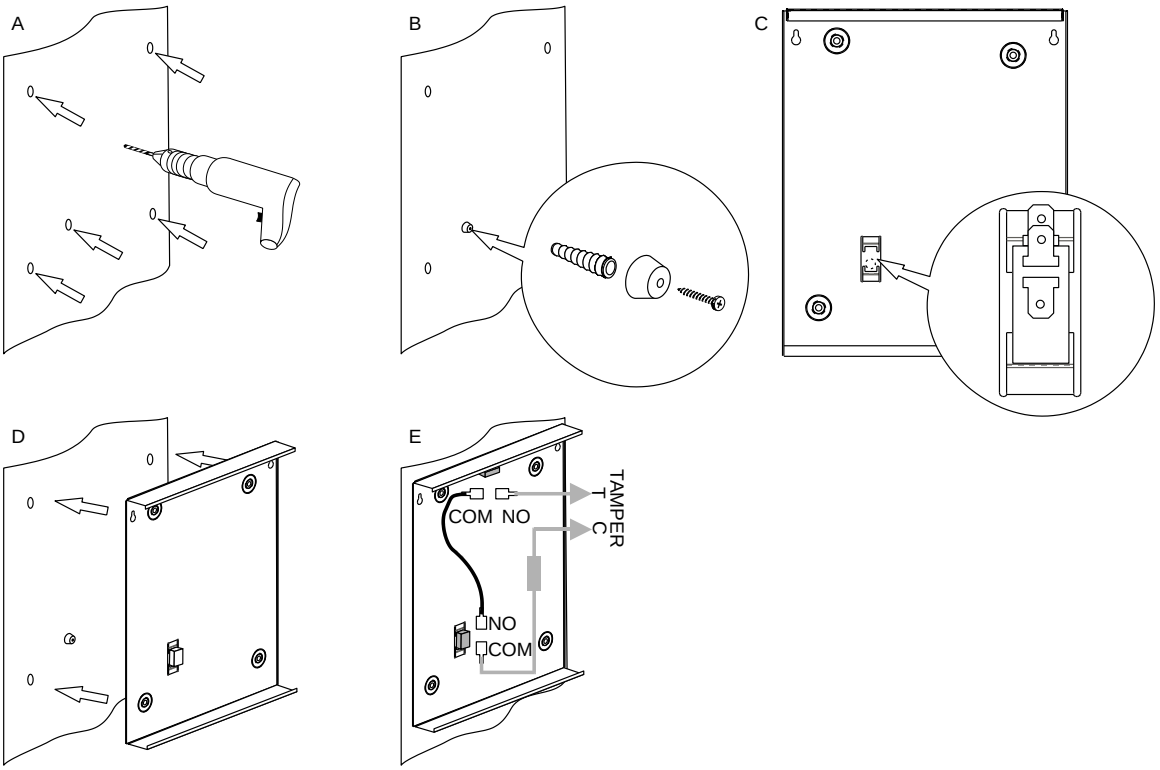
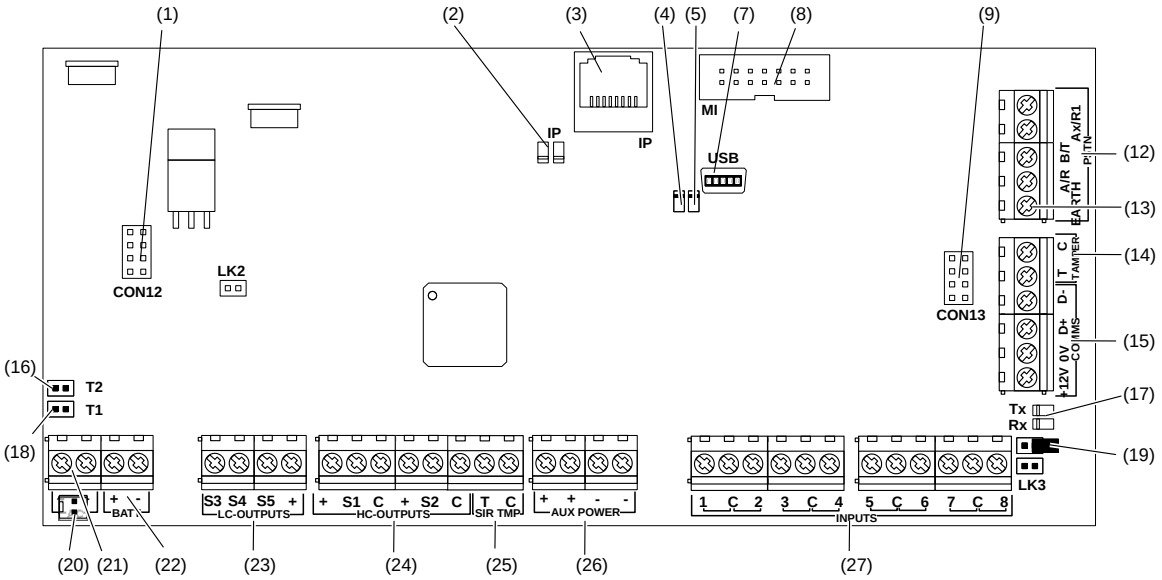


Figure 6: Medium(-MM) housing pry-off tamper mount



Advisor Advanced layout

Figure 7: Advisor Advanced ATSx000A(-IP) PCB layout



(1) Interface to output expander
(2) IP communication LED (ATS-IP only)
(3) Ethernet RJ-45 connector (ATS-IP only)
(4) USB fault LED
(5) USB power LED
(7) USB connector (mini-B type)
(8) MI-bus connector for MI devices
(9) Interface to input expander
(12) PSTN line connection and panel earth terminal
(13) Panel earth terminal
(14) External tamper switch
(15) RS-485 system databus connections
(16) T2: Device firmware upgrade mode (DFU)
(17) RS-485 system databus communication LEDs
(18) T1: Restores the codes of master users (installer and supervisor)
(19) System databus termination jumper
(20) AC power supply connector (ATS1000A-SM only)
(21) AC power supply terminal
(22) Battery connection
(23) Low current (OC) outputs
(24) High current outputs
(25) Siren tamper switch
(26) 12 VDC auxiliary power output
(27) Zone inputs

Keypads and readers

Figure 8: ATS111xA keypad

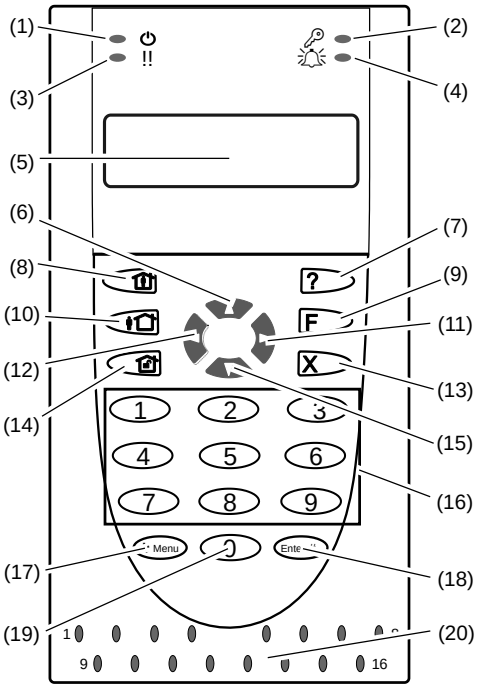
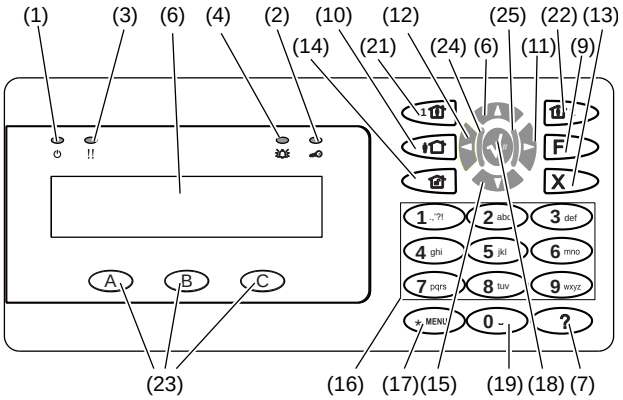


Figure 9: ATS1135 keypad



(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 Enable/disable word library 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 40.
(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 10: ATS1190/ATS1192 readers

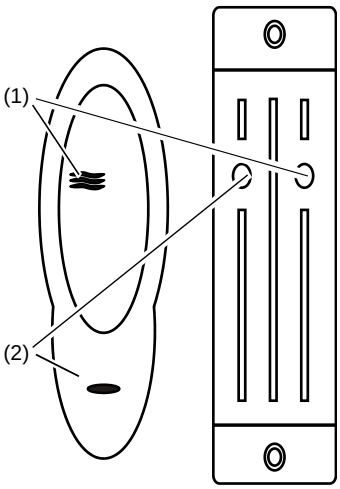


Figure 11: ATS1197 reader with keypad

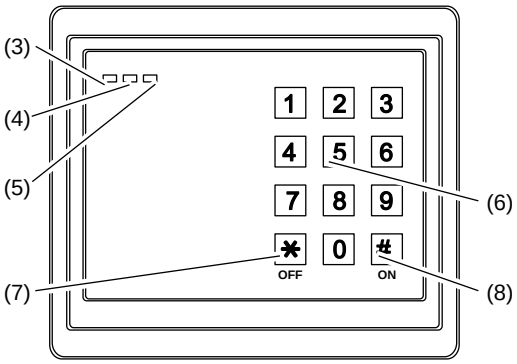
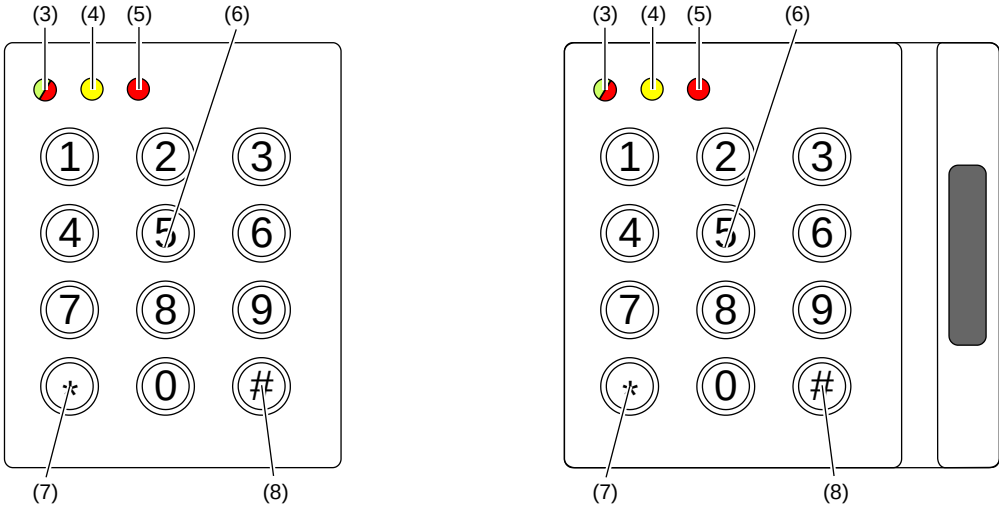


Figure 12: ATS1151/ATS1156 readers



(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, 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 25.
- 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

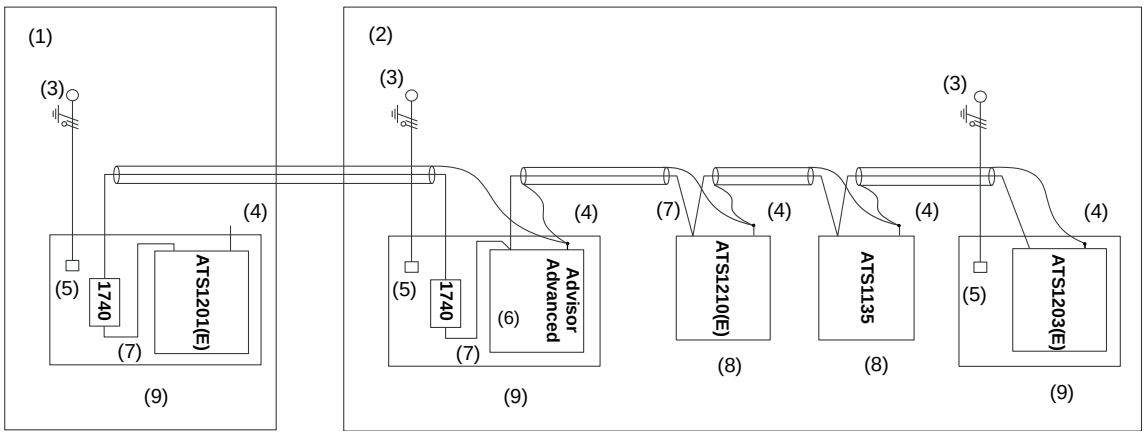
If the wiring extends to separate buildings, more than one common earth system will be used. Use ATS1740 isolator/repeaters to isolate the system databus. In this way the system is protected against variations in earth potential.

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 13 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 13: System shielding



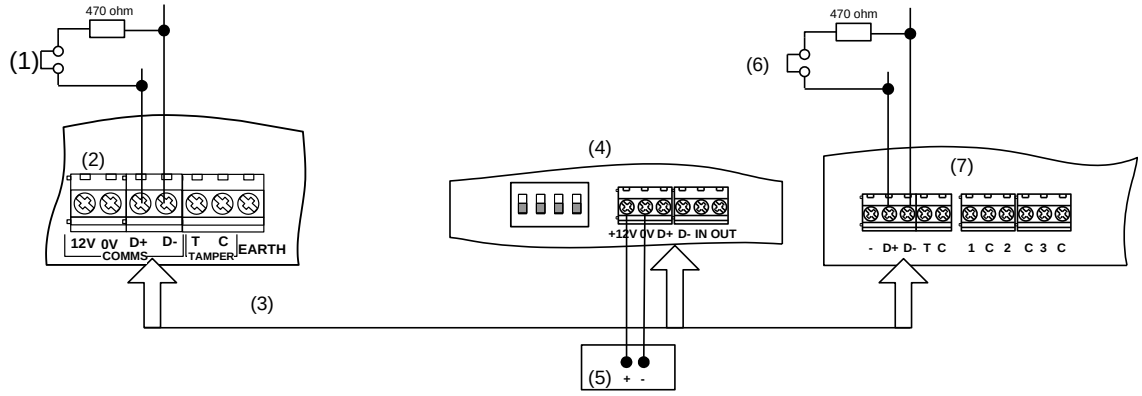
(1) Building 1
(2) Building 2
(3) Mains power with local earth
(4) Earth and shielding
(5) Mains power connector
(6) Advisor Advanced control panel
(7) System databus
(8) Device in plastic housing
(9) Device in metal housing

Cabling Advisor Advanced

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 14: 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 26.

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.

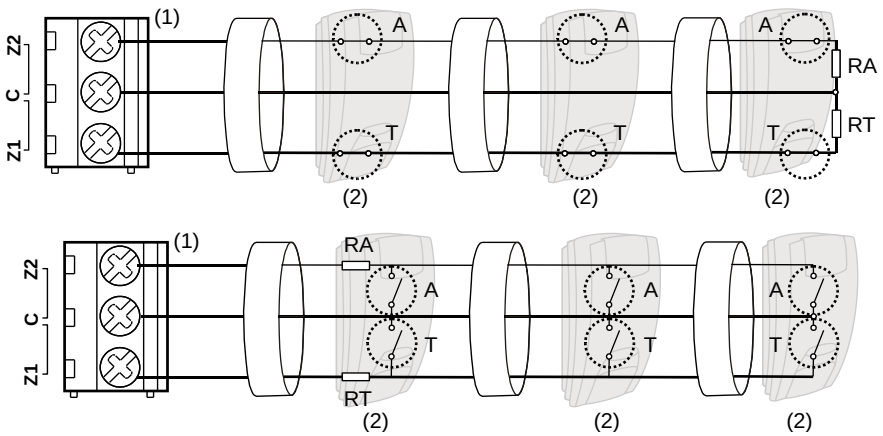
Depending on the detector model, do the following to set up zones:

- Choose your EOL connection type. See “EOL connection types” on page 19.
- Program input mode. See “8.5.1 Input mode” on page 152 for the panel, or “2.2.2.n.4.4 Input mode” on page 76 for expanders.
- Set end-of-line resistor values. See “8.5.2 EOL” on page 152 for the panel, or “2.2.2.n.4.5 EOL” on page 76 for expanders.
- Configure anti-masking option. See “4.1.n.6.6 Anti mask” on page 98.

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 15: Single loop examples



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

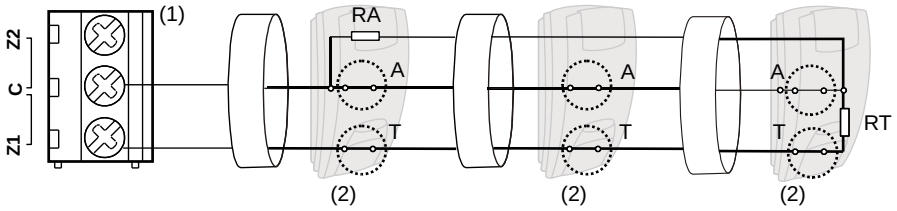
(2) Detector
A Alarm relay
T Tamper relay

Dual loop zone wiring

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

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

Figure 16: Dual loop example



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

Possible EOL connections are listed in “EOL connection types” on page 19.

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]	Zone state						
		Measure [2]	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	—	>11.70
4K7	(Item 3)	R (kΩ)	<1.00	—	1.00–6.67	6.67–16.84	—	>16.84
RA=4.7 kΩ, RT=4.7 kΩ		U (V)	<2.41	—	2.41–8.07	8.07–10.74	—	>10.74

EOL	Connection details [1]	Measure [2]	Zone state					
			Short	Masking	Normal	Alarm	Fault	Open
4K7	(Item 4)	R (kΩ)	<1.00	1.00–3.42	3.42–6.67	6.67–16.84	—	>16.84
RA=4.7 kΩ, RT=2.35 kΩ, RF=2.35 kΩ		U (V)	<2.41	2.41–5.79	5.79–8.07	8.07–10.74	—	>10.74
4K7	(Item 7)	R (kΩ)	<1.00	16.84–55.00	1.00–6.67	6.67–11.75	11.75–16.84	>55.00
RA=4.7 kΩ, RT=4.7 kΩ, RF=10 kΩ		U (V)	<2.41	10.74–12.70	2.41–8.07	8.07–9.82	9.82–10.74	>12.70
2K2	(Item 4)	R (kΩ)	<0.73	0.73–1.47	1.47–2.93	2.93–5.87	—	>5.87
RA=2.2 kΩ, RT=1.1 kΩ, RF=1.1 kΩ		U (V)	<1.90	1.90–3.30	3.30–5.30	5.30–7.70	—	>7.70
6K8	(Item 4)	R (kΩ)	<2.27	2.27–4.53	4.53–9.07	9.07–18.13	—	>18.13
RA=6.8 kΩ, RT=3.4 kΩ, RF=3.4 kΩ		U (V)	<4.50	4.50–6.80	6.80–9.10	9.10–11.00	—	>11.00
5K6	(Item 4)	R (kΩ)	<1.87	1.87–3.73	3.73–7.47	7.47–14.93	—	>14.93
RA=5.6 kΩ, RT=2.8 kΩ, RF=2.8 kΩ		U (V)	<3.90	3.90–6.10	6.10–8.50	8.50–10.50	—	>10.50
3K74	(Item 4)	R (kΩ)	<1.25	1.25–2.45	2.45–4.99	4.99–9.98	—	>9.98
RA=3.74 kΩ, RT=1.87 kΩ, RF=1.87 kΩ		U (V)	<2.90	2.90–4.80	4.80–7.10	7.10–9.40	—	>9.40
3K3	(Item 4)	R (kΩ)	<1.10	1.10–2.20	2.20–4.40	4.40–8.80	—	>8.80
RA=3.3 kΩ, RT=1.65 kΩ, RF=1.65 kΩ		U (V)	<2.60	2.60–4.40	4.40–6.70	6.70–9.00	—	>9.00
2K	(Item 4)	R (kΩ)	<0.67	0.67–1.33	1.33–2.67	2.67–5.33	—	>5.33
RA=2 kΩ, RT=1 kΩ, RF=1 kΩ		U (V)	<1.70	1.70–3.00	3.00–5.00	5.00–7.30	—	>7.30
1K5	(Item 4)	R (kΩ)	<0.50	0.50–1.00	1.00–2.00	2.00–4.00	—	>4.00
RA=1.5 kΩ, RT=0.75 kΩ, RF=0.75 kΩ		U (V)	<1.30	1.30–2.40	2.40–4.10	4.10–6.30	—	>6.30
2K2+4K7	(Item 3)	R (kΩ)	<3.60	—	3.60–5.60	5.60–8.20	—	>8.20
RA=2.2 kΩ, RT=4.7 kΩ		U (V)	<6.00	—	6.00–7.50	7.50–8.80		>8.80

EOL	Connection details [1]	Measure [2]	Zone state: Short	Masking	Normal	Alarm	Fault	Open
1K	(Item 7)	R (kΩ)	<0.51	4.52–40.00	0.51–1.52	1.52–2.94	2.94–4.52	>40.00
RA=1 kΩ, RT=1 kΩ, RF=12 kΩ		U (V)	<1.35	6.24–12.33	1.35–3.36	3.36–5.29	5.29–6.74	>12.33
8K2	(Item 5)	R (kΩ)	<1.50	—	1.50–5.84	5.84–14.25	—	>14.25
RA=8.2 kΩ, RT=8.2 kΩ		U (V)	<3.33	—	3.33–7.52	7.52–10.33	—	>10.33
8K2	(Item 6)	R (kΩ)	<1.50	14.25–45.00	1.50–5.84	5.84–10.07	10.07–14.25	>45.00
RA=8.2 kΩ, RT=8.2 kΩ, RF=8.2 kΩ		U (V)	<3.33	10.33–12.48	3.33–7.52	7.52–9.37	9.37–10.33	>12.48

[1] Refer to Figure 17 on page 19.

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

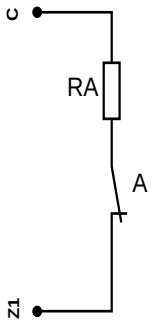
— The state is not available

EOL connection types

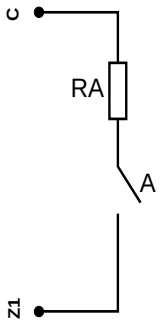
The following EOL connections are used for different input types and EOL values. See “Values for end-of-line resistors” on page 16 for more details.

Figure 17: Connection type

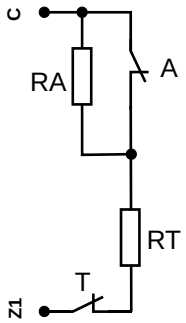
(1) Single NC



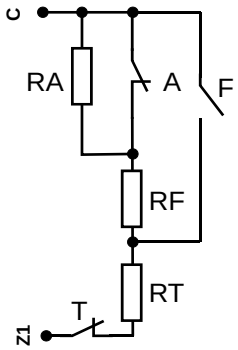
(2) Single NO



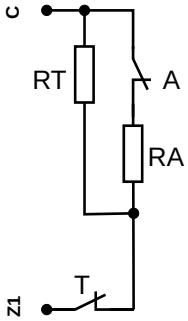
(3) Dual A (default)



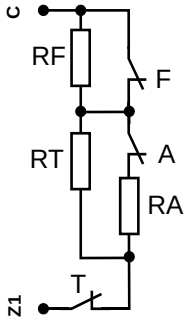
(4) Dual A with AM



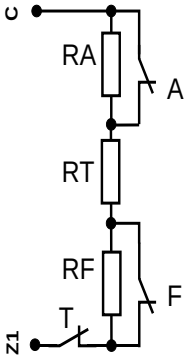
(5) Dual B



(6) Dual C with AM



(7) Dual D with AM



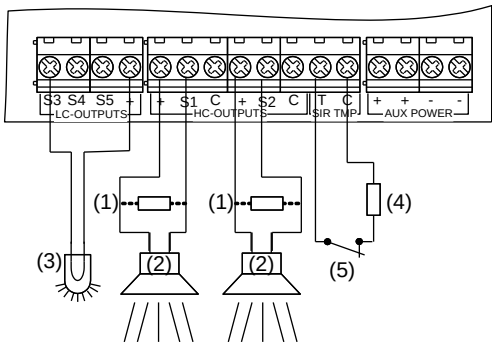
A Alarm relay
T Tamper relay
F Fault / Anti-mask alarm relay

RA Alarm resistor
RT Tamper resistor
RF Fault / Anti-mask alarm resistor

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.6.6 Anti mask” on page 98.

Siren connection

Figure 18: Siren connection examples



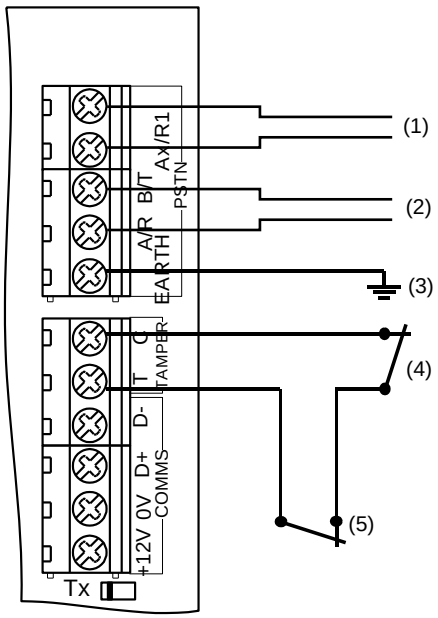
(1) Siren EOL resistor (1 kΩ). It must be installed if siren does not contain a built-in resistor.
(2) Siren.
(3) Beacon, maximum 50 mA.
(4) Siren tamper EOL resistor.
(5) Siren tamper (normally closed).

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 23 and “Filters, outputs, and triggers” on page 116.

Other connections

Tamper connection

Figure 19: Earthing, external tamper, and PSTN connection in ATSx000A(-IP)



(1) Phone (switched)
(2) PSTN line
(3) Earthing
(4) External tamper (normally closed)
(5) Optional pry-off tamper (normally closed) required by EN 50131 Grade 3 and VdS-C regulations

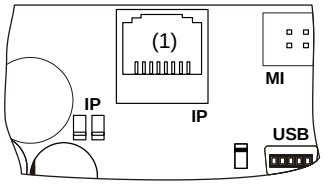
PSTN connection

For ATSx000A(-IP), refer to Figure 19 above.

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 20: 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.

In ATSx000A(-IP), place FTP Ethernet cable through the ferrite, wrap the cable around and bring it through again as it is shown in “Advisor Advanced housings” on page 1. Close ferrite securely.

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 43.

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 26.

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 26.

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 input from zone number 1 to 128 and 257 to 368. See “Specifications > General features” on page 26.

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 26.

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 3 below).

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

To enable the siren output, the programmed output must have the required condition filter assigned (defined by an alarm event or a siren event, depending on the preference settings). See “Filters, outputs, and triggers” on page 116 for more details.

Default output assignments

The default output assignments are shown in Table 3 below.

Table 3: Default output assignments

Output	Name	Type	Default output function
Panel 1	S1	High current output	EN 50131 Grade 3: Internal siren output S1 VdS: External siren output S1
Panel 2	S2	High current output	EN 50131 Grade 3: External siren output S1 VdS: External siren output S2
Panel 3	S3	Low current output	A1 burglar alarm
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 and output addressing

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

Table 4: 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
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

Device	Zones	Outputs	Device	Zones	Outputs
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 [2]	465–496	Keypad 15	—	1113–1120
			Keypad 16	—	1121–1128

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

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

Specifications

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

Mains power specifications

Mains input voltage	230 VAC +10%, −15%, 50 Hz ±10%
Current consumption at 230 VAC:	
ATS1000A(-IP)	300 mA max.
ATS2000A(-IP)	500 mA max.
Transformer output:	
ATS1000A(-IP)-SM/LP	20 VAC, 31 VA
ATSx000A(-IP)-MM	23 VAC, 58 VA

Power supply specifications

Power supply type	Type A per EN 50131-6
Power supply voltage	13.8 V⎓ ±0.2 V
Power supply current:	
ATS1000A(-IP)	1.1 A max. at 13.8 V⎓ ±0.2 V
ATS2000A(-IP)	2.1 A max. at 13.8 V⎓ ±0.2 V
Main board consumption:	
ATSx000A	100 mA at 13.8 V⎓ ±0.2 V
ATSx000A-IP	150 mA at 13.8 V⎓ ±0.2 V
Maximum system current available [1]:	
ATS1000A	1000 mA at 13.8 V⎓ ±0.2 V
ATS1000A-IP	950 mA at 13.8 V⎓ ±0.2 V
ATS2000A	2000 mA at 13.8 V⎓ ±0.2 V
ATS2000A-IP	1950 mA at 13.8 V⎓ ±0.2 V
Auxiliary power output (AUX. POWER) [2]	13.8 V⎓ ±0.2 V, 1 A max.
Battery power output (BAT) [3]	13.8 V⎓ ±0.2 V, 1 A max.
Battery type	Lead acid rechargeable, 7.2 Ah 12 V nom. (BS127) or 18 Ah 12 V nom. (BS131) [4]
Maximum voltage at power supply, auxiliary power output and battery power output	14.5 V⎓
Battery low condition	From 9.5 V⎓ to 10.5 V⎓
Battery test level [5]	11.2 V⎓
Minimum voltage (battery recharging) at power supply, auxiliary power output and battery power output [6]	9.45 V⎓
Maximum ripple voltage V, p-p [7]	100 mV typical, 300 mV max.
Overvoltage trigger value [8]	15.5 V⎓ min.

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

[2] 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 28.

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

[4] The specifications depend on the battery capacity. The above table gives BS127 and BS131 as an example.

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

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

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

[8] Overvoltage protection mechanism monitors the power supply voltage and shuts down the PSU if the voltage raises above indicated value.

General features

Code combinations	From 10,000 (4 digits) to 10 billion (10 digits)
End-of-line resistor	1 kΩ, 1.5 kΩ, 2 kΩ, 2.2 kΩ, 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:	
ATS1000A(-IP)	32
ATS2000A(-IP)	64
Onboard outputs	5 (expandable to 9 with 1X ATS624, or to 21 with 1X ATS626). See “Standard onboard outputs” on page 27.
Maximum output number	128
Areas:	
ATS1000A(-IP)	4
ATS2000A(-IP)	8
Maximum keypad / RAS number	8
Maximum expander / DGP number	7
Maximum user number:	
ATSx000A(-IP)	100
User groups	16
Event log capacity	500
Data retention (log, program settings)	20 years

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	High current electronic output, rating: 1 A at 13.8 V⎓
S3, S4, S5 [1]	Low current electronic output, rating: 50 mA at 13.8 V⎓

[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 vi
EN 50131 grade and class	ATSx000A(-IP): Grade 2, Class II
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	2 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
Mains, mains fuse:	
ATS1000A(-IP)	315 mA, fast 20x5
ATS2000A(-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 8).

Auxiliary current and battery capacity

Table 5: ATS1000A(-IP) maximum available auxiliary current

Battery		7.2 Ah	18 Ah	25 Ah	36 Ah	2x25 Ah	Reference
Discharge time (h)	Charge time (h)	Auxiliary current (mA)					
12	72	500	840	—	—	—	EN 50131 Grade 1 and 2
24	24	200	450	—	—	—	INCERT
36	30	100	380	400	—	—	
30	24	140	380	—	—	—	
60	24	20	190	210	—	—	

Table 6: ATS2000A(-IP) maximal available auxiliary current

Battery		7.2 Ah	18 Ah	25 Ah	36 Ah	2x25 Ah	Reference
Discharge time (h)	Charge time (h)	Auxiliary current (mA)					
12	72	500	1400	—	—	—	EN 50131 Grade 1 and 2
24	24	200	650	875	900	900	INCERT
36	30	100	400	590	800	800	
30	24	140	500	725	785	785	
60	24	20	200	310	455	470	

Example for ATS1000A(-IP) EN Grade 2

When using battery backup as specified for EN Grade 2 using a 7.2 Ah battery, the maximum available auxiliary current is 500 mA.

Common key sequences

The authorization method depends on system settings. See “2.2.1.n.3.5 Login options” on page 70 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 7: Common key sequences for LCD keypad

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

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

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

[2] The functionality depends on “8.7.3 Authorization” on page 155.

[3] The functionality depends on “8.7.8 Easy unset” on page 157.

[4] The functionality depends on “8.7.4 Duress method” on page 155.

[5] Panic alarm functionality depends on the “8.8.1 Panic mode” option described on page 158. It also depends on the “2.2.1.n.3.18 1+3 keys” option described on page 74.

[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 148.

Common key sequences for keypad without LCD

Table 8: Common key sequences for keypad without LCD

Action	Programmed method	Key sequence	[1]
Set [2]	Set with PIN	On, PIN, On	❑
	Set with card	Card	❑
		On, card	❑
		3 x card	❑
	Set with card and PIN	On, card, PIN, On	❑
		Card, PIN, On	❑

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

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

[2] The functionality depends on “8.7.3 Authorization” on page 155.

[3] The functionality depends on “8.7.8 Easy unset” on page 157.

[4] The functionality depends on “8.7.4 Duress method” on page 155.

[5] Panic alarm functionality depends on the “8.8.1 Panic mode” option described on page 158.

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 9 below to describe function keys functionality and availability.

See also “2.2.1.n.3.10 Function keys” on page 72.

Table 9: Function keys

Action	Key	[1]
	A	❑
	B	❑
	C	❑
	F1 (F + 1)	❑
	F2 (F + 2)	❑
	F3 (F + 3)	❑
	F4 (F + 4)	❑

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

Programming sequence

Advisor Advanced control panels feature a wide range of options designed to match varied requirements. This versatility makes correct configuration more demanding. It's important that you use a structured and controlled approach when programming Advisor Advanced systems.

Basic setup

The basic setup covers all settings needed to put an Advisor Advanced control panel into operation with the most common programming.

1. Draw the floor plan and label all zones, equipment, areas etc. Use programming sheets to fill out all information.
2. Perform the initial installation of the control panel (see “Initial start-up” on page 43).
3. Change the installer code using user menu “1.4 Change PIN” (see page 64).
4. Set the correct time and date using menu “8.1.1 Time and date” (see page 138).
5. Program the area options like Area names and entry/exit times using menu “5 Area menu” (see page 113).
6. Use “2.1 Installed remote devices” to enable any keypad or expander connected on the bus.
7. If necessary, configure additional details for keypads using menu “2.2.1 Keypad devices” (see page 68).
8. If necessary, configure additional details for expanders using menu “2.2.2 Expander devices” (see page 75).
9. Program the necessary system-wide input settings using menu “8.5 Zone options” on page 152.
10. Program the necessary zone details like zone type, zone name and reporting options using menu “4 Zones and RF fobs” (see page 94).
11. Program the central station and communications details using menu “9 Dialler menu” (see page 162).
12. Map events to outputs as required using menu “6 Outputs and filters” on page 116.

Advanced setup

The steps given in “Basic setup” above are required for all systems. The following additional steps may be required for advanced installations.

1. Program additional system options using menu “8 System option menu” (see page 138).

2. Program up/download facilities using menu “9.4 PC connection” (see page 188).
3. Program necessary condition filters using menu “6.1 Condition filters” (see page 117).
4. When outputs are used, program menu “6 Outputs and filters” (see page 116).
5. Program the custom LCD text in menu “8.3.2 Custom message” (see page 147).
6. Program shock sensors using menu “4.1.n.7 Gross and Pulse options” (see page 104).
7. Program schedules and actions for them using menu “7 Calendar” on page 127.
8. Program function keys in “2.2.1.n.3.10 Function keys” on page 72.
9. Program wireless devices. See “Wireless device programming” on page 197 for details.
10. Program PIR cameras. See “Using cameras” on page 203 for details.

Test menus

After programming, the system has to be tested. Menus providing support in testing are:

Table 10: User menus with test options

Menu entry	Description
1 Inhibit zones	View and inhibit / uninhibit any zone
2 Isolate zones	View and isolate / de-isolate any zone
3 Display logs	Lists all events that occurred
4 Panel status	Provides system information, including open zones
8 Service menu	Provides walk test and test call

Table 11: Installer menus with test options

Menu entry	Description
1 Service menu	Lists all events that occurred Lists all active zones, tampers and faults Perform various tests and diagnostics Allows reinstalling the system
2 Device menu	Lists all keypads and expanders and their current statuses
4 Zones and RF fobs	Isolates / de-isolates zones
9 Dialler menu	Allows you to ping the selected central station or PC

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 143).

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 141.

The option is enabled in “8.2.6 Challenge code” on page 146.

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 43 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 143) 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 141.

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

Option	Action	Result
Enter the menu entry	Enter menu entry number, or Press Enter or Right to enter the selected one	Jump to a specific menu entry
Show help	Press Help	The description of the selected menu entry is displayed (if available)
Exit the menu entry	Press Left or Clear	Exit the menu entry

You can now select the menu option you want to program. See “Programming Map” on page 251 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 40.

- 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

See also “Word library” on page 41.

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

How to edit a host address

```
Host name
>              <
```

Using the same rules as described in “How to edit text” above, 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 176, 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 menu.

If any faults or any open inputs are present, they are listed the same way as in menu “1.2.4 Alarms and faults” on page 50.

- Press Enter to confirm exit
- Press Clear to return to the programming

Keypad layout

Table 12: ATS111xA keypad layout for entering text

Key	Character sequence
1	a b c A B C 1
2	d e f D E F 2
3	g h i G H I 3
4	j k l J K L 4
5	m n o M N O 5
6	p q r P Q R 6
7	s t u S T U 7
8	v w x V W X 8
9	y z Y Z 9
0	Space . , + – * % 0

Table 13: ATS1135 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.

Word library

The Advisor Advanced panel has a programmable word library that helps you enter user text.

Enable or disable the word library using the Help key. In the display '>' and '<' change to '[' and ']'.

In the word library mode, when the cursor is on the end of the last word in the edited string, the upper line prompts with a word from the library, if there is one.

```
:street
>st_          <
```

Use Up and Down keys to choose a word (if there is more than one).

Use the Enter key to enter the word proposed.

If the typed word does not respond to any word in the library, the system prompts you to save the word.

```
No hint, add?
>stove_       <
```

Use the Partset key if you want to store the word under the cursor.

Word library facility is case-sensitive. For example, the word 'street' is not prompted if you type 'St'.

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 85.

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 “8.7.5 PIN length” described on page 155) 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.

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 14: 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 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 138.
4 Variant	PSTN/ISDN/GSM	PSTN/ISDN/GSM enables onboard soft modem, allowing the appropriate communication path functionality and connection of GSM and ISDN dialers. PSTN, ISDN, GSM and voice communication can be available (depending on the installed modules). PIRCam enables wireless PIR camera functionality and connection of ATS1238 wireless expander. PSTN and ISDN communication paths are unavailable. Only SMS reporting is available via GSM equipment.

* 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. After the installation and the first restart you automatically enter to the programming menu. Next time you will need an authorization to enter the menu.

You can change most of these values later using menu “8.7 Panel and AB options” (see page 154).

See also “1.6 Default panel” on page 65.

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

Service

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:

Table 15: Log types

Entry	Description
1.1.1 All	All events.
1.1.2 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.)
1.1.3 Non mandatory	Events other than mandatory events mentioned above
1.1.4 Installer	Events caused by an installer (programming mode, PC connection etc.)
1.1.5 Access	Access events, like access granted and access denied
1.1.6 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. Lets you 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 ATS1235 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 ATS1235, the value is updated automatically each time the selected zone is activated.

If the wireless detector is equipped with two wireless transmitters, LDR (Low Data Rate) and HDR (High Data Rate), the screen above shows LDR data.

Press Right to toggle between LDR and HDR receiver data, or wait 2 seconds for the screen to scroll automatically.

```
Zone 1
QI=50% [III  ]
```

For more information on the communication quality, refer to the appropriate wireless expander manual.

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 ATS1235 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 fault
- 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 142.

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.

1.2.2 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 104 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&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 Alarms and faults

```
0>All
1 Area 1
```

The Alarms and faults menu provides an overview of all zones that are not in normal state and all faults present in the system. All items scroll automatically.

You can view a single area or all areas together.

Use the Clear or Enter button to exit this view.

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.

This menu 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.

1.2.5.1 Walk test start

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 37 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 53.

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.6.10 Engineer walk test” on page 99).

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 140). 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 “Reporting codes used in Advisor Advanced” on page 223).

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 tested zone activation 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:

Table 16: Walk test frequency

Value	Description
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 Walk test start” on page 51 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 Walk test start” on page 51 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 Walk test start” on page 51.

1.2.5.4 Special WT mode

```
4 Walk test mode
            >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.

1.2.6 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 central station

```
1>Test call mode
2 Period
```

Select central station to configure test call options.

1.2.6.n.1 Test call mode

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

Choose one of the following modes for the automatic test call.

- Off: Automatic test call is disabled.
- Period: Automatic test call recurs at defined intervals.
- Time: Automatic test call occurs every day at a specified time.

1.2.6.n.2 Period / Time

```
1 Period
              >4<
```

If “1.2.6.n.1 Test call mode” on page 54 is set to *Period*, the menu defines the interval between automatic test calls. The allowed range is 0 (never repeat) to 999 hours.

Note: The first test call occurs after a panel restart or a configuration change.

If the option “1.2.6.n.3 Extend” below is set to Yes, the real time of the test call can vary depending on other events reported to the central station.

If “1.2.6.n.1 Test call mode” on page 54 is set to *Time*, the menu defines the time when the test call occurs. The test call time is set in 24 h format, as HH:MM.

1.2.6.n.3 Extend

```
3 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.

Note: The option is only applicable if “1.2.6.n.1 Test call mode” on page 54 is set to Period.

1.2.6.n.4 Freq TC if FTC

```
4 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 depending on the “1.2.6.n.2 Period / Time” option described above.

1.2.6.n.5 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.

1.2.6.n.6 RSSI in report

```
6 RSSI in report
           >Yes<
```

If the option is set to yes, the test call event contains RSSI value as a subevent.

The option is only applicable when GSM communication path reporting is used.

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 in the table below.

Table 17: IP statistics data and functions

Item	Description
1.2.7.n.1.1 TX packets	Number of packets sent
1.2.7.n.1.2 RX packets	Number of packets received
1.2.7.n.1.3 Rej. packets	Number of packets that are rejected by built-in firewall*
1.2.7.n.1.4 TX bytes	Number of bytes sent
1.2.7.n.1.5 RX bytes	Number of bytes received
1.2.7.n.1.6 Clear stat?	This command clears the data described above

* See “9.3.n.7 Firewall” on page 177 for more information.

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 191 for more details. See also “1.2.7.n.2 Ping host” on page 56.

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 168 for more details. See also “1.2.7.n.2 Ping host” on page 56.

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 in Table 18 below.

Table 18: NTP statuses

Status	Description
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.” above.

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 185 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 19: 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.

Table 20: Msg sent 24h submenus

Menu	Description
1.2.8.9.1 All SMSes	All messages.
1.2.8.9.2 Report SMSes	Reporting messages.
1.2.8.9.3 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 183.

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 Test time

```
1 Test time
          > 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

1.2.9.1.m.n.3 Start time

```
3 Start time
         >00:00<
```

Set the time of the day when the device runs an automatic battery test.

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>Test time
2 Run/Stop test
```

Select the appropriate device.

1.2.9.2.m.n.1 Test time

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

Set duration (in minutes) for battery test.

Allowed range is 1 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 Test time” on page 61.

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

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 “Adding a card” on page 86).

Note: The keypad for user card programming is defined in “8.8.6 Card learn-in” on page 159.

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 45.
- 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.

1.3 Panel info

```
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 43 for details.

1.3.2 Defaults

The screen shows panel defaults set during installation.

See “Initial start-up” on page 43 for details.

1.4 Change PIN

```
4>PIN
      **********
```

You can change your own PIN using the Change PIN menu.

The principles of PIN programming are described in “3.1.n.2.1 Change PIN” on page 84.

1.5 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 “1.5.1 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 “1.5.2 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.

1.5.1 Panel lid time

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

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

1.5.2 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.

1.6 Default panel

```
6 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 43 for more details.

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

1.7 Can Inst.time

```
7 Cancel in.time
        Disable?
```

The Cancel installer in-time menu lets you disallow the Installer in function before the Installer in-time expires (see “8.1.3.6 Installer in-time” on page 141).

Note: This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 143.

Use this function after the panel programming is complete. To cancel the installer in-time, 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 143.

Devices

2 Device menu

```
1>Inst. Remotes
2 Edit Rkp&Exp
```

There are two 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.

Bus 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).

Viewing devices

2.1 Installed remote devices

```
>Rkp    R--x----
 Exp     ---?---
```

The Installed remote devices screen shows the status of all connected remote keypads and expanders.

Note: The maximum number of devices allowed on the databus is given in “General features” on page 26.

The line has a list of device states; each device state is shown as one character, which can be one of the following.

Table 21: Device states

Character	State
?	Device is currently being read
x	Device is offline or not supported
I	Device is configured but isolated
R	Keypad is online and configured (polled)
r	Keypad is online, but not configured (new)
D	Expander is online and configured (polled)
d	Expander is online, but not configured (new)
M	MI bus expander is online and configured (polled)

Character	State
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	ATS74xx series IP/GPRS dialler is online and configured (polled)
—	No device

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.

Editing devices

2.2 Edit Keypad&Exp

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

Choose what type of device you want to configure.

Keypads

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 26.

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.

Adding keypad with a higher number

If the number programmed in a keypad is higher than 8, the keypad cannot be added to the system. But it is possible to change this number from the panel via the keypad internal menu. Adding keypad number 9 to 16 brings you to a simplified menu that contains only own keypad menu entry.

For example, to program keypad with programmable number 16:

1. Add keypad 16. It will bring you to “2.2.1.n.4 Keypad menu” (described on page 74).
2. Enter keypad menu.
3. Change keypad address to 7. Refer to the appropriate keypad manual.
4. Add keypad 7.

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
               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

```
3>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 39.

Note: After changing this list, the control of selected areas is also enabled (see “2.2.1.n.3.4 Control areas” on page 70).

2.2.1.n.3.4 Control areas

```
4>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.

2.2.1.n.3.5 Login options

```
1>1xDoor access
              No
```

The menu contains a set of options connected to the login configuration for the selected keypad.

See also “Common key sequences” on page 29.

2.2.1.n.3.5.1 1 x door access

```
1 1xDoor Access
            >No<
```

One-time badge door access allows the selected keypad to control the door with a single badge.

2.2.1.n.3.5.2 Card and PIN mode

```
2 Card&PIN mode
      >PIN only<
```

The Card and PIN mode option allows you to select one of the following control methods.

Table 22: Card & PIN modes

Value	Description
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.3.5.3 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.

Note: If the user privileges allow him to control doors, and “2.2.1.n.3.5.1 1 x door access” on page 70 is set to Yes, the door access is also granted upon one-time badge unset. If there are messages that require acknowledge, the access is granted only after the acknowledgement.

2.2.1.n.3.5.4 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.3.5.2 Card and PIN mode” on page 70 for available modes.
- This functionality is available only if the “2.2.1.n.3.5.3 1 x set/unset” option described on page 70 is not configured as Set-Unset.

2.2.1.n.3.6 EE PIN lock

```
6 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.

2.2.1.n.3.7 Isolate keypad

```
7 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.3.8 Buzzer silent

```
8 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.3.9 Quick set

```
9 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.3.10 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 193 for more details.

Function keys availability depends on the keypad type. See also “2.2.1.n.1 Keypad type” on page 68.

2.2.1.n.3.11 Area ind.LED1

```
11 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 69 and “2.2.1.n.3.4 Control areas” on page 70.

2.2.1.n.3.12 Area ind.LED2

```
12 Area ind.LED2
     >........<
```

Use Area ind.LED2 to program LED 2 indicator in the same way as described in “2.2.1.n.3.11 Area ind.LED1” on page 72.

2.2.1.n.3.13 Status ind.

```
13 Status ind.
          >List<
```

Status indication defines how the area status list is displayed. The following options are available:

- 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.

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

2.2.1.n.3.14 LCD backlight

```
14 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.3.15 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.6.25 ACK on keypad” on page 101 for more details.

2.2.1.n.3.16 EE 1 buzzer

```
16 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 233 for more details.

2.2.1.n.3.17 EE 2 buzzer

```
17 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 235 for more details.

2.2.1.n.3.18 1+3 keys

```
18 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.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.

Expanders

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 26.

Expander options

2.2.2.0 Add expander

```
Expander number
             >_<
```

One 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
         ATS1201
```

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

2.2.2.n.2 Expander address

```
2>Exp address
              01
```

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 78 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 “8.5.1 Input mode” on page 152.

See “Zone connection” on page 15 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 “8.5.2 EOL” on page 152.

See “Zone connection” on page 15 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 a fault 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 203 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 203.

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” above

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 80

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.

Users and user groups

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.

Users

3.1 Users

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

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

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” below for more details.

For each user, the system records these options:

- Number (a panel ID number between 1 and 50)
- Name
- PIN
- Card ID number
- User group (which determines options the user can access)
- Language

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.

Predefined users

There are two users predefined 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.

For more information see “3.2 User groups” on page 89.

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” below, 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 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
     **********
```

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 “8.7.6 PIN chg mode” (see page 155).

PIN length is programmed using “8.7.5 PIN length” on page 155. 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.

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.

See “Remote access” on page 42 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.

Adding a 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 “8.8.6 Card learn-in” on page 159 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 RF fobs > 4.2 RF fobs menu described on page 108.

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 89.

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 170.

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.5 User group options” on page 91 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.5 User group options” on page 91 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*.

3.1.n.8 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:

```
8 Delete user
        >Cancel<
```

Choose Ok and press Enter. This removes the user.

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

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

User groups

3.2 User groups

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

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

What is a user group?

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 options

3.2.0 Add user group

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<
```

There are three types of user groups: Normal user, Installer, and Supervisor. 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.

Table 23 below denotes default and allowed user group options (user privileges).

Table 23: User group types and allowed options [1]

#	Option	User group			
		Normal user	Supervisor	Installer	Guard
1.	Full set	Y (U)	Y (U)	Y	Y (U)
2.	Part set 1	N (U)	Y (U)	Y	Y (U)
3.	Part set 2	N (U)	N (U)	Y	Y (U)
4.	Unset	Y (U)	Y (U)	Y	Y (U)
5.	Inhibit	Y (U)	Y (U)	Y	Y (U)
6.	Isolate	N (U)	N (U)	[Y]	N (U)
7.	Time and date	N (U)	Y (U)	[Y]	Y (U)
8.	User adding (none / restricted / all)	N (U)	Y (U)	[Y]	N (U)
9.	Forced set	N (U)	Y (U)	Y	N (U)
10.	Change PIN	Y (U)	Y (U)	[Y]	Y (U)
11.	Walk test	N (U)	Y (U)	[Y]	Y (U)
12.	Engineer reset	N (U)	Y (U)	[Y]	Y (U)
13.	Duress code	N (U)	Y (U)	Y	Y (U)
14.	Reporting test	N (U)	Y (U)	[Y]	N (U)
15.	Remote connection	N (U)	Y (U)	[Y]	N (U)
16.	Cleaner	Y (U)	Y (U)		N (U)
17.	UG area list	Y (U)	Y (U)	[Y]	Y (U)
18.	Menu access	Y (U)	Y (U)	[Y]	Y (U)
19.	Inst. access	N (U)	Y (U)		N (U)
20.	Logs access	N (U)	Y (U)	[Y]	Y (U)
21.	Stop report	N (U)	N (U)		N (U)
22.	SMS reporting	N (U)	Y (U)	Y	N (U)
23.	SMS control	N (U)	Y (U)	Y	N (U)
24.	Card and PIN mode	Y (U)	Y (U)	Y	Y (U)
25.	No OP/CL reports	N (U)	Y (U)		N (U)
26.	Door access	1 to 16 (U)	1 to 16 (U)		1 to 16 (U)

#	Option	User group			
		Normal user	Supervisor	Installer	Guard
27.	Schedule access	N (U)	Y (U)	[Y]	Y (U)
28.	Fob learning	N (U)	Y (U)	[Y]	N (U)
29.	Remote pics	N (U)	N (U)		N (U)
30.	Pic deletion	N (U)	N (U)		N (U)
31.	CS configuration	N (U)	Y (U)	[Y]	N (U)

Y/N :Default option value (yes or no)

[Y/N]: Option is read only.

(U): Option can be changed by a user programmable function. See “User programmable functions” on page 193.

For detailed descriptions of user group options see “3.2.n.5 User group options” below.

3.2.n.3 User group areas

```
3 UG areas
     >1.......<
```

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

3.2.n.4 User group filter

```
4>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 117.

3.2.n.5 User group options

```
5>UG options
            >>>
```

User group options define the user access rights to the particular options. The following options can be configured.

Table 24: 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 (none / restricted / all)	Create new users (see also “User privilege limitation” on page 93).
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: • PIN only • Card only • Card or PIN
25.	No OP/CL reports	Open/close events are not reported.
26.	Door access	Open doors using selected keypads (1 to 8).
27.	Schedule access	Access to schedule. The following options are available: • None: No access • View: Restricted access. Users can view schedule and cancel actions for the present day. • Configure: Full access.
28.	Fob learning	Program a fob.
29.	Remote pics	Enable remote picture triggering.
30.	Pic deletion	Delete pictures.
31.	CS configuration	Configure CS communication

User privilege limitation

The User adding option (see Table 24 on page 91) determines whether the user can add new users and what user rights these newly created users have.

Table 25: User adding possibilities

Option value	Privileges
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 83.

3.2.n.6 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:

```
6 Remove UG
        >Cancel<
```

Choose Ok and press Enter. This removes the user group.

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

Note: You cannot delete a user group if you have users, actions or central stations assigned to it.

Zones, fobs, and cameras

4 Zones and RF fobs

```
1>Zone menu
2 RF fobs
```

In the Zones and Fobs programming section all zone and fob parameters are programmed. 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.

Zones

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.

Zone options

4.1.0 Add zone

```
1>Panel
2 Input Exp
```

Use the Add zone menu to add a new zone. When adding a zone, specify whether the zone is connected to the control panel PCB, an internal or a remote expander. See “Zone and output addressing” on page 23 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 197.

If the device is a wireless PIR camera, a corresponding camera will be also created in the camera database. See “Cameras” on page 110.

4.1.n Select zone

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

Select an existing zone to program. Every zone has a number between 1 and 16, depending on the location in the system.

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 233).

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 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 233).

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 Excl. in PS1

```
2 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.6.3 Excl. in PS2

See “4.1.n.6.2 Excl. in PS1” above.

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 “8.6.1 Report BA” (see page 153). 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.

4.1.n.6.4 Double knock

```
4 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

141) 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 141).

Note: If the option is active, the option “4.1.n.6.29 Held open” on page 103 is not available.

4.1.n.6.5 Swinger shunt

```
5 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 “8.5.4 Swinger shunt” (see page 153) for one set/unset cycle.

4.1.n.6.6 Anti mask

```
6 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 15 for more details.

4.1.n.6.7 Zone pairing

```
7 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.6.8 Chime

```
8 Chime
           >Off<
```

If the Chime option is On, the zone can be switched off and, depending on “8.8.2 Chime” setting (see page 158), 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.6.9 Soak test

```
9 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.6.10 Engineer walk test

```
10 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 50 for more details.

4.1.n.6.11 User walk test

```
11>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 50 for more details.

4.1.n.6.12 Shock sensor

```
12 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 Gross and Pulse options” (see page 104).

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

4.1.n.6.13 Extend EE

```
13 Extend EE
            >No<
```

If the Extend EE option is Yes, the zone activation expands the entry time for the value defined by “5.n.5 Prealarm time” on page 115.

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

4.1.n.6.14 Final door

```
14 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 140) and the area is set.

4.1.n.6.15 Key latch

```
15 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.6.16 Key set

```
16 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.6.17 Key unset

```
17 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.6.18 Technical full set

```
18 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.6.19 Technical unset

```
19 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.6.20 Technical part set

```
20 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.6.21 Keypad LCD

```
21 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.6.22 Log

```
22 Log
            >No<
```

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

4.1.n.6.23 CS report

```
23 CS report
            >No<
```

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

4.1.n.6.24 Delay timer

```
24 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 142).

4.1.n.6.25 ACK on keypad

```
25 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.6.26 ACK by user” below must be also set for the acknowledgement functionality to work.

4.1.n.6.26 ACK by user

```
26 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.6.25 ACK on keypad” above must be also set for the acknowledgement functionality to work.

See “4.1.n.6.25 ACK on keypad” above for more details.

See also “2.2.1.n.3.15 ACK on keypad” on page 73.

4.1.n.6.27 Sensor type

```
27 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 is the sensor 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 26 below lists events that may be reported for each sensor type.

Table 26: Sensor types and reported events

Sensor Type	Code	Alarm	Alarm restore	Bypass	Unby-pass	Super-vision long	Super-vision 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 “Reporting codes used in Advisor Advanced” on page 223.

4.1.n.6.28 Virtual zone

```
28 Virtual zone
         Not set
```

The menu allows mapping the selected zone to an existing output.

If an output 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.

See also “Outputs” on page 120.

4.1.n.6.29 Held open

```
29 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 142.

Note: If the option is active, the option “4.1.n.6.4 Double knock” on page 97 is not available.

4.1.n.6.30 EE set check

```
30 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.6.31 Alarm in PS1

```
31 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 233
- The zone must be included into part set 1. See “4.1.n.6.2 Excl. in PS1” on page 97.
- Zone functionality does not change if the same zone belongs to an area in full set state.

4.1.n.6.32 Alarm in PS2

The same as “4.1.n.6.31 Alarm in PS1” above, but for part set 2.

4.1.n.6.33 Report as

```
33 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 “Reporting codes used in Advisor Advanced” on page 223 for details.

Notes

- This option is only available for panic type zones. See “Zone types” on page 233.
- 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 158.

Shock sensor options

4.1.n.7 Gross and Pulse options

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

The Gross and Pulse options are valid if the “4.1.n.6.12 Shock sensor” functionality (see page 99) 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 49).

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 27 below.

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 27: 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 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 77 for more details.

4.1.n.7.4 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 28: 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.7.5 Remove RF dev

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

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

Copying 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
             >>>
```

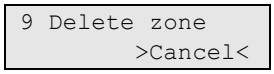
Use the Block assign menu to copy all selected zone parameters to a range of inputs, creating the appropriate zones.

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 104 for more details.

4.1.n.9 Delete zone



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 201 for more details.

Fobs

4.2 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

4.2.0 Add fob

To add a fob, follow one of the procedures described in “Wireless device programming” on page 197.

4.2.n Select fob

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

Select an existing fob to program.

4.2.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.

4.2.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.

4.2.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.

Table 29 on page 109 lists buttons and combinations that are available.

Table 29: 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	—

4.2.n.3.1 Select button

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

Select a button to assign a user function to it. See “User programmable functions” on page 193 for more details.

4.2.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.

4.2.n.4.1 Sensor ID

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

The screen allows you to view the sensor ID.

4.2.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.

4.2.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.

Cameras

For more details on cameras, see also “Using cameras” on page 203.

4.3 Cameras

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

The menu allows you to configure camera modules in wireless PIR cameras.

4.3.n Select camera

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

Select an appropriate camera to configure.

4.3.n.1 Camera name

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

Enter camera name.

4.3.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.

4.3.n.3 Pics by filter

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

Additionally to the zones listed in “4.3.n.2 Pics by zone” above, there can be up to two condition filters that also trigger the camera.

4.3.n.3.m Select filter

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

Select one of two filters to configure.

4.3.n.3.m.1 Choose filter

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

Choose a filter that activates the selected camera.

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

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

Define a type of the condition filter chosen in “4.3.n.3.m Select filter” on page 110.

The available filter types are listed in “Camera event types” on page 203.

4.3.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 “Reporting codes used in Advisor Advanced” on page 223 for details.
- Only particular reporting events are available.

4.3.n.4 Pics by rep ev

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

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

4.3.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 “Reporting codes used in Advisor Advanced” on page 223 for details.
- Only particular reporting events are available.

4.3.n.5 Isolated

```
5 Isolated
            >No<
```

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

4.3.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.

4.3.n.7 Remote pics

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

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

4.3.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.

Areas

5 Area menu

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

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

5.n Select area

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

Select an area to program.

5.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.

5.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 96) or a zone with the final door option (see “4.1.n.6.14 Final door” on page 99) to complete.

Note: If zones are assigned to more then one area, the longest exit time is used. See “4 Zones and RF fobs” on page 94.

5.n.2.1 Exit time 1

5.n.2.2 Exit time 2

Configure exit timers for entry/exit 1 and entry/exit 2 zone types. See “5.n.2 Exit time” above for details on exit timer programming.

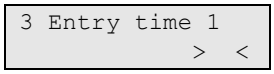
5.n.2.3 PS Exit time 1

5.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 “5.n.2 Exit time” on page 113 for details on exit timer programming.

5.n.3 Entry time



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 “5.n.5 Prealarm time” on page 115 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 then one area, the longest entry and exit time is used. See “4 Zones and RF fobs” on page 94.

5.n.3.1 Entry time 1

5.n.3.2 Entry time 2

Configure entry timers for entry/exit 1 and entry/exit 2 zone types. See “5.n.3 Entry time” above for details on entry timer programming.

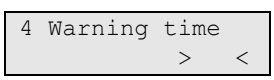
5.n.3.3 PS Entry time 1

5.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 “5.n.3 Entry time” above for details on entry timer programming.

5.n.4 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 “5.n.8 Autoset retry” on page 115.

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

5.n.5 Prealarm time

```
5 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.6.13 Extend EE” described on page 99.

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 then one area, the longest prealarm time is used. See “4 Zones and RF fobs” on page 94.

5.n.7 Entry alarms

```
7 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.

5.n.8 Autoset retry

```
8 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 “5.n.4 Warning time” on page 114). If the autoset has been postponed by a normal user, the system will attempt autoset again after a time period defined in “8.4.7 AS user retry” on page 151.

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

5.n.9 Silent set

```
9 Silent set
           >Off<
```

If Silent set is on, the keypad buzzer remains silent during the “5.n.4 Warning time” described on page 114.

Filters, outputs, and triggers

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.

Condition filters

6.1 Condition filters

```
01>Internal Sir>
02 External Sire
```

A condition filter is an evaluation and a decision-making algorithm. There are 64 pre-programmed filters.

How condition filter works

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 21: 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 118.
2. Change the name of the filter to “Door open” in menu “6.1.n.1 Filter name” on page 118.

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 RF fobs” menu.
4	AND	
5	Area.1.3	Area 1 unset.

The next step is assigning this condition filter to the door lock, connected to output N, which is described in “Door control example” on page 124.

Filter settings

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
            Area
```

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 “Advisor Advanced events” on page 215.

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 the “Advisor Advanced events” on page 215.

The following functions are available for the selected event:

Table 30: Event configuration commands

Menu	Description
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.

Outputs

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 and output addressing” on page 23 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 123.

  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 123. After the time passes, the output activates for a time defined in “6.2.n.7.2 Active time” on page 123, and then it switches off.

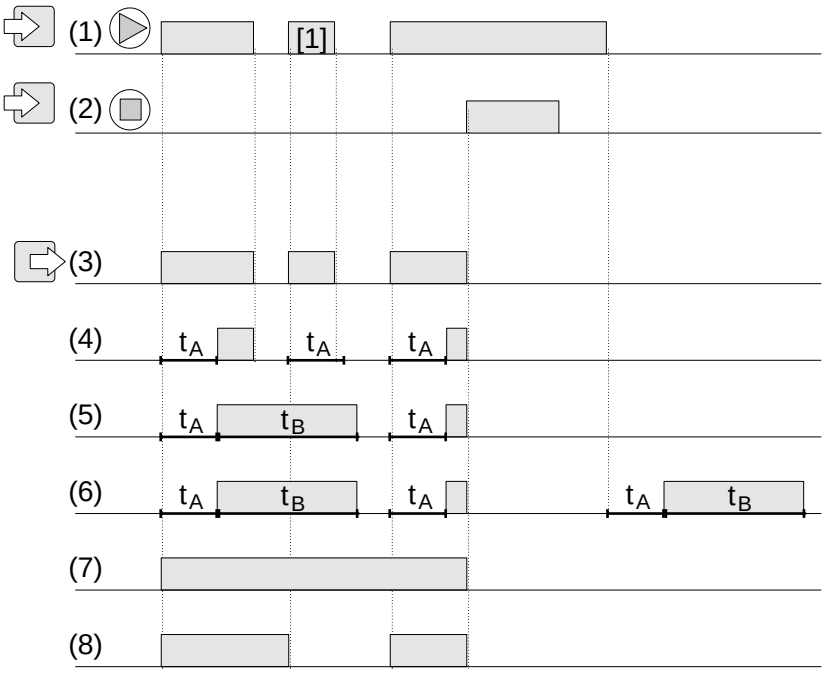
If the stop condition filter is set, its activation deactivates the output and resets both described timers.

- 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 22 below shows examples of described output activation modes.

Figure 22: Output activation mode examples



(1) Start filter
(2) Stop filter
(3) Follow mode without delay
(4) Follow mode with delay
(5) Pulsed mode
(6) Double pulsed mode
(7) Latched mode
(8) Toggled mode
t_A Delay time
t_B Active time

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 123 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 121.

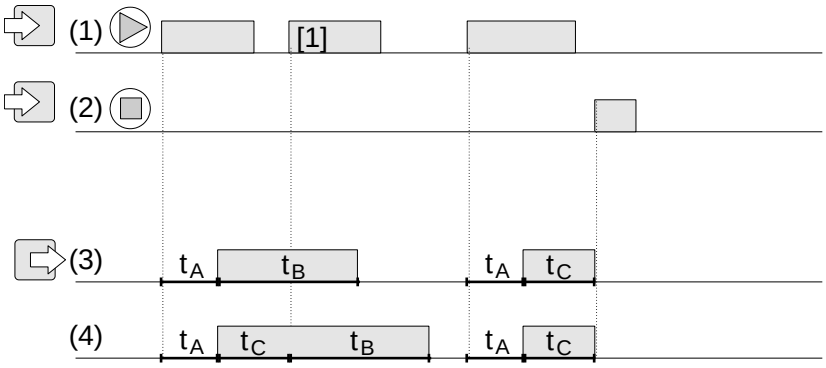
6.2.n.7.3 Retriggerable

```
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 23 below shows the output retrigging when the start filter is reactivated [1].

Figure 23: Output examples



(1) Start filter
(2) Stop filter
(3) Pulsed mode, not retriggerable
(4) Pulsed mode, retriggerable

t_A Delay time
t_B Active time
t_C Interrupted active time

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.

Door control example

To program a door control function described in example on page 117, 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.

See “6.1 Condition filters” on page 117 for more information.

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.

Triggers

6.3 Triggers

```
0>Add trigger
1 Trigger 1
```

The Triggers menu allows you to configure system triggers.

There can be up to 255 triggers in the system. They can be used in condition filters to control outputs remotely. See “6.1 Condition filters” on page 117 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 “7 Calendar” on page 127.
- 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 an appropriate wireless expander installation manual for more information on keyfob programming.
- Advisor Advanced compatible PC software.

See “Advisor Advanced events” on page 215 for more information about trigger flags.

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 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:

```
2 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.

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

Calendar

7 Calendar

```
1>Actions
             >>>
```

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

The Calendar functionality is based on actions. Every action has the following settings:

- Name
- Start time: Day time to trigger the action on
- Condition filter: An additional filter that must be active to enable the action
- Activation: Enabled, disabled, or disabled temporarily
- User function: See “User programmable functions” on page 193.

The actions can be grouped into Action lists, which can contain up to 8 actions.

This menu let you to configure schedule Exceptions. Exceptions represent particular time periods when everyday actions are expanded or substituted by other actions. An example of exception is a holiday, when the premises must stay set for 24 hour.

Finally, this menu provides a Schedule configuration possibility. The Schedule allows configuration of actions taken on a weekly basis.

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. To avoid this scenario, apply appropriate exceptions on programmed daylight change days (see “Exceptions” on page 133).

For more information on daylight saving programming, see “8.1.1 Time and date” on page 138.

Viewing calendar

7.1 View

```
1>Current view
2 Date view
```

Use the View menu to see actions, action plans, and exceptions provided by the selected schedule for the particular day.

This menu also allows users to cancel particular actions planned for the present day.

Note: When calendar settings change, all cancelled actions become active again.

7.1.1 Current view

```
1>Actions
2 Action lists
```

Show actions, action lists, and exceptions scheduled for the current day.

Choose actions, action lists, or exceptions to view.

7.1.2 Date view

```
1 Date
    >01.01.2000<
```

Show actions, action lists, and exceptions scheduled for the selected day.

Enter a date to view.

Next, choose actions, action lists, or exceptions to view.

Actions

7.2 Actions

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

Action is a user programmed function, which can be done automatically by the system according to the programmed schedule. There can be up to 64 programmable actions in the Advisor Advanced system. Each action can be programmed with a number of options. Before going any further, select the action to program.

Action settings

7.2.0 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 Select action

```
1>Name
        Action 1
```

Select an action to program.

7.2.n.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.2 Start time

```
2 Start time
         >00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected action is performed.

7.2.n.3 Active

```
3 Active
           >Off<
```

The Active action menu allows you to disable or enable the action permanently.

7.2.n.4 Function

```
4 Function
              >>>
```

The Function menu lets you to assign a user programmable function that should be executed during this action.

User function programming is described in “User programmable functions” on page 193.

7.2.n.5 Action filter

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

Assign an additional condition filter to the action.

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

See “6.1 Condition filters” on page 117 for more details.

7.2.n.6 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:

```
6 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.

Action lists

7.3 Action lists

```
0>Add Actlst
1 Action list 1
```

Action lists are used to group configured actions. An action list can contain up to 8 actions. Action list provides a name as a common description for these actions, as well as the possibility to enable or disable all of them in one menu.

There can be up to 32 action lists available in the system.

Action list settings

7.3.0 Add action list

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

```
      INFO
  Actlst added
```

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

7.3.n Select action list

```
1>Name
   Action list 1
```

Select an action list to program.

7.3.n.1 Action list name

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

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

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

7.3.n.2 Active

```
4 Active
           >Off<
```

The Active action list menu allows you to disable or enable all actions in this action list permanently.

7.3.n.3 Actions

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

Choose previously configured actions to configure the action list.

An action list can contain up to 8 actions.

Choose “Action” to select an action.

Choose “Remove” to remove an action from the action list.

7.3.n.4 Delete action list

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

The display shows:

```
4 Delete actlst
        >Cancel<
```

Choose Ok and press Enter. This removes the action list.

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

Notes

- You cannot delete an action list unless your user group authorizes you to do so.
- You cannot delete an action list if you have actions assigned to it.

Exceptions

7.4 Exceptions

```
0>Add exception
1 Exception 1
```

Exceptions represent particular time periods when everyday actions are expanded or substituted by other actions. An example of exception is a holiday, when the premises must stay set for 24 hour.

Exception validity note

There can be up to 64 exceptions available in the system. However, if there are a few exceptions valid in the present day, only one exception (with the highest number of all valid exceptions) is applied.

Exception settings

7.4.0 Add exception

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

```
      INFO
Exception added
```

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

7.4.n Select exception

```
1>Name
     Exception 1
```

Select an exception to program.

7.4.n.1 Exception name

```
1 Name
>Exception 1   <
```

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

Use the Exception name screen to enter or edit the exception name. Exception name can contain up to 16 characters.

7.4.n.2 Start date

```
2 Start [dd.mm]
         >01.01<
```

Enter the first day of the exception in DD.MM format.

7.4.n.3 Stop date

```
3 Stop [dd.mm]
         >01.01<
```

Enter the last day of the exception in DD.MM format.

7.4.n.4 Year

```
4 Year
           >All<
```

Enter the year of the selected exception. The allowed range is 2000 to 2099. Value below 2000 is equal to All.

7.4.n.5 Week days

```
1 Monday
           >Yes<
```

Define if the exception is valid for particular days of the week.

7.4.n.6 Substitute

```
6 Substitute
            >On<
```

If the Substitute option is set to On, only actions and action lists assigned to this exception are performed during the exception time. If the option is set to Off, the exception actions are executed together with the other actions that must occur at the configured time.

7.4.n.7 Active

```
7 Active
           >Off<
```

The Exception activation menu allows you to disable or enable the exception permanently.

7.4.n.8 Actions

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

Choose previously configured actions to configure the exception.

An exception can contain up to 4 actions.

Choose “Action” to select an action.

Choose “Remove” to remove an action from the exception.

7.4.n.9 Action lists

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

Choose previously configured action lists to configure the exception.

An exception can contain up to 4 action lists.

Choose “Action list” to select an action.

Choose “Remove” to remove an action list from the exception.

7.4.n.10 Delete exception

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

The display shows:

```
4 Delete excp
        >Cancel<
```

Choose Ok and press Enter. This removes the exception.

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

Notes

- You cannot delete an exception unless your user group authorizes you to do so.
- You cannot delete an exception if you have actions or action lists assigned to it.

Schedules

7.5 Schedules

```
01>Schedule 1
02 Schedule 2
```

Schedules are timed sets of actions with a weekly structure. Each schedule can contain actions and action lists assigned to particular days of the week.

Schedule settings

7.5.n Select schedule

```
1>Name
      Schedule 1
```

Select a schedule to program. There can be up to 4 schedules in the system.

Note: Only one schedule can be processed at a time. If there are more active schedules on a particular date, the one with the highest number is processed. For example, if schedules 2 and 4 are active, only schedule 4 actions are executed.

7.5.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. Schedule name can contain up to 16 characters.

7.5.n.2 Active

```
2 Active
           >Off<
```

If set to On, the schedule is active.

7.5.n.3 Start date

```
3 Start [dd.mm]
         >01.01<
```

Enter the first day of the schedule in DD.MM format.

7.5.n.4 Stop date

```
4 Stop [dd.mm]
         >01.01<
```

Enter the last day of the schedule in DD.MM format.

7.5.n.5 Week days

```
1>Monday
2 Tuesday
```

The Week days menu allows you to assign actions and action lists to each day of the week.

Choose a day of the week to assign actions and action lists.

```
1>Actions
2 Action lists
```

Go to the Actions submenu to assign or remove actions for the selected day of the week.

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

Choose previously configured actions to configure the schedule.

There can be 16 actions programmed.
Choose “Action” to select an action.
Choose “Remove” to remove an action from the selected day.
Go to the Action lists submenu to assign or remove action lists for the selected day of the week.

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

Choose previously configured action lists to configure the schedule.

There can be 4 action lists programmed.

Choose “Action list” to select an action.
Choose “Remove” to remove an action list from the selected day.

7.5.n.6 Exceptions

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

You can assign up to 64 exceptions to the schedule. See “7.4 Exceptions” on page 133 for more details.

7.5.n.7 View

```
1>Current view
2 Date view
```

Use the View menu to see actions, action plans, and exceptions planned for the particular day according to selected schedule.

This menu is similar to “7.1 View” described on page 127, except it applies only to the selected schedule.

This menu also allows users to cancel particular actions planned.

Note: When calendar settings change, all cancelled actions become active again.

System options

8 System option menu

```
1>Timer menu
2 Engineer opt
```

Use the System menu to program the global system options including timers.

Timer options

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.

Table 31: Time and date menu options

Option	Note
8.1.1.1 Time zone	The system time zone.
8.1.1.2 Date	Date format is DD-MM-YYYY.
8.1.1.3 Time	Time format is 24 hours.
8.1.1.4 DST start mth	The DST start month.
8.1.1.5 DST start wk	The DST start week. The available options are: 1st week, 2nd week, 3rd week, 4th week, last week.
8.1.1.6 DST end mth	As above.
8.1.1.7 DST end wk	As above.
8.1.1.8 Set correction	Allows configuring time correction if necessary.
8.1.1.8.1 Time/7days	This submenu allows setting the time correction that is performed each 7 days of panel work. Maximum value is 5 min 40 s. Positive value means the clock is set forward, negative — backward.

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

Note: See “Daylight saving note” on page 127 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 54.

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 143). 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.6.9 Soak test” on page 98) 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.6.29 Held open” on page 103.

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 48.

Engineer options

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 212 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.

Engineer reset procedure

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 146.
- 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 145, 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 96). 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.

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 149).

This option is ignored in case AB alarm confirmation is enabled. For more information see “8.2.4.4 Confirmed alarm” below.

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 is 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 143.

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 procedure” on page 143 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 procedure” on page 143.

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 procedure” on page 143 for more information.

8.2.5 Cancel in.time

```
5 Cancel in.time
        Disable?
```

The Cancel installer in-time menu lets you disallow the Installer in function before the Installer in-time expires (see “8.1.3.6 Installer in-time” on page 141).

Note: This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 143.

Use this function after the panel programming is complete. To cancel the installer in-time, 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 35.

8.2.6 Challenge code

```
6 Challenge code
              No
```

Use this menu to activate challenge code functionality. See “Challenge code requirement” on page 35 for more details.

Caution: Once activated, this option cannot be deactivated by software settings.

8.2.7 Remote configuration

```
7 Remote config
             Yes
```

If the option is set to Yes, it is allowed to change panel settings remotely via configuration software when the panel is set. Otherwise, the panel must be unset prior to remote programming.

LCD display options

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 140).

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:

Table 32: Armed display options

Option	Description
8.3.1.1 Off	Armed display is disabled.
8.3.1.2 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).
8.3.1.3 Always	Armed display always activates. No status information is displayed on keypad LCD and LEDs (except mains LED and Alert message).
8.3.1.4 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 “Common key sequences” on page 29.
- 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 147 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.

Set options

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.

Table 33: Ready To Set conditions

Condition	Description
8.4.1.1 Zone alarm	Active zone
8.4.1.2 Zone panic	Hold-up device active
8.4.1.3 Zone masking	Masking / fault state on input
8.4.1.4 Zone fault	Intrusion detector fault
8.4.1.5 Zone tamper	Tamper in zone
8.4.1.6 Interconnection fault	A critical error caused by communication trouble between internal panel components
8.4.1.7 Mains fault	Mains fault, including external fault
8.4.1.8 Battery fault	Battery fault, including external fault
8.4.1.9 FTC (Failed to Communicate)	Alarm reporting has failed to deliver events
8.4.1.10 Siren fault	Siren output fault
8.4.1.11 Zone technical	An alarm in the technical zone
8.4.1.12 Keypad fault	A fault reported by keypad
8.4.1.13 Expander fault	A fault reported by remote expander
8.4.1.14 Comms fault	All transmission paths are down (no communication)
8.4.1.15 Engineer reset	Engineer reset requirement
8.4.1.16 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.

Table 34: Inhibit inclusion options

Condition	Description
8.4.2.1 Zone panic	Holdup device active
8.4.2.2 Zone masking	Masking / fault state on input

Condition	Description
8.4.2.3 Zone fault	Intrusion detector fault
8.4.2.4 Zone tamper	Tamper in zone
8.4.2.5 Interconnection fault	A critical error caused by communication trouble between internal panel components
8.4.2.6 Mains fault	Mains fault, including external fault
8.4.2.7 Battery fault	Battery fault, including external fault
8.4.2.8 FTC (Failed to Communicate)	Reporting attempts are failed
8.4.2.9 Siren fault	Siren output fault
8.4.2.10 Zone technical	An alarm in the technical zone
8.4.2.11 Keypad fault	A fault reported by keypad
8.4.2.12 Expander fault	A fault reported by remote expander
8.4.2.13 Comms fault	All transmission paths are down (no communication)
8.4.2.14 Engineer reset	Engineer reset requirement
8.4.2.15 Siren tamper	Siren tamper active

8.4.3 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.

8.4.4 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.

Table 35: Forced set options

Option	Description
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.

8.4.5 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.

8.4.6 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 196 for more details.

8.4.7 AS user retry

```
6 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 196 for more details.

The user must have a privilege for full setting to be allowed to postpone the autoset. See “3.2.n.5 User group options” on page 91 for more details.

Zones

8.5 Zone options

```
1>Input mode
       Dual loop
```

The Input options menu defines options of zone inputs.

8.5.1 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 “8.5.2 EOL” below, normal state for Single NO zone is open.
- Single NC: Similar to Single NO above, but If EOL is disabled in “8.5.2 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 “8.5.2 EOL” below. See “Zone connection” on page 15 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 76.

8.5.2 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 “8.5.1 Input mode” option above.

See “Zone connection” on page 15 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 76.

8.5.3 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 “8.5.2 EOL” on page 152.

8.5.4 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.6.5 Swinger shunt” option enabled (see page 98).

8.5.5 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.

Part set options

8.6 Part set

```
1>Report BA
             Yes
```

The Part set menu allows you to configure the part set options.

8.6.1 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.

8.6.2 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.

8.6.3 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 “5.n.2 Exit time” on page 113 must be longer than 0.

8.6.4 PS1 name

8.6.5 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.

Panel and AB options

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 43.

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 40.

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 43, and “Predefined users” on page 83.

8.7.3 Authorization

```
3 Authorization
      >Card&PIN<
```

The Authorization menu allows you to change the panel authorization method.

8.7.4 Duress method

```
4 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.

8.7.5 PIN length

```
5 PIN length
            >  <
```

The PIN length menu allows you to change the PIN length. See “3.1.n.2.1 Change PIN” on page 84 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 85 for details.

8.7.6 PIN chg mode

```
6 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 84 for more details.

8.7.7 Alarm confirm

```
1>AB mode
             >>>
```

The Alarm confirm menu allows you to set a various options connected to the alarm verification.

8.7.7.1 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.

8.7.7.2 AB time

```
1>Intr. AB time
               1
```

The menu allows you to configure the maximum delay between A and B alarms.

8.7.7.2.1 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.

8.7.7.2.2 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 “8.7.7.2.1 Intrusion AB time” above.

8.7.7.3 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.

8.7.7.4 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.

8.7.7.5 EE inhibit

```
5 EE inhibit
    >Entry/Exit<
```

The EE inhibit 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.

8.7.7.6 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.

8.7.7.7 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 “8.7.7.1 AB mode” on page 155.

8.7.7.8 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.

8.7.7.9 Reporting delayed

```
9 Rep. delayed
           >Yes<
```

Enable a 30-second delay before alarm reporting required by ACPO regulations.

8.7.8 Easy unset

```
8 Easy unset
           >Yes<
```

If enabled, you can unset premises entering a PIN or badging a valid card without pressing any other keys.

Other options

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.

Table 36: Panic modes

Option	Description
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

```
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 retrig.
            >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 Short sup. and IP polling

```
5 Spvn&IP poll
        >Always<
```

The option defines when wireless devices short supervision and OH IP polling events are indicated. The following options are available:

- Always: Short supervision and IP polling events are always shown.
- On set: Short supervision and IP polling events are displayed only when system set attempt.

See also “2.2.2.n.4.4.1 Short superv.” on page 77 and “9.1.n.8.3.2 Heartbeat time” on page 169.

8.8.6 Card learn-in

```
6 Card learn-in
      >Keypad 1<
```

Choose a keypad for user card learning. See also “3.1.n.3 User card” on page 85.

8.8.7 Test inputs

```
7 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 46. The following options are available:

- All: All inputs are visible.
- If used: Only the inputs assigned to the existing zones are visible.

8.8.8 Buzzer mode

```
8 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.

8.8.9 Card number

```
10 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.

Library

8.9 Library

```
01>Alarm
02 Area
```

The Library menu allows you to view or delete words stored in the “Word library” (see page 41).

You can choose a word to delete. It is not possible to add or edit words from this menu. Library words can be added only while editing text using word library switched on. See “Word library” on page 41 for more information.

Communications

9 Dialler menu

```
1>CS
2 Event options
```

The menu is used to program all system-wide communication options.

Central stations

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 168
- “IP and GSM/GPRS specific options” on page 168
- “Photo transmission specific options” on page 170
- “GSM/phone specific options” on page 170

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 173.

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” on page 163, 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 167 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 165).

- 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 163). 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 “Alarm reporting principles” on page 206 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 208 for more information.

The value ranges from 1 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 164.

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 166).

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 164 for more details.

9.1.n.10 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 39.

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” above.

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 56 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" above.

Photo transmission specific options

Additionally to “IP and GSM/GPRS specific options” described on page 168, it is necessary to set the options below.

9.1.n.4.4 Vid dest port

```
4 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 168.

9.1.n.4.5 Encryption

```
5 Encryption
             >No<
```

If the Encryption option is set to Yes, the pictures are sent encrypted with AES algorithm.

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” on page 171 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” on page 171.
- 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” on page 171.

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 87.
- The SMS reporting must be enabled for these users. See “3.1.n.7.2 SMS reporting” on page 88.
- At least one of the user groups must allow these users to receive SMS reports. See “3.2.n.5 User group options” on page 91).

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” on page 170 for parameters description.

Events

9.2 Event options

```
1>CS mapping
2 Voice mapping
```

The Event options menu contains event options.

See “Alarm reporting principles” on page 206 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 “Reporting codes used in Advisor Advanced” on page 223.

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 the “Reporting codes used in Advisor Advanced” on page 223.

9.2.3 Delayed events

```
00>Delay timer
              0
```

The Delayed events menu allows you to set a delay for particular events.

The first menu entry, 9.2.3.0 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 the “Reporting codes used in Advisor Advanced” on page 223.

Communication paths

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:

- PSTN
- IP

Depending on the hardware configuration, the following transmission paths may also be available:

- ISDN
- GSM
- TDA74xx

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

- “PSTN specific options” on page 174
- “ISDN specific options” on page 175
- “IP specific options” on page 175
- “GSM/SMS/GPRS specific options” on page 178

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.

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 Dialling menu allows you to select the PSTN dial mode: pulse or tone (DTMF).

9.3.n.7 Ring count

```
7 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 the incoming calls are not answered at all.

9.3.n.8 Encryption

```
8 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 190.

Note: IP connection is always encrypted. USB communication does not use encryption.

ISDN specific options

9.3.n.6 MSN

```
6 MSN
```

The MSN option lets you enter the ISDN MSN number.

9.3.n.7 Ring count

See “9.3.n.7 Ring count” above.

9.3.n.8 Encryption

See “9.3.n.8 Encryption” above.

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 175 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 176.

9.3.n.6 NTP config

```
6 NTP config
        >Static<
```

The NTP config menu is used to configure the NTP (Network Time Protocol) server.

It is configured in the same way as DNS server in menu “9.3.n.5 DNS config” on page 176.

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 191.

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 182 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 58 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 59 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 59 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 179.

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 59.

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 179.

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” below.

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” above.

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 183 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” on page 181.

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 ATS7310 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.5 User group options" on page 91)
- Have their phone numbers configured (see "3.1.n.7.1 User phone" on page 87)

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 164

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 175.

9.3.n.7.5 DNS config

See “9.3.n.5 DNS config” on page 176.

9.3.n.7.6 Firewall

See “9.3.n.7 Firewall” on page 177.

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 178.

9.3.n.8 Ring setup

```
1>Ring count
2 Omit 1st call
```

The menu contains ringing configuration options.

9.3.n.8.1 Ring count

See “9.3.n.7 Ring count” on page 175.

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” above, and answers immediately to the second incoming call received within 30 seconds after the first one.

If set to No, the panel answers after a number of incoming rings programmed in “9.3.n.8.1 Ring count”.

9.3.n.9 Encryption

See “9.3.n.8 Encryption” on page 175.

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 184 for details.

9.3.n.10.3 User name

See “9.3.n.7.2 User name” on page 184 for details.

9.3.n.10.4 User password

See “9.3.n.7.3 User password” on page 184 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 GPRS transmission 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.

PC connections

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 connection

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 190
- “IP and GSM/GPRS specific options” on page 191
- “GSM specific options” on page 192

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 pespectively.

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 189. 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
>000000000000<
```

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.8 Encryption” on page 175. USB communication is never encrypted.

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 and GSM/GPRS 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 39.

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.

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 185 for more details.

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.

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 using submenu 1.

Next, configure function parameters in submenu 2.

Available parameters depend on the selected function type. For particular types submenu 2 is 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 37: Available function types and parameters

Type	Description	Available parameters
None	No function is assigned	None
Set	Set areas [1][2]	1. Areas selection 2. User code requirement
Unset	Unset areas [1]	1. Areas 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
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

Type	Description	Available parameters
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. 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.5 User group options” on page 91 for more 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 139. 2. User code requirement.
Test pic to CS	Take a picture and send it to a central station	1. Camera 2. Central station
Fire	Raise a fire alarm	None
Medical alarm	Raise a medical alarm	None
Show inhibited	Show inhibited or isolated zones, keypads, and expanders.	None
GSM credit	Check GSM credit	None

[1] Depending on system settings, the function may require logging in of a user with the appropriate privileges. See “2.2.1.n.3.9 Quick set” on page 72 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 “5.n.4 Warning time” on page 114 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.

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

- Schedule. See “Calendar” on page 127 for more details.
- Function key. See “Function keys” on page 32 and “2.2.1.n.3.10 Function keys” on page 72.
- Fob. See “Fobs” on page 108 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 “7.2 Actions” on page 129, create an action with Set function. See also “User programmable functions” on page 193.
- Configure an appropriate schedule as described in menu “7.5 Schedules” on page 136 and make sure it is active.
- Enable or disable “5.n.9 Silent set” option on page 115.
- If necessary, set “5.n.8 Autoset retry” option on page 115.

  If Set retry is allowed, configure “8.4.7 AS user retry” on page 151.
- Set “5.n.4 Warning time” option on page 114 as well.
- Optionally, configure “8.4.6 AS fault retry” option on page 151.

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 95.

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

2. Select zone location.

```
Learn mode
    >Sequential<
```

3. Choose Sequential mode and press Enter.

```
Input number
            > 2<
```

4. Choose an input number.

   Note: Depending on the hardware configuration, door/window and shock sensors can require two wireless zones to report main sensor and auxiliary input states. In this case, two unoccupied consecutive zones are required. See “Two-zone RF sensors” on page 201 for more details.

```
      INFO
  Tamper RF 1
```

5. Activate the wireless device. See “Device activation” on page 202 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 95.

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

2. Select zone location.

   ```
   Learn mode
           >Manual<
   ```

3. Choose Manual mode and press Enter.

   ```
   Input number
               > 2<
   ```

4. Enter the input number.

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

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

5. Activate the device, or press Enter to enter the wireless device identifier manually. See “Device activation” on page 202 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<nnnnnnn>”. For example, “Tx H103EB2B” mark identifies a sensor with the ID 103EB2B. See also “4.1.n.7.1 Sensor ID” on page 105 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 201.

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 203 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 “4.2.0 Add fob” menu described on page 108.

```
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 202 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 “4.2.0 Add fob” menu described on page 108.

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

2. Select zone location.

```
Learn mode
        >Manual<
```

3. Choose Manual mode and press Enter.

```
Input number
             > <
```

4. Enter the input number.

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

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

5. Press the programming key sequence to activate the fob, or press Enter to enter fob identifier and fob encryption key manually. See “Device activation” on page 202 for more information about activation.

```
Fob ID
     >         <
```

```
Fob key
     >         <
```

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

```
      INFO
   Fob exists
```

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

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

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

```
     INFO
  Fob learned
```

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

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

Chose Yes and press Enter to edit fob settings.

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

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

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

Two-zone RF sensors

Particular RF devices, for example, door/window sensors and shock sensors, have two inputs onboard. 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 38 on page 202 for more details.

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

If 1 zone is selected, this zone functionality depends on sensor configuration. See “4.1.n.7.4 Sensor opt” on page 105.

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
```

Note: If the expander is configured for 32 zones range, a device cannot occupy expander inputs 16 and 17, because the lower and the higher zone range of such expander are not adjacent. See “2.2.2.n.4.6 Expander mode” on page 78 for more details.

Device activation

Depending on the device type, the learning activation of this device can differ. Table 38 below lists all compatible devices and their activation methods.

Table 38: 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	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 “4.3.n.2 Pics by zone” on page 110.

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

  See also “Zone types” on page 233.
- Activation of a condition filter. The event type is defined for the programmed filter. See “4.3 Cameras” on page 110.
- Activation of a standard reporting event. See “4.3.n.4 Pics by rep ev” on page 111.
- 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, firedoor 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 “4.3.n.3.m.2 Event type <n>” on page 111.
- Custom type 2. Generated by conditional filters of this type.

Event type details are listed in Table 39 on page 204.

Table 39: 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 “Reporting codes used in Advisor Advanced” on page 223.

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

[4] See “4.3.n.3.m.3 Report as” on page 111 for details.

Each of these types can be configured in “2.2.2.n.4.9.1 Pic settings” on page 79.

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 “Devices” on page 66 for more details.
2. Program a wireless PIR camera as a wireless PIR detector. See “Wireless device programming” on page 197 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 “4.3 Cameras” on page 110.
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 “4.3.n.2 Pics by zone” on page 110.

   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 “4.3 Cameras” on page 110 for details.
6. If necessary, program reporting events that activate the camera. See “4.3 Cameras” on page 110 for details.

Diagnostics

If necessary, use the following menus for diagnostics:

- “1.2.1.3 RF RSSI test” on page 46
- “1.2.1.4 RF diagnostics” on page 47
- “1.2.1.5 Cam range test” on page 48

Troubleshooting

Camera busy message

Camera busy message may appear when a camera or a wireless expander do not respond to a request because one 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.

Alarm reporting principles

Event conditions

See “Reporting codes used in Advisor Advanced” on page 223 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 172.

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 172, 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 167 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 41 on page 223 for event priority values.

Failed to communicate (FTC)

Each central station has the “9.1.n.7 Retry count” described on page 165. 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 167.

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 54.

Note: If “1.2.6.n.4 Freq TC if FTC” on page 55 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.

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 190 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 143). 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 141) 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 1 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 AAFlash program directory (C:\Program Files\Advisor\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 programing, 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 AAFlash located in the Start > Programs menu.
2. Create filename for the appropriate firmware back-up *.dfu by clicking “...”(Browse). Enter file name and click Save.
3. Click Upload.

   AAFlash uploads existing firmware including settings in dfu-file.

Upgrading Advisor Advanced firmware

To upgrade the panel firmware:

1. While connected to the Advisor Advanced panel, run AAFlash located in the Start > Programs menu.
2. Choose the appropriate firmware file *.dfu by clicking “...” (Browse). Select the appropriate file and click Open.
3. Click Upgrade.

   AAFlash erases the existing firmware, writes the new one, and then verifies it.

   After the firmware is upgraded, the TX LED blinks to indicate that the panel is ready to leave the firmware upgrade mode. USB LED turns off.

   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.

Troubleshooting

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 69 and “2.2.1.n.3.4 Control areas” on page 70 for more details.

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 Advisor Advanced” on page 14.
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 Advisor Advanced” on page 14.

Condition	Possible cause
The panel is not reporting to the central station	The telephone line connections may be wired incorrectly. See “Cabling Advisor Advanced” on page 14. The central station receiver does not support the programmed protocol. The account number in “9.1.n.5 Accounts” on page 164 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 163. The zone is not programmed to be reported. See “4.1.n.6.23 CS report” on page 101”.

LCD keypads

Condition	Possible cause
All the LEDs on the keypad are flashing	The DIP switches may be incorrectly set (the address set on the keypad may be incorrect and therefore polling to the keypad is not being acknowledged). The system data bus line may be connected incorrectly. The keypad is not being polled (it may not have been included in keypads to be polled when programming keypads).
LEDs do not appear to be indicating the correct condition	The keypad type may have been defined incorrectly: LCD keypad must be set to Yes.
The keypad appears to be going off-line and on-line (indicated by the “Keypad fail” message on the LCD)	The termination may be incorrect. See “Cabling Advisor Advanced” on page 14.
An error is indicated when a code is entered on the keypad (seven beeps)	An invalid PIN may have been used. The keypad may not have been programmed with an alarm group. The alarm group of the PIN may not permit access at this keypad.

Remote expanders — Models ATS1201, ATS1210, ATS1211, ATS1220

Condition	Possible cause
The Tx LED on the expander is not flashing	The DIP switches may be incorrectly set (the address recorded on the expander may be incorrect and therefore polling to the expander is not being acknowledged). The system data bus cable may be connected incorrectly. The expander is not programmed to be polled.
Tx and Rx LEDs are not operating	No power or low power. The system data bus cable may be connected incorrectly or the power supply is faulty (mains or battery).

Condition	Possible cause
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 Advisor Advanced” on page 14.
Some or all expander zones are permanently in tamper (or permanently in alarm if “8.5.1 Input mode” on page 152 is set to Single NO or Single NC).	The zone numbers for the expander have been calculated incorrectly, and zone type numbers have therefore been assigned to the wrong zones in the zone database. See “Configuration” on page 22. The end-of-line resistors are wrong or the wrong resistor value is programmed in “8.5.2 EOL” (see page 152). There is a problem with wiring the zones. To check the voltage or resistor values, see “Zone connection” on page 15. The ATS1202 expansion modules (if fitted) have the DIP switches incorrectly set. 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.

Advisor Advanced events

Table 40: Advisor Advanced events

Group	Event	#	Event description	Notes
Zone	ACTIVE	01	Zone active	Zone in active state
	TAMPER	02	Zone tamper	Zone in tamper state
	AM	03	Zone masking	Zone in anti-mask alarm state
	BATTFAULT	04	Zone battery fault	Zone in battery fault state
	FAULT	05	Zone fault	Zone in fault state
	DIRTY	06	Zone dirty	Zone in dirty state
	SVSHORT	07	Zone supervision short	Zone in short supervision state
	SVLONG	08	Zone supervision long	Zone in short supervision state
	INHIBIT	09	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
	Inactive days	16	Zone inverted walk test failed	Zone has been inactive for longer than inactive day limit
Area	FULLSET	01	Area full set	Area is in full set state
	PARTSET1	02	Area part set 1	Area is in part set 1 state
	UNSET	03	Area unset	Area is in unset state
	ALARM	04	Intrusion alarm	Area Intrusion alarm is active
	FSALARM	05	Alarm during full set	Area alarm while in full set
	PSALARM	06	Alarm during part set	Area alarm while in part set
	USALARM	07	Alarm during unset	Area alarm while unset
	FTCALARM	08	Alarm and FTC	Area alarm while FTC present
	FIREDOOR	09	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

Group	Event	#	Event description	Notes
	FTCFIREDOOR	13	Fire door and FTC	A fire door active while FTC present
	FIRE	14	Fire alarm	A fire alarm active
	FSFIRE	15	Fire alarm during full set	A fire alarm active while area full set
	PSFIRE	16	Fire alarm during part set	A fire alarm active while area part set
	USFIRE	17	Fire alarm during unset	A fire alarm active while area unset
	FTCFIRE	18	Fire alarm and FTC	A fire alarm active while FTC present
	PANIC	19	Panic alarm	A panic alarm active
	FSPANIC	20	Panic during full set	A panic alarm active while area full set
	PSPANIC	21	Panic during part set	A panic alarm active while area part set
	USPANIC	22	Panic during unset	A panic alarm active while area unset
	FTCPANIC	23	Panic and FTC	A panic alarm active while FTC present
	MEDICAL	24	Medical alarm	A medical alarm active
	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

Group	Event	#	Event description	Notes
	FTCTAMPER	38	Tamper and FTC	A tamper alarm active while FTC present
	CHIME	39	Chime	Active for 2 sec when zone with chime option is active
	PSCHIME	40	Chime during part set	Active for 2 sec when zone with chime option is active during part set
	USCHIME	41	Chime during unset	Active for 2 sec when zone with chime option is active during unset
	ZNACTIVE	42	Zone active	At least one zone in the area is in active state
	ZNINHIBIT	43	Zone inhibit	At least one zone in the area is inhibited
	ZNISOLATE	44	Zone isolate	At least one zone in the area is isolated
	ZNFAULT	45	Zone fault	At least one zone in the area is in fault state
	ZNAM	46	Zone masking	At least one zone in the area is in anti-mask alarm state
	ZNTAMPER	47	Zone tamper	At least one zone in the area is in tamper state
	KEYPADTAMPER	48	Keypad tamper	A keypad assigned to the area is in tamper state
	KEYPADFAULT	49	Keypad fault	A keypad assigned to the area is in fault state
	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

Group	Event	#	Event description	Notes
	EXITFAULT	60	Exit fault	Alarm detected during exit state before changing to part or full set state
	RTS	61	Ready To Set	Active when all configured RTS conditions are valid
	SETOK	62	Area set OK	Active for 2 s when area set successfully
	SETFAULT	63	Area set failed	Active during 30 s after unsuccessful area setting
	UNSETOK	64	Area unset OK	Active for 2 sec when area has been unset
	ALARMACK	65	Alarms to ACK	Alarms present waiting for acknowledge
	FIRERESET	66	Fire reset	For FIRE zone, event active for 10 s after fire alarm acknowledge (also inhibits fire zone for 15 s). Also active for 10 s during fire zone walk test
	WALK	67	Walk test	User/Installer Walk test is active
	WALKZNACTV	68	Walk test zone active	Zone in walk test is activated
	A-ALARM	69	A-Alarm	A-alarm active (unconfirmed alarm), reset after unset or expiration of AB timer and no B-alarm.
	B-ALARM	70	B-Alarm	B-alarm active (confirmed alarm). Reset after unset
	ISIREN	71	Internal siren	Internal siren. Activated on alarm during the internal siren time. Activation may be delayed by Siren delay time. Can be retriggered by next alarm.
	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

Group	Event	#	Event description	Notes
	HA-ALARM	79	A hold-up alarm	Reset after unset
	HB-ALARM	80	B hold-up alarm	Reset after unset
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
Expander	OFFLINE	1	Expander is offline	Active if device is offline
	MAINSFAULT	2	Mains fail	
	BATTFAULT	3	Battery fail	
	TAMPER	4	Expander tamper	Device tamper
	FUSEFAULT	5	Fuse fault	
	SIRENFAULT	6	Siren fault	
	RCVFAULT	7	Receiver fault	Wireless expander receiver fault
	ISOLATED	8	Expander isolated	
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

Group	Event	#	Event description	Notes
	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
	MIFAULT	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
	GSMJAMMING	20	GSM line jamming	GSM jamming detected
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
Output	ACTIVE	1	Output active	Specified output activates
	ON	2	Output on	Physical output activates
Filter	ACTIVE	1	Condition true	The selected filter condition is true / valid.
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.
System	ALLSET	1	All set	All areas in the system are set
	AUTOANS	2	Auto Answer	Auto answer procedure started (1 min)
	RCONNACTV	3	Remote connection	Remote connection active
	RCONNFAIL	4	Remote connection fail	Remote connection fail (1 min)
	LPRGACTV	5	Local programming	Local programming active

Group	Event	#	Event description	Notes
	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
CS	FTC	1	Failed To Communicate	Failed to deliver an alarm message
	HB	2	OH heartbeat fault	OH protocol heartbeat fault
	BUSY	3	CS busy	CS is busy (in use)
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	7	Trigger is activated by a fob	
Exception	CALEXCPACTIVE	1	Exception active	
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
	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	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	
Camera	Pic captured	1	Picture has been taken	Active for 3 seconds
	Pic limit exc	2	Picture limit has been exceeded	

Reporting codes used in Advisor Advanced

Table 41 below shows descriptions of SIA, CID, and VdS reporting codes used in Advisor Advanced.

Table 42 on page 228 lists allowed values for the appropriate reporting codes.

Table 41: 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 unbypass	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
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

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
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 unbypass	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 unbypass		Low
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

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
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
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

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
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 unbypass — 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
93.	GB	0x51	E570	Technical bypass — gas	Gas detector inhibit	Low
94.	GU	0xD1	R570	Technical unbypass — 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

#	SIA code	VdS code	CID code	Function	Note	Reporting priority
99.	KB	0x51	E570	Technical bypass — high temperature	High temperature detector inhibit	Low
100.	KU	0xD1	R570	Technical unbypass — 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 unbypass — 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
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.	JA	0x23	E461	Wrong Code Entry	Code tamper	Low
121.	DD	—	E421	Access denied	Card is unknown	Low

Table 42: 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)	E408	System (0)	User (1–50)
		Zone (1–128, 257–368)		Area (1–8)	Zone (1–128, 257–368)
16.	CG	User (1–50),	E456	System (0)	User (1–50)
		Zone (1–128, 257–368)		Area (1–8)	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)
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)

#	SIA code	Subevent type and range	CID code	Group range	Point range
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)	
		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)	–

#	SIA code	Subevent type and range	CID code	Group range	Point range
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)
		Communication path (0–6) [1]			
67.	XQ	Expander (299–307)	E344	System (0)	Expander (65–72)
		Communication path (0–6) [1]			
68.	XR	Zone (1–128, 257–368)	R384	Area (1–8)	Zone (1–128, 257–368)
		Fob (1–112)			
69.	XT	Zone (1–128, 257–368)	E384	Area (1–8)	Zone (1–128, 257–368)
		Fob (1–112)			
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)	E302	System (0)	Expander (65–72)
		Zone (1–128, 257–368)			
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)

#	SIA code	Subevent type and range	CID code	Group range	Point range
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)
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)

#	SIA code	Subevent type and range	CID code	Group range	Point range
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.	JA	Keypad (401–408)	E461	System (0)	Keypad (1–8)
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

Note: SIA reporting range assumes expanders numbering from 0 to 8, where expander 0 is the control panel itself.

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 “5 Area menu” on page 113 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 “5 Area menu” on page 113 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 158.

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 140).

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.6.15 Key latch” on page 99, “4.1.n.6.16 Key set” on page 100, “4.1.n.6.17 Key unset” on page 100.

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.6.18 Technical full set” on page 100, “4.1.n.6.19 Technical unset” on page 100.

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 233.

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 142). 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 “5.n.2 Exit time” on page 113” and “5.n.3 Entry time” on page 114.

See also “2. Entry/Exit 1” on page 233 for more details.

Table 43: 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. Keyswitch	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
4.1.n.3 Isolated		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4.1.n.6.1 Inhibit		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.1.n.6.2 Excl. in PS1		–	–	–					–	–							–		–
4.1.n.6.3 Excl. in PS2		–	–	–					–	–							–		–
4.1.n.6.4 Double knock		–			–		–					–	–	–	–	–			
4.1.n.6.5 Swinger shunt		+	+	+			–	–				–		–	–	–	–		+
4.1.n.6.6 Anti mask		–	–	–			–					–		–					–
4.1.n.6.7 Zone pairing		–			–							–		–					
4.1.n.6.8 Chime		–	–	–								–		–					–
4.1.n.6.9 Soak test		–	–	–	–	–	–	–				–		–	–	–	–	–	–
4.1.n.6.10 Engineer walk test		+	+	+	+	+	+	+			+	+	+	+	+	+		+	+
4.1.n.6.11 User walk test		+	+	+		+	+				+	+		+	+	+		+	+
4.1.n.6.12 Shock sensor		–	–	–			–							–					–
4.1.n.6.13 Extend EE			–																–
4.1.n.6.14 Final door			–	–															–
4.1.n.6.15 Key latch										–									
4.1.n.6.16 Key set — full set										–									
4.1.n.6.16 Key set — part set										–									
4.1.n.6.17 Key unset										–									

Options:	Zone type	1. Alarm	2. Entry/Exit 1	3. Access	4. Fire	5. Panic	6. 24H	7. Tamper	8. Exit terminator	9. Keyswitch	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
4.1.n.6.18 Technical full set												+							
4.1.n.6.19 Technical unset												+							
4.1.n.6.20 Technical part set												+							
4.1.n.6.21 Keypad LCD							–				–	–	–	–	–	–			
4.1.n.6.22 Log		•	•	•	•	•	•	•			+	+	•	•	+	+	+		•
4.1.n.6.23 CS report		•	•	•	•	•	•	•			+	+	•	•	+	+	+		•
4.1.n.6.24 Delay timer												–	–		–	–			
4.1.n.6.25 ACK on keypad																			
4.1.n.6.26 ACK by user																			
4.1.n.6.27 Sensor type																			
4.1.n.6.28 Virtual zone																			
4.1.n.6.29 Held open																			
4.1.n.6.30 EE set check																			
4.1.n.6.31 Alarm in PS1																			
4.1.n.6.32 Alarm in PS2																			
4.1.n.6.33 Report as																			

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.

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.2 Period / Time, 24 h for every path to meet ATS Class 2, 4 h for the IP path to meet ATS Class 4.
- 2.2.1.n.3.3 View areas and 2.2.1.n.3.4 Control areas settings are identical
- 2.2.1.n.3.8 Buzzer silent, never
- 2.2.1.n.3.9 Quick set, off
- 2.2.1.n.3.10 Function keys, all set to None
- 2.2.1.n.3.15 ACK on keypad, set to None for non-LCD keypads
- 3.1.n.7.3 SMS control, disabled for all users
- 3.2.n.5 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.6.5 Swinger shunt, set to Yes for all zones
- 4.1.n.6.25 ACK on keypad, set to None for all zones with type 9. Keyswitch
- 5.n.3 Entry time, 45 s maximum
- 5.n.7 Entry alarms, Instant
- 7.5.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
- 8.4.5 Pending alarms, enabled
- 8.5.4 Swinger shunt ≥ 3
- 8.5.5 Report restore, on ACK
- 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
- ATS1238 Advanced Wireless DGP
- TX-2344-03-1 Wireless PIR Camera
- ATS7310 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
- 4.3 Cameras
- 9.1.n.4.4 Vid dest port
- 9.3.n.10 Max Pics 24h, 9.3.n.7.9 Max Pics 24h

Options affected by other regulations

ACPO policy

Required settings are all EN 50131 Grade 2 settings with the following modifications:

- 5.n.7 Entry alarms, Delayed
- 8.2.4 Engineer reset, tamper enabled
- 8.7.7 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.5 User group options
- Full Set/Part Set/Unset/Forced Set for Installer disabled in 3.2.n.5 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 “8.7.5 PIN length”.

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 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.
Alarm control	The control over alarm functions.
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 own zones. Each area is identified by a number and a name. For example, Area 1 Office, Area 2 Workshop, Area 3 Boardroom, etc.
Armed	See Set.
Armed display	Armed display activates on a keypad after particular idle time. In this mode, the information displayed on LCD and LED is very limited for security reasons. A user intervention is necessary for return to a normal display mode.
Arming station (RAS)	See Keypad.
Autoset	An automatic setting of the premises started by a schedule or an exception. See Schedule, Exception.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.
Central station	A company that monitors whether an alarm has occurred in a security system. The central station is located away from the premises/area it monitors.
Condition filter	A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.
Control panel	An electronic device that is used to gather all data from zones on the premises. Depending on programming and status of areas, it generates alarm signals. If required, alarms and other events can be reported to the central station.
Cursor	A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.

DGP	Data gathering panel. See Expander.
Dialler	An electronic device that allows the 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.
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.
Exception	Particular time periods when a schedule is extended or changed.
Expander	A device that collects data from other security devices within an area, and transfers it to the 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.
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.
Inverted walk test	A test based on counting days of inactivity for each zone.
Key switch	A device using a switch to arm or disarm areas. The switch needs a key to switch.
Keypad	A device that is the user control panel for security options for areas or for access points (doors). The keypad can be a console (LCD keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as set/unset, open doors, etc.
LCD	Liquid crystal display. The part of a keypad where messages are displayed.
LED	Light emitting diode. A light indicator on a keypad which conveys a condition. For example, area in alarm, communication fault, etc.

Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault	Describes the condition of a zone. • Normal: The zone is *not* 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.
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.
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.
Schedule	A timed set of actions with a weekly structure.
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 (PIR detector, door contact) to the Advisor Advanced system. Each device is identified by a zone number and name. For example, 14 Reception Hold-up Button, 6 Fire Exit Door.

Index

A

access zone, 233
account, 181
action, **127**
  action list, 131
  condition filter, 130
  creating, 129
  deleting, 130
  function, 130
  name, 129
  settings, 129
  start, 129
action list, 127, **131**, 132
  creating, 131
  deleting, 132
  name, 131
add
  action, 129
  action list, 131
  central station, 163
  event, 118
  exception, 133
  expander, 75
  fob, 108, 199
  keypad, 68
  output, 120
  PC connection, 188
  trigger, 125
  user, 84
  user group, 89
  zone, 95
adding a central station, 163
adding a PC connection, 188
adding a trigger, 125
adding a user group, 89
adding a user to the system, 84
adding an action, 129
adding an action list, 131
adding an exception, 133
advanced setup, 33
alarm
  restore, 153
alarm confirmation, 155
alarm history, 45
alarm restore, 153
anti-mask, 98
APN, 184
area, 96, **113**
  entry/exit time, 113, 114
  prealarm time, 115
  warning time, 114
area indicator, 72
area modifier, 164, 167
area status, 73
armed display, 147
  timeout, 140
automatic battery test, **60**, **61**
autoset, 114, 196

B

basic setup, 33
battery
  status, 60
battery test, **60**
  automatic test, 60, 61
  duration, 61
  frequency, 61
  start time, 61
bus devices, **66**
buzzer, 159

C

calendar, 127
  exception, 133
  schedule, 136
  view, 137
callback, 190
camera, **110**
  filter, 110, 111
  isolate, 111
  taking picture, 112
  zone list, 110
camera range test, 48
cameras, 203
card
  check, 62
card & PIN mode, 70
card and PIN timeout, 140
card reader, **6**
central station, 163
  backup, 207
  creating, 163
  deleting, 167
  mapping, 206
  primary, 207
challenge code, 146
change PIN, 64, 84
changing a user, 84
changing user group, 89
check card, 62
chime, 98, 158
CID codes, 223
code tamper, 29, 35
combined reporting, 206
communication, **162**
  account code, 164
  auto-answer, 190
  callback, 190

central station, 163
destination name, 168, 191
destination port, 168, 191
Downloader, 209
encryption, 170
events, 172
frequent heartbeat, 169
GSM, 178
GSM network, 179, 180
heartbeat, 169
line number, 169
PC connection, 188
phone number, 168
protocol, 164, 165
receiver number, 169
subevents, 166
Titan, 209
transmission path, 163, 173
video port, 170
condition filter, 130
condition filters, **117**, 121
configuration software, 209
configure
area, 113
condition filter, 118
event, 119
expander, 75
fob, 108
input, 152
keypad, 68
output, 120
part set, 153
user, 84
zone, 95, 152
creating a central station, 163
creating a PC connection, 188
creating a trigger, 125
creating a user, 84
creating a user group, 89
creating an action, 129
creating an action list, 131
creating an exception, 133
credit, 181
custom LCD message, 147
custom mode, 64

D

date, 138
daylight saving time, 138
default, 65
defaults, 43, 154
de-isolate, 96
delete
expander, 77
keypad, 74
output, 124
zone, 107
deleting a central station, 167
deleting a PC connection, 189
deleting a trigger, 126
deleting a user, 88
deleting a user group, 93
deleting an action, 130
deleting an action list, 132
deleting an exception, 135
demo, 63
device states, 66
DHCP, 176
dialler
battery, 60
DNS, 176
double knock, 97
timers, 141
Downloader, **209**
DST, 138
dual loop, 76

E

earthing, 12
encryption, 170, 175
key, 190
engineer lockout, 143
engineer reset, 143
auto reset, 145
disable when service in, 145
engineer walk test, 50, 99
entry
extend time, 99
entry alarms, 115
entry time, 99, 114
entry timer, 148
entry/exit, 103, 233, 235
access, 153
full set, 154
PIN lock, 71
entry/exit time, 113, 114
entry/exit zone, 73, 74
EOL, 76, 152
event list, 215
events, **172**
mapping, 172
exception, 127, **133**, 137
action lists, 134
actions, 134
creating, 133
deleting, 135
name, 133
start date, 133
stop date, 134
substitute, 134
week days, 134
year, 134
exit terminator, 99, 140, 234
exit time, 113
exit timer, 148

expander, 66, **75**
dual loop, 76
EOL, 76
input mode, 76
isolate, 76
name, 76
resistor values, 76
settings, 76
single zone, 76
troubleshooting, 213
extend entry timer, 99
extend test call, 55

F

fault indication, 148
filter, **116**
final door, 99
final set, 140
firewall, 177
firmware, 210
flash, 210
fob, 86, **108**
add, 108, 199
assigned user, 108
buttons, 108
name, 108
remove, 109
forced set, 150
formula, 118
frame rate, 80
frequent heartbeat, 169
frequent test call, 55
FTC, 208
function, 130
function key, 72

G

gateway, 176
glossary, 241
GPRS, 184
disconnection time, 185
line fault, 185
password, 184
picture limit, 178
user name, 184
GPRS network
registration, 58
state, 58
gross level, 104
GSM, 178
battery status, 60
reporting, 170
GSM network, 179
availability, 179
code, 59
diagnostic, 57
PIN status, 58
registration, 58
scan, 180
signal strength, 59

H

HDR, 47
heartbeat, 169
frequent, 169
held open alarm, 103
time, 142

I

inactive days, 48, 142
inhibit, 97
input, 95
delay, 142
options, 152
resistance, 48
test, 46
input mode, 76
input state, 46
installation, **43**
installer, **83**
in-time, 141
user confirmation, 143
installer code, 43
installer in, 65, 146
invert output, 121
inverted walk test, 48
timer, 142
IP
picture limit, 178
IP address, 175
IP diagnostic, 56
IP interface, 56
IP statistics, 56
isolate, 96
camera, 111
keypad, 71

K

key, 99
key box
time, 142
key switch, 99, 234
keypad, **5**, 66, **68**
buzzer, 159
troubleshooting, 213
keypad layout, 40
keypad lockout, 29, 35

L

LCD
    EE timer, 148
LCD backlight, 73
LCD message, 147
LCD options, 147
LDR, 47
learn card, 86
LED test, 50
line number, 169
link speed, 178
listing open zones, 46
lock user data, 83
lockout, 29, 35
log, 45
logout, 65, 146

M

MAC, 178
mains fail reporting delay, 140
manual test, **55**
menu entries, 147
    accessing, 37
    confirmation of changes, 40
    exit, 40
    explanation of the LCD display, 38
    how to edit host address, 39
    how to edit list, 39
    how to edit text, 39
    how to program values, 38
    how to program Yes/No options, 39
    programming, 38
    scrolling the list of menus, 37
    unauthorized access, 35
    using PIN, 35
menu tree, 251
MMS, 186
    limit, 186
    proxy, 186

N

need acceptance, 37
need to set, 53
notational and typographical conventions, vi
NTP, 57, 177

O

OH 2000, 169
omit first call, 185
open zones, 46
output, **116**
    active time, 123
    add, 120
    delay, 123
    delete, 124
    edit, 120
    mode, 121
    name, 120
    test, 49

P

panel diagnostics, 62
panel information, 63
panel lid, 64
panel version, 63
panic alarm, 74, 158
part set, 97, 103
    name, 154
    options, 153
PC connection, 188, 209
    creating, 188
    deleting, 189
    host, 191
    port, 191
picture auto deletion, 81
picture frame rate, 80
picture options, 79
picture quality, 80
picture settings, 79
PIN, **84**, 179
PIN of the day, 146
ping, 56, 168, 177, 191
prealarm time, 115
predefined users, 83
preface, vi
prepaid, 181
privilege limitation, 93
programmable functions, 193
programming, 251
programming cameras, 203
programming map, 251
programming users, 82
programming wireless devices, 197
protocol, 164, 165
PUK, 58, 179
pulse count, 104

Q

quick set, 72

R

random mode, 64
range test, 48
ready to set, 149
receiver number, 169
reduced walk test, 53
regulations, 237
reinstall, 65

remote configuration, 147
remote login, 85
remote PIN, **85**
remove
  fob, 109
  RF device, 106, 109
reporting, 206
  account code, 164
  phone numbers, 168
resistance, 48
resistor values, 76, 152, 153
resolution, 80
RF device
  configuration, 104, 109
  remove, 106, 109
  supervision, 105
RF state, 47
ring setup, 185
RSSI, 46
  report, 56
RTS, 149

S

schedule, **136**
  action lists, 137
  actions, 137
  active schedule, 136
  days, 137
  exceptions, 137
  name, 136
  start date, 136
  stop date, 136
  view, 127
sensor type, 102
service, **45**
  time, 141
  user confirmation, 143
service in, 37, 65, 146
set options, 148
shielding, 13
shock sensor, 49, 99, 104
  sensitivity, 104
SIA codes, 223
SIA frequency, 166
SIM, 179
single zone, 76
single zone walk test, 54
siren EOL, 153
siren timers, 139
SMS, 182
  center, 182
  charset, 183
  control, 88, 92
  counter, 59
  forwarding, 183
  header, 183
  messages limit, 183
  PIN, 183
  reporting, 88, 92
soak test, 98
  time, 141
software revision, 63
special walk test mode, 54
standard walk test, 51
start filter, 121
start time, 129
stop filter, 121
subevents, **166**
substitute, 127, **134**
supervision, 105
suppress FTC, 167
swinger shunt, 98, 153
system code, 145
system options, **138**

T

tamper area, 69
technical alarm, 100
technical zone sensor, 102
telephone number, 168
test, 46
  battery, 60
test call, 54, 55
  extend test call, 55
  frequent test call, 55
  FTC, 55
  RSSI, 56
test menus, 34
time and date, 138
time zone, 138
timers, **138**
Titan, 209
transmission path, 163, 173
trigger, **116**
  creating, 125
  deleting, 126
  name, 125
  state, 50
troubleshooting, **212**
  data gathering panels, 213
  LCD keypads, 213

U

uninhibit, 97
upgrade, 210
user, **83**
  card, 85
  changing, 84
  creating, 84
  deleting, 88
  language, 86
  PIN, 84
  programming, 82
  user group, 89
user card, 85
user confirmation, 143
user data lock, 83

user group, **89**
changing, 89
creating, 89
deleting, 93
name, 89
options, 90, 91
privilege limitation, 93
type, 90
what is a user group, 89
user LCD message, 147
user management, 82
user name, **84**
user phone, 87
user privilege, 90
user programmable functions, 193
user walk test, 50, 53, 99
using cameras, 203

V

VdS codes, 223
version, 210
video port, 170
view calendar, 137
virtual zone, 102

W

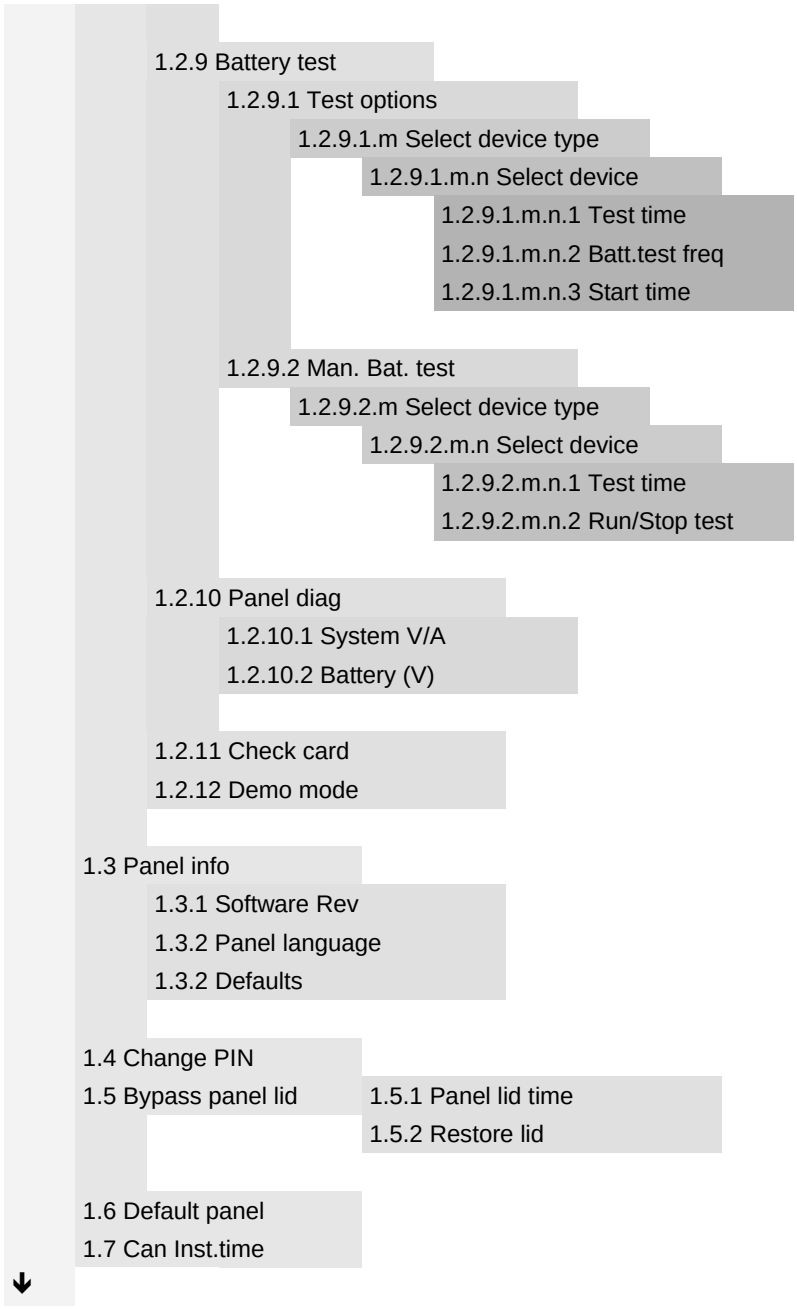
walk test, 50, 99
frequency, 53
reduced walk test, 53
single zone, 54
standard walk test, 51
timeout, 140
walk test mode, 54
warning time, 114
week days, 137
wireless device, 104, 109, 197
supervision, 105
wireless sensor, 197
word library, 41, 161

Z

zone, **95**
access, 103
area, 96
copy, 106
de-isolate, 96
delete, 107
entry/exit, 103
entry/exit time, 113, 114
held open alarm, 103
inhibit, 97, 149
isolate, 96
name, 95
open too long, 103, 142
options, 97, 152
part set, 97
prealarm time, 115
report as duress, 103
report as panic, 103
reporting, 101
resistance, 48
type, 96, **233**
uninhibit, 97
warning time, 114
zone acknowledgement, 101
zone delay, 101
zone options, 97
zone pairing, 98
zone type, 96, **233**

Programming Map

- 1 Service menu
  - 1.1 Display logs
  - 1.2 Test menu
    - 1.2.1 Input tests
      - 1.2.1.1 Show open zones
      - 1.2.1.2 Number of used zones
      - 1.2.1.3 RF RSSI test
      - 1.2.1.4 RF diagnostics
      - 1.2.1.5 Cam range test
      - 1.2.1.6 Inactive days
      - 1.2.1.7 Zone kOhm
    - 1.2.2 ShockSens test
    - 1.2.3 Outs&triggers
      - 1.2.3.1 Output test
        - 1.2.3.1.1 Outputs
        - 1.2.3.1.2 Keypad LEDs
      - 1.2.3.2 Trigger state
    - 1.2.4 Alarms and faults
    - 1.2.5 Walk test
      - 1.2.5.1 Walk test start
      - 1.2.5.2 Walk test opts
        - 1.2.5.2.1 Use internal siren
        - 1.2.5.2.2 Use buzzers
        - 1.2.5.2.3 Log untested
        - 1.2.5.2.4 Zone tamper
        - 1.2.5.2.5 Rkp/Exp tamper
        - 1.2.5.2.6 Siren tamper
        - 1.2.5.2.7 Frequency
        - 1.2.5.2.8 Need to set
        - 1.2.5.2.9 Reduced walk
      - 1.2.5.3 Single zone WT
      - 1.2.5.4 Special WT mode
    - 1.2.6 Test call opts
      - 1.2.6.n Select central station
        - 1.2.6.n.1 Test call mode
        - 1.2.6.n.2 Period / Time
        - 1.2.6.n.3 Extend
        - 1.2.6.n.4 Freq TC if FTC
        - 1.2.6.n.5 Man. test call
        - 1.2.6.n.6 RSSI in report
    - 1.2.7 IP diagnostic
      - 1.2.7.n Choose interface
        - 1.2.7.n.1 IP statistics
        - 1.2.7.n.2 Ping host
        - 1.2.7.n.3 Ping PC
        - 1.2.7.n.4 Ping CS
        - 1.2.7.n.5 NTP status
    - 1.2.8 GSM diagnostic
      - 1.2.8.1 PIN status
      - 1.2.8.3 GSM net.reg.
      - 1.2.8.4 GPRS net.reg.
      - 1.2.8.5 GPRS state
      - 1.2.8.6 Network name
      - 1.2.8.7 Network code
      - 1.2.8.8 RSSI
      - 1.2.8.9 Msg sent 24h
      - 1.2.8.10 Battery status


1.2.9 Battery test
1.2.9.1 Test options
1.2.9.1.m Select device type
1.2.9.1.m.n Select device
1.2.9.1.m.n.1 Test time
1.2.9.1.m.n.2 Batt.test freq
1.2.9.1.m.n.3 Start time
1.2.9.2 Man. Bat. test
1.2.9.2.m Select device type
1.2.9.2.m.n Select device
1.2.9.2.m.n.1 Test time
1.2.9.2.m.n.2 Run/Stop test
1.2.10 Panel diag
1.2.10.1 System V/A
1.2.10.2 Battery (V)
1.2.11 Check card
1.2.12 Demo mode
1.3 Panel info
1.3.1 Software Rev
1.3.2 Panel language
1.3.2 Defaults
1.4 Change PIN
1.5 Bypass panel lid
1.5.1 Panel lid time
1.5.2 Restore lid
1.6 Default panel
1.7 Can Inst.time

- 2 Device menu
  - 2.1 Installed remote devices
  - 2.2 Edit Keypad&Exp
    - 2.2.1 Keypad devices
      - 2.2.1.0 Add keypad
      - 2.2.1.n Select keypad
        - 2.2.1.n.1 Keypad type
        - 2.2.1.n.2 Keypad address
        - 2.2.1.n.3 Keypad options
          - 2.2.1.n.3.1 Keypad name
          - 2.2.1.n.3.2 Tamper area
          - 2.2.1.n.3.3 View areas
          - 2.2.1.n.3.4 Control areas
          - 2.2.1.n.3.5 Login options
            - 2.2.1.n.3.5.1 1 x door access
            - 2.2.1.n.3.5.2 Card and PIN mode
            - 2.2.1.n.3.5.3 1 x set/unset
            - 2.2.1.n.3.5.4 3 x badge set
          - 2.2.1.n.3.6 EE PIN lock
          - 2.2.1.n.3.7 Isolate keypad
          - 2.2.1.n.3.8 Buzzer silent
          - 2.2.1.n.3.9 Quick set
          - 2.2.1.n.3.10 Function keys
          - 2.2.1.n.3.11 Area ind.LED1
          - 2.2.1.n.3.12 Area ind.LED2
          - 2.2.1.n.3.13 Status ind.
          - 2.2.1.n.3.14 LCD backlight
          - 2.2.1.n.3.15 ACK on keypad
          - 2.2.1.n.3.16 EE 1 buzzer
          - 2.2.1.n.3.17 EE 2 buzzer
          - 2.2.1.n.3.18 1+3 keys
        - 2.2.1.n.4 Keypad menu
        - 2.2.1.n.5 Delete keypad
    - 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

3 User menu

- 3.1 Users
  - 3.1.0 Add user
  - 3.1.n Select user
    - 3.1.n.1 User name
    - 3.1.n.2 PIN
      - 3.1.n.2.1 Change PIN
      - 3.1.n.2.2 Remote PIN
    - 3.1.n.3 User card
      - 3.1.n.2.2.1 Set PIN
      - 3.1.n.2.2.2 Enable login
    - 3.1.n.4 RF fobs
    - 3.1.n.5 Language
    - 3.1.n.6 User groups
    - 3.1.n.7 SMS and Voice
      - 3.1.n.7.1 User phone
      - 3.1.n.7.2 SMS reporting
      - 3.1.n.7.3 SMS control
    - 3.1.n.8 Delete user

- 3.2 User groups
  - 3.2.0 Add user group
  - 3.2.n Select user group
    - 3.2.n.1 User group name
    - 3.2.n.2 User group type
    - 3.2.n.3 User group areas
    - 3.2.n.4 User group filter
    - 3.2.n.5 User group options
    - 3.2.n.6 Remove user group

- 4 Zones and RF fobs
  - 4.1 Zone menu
    - 4.1.0 Add zone
    - 4.1.n Select zone
      - 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 Areas
      - 4.1.n.6 Zone options
        - 4.1.n.6.1 Inhibit
        - 4.1.n.6.2 Excl. in PS1
        - 4.1.n.6.3 Excl. in PS2
        - 4.1.n.6.4 Double knock
        - 4.1.n.6.5 Swinger shunt
        - 4.1.n.6.6 Anti mask
        - 4.1.n.6.7 Zone pairing
        - 4.1.n.6.8 Chime
        - 4.1.n.6.9 Soak test
        - 4.1.n.6.10 Engineer walk test
        - 4.1.n.6.11 User walk test
        - 4.1.n.6.12 Shock sensor
        - 4.1.n.6.13 Extend EE
        - 4.1.n.6.14 Final door
        - 4.1.n.6.15 Key latch
        - 4.1.n.6.16 Key set
        - 4.1.n.6.17 Key unset
        - 4.1.n.6.18 Technical full set
        - 4.1.n.6.19 Technical unset
        - 4.1.n.6.20 Technical part set
        - 4.1.n.6.21 Keypad LCD
        - 4.1.n.6.22 Log
        - 4.1.n.6.23 CS report
        - 4.1.n.6.24 Delay timer
        - 4.1.n.6.25 ACK on keypad
        - 4.1.n.6.26 ACK by user
        - 4.1.n.6.27 Sensor type
        - 4.1.n.6.28 Virtual zone
        - 4.1.n.6.29 Held open
        - 4.1.n.6.30 EE set check
        - 4.1.n.6.31 Alarm in PS1
        - 4.1.n.6.32 Alarm in PS2
        - 4.1.n.6.33 Report as
      - 4.1.n.7 Gross and Pulse options
        - 4.1.n.7.1 Pulse count
        - 4.1.n.7.2 Gross level

        Wireless sensor options:

        - 4.1.n.7 RF details
          - 4.1.n.7.1 Sensor ID
          - 4.1.n.7.2 Sensor type
          - 4.1.n.7.3 Supervision
          - 4.1.n.7.4 Sensor opt
          - 4.1.n.7.5 Remove RF dev
      - 4.1.n.8 Copy
        - 4.1.n.8.1 Copy par. from
        - 4.1.n.8.2 Block assign
      - 4.1.n.9 Delete zone



- 4.2 RF fobs
  - 4.2.0 Add fob
  - 4.2.n Select fob
    - 4.2.n.1 Fob name
    - 4.2.n.2 Assigned user
    - 4.2.n.3 Buttons
      - 4.2.n.3.1 Select button
    - 4.2.n.4 RF details
      - 4.2.n.4.1 Sensor ID
      - 4.2.n.4.2 Remove RF dev
    - 4.2.n.5 Remove fob
- 4.3 Cameras
  - 4.3.n Select camera
    - 4.3.n.1 Camera name
    - 4.3.n.2 Pics by zone
    - 4.3.n.3 Pics by filter
      - 4.3.n.3.m Select filter
        - 4.3.n.3.m.1 Choose filter
        - 4.3.n.3.m.2 Event type <n>
        - 4.3.n.3.m.3 Report as
    - 4.3.n.4 Pics by rep ev
      - 4.3.n.4.m Select event
    - 4.3.n.5 Isolated
    - 4.3.n.6 Max pics 24h
    - 4.3.n.7 Remote pics
    - 4.3.n.8 Test pic to CS

- 5 Area menu
  - 5.n Select area
    - 5.n.1 Area name
    - 5.n.2 Exit time
      - 5.n.2.1 Exit time 1
      - 5.n.2.2 Exit time 2
      - 5.n.2.3 PS Exit time 1
      - 5.n.2.4 PS Exit time 2
    - 5.n.3 Entry time
      - 5.n.3.1 Entry time 1
      - 5.n.3.2 Entry time 2
      - 5.n.3.3 PS Entry time 1
      - 5.n.3.4 PS Entry time 2
    - 5.n.4 Warning time
    - 5.n.5 Prealarm time
    - 5.n.7 Entry alarms
    - 5.n.8 Autoset retry
    - 5.n.9 Silent set



- 6 Outputs and filters
  - 6.1 Condition filters
    - 6.1.n Select filter
      - 6.1.n.1 Filter name
      - 6.1.n.2 Formula
        - 6.1.n.2.0 Add event
        - 6.1.n.2.x Select event
        - 6.1.n.2.y Select operator
      - 6.1.n.3 Invert
  - 6.2 Outputs
    - 6.2.0 Add output
    - 6.2.n Select output
      - 6.2.n.1 Output name
      - 6.2.n.2 Output location
      - 6.2.n.3 Invert output
      - 6.2.n.4 Start filter
      - 6.2.n.5 Stop filter
      - 6.2.n.6 Mode
      - 6.2.n.7 Parameters
        - 6.2.n.7.1 Delay time
        - 6.2.n.7.2 Active time
        - 6.2.n.7.3 Retriggerable
      - 6.2.n.8 Log limit
      - 6.2.n.9 Delete output
  - 6.3 Triggers
    - 6.3.0 Add trigger
    - 6.3.n Select trigger
      - 6.3.n.1 Trigger name
      - 6.3.n.2 Delete trigger
- 7 Calendar
  - 7.1 View
    - 7.1.1 Current view
    - 7.1.2 Date view
  - 7.2 Actions
    - 7.2.0 Add action
    - 7.2.n Select action
      - 7.2.n.1 Action name
      - 7.2.n.2 Start time
      - 7.2.n.3 Active
      - 7.2.n.4 Function
      - 7.2.n.5 Action filter
      - 7.2.n.6 Delete action
  - 7.3 Action lists
    - 7.3.0 Add action list
    - 7.3.n Select action list
      - 7.3.n.1 Action list name
      - 7.3.n.2 Active
      - 7.3.n.3 Actions
      - 7.3.n.4 Delete action list
  - 7.4 Exceptions
    - 7.4.0 Add exception
    - 7.4.n Select exception
      - 7.4.n.1 Exception name
      - 7.4.n.2 Start date
      - 7.4.n.3 Stop date
      - 7.4.n.4 Year
      - 7.4.n.5 Week days
      - 7.4.n.6 Substitute
      - 7.4.n.7 Active
      - 7.4.n.8 Actions
      - 7.4.n.9 Action lists
      - 7.4.n.10 Delete exception
  - 7.5 Schedules
    - 7.5.n Select schedule
      - 7.5.n.1 Schedule name
      - 7.5.n.2 Active
      - 7.5.n.3 Start date
      - 7.5.n.4 Stop date
      - 7.5.n.5 Week days
      - 7.5.n.6 Exceptions
      - 7.5.n.7 View

- 8 System option menu
  - 8.1 Timer menu
    - 8.1.1 Time and date
    - 8.1.2 Siren options
      - 8.1.2.1 Activation
        - 8.1.2.1.1 Internal siren
        - 8.1.2.1.2 External siren
        - 8.1.2.1.3 F/P/M internal
        - 8.1.2.1.4 F/P/M external
      - 8.1.2.2 Delay time
        - 8.1.2.2.1 Internal siren
        - 8.1.2.2.2 External siren
    - 8.1.3 System misc opts
      - 8.1.3.1 Armed display
      - 8.1.3.2 Card and PIN
      - 8.1.3.3 Walk test time
      - 8.1.3.4 Mains reporting delay
      - 8.1.3.5 Final set delay
      - 8.1.3.6 Installer in-time
    - 8.1.4 Zone timer menu
      - 8.1.4.1 Double knock interval
      - 8.1.4.2 Double knock open
      - 8.1.4.3 Soak test
      - 8.1.4.4 Input delay
      - 8.1.4.5 Key box time
      - 8.1.4.6 Held open time
      - 8.1.4.7 Inactive days
  - 8.2 Engineer 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
      - 8.2.4.2 Tamper
      - 8.2.4.3 Panic
      - 8.2.4.4 Confirmed alarm
      - 8.2.4.5 Battery fail
      - 8.2.4.6 Aux fuse
      - 8.2.4.7 Mains fail
      - 8.2.4.8 Siren fault
      - 8.2.4.9 Interconn fault
      - 8.2.4.10 Auto reset
      - 8.2.4.11 Dis by service
      - 8.2.4.12 System code
      - 8.2.4.13 Do reset
      - 8.2.4.14 Custom text
    - 8.2.5 Cancel in.time
    - 8.2.6 Challenge code
    - 8.2.7 Remote configuration
  - 8.3 LCD display options
    - 8.3.1 Armed display
    - 8.3.2 Custom message
    - 8.3.3 Alarm list
    - 8.3.4 Indicate faults
    - 8.3.5 View EE timer
  - 8.4 Set options
    - 8.4.1 RTS options
    - 8.4.2 Inhibit includes
    - 8.4.3 Forced set
    - 8.4.4 Forced set options
    - 8.4.5 Pending alarms
    - 8.4.6 AS fault retry
    - 8.4.7 AS user retry

- 8.5 Zone options
  - 8.5.1 Input mode
  - 8.5.2 EOL
  - 8.5.3 Siren tamper EOL
  - 8.5.4 Swinger shunt
- 8.6 Part set
  - 8.6.1 Report BA
  - 8.6.2 Access to EE
  - 8.6.3 EE full set
  - 8.6.4 PS1 name
  - 8.6.5 PS2 name
- 8.7 Panel and AB options
  - 8.7.1 Panel name
  - 8.7.2 Panel language
  - 8.7.3 Authorization
  - 8.7.4 Duress method
  - 8.7.5 PIN length
  - 8.7.6 PIN chg mode
  - 8.7.7 Alarm confirm
    - 8.7.7.1 AB mode
    - 8.7.7.2 AB time
      - 8.7.7.2.1 Intrusion AB time
      - 8.7.7.2.2 Holdup AB time
    - 8.7.7.3 System confirm
    - 8.7.7.4 EE confirm
    - 8.7.7.5 EE inhibit
    - 8.7.7.6 TA confirm
    - 8.7.7.7 Sirens
    - 8.7.7.8 Call CS message
    - 8.7.7.9 Reporting delayed
  - 8.7.8 Easy unset
- 8.8 PA and other
  - 8.8.1 Panic mode
  - 8.8.2 Chime
    - 8.8.2.1 Chime in part set
    - 8.8.2.2 Latched chime
  - 8.8.3 System tamper areas
  - 8.8.4 Siren retrigger
  - 8.8.5 Short sup. and IP polling
  - 8.8.6 Card learn-in
  - 8.8.7 Test inputs
  - 8.8.8 Buzzer mode
  - 8.8.9 Card number
- 8.9 Library



- 9 Dialler menu
  - 9.1 Central station
    - 9.1.0 Add CS
    - 9.1.n Select central station

      Common options:
      - 9.1.n.1 CS name
      - 9.1.n.2 Transm path
      - 9.1.n.3 Protocol
      - 9.1.n.5 Accounts
        - 9.1.n.5.m Select area
      - 9.1.n.6 Mode
      - 9.1.n.7 Retry count
      - 9.1.n.8 Protocol opt
        - 9.1.n.8.1 XSIA
          - 9.1.n.8.1.1 Area modifier
          - 9.1.n.8.1.2 Name chars
          - 9.1.n.8.1.3 Event number
          - 9.1.n.8.1.4 Subev coding
          - 9.1.n.8.1.5 SIA frequency
        - 9.1.n.8.2 VOICE
          - 9.1.n.8.2.1 Suppress FTC
          - 9.1.n.8.2.2 Without ACK
      - 9.1.n.9 OP/CL report
      - 9.1.n.10 Delete CS

      PSTN and ISDN specific options:
      - 9.1.n.4 Phone

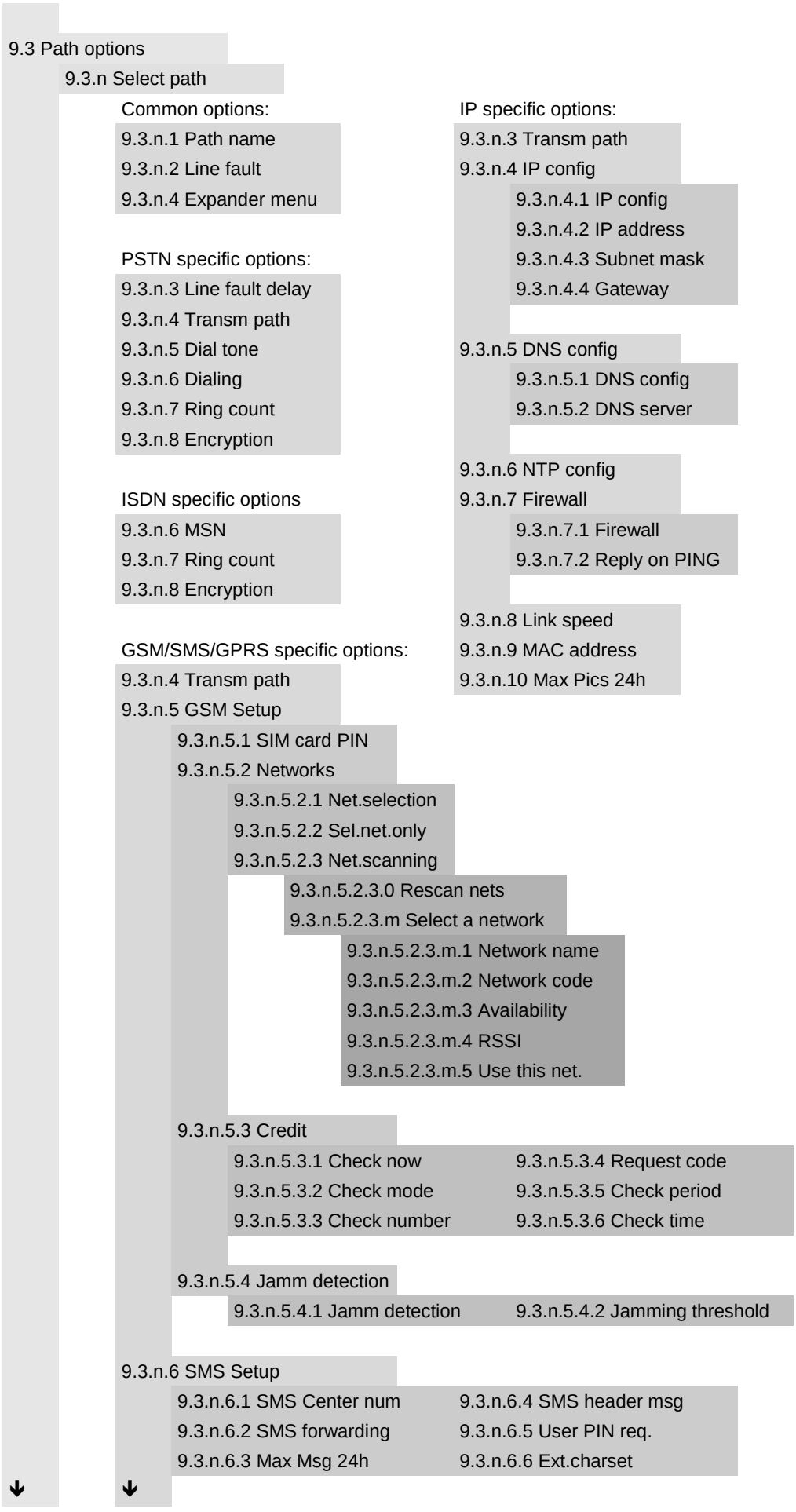
      IP and GSM/GPRS specific options:
      - 9.1.n.4 Destination/IP
        - 9.1.n.4.1 Dest name
        - 9.1.n.4.2 Dest port
        - 9.1.n.4.3 Ping host

      Photo transmission specific options:
      - 9.1.n.4.4 Vid dest port
      - 9.1.n.4.5 Encryption

      GSM/phone specific options:
      - 9.1.n.4 Destination
        - 9.1.n.4.1 Type
        - 9.1.n.4.2 Phone/User/UG

      IP and GSM/GPRS specific options:
      - 9.1.n.8.3 OH 2000
        - 9.1.n.8.3.1 Version
        - 9.1.n.8.3.2 Heartbeat time
        - 9.1.n.8.3.3 Receiver nbr
        - 9.1.n.8.3.4 Line nbr
        - 9.1.n.8.3.5 Freq. HB time
  - 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
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
9.3.n.7 Ring count
9.3.n.8 Encryption
ISDN specific options
9.3.n.6 MSN
9.3.n.7 Ring count
9.3.n.8 Encryption
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.5.3.2 Check mode
9.3.n.5.3.3 Check number
9.3.n.5.3.4 Request code
9.3.n.5.3.5 Check period
9.3.n.5.3.6 Check time
9.3.n.5.4 Jamm detection
9.3.n.5.4.1 Jamm detection
9.3.n.5.4.2 Jamming threshold
9.3.n.6 SMS Setup
9.3.n.6.1 SMS Center num
9.3.n.6.2 SMS forwarding
9.3.n.6.3 Max Msg 24h
9.3.n.6.4 SMS header msg
9.3.n.6.5 User PIN req.
9.3.n.6.6 Ext.charset
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.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

- 9.3.n.7 GPRS Setup
  - 9.3.n.7.1 APN
  - 9.3.n.7.2 User name
  - 9.3.n.7.3 User password
  - 9.3.n.7.4 IP config
  - 9.3.n.7.5 DNS config
  - 9.3.n.7.6 Firewall
  - 9.3.n.7.7 Line fault
  - 9.3.n.7.8 Disconn.time
  - 9.3.n.7.9 Max Pics 24h
- 9.3.n.8 Ring setup
  - 9.3.n.8.1 Ring count
  - 9.3.n.8.2 Omit 1st call
- 9.3.n.9 Encryption
- 9.3.n.10 MMS Setup
  - 9.3.n.10.1 MMS Center
  - 9.3.n.10.2 APN
  - 9.3.n.10.3 User name
  - 9.3.n.10.4 User password
  - 9.3.n.10.5 Proxy
  - 9.3.n.10.6 Proxy port
  - 9.3.n.10.7 Max MMS 24h
- 9.3.n.11 Module info

9.4 PC connection

Common options:

- 9.4.1 Connections
  - 9.4.1.0 Add PC connection
  - 9.4.1.n Select PC connection
    - 9.4.1.n.1 Name
    - 9.4.1.n.2 Transm path
    - 9.4.1.n.4 Phone number
    - 9.4.1.n.5 Retry limit
    - 9.4.1.n.6 Delete PC conn

PSTN specific options:

- 9.4.1.n.3 Modem protocol

GSM specific options:

- 9.4.1.n.3 Conn. type

IP and GSM/GPRS specific options:

- 9.4.1.n.4 Destination/IP
  - 9.4.1.n.4.1 Dest. name
  - 9.4.1.n.4.2 Destination port
  - 9.4.1.n.4.3 Ping host

- 9.4.2 PC callback
  - 9.4.2.1 Primary
  - 9.4.2.2 Backup
- 9.4.3 Encryption key 1
- 9.4.4 Encryption key 2

IP and GSM/GPRS specific options:

- 9.4.5 Listening port