These products are intended for sale to, and installation by, an experienced security professional. UTC Fire & Security cannot provide any assurance that any person or entity buying its products, including any “authorized dealer,” is properly trained or experienced to correctly install security related products.

For more information on product warnings, refer to www.utcfssecurityproducts.eu/productwarning/ or scan the code.

This document applies to the following Advisor Advanced firmware version: MR_4.0

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

ATS1500A(-IP): Security Grade 2, Environmental class II
ATS3500A(-IP): Security Grade 3, Environmental class II
ATS4500A(-IP): Security Grade 3, Environmental class II

Note: ATS1500A(-IP) is upgradable to Security Grade 3 using the ATS-MM-TK (MM enclosure) or the ATS-SM-TK (SM enclosure) tamper kit.

Tested and certified by VdS Schadenverhütung GmbH

Important: To comply with the above standards, it is required to configure the system according to settings listed in Chapter 8 “Regulations” on page 327 onwards.

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

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

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

Important information iii

Chapter 1 Quick installation and programming 1
Quick installation 2
Quick programming 4

Chapter 2 Installation 7
General installation information 8
Maintenance 17
Mounting 19
Earthing 21
Shielding 22
Cabling 23
Configuration 31
Specifications 36

Chapter 3 System functions 43
Function list 45
Zones 47
Areas 52
Set and unset 54
Inhibit and isolate 56
Keys 58
Bus devices 62
Users 64
User groups 66
PIN 71
Outputs 73
Access control 74
Condition filters 80
Triggers 82
Calendar 83
Events 86
Tests and diagnostics 88
Alarm reporting 92
User programmable functions 97
Autoset 101
Wireless device programming 102
Using cameras 109
Engineer reset 113
Timed unset / ATM 114
Two-way audio 115
UltraSync 117
Mobile Application 120
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Programming</td>
<td>121</td>
</tr>
<tr>
<td></td>
<td>The Advisor Advanced menu</td>
<td>122</td>
</tr>
<tr>
<td></td>
<td>How to program the options</td>
<td>124</td>
</tr>
<tr>
<td></td>
<td>Remote access</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>Initial start-up</td>
<td>130</td>
</tr>
<tr>
<td>5</td>
<td>Menu reference</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>1 Service menu</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>2 Device menu</td>
<td>159</td>
</tr>
<tr>
<td></td>
<td>3 User menu</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>4 Zones and areas</td>
<td>191</td>
</tr>
<tr>
<td></td>
<td>5 Door menu</td>
<td>217</td>
</tr>
<tr>
<td></td>
<td>6 Outputs and filters</td>
<td>238</td>
</tr>
<tr>
<td></td>
<td>7 Calendar</td>
<td>246</td>
</tr>
<tr>
<td></td>
<td>8 System option menu</td>
<td>254</td>
</tr>
<tr>
<td></td>
<td>9 Communication</td>
<td>280</td>
</tr>
<tr>
<td>6</td>
<td>Software</td>
<td>313</td>
</tr>
<tr>
<td></td>
<td>Programming Advisor Advanced via configuration software</td>
<td>314</td>
</tr>
<tr>
<td></td>
<td>Upgrading Advisor Advanced firmware</td>
<td>316</td>
</tr>
<tr>
<td>7</td>
<td>Troubleshooting</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Recovery procedure</td>
<td>322</td>
</tr>
<tr>
<td></td>
<td>Device troubleshooting</td>
<td>323</td>
</tr>
<tr>
<td>8</td>
<td>Regulations</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Options affected by EN 50131 regulations</td>
<td>328</td>
</tr>
<tr>
<td></td>
<td>Options affected by other regulations</td>
<td>334</td>
</tr>
<tr>
<td>A</td>
<td>Appendix A</td>
<td>337</td>
</tr>
<tr>
<td></td>
<td>Advisor Advanced events</td>
<td>337</td>
</tr>
<tr>
<td>B</td>
<td>Appendix B</td>
<td>353</td>
</tr>
<tr>
<td></td>
<td>Advisor Advanced reporting codes</td>
<td>353</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>365</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>371</td>
</tr>
<tr>
<td></td>
<td>Programming map</td>
<td>380</td>
</tr>
</tbody>
</table>
Important information

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

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

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

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

Important note

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

List of panel variants

Table 1: List of ATSx500A(-IP) panel variants

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

Notes

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

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

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

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

Advisory messages

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

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

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

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

Safety sign identifies actions or practices that are required by EN 60950 Safety Standard.
Chapter 1
Quick installation and programming

Summary
The chapter contains basic steps of connection and programming of the Advisor Advanced control panel and auxiliary devices.
For more detailed description of the installation process, see Chapter 2 “Installation” on page 7.
For details on programming, see Chapter 4 “Programming” on page 121 and Chapter 5 “Menu reference” on page 133.

Content
Quick installation  2
Quick programming  4
Quick installation

**Chapter 1: Quick installation and programming**

**Quick installation**

1. **USB**
2. **TDA74xxNG**
3. **DC101**
4. **DD1012AM**

**SW1 - Generic settings**
- **LED ON**
- **LED OFF**
- **Remote ON**
- **Remote OFF**
- **Auto Rem. Test ON**
- **Auto Rem. Test OFF**
- **Positive Polarity**
- **Negative Polarity**
- **Range**
  - **4 m (13 ft)**
  - **12 m (40 ft)**
  - **6 m (20 ft)**
  - **9 m (30 ft)**

**SW2 - AM/Fault settings**
- **Mask to alarm and fault relay**
- **Auto reset**
- **Authorized reset**
- **Advanced AM sens.**
- **Standard AM sens.**
- **AM Day mode only**

- **J1**
  - **1K 242**
  - **3K JF**
  - **1K JT**
  - **1K J1**
  - **On = 3 resistor single zone (Terminal 3-10)**
  - **Off = Isolated fault contact**

- **Range**
  - **1**
  - **2**
  - **3**
  - **4**

- **Mask to alarm only**
- **Fault relay only**
- **Authorized reset**
- **Standard AM sens.**
- **AM Day and Night**

- **LED ON**
- **LED OFF**
- **Remote ON**
- **Remote OFF**
- **Auto Rem. Test ON**
- **Auto Rem. Test OFF**
- **Positive Polarity**
- **Negative Polarity**
- **Range**
  - **4 m (13 ft)**
  - **12 m (40 ft)**
  - **6 m (20 ft)**
  - **9 m (30 ft)**

**Adv ADVANCED ATSx500A(-IP) Installation and Programming Manual**
Quick programming

Initial start-up

Note: See “The Advisor Advanced menu” on page 122 for menu explanation. For more information on editing options, see “How to program the options” on page 124.

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

<table>
<thead>
<tr>
<th>Display</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO</td>
<td>Press Enter to continue</td>
</tr>
<tr>
<td>Inst required</td>
<td></td>
</tr>
<tr>
<td>1&gt;Panel language</td>
<td>Choose English</td>
</tr>
<tr>
<td>2&gt;Defaults</td>
<td>Choose EN 50131 Grade 3</td>
</tr>
<tr>
<td>3&gt;Date&amp;time</td>
<td>Set current time and date</td>
</tr>
<tr>
<td>4&gt;UltraSync</td>
<td>Set UltraSync options</td>
</tr>
<tr>
<td></td>
<td>If required, enable UltraSync connectivity, and then enter UltraSync password. If UltraSync is enabled, the panel communication will be configured via security cloud.</td>
</tr>
<tr>
<td>5&gt;Other options</td>
<td>Set other panel options</td>
</tr>
</tbody>
</table>

The following options can be set:

- Duress method
- PIN length
- PIN change mode

See also “Initial start-up” on page 130.

<table>
<thead>
<tr>
<th>Change PIN</th>
<th>Press Enter to continue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor</td>
<td></td>
</tr>
<tr>
<td>New PIN</td>
<td>Enter the new supervisor PIN and press Enter</td>
</tr>
<tr>
<td>Verify</td>
<td>Next, enter the PIN again to verify it.</td>
</tr>
</tbody>
</table>

The panel restarts.

Auto configuration

<table>
<thead>
<tr>
<th>Auto Config?</th>
<th>Press Enter to continue.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Rkp 1-16 BUS1</td>
<td>Wait until the panel configures all bus devices and zones.</td>
</tr>
<tr>
<td>Exp 1-15 BUS1</td>
<td></td>
</tr>
<tr>
<td>Aud 1-16 BUS1</td>
<td></td>
</tr>
</tbody>
</table>

Enabling service in

<table>
<thead>
<tr>
<th>UTC F&amp;S</th>
<th>Enter the supervisor PIN and press Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>THU 05 Mar 12:21</td>
<td></td>
</tr>
<tr>
<td>l&gt;Zone options</td>
<td>Go to menu 8.8 Service in</td>
</tr>
<tr>
<td>2 Isolate</td>
<td></td>
</tr>
<tr>
<td>8&gt;Service in</td>
<td>Enable Installer in time</td>
</tr>
<tr>
<td>Enable?</td>
<td></td>
</tr>
</tbody>
</table>

Press Cancel, Cancel to log off.

Programming menu entry

<table>
<thead>
<tr>
<th>UTC F&amp;S</th>
<th>Enter the installer PIN and press Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>THU 05 Mar 12:21</td>
<td></td>
</tr>
<tr>
<td>Inh reports</td>
<td>Press Enter to continue.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Inh tampers</td>
<td></td>
</tr>
<tr>
<td>Unset areas</td>
<td></td>
</tr>
<tr>
<td>1&gt;Service menu</td>
<td></td>
</tr>
<tr>
<td>2 Device menu</td>
<td></td>
</tr>
</tbody>
</table>
The installer menu is displayed.

**Changing encryption key**

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

Go to 9.4.3 Encryption key 1 and 9.4.4 Encryption key 2 (see page 308).

3 Encrypt.key 1
>000000000000<

Provide encryption key 1.

4 Encrypt.key 2
>000000000000<

Provide encryption key 2.

**Configuring zones**

Go to 4.1 Zone menu (see page 191).

4>Zones&Areas
Press Enter.

1>Zone menu
Press Enter.

0>Add zone
1 Zone 1
Select a zone.

For each zone used in the system, enter zone name in 4.1.n.1 Zone name (page 192).

01 Zone name
>1 Zone 1 <

Next, set its zone type in 4.1.n.2 Zone type (see page 192).

02 Zone type
>Entry/Exit 1<

**Adding users**

Go to menu 3.1 Users (see page 182).

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

Add mode
>Manual<
Press Enter.

INFO
User added

01>User name
User 3

01 User name
> User 3 <

Enter a new user name.

Configure other options of the user:

- 3.1.n.2 PIN (page 183)
- 3.1.n.3 User card (page 184)
- 3.1.n.6 User groups (page 185), etc.

Repeat for other users.

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

[Lock user data?]
>Cancel<

Choose OK and confirm.

**Configuring areas**

Go to 4.2 Areas (see page 206).

Change the area name in 4.2.n.1 Area name (see page 206).

1 Area name
>Area 1 <

Enter a new area name.

Configure other options of the area:

- 4.2.n.2 Exit time (see page 206)
- 4.2.n.3 Entry time (see page 207), etc.

**Caution:** Before enabling 4.2.n.5.4 Dual unset (see page 209), make sure to add users that can assist the unset. See “Adding users” above.

**Configuring Central Station**

Configure the communication path in 9.3 Path options (page 291).

1>PSTN
3 GSM/SMS/GPRS

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

Next, go to menu 9.1 Central station (page 280).

0>Add CS
1 CS 1

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

- 9.1.n.1 CS name (page 281)
- 9.1.n.2 Transm path (page 281)
- 9.1.n.3 Protocol (page 281)
- 9.1.n.5 Accounts (page 282)
Chapter 1: Quick installation and programming

- Other options, depending on the communication path used.

Test the communication using menu 1.2.6.n.6 Man. test call (page 147), where <n> is the number of the configured Central Station.

Calling CS 1...
Ready

Regulations

If necessary, follow the instructions given in Chapter 8 “Regulations” on page 327 to configure other options, required by the appropriate standards and norms.
Chapter 2
Installation

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

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

Content
General installation information 8
  Advisor Advanced housings 8
  Advisor Advanced layout 12
  Keypads and readers 13
Maintenance 17
  Mains power connection 17
  Battery replacement 17
Mounting 19
  General installation guidelines 19
Earthing 21
Shielding 22
Cabling 23
  System databus preferred wiring 23
  System databus connection 23
  Zone connection 24
  Values for end-of-line resistors 25
  EOL connection types 28
  Siren connection 29
  Other connections 29
Configuration 31
  Defaulting the panel 31
  Zone configuration 31
  Outputs 31
  Zone, output, and door addressing 32
Specifications 36
  Auxiliary current and battery capacity 40
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)

![Small metal housing diagram]

Figure 2: Medium metal housing (-MM)

![Medium metal housing diagram]
Figure 3: Large polycarbonate housing (-LP)

Figure 4: Medium metal housing (-MM+)
For more details on connections and connecting devices to the Advisor Advanced, see “Cabling” on page 23.

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

**Pry-off tamper mounting**

For small housing (SM), follow the steps in Figure 6 on page 11 to install pry-off tamper. For medium (MM and MM+), and large housings (LM), follow the steps in Figure 7 on page 11. For large plastic housing (LP), follow the steps in Figure 8 on page 12.
Chapter 2: Installation

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

Figure 7: Medium (MM and MM+) and large housing (LM) pry-off tamper mount
Chapter 2: Installation

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

**Advisor Advanced layout**

**Figure 9: Advisor Advanced ATSx500A(-IP) PCB layout**

- (1) Interface to output expander
- (2) USB fault LED
- (3) USB power LED
- (4) USB connector (micro-A/B type)
- (5) IP communication LED (ATS-IP only)
- (6) Heartbeat LED
- (7) Mi-bus connector for MI devices
- (8) Interface to input expander
- (9) Interface to PSTN module
- (10) Optional: enclosure ambient temperature sensor
- (11) ATS670 databus expander connector
- (12) Panel earth terminal
- (13) External tamper switch
- (14) Optional: enclosure ambient temperature sensor
- (15) RS-485 system databus connections
- (16) T2: Device firmware upgrade mode (DFU)
- (17) RS-485 system databus communication LEDs
- (18) T1: Restores installer default PIN
- (19) System databus termination jumper
- (20) AC power supply terminal
- (21) Battery connection
- (22) Low current (OC) outputs
- (23) High current outputs
- (24) Siren tamper switch
- (25) 12 VDC auxiliary power output
- (26) Zone inputs
Keypads and readers

Figure 10: ATS111xA keypad

Figure 11: 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
            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
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 15 | ▼ / Down | Scroll down in the menus
|   |   | Change value
|   |   | Backspace
| 16 | Alphanumeric keys | Keys 1 to 9, alphanumerical data. See “Keypad layout” on page 128.
| 17 | Menu | Request entry to the menus
| 18 | Enter | Complete the step
|   |   | Enter the selected menu entry
| 19 | 0 | Key 0
|   |   | Toggle selection
| 20 | Area LEDs 1 to 16 | On: area set. See also "Access control indication note" on page 16.
|   |   | Off: area unset.
|   |   | Flashing: area alarm condition.
| 21 | Partset 1 | Part set 1 of areas
| 22 | Partset 2 | Part set 2 of areas
| 23 | A, B, C | Programmable function keys
| 24 | LED1 | Programmable LED 1
| 25 | LED2 | Programmable LED 2
### Figure 12: ATS1190/ATS1192 readers

![ATS1190/ATS1192 readers diagram]

### Figure 13: ATS1197 reader with keypad

![ATS1197 reader with keypad diagram]

### Figure 14: ATS1151/ATS1156 readers

![ATS1151/ATS1156 readers diagram]

<table>
<thead>
<tr>
<th>(1) Blue LED</th>
<th>Access granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Red LED</td>
<td>On: area set</td>
</tr>
<tr>
<td></td>
<td>Flashing: general alert (EN 50131)</td>
</tr>
<tr>
<td>(3) Dual LED</td>
<td>Green on: AC mains supply on.</td>
</tr>
<tr>
<td></td>
<td>Green flashing: AC mains supply off, or unlocked while unset.</td>
</tr>
<tr>
<td></td>
<td>Red on: all areas set. See also “Access control indication note” on page 16.</td>
</tr>
<tr>
<td></td>
<td>Red flashing: unlocked while set.</td>
</tr>
<tr>
<td>(4) Yellow LED</td>
<td>On: All zones are in normal state</td>
</tr>
<tr>
<td></td>
<td>Red flashing: general alert (EN 50131)</td>
</tr>
<tr>
<td>(5) Red LED</td>
<td>Flashtaking: alarm</td>
</tr>
<tr>
<td>(6) Numeric keys</td>
<td>Keys 0 to 9, numerical data</td>
</tr>
<tr>
<td>(7) Off</td>
<td>Unset an area</td>
</tr>
<tr>
<td>(8) On</td>
<td>Full set an area</td>
</tr>
</tbody>
</table>
Access control indication note

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

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

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

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

Mains power connection

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

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

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

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

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

In all cases local regulations must be observed.

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

Battery replacement

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

**To remove a battery:**

1. Make sure that your product settings allow you to open the cover without starting the tamper alarm.

2. Switch off the mains power, if necessary, and remove the cover.
3. Disconnect the battery. Note that depending on the battery model the connectors may be located differently.

4. Remove the battery from the holder.

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

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

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

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

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

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

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

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

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

General installation guidelines

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

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

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

• Ensure that there is a good earth available for the alarm system.

• Maintain a separation between low voltage and mains supply cables. Use separate points of cable entry to the control panel cabinet.

• If the upper and/or lower cabinet entry cable holes are used to route wiring into the control panel, always use a proper pipe fitting system by means of an appropriate conduit and junction box. For this purpose, use only materials of suitable flammability class (HB or better).
• For mains power connection, use the mains connector terminal either through a permanent wiring or a flexible mains cable to an earthed mains outlet. Always use cable ties to fix the mains cable at the dedicated fixing point provided near the mains terminal connector.

  - When installing permanent, fixed wiring, insert an easily accessible, dedicated bipolar circuit breaker in the power distribution network.
  
  - Never attempt to solder mains connection wires at the ends where they will be wired to the terminal connectors.

• Avoid loops of wire inside the control panel cabinet and route cables so that they do not lie on top or underneath of the printed circuit board. The use of cable ties is recommended and improves neatness of the wiring within the box.

• The battery used with this unit, must be made of materials of suitable flammability class (HB or better).

• Any circuit connected either directly to the onboard relay contacts or to the external relay contacts through the onboard electronic output must be rated as a SELV (safety extra-low voltage) operating circuit.

  - A mains switching relay must not be fitted inside the control panel cabinet.
  
  - Always place a suppression diode (e.g. a 1N4001) across the relay coil.
  
  - Use only relays with good insulation between the contacts and the coil.
  
  - Maximum cable length for open collector output connection may not exceed 30 m. For longer distances, use relay output expansion (for example, ATS624 four-relay expander).

• The minimum clearance between equipment closures is 50 mm (between equipment vents).

• Only use these units in a clean environment and not in humid air. Environmental requirements are given in “Specifications” on page 36.

• 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.
Chapter 2: Installation

Shielding

The shielding of all shielded cables used in the system should only be connected at one side to one common earthing point in a building (see Figure 15 below). If a shielded databus cable is routed via more than one plastic device the shielding from incoming and outgoing cable must be connected.

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

Figure 15: System shielding

(1) Building 1
(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

System databus preferred wiring

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

Figure 16: System databus wiring

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

System databus connection

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

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

We recommend that you use a separate power supply for a keypad when the distance between that keypad and the nearest device is more than 100 meters.

If the keypad is powered with a separate power supply, do not connect “+” from the system databus. Connect “+” of the local power supply to “+” on the keypad, and connect 0 volts from the power supply and 0 volts from the system databus.
to the keypad terminal marked “−”. The maximum number of devices allowed on the databus is given in “General features” on page 37.

**Two system databuses (ATS4500A only)**

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

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

**Note:** Door controllers can only be installed on BUS1.

**Zone connection**

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

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

- Choose your EOL connection type. See “EOL connection types” on page 28.
- Program input mode. See “8.6.1 Input mode” on page 270 for the panel, or “2.2.2.n.4.4 Input mode” on page 170 for expanders.
- Set end-of-line resistor values. See “8.6.2 EOL” on page 270 for the panel, or “2.2.2.n.4.5 EOL” on page 170 for expanders.
- Configure anti-masking option. See “4.1.n.6.7 Anti mask” on page 194.

**Single loop zone wiring**

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

**Figure 17: Single loop examples**
Dual loop zone wiring

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

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

Figure 18: Dual loop example

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.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Single NC (Item 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No EOL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R (kΩ)</td>
<td></td>
<td></td>
<td></td>
<td>&lt;1</td>
<td>&gt;1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
<td></td>
<td></td>
<td></td>
<td>&lt;3.5</td>
<td>&gt;3.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: Values for other EOL are equal to Dual, except all ranges but normal are alarm ranges.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single NO (Item 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No EOL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;44.70</td>
<td>&lt;44.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
<td></td>
<td></td>
<td></td>
<td>&gt;11.14</td>
<td>&lt;11.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: Values for other EOL are equal to Dual, except all ranges but normal are alarm ranges.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA=10 kΩ, RT=5 kΩ, RF=5 kΩ</td>
<td>U (V)</td>
<td>&lt;5.70</td>
<td>5.70– 8.10</td>
<td>8.10– 10.20</td>
<td>10.20– 11.70</td>
<td>—</td>
<td>&gt;11.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4K7 (Item 3)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;1.00</td>
<td>1.00– 6.67</td>
<td>6.67– 16.84</td>
<td>—</td>
<td>&gt;16.84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA=4.7 kΩ, RT=4.7 kΩ</td>
<td>U (V)</td>
<td>&lt;2.41</td>
<td>2.41– 8.07</td>
<td>8.07– 10.74</td>
<td>—</td>
<td>&gt;10.74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4K7 (Item 4)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;1.00</td>
<td>1.00– 6.67</td>
<td>6.67– 16.84</td>
<td>—</td>
<td>&gt;16.84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA=4.7 kΩ, RT=2.35 kΩ, RF=2.35 kΩ</td>
<td>U (V)</td>
<td>&lt;2.41</td>
<td>2.41– 5.79</td>
<td>5.79– 8.07</td>
<td>8.07– 10.74</td>
<td>—</td>
<td>&gt;10.74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4K7 (Item 7)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;1.00</td>
<td>1.00– 6.67</td>
<td>6.67– 11.75</td>
<td>11.75– 16.84</td>
<td>—</td>
<td>&gt;55.00</td>
<td></td>
</tr>
<tr>
<td>RA=4.7 kΩ, RT=4.7 kΩ, RF=10 kΩ</td>
<td>U (V)</td>
<td>&lt;2.41</td>
<td>2.41– 12.70</td>
<td>12.70– 24.1</td>
<td>24.1– 31.7</td>
<td>31.7– 40.0</td>
<td>40.0– 50.0</td>
<td>&gt;12.70</td>
<td></td>
</tr>
<tr>
<td>2K2 (Item 4)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;0.73</td>
<td>0.73– 1.47</td>
<td>1.47– 2.93</td>
<td>2.93– 5.87</td>
<td>—</td>
<td>&gt;5.87</td>
<td></td>
</tr>
<tr>
<td>RA=2.2 kΩ, RT=1.1 kΩ, RF=1.1 kΩ</td>
<td>U (V)</td>
<td>&lt;1.90</td>
<td>1.90– 3.30</td>
<td>3.30– 5.30</td>
<td>5.30– 7.70</td>
<td>—</td>
<td>&gt;7.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6K8 (Item 4)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;2.27</td>
<td>2.27– 4.53</td>
<td>4.53– 9.07</td>
<td>9.07– 18.13</td>
<td>—</td>
<td>&gt;18.13</td>
<td></td>
</tr>
<tr>
<td>RA=6.8 kΩ, RT=3.4 kΩ, RF=3.4 kΩ</td>
<td>U (V)</td>
<td>&lt;4.50</td>
<td>4.50– 6.80</td>
<td>6.80– 9.10</td>
<td>9.10– 11.00</td>
<td>—</td>
<td>&gt;11.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5K6 (Item 4)</td>
<td></td>
<td>R (kΩ)</td>
<td>&lt;1.87</td>
<td>1.87– 3.73</td>
<td>3.73– 7.47</td>
<td>7.47– 14.93</td>
<td>—</td>
<td>&gt;14.93</td>
<td></td>
</tr>
<tr>
<td>RA=5.6 kΩ, RT=2.8 kΩ, RF=2.8 kΩ</td>
<td>U (V)</td>
<td>&lt;3.90</td>
<td>3.90– 6.10</td>
<td>6.10– 8.50</td>
<td>8.50– 10.50</td>
<td>—</td>
<td>&gt;10.50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Zone state

<table>
<thead>
<tr>
<th>EOL</th>
<th>Connection details [1]</th>
<th>Zone state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Measure [2]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=3.74 kΩ, RT=1.87 kΩ, RF=1.87 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3K3</td>
<td>(Item 4)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=3.3 kΩ, RT=1.65 kΩ, RF=1.65 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2K</td>
<td>(Item 4)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=2 kΩ, RT=1 kΩ, RF=1 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1K5</td>
<td>(Item 4)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=1.5 kΩ, RT=0.75 kΩ, RF=0.75 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2K2+4K7</td>
<td>(Item 3)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=2.2 kΩ, RT=4.7 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1K</td>
<td>(Item 7)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=1 kΩ, RT=1 kΩ, RF=12 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8K2</td>
<td>(Item 5)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U (V)</td>
</tr>
<tr>
<td>RA=8.2 kΩ, RT=8.2 kΩ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8K2</td>
<td>(Item 6)</td>
<td>R (kΩ)</td>
</tr>
<tr>
<td>RA=8.2 kΩ, RT=8.2 kΩ, RF=8.2 kΩ</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[1] Refer to Figure 19 on page 28.

[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 25 for more details.

Figure 19: Connection type

<table>
<thead>
<tr>
<th>(1) Single NC</th>
<th>(2) Single NO</th>
<th>(3) Dual A (default)</th>
<th>(4) Dual A with AM</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Connection Diagram" /></td>
<td><img src="image2" alt="Connection Diagram" /></td>
<td><img src="image3" alt="Connection Diagram" /></td>
<td><img src="image4" alt="Connection Diagram" /></td>
</tr>
<tr>
<td>(5) Dual B</td>
<td>(6) Dual C with AM</td>
<td>(7) Dual D with AM</td>
<td></td>
</tr>
<tr>
<td><img src="image5" alt="Connection Diagram" /></td>
<td><img src="image6" alt="Connection Diagram" /></td>
<td><img src="image7" alt="Connection Diagram" /></td>
<td></td>
</tr>
</tbody>
</table>

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.6.7 Anti mask” on page 194.
Siren connection

Figure 20: Siren connection examples

1. Siren EOL resistor (1 kΩ). It must be installed if siren does not contain a built-in resistor.
2. Siren.
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 32 and “Outputs” on page 73.

Other connections

Tamper connection

Figure 21: Earthing and tamper connection in ATSx500A(-IP)

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

PSTN connection

To connect PSTN in ATSx500A(-IP) control panels, use ATS7700 PSTN module. See ATS7700 PSTN Module Installation Sheet for details.

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

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

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

Defaulting the panel
When the panel is initially powered up, you are prompted to choose the appropriate default settings. Choose the correct settings for your local regulations. The panel then completes the installation process. See “Initial start-up” on page 130.

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 37.

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 37.

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

Note: Zone capacity is the number of configurable zones in the system. These zones may be located at any available input. See “Specifications > General features” on page 37.

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 37.
Notes

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

Siren outputs

The siren outputs on the Advisor Advanced control panel have addresses starting from 1 (see Table 2 below).

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

To enable the siren output, the programmed output must have the required condition filter assigned (defined by an alarm event or a siren event, depending on the preference settings). See “Outputs” on page 73 for more details.

Default output assignments

The default output assignments are shown in Table 2 below.

<table>
<thead>
<tr>
<th>Output</th>
<th>Name</th>
<th>Type</th>
<th>Default output function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel 1</td>
<td>S1</td>
<td>High current output</td>
<td>EN 50131 Grade 3: Internal siren output S1 VdS: External siren output S1</td>
</tr>
<tr>
<td>Panel 2</td>
<td>S2</td>
<td>High current output</td>
<td>EN 50131 Grade 3: External siren output S1 VdS: External siren output S2</td>
</tr>
<tr>
<td>Panel 3</td>
<td>S3</td>
<td>High current output</td>
<td>EN 50131 Grade 3: Programmable siren output VdS: External strobe output S3</td>
</tr>
<tr>
<td>Panel 4</td>
<td>S4</td>
<td>Low current output</td>
<td>A1 ready to set</td>
</tr>
<tr>
<td>Panel 5</td>
<td>S5</td>
<td>Low current output</td>
<td>A1 set</td>
</tr>
<tr>
<td>Keypad 7</td>
<td>—</td>
<td>Virtual</td>
<td>Continuous buzzer sound</td>
</tr>
<tr>
<td>Keypad 8</td>
<td>—</td>
<td>Virtual</td>
<td>Intermittent buzzer sound</td>
</tr>
</tbody>
</table>

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

Zone, output, and door addressing

Zones and outputs

Table 3 on page 33 shows the zone and output addressing in the Advisor Advanced system.

Note: This is the default numbering in a classic numbering scheme. To change it and create objects with numbering independent on physical inputs or outputs, use menu “8.7.9 Object scheme” on page 276.
### Table 3: Zone and output numbering

<table>
<thead>
<tr>
<th>Device</th>
<th>Zones</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel</td>
<td>1–8</td>
<td>1–8</td>
</tr>
<tr>
<td>Input expander (ATS608)</td>
<td>9–16</td>
<td>N/A</td>
</tr>
<tr>
<td>Expander 1</td>
<td>17–48</td>
<td>17–48</td>
</tr>
<tr>
<td>Expander 2</td>
<td>49–80</td>
<td>49–80</td>
</tr>
<tr>
<td>Expander 3</td>
<td>81–112</td>
<td>81–112</td>
</tr>
<tr>
<td>Expander 4</td>
<td>113–144</td>
<td>113–144</td>
</tr>
<tr>
<td>Expander 5</td>
<td>145–176</td>
<td>145–176</td>
</tr>
<tr>
<td>Expander 6</td>
<td>177–208</td>
<td>177–208</td>
</tr>
<tr>
<td>Expander 7</td>
<td>209–240</td>
<td>209–240</td>
</tr>
<tr>
<td>Expander 8</td>
<td>241–272</td>
<td>241–272</td>
</tr>
<tr>
<td>Expander 9</td>
<td>273–304</td>
<td>273–304</td>
</tr>
<tr>
<td>Expander 10</td>
<td>305–336</td>
<td>305–336</td>
</tr>
<tr>
<td>Expander 11</td>
<td>337–368</td>
<td>337–368</td>
</tr>
<tr>
<td>Expander 12</td>
<td>369–400</td>
<td>369–400</td>
</tr>
<tr>
<td>Expander 13</td>
<td>401–432</td>
<td>401–432</td>
</tr>
<tr>
<td>Expander 14</td>
<td>433–464</td>
<td>433–464</td>
</tr>
<tr>
<td>Expander 17</td>
<td>529–560</td>
<td>529–560</td>
</tr>
<tr>
<td>Expander 18</td>
<td>561–592</td>
<td>561–592</td>
</tr>
<tr>
<td>Expander 19</td>
<td>593–624</td>
<td>593–624</td>
</tr>
<tr>
<td>Expander 20</td>
<td>625–656</td>
<td>625–656</td>
</tr>
<tr>
<td>Expander 21</td>
<td>657–688</td>
<td>657–688</td>
</tr>
<tr>
<td>Expander 22</td>
<td>689–720</td>
<td>689–720</td>
</tr>
<tr>
<td>Expander 23</td>
<td>721–752</td>
<td>721–752</td>
</tr>
<tr>
<td>Expander 24</td>
<td>753–784</td>
<td>753–784</td>
</tr>
<tr>
<td>Expander 25</td>
<td>785–816</td>
<td>785–816</td>
</tr>
<tr>
<td>Expander 26</td>
<td>817–848</td>
<td>817–848</td>
</tr>
<tr>
<td>Expander 27</td>
<td>849–880</td>
<td>849–880</td>
</tr>
<tr>
<td>Expander 28</td>
<td>881–912</td>
<td>881–912</td>
</tr>
<tr>
<td>Expander 29</td>
<td>913–944</td>
<td>913–944</td>
</tr>
<tr>
<td>Expander 30</td>
<td>945–976</td>
<td>945–976</td>
</tr>
<tr>
<td>2X ATS1810 relay cards</td>
<td>—</td>
<td>17–24 [1]</td>
</tr>
<tr>
<td>Output expander (ATS62x)</td>
<td>—</td>
<td>9–16 [2]</td>
</tr>
<tr>
<td>Keypad 1</td>
<td>—</td>
<td>1001–1008</td>
</tr>
<tr>
<td>Keypad 2</td>
<td>—</td>
<td>1009–1016</td>
</tr>
<tr>
<td>Keypad 3</td>
<td>—</td>
<td>1017–1024</td>
</tr>
<tr>
<td>Keypad 4</td>
<td>—</td>
<td>1025–1032</td>
</tr>
<tr>
<td>Keypad 5</td>
<td>—</td>
<td>1033–1040</td>
</tr>
<tr>
<td>Keypad 6</td>
<td>—</td>
<td>1041–1048</td>
</tr>
<tr>
<td>Keypad 7</td>
<td>—</td>
<td>1049–1056</td>
</tr>
<tr>
<td>Keypad 8</td>
<td>—</td>
<td>1057–1064</td>
</tr>
<tr>
<td>Keypad 9</td>
<td>—</td>
<td>1065–1072</td>
</tr>
<tr>
<td>Keypad 10</td>
<td>—</td>
<td>1073–1080</td>
</tr>
<tr>
<td>Keypad 11</td>
<td>—</td>
<td>1081–1088</td>
</tr>
<tr>
<td>Keypad 12</td>
<td>—</td>
<td>1089–1096</td>
</tr>
<tr>
<td>Keypad 13</td>
<td>—</td>
<td>1097–1104</td>
</tr>
<tr>
<td>Keypad 14</td>
<td>—</td>
<td>1105–1112</td>
</tr>
<tr>
<td>Keypad 15</td>
<td>—</td>
<td>1113–1120</td>
</tr>
<tr>
<td>Keypad 16</td>
<td>—</td>
<td>1121–1128</td>
</tr>
<tr>
<td>Keypad 18</td>
<td>—</td>
<td>1137–1144</td>
</tr>
<tr>
<td>Keypad 19</td>
<td>—</td>
<td>1145–1152</td>
</tr>
<tr>
<td>Keypad 20</td>
<td>—</td>
<td>1153–1160</td>
</tr>
<tr>
<td>Keypad 21</td>
<td>—</td>
<td>1161–1168</td>
</tr>
<tr>
<td>Keypad 22</td>
<td>—</td>
<td>1169–1176</td>
</tr>
<tr>
<td>Keypad 23</td>
<td>—</td>
<td>1177–1184</td>
</tr>
<tr>
<td>Keypad 24</td>
<td>—</td>
<td>1185–1192</td>
</tr>
<tr>
<td>Keypad 25</td>
<td>—</td>
<td>1193–1200</td>
</tr>
<tr>
<td>Keypad 26</td>
<td>—</td>
<td>1201–1208</td>
</tr>
<tr>
<td>Keypad 27</td>
<td>—</td>
<td>1209–1216</td>
</tr>
<tr>
<td>Keypad 28</td>
<td>—</td>
<td>1217–1224</td>
</tr>
<tr>
<td>Keypad 29</td>
<td>—</td>
<td>1225–1232</td>
</tr>
<tr>
<td>Keypad 30</td>
<td>—</td>
<td>1233–1240</td>
</tr>
<tr>
<td>Keypad 31</td>
<td>—</td>
<td>1241–1248</td>
</tr>
<tr>
<td>Keypad 32</td>
<td>—</td>
<td>1249–1256</td>
</tr>
</tbody>
</table>

[1] Output 17 to 24 states are duplicated on ATS1810 relays and Expander 1 outputs.
Chapter 2: Installation

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

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

[4] You cannot connect more than 15 expanders and 16 keypads to one system databus. To connect more bus devices to a panel, it is necessary to install ATS670 second RS485 LAN extension module. See also “Two system databuses” on page 24.

Doors

There are two types of doors, intelligent and standard. Standard doors (1 to 16) are handled by the control panel. Keypads or readers 1 to 32 connected to the Advisor Advanced control panel system databuses are used for simple access control functions.

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

See “Doors” on page 74 for more details.

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

Table 4: Door, zone, and output numbering in door controllers

<table>
<thead>
<tr>
<th>Door controller</th>
<th>Doors</th>
<th>Zones</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17–20</td>
<td>17–48</td>
<td>17–48</td>
</tr>
<tr>
<td>2</td>
<td>21–24</td>
<td>49–80</td>
<td>49–80</td>
</tr>
<tr>
<td>3</td>
<td>25–28</td>
<td>81–112</td>
<td>81–112</td>
</tr>
<tr>
<td>4</td>
<td>29–32</td>
<td>113–144</td>
<td>113–144</td>
</tr>
<tr>
<td>5</td>
<td>33–36</td>
<td>145–176</td>
<td>145–176</td>
</tr>
<tr>
<td>6</td>
<td>37–40</td>
<td>177–208</td>
<td>177–208</td>
</tr>
<tr>
<td>7</td>
<td>41–44</td>
<td>209–240</td>
<td>209–240</td>
</tr>
<tr>
<td>8</td>
<td>45–48</td>
<td>241–272</td>
<td>241–272</td>
</tr>
<tr>
<td>9</td>
<td>49–52</td>
<td>273–304</td>
<td>273–304</td>
</tr>
<tr>
<td>10</td>
<td>53–56</td>
<td>305–336</td>
<td>305–336</td>
</tr>
<tr>
<td>11</td>
<td>57–60</td>
<td>337–368</td>
<td>337–368</td>
</tr>
<tr>
<td>12</td>
<td>61–64</td>
<td>369–400</td>
<td>369–400</td>
</tr>
</tbody>
</table>
Table 5 below shows the default zone and output assignment for door controllers.

Table 5: Default zone and output assignment in door controllers

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

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

Table 6: Default reader assignment in door controllers

<table>
<thead>
<tr>
<th>Reader function</th>
<th>IN reader</th>
<th>IN reader 2</th>
<th>OUT reader</th>
<th>OUT reader 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st door</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>2nd door</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>3rd door</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>4th door</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>
Specifications

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

<table>
<thead>
<tr>
<th>Mains power specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mains input voltage</td>
</tr>
<tr>
<td>Current consumption at 230 VAC:</td>
</tr>
<tr>
<td>ATS1500A(-IP)</td>
</tr>
<tr>
<td>ATS3500A(-IP), ATS4500A-IP</td>
</tr>
<tr>
<td>Transformer output:</td>
</tr>
<tr>
<td>ATS1500A(-IP)-SM/LP</td>
</tr>
<tr>
<td>ATSx500A(-IP)-MM/MM+/LM</td>
</tr>
<tr>
<td>ATS3500A(-IP)-LP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power supply specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Power supply voltage [1]</td>
</tr>
<tr>
<td>Power supply current:</td>
</tr>
<tr>
<td>ATS1500A(-IP)</td>
</tr>
<tr>
<td>ATS3500A(-IP)</td>
</tr>
<tr>
<td>ATS4500A-IP</td>
</tr>
<tr>
<td>Main board consumption:</td>
</tr>
<tr>
<td>ATSx500A</td>
</tr>
<tr>
<td>ATSx500A-IP</td>
</tr>
<tr>
<td>Maximum system current available [2]</td>
</tr>
<tr>
<td>ATS1500A</td>
</tr>
<tr>
<td>ATS1500A-IP</td>
</tr>
<tr>
<td>ATS3500A</td>
</tr>
<tr>
<td>ATS3500A-IP</td>
</tr>
<tr>
<td>ATS4500A-IP</td>
</tr>
<tr>
<td>Auxiliary power output (AUX. POWER) [3]</td>
</tr>
<tr>
<td>Battery power output (BAT) [4]</td>
</tr>
<tr>
<td>Battery type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Maximum voltage at power supply, auxiliary power output and battery power output | 14.5 V≈
---|---
Battery low condition | From 9.5 to 10.5 V≈
Battery test level [6] | 11.2 V≈
Minimum voltage (battery recharging) at power supply, auxiliary power output and battery power output [7][8] | 9.45 V≈
Maximum ripple voltage V, p-p [9] | 100 mV typical, 300 mV max.
Overvoltage trigger value [10] | 15.5 V≈ min.

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


[3] Maximum permanent current to power devices external to the control equipment in the absence of alarm conditions. The sum of the auxiliary and COMM power output current cannot exceed the maximum current specified in “Auxiliary current and battery capacity” on page 40.

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

[5] The housings applicable for particular batteries are specified in “Auxiliary current and battery capacity” on page 40.

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

[7] Deep discharge protection mechanism monitors the battery voltage and disconnects the battery if the voltage falls below indicated value, as required by EN 50131 Grade 3 and VdS-C regulations.

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

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

[10] Overvoltage protection mechanism monitors the power supply voltage and shuts down the PSU if the voltage raises above indicated value, as required by EN 50131 Grade 3 and VdS-C regulations.

### General features

<table>
<thead>
<tr>
<th>Code combinations</th>
<th>ATS1500A(-IP)</th>
<th>ATS3500A(-IP)</th>
<th>ATS4500A-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-of-line resistor</td>
<td>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</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Onboard zones</td>
<td>8 (expandable to 16 with 1X ATS608)</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Maximum zone number</td>
<td>32</td>
<td>128</td>
<td>512</td>
</tr>
<tr>
<td>Onboard outputs</td>
<td>5 (expandable to 9 with 1X ATS624, or to 21 with 1X ATS626). See “Standard onboard outputs” on page 39.</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Maximum output number</td>
<td>---</td>
<td>---</td>
<td>128</td>
</tr>
<tr>
<td>Areas</td>
<td>4</td>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>Area groups</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Maximum keypad / RAS number</td>
<td>8</td>
<td>16</td>
<td>32 [1]</td>
</tr>
<tr>
<td>Maximum expander / DGP number</td>
<td>7</td>
<td>15</td>
<td>30 [1]</td>
</tr>
</tbody>
</table>

[1] It is necessary to install ATS670 second RS485 LAN extension module to connect more than 16 RASes and 15 DGPs.
### Maximum user number (for users with SMS and voice reporting functionality)

<table>
<thead>
<tr>
<th></th>
<th>50</th>
<th>200</th>
<th>1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>User groups</td>
<td>16</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>Inhibit / isolate / shunt limit, max.</td>
<td>32</td>
<td>128</td>
<td>512</td>
</tr>
<tr>
<td>Schedules</td>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time frames</td>
<td></td>
<td></td>
<td>4 per schedule</td>
</tr>
<tr>
<td>Special days</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Actions per schedule</td>
<td></td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>

### Event log capacity

15500, which includes:
- 1000 mandatory events
- 1500 non-mandatory events
- 10000 access events
- 1000 installer events
- 1000 dialler events
- 1000 extended events

**Note:** See also “Events” on page 86.

### Data retention (log, program settings)

20 years

### Access control features

<table>
<thead>
<tr>
<th></th>
<th>ATS1500A(-IP)</th>
<th>ATS3500A(-IP)</th>
<th>ATS4500A-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door controllers supported</td>
<td>7</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Standard doors</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Intelligent doors</td>
<td>28</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Regions</td>
<td></td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>Door groups</td>
<td></td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Maximum user number (with door controllers connected)</td>
<td>2000</td>
<td>17488 (with ATS1831 IUM installed)</td>
<td>64532 (with ATS1832 IUM installed)</td>
</tr>
</tbody>
</table>

**Note:** SMS and voice reporting features are only available for a limited user number. Maximum number of users with full control and reporting functionality is given in “General features” on page 37.

### Audio features

<table>
<thead>
<tr>
<th></th>
<th>8</th>
<th>16</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum audio device number</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### UltraSync features

<table>
<thead>
<tr>
<th></th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of push notifications</td>
<td></td>
</tr>
</tbody>
</table>

### Ethernet connection (IP only)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported standard</td>
<td>IEEE 802.3u</td>
</tr>
<tr>
<td>Speed</td>
<td>10BASE-T or 100BASE-TX</td>
</tr>
<tr>
<td>Duplex</td>
<td>Half-duplex and full-duplex</td>
</tr>
<tr>
<td>Cabling</td>
<td>FTP (foiled twisted pair) Cat 5e cable or better</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>MDIX</td>
</tr>
</tbody>
</table>
## Standard onboard outputs

| S1, S2, S3 | High current electronic output, rating: 1 A at 13.8 V<sub>max</sub> |
| S4, S5 [1] | Low current electronic output, rating: 50 mA at 13.8 V<sub>max</sub> |

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

## Environmental

| Operating temperature | 0 to +40°C |
| Tested temperature according EN 50131 | −10 to +55°C |
| Humidity | 95% noncondensing |
| IP protection grade | IP31 |
| Colour | Beige |
| Dimensions | See “List of panel variants” on page iii |

### EN 50131 grade and class

- ATS1500A(-IP): Grade 2, Class II
- ATS3500A(-IP): Grade 3, Class II
- ATS4500A(-IP): Grade 3, Class II

**Note:** ATS1500A(-IP)-MM can be upgraded to an EN Grade 3 setup with the use of the ATS-MM-TK tamper kit. ATS1500A(-IP)-SM can be upgraded to an EN Grade 3 setup with the use of the ATS-SM-TK tamper kit.

### Safety class

Class I

### Enclosure type

Enclosure (meets UL94V-0)

### Overvoltage category

Category II

### Maximum altitude, or minimum air pressure

2000 m above mean sea level

## Fuses

### Battery

- ATS1500A(-IP), ATS3500A(-IP): 2 A, resettable
- ATS4500A(-IP): 3 A, resettable

### 12 V aux

1 A, resettable

### System databus

1 A, resettable

### Siren 1, high current output S1

1 A, resettable

### Siren 2, high current output S2

1 A, resettable

### Siren 3, high current output S3

1 A, resettable

### Mains, mains fuse:

- ATS1500A(-IP): 315 mA, fast 20x5
- ATS3500A(-IP), ATS4500A-IP: 630 mA, fast 20x5

**Note:** Mains fuse is part of the mains terminal block.
WARNING: Before removing the mains fuse, mains power must be disconnected (see “Mains power connection” on page 17).

Auxiliary current and battery capacity

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

<table>
<thead>
<tr>
<th>Battery capacity, Ah</th>
<th>7.2</th>
<th>12</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable housing</td>
<td>SM, MM, LP</td>
<td>LP</td>
<td>MM</td>
</tr>
<tr>
<td>Security approval / Grade</td>
<td>Discharge time, h</td>
<td>Charge time, h</td>
<td>Auxiliary current, mA</td>
</tr>
<tr>
<td>EN Grade 2</td>
<td>12</td>
<td>72</td>
<td>450</td>
</tr>
<tr>
<td>INCERT</td>
<td>24</td>
<td>24</td>
<td>150</td>
</tr>
<tr>
<td>EN Grade 3, VdS-B</td>
<td>30</td>
<td>24</td>
<td>90</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 2 (EN+RTC)</td>
<td>36</td>
<td>72</td>
<td>—</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 3 (EN+RTC), VdS-C</td>
<td>60</td>
<td>24</td>
<td>—</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Battery capacity, Ah</th>
<th>7.2</th>
<th>12</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable housing</td>
<td>MM, LP</td>
<td>LP</td>
<td>MM</td>
</tr>
<tr>
<td>Security approval / Grade</td>
<td>Discharge time, h</td>
<td>Charge time, h</td>
<td>Auxiliary current, mA</td>
</tr>
<tr>
<td>EN Grade 2</td>
<td>12</td>
<td>72</td>
<td>450</td>
</tr>
<tr>
<td>INCERT</td>
<td>24</td>
<td>24</td>
<td>150</td>
</tr>
<tr>
<td>EN Grade 3, VdS-B</td>
<td>30</td>
<td>24</td>
<td>90</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 2 (EN+RTC)</td>
<td>36</td>
<td>72</td>
<td>—</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 3 (EN+RTC), VdS-C</td>
<td>60</td>
<td>24</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 9: ATS4500A-IP maximal available auxiliary current

<table>
<thead>
<tr>
<th>Battery capacity, Ah</th>
<th>7.2</th>
<th>12</th>
<th>18</th>
<th>25</th>
<th>36</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable housing</td>
<td>MM+, LM</td>
<td>LM</td>
<td>MM+, LM</td>
<td>LM</td>
<td>LM</td>
</tr>
<tr>
<td>Security approval / Grade</td>
<td>Discharge time, h</td>
<td>Charge time, h</td>
<td>Auxiliary current, mA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN Grade 2</td>
<td>12</td>
<td>72</td>
<td>450</td>
<td>850</td>
<td>1350</td>
</tr>
<tr>
<td>INCERT</td>
<td>24</td>
<td>24</td>
<td>150</td>
<td>350</td>
<td>600</td>
</tr>
<tr>
<td>EN Grade 3, VdS-B</td>
<td>30</td>
<td>24</td>
<td>90</td>
<td>250</td>
<td>450</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 2 (EN+RTC)</td>
<td>36</td>
<td>72</td>
<td>—</td>
<td>180</td>
<td>350</td>
</tr>
<tr>
<td>NF&amp;A2P Grade 3 (EN+RTC), VdS-C</td>
<td>60</td>
<td>24</td>
<td>—</td>
<td>—</td>
<td>150</td>
</tr>
</tbody>
</table>

Note: 18 Ah battery blocks some entry holes in the MM housing.
Example for ATS1500A(-IP) EN Grade 2
When using battery backup as specified for EN Grade 2 using a 12 Ah battery, the maximum available auxiliary current is 750 mA.

Example for ATS3500A(-IP) EN Grade 3
When using battery backup as specified for EN Grade 3 using an 18 Ah battery, the maximum available auxiliary current is 450 mA.

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

- Devices on the Advisor Advanced system databus
- Detectors on the auxiliary power output
- Communication devices via MI-bus (e.g. GSM, IP)

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

Fuse rating must be taken into account.

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

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

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

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

System monitoring
The system provides monitoring for the following items.

<table>
<thead>
<tr>
<th>Monitoring function</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Mains</td>
<td>Mains fail</td>
<td>Loss of external power supply [1]</td>
</tr>
<tr>
<td>Battery</td>
<td>Battery low</td>
<td>Battery low voltage [1]</td>
</tr>
<tr>
<td></td>
<td>Battery test fail</td>
<td>Exhausted battery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Battery charger fail</td>
</tr>
<tr>
<td></td>
<td>Fuse/power output fail</td>
<td>Output overload</td>
</tr>
<tr>
<td>Power outputs</td>
<td>Fuse/power output fail</td>
<td>Exhausted fuse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fuse loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Short circuit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overload</td>
</tr>
<tr>
<td>Monitoring function</td>
<td>Message</td>
<td>Cause</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Power supply</td>
<td>Power unit/power output fail</td>
<td>Power unit failure</td>
</tr>
<tr>
<td>Tampers</td>
<td>Device tamper</td>
<td>Device sabotage</td>
</tr>
</tbody>
</table>

[1] Mains fail and Battery low will finally result in Battery deep discharge protection.
Chapter 3
System functions

Summary

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

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

Content

Function list 45
Zones 47
  Zone types 47
Areas 52
Set and unset 54
  Delayed unset 55
Inhibit and isolate 56
  Inhibit 56
  Isolate 56
  Zone shunt 56
Keys 58
  Common key sequences for LCD keypad 58
  Common key sequences for keypad without LCD 59
  Function keys 60
Bus devices 62
  Bus device numbering 62
  Adding keypad with a higher number 62
Keypads 63
  Expanders 63
  Audio devices 63
Users 64
  Predefined users 64
  User data lock 65
User groups 66
PIN 71
Outputs 73
Chapter 3: System functions

Access control 74
  Door controller 74
Doors 74
Door groups 75
Basic access control functions 75
Advanced access control functions 75
Door controller macro logic 76
Pulsed lock and unlock 77
Condition filters 80
Triggers 82
Calendar 83
  Schedule shortcut menu 84
Events 86
  Log 86
  Programming 86
Tests and diagnostics 88
  Walk test 88
  Other tests 91
Alarm reporting 92
  Reporting principles 92
  Reporting order 93
  Failed to communicate (FTC) 94
  Two-way audio 95
User programmable functions 97
AutoSet 101
Wireless device programming 102
  Learning wireless sensors 102
  Learning fobs 104
  Two-zone RF sensors 106
  Device activation 107
Using cameras 109
  Configuration 109
  Diagnostics 111
  Troubleshooting 111
Engineer reset 113
Timed unset / ATM 114
Two-way audio 115
UltraSync 117
Mobile Application 120
### Function list

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>“Access control” on page 74</td>
</tr>
<tr>
<td>Areas</td>
<td>“Areas” on page 52</td>
</tr>
<tr>
<td>ATM</td>
<td>“Timed unset / ATM” on page 114</td>
</tr>
<tr>
<td>Autoset</td>
<td>“Autoset” on page 101</td>
</tr>
<tr>
<td>Calendar</td>
<td>“Calendar” on page 83</td>
</tr>
<tr>
<td>Cameras</td>
<td>“Using cameras” on page 109</td>
</tr>
<tr>
<td>Condition filters</td>
<td>“Condition filters” on page 80</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>“Tests and diagnostics” on page 88</td>
</tr>
<tr>
<td>Doors</td>
<td>“Doors” on page 74</td>
</tr>
<tr>
<td>Events</td>
<td>“Events” on page 86</td>
</tr>
<tr>
<td>Expanders / DGPs</td>
<td>“Bus devices” on page 62, “Expanders” on page 63</td>
</tr>
<tr>
<td>Inhibit</td>
<td>“Inhibit and isolate” on page 56</td>
</tr>
<tr>
<td>Inputs</td>
<td>“Zones” on page 47</td>
</tr>
<tr>
<td>Isolate</td>
<td>“Inhibit and isolate” on page 56</td>
</tr>
<tr>
<td>Keypads / RASes</td>
<td>“Bus devices” on page 62, “Keypads” on page 63</td>
</tr>
<tr>
<td>Keys</td>
<td>“Keys” on page 58</td>
</tr>
<tr>
<td>Mobile Application</td>
<td>“Mobile Application” on page 120</td>
</tr>
<tr>
<td>Outputs</td>
<td>“Outputs” on page 73</td>
</tr>
<tr>
<td>Part set</td>
<td>“Set and unset” on page 54</td>
</tr>
<tr>
<td>PIN</td>
<td>“PIN” on page 71</td>
</tr>
<tr>
<td>Reporting</td>
<td>“Alarm reporting” on page 92</td>
</tr>
<tr>
<td>Set</td>
<td>“Set and unset” on page 54</td>
</tr>
<tr>
<td>Shunt</td>
<td>“Zone shunt” on page 56, “Door shunt” on page 75</td>
</tr>
<tr>
<td>Tests</td>
<td>“Tests and diagnostics” on page 88</td>
</tr>
<tr>
<td>Timed unset</td>
<td>“Timed unset / ATM” on page 114</td>
</tr>
<tr>
<td>Triggers</td>
<td>“Triggers” on page 82</td>
</tr>
<tr>
<td>Two-way audio</td>
<td>“Two-way audio” on page 115</td>
</tr>
<tr>
<td>UltraSync</td>
<td>“UltraSync” on page 117</td>
</tr>
<tr>
<td>Unset</td>
<td>“Set and unset” on page 54</td>
</tr>
<tr>
<td>User groups</td>
<td>“User groups” on page 66</td>
</tr>
</tbody>
</table>
## Chapter 3: System functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>User programmable functions</td>
<td>“User programmable functions” on page 97</td>
</tr>
<tr>
<td>Users</td>
<td>“Users” on page 64</td>
</tr>
<tr>
<td>Walk test</td>
<td>“Walk test” on page 88</td>
</tr>
<tr>
<td>Wireless devices</td>
<td>“Wireless device programming” on page 102</td>
</tr>
<tr>
<td>Zones</td>
<td>“Zones” on page 47</td>
</tr>
</tbody>
</table>
Zones

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

Zone connection is described in Chapter 2 “Installation” > “Zone connection” on page 24.

For zone configuration, see “Zone configuration” on page 31.

Zone addressing is described in “Zone, output, and door addressing” on page 32.

Zone programming is done via “4.1 Zone menu” on page 191 (in Chapter 5 “Menu reference”).

Zone types

The following zone types are available.

1. Alarm
Generates no alarm when the area is unset.
Generates an alarm when the area is set.
Example: Internal door, PIR (motion detector).

2. Entry/Exit 1
Generates no alarm when the area is unset.
When the area is set, the exit timer starts and activating the zone generates no alarm. If the zone is activated when the exit time has expired, the entry timer starts. Only when the entry time has expired, an alarm is generated.
Example: Front door.
You need to program the entry/exit time. See “4.2 Areas” on page 206 for more information.

3. Access
Generates no alarm when the area is unset.
Generates an alarm when the area is set, and the no exit timer or entry timer is not running.
Example: PIR at entrance with a door contact on the entry door.
You need to program the entry/exit time. See “4.2 Areas” on page 206 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 276.

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 257).

9. Keyswitch
When the zone switches, the area is set / unset / part set depending on the zone options selected.
Example: Key switch next to Front door.
See options “4.1.n.6.16 Key latch” on page 196, “4.1.n.6.17 Key set” on page 196, “4.1.n.6.18 Key unset” on page 196.

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.

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 48.

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 258). It generates an alarm when opened outside of this period.

17. Eng. reset
This zone activation causes the engineer reset.

18. Entry/Exit 2
An alternative entry/exit zone.
Example: Back entrance.
Entry/exit 2 zone initiates alternative entry/exit timers. See “4.2.n.2 Exit time” on page 206” and “4.2.n.3 Entry time” on page 207.
See also “2. Entry/Exit 1” on page 47 for more details.

19. Shunt
Zone activation causes shunt of all area zones that have shunting allowed. Shunt is allowed by the option “4.1.n.6.36 Shunt” on page 201.
See also “Zone shunt” on page 56.

Table 12: Available zone options

<table>
<thead>
<tr>
<th>Options:</th>
<th>Zone type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.n.6.1 Inhibit</td>
<td>+</td>
</tr>
</tbody>
</table>
## Options:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.n.6.2 Isolate</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.3 Excl. in PS1</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.4 Excl. in PS2</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.5 Double knock</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.6 Swinger shunt</td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.7 Anti mask</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.8 Zone pairing</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.9 Chime</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.10 Soak test</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.11 Engineer walk test</td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.12 User walk test</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.13 Shock sensor</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.14 Extend EE</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.15 Final door</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.16 Key latch</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.17 Key set — full set</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.17 Key set — part set</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.18 Key unset</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.19 Technical full set</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.20 Technical unset</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.21 Technical part set</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.22 Keypad LCD</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.23 Log</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.24 CS report</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.25 Delay timer</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.26 ACK on keypad</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Options:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.27 ACK by user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.28 Sensor type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.29 Virtual zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.30 Held open</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.31 EE set check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.32 Alarm in PS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.33 Alarm in PS2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.34 Report as</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.35 Auto test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.36 Shunt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.37 View isolated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.38 Stop report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.n.6.39 Limit reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:

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

Menu reference

The following menus are applicable for zones.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.n.3 Expander range</td>
<td>169</td>
<td>View zone range of the selected expander</td>
</tr>
<tr>
<td>4.1 Zone menu</td>
<td>191</td>
<td>Add, remove, and configure zones</td>
</tr>
<tr>
<td>4.5.n.2 Pics by zone</td>
<td>214</td>
<td>Choose zones that can trigger the camera when active.</td>
</tr>
<tr>
<td>5.1.n.6.1 Door zones</td>
<td>220</td>
<td>Assign required zones to the selected door</td>
</tr>
<tr>
<td>5.1.n.8.1 Zones</td>
<td>232</td>
<td>Select zones that must be shunted on the door opening.</td>
</tr>
<tr>
<td>8.1.4 Zone timer menu</td>
<td>257</td>
<td>Configure timers used in zone configuration options</td>
</tr>
<tr>
<td>8.6 Zone options</td>
<td>270</td>
<td>Configure system options for zones</td>
</tr>
<tr>
<td>8.7.6 Alarm confirm</td>
<td>273</td>
<td>Configure A and B zone confirmation (ACPO)</td>
</tr>
<tr>
<td>8.7.9 Object scheme</td>
<td>276</td>
<td>Configure zone numbering scheme</td>
</tr>
</tbody>
</table>
Areas

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

Each area can have one of the following statuses:

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

See “Set and unset” on page 54 for details.

Areas are configured in “4.2 Areas” on page 206 in Chapter 5 “Menu reference”.

Area groups

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

Area groups are configured in “4.3 Area groups” on page 211.

Note: Area group availability depends on the control panel variant. See “Specifications” on page 36 in Chapter 2 “Installation”.

Area hierarchy

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

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

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

Area hierarchy is set via menu “4.2.n.6 Hierarchy” on page 210.

Menu reference

The following menus are applicable for areas.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.3 View areas,</td>
<td>161</td>
<td>Specify which area and area group will display information on the keypad without a user authorization.</td>
</tr>
<tr>
<td>2.2.1.n.3.4 View AG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.1.n.3.5 Control areas,</td>
<td>162</td>
<td>Select areas and area groups that can be set and unset by the keypad.</td>
</tr>
<tr>
<td>2.2.1.n.3.6 Control AG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu</td>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2.2.1.n.3.13 Area ind.LED1, 2.2.1.n.3.14 Area ind.LED2</td>
<td>165</td>
<td>Assign areas to programmable LEDs of the keypad.</td>
</tr>
<tr>
<td>2.2.1.n.3.2 Tamper area, 2.2.2.n.4.2 Tamper area,</td>
<td>161</td>
<td>Determine which area receives the selected device tamper and fault events.</td>
</tr>
<tr>
<td>3.1.n.9 Select mode</td>
<td>186</td>
<td>Specify if the user operates on areas or area groups.</td>
</tr>
<tr>
<td>3.2.n.3 User group areas, 3.2.n.4 User group AG</td>
<td>189</td>
<td>Define which areas and area groups the user can control.</td>
</tr>
<tr>
<td>4.1.n.5 Zone areas</td>
<td>193</td>
<td>Assign areas to the zone that have to alarm when the zone is activated and area set or unset status meets the requirement for the zone type.</td>
</tr>
<tr>
<td>4.2 Areas</td>
<td>206</td>
<td>Configure areas.</td>
</tr>
<tr>
<td>4.3 Area groups</td>
<td>211</td>
<td>Assign areas to area groups.</td>
</tr>
<tr>
<td>5.1.n.6.3.1 Door areas, 5.1.n.6.3.2 Door AGs</td>
<td>220</td>
<td>Assign the selected door to areas and area groups for area status indication on readers.</td>
</tr>
</tbody>
</table>
Set and unset

Each area can have one of the following statuses:

- **Set (armed):** The condition of an area where a change in the status of any zone (from normal to active) causes an alarm. An area or premise is only set when it is unoccupied. Some zones (like vaults) can remain armed continually.

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

- **Part set:** The condition of part of an area where a change in the status of certain zones (from normal to active) causes an alarm. An area or premise is part set when it is partially unoccupied like the outside of a home is part set but the inside is still unset.

See also “Areas” on page 52.

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

- By users via a keypad or a reader. See “Users” on page 64 and “Bus devices” on page 62. The available key sequences are listed in “Keys” on page 58.

- By users via SMS command. See Advisor Advanced SMS Control Reference Manual for details.

- By operators remotely via management software. See Chapter 6 “Software” on page 313.

- Automatically via the autoset functionality. See “Autoset” on page 101 for details.

**How to use part set**

When users performs a part set, the system sets all requested areas with all full set (perimeter) zones supervised but all part set (interior) zones ignored. As this setting mode is for personal safety, reporting to the central station depends on option “8.4.3.1 Report BA” (see page 266). Further, any alarms that occur while part set is applied, are treated as local alarms that activate sirens, keypad buzzers (if enabled), and keypad indicators.

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

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

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

Unset delay
Please wait

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

The delay period is set in “4.2.n.4.3 Unset delay” on page 208.

There is no way to manually override the delay.

Menu reference

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.5 Control areas, 2.2.1.n.3.6 Control AG</td>
<td>162</td>
<td>Select areas and area groups that can be set and unset by the keypad.</td>
</tr>
<tr>
<td>2.2.1.n.3.7.1 Card&amp;PIN mode</td>
<td>163</td>
<td>Select an authorization method for the keypad.</td>
</tr>
<tr>
<td>2.2.1.n.3.7.3 1 x set/unset</td>
<td>163</td>
<td>Define if the selected keypad allows you to set or unset areas with one badge.</td>
</tr>
<tr>
<td>2.2.1.n.3.7.4 3 x badge set</td>
<td>163</td>
<td>Define if the selected keypad allows you to set areas with triple badge.</td>
</tr>
<tr>
<td>2.2.1.n.3.11 Quick set</td>
<td>164</td>
<td>Allow setting areas without providing user PIN or card.</td>
</tr>
<tr>
<td>3.1.n.9 Select mode</td>
<td>186</td>
<td>Specify if the user operates on areas or area groups.</td>
</tr>
<tr>
<td>3.2.n.3 User group areas, 3.2.n.4 User group AG</td>
<td>189</td>
<td>Define which areas and area groups the user can control.</td>
</tr>
<tr>
<td>4.2.n.2 Exit time</td>
<td>206</td>
<td>Set area exit timers.</td>
</tr>
<tr>
<td>4.2.n.3 Entry time</td>
<td>207</td>
<td>Set area entry timers.</td>
</tr>
<tr>
<td>4.2.n.4.3 Unset delay</td>
<td>208</td>
<td>Set timer for delayed unset.</td>
</tr>
<tr>
<td>4.2.n.5 Set/unset options</td>
<td>209</td>
<td>Set various system setting and unsetting options.</td>
</tr>
<tr>
<td>5.1.n.6.3 Alarm control</td>
<td>220</td>
<td>Set alarm control options for the selected door.</td>
</tr>
<tr>
<td>8.1.3.5 Final set delay</td>
<td>257</td>
<td>Define the delay time between the completion of an area being set by an exit terminator or final door set and the area being armed.</td>
</tr>
<tr>
<td>8.4 Set options</td>
<td>264</td>
<td>Define the set conditions.</td>
</tr>
<tr>
<td>8.7.7 Easy unset</td>
<td>275</td>
<td>If enabled, you can unset premises entering a PIN or badging a valid card without pressing any other keys.</td>
</tr>
<tr>
<td>8.9 Timed Unset / ATM</td>
<td>279</td>
<td>Configure the ATM (automated teller machine) interface options, for example, unset delay and extended unset delay.</td>
</tr>
</tbody>
</table>
Inhibit and isolate

A faulty device can be inhibited or isolated.

**Inhibit**

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

The zone is inhibited until the next unset.

A zone can be inhibited automatically when using the forced set functionality. It is configured via menu “8.4.4 Forced set” on page 266 in Chapter 5 “Menu reference”.

**Isolate**

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

**Zone shunt**

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

A zone can be shunted in the following ways:

- Manually by the installer. Use menu “1.2.1.9 Shunt zones” on page 140.
- By a schedule. See “Calendar” on page 83 for details.
- By a conditional filter. See “Condition filters” on page 80 for details.
- By a zone with Shunt type. See “Zone types” on page 47 for details.

---

**Caution:** There is a limitation of the number of zones that can be shunted simultaneously. The limit is set in “4.2.n.7.3 Shunt limit” on page 210.

During the shunt time the zone is inhibited.

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

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

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

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1.9 Shunt zones</td>
<td>140</td>
<td>Shunt zones manually.</td>
</tr>
<tr>
<td>2.2.1.n.3.9 Isolate keypad</td>
<td>164</td>
<td>Isolate the tamper fault events on the selected keypad (the keypad remains functional).</td>
</tr>
<tr>
<td>2.2.2.n.4.3 Isolate expander</td>
<td>170</td>
<td>Isolate the tamper fault events on the selected expander (the expander remains functional).</td>
</tr>
<tr>
<td>4.1.n.3 Isolated</td>
<td>193</td>
<td>Isolate or de-isolate the selected zone.</td>
</tr>
<tr>
<td>4.1.n.6.1 Inhibit</td>
<td>193</td>
<td>If set to Yes, this zone can be inhibited by users.</td>
</tr>
<tr>
<td>4.1.n.6.2 Isolate</td>
<td>193</td>
<td>If set to Yes, this zone can be isolated by users.</td>
</tr>
<tr>
<td>4.1.n.6.6 Swinger shunt</td>
<td>194</td>
<td>If set to Yes, the number of alarms from the zone is limited to the specified number for one set/unset cycle.</td>
</tr>
<tr>
<td>4.1.n.6.36 Shunt</td>
<td>201</td>
<td>If set to Yes, the zone can be shunted.</td>
</tr>
<tr>
<td>4.1.n.6.37 View isolated</td>
<td>201</td>
<td>If set to On, users are warned about this zone being isolated when attempting to set or unset the appropriate area.</td>
</tr>
<tr>
<td>4.2.n.7 Limits</td>
<td>210</td>
<td>Limit the number of system elements that can be isolated, inhibited, or shunted at any one time.</td>
</tr>
<tr>
<td>4.5.n.5 Isolated</td>
<td>216</td>
<td>Isolate the selected camera.</td>
</tr>
<tr>
<td>8.6.4 Swinger shunt</td>
<td>271</td>
<td>Define the number of alarms from a zone until it is shunted.</td>
</tr>
</tbody>
</table>
Keys

The authorization method depends on system settings. See “2.2.1.n.3.7 Control options” on page 162 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>
<thead>
<tr>
<th>Action</th>
<th>Programmed method</th>
<th>Key sequence</th>
<th>[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set [2]</td>
<td>Set with key</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set with PIN</td>
<td>On, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN, On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set with card</td>
<td>Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>On, card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 x card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set with card and PIN</td>
<td>On, card, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Card, PIN, On</td>
<td></td>
</tr>
<tr>
<td>Unset [2][3]</td>
<td>Unset with PIN</td>
<td>Off, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN, Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unset with card</td>
<td>Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off, card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unset with card and PIN</td>
<td>Off, card, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Card, PIN, Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Card, PIN</td>
<td></td>
</tr>
<tr>
<td>Part set [2]</td>
<td>Part set with key</td>
<td>Partset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Part set with PIN</td>
<td>Partset, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Part set with card</td>
<td>Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partset, card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 x card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Part set with card and PIN</td>
<td>Partset, card, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Card, PIN, Partset</td>
<td></td>
</tr>
<tr>
<td>Door access [2][3]</td>
<td>Door access with PIN</td>
<td>PIN, Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Door access with card</td>
<td>Card</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Programmed method</td>
<td>Key sequence</td>
<td>[1]</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>--------------</td>
<td>-----</td>
</tr>
<tr>
<td>Door access with card and PIN</td>
<td>Card, PIN, Enter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu access [2]</td>
<td>Menu access with PIN</td>
<td>Menu, PIN, Enter</td>
<td></td>
</tr>
<tr>
<td>Menu access with card</td>
<td>Menu, card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu access with card and PIN</td>
<td>Menu, card, PIN, Enter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duress [4]</td>
<td>Duress with PIN</td>
<td>Any set key (On / Off / Partset), duress code, Enter</td>
<td></td>
</tr>
<tr>
<td>Duress with card and PIN</td>
<td>Any set key (On / Off / Partset), duress code, card, Enter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change keypad buzzer volume</td>
<td>Increase volume</td>
<td>X + Right</td>
<td></td>
</tr>
<tr>
<td>Decrease volume</td>
<td>X + Left</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panic [5]</td>
<td>Panic alarm</td>
<td>1 + 3</td>
<td></td>
</tr>
<tr>
<td>Exit [6]</td>
<td>Quick exit from the programming</td>
<td>Menu + Clear</td>
<td></td>
</tr>
<tr>
<td>Active alarms [7]</td>
<td>Display active zones and faults that should be acknowledged</td>
<td>Function, Function</td>
<td></td>
</tr>
<tr>
<td>Alarm memory [7]</td>
<td>Display alarms that occurred when set</td>
<td>Enter, Enter</td>
<td></td>
</tr>
</tbody>
</table>

[1] Use the check box to note which options are available for this system.
[2] The functionality depends on “2.2.1.n.3.7.1 Card&PIN mode” on page 163.
[3] The functionality depends on “8.7.7 Easy unset” on page 275.
[5] Panic alarm functionality depends on the “8.8.1 Panic mode” option described on page 276. It also depends on the “2.2.1.n.3.20 1+3 keys” option described on page 167.
[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 263.

**Common key sequences for keypad without LCD**

### Table 14: Common key sequences for keypad without LCD

<table>
<thead>
<tr>
<th>Action</th>
<th>Programmed method</th>
<th>Key sequence</th>
<th>[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set [2]</td>
<td>Set with PIN</td>
<td>On, PIN, On</td>
<td></td>
</tr>
<tr>
<td>Set with card</td>
<td>Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set with card and PIN</td>
<td>On, card, PIN, On</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Card, PIN, On</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 3: System functions

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

[1] Use the check box to note which options are available for this system.
[2] The functionality depends on "2.2.1.n.3.7.1 Card&PIN mode" on page 163.
[3] The functionality depends on "8.7.7 Easy unset" on page 275.

When a PIN can be entered, the keypad beeps twice and flashes the red and green LEDs. When an operation fails the keypad beeps seven times.

## Function keys

Use Table 15 below to describe function keys functionality and availability.

See also “2.2.1.n.3.12 Function keys” on page 165.

### Table 15: Function keys

<table>
<thead>
<tr>
<th>Action</th>
<th>Key</th>
<th>[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>❑</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>❑</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>❑</td>
</tr>
<tr>
<td></td>
<td>F1 (F + 1)</td>
<td>❑</td>
</tr>
<tr>
<td></td>
<td>F2 (F + 2)</td>
<td>❑</td>
</tr>
</tbody>
</table>
Action | Key | [1]
---|---|---
| F3 (F + 3) | ☐
| F4 (F + 4) | ☐

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

Menu reference

The following menus are applicable for key configuration.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.7.1 Card&amp;PIN mode</td>
<td>163</td>
<td>Select a control method.</td>
</tr>
<tr>
<td>2.2.1.n.3.7.3 1 x set/unset</td>
<td>163</td>
<td>Define if the selected keypad allows you to set or unset areas with one badge.</td>
</tr>
<tr>
<td>2.2.1.n.3.7.4 3 x badge set</td>
<td>163</td>
<td>Define if the selected keypad allows you to set areas with triple badge.</td>
</tr>
<tr>
<td>2.2.1.n.3.11 Quick set</td>
<td>164</td>
<td>Allow setting areas without providing user PIN or card.</td>
</tr>
<tr>
<td>2.2.1.n.3.12 Function keys</td>
<td>165</td>
<td>Assign a user programmable function to any of available function keys.</td>
</tr>
<tr>
<td>2.2.1.n.3.17 ACK on keypad</td>
<td>166</td>
<td>Select an additional LCD keypad that displays an acknowledgement prompt after the system is unset.</td>
</tr>
<tr>
<td>2.2.1.n.3.20 1+3 keys</td>
<td>167</td>
<td>Enable a panic alarm by combination of 1 and 3 keys.</td>
</tr>
<tr>
<td>3.1.n.9 Select mode</td>
<td>186</td>
<td>Specify if the user operates on areas or area groups.</td>
</tr>
<tr>
<td>5.1.n.3.5.1 Card and PIN</td>
<td>226</td>
<td>Specify what method is required to open the door from the selected reader.</td>
</tr>
<tr>
<td>5.1.n.3.5.2 Two cards</td>
<td>226</td>
<td>Define if two user cards or PINs are required to gain access.</td>
</tr>
<tr>
<td>5.1.n.6.3.6 Control type</td>
<td>229</td>
<td>Specify what type of alarm control is available for the selected door.</td>
</tr>
<tr>
<td>8.1.3.2 Card and PIN</td>
<td>256</td>
<td>Set the maximum delay time between presenting the card and entering the PIN.</td>
</tr>
<tr>
<td>8.7.7 Easy unset</td>
<td>275</td>
<td>If enabled, you can unset premises entering a PIN or badging a valid card without pressing any other keys.</td>
</tr>
</tbody>
</table>
Bus devices

There are the following kinds of bus devices:

- Keypads are used to provide system control, such as setting or unsettting areas. Depending on the type of keypad, additional functions may be available, such as LCD displays, menus to set time and date etc.
- Expanders are used to provide remote inputs and outputs.
- Readers are connected to door controllers and used to control intelligent doors. See “Access control” on page 74 for details.
- Audio devices: 2-way audio devices used for audio verification. See “Two-way audio” on page 115 for details.

Bus device numbering

Devices use DIP switches to set bus address. The Advisor Advanced normally uses the keypad/expander number. For the dependence between device address and its number, refer to the appropriate bus device installation manual. The address of the programmed device can be viewed in “2.2.1.n.2 Keypad address” (keypad), “2.2.2.n.2 Expander address” (expander), “2.2.4.n.2 Audio address”.

See also Chapter 2 “Installation > Zone, output, and door addressing” on page 32.

Adding keypad with a higher number

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

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

1. Add keypad 16. It will bring you to “2.2.1.n.4 Keypad menu” (described on page 167).
2. Enter keypad menu.
3. Change keypad address to 7. Refer to the appropriate keypad manual.
Keypads
A device that is the user control panel for security options for areas or for access points (doors). The keypad can be a console (LCD keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as set/unset, open doors, etc.

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

Keypads are configured in “2.2.1 Keypad devices” on page 160 in Chapter 5 “Menu reference”.

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

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

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

Expander options are set in “2.2.2 Expander devices” on page 168 in Chapter 5 “Menu reference”.

Audio devices
Two-way audio devices allow the central station operator to listen to the live audio from the protected premises in alarm, and speak back.

See “Two-way audio” on page 115 for details.

Menu reference
The following menus are applicable for bus devices.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Device menu</td>
<td>159</td>
<td>View and configure bus devices.</td>
</tr>
<tr>
<td>8.5.2 DGP options</td>
<td>269</td>
<td>Door controller settings.</td>
</tr>
</tbody>
</table>
Users

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

**Note:** If the system is EN 50131 compliant, you can edit only your own settings, and configure only newly added users. See “User data lock” on page 65 for more details.

For each user, the system records the following:

- Number
- Name
- PIN
- Card ID number
- Phone number
- User group (which determines options the user can access)
- Door group (which determines regions the user can access)
- Language
- Various programmed options

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

Maximum user number in the system is defined in “Specifications” on page 36.

**Note:** Connecting door controllers to the Advisor Advanced system increases the maximum user number in the system (see “Specifications > Access control features” on page 38 for details). However, additional users do not have the following records:

- Phone number
- Language

Predefined users

There are two predefined users in the system:

- Installer is used to enter the Advisor Advanced system configuration. He has user group “Installer group” assigned.

- A user with default name Supervisor who can grant access to the installer menu for the service engineer. He has user group “Supervisor group” assigned. The default supervisor PIN is 1122.

**Note:** If the configured PIN length is configured for more than 4 digits, zeroes are added to the default PIN values. For example, if the system is configured for 6-digit PINs, the supervisor PIN is 112200.
There is always one installer in the system. More than one user can have rights that allow granting access to the installer or service engineer.

See also “User groups” on page 66.

User data lock

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

After a new user is added via menu “3.1.0 Add user” on page 182, 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.

Menu reference

The following menus are applicable for users.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.11 Check card</td>
<td>154</td>
<td>Read data from a user card.</td>
</tr>
<tr>
<td>1.6 Service in</td>
<td>158</td>
<td>Disallow the Installer in function before the Installer in-time expires.</td>
</tr>
<tr>
<td>3 User menu</td>
<td>182</td>
<td>Add, edit, or delete users and user groups.</td>
</tr>
<tr>
<td>4.4.n.2 Assigned user</td>
<td>212</td>
<td>Assign an existing user to the selected fob.</td>
</tr>
<tr>
<td>5.1.n.9.4 HSU options</td>
<td>235</td>
<td>Configure high security user options.</td>
</tr>
<tr>
<td>8.2 Engineer options</td>
<td>259</td>
<td>Configure options that apply to maintenance and installation functions.</td>
</tr>
<tr>
<td>8.8.5 Card learn-in</td>
<td>277</td>
<td>Choose a keypad for user card learning.</td>
</tr>
<tr>
<td>9.1.n.4 Destination</td>
<td>288</td>
<td>Configure GSM communication with users.</td>
</tr>
</tbody>
</table>
User groups

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

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

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

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

User group types

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

There are the following types of user groups:

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

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

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

User group type is set in “3.2.n.2 User group type” on page 189.

Table 16 on page 67 denotes default and allowed user group options (user privileges).

Note: Not all of read-only options are visible for particular user group types.
Table 16: User group types and allowed options [1]

<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Normal user</th>
<th>Supervisor</th>
<th>Installer</th>
<th>Guard</th>
<th>Timed Unset / ATM</th>
<th>Reset only</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Full set</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>2</td>
<td>Part set 1</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>3</td>
<td>Part set 2</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>4</td>
<td>Unset</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>5</td>
<td>Inhibit</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>[No]</td>
</tr>
<tr>
<td>6</td>
<td>Isolate</td>
<td>[No]</td>
<td>No [1]</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>7</td>
<td>Time and date</td>
<td>[No]</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>8</td>
<td>User adding (none / restricted / all)</td>
<td>[none]</td>
<td>[all]</td>
<td>[all]</td>
<td>[none]</td>
<td>[none]</td>
<td>[none]</td>
<td>[none]</td>
</tr>
<tr>
<td>9</td>
<td>Forced set</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>[No]</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>10</td>
<td>Change PIN</td>
<td>Yes</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>11</td>
<td>Walk test</td>
<td>No</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>12</td>
<td>Engineer reset</td>
<td>[No]</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>13</td>
<td>Duress code</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>14</td>
<td>Reporting test</td>
<td>[No]</td>
<td>Yes</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>15</td>
<td>Remote connection</td>
<td>No</td>
<td>Yes</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>16</td>
<td>Cleaner</td>
<td>No</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>17</td>
<td>UG area list</td>
<td>No</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>18</td>
<td>Menu access</td>
<td>Yes</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>Inst. access</td>
<td>[No]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>20</td>
<td>Logs access</td>
<td>No</td>
<td>Yes</td>
<td>[Yes]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>21</td>
<td>Stop report</td>
<td>No</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>22</td>
<td>SMS reporting</td>
<td>No</td>
<td>Yes [1]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>23</td>
<td>SMS control</td>
<td>No</td>
<td>Yes [1]</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>24</td>
<td>Card and PIN mode</td>
<td>Card or PIN</td>
<td>Card or PIN</td>
<td>Card or PIN</td>
<td>Card or PIN</td>
<td>Card or PIN</td>
<td>Card or PIN</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>No OP/CL reports</td>
<td>No</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>26</td>
<td>Schedule access (none, view, control/view)</td>
<td>view</td>
<td>control/view</td>
<td>[control/view]</td>
<td>control/view</td>
<td>[none]</td>
<td>[none]</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Fob learning</td>
<td>[No]</td>
<td>Yes</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>28</td>
<td>Remote pics</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>29</td>
<td>Pic deletion</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>30</td>
<td>CS configuration</td>
<td>No</td>
<td>Yes</td>
<td>[Yes]</td>
<td>No</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
<tr>
<td>31</td>
<td>Shunt</td>
<td>No</td>
<td>No</td>
<td>[Yes]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
<td>[No]</td>
</tr>
</tbody>
</table>

[1] Some options are not available for all user group types.

[2] Options for forced set are not applicable to normal users.
# Option | User group type
<table>
<thead>
<tr>
<th>Normal user</th>
<th>Supervisor</th>
<th>Installer</th>
<th>Guard</th>
<th>Timed Unset / ATM</th>
<th>Reset only</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>32. Region ctrl</td>
<td>No</td>
<td>[Yes]</td>
<td>[Yes]</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>33. Door control</td>
<td>No</td>
<td>[Yes]</td>
<td>[Yes]</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

[value]: Option is read only.

[1] The value may depend on defaults selected during the initial start-up. See “Initial start-up” on page 130 for details.


[3] Allowed keypad numbers depend on the panel variant. For details, see “General features” on page 37.

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

**User privilege limitation**

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

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

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

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

See also “User data lock” on page 65.

**User group options**

User group options are set in menu “3.2.n.6 User group options” on page 190.

The following options are available.

**Table 17: User group options as user privileges**

<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Full set</td>
<td>Set the premises.</td>
</tr>
<tr>
<td>2.</td>
<td>Part set 1</td>
<td>Perform a partial set 1.</td>
</tr>
<tr>
<td>4.</td>
<td>Unset</td>
<td>Unset.</td>
</tr>
<tr>
<td>5.</td>
<td>Inhibit</td>
<td>Inhibit zones.</td>
</tr>
<tr>
<td>6.</td>
<td>Isolate</td>
<td>Isolate zones, bus devices, cameras etc.</td>
</tr>
<tr>
<td>7.</td>
<td>Time and date</td>
<td>Change system time and date.</td>
</tr>
<tr>
<td>#</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8</td>
<td>User adding</td>
<td>Create new users (see also &quot;User privilege limitation&quot; on page 68).</td>
</tr>
<tr>
<td>9</td>
<td>Forced set</td>
<td>Perform a forced set. The availability of this option depends on the system configuration.</td>
</tr>
<tr>
<td>10</td>
<td>Change PIN</td>
<td>Change own PIN.</td>
</tr>
<tr>
<td>11</td>
<td>Walk test</td>
<td>Perform a walk test.</td>
</tr>
<tr>
<td>12</td>
<td>Engineer reset</td>
<td>Perform an engineer reset.</td>
</tr>
<tr>
<td>13</td>
<td>Duress code</td>
<td>Use a duress code.</td>
</tr>
<tr>
<td>14</td>
<td>Reporting tests</td>
<td>Make a test call to the particular central station.</td>
</tr>
<tr>
<td>15</td>
<td>Remote connection</td>
<td>Respond to a remote access request.</td>
</tr>
<tr>
<td>16</td>
<td>Cleaner</td>
<td>Leave zones inhibited after the unset.</td>
</tr>
<tr>
<td>17</td>
<td>User group area list</td>
<td>Display the list of areas.</td>
</tr>
<tr>
<td>18</td>
<td>Menu access</td>
<td>Enter the user menu.</td>
</tr>
<tr>
<td>19</td>
<td>Inst. access</td>
<td>Grant the Installer an access to the system configuration.</td>
</tr>
<tr>
<td>20</td>
<td>Logs access</td>
<td>Access the panel logs.</td>
</tr>
<tr>
<td>21</td>
<td>Stop report</td>
<td>Stop reporting in progress.</td>
</tr>
<tr>
<td>22</td>
<td>SMS reporting</td>
<td>Receive SMS reports.</td>
</tr>
<tr>
<td>23</td>
<td>SMS control</td>
<td>Control the system via SMS.</td>
</tr>
<tr>
<td>24</td>
<td>Card and PIN mode</td>
<td>Set the mode for this particular user group (if possible). The following modes are available:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PIN only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Card only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Card or PIN</td>
</tr>
<tr>
<td>25</td>
<td>No OP/CL reports</td>
<td>Open/close events generated by users of the user group are not reported</td>
</tr>
<tr>
<td>26</td>
<td>Schedule access</td>
<td>Access to schedule. The following options are available:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• None: No access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View: Restricted access. Users can view schedule and cancel actions for the present day.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure: Full access.</td>
</tr>
<tr>
<td>27</td>
<td>Fob learning</td>
<td>Program a fob.</td>
</tr>
<tr>
<td>28</td>
<td>Remote pics</td>
<td>Enable remote picture triggering.</td>
</tr>
<tr>
<td>29</td>
<td>Pic deletion</td>
<td>Delete pictures.</td>
</tr>
<tr>
<td>30</td>
<td>CS configuration</td>
<td>Configure CS communication.</td>
</tr>
<tr>
<td>31</td>
<td>Shunt</td>
<td>Shunt zones.</td>
</tr>
<tr>
<td>32</td>
<td>Region ctrl</td>
<td>Move users between regions.</td>
</tr>
<tr>
<td>33</td>
<td>Door control</td>
<td>Control door state: lock, unlock, open, timed open, enable and disable.</td>
</tr>
</tbody>
</table>
## Menu reference

The following menus are applicable for user groups.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 User menu</td>
<td>182</td>
<td>Add, edit, or delete users and user groups.</td>
</tr>
<tr>
<td>9.1.n.4 Destination</td>
<td>288</td>
<td>Configure GSM communication with users.</td>
</tr>
</tbody>
</table>
PIN

PIN (Personal Identification Number) is a 4 to 10 digit number given to, or selected by, a user. It is necessary to enter a PIN on an Advisor keypad as a prerequisite to perform most Advisor Advanced options. In the Advisor Advanced configuration the PIN is associated with a user, which identifies the PIN holder to the system.

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

- PINs are generated by the system. The user can request a new PIN generation.
  A PIN is generated by selecting Yes and pressing Enter in this menu. The generated PIN is shown until Enter is pressed again.

- PINs are entered manually.
  Pressing Enter lets you enter or edit the PIN of the selected user.

The PIN change mode can be set in menu “8.7.5 PIN chg mode” (see page 273). PIN length is programmed using “8.7.4 PIN length” on page 272. The number of available PINs varies from 10000 (for 4-digit PINs) to 1000000000 (for 10-digit PINs).

No PINs are reserved for system use. Any PIN can be generated or entered for use. PINs must be unique. A PIN cannot be assigned to more than one user. The system will not generate or accept entry of PINs already in use.

The selected user PIN can be changed in “3.1.n.2 PIN” on page 183 if the user data is not locked. See “User data lock” on page 65 for more information.

See also “Keys” on page 58.

Menu reference

The following menus are applicable for PIN configuration and use.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.7.1 Card&amp;PIN mode</td>
<td>163</td>
<td>Select a control method.</td>
</tr>
<tr>
<td>2.2.1.n.3.8 EE PIN lock</td>
<td>164</td>
<td>If set to Yes, it is not possible to use a PIN during the entry time.</td>
</tr>
<tr>
<td>2.2.1.n.3.11 Quick set</td>
<td>164</td>
<td>Allow setting areas without providing user PIN or card.</td>
</tr>
<tr>
<td>3.1.n.2 PIN</td>
<td>183</td>
<td>Change user PIN.</td>
</tr>
<tr>
<td>5.1.n.6.3.3.1 Low Security</td>
<td>221</td>
<td>Define when the user authorization is changed from Card and PIN to Card or PIN.</td>
</tr>
<tr>
<td>5.1.n.6.3.4.3 EE PIN lock</td>
<td>222</td>
<td>If set to Yes, it is not possible to use a PIN during the entry time.</td>
</tr>
</tbody>
</table>
## Menu

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.n.3.5.1 Card and PIN</td>
<td>226</td>
<td>Specify what method is required to open the door from the selected reader.</td>
</tr>
<tr>
<td>5.1.n.6.3.7 If PIN sets</td>
<td>229</td>
<td>Configure the door operation if the area is set using PIN.</td>
</tr>
<tr>
<td>5.1.n.7.2 Low Security</td>
<td>232</td>
<td>Define when the user authorization is changed from Card and PIN to Card or PIN.</td>
</tr>
<tr>
<td>8.1.3.2 Card and PIN</td>
<td>256</td>
<td>Set the maximum delay time between presenting the card and entering the PIN.</td>
</tr>
<tr>
<td>8.1.3.6 Installer in-time</td>
<td>257</td>
<td>Configure the time in which an engineer is allowed to access when granted by a user.</td>
</tr>
<tr>
<td>8.2.1 User code required</td>
<td>259</td>
<td>Define if a user is required to grant the installer an access to the programming menu.</td>
</tr>
<tr>
<td>8.2.5 Service in</td>
<td>262</td>
<td>Disallow the Installer in function before the Installer in time expires.</td>
</tr>
<tr>
<td>8.2.6 Challenge code</td>
<td>262</td>
<td>Activate challenge code functionality.</td>
</tr>
<tr>
<td>8.5.1.1 Card to PIN</td>
<td>268</td>
<td>The amount of time allowed between presenting a valid card to a door reader and entering a valid PIN.</td>
</tr>
<tr>
<td>8.7.4 PIN length</td>
<td>272</td>
<td>Change the PIN length.</td>
</tr>
<tr>
<td>8.7.5 PIN chg mode</td>
<td>273</td>
<td>Choose the appropriate PIN change mode.</td>
</tr>
<tr>
<td>8.7.7 Easy unset</td>
<td>275</td>
<td>If enabled, you can unset premises entering a PIN or badging a valid card without pressing any other keys.</td>
</tr>
</tbody>
</table>
Outputs

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

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

Advisor Advanced outputs are assigned to physical outputs and configured in the menu “6 Outputs and filters” described on page 238 in Chapter 5 “Menu reference”.

These outputs can be controlled by zones, user actions, triggers, schedule, or system events using condition filters. See “Condition filters” on page 80 for more details.

Menu reference

The following menus are applicable for outputs.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.1 Output test</td>
<td>141</td>
<td>Check outputs and LEDs.</td>
</tr>
<tr>
<td>1.2.5.4 Test No Bells</td>
<td>145</td>
<td>Verify of the whole alarm system functionality.</td>
</tr>
<tr>
<td>2.2.2.n.4.6 Output modules</td>
<td>175</td>
<td>Number of output controllers fitted to the door controller.</td>
</tr>
<tr>
<td>6 Outputs and filters</td>
<td>238</td>
<td>Configure outputs.</td>
</tr>
<tr>
<td>8.1.2 Siren options</td>
<td>255</td>
<td>Set timers applicable to internal and external sirens.</td>
</tr>
<tr>
<td>8.5.2.1 Map relays</td>
<td>269</td>
<td>Define whether door controller unlock outputs can be controlled as standard outputs.</td>
</tr>
</tbody>
</table>
Access control

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

- Basic access control function is controlling alarm function by shunting door contact when an authorized user badges a valid card or enters a valid PIN, or presses request to exit button. Such access control functions are provided using standard doors.
  
  See “Door shunt” on page 75 for more information on door shunts.
  
  See also “Doors” below, “Zone shunt” on page 56.

- Advanced access control functions include anti-passback, high security regions etc. These functions are only available while using intelligent doors, which are controlled by door controllers (see “Door controller” below).
  
  See also “Advanced access control functions” on page 75.

Door controller

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

One door controller can control up to four intelligent doors.

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

See “Expanders” on page 63 for more information on expander installation.

Doors

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

- Standard door: A door with a reader or a keypad assigned to each side of the door, and a request to exit button for an exit. Unauthorised door opening causes an intrusion alarm. See “Basic access control functions” on page 75.

- Intelligent door: A door, which can be used for advanced access control. Such door has up to two readers and a region assigned to each side, entry and exit. Such doors are controlled by door controllers. See “Advanced access control functions” on page 75.

Use menu “5 Door menu” on page 217 to configure doors.

For reader, door zone and lock outputs default addressing, see “Zone, output, and door addressing” on page 32 in Chapter 2 “Installation”.

**Note:** It is not required to configure triggers to control door locks. The output set in menu “5.1.n.4 Door output” on page 219 overwrites output configuration.

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

Door groups are programmed in “5.2 Door groups” on page 235.

You can assign door groups to users in “3.1.n.8.1 Door group” on page 187.

**Basic access control functions**

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

A door can be shunted by a keypad or a reader, or a door controller. See “5 Door menu” on page 217 for details on door shunting.

**Advanced access control functions**

**Regions**
A region is a defined access control area having doors acting as boundaries. Regions are used by the anti-passback functions to monitor in which regions users are present. Transfers from one region to another may be prohibited by the anti-passback settings.

Note that region 1 is “outside” region.

Use menu “5.3 Regions” on page 237 to edit regions.

The menu “5.1.n.9.1 Regions” on page 234 allows you to assign specific door readers to regions.

**Anti-passback**
Anti-passback function enables users to transfer from one region to another. Entering a region twice in succession is either not possible, or will result in an event being logged and reported to the operator.

The following anti-passback types are available:

- Soft anti-passback: A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
- Hard anti-passback. A valid card or PIN does not open the door when used to enter the region a second time without leaving first. An attempt to do so generates a report.
Chapter 3: System functions

- Regions anti-passback. A valid card or PIN does not open the door when used to leave a region other than the one entered previously. For example, if the user had entered region 3 from region 2, he will be denied when trying to enter region 2 from region 1. An attempt to do so generates a report.

Use menu “5.1.n.9.2 Anti-passback” on page 234 program the anti-passback for the selected door.

High security

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

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

Set HSU options in “5.1.n.9.4 HSU options” on page 235.

Door controller macro logic

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

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

These pages explain the door control macro logic principles.

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

Macros

A macro is an evaluation and a decision-making device. It has up to four inputs and one output. There are 32 macros available for each door controller.

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

Notes

- All inputs may be optionally individually inverted using the NOT function.
- Any unused inputs should be set to OR.
The macros timers
The output has many timed and a latched option. Each of the timed options may be programmed in minutes or seconds within the range of 1 to 255.

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

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

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

The two relay needed are taken from the relay specified in menu “5.1 Doors” on page 217. The “5.1.n.4 Door output” on page 219 specifies one relay, and door controller takes the next sequential relay number for the second relay it needs to operate the lock. For example; if output 17 is entered as an Unlock output
number and this option is set to Yes, then outputs 17 and 18 are used for the lock.

Two zones are also needed for this operation to work. One for the normal door open contact (for example, reed switch) and one for the monitoring of the door lock status that comes from the electronic lock. The two zones needed are taken from options “5.1.n.6.1.1 Door zone” on page 220 and “5.1.n.6.1.2 Second zone” on page 228.

The function is programmed in “5.1.n.6.2.3 Pulsed L&UnL” on page 229.

The specific operation is as follows.

**Door Open procedure**

On presenting a valid user at this reader, the second relay will pulse on for 0.5 s. After 0.2 s of the second relay switching on, the first relay will pulse on for 0.5 s. If according to the zone monitoring (explained below) the door has not opened, it will continue this procedure for the “5.1.n.5.1 Unlock time” described on page 219. If a “Door Unlock” command is sent, this procedure is permanently continued. The procedure continues every 1.5 seconds. See timing diagram in Figure 23 below.

The difference between Door Open and Door Unlock is: The Door Open command only unlocks the door for the Unlock Time, whereas the Door Unlock command opens the door permanently until a Door Lock command is sent. See also “1.2.13 Door control” on page 155.

**Door Lock procedure**

The second relay will pulse on for 0.5 s. If according to the zone monitoring (explained below) the door has not closed, this procedure will continue until it does. See timing diagram in Figure 24 on page 79.
Zone monitoring

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

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

Menu reference

The following menus are applicable for access control.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.13 Door control</td>
<td>155</td>
<td>Send a direct command to a specific door.</td>
</tr>
<tr>
<td>2.2.2 Expander devices</td>
<td>168</td>
<td>Configure door controllers.</td>
</tr>
<tr>
<td>2.2.3 DC/LC Exp Rdrs</td>
<td>178</td>
<td>Configure keypads and readers, connected to a door controller local bus.</td>
</tr>
<tr>
<td>3.1.n.8 Access options</td>
<td>187</td>
<td>Configure access control options for the selected user.</td>
</tr>
<tr>
<td>5 Door menu</td>
<td>217</td>
<td>Add, edit, or delete doors, door groups, and regions.</td>
</tr>
<tr>
<td>8.5 Access options</td>
<td>268</td>
<td>Various access control options.</td>
</tr>
</tbody>
</table>
Condition filters

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

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

**Figure 25: How a condition filter works**

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

**Example of a condition filter use**

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

1. Select an appropriate condition filter using menu “6.1.n Select filter” on page 238.
2. Change the name of the filter to “Door open” in menu “6.1.n.1 Filter name” on page 238.
3. In menu “6.1.n.2 Formula” program the condition filter as below:

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

4. In menu “6.2 Outputs” on page 240 set the following values:
- Select filter “Door open” for output 10. Output 10 can then be used to unlock a door.
- Select Pulsed mode.
- Set Delay time to 00:00’00.
- Set Active time to 00:00’05 s.

Menu reference
The following menus are applicable for condition filters.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.n.3 Pics by filter</td>
<td>215</td>
<td>Configure condition filters that trigger the camera.</td>
</tr>
<tr>
<td>6.1 Condition filters</td>
<td>238</td>
<td>Add, edit, and delete condition filters.</td>
</tr>
<tr>
<td>6.2.n.4 Start filter</td>
<td>241</td>
<td>Specify a condition filter that activates the output.</td>
</tr>
<tr>
<td>6.2.n.5 Stop filter</td>
<td>241</td>
<td>Specify an optional condition filter that deactivates the output.</td>
</tr>
<tr>
<td>7.2.n.7 Filter</td>
<td>252</td>
<td>Assign an optional conditional filter, which enables the schedule.</td>
</tr>
</tbody>
</table>
Triggers

There can be up to 255 triggers in the system. They can be used in condition filters to control outputs remotely. See “Condition filters” on page 80 for more information.

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

- Advisor Advanced schedule. See “Calendar” on page 83.
- SMS commands. See Advisor Advanced SMS Control Reference Manual for more information.
- Keyfobs. The keyfobs can be assigned to triggers in the wireless expander settings. See “Wireless device programming” on page 102 for details.
- Advisor Advanced compatible PC software. Refer to Chapter 6 “Software” on page 313.

See “Events” on page 86 for more information about trigger events.

Menu reference

The following menus are applicable for triggers.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.2 Trigger state</td>
<td>142</td>
<td>Manually change trigger flag states.</td>
</tr>
<tr>
<td>6.3 Triggers</td>
<td>244</td>
<td>Add, edit, and delete triggers.</td>
</tr>
</tbody>
</table>
Calendar

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

The calendar is configured via menu “7 Calendar” on page 246 in Chapter 5 “Menu reference”.

The Calendar functionality is based on schedules.

Schedules

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

Maximum numbers of schedules, actions, time frames and special days in the system are listed in “Specifications > General features” on page 37.

Schedules are defined by the following parameters.

• Date: Start date and end date determine a time period, when the schedule is valid, or two days when the actions will be activated, depending on time frame configuration.

• Time: It is possible to define up to 4 time frames for each schedule.

  Caution: Time frames should not overlap.

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

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

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

• Action list: A list of actions that must be performed by the system when the schedule is active. See “Actions” below.

• Special day time: Alternative time frames, which become valid if the current day is a special day. See “Special days in schedules” on page 84.

• Filter: A conditional filter that enables the schedule when becomes true. See also “Condition filters” on page 80.

Actions

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

Every action has the following settings:

• Name
• User function: See “User programmable functions” on page 97.

**Counteractions**

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

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

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

**Special days in schedules**

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

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

Special days are assigned to dates in the menu “7.1 View” on page 246.

**Daylight saving note**

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

For more information on daylight saving programming, see “8.1.1 Time and date” on page 254.

**Schedule shortcut menu**

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

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

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

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

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

To edit schedules, use menu “7.2 Schedules” on page 247.

**Note:** Available elements and parameters are described in “User programmable functions” on page 97.
Menu reference

The following menus are applicable for calendar and schedules.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.21 Schedule</td>
<td>167</td>
<td>Assign schedules to the selected keypad.</td>
</tr>
<tr>
<td>3.2.n.7 Schedule</td>
<td>190</td>
<td>Assign schedules to the selected user group.</td>
</tr>
<tr>
<td>4.2.n.8 Schedule</td>
<td>210</td>
<td>Assign schedules to the selected area.</td>
</tr>
<tr>
<td>5.1.n.7 Schedule opts</td>
<td>222</td>
<td>Configure schedule options for the selected door.</td>
</tr>
<tr>
<td>5.1.n.3.5.3 NoSchedule req</td>
<td>226</td>
<td>Extend the exit access for the selected OUT reader.</td>
</tr>
<tr>
<td>6.3.n.2 Schedule</td>
<td>245</td>
<td>Assign schedules to the selected trigger.</td>
</tr>
<tr>
<td>7 Calendar</td>
<td>246</td>
<td>Configure an automatic execution of specific actions at particular time and date.</td>
</tr>
<tr>
<td>8.2.7 Inspection</td>
<td>262</td>
<td>Set up a periodic inspection reminder.</td>
</tr>
</tbody>
</table>
Events

Log
All events are recorded in the Advisor Advanced log. The log size is specified in “Specifications” on page 36, Chapter 2 “Installation”.

The log can be viewed using “1.1 Display logs” on page 136.
Note: The mandatory event log limits the number of repeating events to 3 within one set/unset cycle. The excessive events are stored in the extended event log instead.
See also “Alarm reporting” on page 92.

Programming
Advisor Advanced events can be also used for user function programming. See “Condition filters” on page 80 for details. Events and groups of events, available for condition filter programming, are listed in Appendix A “Advisor Advanced events” on page 337.

Menu reference
The following menus are applicable for events.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Display logs</td>
<td>136</td>
<td>Review alarm details</td>
</tr>
<tr>
<td>1.2.5.2.3 Log untested</td>
<td>143</td>
<td>If set to Yes, zones untested during walk test are recorded in the system log.</td>
</tr>
<tr>
<td>4.1.n.6.23 Log</td>
<td>197</td>
<td>Determine whether the zone event is recorded in the system log.</td>
</tr>
<tr>
<td>4.5.n.4 Pics by rep ev</td>
<td>215</td>
<td>Allow the camera to be triggered by a selected reporting event.</td>
</tr>
<tr>
<td>5.1.n.6.5 Reporting</td>
<td>230</td>
<td>Determine when access control events are reported.</td>
</tr>
<tr>
<td>6.1 Condition filters</td>
<td>238</td>
<td>Configure condition filters activated by events.</td>
</tr>
<tr>
<td>6.2.n.8 Log limit</td>
<td>244</td>
<td>Limit recording of activating and restoring events from the selected output to three per one set cycle.</td>
</tr>
<tr>
<td>8.6.5 Report restore</td>
<td>271</td>
<td>Determine if the restore event is reported to the central station when a user acknowledges an alarm.</td>
</tr>
<tr>
<td>8.7.6.8 Call CS message</td>
<td>275</td>
<td>Display a message with advice for the user to call the central station when a report has been sent.</td>
</tr>
<tr>
<td>8.7.6.9 Reporting delayed</td>
<td>275</td>
<td>Enable a 30-second delay before alarm reporting required by ACPO regulations.</td>
</tr>
</tbody>
</table>
### Chapter 3: System functions

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.10 Anonymize Log</td>
<td>278</td>
<td>Set a time period, after which the user details are removed from a log entry.</td>
</tr>
<tr>
<td>9.1 Central station</td>
<td>280</td>
<td>Configure central stations and reporting options.</td>
</tr>
<tr>
<td>9.2 Event options</td>
<td>290</td>
<td>Assign events to central stations and program the reporting delay.</td>
</tr>
</tbody>
</table>
Tests and diagnostics

The Advisor Advanced system provides a range of test features. Most of them are accessible from “1.2 Test menu” on page 137.

Input and detector tests

To test single inputs or detectors, use “1.2.1 Input tests” on page 137. A single input state can be checked in “1.2.1.7 Zone kOhm” on page 139.

To verify wireless input status, use “1.2.1.3 RF RSSI test” on page 138 and “1.2.1.4 RF diagnostics” on page 138.

Wireless PIR camera range can also be verified in “1.2.1.5 Cam range test” on page 139.

If the detector has an internal test functionality, use “1.2.1.8 Detector test” on page 140 to configure an autotest, or to run it manually.

Test shock sensors via “1.2.2 ShockSens test” on page 141.

Outputs

Test outputs or verify their state using the “1.2.3 Outs&triggers” menu on page 141.

Walk test

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

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

The menu “1.2.5 Walk test” on page 143 allows you to run the test manually (engineer walk test), as well as define conditions when the user has to perform the walk test, including a required walk test before setting an area (user walk test).

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

Engineer walk test

The walk test initiated and executed by the service engineer.

The walk test applies to all zones that have option “4.1.n.6.11 Engineer walk test” on page 195 enabled.
Configure test parameters using “1.2.5.1 Start” menu on page 143.

After this, run the walk test by “1.2.5 Walk test” on page 143.

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 124 for more details.

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

**Walk test 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 145.

Choose a walk test scope and press Enter.

The Walk test start command starts the engineer walk test for zones that have the engineer walk test option enabled (see “4.1.n.6.11 Engineer walk test” on page 195).

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 256). The test fails if this timer expires. If engineer reset fails and inhibit reporting has not been enabled when accessing the programming mode then a message is sent to the central station to indicate that the test failed (see “Accessing the installer programming menu” on page 124).

**Single zone walk test**

You can also use “1.2.5.3 Single zone WT” on page 145 to perform a single zone walk test on the same rules as the engineer walk test described above.

**Walk test mode**

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

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

**Active walk test**

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

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

First, activate zone A, and then zone B.

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

**Notes**

- Options “4.1.n.6.11 Engineer walk test” on page 195 for these zones must be enabled.
- The user privileges in this area must have Walk test allowed. See “3.2 User groups” on page 189 for more details.

**User walk test**

If the user walk test is configured and enabled, the user is requested to perform the user walk test prior to setting an area. The frequency of this request is defined in “1.2.5.2.7 Frequency” on page 144. If the option “1.2.5.2.8 Need to set” on page 144 is enabled, setting an area without prior user walk test is not allowed.
Note: For walk test purposes Advisor Advanced stores information on any zone activation for 4 hours. Therefore if the zone was activated during the last 4 hours before walk test, it is not included into the list of zones required to test. If each walk test zone was activated during this time, the walk test is not requested.

Other tests

Communication
To configure automatic communication test or run it manually, use “1.2.6 Test call opts” on page 146.

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

- IP: “1.2.7 IP diagnostic” on page 147
- GSM: “1.2.8 GSM diagnostic” on page 149

Battery
Use “1.2.9 Battery test” on page 151 to diagnose the panel battery status. The menu also allows you to configure automatic battery tests.

Audio session test
Use the menu “1.2.14 Listen-in” on page 155 to run a two-way audio test session with another phone number.

See also Chapter 3 “System functions > Two-way audio” on page 115.

Menu reference
The following menus are applicable for testing.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 Test menu</td>
<td>137</td>
<td>Access to all testing functions.</td>
</tr>
<tr>
<td>4.1.n.6.10 Soak test</td>
<td>195</td>
<td>Enable the soak test mode for the selected zone.</td>
</tr>
<tr>
<td>4.1.n.6.11 Engineer walk test,</td>
<td>195</td>
<td>Enable engineer and user walk tests for the selected zone.</td>
</tr>
<tr>
<td>4.1.n.6.12 User walk test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.5.n.8 Test pic to CS</td>
<td>216</td>
<td>Take picture and send it to a selected central station.</td>
</tr>
<tr>
<td>8.1.4.3 Soak test</td>
<td>258</td>
<td>Specify the number of days the soak test for a zone is active.</td>
</tr>
<tr>
<td>8.8.6 Test inputs</td>
<td>278</td>
<td>Define what inputs should be accessible when performing input tests.</td>
</tr>
<tr>
<td>9.3.n.11 Module info</td>
<td>305</td>
<td>Display GSM dialler firmware version, modem type, etc.</td>
</tr>
</tbody>
</table>


Alarm reporting

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

The Advisor Advanced reporting features are configured via menu “9 Communication” on page 280 in Chapter 5 “Menu reference”.

Available reporting codes for different protocols are listed in Appendix B “Advisor Advanced reporting codes” on page 353.

Reporting principles

See Appendix B “Advisor Advanced reporting codes” on page 353 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 290.

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 290, 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 284 is set to combined, only the initial area disarming (opening) and the final area arming (closing) in the group of areas with the same account code is reported to the central station. Other area set and unset events are not reported.

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

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

**Reporting order**

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

**Connect to primary central stations**

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

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

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

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

If there are configured the same delays and connection attempt numbers, Advisor Advanced attempts to report to central stations in the following order: 1, 1, 3, 3, 6, 6, 1, 3, 6, 1, 3, 6, etc.
Use the backup central stations

In case the primary central station reporting fails, the system tries to send the event to the appropriate backup central station. For example, if there are primary central stations CS 1 and CS 4, and there are central stations CS 2 and CS 3, which are backup stations for CS 1. Advisor Advanced tries to report to central stations in the following order:

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

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

Report all necessary events to the central station

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

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

**Event priority**

In the queue of events waiting for the central station reporting, events with higher priority are transmitted first. See Table 33 on page 353 for event priority values.

Failed to communicate (FTC)

Each central station has the “9.1.n.7 Retry count” described on page 283. 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 284.

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 146.

**Note:** If “1.2.6.n.5 Freq TC if FTC” on page 147 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.

Two-way audio

Two-way audio allows the central station operator to listen to the live audio from the protected premises in alarm, and speak back.

Notes

- Only specific firmware versions are compatible with the two-way audio.
- The two-way audio verification is available only for (X)SIA reporting protocol and PSTN and GSM reporting paths.

Note: Sending analogue messages over the GSM channel correctly depends on the quality of the GSM network, which changes often.

Audio session with the central station starts when one of the objects with listen-in function configured (zone, keyfob or keypad) generates an alarm. When the audio session is established, the audio device assigned to the object in alarm is turned on in the listening mode.

During the audio session the central station operator can send specific commands using DTMF codes if the panel configuration allows him to do so.

For more information, see “Two-way audio” on page 115.

Menu reference

The following menus are applicable for alarm reporting.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.6 Test call opts</td>
<td>146</td>
<td>Define the automatic test call interval, and perform a test call on demand.</td>
</tr>
<tr>
<td>1.2.7 IP diagnostic</td>
<td>147</td>
<td>Diagnostic tools for IP connectivity.</td>
</tr>
<tr>
<td>3.1.n.7 SMS and Voice</td>
<td>186</td>
<td>Configuration menus for SMS and voice reporting.</td>
</tr>
<tr>
<td>4.1.n.6.24 CS report</td>
<td>197</td>
<td>Determine whether the zone event is reported to the central station.</td>
</tr>
<tr>
<td>4.1.n.6.38 Stop report</td>
<td>201</td>
<td>Allow keyswitch zone activation to stop voice reporting.</td>
</tr>
<tr>
<td>4.5.n.3.m.3 Report as</td>
<td>215</td>
<td>Assign a SIA reporting event to the selected camera conditional filter.</td>
</tr>
<tr>
<td>8.1.3.4 Mains reporting delay</td>
<td>256</td>
<td>Define the delay time before a mains fail is reported to the central station.</td>
</tr>
<tr>
<td>8.4.3.1 Report BA</td>
<td>266</td>
<td>If set to Yes, in the part set the system reports burglar alarms triggered during part set to the central station.</td>
</tr>
<tr>
<td>8.6.5 Report restore</td>
<td>271</td>
<td>Report the restore event to the central station when a user acknowledges an alarm.</td>
</tr>
<tr>
<td>Menu</td>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8.7.6.8 Call CS message</td>
<td>275</td>
<td>Allow the keypad to display a message with advice for the user to call the central station when an alarm report is sent.</td>
</tr>
<tr>
<td>8.7.6.9 Reporting delayed</td>
<td>275</td>
<td>Enable a 30-second delay before alarm reporting required by ACPO regulations.</td>
</tr>
<tr>
<td>9 Communication</td>
<td>280</td>
<td>Program all system-wide communication options.</td>
</tr>
</tbody>
</table>
User programmable functions

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

Programming menu

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

The list of allowed functions may vary for different menus.

To program a user function:

1. Type >None<

First, choose an appropriate function type.

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

Next, configure function parameters.

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

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

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

<table>
<thead>
<tr>
<th>Table 18: Available function types and parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>
| Set | Set areas [1][2] | 1. Areas selection  
2. Area groups selection  
3. User code requirement |
| Unset | Unset areas [1] | 1. Areas selection  
2. Area groups selection |
| Trigger | Change a trigger state | 1. Trigger name  
2. State change: Clear, Set, or Toggle |
| Part set 1 | Part set 1 for areas [1][2] | 1. Areas selection  
2. User code requirement |
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Available parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part set 2</td>
<td>Part set 2 for areas [1][2]</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. User code requirement</td>
</tr>
<tr>
<td>Inhibit</td>
<td>Inhibit zones [1][3]</td>
<td>None</td>
</tr>
<tr>
<td>Test call</td>
<td>Execute a test call [3][4]</td>
<td>None</td>
</tr>
<tr>
<td>PC connection</td>
<td>Establish connection with the PC [1][3]</td>
<td>None</td>
</tr>
<tr>
<td>Service in</td>
<td>Allow service in [5]</td>
<td>None</td>
</tr>
<tr>
<td>Panic</td>
<td>Activate panic alarm</td>
<td>None</td>
</tr>
<tr>
<td>Chime area</td>
<td>Change a chime functionality status in the area</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Status change: Clear, Set, or Toggle</td>
</tr>
<tr>
<td>Chime keypad</td>
<td>Change a chime functionality status on the keypad</td>
<td>1. Keypad selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Status change: Clear, Set, or Toggle</td>
</tr>
<tr>
<td>Set without exit</td>
<td>Immediate set (without exit time) [1]</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Area groups selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. User code requirement</td>
</tr>
<tr>
<td>Fire reset</td>
<td>Reset fire detectors [1]</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td>Show open zones</td>
<td>Show open zones [1]</td>
<td>1. User code requirement</td>
</tr>
<tr>
<td>Active alarms</td>
<td>Show zones in alarm state [1]</td>
<td>1. User code requirement</td>
</tr>
<tr>
<td>Active faults</td>
<td>Show faulty zones [1]</td>
<td>1. User code requirement</td>
</tr>
<tr>
<td>Alarm memory</td>
<td>Show acknowledged alarms [1]</td>
<td>1. User code requirement</td>
</tr>
<tr>
<td>Alarms to ACK</td>
<td>Show unacknowledged alarms [1]</td>
<td>None</td>
</tr>
<tr>
<td>UG control</td>
<td>Change user group privileges</td>
<td>1. UG identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 and further - user group privilege.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Choose a privilege, and then change it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “3.2.n.6 User group options” on page 190 for more details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that the user group type must allow this change. See “3.2.n.2 User group type” on page 189 for details.</td>
</tr>
<tr>
<td>Keypad control</td>
<td>Change keypad options</td>
<td>1. Keypad identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. State change: lock or unlock</td>
</tr>
<tr>
<td>Walk test</td>
<td>Run walk test [1]</td>
<td>1. Area selection</td>
</tr>
<tr>
<td>Output test</td>
<td>Test outputs [1][4]</td>
<td>1. Output selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 outputs can be assigned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These outputs are switched on simultaneously for the longest time period configured in “8.1.2.1 Activation” on page 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. User code requirement</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td>Available parameters</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Test pic to CS</td>
<td>Take a picture and send it to a central station</td>
<td>1. Camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Central station</td>
</tr>
<tr>
<td>Fire</td>
<td>Raise a fire alarm</td>
<td>None</td>
</tr>
<tr>
<td>Medical alarm</td>
<td>Raise a medical alarm</td>
<td>None</td>
</tr>
<tr>
<td>Show inhibited</td>
<td>Show inhibited zones</td>
<td>None</td>
</tr>
<tr>
<td>GSM credit</td>
<td>Check GSM credit</td>
<td>None</td>
</tr>
<tr>
<td>UG area access</td>
<td>Change user access to areas</td>
<td>1. UG identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Area groups selection</td>
</tr>
<tr>
<td>Prohibit unset</td>
<td>Disable area unset</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. State change: On or Off</td>
</tr>
<tr>
<td>Shunt</td>
<td>Allow shunt in areas</td>
<td>1. Areas selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. State change: Shunt, Unshunt, Toggle</td>
</tr>
<tr>
<td>Show shunted</td>
<td>Show shunted zones</td>
<td>None</td>
</tr>
<tr>
<td>Show isolated</td>
<td>Show isolated zones, keypads, and expanders</td>
<td>None</td>
</tr>
<tr>
<td>Unlocked</td>
<td>Unlock doors</td>
<td>1. Door selection</td>
</tr>
<tr>
<td>RTE</td>
<td>Enable Request To Exit input for specific doors</td>
<td>1. Door selection</td>
</tr>
<tr>
<td>Low security</td>
<td>Enable Low security mode for specific doors</td>
<td>1. Door selection</td>
</tr>
<tr>
<td>Access enabled</td>
<td>Enable access to doors in a door group [6]</td>
<td>1. Door group selection</td>
</tr>
</tbody>
</table>

[1] Depending on system settings, the function may require logging in of a user with the appropriate privileges. See “2.2.1.n.3.11 Quick set” on page 164 for more details.

[2] Set and part set function start time is the time when the warning timer is started. The warning time must be taken into account. See “4.2.n.4.1 Warning time” on page 208 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.


[6] Caution: This function should be only performed in a time frame with specified end time. See also Chapter 3 “System functions > Counteractions” on page 84.

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

- Schedule. See “Calendar” on page 83 for more details.
- Function key. See “Function keys” on page 60.
- Fob. See “Wireless device programming” on page 102 for more details.
Menu reference

The following menus are applicable for user programmable functions.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1.n.3.12 Function keys</td>
<td>165</td>
<td>Assign a user programmable function to any of available function keys.</td>
</tr>
<tr>
<td>4.4.n.3 Buttons</td>
<td>212</td>
<td>Assign an appropriate function to a button or a button combination.</td>
</tr>
<tr>
<td>7.2.n.5 Action list</td>
<td>247</td>
<td>Select actions that must be performed by the system according to the selected schedule.</td>
</tr>
</tbody>
</table>
Autoset

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

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

- Using menu “7 Calendar” on page 246, create an action with Set function. See also “User programmable functions” on page 97.
- Configure an appropriate schedule using the menu “7.2 Schedules” on page 247.
- Enable or disable “4.2.n.5.3 Silent autoset” option on page 209.
- If necessary, set “4.2.n.5.2 Set retry” option on page 209.
  If Set retry is allowed, configure “8.4.8 AS user retry” on page 267.
- Set “4.2.n.4.1 Warning time” option on page 208 as well.
- Optionally, configure “8.4.7 AS fault retry” option on page 267.

Menu reference

The following menus are applicable for autoset.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.n.4.1 Warning time</td>
<td>208</td>
<td>Period of time during which the automatic set procedure can be postponed.</td>
</tr>
<tr>
<td>4.2.n.5.2 Set retry</td>
<td>209</td>
<td>Define whether users can postpone or cancel an autoset.</td>
</tr>
<tr>
<td>4.2.n.5.3 Silent autoset</td>
<td>209</td>
<td>The keypad buzzer remains silent during the warning time.</td>
</tr>
<tr>
<td>7 Calendar</td>
<td>246</td>
<td>Configure an automatic setting at particular time and date.</td>
</tr>
<tr>
<td>8.4.7 AS fault retry</td>
<td>267</td>
<td>Define if and when the system repeats an attempt to set automatically in if a system fault has made an autoset impossible.</td>
</tr>
<tr>
<td>8.4.8 AS user retry</td>
<td>267</td>
<td>Define a time for which a normal user can postpone an autoset.</td>
</tr>
</tbody>
</table>
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 191.

   1>Expander 1
   2 Expander 2

2. Select zone location.

   Learn mode
   >Sequential<

3. Choose Sequential mode and press Enter.

   INFO
   Tamper RF 1

4. Activate the wireless device. See “Device activation” on page 107 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 191.

   1>Expander 1
   2 Expander 2

2. Select zone location.

   Learn mode
   >Manual<


   Tamper RF 1
   Press # for ID

4. Activate the device, or press Enter to enter the wireless device identifier manually. See “Device activation” on page 107 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 204 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 106.
If the device is programmed successfully, the keypad shows an information message and beeps once.

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

Chose Yes and press Enter to edit zone settings.
Otherwise you are asked if you want to learn another wireless device.

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.

See “Using cameras” on page 109 for more details.

**Learning fobs**

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

**Sequential mode**

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

**To learn fobs in sequential mode:**

1. Go to the “4.4.0 Add fob” menu described on page 211.

2. Select fob zone location.

3. Choose Sequential mode and press Enter.

4. Choose an input number.
5. Press the programming key sequence to activate the fob. See “Device activation” on page 107 for more information about activation.

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

WARNING
ERROR

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

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

INFO
Fob learned

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

INFO
Program fob 2

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

Proceed with the fob configuration.

**Manual mode**

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

**To learn a fob in manual mode:**

1. Go to the “4.4.0 Add fob” menu described on page 211.

   1>Expander 1
   2 Expander 2

2. Select zone location.

   Learn mode
   >Manual<


   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 107 for more information about activation.

<table>
<thead>
<tr>
<th>Fob ID</th>
<th>&gt;</th>
<th>&lt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fob key</td>
<td>&gt;</td>
<td>&lt;</td>
</tr>
</tbody>
</table>

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

INFO
Fob exists

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

Replace fob?
>No<

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

INFO
Fob learned

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

Edit fob?
>No<

Choose Yes and press Enter to edit fob settings.

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

Next fob?
>No<

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

Two-zone RF sensors

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

Note: For two zones to be visible upon device learning process, the device must have an appropriate configuration during the activation. See Table 19 on page 107 for more details.

1 or 2 zones
>2<
If 1 zone is selected, this zone functionality depends on sensor configuration. See “4.1.n.7.5 Sensor opt” on page 205.

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.

**Device activation**

Depending on the device type, the learning activation of this device can differ. Table 19 below lists all compatible devices and their activation methods.

**Table 19: Wireless device learning activation**

<table>
<thead>
<tr>
<th>Device type</th>
<th>Learning activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door / window sensor</td>
<td>Raise a tamper alarm by opening the housing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For two zones programming in sequential mode, the external contact input must be in open state.</td>
</tr>
<tr>
<td>Shock sensor</td>
<td>Raise a tamper alarm by opening the housing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For two zones programming in sequential mode, the reed contact must be enabled and closed with the magnet.</td>
</tr>
<tr>
<td>Smoke detector</td>
<td>Raise a tamper alarm by removing the detector head from the base.</td>
</tr>
<tr>
<td>PIR camera</td>
<td>Raise a tamper alarm by removing the PIR camera from its mounting plate.</td>
</tr>
<tr>
<td>Fob</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>2. Press the unlock button quickly, then press and hold until fob LED flashes 2 times. Release the button immediately after the second flash.</td>
</tr>
<tr>
<td></td>
<td>3. Press and hold the unlock button until touchpad light flashes once, and then release the button immediately.</td>
</tr>
</tbody>
</table>

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

**Menu reference**

The following menus are applicable for wireless devices.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1.3 RF RSSI test</td>
<td>138</td>
<td>Display received signal strength indicator (RSSI).</td>
</tr>
<tr>
<td>1.2.1.4 RF diagnostics</td>
<td>138</td>
<td>Display wireless device status.</td>
</tr>
<tr>
<td>1.2.1.5 Cam range test</td>
<td>139</td>
<td>Verify wireless PIR camera signal reception.</td>
</tr>
<tr>
<td>2.2.2 Expander devices</td>
<td>168</td>
<td>Configure wireless expanders.</td>
</tr>
<tr>
<td>3.1.n.4 RF fobs</td>
<td>184</td>
<td>Configure the selected user fobs.</td>
</tr>
<tr>
<td>4.1.n.7 RF details</td>
<td>204</td>
<td>Program a wireless device manually, or remove it from the wireless expander.</td>
</tr>
</tbody>
</table>
## Chapter 3: System functions

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4 RF fobs</td>
<td>211</td>
<td>Configure fobs.</td>
</tr>
<tr>
<td>4.5 Cameras</td>
<td>214</td>
<td>Configure camera modules in wireless PIR cameras.</td>
</tr>
</tbody>
</table>
Using cameras

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

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

Configuration

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

- Activation of one of 4 assigned zones. Zones are assigned in menu “4.5.n.2 Pics by zone” on page 214.
  
  In this case camera event type depends on the zone type. See “Camera event types” below.

  See also “Zone types” on page 47.

- Activation of a condition filter. The event type is defined for the programmed filter. See “4.5 Cameras” on page 214.

- Activation of a standard reporting event. See “4.5.n.4 Pics by rep ev” on page 215.

- User command.

- Remote request from configuration software.

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

Camera event types

There are the following camera event types available.

- Burglar alarm. Generated by alarm, entry/exit, access, 24 H, fire door and keybox type zones.

- Fire alarm. Generated by fire zones.

- Panic alarm. Generated by panic zones.

- Medical alarm. Generated by medical zones.

- Tamper alarm. Generated by tamper zones.

- Fault. Generated by technical, transmission fault, aux mains fault and aux battery fault type zones.

- Custom type 1. Generated by conditional filters of this type.

  The types are assigned to conditional filters in “4.5.n.3.m.2 Event type <n>” on page 215.

- Custom type 2. Generated by conditional filters of this type.
Event type details are listed in Table 20 below.

### Table 20: Camera events and reporting codes

<table>
<thead>
<tr>
<th>Event type</th>
<th>Activated by zone type [1]</th>
<th>SIA code [2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire alarm</td>
<td>4. Fire</td>
<td>FA</td>
</tr>
<tr>
<td>Panic alarm</td>
<td>5. Panic</td>
<td>PA</td>
</tr>
<tr>
<td>Medical alarm</td>
<td>10. Medical</td>
<td>MA</td>
</tr>
<tr>
<td>Tamper alarm</td>
<td>7. Tamper</td>
<td>TA</td>
</tr>
</tbody>
</table>

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

[2] If the camera has been activated by a standard reporting event, another event caused by camera activation does not occur. Detailed codes and subevent values are described in Appendix B “Advisor Advanced reporting codes” on page 353.

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

[4] See “4.5.n.3.m.3 Report as” on page 215 for details.

Each of these types can be configured in “2.2.2.n.4.9.1 Pic settings” on page 173.

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

**How to program a camera:**

1. Program the wireless PIR camera expander. See “Bus devices” on page 62 for more details.

2. Program a wireless PIR camera as a wireless PIR detector. See “Wireless device programming” on page 102 for more details.

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

3. Program the camera options. See “4.5 Cameras” on page 214.

4. Assign zones to the camera. Choose up to four zones. The camera is useful if its field of view covers these zones or possible burglar escape paths from there. See “4.5.n.2 Pics by zone” on page 214.

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

5. If necessary, program conditional event filters that activate the camera. See “4.5 Cameras” on page 214 for details.
6. If necessary, program reporting events that activate the camera. See “4.5 Cameras” on page 214 for details.

**Diagnostics**

If necessary, use the following menus for diagnostics:

- “1.2.1.3 RF RSSI test” on page 138
- “1.2.1.4 RF diagnostics” on page 138
- “1.2.1.5 Cam range test” on page 139

**Menu reference**

The following menus are applicable for wireless PIR cameras.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1.3 RF RSSI test</td>
<td>138</td>
<td>Display received signal strength indicator (RSSI).</td>
</tr>
<tr>
<td>1.2.1.4 RF diagnostics</td>
<td>138</td>
<td>Display wireless device status.</td>
</tr>
<tr>
<td>1.2.1.5 Cam range test</td>
<td>139</td>
<td>Verify wireless PIR camera signal reception.</td>
</tr>
<tr>
<td>2.2.2 Expander devices</td>
<td>168</td>
<td>Configure wireless expanders.</td>
</tr>
<tr>
<td>4.1.n.7 RF details</td>
<td>204</td>
<td>Program a wireless device manually, or remove it from the wireless expander.</td>
</tr>
<tr>
<td>4.5 Cameras</td>
<td>214</td>
<td>Configure camera modules in wireless PIR cameras.</td>
</tr>
<tr>
<td>9.1 Central station</td>
<td>280</td>
<td>Set photo transmission options.</td>
</tr>
</tbody>
</table>

**Troubleshooting**

See also Chapter 7 “Troubleshooting” on page 321.

**Camera busy message**

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

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

Solution: repeat the request after a delay of a few seconds.
Chapter 3: System functions

**Camera error message**

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

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

Solutions:

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

See also “Diagnostics” on page 111.

**OH receiver line trouble when MMS sending**

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

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

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

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

- The engineer (installer) performs an engineer reset from the Engineer menu. See “8.2.4.13 Do reset” on page 261.
- 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 261, 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 192). This is used in systems using RedCare transmitters, where the central station operator can switch an output that is wired back into the panel to perform an engineer reset.

**Menu reference**

The following menus are applicable for the engineer reset.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.4 Engineer reset</td>
<td>259</td>
<td>Define which conditions require an engineer reset, perform the reset.</td>
</tr>
</tbody>
</table>
Timed unset / ATM

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

- **Double code unset.** The ATM user must enter the code, and then enter it again after the programmed delay period.
  
  The delay is set in “8.9.1 Delay” on page 279.
  
  After this delay, the user is prompted to enter the code again.
  
  The user must belong to a user group with Timed unset / ATM type. See “3.2.n.2 User group type” on page 189 for details.

- **Timed unset.** The ATM is unset for a programmed time period. This period is defined in “8.9.2 Unset Time” on page 279.
  
  The keypad displays the remaining unset time.

  
  ![Time left 11 min](Time_left_11_min)

- **Extended time.** The user can extend the unset time for an additional time period, if this period is set in “8.9.3 Ext Unset Time” on page 279 as longer than 0.

  
  ![Time left 11 min](Time_left_11_min)

  
  * to extend time

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

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

**Menu reference**

The following menus are applicable for the timed unset.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.9 Timed Unset / ATM</td>
<td>279</td>
<td>Configure the ATM (automated teller machine) interface options, for example, unset delay and extended unset delay.</td>
</tr>
</tbody>
</table>
Two-way audio

Two-way audio allows the central station operator to listen to the live audio from the protected premises in alarm, and speak back.

Note: Only specific firmware versions are compatible with the two-way audio.

The following equipment is required for the two-way audio to function:

• ATS1520 two-way audio controller (installed in the control panel housing)
• ATS1521 satellite two-way audio devices (installed in the protected premises)
• ATS7700 PSTN module (installed in the control panel housing) or ATS73X0 GSM module.

Note: Sending analogue messages over the GSM channel correctly depends on the quality of the GSM network, which changes often.

Refer to the specific installation sheets for mounting and installation details.

To enable the two-way audio:

• Install audio devices using menu “2.2.4 Audio devices” on page 179.
• Configure the necessary central station and DTMF settings in the menu “9.1.n.10 Listen-in” on page 288.
• Configure zone settings in the menu “4.1.n.8 Listen-in” on page 201.
• Configure fob settings in the menu “4.4.n.5 Listen-in” on page 213.
• Configure keypad settings using “2.2.1.n.5 Listen-in” on page 167.
• Set the transmission path to PSTN using “9.1.n.2 Transm path” on page 281.
• Set the reporting protocol to SIA or XSIA in the menu “9.1.n.3 Protocol” on page 281.
• Choose events for audio reporting in “9.2.4 Lis-in events” on page 290.

Audio session

Audio session with the central station starts when one of the objects with listen-in function configured (zone, keyfob or keypad) generates an event. When the audio session is established, the audio device assigned to this object is turned on in the listening mode.

Next events don’t stop the active session, but activate consecutive audio devices and add them to the follow list. There can be up to 32 microphones and 4 speakers in the follow list. The follow list is cleared every set cycle.

During the audio session all sirens are silenced, however the appropriate siren timers do not stop. All other reporting over PSTN is put on hold until the session is over.

In case of a duress alarm, all speakers are disabled, so speaking mode has no effect.
**DTMF control**

During the audio session the central station operator can send specific commands using DTMF codes if the panel configuration allows him to do so.

The following DTMF tones are available: 1, 2, 3, 4, 5, 6, 7, 8, 9, *, 0, #, 99.

Using menu “9.1.n.10.3 DTMF control” on page 289, you can assign command to tones. The following commands are available:

- Disabled: No action assigned.
- Listen: Switch the audio session to the listening mode.
- Speak: Switch the audio session to the speaking mode.
- Extend session: Extend the session time by 30 s.
- End session: End the audio session.
- Trigger Flag 1 to 4: Trigger central station flag 1 to 4.

To allow the central station operator switching output states on the control panel for external equipment control, do the following:

- Configure appropriate outputs or user programmable functions. See also “Outputs” on page 73 and “User programmable functions” on page 97.
- Assign appropriate DTMF codes to central station events. Use “9.1.n.10.3 DTMF control” on page 289. See also Appendix A “Advisor Advanced events” on page 337.
- Use “Condition filters” described on page 80 if necessary.

**Audio specific menus**

The following menus are specific for the panels with two-way audio functionality.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.14 Listen-in</td>
<td>155</td>
<td>Test a two-way audio session between the system and a phone</td>
</tr>
<tr>
<td>2.1.3 Audio devices</td>
<td>159</td>
<td>View installed audio devices</td>
</tr>
<tr>
<td>2.2.1.n.5 Listen-in</td>
<td>167</td>
<td>Configure two-way audio for the selected keypad</td>
</tr>
<tr>
<td>2.2.4 Audio devices</td>
<td>179</td>
<td>Configure audio devices</td>
</tr>
<tr>
<td>4.1.n.8 Listen-in</td>
<td>201</td>
<td>Configure two-way audio for the selected zone</td>
</tr>
<tr>
<td>4.4.n.5 Listen-in</td>
<td>213</td>
<td>Configure two-way audio for the selected fob</td>
</tr>
<tr>
<td>9.1.n.10 Listen-in</td>
<td>288</td>
<td>Configure two-way audio for the selected central station</td>
</tr>
<tr>
<td>9.2.4 Lis-in events</td>
<td>290</td>
<td>Select events that activate a two-way audio session with a central station</td>
</tr>
</tbody>
</table>
UltraSync

UltraSync is a secure cloud solution, connecting alarm devices to remote application via a managed web portal, supported by a service model. The UltraSync connectivity can be enabled in the panel (all ATSx500A variants), Advisor Advanced mobile application (IOS/Android), and the ATS8500 software.

Path communication to the UltraSync cloud can be single or dual: via the on-board Ethernet connection, and GSM/GPRS communicator (ATS73X0) connected to the panel.

The events can be delivered via push notification to the mobile devices of maximum 10 users.

Note: A push notifications can only be received if the phone is switched on when the notification is being sent. There is no buffering for notifications. The mobile application must be running for push notifications to be received.

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

The panel is identified in the UltraSync cloud by its unique serial number. The serial number is shown in the “9.5.2 SID number” screen described on page 310.

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

Service model

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

- Basic Service model
- Portal Service model

In the Basic Service model, you use the unique serial number in the Mobile Application and Downloader in order to connect in an easy way. This model includes smartphone push messages. The alarm reporting has to be configured by the installer to an OH Receiver using Ethernet or a GSM module for communication. When you use the mobile connection, you need to use your own SIM card.

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

Registering the panel in the UltraSync portal is linked to a monthly service cost. Unregistered panel does not support UltraSync SIM cards. Also, the UltraSync communication path monitoring is not supported.

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

UltraSync SIM card

ATS7320-SIM is an ATS7320 GSM module with a preinstalled UltraSync SIM card. This module and its SIM card should be used for UltraSync functionality only when the panel is registered in the UltraSync portal. Registering the panel in the UltraSync portal is linked to a monthly service cost.

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

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

Configuring a control panel from Advisor Advanced Mobile Application

See “Mobile Application” on page 120 for information.

Creating a site in Web portal

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

1. Ensure that your panel is connected to the secure cloud via Ethernet or GPRS.
2. Sign in on Web portal using the URL address and credentials obtained from the manufacturer.
3. On the list of available sites (panels), click New Site.
4. Select your central station (defined by the manufacturer), or choose Self Monitoring.
5. Provide your site name, which identifies your site in Web portal.
6. Enter the site address and contact information, if necessary.
7. Enter your panel serial ID number, which can be found on the package box, or in the “9.5.2 SID number” screen described on page 310.
8. Select your time zone.
9. Choose a reporting channel (VFNN).
10. Enter the account number.

Note: Web portal allows only one account number per panel to be defined.
11. Enter the required service grade.  
   Service grade defines security grade and reporting communication path,  
   which can be IP (Ethernet), cellular (GPRS), or dual path (IP primary  
   reporting and cellular backup reporting).

12. Select the reporting format, required by the central station.

13. Click Create.

Your site is now created.

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

**Menu reference**

The following menus are applicable for the UltraSync functionality.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.n.2 Transm path</td>
<td>281</td>
<td>Set the central station communication to UltraSync Cloud.</td>
</tr>
<tr>
<td>9.5 UltraSync</td>
<td>310</td>
<td>Configure UltraSync communication.</td>
</tr>
</tbody>
</table>
Mobile Application

Advisor Advanced Mobile Application allows you to monitor and control your Advisor Advanced security system via TCP/IP using a smartphone running Android or iOS operating system.

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

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

Contact your installer to enable the mobile control functionality in your panel, and to obtain all connection details.

**Connecting to the panel via UltraSync cloud**

To connect to the panel from the Mobile Application via UltraSync cloud, do the following:

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

Enter your panel PIN and select the PIN prompt mode.

Tap Log in, or Setup next panel if required.

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

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

**Menu reference**

The following menus are applicable for the Mobile App functionality.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 User menu</td>
<td>182</td>
<td>Add, edit, or delete users and user groups.</td>
</tr>
<tr>
<td>4.5 Cameras</td>
<td>214</td>
<td>Configure camera modules in wireless PIR cameras.</td>
</tr>
<tr>
<td>6 Outputs and filters</td>
<td>238</td>
<td>Configure outputs.</td>
</tr>
<tr>
<td>9 Communication</td>
<td>280</td>
<td>Program all system-wide communication options.</td>
</tr>
</tbody>
</table>
Chapter 4
Programming

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

Content
The Advisor Advanced menu 122
  How the menu sections are organized in this manual 122
  Option availability 123
How to program the options 124
  Accessing the installer programming menu 124
  What the LCD display tells you 125
  Editing the options 125
  Confirmation of changes 127
  Exit from menu 127
  Keypad layout 128
Remote access 129
Initial start-up 130
  Auto configuration 132
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 259).

**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 257.

The option is enabled in “8.2.6 Challenge code” on page 262.

**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 130 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 259) 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 257.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change selection</td>
<td>Press Up or Down</td>
<td>Select previous or next menu entry</td>
</tr>
<tr>
<td>Enter the menu entry</td>
<td>Enter menu entry number, or</td>
<td>Jump to a specific menu entry</td>
</tr>
<tr>
<td></td>
<td>Press Enter or Right to enter the selected one</td>
<td></td>
</tr>
<tr>
<td>Show help</td>
<td>Press Help</td>
<td>The description of the selected menu entry is displayed (if available)</td>
</tr>
<tr>
<td>Exit the menu entry</td>
<td>Press Left or Clear</td>
<td>Exit the menu entry</td>
</tr>
</tbody>
</table>

You can now select the menu option you want to program. See “Programming map” on page 380 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
Chapter 4: Programming

- 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 128.

- 1 to 0: Enter a character
- Up: Delete a character
- Down: Backspace
- Left and Right: Move the cursor
- Function, and then Left: delete text backwards
- Function, and then Right: delete text onwards
- Enter: Confirm the entry
- Clear: Exit without changes

How to edit a list

5 Areas
  >12,4....<

- Up and Down: Toggle the value under cursor
- 0: Include or exclude all values in the list
- Left and Right: Move the cursor to a specific item
- Enter: Confirm the entry
- Clear: Exit without changes

If the number of allowed list elements is higher than 16, the list elements are grouped, for example:

01-10 Areas
  >12,4....<

In this case, select a group first, and then edit the selected group as described above.
How to edit a host address

Using the same rules as described in “How to edit text” on page 126, 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 295, and must be available.

Confirmation of changes

If particular settings are changed, you are prompted to confirm those changes when you exit from the current menu. The following screen appears:

Apply settings?
> No <

Changing of other settings that affect user configuration, like PIN length, Duress method, etc., requires all user database reset. In this case you are prompted to confirm all user removal.

Reset users?
> No <

If you want to keep the changes, choose “Yes” and press Enter, otherwise the changes are cancelled.

Exit from menu

You must confirm your decision to exit from the menu system. The appropriate prompt appears. Choose “Yes” and press Enter to exit from the menu.

Goodbye?
> No <

Alternatively, choose “Engineer mode”. In this case the panel remains in the service in mode, while the installer logs off the keypad. It lets the installer to log in another keypad without leaving the programming mode.

If any faults or any open inputs are present, they are listed the same way as in the menu “1.2.4 Panel status” on page 142.
Keypad layout

Table 21: ATS111xA keypad layout for entering text

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

Table 22: ATS1135 keypad layout for entering text

<table>
<thead>
<tr>
<th>Key</th>
<th>Character sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>. , ' ? ! − &amp; % * / _ &lt; &gt; @ 1</td>
</tr>
<tr>
<td>2</td>
<td>a b c A B C 2</td>
</tr>
<tr>
<td>3</td>
<td>d e f D E F 3</td>
</tr>
<tr>
<td>4</td>
<td>g h i G H I 4</td>
</tr>
<tr>
<td>5</td>
<td>j k l J K L 5</td>
</tr>
<tr>
<td>6</td>
<td>m n o M N O 6</td>
</tr>
<tr>
<td>7</td>
<td>p q r s P Q R S 7</td>
</tr>
<tr>
<td>8</td>
<td>t u v T U V 8</td>
</tr>
<tr>
<td>9</td>
<td>w x y z W X Y Z 9</td>
</tr>
<tr>
<td>0</td>
<td>Space 0</td>
</tr>
</tbody>
</table>

The keypad layout, as well as the menu text, depends on the language programmed for the user currently logged in.

The layout may change depending on the context of the edited value. For example, digits are entered prior to characters when editing phone numbers.
Remote access

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

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

By default, the menu is accessible remotely with the same installer PIN. The remote access PIN can be altered using menu “3.1.n.2.2 Remote PIN” on page 183.

**Cautions**

- Once enabled, remote PIN can be neither disabled nor changed locally, and the Remote PIN menu is disabled.
- If PIN length gets changed (via “8.7.4 PIN length” described on page 272) while remote PIN is enabled, the configuration software will not be able to connect the programmed panel anymore. It will be necessary to delete the panel configuration in the software, and then recreate it.

The remote configuration is allowed only if the option “8.7.8.1 Remote config” on page 275 is set to Yes.

The supervisor is allowed to configure the panel remotely only if the option “8.7.8.2 Superv config” on page 275 allows 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 23: Values set during installation

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Panel language</td>
<td>Defines the language [1] of the panel menus. This language is used for messages when no user is logged in. After login the language is switched to the one assigned to the logged user (set by system manager).</td>
</tr>
<tr>
<td>2 Defaults</td>
<td>Defines approval dependent default values [1].</td>
</tr>
<tr>
<td>3 Time and date</td>
<td>Time and date must be set during installation. See also “8.1.1 Time and date” on page 254.</td>
</tr>
<tr>
<td>4 UltraSync</td>
<td>UltrasSync options. See “UltraSync” on page 117 for details.</td>
</tr>
<tr>
<td>4.1 Connectivity</td>
<td>Enable or disable the UltraSync cloud connection. See also “9.5.1 Connectivity” on page 310.</td>
</tr>
<tr>
<td>4.2 Password</td>
<td>The UltraSync password is necessary to connect to the panel remotely via UltraSync cloud. See also “9.5.3.1 Password” on page 311.</td>
</tr>
<tr>
<td>5 Other options</td>
<td></td>
</tr>
<tr>
<td>5.1 Duress method</td>
<td>Default duress method. See Advisor Advanced Manager Manual for more information. See also “8.7.3 Duress method” on page 272.</td>
</tr>
<tr>
<td>5.2 PIN length</td>
<td>Default length of PIN (allowed range is from 4 to 10). See “8.7.4 PIN length” on page 272 for more details.</td>
</tr>
<tr>
<td>5.3 PIN change mode</td>
<td>PIN change mode. See “PIN” on page 71 for details on PIN usage. See also “8.7.5 PIN chg mode” on page 273.</td>
</tr>
<tr>
<td>6 Install</td>
<td>Run the installation process</td>
</tr>
</tbody>
</table>

[1] Contact your supplier for a list of available languages and approved versions.

Set the appropriate options and run the installation, then choose OK and press Enter.

Next, you are prompted to change the installer and the supervisor PINs.
Press Enter.

New PIN
>_ 

Verify
>_ 

Provide the new installer PIN of the required length, and press Enter. Next, enter the PIN again to verify it.

If the PIN is changed successfully, the following message appears.

INFO
PIN changed

If the provided PIN is shorter than required, or the new PIN is the same as the previous one, the warning is displayed.

WARNING
Wrong PIN

If the PIN confirmation fails, the following warning is displayed.

WARNING
PIN NOT changed

Repeat the above steps for the supervisor PIN.

After both PINs are successfully set, the panel continues the installation process.

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

The display shows the installation progress percentage complete.

After the installation is complete, the panel restarts.

Note: You can change most of these values later using menu “8.7 Panel and AB options” (see page 272).

See also “1.5 Default panel” on page 158.

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

During the second system start, the panel prompts to activate an automatic system configuration.

![Auto Config?]

Select No and press Enter to cancel.
Select Yes and press Enter to run the automatic configuration process.

The system configures the following elements:

1. **Keypads and expanders.**
   
   ![Rkp 1-16 BUS1]
   ![Exp 1-15 BUS1]
   ![Aud 1-16 BUS1]

   Bus devices are automatically configured in a way that is similar to the configuration via viewing devices menu. See “2.1 Installed remotes” on page 159 for details.

2. **Zones.**

   Zones are configured according to the number of installed internal and external expanders, as well as the number of physical inputs in a state, which is equal to the normal state of the zone.

   **Note:** Normal zone state depends on “2.2.2.n.4.4 Input mode” on page 170 and “8.6.1 Input mode” on page 270.

After the configuration is complete, the number of configured elements is displayed.

![Added]

The following elements are displayed: R – remote keypads (or RASes), D – remote expanders (DGPs), Z – zones, A – audio devices.

**Caution:** After the installation and the auto configuration you automatically enter to the programming menu. Next time you will need an authorization to enter the menu.
Chapter 5
Menu reference

Summary
This chapter contains descriptions of all programming menu entries of Advisor Advanced control panel.
See “The Advisor Advanced menu” on page 122 for more information about menu organization.

Content
1 Service menu 136
   Test options 137
2 Device menu 159
   2.1 Installed remotes 159
   2.2 Edit Keypad&Exp 160
   2.2.1 Keypad devices 160
   Keypad options 160
   2.2.2 Expander devices 168
   Expander options 168
   Wireless specific options 171
   Camera specific options 173
   Four-door expander specific options 175
   2.2.3 DC/LC Exp Rdrs 178
   Reader options 178
   2.2.4 Audio devices 179
   Audio device options 180
3 User menu 182
   3.1 Users 182
   Common options 182
   Mobile phone options 186
   Access control options 187
   3.2 User groups 189
   User group settings 189
4 Zones and areas 191
   4.1 Zone menu 191
   Zone options 191
Adding a wireless sensor  191
Common options  192
Shock sensor options  203
Wireless sensor options  204
4.2 Areas  206
Area options  206
4.3 Area groups  211
Area group options  211
4.4 RF fobs  211
Fob options  211
4.5 Cameras  214
5 Door menu  217
  5.1 Doors  217
    Common door options  217
    Standard door specific options  225
    Intelligent door specific options  225
    5.2 Door groups  235
    5.3 Regions  237
6 Outputs and filters  238
  6.1 Condition filters  238
    Filter settings  238
  6.2 Outputs  240
    Output settings  240
  6.3 Triggers  244
    Trigger settings  244
7 Calendar  246
  7.1 View  246
  7.2 Schedules  247
    Schedule settings  248
8 System option menu  254
  8.1 Timer menu  254
  8.2 Engineer options  259
  8.3 LCD display options  263
  8.4 Set options  264
  8.5 Access options  268
  8.6 Zone options  270
  8.7 Panel and AB options  272
  8.8 PA and other  276
  8.9 Timed Unset / ATM  279
9 Communication  280
  9.1 Central station  280
    Common options  281
    PSTN and ISDN specific options  285
    IP and GSM/GPRS specific options  285
    Photo transmission specific options  287
    GSM/phone specific options  288
    Audio specific options  288
UltraSync specific options 289
9.2 Event options 290
9.3 Path options 291
Common options 291
PSTN specific options 293
ISDN specific options 294
IP specific options 294
GSM/SMS/GPRS specific options 297
9.4 PC connection 306
Common options 306
PSTN specific options 309
IP specific options 309
GSM specific options 310
9.5 UltraSync 310
1 Service menu

1>Display logs
2 Test menu

The Service menu provides an installer with options for commissioning and maintenance such as hardware overview, logs listing, etc.

1.1 Display logs

1>All
2 Mandatory

The View logs menu is a fast and easy way to review where alarms have happened. This information is useful when you have had to reset an alarm without initially checking its cause.

You can select one of the following message types:

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

The display shows where the alarm occurred.

1>Access granted
User 3

You can now:

- Scroll through the alarm list. Press Up or Down.
- View details. Press Enter.

05May08 15:04:54
Keypad 1

If there is additional information, it is scrolled automatically.

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

1.2 Test menu

1>Input tests
2 ShockSens test

The Tests menu gives you access to all testing functions.

1.2.1 Input tests

1> Show open zn
2 Nbr of used zn

Enter the Input test menu to test inputs.

1.2.1.1 Show open zones

0>Zone
1 Panel

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

Zone number, name, and input state are displayed.

12>Warehouse
Normal

You can now:

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

12>Warehouse
Alarm

12>Warehouse
Panel Exp 1.12

• Exit input test. Press Clear.

1.2.1.2 Number of used zones

Zone capacity 64
Zones used 8

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

• Zone capacity: Maximum zone number in the Advisor Advanced system
• Zones used: Number of zones currently programmed.
1.2.1.3 RF RSSI test

Select the input location first.

Notes

• Only existing RF expanders are displayed.
• The function is not supported in wireless expanders ATS1235 with firmware version older than 1.20.

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

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.

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

1.2.1.4 RF diagnostics

Select the input location first.

Notes

• Only existing RF expanders are displayed.
• The function is not supported in wireless expanders ATS1235 with firmware version older than 1.20.

Enter the physical input number on this location. The RF state is then displayed, for example:

The device can report the following states:

• RF state OK: The RF device is working properly
• No data: No data received from the RF device
• LB: Low battery fault
• SS: Short supervision fault
• LS: Long supervision alarm
• D: Fire sensor is contaminated

1.2.1.5 Cam range test

Range test allows you to verify wireless PIR camera signal reception.
Select a camera to activate 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

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.

See also “8.1.4.7 Inactive days” on page 258.

1.2.1.7 Zone kOhm

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 | 4.6kΩ |

Values above 65 kΩ are considered as open state.

You can now scroll through the list of inputs by pressing Up or Down.

**Note:** External expanders (DGP) do not support this functionality.

### 1.2.1.8 Detector test

#### 1.2.1.8.1 Duration

| 1 Duration | >10< |

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

#### 1.2.1.8.2 Test time

| 2 Test time | >00:00< |

The time of day the system activates an automatic detector test on.

The allowed range is 00:00 to 23:59, while 00:00 is equal to Off and means that the automatic test is disabled.

#### 1.2.1.8.3 Test when Set

| 3 Test when set | >Off< |

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

#### 1.2.1.8.4 Manual test

| 4 Manual test | >Cancel< |

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

### 1.2.1.9 Shunt zones

| 1>Exit Button | Shunt Off |

The menu allows you to shunt zones manually.
1.2.2 ShockSens test

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.

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 204 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

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

1.2.3.1 Output test

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.

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

Use the Keypad LEDs menu to test keypad and reader LEDs.
Choose the keypad and press Enter.

You can now:

- Switch all keypad LEDs to the on or off state using the Enter button.
- Exit keypad LED test. Press Clear to exit from test and restore the LED states.

### 1.2.3.2 Trigger state

1>Trigger 1
2 Trigger 2

The trigger state menu allows you to manually change trigger flag states. Choose the trigger and then choose the appropriate flag. Next, set the required state.

1>SCHEDULE

**off**

### 1.2.4 Panel status

1>View open ZN
2 Alarms

The Panel status menu provides an overview of all abnormal zone states, alarms and faults present in the system. Select the required state to view.

#### 1.2.4.1 View open ZN

INFO
View open ZN

2>Front Door
Zone tamper

View abnormal zone states. All items scroll automatically. Press Enter to exit.

#### 1.2.4.2 Alarms

INFO
No alarms

View active alarms. Press Enter to exit.

#### 1.2.4.3 Faults

INFO
No faults

View active system faults. Press Enter to exit.
1.2.5 Walk test

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

See also “Walk test” on page 88 in Chapter 3 “System functions”.

1.2.5.1 Start

Run the engineer walk test.

See “Engineer walk test” on page 88 for details.

1.2.5.2 Walk test opts

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

1.2.5.2.1 Use internal siren

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

1.2.5.2.2 Use buzzers

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

1.2.5.2.3 Log untested

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

1.2.5.2.4 Zone tamper

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

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

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

The Frequency setting defines, how often the user is requested to perform the user walk test prior to setting an area. The following options are available:

- Never: User walk test is not requested
- Every set: User is asked to perform the walk test prior to each set
- 1st set of day: User is asked to perform the walk test prior to the first set each day
- 1st set of week: User is asked to perform the walk test prior to the first set each week
- 1st set of month: User is asked to perform the walk test prior to the first set each month

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

1.2.5.2.8 Need to set

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

Reduced walk test period is a time period before reduced walk test start, in which particular zone activation excludes this zone from the list of zones being tested. The following options are available:

- **4h**: Reduced walk test only includes zones that were not active during last 4 hours.
- **Set2set**: Reduced walk test only includes zones that were not active since the last set.

See “1.2.5.1 Start” on page 143 for more details on reduced walk test.

1.2.5.3 Single zone WT

Before walk test starts, you are asked if the reporting to central stations must be enabled (see “1.2.5.1 Start” on page 143 for details).

Select the input location first (panel, internal or external expander). Then enter the (physical) input number on this location.

Proceed with walk test for this particular zone the same way as for all zones in a standard walk test. See “1.2.5.1 Start” on page 143.

1.2.5.4 Test No Bells

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

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

1.2.5.5 Active walk test

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

See “Active walk test” on page 90 for more details.
1.2.6 Test call opts

The Test call menu allows you to define the automatic test call interval, and to perform a test call on demand.

1.2.6.n Select CS

Select central station to configure test call options.

1.2.6.n.1 Test call mode

Select test call mode. The following modes are available:

- Off: Automatic test call functionality is disabled.
- Time: Automatic test call triggers every day at the time of the day programmed in “1.2.6.n.2 Test call time” below.
- Period: Automatic test call triggers once at the time specified in “1.2.6.n.2 Test call time” below, and then repeats with the interval programmed in “1.2.6.n.3 Period” on page 147.

1.2.6.n.2 Test call time

If the “1.2.6.n.1 Test call mode” above is set to Time, the menu allows you to define the time of the day for test calls to the central station.

If the “1.2.6.n.1 Test call mode” above is set to Period, the menu allows you to define the time of the day for the first test call to the central station. Once the time is defined in this menu, the panel starts sending the event RP (Automatic test/ring-in test) report to the appropriate central stations. The event is sent periodically, the period is defined in the menu “1.2.6.n.3 Period” on page 147.

Note: If the option “1.2.6.n.4 Extend” on page 147 is set to Yes, the real time of the test call can vary depending on other events reported to the central station.

This start time is used by the panel when one of the following occurs:

- The panel is reset
- One of the test call options is changed by installer

The test call time is set in 24 h format, as HH:MM.
1.2.6.n.3 Period

The Period menu defines an interval for test calls that are described in “1.2.6.n.2 Test call time” on page 146.

The allowed range is 1 to 999 hours.

1.2.6.n.4 Extend

The Extend option defines whether the test call interval is counted from the previous test call or from the last successful event report.

If this option is set to Yes, after an event transmitted to the central station the test call delay is extended and the next test call is postponed.

If this option is set to No, the next test call occurs in a test call period after the previous test call, regardless of other reported events.

1.2.6.n.5 Freq TC if FTC

If this option is set to Yes, during the communication fault (FTC) the panel tries to establish a communication by initiating a test call every hour. Otherwise, the test call is attempted as usual.

Caution: Enable this function only for primary central station.

1.2.6.n.6 Man. test call

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

The call progress status is shown on the display.

1.2.7 IP diagnostic

The IP diagnostic menu provides an access to diagnostic tools for IP connectivity.
1.2.7.n Choose interface

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

The IP statistics menu allows viewing of the statistics listed below.

- 1 TX packets: Number of packets sent.
- 2 RX packets: Number of packets received.
- 3 Rej. packets: Number of packets that are rejected by built-in firewall. See “9.3.n.7 Firewall” on page 296 for more information.
- 4 TX bytes: Number of bytes sent.
- 5 RX bytes: Number of bytes received.
- 6 Clear stat: This command clears the data described above.

1.2.7.n.2 Ping host

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

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 310 for more details. See also “1.2.7.n.2 Ping host” above.

1.2.7.n.4 Ping CS

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 286 for more details. See also “1.2.7.n.2 Ping host” on page 148.

1.2.7.n.5 NTP status

The NTP status screen allows you to check the current status of the Network Time Protocol server configured. Possible server statuses are listed below.

- Inactive: The NTP server is not queried yet. This status is usually present after panel restart or NTP configuration.
- Unknown: The query was sent, but no answer from NTP server was received yet.
- Fail: No answer from NTP server.
- OK: NTP server answered the query.
- Link error: Faulty Ethernet line.

1.2.8 GSM diagnostic

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

1.2.8.1 PIN status

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.

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.

The GPRS network registration state can have the same values as described in “1.2.8.3 GSM net.reg.” on page 149.

1.2.8.5 GPRS state

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 304 for more details.
• No data: Unknown error.

1.2.8.6 Network name

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

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

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

Table 24: RSSI ranges

<table>
<thead>
<tr>
<th>RSSI</th>
<th>Signal level</th>
<th>Bar indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>&lt;-112 dBm</td>
<td>[ ]</td>
<td>No signal</td>
</tr>
<tr>
<td>1 to 7</td>
<td>-111 to -99 dBm</td>
<td>[I ]</td>
<td>Insufficient signal</td>
</tr>
<tr>
<td>8 to 12</td>
<td>-97 to -89 dBm</td>
<td>[II ]</td>
<td>Mediocre signal</td>
</tr>
<tr>
<td>13 to 20</td>
<td>-87 to -73 dBm</td>
<td>[III ]</td>
<td>Good signal</td>
</tr>
<tr>
<td>21 to 26</td>
<td>-71 to -61 dBm</td>
<td>[III ]</td>
<td>Excellent signal</td>
</tr>
<tr>
<td>27 to 31</td>
<td>&gt;-60 dBm</td>
<td>[IIIIII ]</td>
<td>Excellent signal</td>
</tr>
</tbody>
</table>

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

1.2.8.9 Msg sent 24h

1>All SMSes 0

The Msg sent 24h menu lists the SMS messages sent since midnight (00:00). The following submenus are available.

• 1 All SMSes: All messages.
• 2 Report SMSes: Reporting messages.
• 3 Unknown SMSes: User SMS control messages that were not recognized and therefore forwarded to the Supervisor.

Note: This counter works only if the SMS forwarding is enabled. See “9.3.n.6.2 SMS forwarding” on page 302.

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, ATS120xEx expanders.
• Battery test works only if there is no mains fault present.
1.2.9.1 Test options

1>Panel
3 Exp

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

1.2.9.1.m Select device type

1>Expander 1
2 Expander 2

Select the appropriate device group.

1.2.9.1.m.n Select device

1>Test time
10

Select the appropriate device.

1.2.9.1.m.n.1 Duration

1 Duration
> 10<

Set duration (in minutes) for battery test. Allowed range is 2 to 254.

1.2.9.1.m.n.2 Batt.test freq

2 Batt.test freq
>Disabled<

Set automatic battery test frequency. The following values are available:

- Disabled
- Every working day
- Every Monday
- First Monday of month
- Everyday

1.2.9.2 Man. Bat. test

1>Panel
3 Exp

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

1.2.9.2.m Select device type

1>Exp 1
2 Exp 2

Select the appropriate device group.
1.2.9.2.m.n Select device

1.2.9.2.m.n.1 Duration [min]

Set duration (in minutes) for battery test.
Allowed range is 2 to 254.

1.2.9.2.m.n.2 Run/Stop test

Run battery test.
Test duration is set in “1.2.9.2.m.n.1 Duration [min]” above.
If battery test for this device is already running, you are prompted to stop this test.

1.2.9.3 Battery replaced

After replacing the battery the installer should confirm this by using the Battery replaced menu.
Select Yes and press Enter. The confirmation is displayed for 3 seconds.

INFO
Bat. confirmed

The battery replacement is recorded in the control panel event log.

1.2.10 Panel diag

1.2.10.1 System V/A

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

System voltage: 13.8V
System current: 0.8A

The scrolled screens show the system power supply voltage and current.
1.2.10.2 Battery (V)

**Battery voltage:**

12.8V

The screen shows the battery voltage.

1.2.11 Check card

**Badge card**

Keypad 1

Use the menu to read data from a user card.

Badge card on the keypad indicated on the screen the same way as it is done when user card programming (see “3.1.n.3.1 Assign card” on page 184).

**Note:** The keypad for user card programming is defined in “8.8.5 Card learn-in” on page 277.

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 136.

- Engineer reset is disabled.

- Walk test is disabled.

- Internal and external siren outputs are disabled.
The demo mode is cancelled:
• Automatically after 15 minutes
• When the option is switched off
• When the system is restarted

The mode can be only activated via keypad.

**Note:** The demo mode should be activated only when all areas are unset.

### 1.2.13 Door control

1 Door open

The menu allows you to send a direct command to a specific door.
• 1 Door open: Open a specific door for a period configured for this door. See “5.1.n.5.1 Unlock time” on page 219.
• 2 Door lock: Lock a specific door.
• 3 Door unlock: Unlock a specific door until Door lock command is sent.
• 4 Door disable: Disable a specific door. This makes access for all users denied.
• 5 Door enable: Enable a disabled door.

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

### 1.2.14 Listen-in

1 Phone number

Use the menu to test a two-way audio session between the system and another phone number.

This option is only available for systems with two-way audio. See Chapter 3 “System functions > Two-way audio” on page 115 for more details.

#### 1.2.14.1 Phone number

Enter a phone number for a test call.

#### 1.2.14.2 Test call

Enter the menu to run a two-way audio test session.

**Notes**
• This test call is only limited to the audio reporting. No events are sent.
• Only one audio device can be tested at a time.
First, select one of the following communication paths:

- PSTN
- GSM/SMS/GPRS

**Note:** Sending analogue messages over the GSM channel correctly depends on the quality of the GSM network, which changes often.

Select an audio device to test. Asterisk “*” marks the device, which is currently being tested.

The status of the session is displayed in the bottom line. It can be one of the following:

- Ready: The device is ready for testing.
- Line busy: Phone number is busy.
- Dialing: Dialing is in progress.
- Listen: The audio session is in the listening mode.
- Speak: The audio session is in the speaking mode.
- DTMF x: A specific DTMF tone is received. Note that the DTMF code is displayed for 3 seconds.

For more information on DTMF tones, see Chapter 3 “System functions > DTMF control” on page 116.

Both the installer and the CS operator can toggle between listening and speaking mode:

- Listen: Press key 1, or DTMF 1
- Speak: Press key 2, or DTMF 2

Exit the menu to end the test session.

**Note:** You must have audio devices configured, and enter the phone number in “1.2.14.1 Phone number” on page 155 before running the test call.

### 1.3 Software Mgmt

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

#### 1.3.1 Software Rev

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 130 for details.

1.3.3 Defaults
The screen shows panel defaults set during installation. See “Initial start-up” on page 130 for details.

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

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

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

1.4 Bypass panel lid

1 Panel lid time

The Bypass panel lid option lets you connect a PC without initiating the panel tamper alarm. The following menus allow setting the isolating timer and running the connection process.

To connect a USB cable to the panel:
1. Ensure the “1.4.1 Panel lid time” value is enough for you to come to the panel, open the housing, and connect the USB cable.
2. Bypass panel lid using menu “1.4.2 Restore lid” on page 158.
3. Open the panel housing and connect the USB cable.

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

1.4.1 Panel lid time

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

Enter the Restore lid menu to bypass the panel lid. The panel lid tamper timer starts timing.
If the panel lid is already bypassed, entering this menu unbypasses it.

1.5 Default panel

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 130 for more details.

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

1.6 Service in

The menu lets you disallow the Installer in function before the Installer in-time expires (see “8.1.3.6 Installer in-time” on page 257).

Note: This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 259.
Use this function after the panel programming is complete. To disable service in, go to this menu and press Enter. Next, log out. After this, the installer log in requires another user confirmation.
See also “8.2.1 User code required” on page 259.
2 Device menu

Device menu allows you to view and configure bus devices: keypads (RASes), expanders (DGPs), readers, and audio devices.

For more information on keypads and expanders, see Chapter 3 “System functions > Bus devices” on page 62.

For more information on readers, see “Access control” on page 74.

For bus device numbering, see “Bus device numbering” on page 62.

2.1 Installed remotes

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

Note: The maximum number of devices allowed on the databus is given in “General features” on page 37.

Select a device type to display.

2.1.1 Keypad devices

2.1.2 Expander devices

2.1.3 Audio devices

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

• ?: Device is currently being read
• x: Device is offline or not supported
• I: Device is configured but isolated
• R: Keypad is online and configured (polled)
• r: Keypad is online, but not configured (new)
• D: Expander is online and configured (polled)
• d: Expander is online, but not configured (new)
• A: Audio device is online and configured (polled)
• a: Audio device is online, but not configured (new)
• M: MI bus expander is online and configured (polled)
• m: MI bus expander is online, but not configured (new)
• c: MI bus expander is online, but its address is in conflict with another expander
• O: ATS74xx series IP/GPRS dialler is online and configured (polled)
• —: No device

**Note:** For expander local devices, select the expander address first, and then select the local device type.

Press Clear to exit from this view.

Press Enter, then select OK and confirm the new configuration. In this case all new devices are added, and missing devices are removed from the system.

**Note:** The second system bus (BUS2) is only available when using the second RS485 LAN extension module. See also “Two system databuses” on page 24.

### 2.2 Edit Keypad&Exp

Choose what type of device you want to configure.

#### 2.2.1 Keypad devices

**0>** Add keypad
**1 Keypad 1**

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

**Note:** The maximum number of devices allowed on the databus is given in “General features” on page 37.

#### Keypad options

##### 2.2.1.0 Add keypad

Keypad number

On the Add keypad menu, enter the number for this new keypad and press Enter to confirm or Clear to exit without adding a device.

After the device is added, the keypad configuration options are shown.

##### 2.2.1.n Select keypad

Select the keypad number to configure.
2.2.1.n.1 Keypad type

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

2.2.1.n.2 Keypad address

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

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

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

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

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 126.

Notes
• After changing this list, the control of selected areas is also enabled (see “2.2.1.n.3.5 Control areas” below).
• You cannot select an area to view and control using this option, if this area is assigned to a door. To do so, use the menu “5.1.n.6.3 Alarm control” on page 220 instead.

2.2.1.n.3.4 View AG

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

Provides the same functionality as in “2.2.1.n.3.3 View areas” on page 161, but for area groups.
See also “Area groups” on page 52.

2.2.1.n.3.5 Control areas

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

The Control areas menu allows you to select areas that can be controlled by this keypad. The areas are displayed as a list. To change the selection, press Enter or Right, and select the appropriate areas.
See also “2.2.1.n.3.3 View areas” on page 161.

2.2.1.n.3.6 Control AG

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

Provides the same functionality as in “2.2.1.n.3.5 Control areas” above, but for area groups.
See also “Area groups” on page 52.

2.2.1.n.3.7 Control options

`1>Card&PIN mode`  `Card or PIN`

The menu contains a set of options connected to the selected keypad control functions.
See also “Keys” on page 58.
2.2.1.n.3.7.1 Card&PIN mode

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

- PIN only: Only the PIN is necessary to set and unset areas
- Card only: A single card badge unsets areas
- Card and PIN unset: Both card and PIN are required to unset areas
- Card and PIN always: Both card and PIN are required to set or unset areas
- Card or PIN: Either a PIN or a card is required to set or unset

2.2.1.n.3.7.2 Logoff time

A time period (in minutes) of the keypad inactivity before the user is automatically logged off.

Allowed range is 1 to 255 minutes. Default value is 3.

2.2.1.n.3.7.3 1 x set/unset

One-time badge to set/unset defines if the selected keypad allows you to set or unset areas with one badge. The following values are available:

- Off: One badge does not cause any set or unset action.
- Unset: One badge unsets areas.
- Set-Unset: One badge sets or unsets areas.
- Part set 1-unset / Part set 2-unset: One badge partially sets or unsets areas.

2.2.1.n.3.7.4 3 x badge set

Three-time badge to set defines if the selected keypad allows you to set areas with triple badge. The following values are available:

- Off: Triple badge does not cause any action.
- Set: Triple badge sets areas.
- Partset1 / Partset 2: Triple badge partially sets areas.

Notes

- This functionality works only if areas can be set with a card. See “2.2.1.n.3.7.1 Card&PIN mode” above for available modes.
• This functionality is available only if the “2.2.1.n.3.7.3 1 x set/unset” option described on page 163 is not configured as Set-Unset.

2.2.1.n.3.8 EE PIN lock

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

Note: If the keypad is configured as a reader, using this option is not allowed and causes a warning:

WARNING
Check door conf

In this case program this option using menu “5.1 Doors > 5.1.n.6.3.4.3 EE PIN lock” on page 222 instead.

2.2.1.n.3.9 Isolate keypad

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

2.2.1.n.3.10 Buzzer silent

It is possible to disable the keypad buzzer for particular events. The following options are available:

• Never: Buzzer operates normally. It is impossible to mute the buzzer using X + Left volume control.
• During PS exit: Buzzer does not sound when part setting. The manual volume control is available without limitations.
• Always: Buzzer is disabled. The manual volume control is available without limitations.
• During E/E: Buzzer remains silent during entry and exit time.

2.2.1.n.3.11 Quick set

The Quick set option allows setting areas without providing user PIN or card. If this functionality is on, the premises are set after pressing On without user authorization.

The following options are available:

• Off: Quick set is disabled
• Without list: All areas assigned to the keypad are set after pressing On
• With list: After On is pressed, the system prompts to choose areas from those assigned to the keypad.

This option affects part setting as well.

2.2.1.n.3.12 Function keys

1>F1 key
2 F2 key

Function keys menu allows you to assign a user programmable function to any of available function keys. See “User programmable functions” on page 97 for more details.

Function keys availability depends on the keypad type. See also “2.2.1.n.1 Keypad type” on page 161.

2.2.1.n.3.13 Area ind.LED1

13 Area ind.LED1

Area ind.LED1 allows you to assign areas to the programmable LED 1 of the keypad. The indicator is green when all areas assigned are ready to set. It turns red when any area assigned is set or part set. The red indicator is flashing when there is an alarm in an area assigned to it.

Note: This functionality is different when only one area is assigned to both indicators. In this case the combination of two indicators shows another two states of this area:
• LED 1 is red, LED 2 is off: The area is in part set 1 state.
• LED 1 is off, LED 2 is red: The area is in part set 2 state.

This indication requires the selected keypad to be assigned only to this particular area both for view and control. See “2.2.1.n.3.3 View areas” on page 161 and “2.2.1.n.3.5 Control areas” on page 162.

2.2.1.n.3.14 Area ind.LED2

14 Area ind.LED2

Use Area ind.LED2 to program LED 2 indicator in the same way as described in “2.2.1.n.3.13 Area ind.LED1” above.
2.2.1.n.3.15 Status ind.

| 15 Status ind. | >List< |

Status indication defines how the area status list is displayed. The following options may be available, depending on panel variant and keypad model:

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

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

2.2.1.n.3.16 LCD backlight

| 16 Status ind. | >Always on< |

LCD backlight option defines when the keypad display backlight is lit. There are the following options available:

- **Always on**: LCD backlight never switches off.
- **Normal**: LCD backlight switches off after the particular idle time.
- **Excl. entry**: LCD backlight is off during the entry time, until a key is pressed.

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

2.2.1.n.3.17 ACK on keypad

| 1>Rkp 1 2 Rkp 2 |

The ACK on keypad option allows you to select an additional LCD keypad that displays an acknowledgement prompt after the system is unset using the selected non-LCD keypad or reader.

**Note**: This option is only available for non-LCD keypads and card readers.

See also “4.1.n.6.26 ACK on keypad” on page 198 for more details.

2.2.1.n.3.18 EE 1 buzzer

| 18 EE 1 buzzer | >Yes< |

If the option is set to Yes, the buzzer of the selected keypad is active during entry/exit time 1.

See “2. Entry/Exit 1” on page 47 for more details.
2.2.1.n.3.19 EE 2 buzzer

19 EE 2 buzzer
   >Yes<

If the option is set to Yes, the buzzer of the selected keypad is active during entry/exit time 2.

See “18. Entry/Exit 2” on page 49 for more details.

2.2.1.n.3.20 1+3 keys

20 1+3 keys
   >Yes<

If the option is set to Yes, the combination of 1 and 3 keys allows you to raise a panic alarm.

See Advisor Advanced User Guide for more details.

This functionality is only available for ATS113x keypads.

2.2.1.n.3.21 Schedule

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

See “Schedule shortcut menu” on page 84 for more information.

2.2.1.n.4 Keypad menu

4>Keypad menu
   >>>

The keypad menu provides access to the programming menu built-in to the keypad. For more information, see the appropriate keypad manual.

2.2.1.n.5 Listen-in

1>Listen mode
   Disabled

Use the menu to configure two-way audio for the selected keypad.

This option is only available for systems with two-way audio. See Chapter 3 “System functions > Two-way audio” on page 115 for more details.

2.2.1.n.5.1 Listen mode

1 Listen mode
   >Disabled<

Choose a listening mode for the selected keypad. The following options are available:

- Disabled: No audio.
- Listen only: The central station operator can only listen audio from the audio device assigned to the keypad.
• Listen and speak: The operator can listen audio, or speak using the assigned audio device.

2.2.1.n.5.2 Link audio

Assign an audio device to the selected keypad.

2.2.1.n.6 Delete keypad

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

Note: Before removing a keypad, you should remove any outputs or condition filters connected to the keypad.

2.2.2 Expander devices

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 37.

Expander options

2.2.2.0 Add expander

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

The expander type is an informational screen. The type is set by the expander.
2.2.2.n.2 Expander address

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

2.2.2.n.3 Expander range

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.

See “2.2.2.n.4.6 Expander mode” on page 172 for more details.

2.2.2.n.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

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

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

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

The Input mode option determines the configuration of zone inputs in the expander. This setting is similar to the panel zone input mode, which is described in “8.6.1 Input mode” on page 270.

See “Zone connection” on page 24 for more details on EOL usage.

2.2.2.n.4.5 EOL

The End of line resistor menu allows you to define an end-of-line resistor value for expander zone inputs. This setting is similar to the panel zone input EOL, which is described in “8.6.2 EOL” on page 270.

See “Zone connection” on page 24 for more details on EOL usage.

2.2.2.n.5 Expander menu

The menu provides an access to the programming menu built-in to the expander. For more information, see the appropriate expander manual.

Note: This menu is not available in wireless expanders ATS1235 with firmware version 1.20 and newer.

2.2.2.n.6 Delete expander

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

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

2.2.2.n.4.4 Supervision

1>Short superv.  
20

The supervision is used to disable arming if the wireless expander does not receive a supervision message from a sensor within the short supervision time.

A programmable supervision function checks the state of the devices in the field. The supervision timers in the sensors are “dithered” by a small time so that transmissions occur on a random basis with the effect of minimizing collisions in larger installations.

Notes

• Two- and four-button fobs don’t transmit supervision signals
• Supervision time cannot be set for individual sensors, only for individual wireless expanders

2.2.2.n.4.4.1 Short superv.

1 Short superv.  
>20<

Short supervision is used to disable arming if the wireless expander does not receive a supervision message from a sensor within the short supervision time.

The allowed range is 20 to 1920 minutes.

2.2.2.n.4.4.2 Long superv.

2 Long superv.  
>20<

Long supervision sets an alarm condition in the panel for a sensor which supervision timer expired. Program the supervision time to control how often the wireless expander checks the sensor is communicating and in range of the wireless expander.

The allowed range is 20 to 1920 minutes.

2.2.2.n.4.4.3 Smoke superv.

3 Smoke superv.  
>65<

Smoke supervision sets a fault condition in the panel when a detector supervision timer expired. Program the supervision time to control how often the wireless expander checks that the sensor is communicating and in range of the wireless expander.

The allowed range is 65 to 1920 minutes.
2.2.2.n.4.5 R. Sensitivity

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

Choose one of the following modes for the expander:

- 16 inputs: The expander is fitted with 16 zones.
- 32 inputs: The expander is fitted with 32 zones.

Notes

- 32 inputs mode is only available in the wireless expander with firmware version 1.20 or newer.
- Zones assigned to inputs 17-32 are not adjacent with those assigned to inputs 1-16 of the expander. For example, first 16 inputs are assigned to panel zones 113 to 128, and inputs 17 to 32 are assigned to zones 353 to 368.

2.2.2.n.4.7 Exp version

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

2.2.2.n.4.8 Jamming menu

Use the menu to set the jamming detection options.

2.2.2.n.4.8.1 Jamm detection

The Jamming detection option must be set to Enable if the wireless expander must detect and report communication jamming attempts.
A jamming condition occurs if the jamming is present within any one minute for a longer time period than it is set in “2.2.2.n.4.8.2 Jamming Sec” on page 173. The required jamming threshold is set in “2.2.2.n.4.8.3 Jamm thresh” on page 173.
Note: The above mentioned menus are only available for ATS1235 firmware version V1.20 and newer. In older versions the values are set using the internal expander menu.

2.2.2.n.4.8.2 Jamming Sec

The jamming period can be configured from 10 to 50 seconds. Default value is 30 seconds.

2.2.2.n.4.8.3 Jamm threshold

The jamming threshold can be configured from 25.0 to 75.0%. The default threshold value is 44.8%.

2.2.2.n.4.11 Default expander

Reset the wireless expander to the factory settings.

Camera specific options

2.2.2.n.4.9 Pic options

This menu is specific for systems with wireless PIR camera expanders. See “Using cameras” on page 109 for more details.

2.2.2.n.4.9.1 Pic settings

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 109.

2.2.2.n.4.9.1.1 Burglar settings

1>Pic amount

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

2.2.2.n.4.9.1.1.1 Pic amount

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

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

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 174

2.2.2.n.4.9.2 Show pic mem

| Pictures: 12 |
| Left sp for: 123 |
| Free sp: 3.0MB |
| Total sp: 4.0MB |

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

2.2.2.n.4.9.3 Pic auto deletion

| 3 Pic autodel |
| >1< |

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

The allowed range is 1 to 120 days. 0 or Off mean that pictures are never deleted automatically. Users must control the available memory and remove pictures manually.

2.2.2.n.4.9.4 Total pic cnt

| Total pic cnt: |
| 12 |

The Total picture counter shows how many pictures were stored on the PIR camera expander flash memory since the beginning of its lifetime.

2.2.2.n.4.11 Delete pics

| 11 Delete pics |
| >Cancel< |

Choose OK and press Enter to remove all stored pictures from the wireless PIR camera expander.

Four-door expander specific options

2.2.2.n.4.6 Output modules

| 6 Outp. modules |
| >0< |

Enter the number of output controllers fitted to the door controller.
Allowed range is 0 to 32. 0 means no clocked output card connected. Note that there are four open collector outputs available on the door controller for a 4-way relay card.

### 2.2.2.n.4.7 Region count limit

When the number of users reaches this limit, the door controller sets an internal flag (region count limit) that can be used in the door controller macro logic. You may activate events when a certain number of users are in a region.

The allowed range is 0 to 65534.

Examples:

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

### 2.2.2.n.4.8 Macro Logic

Use the menu to program door controller macros.

For more information on macros, see “Door controller macro logic” on page 76.

#### 2.2.2.n.4.8.0 Add macro

Access the Macro filter menu option to add a macro. If the macro is created successfully, the following message appears:

```
INFO
Macro added
```

The new macro is given the default name “Macro N” and placed on the end of the macro list. You can now start editing its details.

#### 2.2.2.n.4.8.m Select macro

Select an existing macro to program.

#### 2.2.2.n.4.8.m.1 Macro name

The name identifies the macro for installer, making the programming dependencies clearer.
2.2.2.n.4.8.m.2 Formula

1>!Door Open.2
2 OR

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

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

Select the appropriate event to configure it.

1>Group
Door

To choose an appropriate event, you must define the source of the event first. The source is defined by a group of objects, and an object within this group. Available groups are listed in Appendix A, “Advisor Advanced events”, Table 32 on page 349.

When the group and the object (if available) are selected, select the appropriate event. The available selection depends on the selected source. The full event list with sources is shown in Appendix A “Advisor Advanced events”, Table 32 on page 349.

The following functions are available for the selected event:

1. Group: Select group
2. Input flag: Select an input flag from the group above
3. Item: Select an item for the Input flag above
4. Inversion: Invert the selected event. If inverted, it is marked with '!' in the formula

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

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

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

2.2.2.n.4.8.m.3 Macro output

3>Macro output

Configure the output of the selected macro.

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

1 Output func.
   >Non-timed<

Output functions are described in “Door controller macro logic” on page 76.
2.2.2.n.4.8.m.3.2 Duration

2 Duration [s] > <

Provide the duration for the output function from the previous menu. Units are shown in the menu title. The allowed range is 1 to 255.

2.2.2.n.4.8.m.3.3 Activate

1>Group Door

Select the output event the same way as you configure the input event. See “2.2.2.n.4.8.m.2.x Select event” on page 177 for details.

2.2.2.n.4.8.m.4 Delete macro

4 Delete macro >Cancel<

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

2.2.2.n.4.9 Local Devices

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

2.2.3 DC/LC Exp Rdrs

0>Add reader 1 Reader 1

Keypads and readers, connected to one of door controller local buses, can be configured as intelligent system readers to provide access control functions.

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

Note: The maximum number of devices allowed on the databus is given in “General features” on page 37.

Reader options

2.2.3.0 Add reader

Reader number >_<

On the Add reader menu, enter the number for this new reader and press Enter to confirm or Clear to exit without adding a device.

After the device is added, the reader configuration options are shown.
2.2.3.n Select reader
Select the reader number to configure.

2.2.3.n.2 Reader address

2>Reader address
Exp: 1 ADDR: 0

The information screen showing the reader address. The address is set by DIP switches or programmed within the keypad or reader menu.

2.2.3.n.3 Reader options

1>Reader name
Reader 1

The Reader options menu contains the shown below, which are necessary to configure the selected Reader.

2.2.3.n.3.1 Reader name

1 Reader name
>Reader 1<

Use the Reader name option to enter a name that identifies the reader to the end-user.

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

A reader name can consist of 16 characters.

2.2.3.n.3.2 LCD

2 LCD
>Yes<

The LCD option determines whether the selected reader has LCD.

Note: If the door controller recognizes the model of the selected reader, this value will be read-only.

2.2.3.n.5 Delete reader

5 Delete reader
>Cancel<

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

2.2.4 Audio devices

0>Add audio
1 Audio 1

Press 0 to add an audio device, or a number to configure an existing one.
Chapter 5: Menu reference

Note: The maximum number of audio devices allowed is given in “General features” on page 37.

Audio device options

2.2.4.0 Add audio

Enter the number for the new audio device and press Enter to confirm, or Clear to exit without adding a device.

After the device is added, the audio device configuration options are shown.

2.2.4.n Select audio device

Select the audio device number to configure.

2.2.4.n.1 Audio type

The audio device type is an informational screen. The type is set by the device.

2.2.4.n.2 Audio address

The audio device address is an informational screen providing the DIP switch address.

2.2.4.n.3 Audio settings

The menu contains menus shown below, which are necessary to configure the selected audio device.

2.2.4.n.3.1 Audio name

Use the option to enter a name that identifies the audio device to the end-user.

When an audio device is created, it is given the default name “Audio <n>”, where <n> is the audio device address. Enter this menu to edit the current name.

An audio device name can consist of 16 characters.
2.2.4.n.3.2 Tamper area

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

2.2.4.n.3.3 Isolate audio

Use the command to isolate or de-isolate the tamper fault events on the selected device. The device however remains functional when isolated.

2.2.4.n.4 Delete audio

Use the command to remove an audio device. Press Enter, select OK and press Enter again. The device is deleted.
3 User menu

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

3.1 Users

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

Common options

3.1.0 Add user

Access the menu to add users.

Choose manual or sequential mode for user adding.

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

INFO
User added

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

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

Badge the card on the reader programmed in System Options. See “8.8.5 Card learn-in” on page 277 for more details.

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

User 13
Card assigned

Next, you are prompted to badge another card. Press Cancel to exit the sequential user programming and go to the user configuration.
If the card is already used, the error is displayed.

**ERROR**

Card in use

### 3.1.n Select user
Select a user to edit.
The following options can be configured.

#### 3.1.n.1 User name

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

Press Enter to edit the name, or Clear to exit.
The default user name is “User N”, where N is the user number.
The name can have up to 16 characters.

#### 3.1.n.2 PIN

```
1> Change PIN
```>>>
The menu allows changing user PIN as well as setting up the remote user code.

##### 3.1.n.2.1 Change PIN

```
1 PIN
***********
```
Change the selected user PIN.
See “PIN” on page 71 for details on PIN usage.

##### 3.1.n.2.2 Remote PIN

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

**Note:** This submenu is available for installer only. If the option “8.7.8.2 Superv config” on page 275 allows it, the submenu is also available for the supervisor.

See “Remote access” on page 129 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” on page 184.
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” on page 183 for more details.

3.1.n.3 User card

1>Assign card
Card not set

The User card menu lets you assign or delete a user card.
The content of the menu depends whether a card has been already assigned or not.

3.1.n.3.1 Assign card

If the user has no card assigned, the menu lets you enter a user card number.
Press Enter and present the card at the keypad within 10 seconds.

INFO
Badge card

Note: This operation is only possible on LCD keypads with integrated readers.
The keypad for card learning is defined in System Options. See “8.8.5 Card learn-in” on page 277 for more details. If another keypad is defined as a keypad for card learning, the learning keypad name is prompted, for example:

INFO
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.
Chapter 5: Menu reference

The menu contents are similar to the 4 Zones and areas > 4.4 RF fobs menu described on page 211.

3.1.n.5 Language

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

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.

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.

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 189.
3.1.n.9 Select mode

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

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

3.1.n.10 Delete user

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

The display shows:

Choose Ok and press Enter. This removes the user.

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

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

Mobile phone options

3.1.n.7 SMS and Voice

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

3.1.n.7.1 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 288.

This phone number also identifies a sender of an SMS command. See *Advisor Advanced SMS Control Reference Manual* for more information.
3.1.n.7.2 SMS reporting

2 SMS reporting
Off

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

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

This option is editable only if the user belongs to a user group that has the SMS reporting privilege enabled. See “3.2.n.6 User group options” on page 190 for more information.

3.1.n.7.3 SMS control

3 SMS control
Disable

The SMS control menu lets you enable or disable SMS control for the selected user.

This option can be changed only if the user belongs to a user group that has the SMS control privilege enabled. See “3.2.n.6 User group options” on page 190 for more information.

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

Access control options

3.1.n.8 Access options

1>Door group
Not used

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

3.1.n.8.1 Door group

1 Door group
>Not used<

Assign a door group to the selected user.

See Chapter 3 “System functions > Door groups” on page 75 for more information on door groups.
3.1.n.8.2 Trace

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

3.1.n.8.3 Privileged

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

3.1.n.8.4 Extended access

If set to Yes, the selected user has an extended door unlock time granted after badging a valid card or entering PIN. The extended time is set separately for each door. See “5.1.n.5.2 Extended time” on page 219.

3.1.n.8.5 Acc. user type

Defines the type of user for enhanced security.

- Normal: Normal operation.
- Two cards: Requires two valid user codes or cards to be presented to perform any alarm or access control functions.
- Guard: The user code or card can only perform functions when used in conjunction with a visitor code or card.
- Visitor: Requires a code or card from a user who has a Guard user type.
- High security user: only when required number of those users is reached within a high security region, normal users are also permitted to be inside. See “High security” on page 76 for details.
3.2 User groups

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

User group settings

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

INFO
UG added

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

3.2.n Select user group
To edit a user group, select a user group first.

The following options can be configured.

3.2.n.1 User group name
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
Choose a type of the selected user group.

For detailed user group type description and available user group types, see “User group types” on page 66.

3.2.n.3 User group areas
The User group areas option defines which areas the user can control.
3.2.n.4 User group AG

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

3.2.n.5 User group filter

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 238.

3.2.n.6 User group options

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

Available options are listed in “User group options” on page 68.

3.2.n.7 Schedule

Select schedules for the selected user group.

The shortcut menu allows you to assign up to two schedules to each of the following elements:

- 1 Privileges
- 2 Area access

See “Schedule shortcut menu” on page 84 for more information.

3.2.n.8 Remove user group

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

The display shows:

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

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

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

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

4.1 Zone menu

This menu lets you see all programmed zones, select an existing zone, or create a new one.

Each zone can be a physical input on the control panel, an expander, or a plug-in expander, or a wireless device programmed in the wireless expander.

Zone options

4.1.0 Add zone

Use the Add zone menu to add a new zone. When adding a zone, select one of the following options:

- 0 Zone: Add a zone assigned to the specific system input.
- 1 Panel: Add a zone assigned to the specific panel input.
- 2 Panel exp.: Add a zone assigned to the specific panel expander input.
- 3 Exp.: Add a zone assigned to the specific expander input. Select an expander first, and then select an input.
- 4 Auto-detect: Add a zone assigned to the first unused system input.

See "Zone, output, and door addressing" on page 32 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 102.

If the device is a wireless PIR camera, a corresponding camera will be also created in the camera database. See “Using cameras” on page 109.

4.1.n Select zone

Select a zone to program.

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

- “Shock sensor options” on page 203
- “Wireless sensor options” on page 204

Common options

4.1.n.1 Zone name

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

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 47).
4.1.n.3 Isolated

| 3 Isolated | >No< |

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

4.1.n.4 Zone location

| 4>Zone location | Panel 1.1 |

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

4.1.n.5 Zone areas

| 5>Areas | 12..... |

The zone needs an area to be able to send alarm information to the central station, and to be able to reset when an alarm occurs. Use the Areas menu to assign the area to the zone that has to alarm when the zone is activated and the area status (set or unset) meets the requirement for the zone type.

In case multiple areas are selected, the alarm is reported to the lowest area number assigned. The alarm occurs depending on the zone type and only if all assigned areas are set.

The function of the zone depends on the zone type selected during programming.

The screen shows a list of areas that the zone is assigned to. For example, the screen above shows that the zone is assigned to areas 1 and 2.

4.1.n.6 Zone options

| 6>Zone options | >>> |

The Zone options menu contains all zone settings. These settings are described below.

Note: Not all options may be available. The available options depend on the zone type (see “Zone types” on page 47).

4.1.n.6.1 Inhibit

| 1 Inhibit | >Yes< |

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

4.1.n.6.2 Isolate

| 2 Isolate | >Yes< |

If the Isolate option is set to Yes, this zone can be isolated by users.
4.1.n.6.3 Excl. in PS1

When a zone is programmed for excluding while part set (the Exclude in part set option is set to Yes), it is excluded when the assigned area is part set. The normal unset conditions, if relevant, continue to be monitored (tamper, masking, etc). If the Exclude in part set option is set to No, the zone is set in both part set and full set modes.

There are two independent part sets available, PS1 and PS2.

4.1.n.6.4 Excl. in PS2

See “4.1.n.6.3 Excl. in PS1” above.

4.1.n.6.5 Double knock

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 257) 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 257).

Note: If the option is active, the option “4.1.n.6.30 Held open” on page 199 is not available.

4.1.n.6.6 Swinger shunt

If the Swinger shunt option is set to Yes, the number of alarms from this zone is limited to the number set in “8.6.4 Swinger shunt” (see page 271) for one set/unset cycle.

4.1.n.6.7 Anti mask

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 24 for more details.
4.1.n.6.8 Zone pairing

8 Zone pairing
>No<

If the Zone pairing option is set to Yes, this zone is considered as active only when two inputs activate: the assigned (n) and the next to the assigned (n+1).

The zone assigned to the next input (n+1) must exist in the system.

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

4.1.n.6.9 Chime

9 Chime
>Off<

If the Chime option is On, the zone can be switched off and, depending on “8.8.2 Chime menu” setting (see page 277), can activate a short signal on:

• The keypad buzzers on all keypads assigned to the related areas
• The internal siren assigned to the related areas

4.1.n.6.10 Soak test

10 Soak test
>No<

The zone can be set in Soak test mode, which is useful for diagnostic purposes. The zone in soak test does not generate alarms on the system but its activation is logged. This zone is not checked during setting.

4.1.n.6.11 Engineer walk test

11 Eng walk test
>No<

If the Engineer walk test option is set to Yes, the zone is included in the Engineer walk test. See “1.2.5 Walk test” on page 143 for more details.

4.1.n.6.12 User walk test

12 User walk
>Yes<

If the User walk test option is set to Yes, the zone is included in the User walk test. See “1.2.5 Walk test” on page 143 for more details.

4.1.n.6.13 Shock sensor

13 Shock sensor
>No<

The Shock sensor option activates the shock sensor functionality. If this option is set to Yes, the zone operates according to the settings configured in “4.1.n.7 Grs&Pls options” (see page 203).
Only the first eight inputs on the control panel and first eight on the input expander support this option.

### 4.1.n.6.14 Extend EE

14 Extend EE  
> No <

If the Extend EE option is Yes, the zone activation expands the entry time for the value defined by “4.2.n.4.2 Prealarm time” on page 208.  
**Note:** After entry timer times out, local alarm activates.

### 4.1.n.6.15 Final door

15 Final door  
> No <

When the Final door option is set to Yes, the zone has the exit terminator functionality. If the zone is activated during the exit time, the exit timer is terminated after the Final Set delay has expired (see “8.1.3.5 Final set delay” on page 257) and the area is set.

### 4.1.n.6.16 Key latch

16 Key latch  
> No <

If the Key latch option is set to Yes, the key switch zone input is latching. If the zone state is active, the area is set. If the zone changes to normal, the area is unset.

If set to No, the input needs both states to toggle between set and unset (pulse key switch).

### 4.1.n.6.17 Key set

17 Key set  
> Off <

The Key set option defines the zone as a key switch for area set. The following options are available:

- Off: the area set is not affected by the zone.
- Key part set: zone is a key switch for area part set.
- Key full set: zone is a key switch for area full set.

### 4.1.n.6.18 Key unset

18 Key unset  
> No <

If the Key unset option is set to Yes, the zone is a key switch that unsets an area.
4.1.n.6.19 Technical full set

| 19 Tech full set | >No< |

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

4.1.n.6.20 Technical unset

| 20 Tech unset | >No< |

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

4.1.n.6.21 Technical part set

| 21 Tech part set | >No< |

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

4.1.n.6.22 Keypad LCD

| 22 Keypad LCD | >No< |

If the Keypad LCD option is set to Yes, when the zone activates, the zone name is displayed on the keypad LCD on all keypads, related to the area.

4.1.n.6.23 Log

| 23 Log | >No< |

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

4.1.n.6.24 CS report

| 24 CS report | >No< |

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

4.1.n.6.25 Delay timer

| 25 Delay timer | >No< |

A delay timer is activated for this zone if the Delay timer option is set to Yes. The delay timer is set in “8.1.4.4 Input delay” (see page 258).
4.1.n.6.26 ACK on keypad

Acknowledge options are available for keyswitch zone type. They allow you to define a keypad where the particular user is logged in automatically. This causes that an alarm and fault information is displayed instantly on the selected keypad.

The ACK session opens for 2 minutes. During this time you can acknowledge the alarm on the programmed keypad.

**Note:** “4.1.n.6.27 ACK by user” below must be also set for the acknowledgement functionality to work.

4.1.n.6.27 ACK by user

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

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

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

See also “2.2.1.n.3.17 ACK on keypad” on page 166.

4.1.n.6.28 Sensor type

The events reported by a technical zone depend on the type of the sensor connected. The Sensor type option specifies what the sensor is and what events it should report. The following sensor types are available:

- Low temperature detector
- High temperature detector
- Gas detector
- Water detector
- Fire alarm
- Generic

Table 25 below lists events that may be reported for each sensor type.

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>Code</th>
<th>Alarm</th>
<th>Alarm restore</th>
<th>Bypass</th>
<th>Unbypass</th>
<th>Supervision long</th>
<th>Supervision restore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low temp.</td>
<td>SIA</td>
<td>ZA</td>
<td>ZR</td>
<td>ZB</td>
<td>ZU</td>
<td>ZS</td>
<td>ZJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E152</td>
<td>R152</td>
<td>E570</td>
<td>R570</td>
<td>E381</td>
<td>R381</td>
</tr>
<tr>
<td>Sensor Type</td>
<td>Code</td>
<td>Alarm</td>
<td>Alarm restore</td>
<td>Bypass</td>
<td>Unbypass</td>
<td>Supervision long</td>
<td>Supervision restore</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>-------</td>
<td>---------------</td>
<td>--------</td>
<td>----------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Gas</td>
<td>SIA</td>
<td>GA</td>
<td>GR</td>
<td>GB</td>
<td>GU</td>
<td>GS</td>
<td>GJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E151</td>
<td>R151</td>
<td>E570</td>
<td>R570</td>
<td>E381</td>
<td>R381</td>
</tr>
<tr>
<td>High temp.</td>
<td>SIA</td>
<td>KA</td>
<td>KR</td>
<td>KB</td>
<td>KU</td>
<td>KS</td>
<td>KJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E158</td>
<td>R158</td>
<td>E570</td>
<td>R570</td>
<td>E381</td>
<td>R381</td>
</tr>
<tr>
<td>Water</td>
<td>SIA</td>
<td>WA</td>
<td>WR</td>
<td>WB</td>
<td>WU</td>
<td>WS</td>
<td>WJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E154</td>
<td>R154</td>
<td>E570</td>
<td>R570</td>
<td>E381</td>
<td>R381</td>
</tr>
<tr>
<td>Fire</td>
<td>SIA</td>
<td>FA</td>
<td>FR</td>
<td>FB</td>
<td>FU</td>
<td>FT</td>
<td>FJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E110</td>
<td>R110</td>
<td>E570</td>
<td>R570</td>
<td>E373</td>
<td>R373</td>
</tr>
<tr>
<td>Generic</td>
<td>SIA</td>
<td>UA</td>
<td>UR</td>
<td>UB</td>
<td>UU</td>
<td>ZS</td>
<td>ZJ</td>
</tr>
<tr>
<td></td>
<td>CID</td>
<td>E150</td>
<td>R150</td>
<td>E570</td>
<td>R570</td>
<td>E381</td>
<td>R381</td>
</tr>
</tbody>
</table>

See also Appendix B “Advisor Advanced reporting codes” on page 353.

4.1.n.6.29 Virtual zone

1>Outputs
2 Rkp

The menu allows mapping the selected zone to an existing output or a keypad.
If an output or a keypad is not set, the zone state follows the state of the physical input assigned.

- If an output is selected, the zone becomes a virtual zone that is active when the selected output is active. In this case the physical input has no effect on the zone.
- If a keypad is selected, the zone becomes a virtual zone, which is active when the selected keypad has request to exit state (RTE) active.

See also “Outputs” on page 73.

4.1.n.6.30 Held open

30 Held open
> No <

The menu defines if this zone raises a “zone open too long” alarm while held open longer than for a defined period.
The held open period is defined in “8.1.4.6 Held open time” on page 258.

Note: If the option is active, the option “4.1.n.6.5 Double knock” on page 194 is not available.
4.1.n.6.31 EE set check

If set to yes, entry/exit or access zone must be in a normal state when setting the area. Otherwise, the user is not allowed to set premises until the problem is solved.

The option is only available for entry/exit and access type zones.

4.1.n.6.32 Alarm in PS1

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 47.
- The zone must be included into part set 1. See “4.1.n.6.3 Excl. in PS1” on page 194.
- Zone functionality does not change if the same zone belongs to an area in full set state.

4.1.n.6.33 Alarm in PS2

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

4.1.n.6.34 Report as

Defines how panic alarm is reported to central stations.
- Report as panic: PA event is reported.
- Report as duress: HA event is reported.

See Appendix B “Advisor Advanced reporting codes” on page 353 for details.

Notes
- This option is only available for panic type zones. See “Zone types” on page 47.
- 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 276.
4.1.n.6.35 Auto test

35 Auto test
> Yes<

If the option is set to yes, the detector will be tested automatically when auto test is active. See also “1.2.1.8 Detector test” on page 140.

4.1.n.6.36 Shunt

36 Shunt
> Yes<

If the option is set to Yes, the zone can be shunted.
See “Zone shunt” on page 56 for details.

4.1.n.6.37 View isolated

37 View isolated
> On<

If the option is set to On, users are warned about this zone being isolated when attempting to set or unset the appropriate area.

4.1.n.6.38 Stop report

38 Stop report
> No<

If the option is set to Yes, zone activation stops voice reporting, if active.
This option is only available for keyswitch type zones.

4.1.n.6.39 Limit reports

39 Limit reports
> Off<

If the option is set to On, the reporting from the zone is limited with the time frame defined in “8.6.6 Limit reports” on page 271.

4.1.n.8 Listen-in

1>Listen mode
Disabled

Use the menu to configure two-way audio for the selected zone.
This option is only available for systems with two-way audio. See Chapter 3 “System functions > Two-way audio” on page 115 for more details.
4.1.n.8.1 Listen mode

Choose a listening mode for the selected zone. The following options are available:

- **Disabled**: No audio.
- **Listen only**: The central station operator can only listen audio from the audio device assigned to the zone.
- **Listen and speak**: The operator can listen audio, or speak using the assigned audio device.

4.1.n.8.2 Link audio

Assign an audio device to the selected zone.

4.1.n.9 Copy

Use Copy menu to copy zone parameters.

The following copy methods are available.

4.1.n.9.1 Copy par. from

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.9.2 Block assign

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 204 for more details.

4.1.n.10 Move zone

<table>
<thead>
<tr>
<th>Zone</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>004</td>
<td>Not used</td>
</tr>
<tr>
<td>009</td>
<td>Not used</td>
</tr>
</tbody>
</table>

Allows you to move the selected zone to other available zone number.

This option is only available in a flexible zone numbering scheme. See “8.7.9 Object scheme” on page 276 for details.

See also “Zone, output, and door addressing” on page 32.

4.1.n.11 Delete zone

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete zone</td>
</tr>
<tr>
<td>&gt;Cancel&lt;</td>
</tr>
</tbody>
</table>

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 106 for more details.

Shock sensor options

4.1.n.7 Grs&Pls options

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>7&gt;Grs&amp;Pls opts</td>
</tr>
<tr>
<td>&gt;&gt;&gt;</td>
</tr>
</tbody>
</table>

The Gross and Pulse options are valid if the “4.1.n.6.13 Shock sensor” functionality (see page 195) for this zone is set to Yes.

4.1.n.7.1 Pulse count

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&gt;Pulse count</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

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

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 141).

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 1.20 or newer, which is online.

4.1.n.7.1 Sensor ID

The screen allows you to view the sensor ID.

Note: First two digits of the sensor identifier also define the sensor type. See Table 26 below.

4.1.n.7.2 Sensor type

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

Table 26: Wireless sensor types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeater</td>
<td>Wireless signal repeater</td>
<td>0A*</td>
</tr>
<tr>
<td>CO</td>
<td>Carbon monoxide sensor</td>
<td>0D*</td>
</tr>
<tr>
<td>DWS</td>
<td>Door/Window sensor</td>
<td>10*</td>
</tr>
<tr>
<td>Smoke sensor</td>
<td>Smoke sensor</td>
<td>11*</td>
</tr>
<tr>
<td>PIR</td>
<td>Passive infrared detector</td>
<td>12*</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td>ID</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------</td>
<td>----</td>
</tr>
<tr>
<td>2 button panic</td>
<td>2 button panic sensor</td>
<td>14*</td>
</tr>
<tr>
<td>Shock sensor</td>
<td>Shock sensor</td>
<td>18*</td>
</tr>
<tr>
<td>Sound sensor</td>
<td>Glass break sound sensor</td>
<td>1A*</td>
</tr>
<tr>
<td>PIR camera sensor</td>
<td>Wireless PIR camera</td>
<td>23*</td>
</tr>
</tbody>
</table>

### 4.1.n.7.3 Sensor mode

<table>
<thead>
<tr>
<th>Sensor mode</th>
<th>Single</th>
</tr>
</thead>
</table>

The informational screen allows you to see if the sensor operates in two-zone mode. The following values are available:

- Single: Single zone sensor.
- Master: The selected zone is the first zone of a two-zone sensor.
- Slave: The selected zone is the second zone of a two-zone sensor.

See “Two-zone RF sensors” on page 106 for more details.

### 4.1.n.7.4 Supervision

<table>
<thead>
<tr>
<th>Supervision</th>
<th>Off</th>
</tr>
</thead>
</table>

Enables or disables the wireless device supervision. Supervision of all types becomes active. See “2.2.2.n.4.4 Supervision” on page 171 for more details.

### 4.1.n.7.5 Sensor opt

<table>
<thead>
<tr>
<th>Sensor opt</th>
<th>Ignore alarm</th>
</tr>
</thead>
</table>

Sensor options depend on the type of the wireless device.

See an appropriate RF device manual for more information on available options.

The following options may be available.

#### Table 27: Wireless sensor options

<table>
<thead>
<tr>
<th>Option</th>
<th>Sensor type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reed and contact</td>
<td>Door/window sensor</td>
<td>Report alarms from both sources</td>
</tr>
<tr>
<td>Contact</td>
<td>Door/window sensor</td>
<td>Ignore reed alarms</td>
</tr>
<tr>
<td>Reed and shock</td>
<td>Shock sensor</td>
<td>Report alarms from both sources</td>
</tr>
<tr>
<td>Shock sensor</td>
<td>Shock sensor</td>
<td>Ignore reed alarms</td>
</tr>
<tr>
<td>Reed</td>
<td>Door/window sensor, shock sensor</td>
<td>Only report reed alarms</td>
</tr>
<tr>
<td>Notice tamper</td>
<td>Smoke sensor</td>
<td>Control housing tamper alarms</td>
</tr>
<tr>
<td>Ignore tamper</td>
<td>Smoke sensor</td>
<td>Ignore housing tamper alarms</td>
</tr>
</tbody>
</table>
4.1.n.7.6 Remove RF dev

Remove RF dev?
>Cancel<

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

4.2 Areas

1 Area 1
2 Area 2

The Area menu allows you to configure areas.

See “Areas” on page 52 in Chapter 3 “System functions” for details.

Each area can be programmed with a number of options, like the area name, entry and exit times etc. Before going any further, select the area to program.

Area options

4.2.n Select area

1 Area name

Select an area to program.

4.2.n.1 Area name

1 Area name
>Area 1 <

Every area can be programmed with a name to identify the area.

Use the Area name screen to enter or edit the area name. The area name can contain up to 16 characters.

4.2.n.2 Exit time

2 Exit time 1
> <

Every area has its own exit timers. Exit timers allow users that set an area, to leave the premises without generating an alarm (using access or entry/exit zones). Only after the exit timers have expired can an alarm occur.

Each area can be programmed with two exit times, one for entry/exit 1 zone type, another one for entry/exit 2 zone. Select an appropriate timer and set the time.

The exit timers can be programmed from 0 to 255 seconds. 0 means the timer is not engaged and the area is set immediately. 255 means the timer remains active and requires an exit terminator (see “4.1.n.2 Zone type” on page 192) or a
zone with the final door option (see “4.1.n.6.15 Final door” on page 196) to complete.

**Note:** If zones are assigned to more than one area, the longest exit time is used. See “4 Zones and areas” on page 191.

### 4.2.n.2.1 Exit time 1

### 4.2.n.2.2 Exit time 2

Configure exit timers for entry/exit 1 and entry/exit 2 zone types. See “4.2.n.2 Exit time” on page 206 for details on exit timer programming.

### 4.2.n.2.3 PS Exit time 1

### 4.2.n.2.4 PS Exit time 2

Configure part set exit timers for entry/exit 1 and entry/exit 2 zone types. Part set exit timers are configured the same way as full set exit timers. See “4.2.n.2 Exit time” on page 206 for details on exit timer programming.

### 4.2.n.3 Entry time

| 3 Entry time 1 | > | < |

Every area has its own entry timer. When entering the premises via an entry/exit zone, the entry time starts. A user can unset the area while the entry time is running without generating an alarm provided only entry/exit zones or access zones are activated.

**Note:** The entry time can be extended for particular entry zones. See “4.2.n.4.2 Prealarm time” on page 208 for more details.

Each area can be programmed with two entry times, one for entry/exit 1 zone type, another one for entry/exit 2 zone. Select an appropriate timer and set the time.

The entry timers can be programmed from 0 to 255 seconds. 0 means the timer is not engaged and the alarm is activated immediately when entering the armed premises. 255 and more means the time is infinite.

**Note:** If zones are assigned to more than one area, the longest entry and exit time is used. See “4 Zones and areas” on page 191.

### 4.2.n.3.1 Entry time 1

### 4.2.n.3.2 Entry time 2

Configure entry timers for entry/exit 1 and entry/exit 2 zone types. See “4.2.n.3 Entry time” above for details on entry timer programming.
4.2.n.3.3 PS Entry time 1

4.2.n.3.4 PS Entry time 2
Configure part set entry timers for entry/exit 1 and entry/exit 2 zone types.
Part set entry timers are configured the same way as full set entry timers. See “4.2.n.3 Entry time” on page 207 for details on entry timer programming.

4.2.n.4 Other timers

1>Warning time

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

4.2.n.4.1 Warning time

1 Warning time

> <
Warning time is a period of time during which the automatic set procedure can be postponed. After the warning time expires, the system is set.
The set postponing must be allowed in “4.2.n.5.2 Set retry” on page 209.
The warning timer can be programmed from 1 to 15 minutes.

4.2.n.4.2 Prealarm time

2 Prealarm time

> <
Every area has its own prealarm timer. When an alarm is triggered, it only generates a local alarm, and the prealarm timer is started. If the local alarm is not acknowledged during the prealarm time, the alarm is reported.

Note: The entry zone must have activated option “4.1.n.6.14 Extend EE” described on page 196.

Use the PreAlarm time screen to set the prealarm time for the area. Each area can be programmed with one prealarm time.
The prealarm timers can be programmed from 0 to 255 seconds.

Note: If zones are assigned to more than one area, the longest prealarm time is used. See “4 Zones and areas” on page 191.

4.2.n.4.3 Unset delay

3 Unset delay

> <
Set a delay for authorized unset (in minutes). The allowed range is 1 to 30 min. 0 means that no delay is applied. See “Delayed unset” on page 55 for more details.
4.2.n.5 Set/unset options

1>Entry alarms
   Delayed

The menu groups the following setting options.

4.2.n.5.1 Entry alarms

1 Entry alarms
   >Delayed<

The Entry alarms option defines whether the entry fail alarm is reported immediately. The following values are applicable:

- Delayed: The alarm activates 30 s after the entry time passed.
- Instant: The alarm activates immediately.

4.2.n.5.2 Set retry

2 Set retry
   >Off<

Set retry defines whether users can postpone or cancel an autoset. If this option is set to On, you can postpone autoset during the Warning time (see “4.2.n.4.1 Warning time” on page 208). If the autoset has been postponed by a normal user, the system will attempt autoset again after a time period defined in “8.4.8 AS user retry” on page 267.

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

4.2.n.5.3 Silent autoset

3 Silent autoset
   >Off<

If Silent autoset is on, the keypad buzzer remains silent during the “4.2.n.4.1 Warning time” described on page 208.

4.2.n.5.4 Dual unset

4 Dual unset
   >Off<

If the option is set to yes, two valid user authorization is necessary to unset the area.

Note: The users must authorize on the same keypad.

Caution: Before switching this option on, or applying defaults that have this option enabled, add at least one user, otherwise you will lose an access to the programming menu. See also “Recovery procedure” on page 322 in Chapter 7 “Troubleshooting”.
4.2.n.6 Hierarchy

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

See “Area hierarchy” on page 52 for more details.

4.2.n.7 Limits

Limits the number of system elements that can be isolated or inhibited at any one time.

Allowed ranges depend on the panel variant. See “General features” on page 37 in Chapter 2 “Installation”.

See also “Inhibit and isolate” on page 56.

4.2.n.7.1 Inhibit limit

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

4.2.n.7.2 Isolate limit

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

4.2.n.7.3 Shunt limit

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

4.2.n.8 Schedule

Select schedules for the selected area.

The shortcut menu allows you to assign up to two schedules to each of the following elements:

- 1 Set
- 2 Shunt
- 3 Prohibit unset
- 4 Chime area

See “Schedule shortcut menu” on page 84 for more information.
4.3 Area groups

Area group menu allows you to assign areas to area groups.

Note: Area group availability depends on the control panel variant. See “Specifications” on page 36 in Chapter 2 “Installation”.

Area group options

4.3.n Select area group

Select an area group to program.

4.3.n.1 AG name

Every area group can be programmed with a name to identify the area. Use the Area group name screen to enter or edit the area group name. The area group name can contain up to 16 characters.

4.3.n.2 Areas

Assign areas to the selected area group.

4.4 RF fobs

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

Fob options

4.4.0 Add fob

To add a fob, follow one of the procedures described in “Wireless device programming” on page 102.
4.4.n Select fob

Select an existing fob to program.

4.4.n.1 Fob name

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

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

A fob name can consist of 16 characters.

4.4.n.2 Assigned user

Assign an existing user to the selected fob.

Note: One user can have a few fobs assigned. However, one fob can be assigned only to one user.

4.4.n.3 Buttons

Use the Buttons menu to assign an appropriate function to a button or a button combination.

Note: A user must be assigned in “4.4.n.2 Assigned user” above for the button combinations to work.

Table 28 below lists buttons and combinations that are available.

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button 1</td>
<td>Set all areas</td>
</tr>
<tr>
<td>Button 2</td>
<td>Unset all areas</td>
</tr>
<tr>
<td>Button 3</td>
<td>Part set 1 all areas</td>
</tr>
<tr>
<td>Button 4</td>
<td>Toggle trigger 99</td>
</tr>
<tr>
<td>Buttons 1 + 2</td>
<td>—</td>
</tr>
<tr>
<td>Buttons 1 + 3</td>
<td>—</td>
</tr>
<tr>
<td>Buttons 1 + 4</td>
<td>—</td>
</tr>
</tbody>
</table>
4.4.n.3.1 Select button

Select a button to assign a user function to it. See “User programmable functions” on page 97 for more details.

4.4.n.4 RF details

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

4.4.n.4.1 Sensor ID

The screen allows you to view the sensor ID.

4.4.n.4.2 Remove RF dev

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

4.4.n.5 Listen-in

Use the menu to configure two-way audio for the selected fob.

This option is only available for systems with two-way audio. See Chapter 3 “System functions > Two-way audio” on page 115 for more details.

4.4.n.5.1 Listen mode

Choose a listening mode for the selected fob. The following options are available:
- Disabled: No audio.
• Listen only: The central station operator can only listen audio from the audio device assigned to the fob.
• Listen and speak: The operator can listen audio, or speak using the assigned audio device.

4.4.n.5.2 Link audio

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 None</td>
<td></td>
</tr>
<tr>
<td>1 Audio 1</td>
<td></td>
</tr>
</tbody>
</table>

Assign an audio device to the selected fob.

4.4.n.6 Remove fob

Remove fob?
>Cancel<

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

4.5 Cameras

17>Camera 17
18 Camera 18

The menu allows you to configure camera modules in wireless PIR cameras. For more details on cameras, see also “Using cameras” on page 109.

4.5.n Select camera

1>Camera name
Camera 17

Select an appropriate camera to configure.

4.5.n.1 Camera name

1 Camera name
>Camera 17<

Enter camera name.

4.5.n.2 Pics by zone

1>Zone 17
2 Zone 2

Choose 1 to 4 zones that can trigger the camera when active.

By default, the first zone assigned is the zone with PIR detector of this wireless PIR camera.

Choose a zone position to assign a zone, or an existing zone to remove it from the associated zone list.
4.5.n.3 Pics by filter

Additionally to the zones listed in “4.5.n.2 Pics by zone” on page 214, there can be up to two condition filters that also trigger the camera.

4.5.n.3.m Select filter

Select one of two filters to configure.

4.5.n.3.m.1 Choose filter

Choose a filter that activates the selected camera.

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

Define a type of the condition filter chosen in “4.5.n.3.m Select filter” above. The available filter types are listed in “Camera event types” on page 109.

4.5.n.3.m.3 Report as

If the filter has a custom type, it is necessary to assign a reporting event, which occurs when the filter becomes active.

Notes

- After you leave this menu, the event is shown as a reporting code in SIA format. See Appendix B “Advisor Advanced reporting codes” on page 353 for details.
- Only particular reporting events are available.

4.5.n.4 Pics by rep ev

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

4.5.n.4.m Select event

Select one of two reporting events to configure.
Choose an event that activates the selected camera.

**Notes**

- After you leave this menu, the event is shown as a reporting code in SIA format. See Appendix B “Advisor Advanced reporting codes” on page 353 for details.
- Only particular reporting events are available.

**4.5.n.5 Isolated**

5 Isolated  
> No <

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

**4.5.n.6 Max pics 24h**

6 Max pics 24h  
> Infinity <

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

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

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

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

**4.5.n.7 Remote pics**

7 Remote pics  
> Yes <

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

**4.5.n.8 Test pic to CS**

1> CS 1

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

Choose a central station to send the picture.

Calling CS 1...
Transmitting

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

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

5.1 Doors

Use the Door menu to add, edit, or delete doors.

The menu allows you to configure doors of both types, standard and intelligent.

**Note:** Particular options in this menu are specific for different door types. For specific options, see:
- “Standard door specific options” on page 225
- “Intelligent door specific options” on page 225

Common door options

5.1.0 Add door

Access the Add door menu option to add a door.

Choose one of the following locations:
- 0: Door. Add a door providing the system address of this door. If the address is valid, the panel displays the physical door location to confirm.
  
  Exp 3.2
  >OK<

  Select OK to confirm, or Cancel to exit, and then press Enter.
- 1: Panel. Add a standard door providing its number on the control panel.
- 2: DC/LC Exp. Add an intelligent door selecting the door controller, and entering a number of the door on this door controller.

If the door is created successfully, the following message appears:
The new door is given the default name “Door N” and placed on the end of the
door list. You can now start editing the door details for the new door.

For reader, door zone and lock outputs default addressing, see “Zone, output,
and door addressing” on page 32 in Chapter 2 “Installation”.

5.1.n Select door

Select a door to edit.

The following options can be viewed or configured.

5.1.n.1 Door name

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

The default door name is “Door N”, where N is the door number.

The name can have up to 16 characters.

5.1.n.2 Door location

The read-only screen that shows the physical door location of the selected door.

The door location is shown in the same format as zone location. See “4.1.n.4
Zone location” on page 193.

5.1.n.3 Door readers

The menu allows you to assign entry (IN) and exit (OUT) readers to the selected
door.

Note: Standard doors can only have one IN reader and one OUT reader.
Additional door readers can be only assigned to an intelligent door. For options
related to intelligent doors, see “Intelligent door specific options” on page 225.

The following submenus are available for all doors:

• 1 Reader IN: Select an entry reader
• 2 Reader OUT: Select an exit reader

The following submenus are available only for intelligent doors:

• 3 Reader IN 2: Select an additional entry reader
• 4 Reader OUT 2: Select an additional exit reader
5.1.n.4 Door output

Select unlock door output.

For intelligent doors, the output must belong to the appropriate door controller outputs range.

You can also select an output that cannot be directly controlled from the Advisor Advanced system. See “8.5.2.1 Map relays” on page 269 for details.

You cannot select outputs that are already assigned to Forced door, Warning, DOTL or other output.

It is recommended to use one of first four door controller outputs for door unlock.

5.1.n.5 Door timers

Use the menu to configure various timers for the selected door.

Note: For standard doors, the timer value is set in minutes and seconds in mm:ss format, for example, 01’30.

In case of intelligent doors, use two options placed as submenus:

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

5.1.n.5.1 Unlock time

Program the amount of time (value and units) for the door to unlock when a user enters a valid card or PIN at the door reader.

5.1.n.5.2 Extended time

Program the amount of time (value and units) for the door to unlock when a user, with the "Extended access" option enabled, presents a valid card or PIN at the door reader. See also “3.1.n.8.4 Extended access” on page 188.

5.1.n.6 Door options

The menu contains various options for the selected door.

For options related to intelligent doors, see “Intelligent door specific options” on page 225.
5.1.n.6.1 Door zones

Use the menu to assign required zones to the selected door.
In case of standard door, there can be only one door zone indicating door opening.

Note: It is not possible to assign a zone to a particular door function if this zone is already used for other door function. Only unassigned zones are displayed.

5.1.n.6.1.1 Door zone

Select a zone with door contact for the selected door.

5.1.n.6.3 Alarm control

Set alarm control options for the selected door.

5.1.n.6.3.1 Door areas

Select door areas.
In case of an intelligent door, the areas specified here are used for:
• The reader LEDs if the option “5.1.n.3.5.5 LEDs option” described on page 227 is selected to show area status.
• “5.1.n.6.3.4.1 Deny access” when set (described on page 221).
• Option “5.1.n.6.4.3 Dis. when set” on page 230 is set to Yes for IN readers.

Although the areas are not used for area control, the door controller does need to identify the status of these areas to know whether to send an arm or disarm command to the control panel. This is only when using cards by themselves for set/unset, for example, alarm control on 1st or 3rd badge. Remember that the User group determines the areas allowed to be set or unset by a user, not the areas listed here. See also “User groups” on page 66.

See “How to edit a list” on page 126 for details on the area selection.

Note: “2.2.1.n.3.3 View areas” on page 161 and “2.2.1.n.3.5 Control areas” on page 162 are not available for keypads that are configured as door readers.
5.1.n.6.3.2 Door AGs

Select door area groups in the same way as areas in “5.1.n.6.3.1 Door areas” on page 220.

5.1.n.6.3.3 When unset

Define the door functionality when the assigned areas are unset.

5.1.n.6.3.3.1 Low Security

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

5.1.n.6.3.3.2 Unlock Door

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

5.1.n.6.3.4 When set

Define the door functionality when the assigned areas are set.

5.1.n.6.3.4.1 Deny access

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

5.1.n.6.3.4.2 Lock door

If set to Yes, the door is locked when all door areas are set.
5.1.n.6.3.4.3 EE PIN lock

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

The option is equal to “2.2.1 Keypad devices > 2.2.1.n.3.8 EE PIN lock” on page 164.

5.1.n.6.4 RTE options

Configure RTE (Request to exit) functionality options.

5.1.n.6.4.1 Use reader RTE

Specify if the Request To Exit input is enabled on the reader.

First, select the appropriate IN or OUT reader. Next, set Yes or No to configure the option for the specified reader.

For options related to intelligent doors, see “Intelligent door specific options” on page 225.

5.1.n.7 Schedule opts

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

5.1.n.7.1 Door unlocked

Configure schedule options for the door unlock.

5.1.n.7.1.1 Schedule

Select schedules for the door unlock.

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

See “Schedule shortcut menu” on page 84 for more information.

5.1.n.8 Shunt options

Use the menu to set up door shunt options for the door.
See also “Door shunt” on page 75 in Chapter 3 “System functions” for shunt functionality description.

For options specific for standard doors, see “Standard door specific options” on page 225. For options related to intelligent doors, see “Intelligent door specific options” on page 225.

5.1.n.8.2 Shunt timers

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

**Note:** For standard doors, the timer value is set in minutes and seconds in mm'ss format, for example, 01'30.

In case of intelligent doors, use two options as submenus:

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

**5.1.n.8.2.1 Shunt time**

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

**5.1.n.8.2.2 Extended time**

The extended shunt timer, which is applied if the user has extended time option enabled. See “3.1.n.8.4 Extended access” on page 188 for details.

**5.1.n.8.2.3 Warning time**

The warning time is the time period of door shunt warning before shunt time (or extended shunt time) expires.

Appropriate warning event flags, which are active during this time, can be used for in user programmable function. See also “User programmable functions” on page 97, “Zone shunt” on page 56.

**5.1.n.8.3 Shunt type**

The menu contains parameters that define the effect of the shunt.
For options specific for standard doors, see “Standard door specific options” on page 225.

### 5.1.n.8.3.1 Shunting

**1 Shunting**

>Zone shunting<

The option defines the object of the shunt. The following options are available:

- **No shunting.** The door is not shunted.

- **Zone shunting.** The door is shunted. It generates a standard alarm, based on the zone type settings, if left open longer than the programmed shunt time. See “5.1.n.8.2.1 Shunt time” on page 223.

- **Zone shunting & DOTL.** The door is shunted and generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time. Enables Forced Door and DOTL to be reported on separate zone numbers as programmed in “5.1.n.6.5.4 Forced door” on page 231 and “5.1.n.6.5.5 DOTL” on page 231.

  **Note:** This option is only available for intelligent doors.

- **Auto shunting & DOTL.** If the area assigned to the door is unset, shunting of the door commences when the door zone is active (no code or card required). A DOTL (Door Open Too Long) alarm is generated if it is left open longer than the programmed shunt time. Forced Door and DOTL are reported on separate zone numbers as above.

  **Note:** This option is only available for intelligent doors.

### 5.1.n.10 Move Door

**5 Not used**

**6 Not used**

The menu allows you to move the selected door to another physical location. The new location must be unused.

If the door is moved successfully, the following message appears:

**INFO**

Door moved

**Note:** The door name is changed only if it set by default, for example, Door 5 becomes Door 17. If the door has a custom name, it does not change.

This option is only available in a flexible numbering scheme. See “8.7.9 Object scheme” on page 276 for details.

See also “Zone, output, and door addressing” on page 32.
5.1.n.11 Delete door

12 Delete door
   >Cancel<

Use the Delete door command to remove the door from the system. To remove the door, select Ok and press Enter. The door is deleted.

Standard door specific options

5.1.n.8.3.2 Shunt active

2 Shunt active
   >Always<

Allows you to choose system status when the door shunt is activated.

- **Always**: The door shunt activates in every system state.
- **Set**: The door shunt is active only if the areas with the selected door are set.
- **Unset**: The door shunt is active only if the areas with the selected door are unset, or set partially.

5.1.n.8.4 Indication

1>Door held open
   No

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

5.1.n.8.4.1 Door held open

1 Door held open
   >No<

If the option is set to yes, the keypad emits an intermittent signal when the door is held open longer than the shunt timer (or extended shunt timer) allows it.

5.1.n.8.8 EE Shunt

8 EE Shunt
   >No<

If entry/exit shunt is set to E/E 1 or E/E 2, the shunted zone becomes an entry/exit zone, and door shunt starts the entry/exit 1 timer (or entry/exit 2 timer).

Intelligent door specific options

5.1.n.3.5 Readers opts

1>Card and PIN
   >>>

Use the menu to configure readers of the selected door.
5.1.n.3.5.1 Card and PIN

Specify what method is required to open the door from the selected reader.

- **Yes**: Unlock the door by presenting a valid card to the reader and entering a PIN on the reader's keypad.
- **No**: Unlock the door by presenting a valid card to the reader or a valid PIN on the reader’s keypad.

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

5.1.n.3.5.2 Two cards

Defines if two user cards or PINs are required to gain access. If set to yes, two different users need to present their card and/or PIN within the programmed time for the door to unlock.

The time is set in “8.5.1.2 Two cards” on page 268.

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

5.1.n.3.5.3 NoSchedule req

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

- **Yes**: The user has an access to the door from the OUT reader side even if his schedule has already expired. But he must have assigned any schedule for the door in his door group — users without schedule do not have an access to the door.
- **No**: Valid schedule is required for the user to exit.

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

5.1.n.3.5.4 Card format

Set the data format of the reader and card, key or token being used.

- Wiegand 27 bit
- 27-bit Tecom ASP
- K 32 bit
- Wiegand 26 bit (ID=16, FC=8)
• Indala ASC 27 bit
• Indala ASC 26 bit
• Wiegand 32 bit
• C 36 bit
• ATS Wiegand 23 bit
• ATS Wiegand 23 bit
• Mag swipe - Aritech format
• Mag swipe - Midas format

5.1.n.3.5.5 LEDs option

5 LEDs option

>Door locked<

Specifies the status that the reader LEDs indicate (only applicable for door controller readers connected to Wiegand interface).

• Door locked. LED 1 is on when the door is locked.
• Door unlocked. LED 1 is on when the door is unlocked.
• Area set. LED 1 indicates if the area assigned to the door is set. If more than one area is assigned, all areas assigned to the door must be set before LED changes state.
• Area unset. LED 1 indicates if the area assigned to the door is unset. If more than one area is assigned, all areas assigned to the door must be unset before LED changes state.
• Area set/unset. Readers with dual LED control indicate the area unset and set with different LED colours.
• Valid/Void. Readers with dual LED control indicate User Valid or Void using different LED colours.
• LEDs disabled. No LED control.

Note: On readers with dual LED control, LED 2 may also be programmed to indicate other conditions using door controller macro logic programming. See “Door controller macro logic” on page 76.

See also “5.1.n.6.3.1 Door areas” on page 220.

5.1.n.3.5.6 Time&Attendance

6 Time&Attendance

>No<

If set to Yes, the reader function as a time and attendance reader. It causes that user access events occurring on this reader are sent from the door controller to the control panel and may be used for user attendance control.
5.1.n.3.5.7 Disable Duress

7 Disable Duress
   >No<

This option is used to disable duress codes from functioning. If set to Yes, no duress function is available at this door.

5.1.n.6.1.2 Second zone

0>No
17 Zone 17

The door controller allows the system to monitor two door contacts for a single intelligent door. Select a second zone with door contact for the selected door. If there is only one door contact, select No.

See also “5.1.n.6.1.1 Door zone” on page 220.

5.1.n.6.1.3 DOTL zone

0>Not used
17 Zone 17

Specify the zone that reports the DOTL (door open to long) alarm condition for the selected door.

Note: DOTL reporting must be enabled in Shunt options. See “5.1.n.6.5.5 DOTL” on page 231.

5.1.n.6.2 Door unlocked

1>Lock when CL
   No

The menu contains various options for the selected door unlocking process.

5.1.n.6.2.1 Until closed

1 Until closed
   >No<

This option determines when the door will re-lock using the re-lock delay.

• Yes: The door lock will not re-lock until the door is closed. This is used where the lock mechanism, when locked, will stop the door closing.
• No: The door lock will re-lock (after the unlock time has expired, etc.) regardless of the door being open or closed.

5.1.n.6.2.2 Until opened

2 Until opened
   >No<

For security reasons, it is possible for the door to re-lock at the moment it opens. The door stays unlocked until opened, and the door relay is deactivated after the door opens.
The door remains unlocked as long as the unlock time is counting, or the door stays closed, whichever is longer. See also “5.1.n.5.1 Unlock time” on page 219.

5.1.n.6.2.3 Pulsed L&UnL

This function is only used on special electronic locks that require two separate relays to be pulsed at different times for it to open, and two separate zones for monitoring. If this function is set to Yes, then normal lock-strike opening is disabled. This option should always be set to No unless otherwise specified.

The functionality is described in details in Chapter 3 “System functions > Pulsed lock and unlock” on page 77.

5.1.n.6.3.5 User group

Select a user group for the selected door.

See “User groups” on page 66 for details.

5.1.n.6.3.6 Control type

Specify what type of alarm control is available for the selected door.

- No control: Reader has no alarm control. It is not possible to set or unset areas using the readers.
- On 1st badge: Presentation of a valid card at a door reader will unset the areas in the user group on first badge. Badging three times will set the areas.
- On 3rd badge: Presentations of a valid card three times sets or unsets the areas in the user group.
- Always: Presentation of a valid card at the IN reader unsets the areas in the user group. Presentation of a valid card at the OUT reader arms the areas in the user group.

5.1.n.6.3.7 If PIN sets

Configure the door operation if the area is set using PIN.

5.1.n.6.3.7.1 Deny access

If set to Yes, the access to the door is denied if the areas were set using PIN.
5.1.n.6.4.2 RTE zone

Select a zone operating as an RTE input for an intelligent door.

**Note:** It is not possible to choose a zone, which is already used in the door controller (for example, DOTL or door zone, etc.)

See also “5.1.n.6.4 RTE options” on page 222.

5.1.n.6.4.3 Dis. when set

Specify if the RTE functionality is disabled if any of door areas are set.

First, select the appropriate IN or OUT reader. Next, set Yes or No to configure the option for the specified reader.

5.1.n.6.4.4 RTE Control

Defines the operation of the Request To Exit button.

- Timed door open. When the RTE button is pressed, the door unlocks for the programmed unlock time. See “5.1.n.5.1 Unlock time” on page 219.
- Hold door open. Allows the door to be held unlocked for as long as the RTE button is pressed or for the programmed unlock time, whichever is longer.
- Shunt only. When the RTE button is pressed, the zone is shunted, but no access is granted.

5.1.n.6.5 Reporting

Determines when access control events are reported.

5.1.n.6.5.1 CL & Locked

If set to yes, the door is reported when closed and locked (lock command sent, and zone status is normal).

**Note:** There is no event specified in the control panel. This function can only be used in conjunction with next options.
5.1.n.6.5.2 OP&Unl as Unl

| 2 OP&Unl as Unl | >No< |

If set to yes, the door is reported as unlocked, if it is open and unlocked.

5.1.n.6.5.3 Open/Close

| 3 Open/Close | >No< |

If set to yes, opening or closing door is reported. Otherwise there is no reporting unless an alarm occurs (depending on the zone type).

5.1.n.6.5.4 Forced door

| 4 Forced door | >No< |

If set to Yes, opening of the door without a valid card, PIN or Request To Exit is reported.

5.1.n.6.5.5 DOTL

| 5 DOTL | >No< |

Report when the door is open too long. If set to Yes and the zone assigned to the door is in the DOTL state (for example, still open after the shunt timer expires), the DOTL event is reported.

5.1.n.6.5.6 RTE

| 6 RTE | >No< |

If set to Yes, Request To Exit zone activation is reported.

5.1.n.6.6 Interlocking

| 6 Interlocking | 1234567890123456 |

This menu stipulates the zone numbers on the door controller that prevents the doors being accessed at the same time. Numbers must be zone numbers on the same door controller.

To interlock with a door on another door controller, a contact from that door must be wired to a spare zone on the first door controller, and vice versa. In this case, if a zone is being used for interlocking and no door on the door controller has that zone as its “Door Contact”, then the door controller automatically inserts a 2 second delay before a door opens. This is to allow for settling times across the door controllers. Please remember that this two-second delay only occurs when a zone is being used for interlocking, and that zone comes from another door not on this door controller.
To activate or deactivate interlocking, toggle a local zone number.

5.1.n.7.1.2 After entry

Select if the override takes effect immediately after the schedule commences, or after a user has entered.

- Yes: Before the schedule will unlock the door, a user needs to enter the area.
- No: Automatic unlock starts at the schedule start time.

See also “5.1.n.7.1 Door unlocked” on page 222.

5.1.n.7.2 Low Security

Use the menu to configure Low Security functionality of the door. The door low security mode means that the user authorization is changed from Card and PIN to Card or PIN.

The following submenus are available:

- 1 Schedule. Select schedules for low security functionality.
  
  The shortcut menu allows you to assign up to two schedules to the selected element.
  
  See “Schedule shortcut menu” on page 84 for more information.

- 2 RdrIn Inh PIN. If set to yes, the IN reader is in the low security mode if the above schedule is active.

- 3 RdrOut Inh PIN, etc.
  
  The functionality is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

5.1.n.7.3 RTE Schedule

Select schedules for Request To Exit input.

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

See “Schedule shortcut menu” on page 84 for more information.

5.1.n.8.1 Zones

Select zones that must be shunted on the door opening.
To activate or deactivate shunting, toggle a local zone number. See also “5.1.n.8 Shunt options” on page 222.

### 5.1.n.8.4 Indication

<table>
<thead>
<tr>
<th>1&gt;DOTL output</th>
<th>Not used</th>
</tr>
</thead>
</table>

The menu allows you to assign door controller outputs for indication of the specific access control events.

#### 5.1.n.8.4.2 DOTL output

<table>
<thead>
<tr>
<th>00&gt;Not used</th>
<th>19 Output 17</th>
</tr>
</thead>
</table>

Select an output on the door controller to indicate the Door Open Too Long alarm.

#### 5.1.n.8.4.3 Warning output

<table>
<thead>
<tr>
<th>00&gt;Not used</th>
<th>20 Output 17</th>
</tr>
</thead>
</table>

Select an output on the door controller to indicate the warning before the shunt time or extended shunt time expires. See also “5.1.n.8.2 Shunt timers” on page 223.

#### 5.1.n.8.4.4 Forced door

<table>
<thead>
<tr>
<th>00&gt;Not used</th>
<th>19 Output 17</th>
</tr>
</thead>
</table>

Select an output on the door controller to indicate that the door is forced (opened without a successful authorization).

#### 5.1.n.8.5 Until door CL

<table>
<thead>
<tr>
<th>5 Until door CL</th>
<th>&gt;No&lt;</th>
</tr>
</thead>
</table>

If set to Yes, the door shunt zones remain shunted as long as the door is opened.

#### 5.1.n.8.6 CancelAfterCL

<table>
<thead>
<tr>
<th>6 CancelAfterCL</th>
<th>&gt;No&lt;</th>
</tr>
</thead>
</table>

For security reasons, it may be required to limit the shunt period as much as possible. If the option is set to Yes, the door shunt zones are shunted until the door is closed. Opening the door again within the shunt time is not possible, as this will generate an alarm (there is always a debounce time of approximately 2 seconds).
5.1.n.9 Regions & AP

The menu contains door options connected to region control and anti-passback.

5.1.n.9.1 Regions

Use the menu to assign regions to readers. First, select the appropriate reader. Next, choose a region the reader belongs to.

0>Add region
1 Outside

The list of regions allows you to add a new region. The add region menu is equal to the menu in “5.3 Regions” described on page 237. See Chapter 3 “System functions > Regions” on page 75 for details.

5.1.n.9.2 Anti-passback

Controls the operation of the door if a card or PIN is used to attempt to enter the region that the user is currently assigned to. The following options are available:

- No AP: No control of passback.
- Soft anti-passback: A valid card or PIN opens the door when used to enter the region the second time without leaving first, but a report is generated.
- Hard anti-passback. A valid card or PIN does not open the door when used to enter the region a second time without leaving first. An attempt to do so generates a report.
- Regions anti-passback. A valid card or PIN does not open the door when used to leave a region other than the one entered previously. For example, if the user had entered region 2 from region 1, he will be denied when trying to enter region 1 from region 0. An attempt to do so generates a report.

See Chapter 3 “System functions > Anti-passback” on page 75 for details.

5.1.n.9.3 Inh Reg 1 Usr

For users in region 1 (on most occasions is “outside”), a special security feature is available to provide access only via another region. If the option is set to yes, any user in region 1 will be denied access. To access, the user first has to be in another region.
The functionality is configured separately for each door reader. After selecting the option, choose the appropriate reader, and then set the option value.

### 5.1.n.9.4 HSU options

#### 5.1.n.9.4.1 Req HSU Nr

The value defines how many High Security Users (HSU) must be present in the region assigned to the selected door.

### 5.1.n.9.4.2 Prewarn. time

The value defines time (in seconds) for the prewarning timer to run. When there are too few high security users in a high security region, a prewarning timer starts, and when it expires, an alarm is raised and the alarm output activates.

### 5.1.n.9.4.3 HS alarm out

Select an output on the door controller to indicate an anti-passback or high-security alarm.

### 5.2 Door groups

Door groups define when a user can have an access to specific doors. See Chapter 3 “System functions > Door groups” on page 75 for details.

#### 5.2.0 Add Door Gr

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

The new door group is given the default name “Door Gr N” and placed on the end of the door list.
5.2.n Select door group

Select a door group to program.

5.2.n.1 Door Gr name

Every door group can be programmed with a name to identify it.

Use the Door Gr name screen to enter or change the door group name. The name can contain up to 16 characters.

5.2.n.2 Door Gr data

Program the user access for the selected door group.

To configure a door group:

1. Add a door to the group if necessary. The default schedule (Always) is automatically assigned to every added door.
2. Select a door, to which a user with the assigned door group can have an access.
3. Assign up to two schedules that define, when users with this door group have an access to this door.
   - The shortcut menu allows you to assign up to two schedules to the selected element.
   - See “Schedule shortcut menu” on page 84 for more information.
4. Repeat for all doors specific for this door group.

5.2.n.3 Delete Door Gr

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

The display shows:

Choose Ok and press Enter. This deletes the door group.

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

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

Configure regions.

See Chapter 3 “System functions > Regions” on page 75 for more information.

5.3.0 Add region

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

INFO
Region added

The first region is given the name “Outside”, while subsequent regions are named “Region 2”, “Region 3”, etc.

5.3.n Select region

Select a region to program.

5.3.n.1 Region name

Every region, except region 1 “Outside”, can be programmed with a name to identify it.

Use the Region name screen to enter or change the region name. The name can contain up to 16 characters.

5.3.n.2 Delete region

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

The display shows:

Choose Ok and press Enter. This deletes the region.

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

Note: You cannot delete region 1.
6 Outputs and filters

In this programming section outputs, filters and triggers, and their options are programmed. Outputs on panel or expander as well as system triggers can be activated.

6.1 Condition filters

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

Filter settings

6.1.0 Add filter

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

INFO
Filter added

The new filter is given the default name “Filter N” and placed on the end of the condition filter list. You can now start editing its details.

6.1.n Select filter

Select an existing filter to program.

6.1.n.1 Filter name

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

6.1.n.2 Formula

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

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.

To choose an appropriate event, you must define the source of the event first. The source is defined by a group of objects, and an object within this group. Available groups are listed in Appendix A “Advisor Advanced events” on page 337.

When the group and the object (if available) are selected, select the appropriate event. The available selection depends on the selected source. The full event list with sources is shown in Appendix A “Advisor Advanced events” on page 337.

The following functions are available for the selected event:

1. Group: Select group
2. Element: Select an element (or all elements) from the group above
3. Event: Select an event for the element above
4. Invert: Invert the selected event. If inverted, it is marked with '!' in the formula
5. Remove event: Remove the selected event

6.1.n.2.y Select operator

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

6.1.n.3 Invert

The Invert option specifies if the condition filter output is inverted.

6.1.n.4 Delete filter

Use the screen to remove a condition filter from the system. To remove the filter, select OK and press Enter again. The filter is deleted.
6.2 Outputs

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

When adding a new output, use the Add output menu to select whether the output is located on the panel PCB, output expander, remote expander, or keypad.

See “Zone, output, and door addressing” on page 32 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

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.
Chapter 5: Menu reference

6.2.n.2 Output location

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

The Invert output option determines if the output is inverted.

6.2.n.4 Start filter

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

Use the Stop filter menu to specify an optional condition filter that deactivates the output.

6.2.n.6 Mode

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 243.

  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 243. After the time passes, the output activates for a time defined in “6.2.n.7.2 Active time” on page 243, and then it switches off.

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

• Double pulsed: Similar to the previous one, except the delay timer is activated by any change of the start condition filter, activation and deactivation.

• Latched: A single activation of the start condition filter switches the output on. The output can be then deactivated only by activating the stop condition filter.

If the stop condition filter is not set, the output will always remain active.

• Toggled: A single activation of the start condition filter switches the output state to the opposite.

Figure 26 below shows examples of described output activation modes.

Figure 26: Output activation mode examples

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

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 243 for more details.
6.2.n.7 Parameters

6.2.n.7.1 Delay time

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

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 241.

6.2.n.7.3 Retriggerable

Note: The Retriggerable option is only valid for Pulsed and Double pulsed outputs.

If this option is set to Yes, the active timer is restarted when the starting condition becomes valid again during the active state, so the active time is prolonged. Figure 27 below shows the output retrigging when the start filter is reactivated [1].

Figure 27: Output examples

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

tA Delay time  
tB Active time  
tC Interrupted active time  

[1]
6.2.n.8 Log limit

If the Log limit option is set to Enable, only 3 pairs of activating (opening) and restoring (or closing) events coming from a single output are recorded in the log during one set/unset cycle.

6.2.n.9 Delete output

Use the Delete output screen to remove an output from the system. To remove the output, select OK and press Enter again. The output is deleted.

6.3 Triggers

The Triggers menu allows you to configure system triggers.

Trigger settings

6.3.0 Add trigger

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

INFO
Trigger added

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

6.3.n Select trigger

Select a trigger to program.

6.3.n.1 Trigger name

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

Use the Trigger name screen to enter or change the trigger name. The trigger name can contain up to 16 characters.
6.3.n.2 Schedule
Select schedules for the trigger.
The shortcut menu allows you to assign up to two schedules to the selected element.
See “Schedule shortcut menu” on page 84 for more information.

6.3.n.3 Delete trigger
To remove a trigger, select a trigger using the cursor, or by entering the trigger number, and go to the Delete trigger menu.
The display shows:

```
3 Delete trigger
>Cancel<
```

Choose Ok and press Enter. This deletes the trigger.
Repeat the command to delete other triggers, or press Clear to exit and return to the higher menu level.
7 Calendar

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

See “Calendar” on page 83 in Chapter 3 “System functions” the detailed functionality description.

7.1 View

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

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

7.1.n Date

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

7.1.n.1 Auto setting

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

Select All areas, or choose the appropriate area.

7.1.n.2 By object

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

Select object name or type. The available objects are described in “User programmable functions” on page 97.
7.1.n.3 Special day

Enter the menu to configure the selected day as a special day.
For more information, see Chapter 3 “System functions > Special days in schedules” on page 84.

7.1.n.3.1 Day type

Choose a type for the selected day:
• Normal day: A normal day. A special day time frame is not valid.
• Holiday, Special day 2 etc.: The day is one of special days defined in “7.2.n.6 Special days” on page 251.

7.1.n.3.2 Recurring

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

7.1.n.3.3 Until date

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

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

7.2 Schedules

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

The maximum schedule number in the system is given in “General features” on page 37.
For more information on schedules see “Schedules” on page 83 in Chapter 3 “System functions”.
Chapter 5: Menu reference

Schedule settings

7.2.0 Add schedule

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

INFO
Schedule added

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

7.2.n Select schedule

1> Name
Schedule 1

Select a schedule to program.

7.2.n.1 Schedule name

1 Name
> Schedule 1 <

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

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

7.2.n.2 Active

2 Active
> No <

If set to Yes, the schedule is currently active.

7.2.n.3 Date

1> Start date
01.01.2016

Enter the following dates:

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

7.2.n.4 Time

0> Add time frame
1 Time frame 1

Define time frames when the schedule activates.
7.2.n.4.0 Add time frame

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

```
INFO
Time frame added
```

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

Caution: Time frames should not overlap.

7.2.n.4.m Select time frame

1>Start time
00:00

Select a time frame to program.

7.2.n.4.m.1 Start time

1 Start time
>00:00<

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

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

7.2.n.4.m.2 End time

2 End time
>00:00<

Provide the time of the day in 24-hour HH:MM format when the selected time frame ends. The value 00:00 means that the end time is not set, and therefore the counteraction is not performed. See Chapter 3 “System functions > Counteractions” on page 84 for more information.

7.2.n.4.m.3 Week days

Week days
>M.WT...<

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

If no week day is selected, the schedule will only be valid on the first and the last day (non-recurring schedule). In this case only one time frame can be used. See also Chapter 3 “System functions > “Schedules” on page 83.

7.2.n.4.m.4 Delete time frame

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

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

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

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

7.2.n.5 Action list

0>Add Action
1 Action 1

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

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

The maximum action number for each schedule is given in “General features” on page 37.

7.2.n.5.0 Add action

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

```
INFO
Action added
```

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

7.2.n.5.m Select action

1>Name
    Action 1

Select an action to program.

7.2.n.5.m.1 Action name

1 Name
    >Action 1 <

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

Use the Action name screen to enter or edit the action name. The action name can contain up to 16 characters.
7.2.n.5.m.2 Object type

7.2.n.5.m.3 Function

7.2.n.5.m.4 Parameters

Available functions and parameters are described in “User programmable functions” on page 97.

7.2.n.5.m.5 Delete action

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

The display shows:

```
5 Delete action
>CANCEL<
```

Choose Ok and press Enter. This removes the action.

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

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

7.2.n.6 Special days

0>Add sp day
1 Holiday

Configure special days associated with this schedule.

The maximum number of special days for each schedule is given in “General features” on page 37.

7.2.n.6.0 Add special day

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

```
INFO
Sp day added
```

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

7.2.n.6.m Select special day

Select a special day to program.
7.2.n.6.m.1 Special day name

Every special day can be programmed with a name to identify it.
Use the Special day name screen to enter or edit the special day name. The special day name can contain up to 16 characters.

**Note:** Special day names are common for all schedules.

7.2.n.6.m.2 Start time

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

7.2.n.6.m.3 End time

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

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

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

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

Choose Ok and press Enter. This removes the special day.
Repeat the command to delete other special days, or press Clear to exit and return to the higher menu level.

7.2.n.7 Filter

Assign an additional condition filter to the schedule.
If this filter is deactivated, the schedule is disabled. If no condition filter is assigned, the schedule is executed unconditionally.
See “6.1 Condition filters” on page 238 for more details.

7.2.n.8 Delete schedule

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

8 Delete sched
    >Cancel<

Choose Ok and press Enter. This removes the schedule.
Repeat the command to delete other schedules, or press Clear to exit and return
to the higher menu level.
8 System option menu

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

8.1 Timer menu

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

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

The following options are available.

- 1 Time zone. The system time zone.
- 2 Date. Date format is DD-MM-YYYY.
- 3 Time. Time format is 24 hours.
- 4 DST start mth. The DST start month.
- 5 DST start wk. The DST start week. The available options are: 1st week, 2nd week, 3rd week, 4th week, last week.
- 6 DST end mth. See above.
- 7 DST end wk. See above.
- 8 Set correction. Allows configuring time correction if necessary.

- 8.1 Time/7days. This submenu allows setting the time correction that is performed each 7 days of panel work.

Maximum value is 5 min 40 s. Positive value means the clock is set forward, negative — backward.
During daylight saving time change, the time always advances on Sunday at 2:00, and rewinds at 3:00.

**Note:** See “Daylight saving note” on page 84 for information on daylight saving time change on programmed actions.

### 8.1.2 Siren options

#### 8.1.2.1 Activation

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.

#### 8.1.2.1.1 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 146.

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

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

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 259). 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

The Zone timer menu allows you to set up all programmable zone timers.

8.1.4.1 Double knock interval

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

If enabled for a particular zone, Double knock open specifies the time for which the zone may remain active. If the zone remains active after this time exceeded, an alarm is generated without waiting for a second activation.

The input format is mm:ss. The allowed range is from 00’00 to 15’00.
8.1.4.3 Soak test

3 Soak test

The Soak test option defines the number of days the soak test for a zone is active. The allowed range is 0 to 30 days.

Soak test is activated as soon as the zone option Soak test (see “4.1.n.6.10 Soak test” on page 195) 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

The options define the time period of held open, after which the zone raises “open too long” flag, which can be used for filter programming.

See “4.1.n.6.30 Held open” on page 199.

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 139.
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

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

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

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 322 for more information.

8.2.4 Engineer reset

1>Alarm
   No

The Engineer reset menu lets you define which conditions require an engineer reset, and also lets you perform this reset.

8.2.4.1 Alarm

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 264).

This option is ignored in case AB alarm confirmation is enabled. For more information see “8.2.4.4 Confirmed alarm” on page 260.
8.2.4.2 Tamper

2 Tamper >No<

If the Tamper option is set to Yes, tamper alarms require an engineer reset.

8.2.4.3 Panic

3 Panic >No<

If the Panic option is set to Yes, panic alarms require an engineer reset.

8.2.4.4 Confirmed alarm

4 Conf. alarm >Off<

The Alarm confirm menu defines which AB alarm requires an engineer reset. The available options are A-ALARM, B-ALARM, or Off (disabled). This option works only when AB alarm confirmation is enabled.

8.2.4.5 Battery fail

5 Battery fail >Off<

If the Battery fail option is set to Yes, battery faults require an engineer reset.

8.2.4.6 Aux fuse

6 Aux fuse >Off<

If the Aux fuse option is set to Yes, auxiliary fuse faults require an engineer reset.

8.2.4.7 Mains fail

7 Mains fail >Off<

If the Mains fail option is set to Yes, mains supply faults require an engineer reset.

8.2.4.8 Siren fault

8 Siren fault >Off<

If the Siren fault option is set to Yes, siren faults require an engineer reset.

8.2.4.9 Interconn fault

9 Intconn fault >Off<

If the Interconnection fault option is set to Yes, interconnection faults require an engineer reset.
8.2.4.10 Auto reset

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

Dis by service

>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 259.

8.2.4.12 System code

System code

> <

The System code menu allows you to set the system code for engineer reset. The code can have up to 5 digits.

The default value 0 means that the code is not set. In this case the remote reset code generation is disabled.

If the code is set, its value and the engineering code value are used in a special calculation to generate the reset code. See “Engineer reset” on page 113 for more information.

8.2.4.13 Do reset

Do reset

>Cancel<

The Do reset command is used to perform the engineer reset.

8.2.4.14 Custom text

Custom text

> <

Use custom text to program a prompt displayed when an engineer reset is required.

If the custom text is not set, the standard prompt will be displayed as described in “Engineer reset” on page 113.

Otherwise, the prompts will be the following, depending on a user code display or warning message:

<custom text>
Code:23353
8.2.5 Service in

The menu lets you disallow the Installer in function before the Installer in time expires (see “8.1.3.6 Installer in-time” on page 257).

**Note:** This option is only valid if the installer requires a user authorization. See “8.2.1 User code required” on page 259.

Use this function after the panel programming is complete. To cancel the service in, go to this menu and press Enter. Next, log out. After this, the installer log in requires another user confirmation.

See also “User code requirement” on page 122.

8.2.6 Challenge code

Use this menu to activate challenge code functionality. See “Challenge code requirement” on page 122 for more details.

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

8.2.7 Inspection

Set up a periodic inspection reminder.

**8.2.7.1 Date**

Enter the date of the next inspection.

**8.2.7.2 Custom msg**

Enter the message for the inspection reminder.
8.3 LCD display options

The LCD options menu contains options that can be set for LCDs and menus.

8.3.1 Armed display

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 256).

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

You can select one of the following armed display options:

- Off: Armed display is disabled.
- If set: Armed display activates only when the area is set. No status information is displayed on keypad LCD and LEDs (except mains LED and Alert message).
- Always: Armed display always activates. No status information is displayed on keypad LCD and LEDs (except mains LED and Alert message).
- Without code: Armed display always activates. No area LED is lit.

Note: This mode also allows you to deactivate the armed display pressing the Clear key.

8.3.2 Custom message

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

The option defines how zone alarms and faults can be viewed on LCD by an unlogged user.

- Disable: Zone alarms and faults are not shown.
• Enable: The alarm list option allows users to list active zones and faults as well as alarms.
  
  See “Keys” on page 58.

• 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 263 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 unwsetting the system.

8.4 Set options

1>RTS options
2 Inhibit incl

Options on the Set options menu define the set conditions.

8.4.1 RTS options

1>Zone alarm
Yes

The RTS options menu defines conditions that can prevent setting. If a particular condition below has this option set to Yes, its state affects the “Ready To Set” state. The system does not allow for areas to set if any of the conditions are true.

For conditions related to areas, the condition is tested for those areas. For example Zone 5 assigned to area 1 only affects the setting of area 1.

The following options are available.

• 1 Zone alarm: Active zone
• 2 Zone panic: Hold-up device active
• 3 Zone masking: Masking / fault state on input
• 4 Zone fault: Intrusion detector fault
• 5 Zone tamper: Tamper in zone
• 6 Interconnection fault: A critical error caused by communication trouble between internal panel components
• 7 Mains fault: Mains fault, including external fault
• 8 Battery fault: Battery fault, including external fault
• 9 FTC (Failed to Communicate): Alarm reporting has failed to deliver events
• 10 Siren fault: Siren output fault
• 11 Zone technical: Technical zone status
• 12 Keypad fault: A fault reported by keypad
• 13 Expander fault: A fault reported by remote expander
• 14 Comms fault: All transmission paths are down (no communication)
• 15 Engineer reset: Engineer reset requirement
• 16 Alarms pending: Unacknowledged alarms
• 17 Audio fault: A fault reported by audio device

8.4.2 Inhibit includes

The menu defines which conditions a user with particular access level is allowed to inhibit. If a particular condition below has this option set to Access level 2 or Access level 3, a user with this access level can inhibit it using an inhibit menu or during set.

The following options are available.

• 1 Zone panic: Holdup device active
• 2 Zone masking: Masking / fault state on input
• 3 Zone fault: Intrusion detector fault
• 4 Zone tamper: Tamper in zone
• 5 Interconnection fault: A critical error caused by communication trouble between internal panel components
• 6 Mains fault: Mains fault, including external fault
• 7 Battery fault: Battery fault, including external fault
• 8 FTC (Failed to Communicate): Reporting attempts are failed
• 9 Siren fault: Siren output fault
• 10 Zone technical: Technical zone status
• 11 Keypad fault: A fault reported by keypad
• 12 Expander fault: A fault reported by remote expander
• 13 Comms fault: All transmission paths are down (no communication)
• 14 Engineer reset: Engineer reset requirement
• 15 Audio fault: A fault reported by audio device

8.4.3 Part set

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

If the Report BA option is set to Yes, in the part set the system reports burglar alarms triggered during part set to the central station.

8.4.3.2 Access to EE

If the Access to EE option is set to Yes, Access zones become Entry/Exit zones during part set. Users being inside the premises will then trigger the entry timer making them aware that the area is set and an unset procedure is required.

8.4.3.3 EE full set

If the option is set to Yes and the user exits premises during part set exit time (which causes activation of entry/exit zone), part set state changes to full set.

Note: The functionality works only if there is exit time defined for part set. It means that area part set exit time defined in “4.2.n.2 Exit time” on page 206 must be longer than 0.

8.4.3.4 PS1 name

8.4.3.5 PS2 name

Use these menus to change the default part set prompts “Part set 1” and “Part set 2”. Empty string is equal to the default prompt.

See Advisor Advanced User Manual for more details on partial setting.

8.4.4 Forced set

The Forced set option enables the forced set feature. The forced set options are configured below.

Forced set is an option where active zones can automatically be inhibited when setting an area.

Note: This option should be used with care. Users may not be aware which zones are inhibited.
8.4.5 Forced set options

The Forced set options menu defines when the forced set is possible. The following options are available.

- Inhibit till unset: Zone is inhibited until the area is unset.
- Inhibit exit: Zone is inhibited until the exit time expires.
- Inhibit close: Zone is inhibited until its state changes to normal.

8.4.6 Pending alarms

If set to Enable, the Pending alarms option requires all alarms and faults to be acknowledged.

Enable EN Gr3 is equal to Enable except that faults and tampers can only be acknowledged by level 3 user (installer).

When disabled, it does not require alarm acknowledgement. During unsetting or resetting the area, the alarm is acknowledged automatically. However, each alarm and fault is shown 3 times on the keypad screen.

8.4.7 AS fault retry

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 101 for more details.

8.4.8 AS user retry

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 101 for more details.

The user must have a privilege for full setting to be allowed to postpone the autoset. See “3.2.n.6 User group options” on page 190 for more details.

8.5 Access options

The menu contains various access control options.

8.5.1 Access timers

1>Access timers
2 DGP options

The menu contains access timer settings.

Note: All timers are programmed in seconds. The allowed ranges are 0 to 127 s.

8.5.1.1 Card to PIN

1 Card to PIN
> <

This setting is only applicable when a user is required to present a card and enter a PIN to gain access.

The Card to Pin Time is the amount of time allowed between presenting a valid card to a door reader and entering a valid PIN (last digits) on the keypad. If the PIN is not entered before the time expires, the user will need to repeat the door opening function.

8.5.1.2 Two cards

2 Two cards
> <

This setting is only applicable when two users must present their card or PIN to open a door or when a user is identified as a visitor or guard and must be accompanied.

The Two cards time is the amount of time allowed between the first user presenting a card or entering a PIN and the second user presenting a card or entering a PIN. If the second card/PIN is not presented before the time expires, the door opening function will have to be repeated.
8.5.1.3 Multiple badge

This setting is only applicable where the door has been programmed so that presentation of a card three times will arm/disarm the system and the user is authorised to arm/disarm.

The Multiple badge time is the amount of time allowed between the first presentation of the card and the third presentation of the card. If the card is not presented three times before the time expires, the user will need to commence the function again.

8.5.1.4 Re-lock delay

This setting only applies where the door has been programmed so the unlock relay will not re-lock until after the door is closed.

This feature is provided for Drop Bolts and Maglocks etc. where the door must be closed before the unlock relay locks the door.

The Re-lock delay time is the amount of time between the door being closed and the unlock relay deactivating (re-lock). This allows a settling time to ensure that the lock mechanisms are aligned.

8.5.2 DGP options

The menu contains door controller settings.

8.5.2.1 Map relays

Defines whether door controller unlock outputs can be controlled as standard outputs.

- Yes: Door unlock outputs can be controlled by the control panel as its outputs.
- No: Door unlock outputs can only be activated by door controller when using door unlock user menu, or upon presenting a valid card.
8.5.2.2 Map panel LEDs

When this option is set to Yes, LEDs in door readers connected to the door controller will represent the same status as LEDs in keypads connected directly to the panel.

8.6 Zone options

The Input options menu defines options of zone inputs.

8.6.1 Input mode

The Input mode option determines the configuration of zone inputs in the panel. The following values can be set:

- Single NO: In the single zone mode the panel can only detect an alarm from the zone. In the single input mode normal state depends on the EOL value. If this value is set to “No EOL” in “8.6.2 EOL” below, normal state for Single NO zone is open.
- Single NC: Similar to Single NO above, but If EOL is disabled in “8.6.2 EOL” below, normal state for zone is short.
- Dual loop: For dual loop to operate, every zone needs two or three EOL resistors. This enables the panel to detect multiple zone states, including alarm, tamper, masking etc., depending on connection type and EOL value set in “8.6.2 EOL” below. See “Zone connection” on page 24 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 170.

8.6.2 EOL

The menu allows you to define end-of-line resistor values. For different input modes the following values can be available: 1k0, 1k5, 2k, 2k2, 2k2+4k7, 3k3, 3k74, 4k7, 5k6, 6k8, 8k2, 10k, No EOL.

Note: Available EOL values depend on “8.6.1 Input mode” option above.

See “Zone connection” on page 24 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 170.

8.6.3 Siren tamper EOL

The Siren tamper end of line resistor menu allows you to define an end-of-line resistor value for the siren. The available values are the same as in “8.6.2 EOL” on page 270.

8.6.4 Swinger shunt

The Swinger shunt value defines the number of alarms from a zone until it is shunted. The default value is 2, the maximum number is 4.

This zone must have the “4.1.n.6.6 Swinger shunt” option enabled (see page 194).

8.6.5 Report restore

If the Report restore option is set to On ACK, the restore event is reported to the central station when a user acknowledges an alarm.

If the option is set to On input close, the restore event is reported when the zone returns to the normal state.

8.6.6 Limit reports

The option is the idle time (in seconds), which must elapse after an alarm before the next alarm from the same zone is reported to the central station. This time allows you to limit the reporting of multiple alarms from the same zone.

**Note:** Alarms from the same zone occurring within this time are not reported, but the events are stored in the log. Every new alarm from this zone restarts the timer.

The allowed range is 0 to 255 s. The default value is 120 s, 0 means the limit is disabled.

See also “4.1.n.6.39 Limit reports” on page 201.
Chapter 5: Menu reference

8.7 Panel and AB options

8.7.1 Panel name

The Panel name menu lets you change the panel name.

8.7.2 Panel language

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 130, and “Predefined users” on page 64.

8.7.3 Duress method

The Duress method menu allows you to change the duress entering method. See Advisor Advanced User Guide for more information on available duress methods.

8.7.4 PIN length

The PIN length menu allows you to change the PIN length. See “3.1.n.2.1 Change PIN” on page 183 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 183 for details.
8.7.5 PIN chg mode

The PIN change mode option allows you to choose the appropriate PIN change mode. See “PIN” on page 71 for details on PIN usage.

8.7.6 Alarm confirm

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

8.7.6.1 AB mode

The AB mode option enables the AB alarm confirmation feature for particular areas. When set to On, the first alarm is reported as a standard burglar alarm (A-alarm). A second input has to alarm within a certain period to report a confirmed alarm (B-alarm), provided the first alarm in the area did not occur in an entry/exit zone.

The verification mode is programmable per area.

8.7.6.2 AB time

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

8.7.6.2.1 Intrusion AB time

The maximum time (0 to 255 minutes) that the system allows for a second intrusion alarm to occur to report a confirmed alarm.

If the second alarm happens within this time, it is reported as a confirmed alarm (B-alarm). When the AB time has expired, any next alarm is again an unconfirmed alarm (A-alarm). If the zone that created the initial A-alarm is still active, it is inhibited.

8.7.6.2.2 Holdup AB time

The maximum time (8 to 20 hours) that the system allows for a second holdup alarm to occur to report a confirmed alarm.
See also “8.7.6.2.1 Intrusion AB time” on page 273.

8.7.6.3 System confirm

The System confirmation option defines if the AB alarm confirmation works in separate areas only, or if it allows for system-wide validity. If this option is set to Yes, an A-alarm in one area can be confirmed by a B-alarm in another area. Otherwise, the A-alarm can only be confirmed by a B-alarm in the same area.

8.7.6.4 EE confirm

The EE confirmation option configures the AB alarm confirmation during entry time.

If the option is set to Yes, alarm confirmation is suspended during entry time. If no B-alarm was present, all alarms during the entry time are A-alarms. When the entry time has expired, alarm confirmation is enabled. However: entry/exit and access zones cannot generate B-alarms.

If this option is set to No, the start of the entry timer disables any alarm confirmation until the area is set again.

8.7.6.5 Access to EE

The Access to EE option defines the functionality of the access zone in the area (if available) when an entry/exit (EE) zone is inhibited at the end of the AB time (auto-inhibit function). The following values are allowed:

- Entry/Exit: an access zone acts as an entry/exit zone, if the entry/exit zone is inhibited.
- Access: an access zone does not change its functionality and causes an alarm when activated while no EE timer is running.

8.7.6.6 TA confirm

If the TA confirm option is set to Yes, tamper alarm (TA) can report a B-alarm for burglary alarm (BA), and vice versa.
Chapter 5: Menu reference

8.7.6.7 Sirens

The Sirens menu allows you to select per area when the siren is activated: on A-alarm or on B-alarm.

Note: Option B-alarm is valid only if AB mode is enabled. See “8.7.6.1 AB mode” on page 273.

8.7.6.8 Call CS message

If the Call central station message option is set to Yes, in case of alarm the keypad displays a message with advice for the user to call the central station when a report has been sent.

8.7.6.9 Reporting delayed

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

8.7.7 Easy unset

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

8.7.8 Remote options

Set remote configuration options.

8.7.8.1 Remote config

If the option is set to Yes, remote operators can modify user PINs and phone numbers when areas are set. If set to No, user PINs and phone numbers are possible to change by remote operators only when all areas are unset.

8.7.8.2 Superv config

If the option is set to Yes, the supervisor is allowed to configure the panel remotely.
See “Remote access” on page 129 for details.

8.7.9 Object scheme

Choose one of the following object (zone, input, output and door) numbering schemes:

- **Classic.** In the classic numbering scheme, the object default identifiers depend on physical input or output locations, for example, Zone 1 is assigned to the input located on Panel 1.1, Zone 18 is assigned to the input located on Expander 1.2.

- **Flexible.** In the flexible numbering scheme, default identifiers are independent. When adding a new object, the object is created in the first available database position, regardless of the specific input or output physical location.

When attempting to toggle the scheme, the confirmation is displayed.

**Cautions**

- Changing of numbering scheme will require system reboot. After this, the reporting event values will change object numbers according to the new numbering.

- After changing the scheme from classic to flexible, all programmed object dependencies (for example, condition filters, cameras, etc.) will be unavailable. The appropriate parameters will be set to “Not exist” instead of previously programmed objects, until the scheme is changed back.

See also “Zone, output, and door addressing” on page 32 in Chapter 2 “Installation”.

8.8 PA and other

The menu allows you to configure panic alarm mode, chime, and buzzer options, etc.

8.8.1 Panic mode

Panic mode can be one of the following.

- **Silent:** The panic alarm is silent (no siren activation)
- **Audible:** The panic alarm is standard (with siren activation)
- **Audible alarm if line fault:** The panic alarm is audible only if a Line Fault (LF) or a Failed To Communicate (FTC) fault is present
8.8.2 Chime menu

1>Chime in PS
   No

The Chime menu allows you to set up chime options.

8.8.2.1 Chime in part set

1 Chime in PS
   >No<

The Chime in part set option defines whether the chime option is active when the area is in the part set mode.

8.8.2.2 Latched chime

2 Latched chime
   >Yes<

If the Latched chime option is set to Yes, disabling the chime only affects the chime functionality until the next time the area is unset. Otherwise it should be enabled manually.

8.8.3 System tamper areas

3 SysTamp areas
   >1.......<

The System tamper areas option allows assigning system tampers and faults to the specified areas. At least one area must be selected.

8.8.4 Siren retrigger

4 Siren 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 Card learn-in

5 Card learn-in
   >Keypad 1<

Choose a keypad for user card learning. See also “3.1.n.3 User card” on page 184.
8.8.6 Test inputs

The Test inputs option defines what inputs should be accessible when performing input tests as described in “1.2.1 Input tests” on page 137. The following options are available:

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

8.8.7 Buzzer mode

The Buzzer mode menu defines how the keypad buzzer works during the exit time. The following options are available:

- Continuous: The keypad buzzer emits a continuous sound that switches to an intermittent during an entry/exit or access zone activity.
- Intermittent: The keypad buzzer emits a continuous sound and switches to an intermittent 10 seconds before the exit time expires.

8.8.8 Mon 3 HC out

Monitor 3rd high current output option defines whether high current output 3 is monitored or not.

Output 3 mode depends on the panel model. See “Outputs” on page 31 for details.

8.8.9 Card number

Select the way the card number is represented in the control panel.

- Basic. The card number is represented in the standard Advisor Advanced format.
- Titan. The card number is represented in the extended Titan format.

8.8.10 Anonymize Log

The menu allows you to set a time period, after which the user details are removed from a log entry.
The allowed range is 0 to 60 days, 0 means the functionality is disabled. The default value is 30 days.

8.9 Timed Unset / ATM

1>Delay

The menu allows you to configure the ATM (automated teller machine) interface.

8.9.1 Delay

1 Delay > <

The option value is the time between the first and the second ATM user code entering. At the end of the programmed delay period the ATM user is be prompted to re-enter the code.

The allowed range is 0 to 15 minutes. 0 means that the ATM user code can be entered twice without any delay. The default value is 0.

8.9.2 Unset Time

2 Unset Time > <

The maximum allowed unset time of the ATM. The allowed range is 1 to 255 minutes.

8.9.3 Ext Unset Time

3 Ext Unset Time > <

The maximum allowed extended unset time of the ATM. The allowed range is 0 to 255 minutes.

Note: The user can extend the unset time only once.

8.9.4 Uns Warn Time

4 Uns Warn Time > <

Warning time is a time before the ATM time runs out, when a warning signal is raised.

The allowed range is 1 to 14 minutes, while the default value is 10 minutes.
9 Communication

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

9.1 Central station

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

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 285
- “IP and GSM/GPRS specific options” on page 285
- “Photo transmission specific options” on page 287
- “GSM/phone specific options” on page 288
- “Audio specific options” on page 288
- “UltraSync specific options” on page 289
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 291.

9.1.n.3 Protocol

3 Protocol
>(X)SIA<

Choose the appropriate communication protocol.

Depending on the settings in “9.1.n.2 Transm path” above, the following protocols can be available:

- SIA
- (X)SIA
- VOICE
- CID
- OH+SIA
- OH+XSIA
- OH+CID
- SMS TEXT
- SMS+CID
- SMS+SIA
- SMS+XSIA
- VOICE+SMS
- SMS+MMS
- OHPHOTO+CID
- OHPHOTO+SIA
- OHPHOTO+XSIA
- PHOTO+XSIA

The menu is not available for UltraSync communication path. See “UltraSync” on page 117 for details.
9.1.n.5 Accounts

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 284 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 283).

- Area modifier off: Closing is reported when all areas with the same account number have been set. The area that was set last is reported. The first to disarm sends the opening signal for the area to be opened.
- Area modifier on: Opening and closing signals are reported separately. The Area Modifier is used to identify the correct area.

**Note:** System events, as well as Area 1 events, are always reported using Account 1.

The menu is not available for UltraSync communication path. See “UltraSync” on page 117 for details.

9.1.n.5.m Select area

Set account numbers for each area.

9.1.n.6 Mode

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 280). This means that the panel reports to this central station only if the primary CS reporting fails.

For example, if CS 1 and CS 2 are primary CS, and CS 3 and CS 4 are backup CS, it means that CS 1 has no backup, CS 3 is a backup central station for CS 2, and CS 4 is a backup for central station 3.

See “Reporting principles” on page 92 for more information.
9.1.n.7 Retry count

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 94 for more information.

The value ranges from 0 to 14. The default value is 1.

9.1.n.8 Protocol opt

It is possible to customize the communication protocol parameters using the Protocol opt menu.

The menu is not available for UltraSync communication path. See “UltraSync” on page 117 for details.

9.1.n.8.1 XSIA

The XSIA menu allows you to set options for the SIA and XSIA protocol.

9.1.n.8.1.1 Area modifier

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 282.

9.1.n.8.1.2 Name chars

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

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

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

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

The VOICE menu allows you to configure voice reporting options listed below.

9.1.n.8.2.1 Suppress FTC

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

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

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 283).

**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 282 for more details.

The menu is not available for UltraSync communication path. See “UltraSync” on page 117 for details.

### 9.1.n.11 Delete CS

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

The display shows:

```
10 Delete CS
  >Cancel<
```

Choose Ok and press Enter. This removes the central station.

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

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

### PSTN and ISDN specific options

#### 9.1.n.4 Phone

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

The Destination menu contains the configuration of the reporting receiver.
9.1.n.4.1 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 127.

9.1.n.4.2 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

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 148 to send ping to another host.

9.1.n.8.3 OH 2000

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

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

Heartbeat time

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

Receiver nbr

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

Line nbr

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

Freq. HB time

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 285, it is necessary to set the options below.

9.1.n.4.4 Encryption

Encryption

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

9.1.n.4.5 Vid dest port

Vid dest port

The destination port is used to send the pictures to a host set up in “9.1.n.4.1 Dest name” on page 286.
GSM/phone specific options

9.1.n.4 Destination

The Destination menu contains the configuration of the reporting receiver.

9.1.n.4.1 Type

The Type submenu defines who receives the reports directed to the specified central station:

- **Phone**: The report is sent to a specified phone number. Menu “9.1.n.4.2 Phone/User/UG” below configures this phone number.
- **User**: The report is sent to a specified user’s phone number. This user is selected via menu “9.1.n.4.2 Phone/User/UG” below.
- **User Group**: The report is sent to all users that belong to the user group that is set via menu “9.1.n.4.2 Phone/User/UG” below.

User and user group reporting require the following:

- Users must have their phone numbers set in “3.1.n.7.1 User phone” on page 186.
- The SMS reporting must be enabled for these users. See “3.1.n.7.2 SMS reporting” on page 187.
- At least one of the user groups must allow these users to receive SMS reports. See “3.2.n.6 User group options” on page 190).

9.1.n.4.2 Phone/User/UG

This menu depends on the Type value set for the reporting recipient. See menu “9.1.n.4.1 Type” above for parameters description.

Audio specific options

These options are only available for systems with two-way audio. See Chapter 3 “System functions > Two-way audio” on page 115 for more details.

9.1.n.10 Listen-in

The menu allows you to configure the two-way audio for the selected central station.
9.1.n.10.1 Enable

| Enable | >No< |

If set to yes, the two-way audio is enabled when reporting to the selected central station.

9.1.n.10.2 Time

| Time | >120< |

The option configures maximum duration (in seconds) of two way audio session. After this time the session stops automatically.

The allowed range is 0 to 255 s. 0 means that the session does not start.

The time can be extended by using DTMF tone.

9.1.n.10.3 DTMF control

| DTMF 1 | Disabled |

The menu allows you to configure DTMF commands used by the central station operator to control the two-way audio session.

First, select the desired DTMF tone from the list. Next, assign a command to the selected tone.

The available tones and commands are listed in Chapter 3 “System functions > DTMF control” on page 116.

UltraSync specific options

9.1.n.4 Channel number

| Channel no 1 |

The informational screens contain the channel number used for connection to the UltraSync cloud. The channel is configured in UltraSync Web portal. It defines such settings as reporting format, account number, and polling time.

Caution: When the panel is registered in the UltraSync cloud, all security cloud reporting is configured remotely from the cloud.

See Chapter 3 “System functions > UltraSync” on page 117 for more information on cloud connection.
9.2 Event options

1>CS mapping
2 Voice mapping

The Event options menu contains event options.
See “Reporting principles” on page 92 for more details on event reporting.

9.2.1 CS mapping

01>AN Report to
>1234..........<

The CS mapping menu allows you to map reporting events to the specific central stations.
The list of events is shown in Appendix B “Advisor Advanced reporting codes” on page 353.

9.2.2 Voice mapping

01>AN Msg number
0

The Voice mapping menu allows you to assign a particular voice message (0 to 14) to each system event. 0 means that no message is assigned.
The list of events is shown in Appendix B “Advisor Advanced reporting codes” on page 353.

9.2.3 Delayed events

0>Delay timer
0

The Delayed events menu allows you to set a delay for particular events.
The first menu entry, “0 Delay timer”, allows you to set the global reporting delay from 0 to 250 sec.
The next menu entries represent the particular events. If the option is On, the delay is applied.

01>AN Delayed
Off

For the list of events, see Appendix B “Advisor Advanced reporting codes” on page 353.

9.2.4 Lis-in events

001>AN Lis-in
Off

The menu allows you to select events that activate a two-way audio session with a central station.
Chapter 5: Menu reference

For the list of events, see Appendix B “Advisor Advanced reporting codes” on page 353.

See Chapter 3 “System functions > Two-way audio” on page 115 for more details.

9.3 Path options

The Path options menu allows you to configure options for available transmission paths.

9.3.n Select path

Select the appropriate transmission path to configure its options.

Available transmission paths depend on the system configuration. By default, the following transmission paths are available:

- IP

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

- PSTN
- ISDN
- GSM
- TDA74xx
- UltraSync

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

- “PSTN specific options” on page 293
- “ISDN specific options” on page 294
- “IP specific options” on page 294
- “GSM/SMS/GPRS specific options” on page 297

Common options

9.3.n.1 Path name

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

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

Particular diallers have their internal menus. Enter Expander menu to set internal dialler options.

The menu content depends on the equipment.

9.3.n.8 Ring setup

The menu contains ringing configuration options.

Note: This option is not available for IP connection.

9.3.n.8.1 Ring count

The Ring count screen lets you enter the number of rings before answering an incoming call. The allowed range is 1 to 15. Higher value is equal to infinity, so incoming calls are not answered at all.

9.3.n.8.2 Omit 1st call

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”.

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

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

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

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

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 308.

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

PSTN specific options

9.3.n.3 Line fault delay

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

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

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

The Dialling menu allows you to select the PSTN dial mode: pulse or tone (DTMF).
**ISDN specific options**

**9.3.n.6 Point to Point**

| 6 Point to Point | No |

The option must be set to Yes if the ISDN dialler uses point-to-point connection, otherwise it should be set to No.

Contact your ISDN provider for details on the service.

**9.3.n.7 MSN**

| 7 MSN |

The MSN option lets you enter the ISDN MSN number.

**IP specific options**

**9.3.n.3 Transm path**

| 3 Transm path | ETHERNET |

The Transmission path option is a read-only field that identifies a communication method used for this transmission path.

**9.3.n.4 IP config**

| 1 IP config | Dynamic |

The IP config menu allows you to configure the panel IP address.

The following options are configurable in this menu.

**9.3.n.4.1 IP config**

| 1 IP config | Dynamic |

If the IP config is set to Dynamic, the DHCP is enabled. If this value is Static, you must configure the other options in this menu that are described below.

**9.3.n.4.2 IP address**

| 2 IP address | 000.000.000.00 |

You must set the panel IP address prior to use the IP communication, if DHCP is disabled. If DHCP is enabled in “9.3.n.4.1 IP config” menu above, this value shows the dynamic IP address that is assigned by the DHCP server and cannot be changed.
9.3.n.4.3 Subnet mask

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 on page 294, this value shows the dynamic IP subnet mask that cannot be changed.

9.3.n.4.4 Gateway

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 on page 294, this value shows the dynamic gateway address that cannot be changed.

9.3.n.5 DNS config

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

If the IP configuration in menu “9.3.n.4 IP config” on page 294 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

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 294.
9.3.n.6 NTP config

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

The following options are configurable in this menu.

9.3.n.6.1 NTP config

If the IP configuration in menu “9.3.n.4 IP config” on page 294 is set to Dynamic (DHCP is enabled), you can set the NTP configuration option to Static to override the automatic NTP configuration by DHCP server. Set the NTP address in the menu below. If this option is set to Dynamic, the DHCP is used to obtain the NTP IP address.

If DHCP is disabled, this menu is not available.

9.3.n.6.2 NTP server

The NTP server menu allows you to set the NTP address if it is different from the NTP provided by DHCP server, or if DHCP is disabled in menu “9.3.n.4.1 IP config” menu on page 294.

9.3.n.7 Firewall

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 309.

The following options are configurable in this menu.

9.3.n.7.1 Firewall

Use the Firewall menu to enable (On) or disable (Off) the built-in firewall.

9.3.n.7.2 Reply on PING

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

The Link speed menu allows you to choose the Ethernet link speed. The allowed options are:
- 10 MB
- 100 MB
- Auto

9.3.n.9 MAC address

MAC address of the Ethernet controller is a read-only value.

9.3.n.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

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

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 302 for more
details.

9.3.n.5.1 SIM card PIN

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 149 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

The Networks menu lets you configure the GSM network settings.

9.3.n.5.2.1 Net.selection

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

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

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 150 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 150 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 298.

**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 150.
9.3.n.5.2.3.m.5 Use this net.

Enter Use this network menu to connect the selected GSM network. This replaces the network selected in “9.3.n.5.2.1 Net.selection” on page 298.

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

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

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 302 is enabled, otherwise the account state response will be lost.

9.3.n.5.3.6 Check time

The Check time is the time of day in 24 h format when the system performs the automatic account check described in “9.3.n.5.3.5 Check period” above.

9.3.n.5.4 Jamm detection

The menu allows you to configure GSM jamming detection parameters.

9.3.n.5.4.1 Jamm detection

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

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

The SMS Setup menu lets you change various SMS settings.
9.3.n.6.1 SMS Center num

The SMS Center number is the access number for the SMS service. If this value is empty, the system uses the default number stored in the SIM card. Use this menu to enter a number other than the provider’s default one.

Caution: Delete this number before changing the SIM card. Otherwise, the system will overwrite the default SMS center number on the new SIM card with this number.

9.3.n.6.2 SMS forwarding

The SMS forwarding menu lets you choose the phone number to which all unrecognized messages are forwarded (usually the supervisor’s or administrator’s phone). You can also switch off SMS forwarding using this menu. The list contains only those users who:

- Have the appropriate privileges to receive SMS messages (see “3.2.n.6 User group options” on page 190)
- Have their phone numbers configured (see “3.1.n.7.1 User phone” on page 186)

9.3.n.6.3 Max Msg 24h

You can limit the maximum number of SMS messages sent to users during a 24-hour period. If this limit is reached, further incoming messages are ignored by the system.

The SMS reports and unrecognized SMS commands have two separate counters. However, the maximum limit defined in this menu is the same for both counters.

There is no limit for messages if this value is set to 0.

9.3.n.6.4 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 281
9.3.n.6.5 User PIN req.

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

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

The GPRS Setup menu lets you change various GPRS settings.

9.3.n.7.1 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

The User name must be specified by the GPRS provider.

9.3.n.7.3 User password

The User password must be specified by the GPRS provider.
Note: The following GPRS configuration menus are equal to appropriate IP configuration menus, except they apply only to the IP connection via the GPRS path.

9.3.n.7.4 IP config
See “9.3.n.4 IP config” on page 294.

9.3.n.7.5 DNS config
See “9.3.n.5 DNS config” on page 295.

9.3.n.7.6 Firewall
See “9.3.n.7 Firewall” on page 296.

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 297.

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 303 for details.

9.3.n.10.3 User name
See “9.3.n.7.2 User name” on page 303 for details.

9.3.n.10.4 User password
See “9.3.n.7.3 User password” on page 303 for details.

9.3.n.10.5 Proxy

Enter the MMS proxy server address.

9.3.n.10.6 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

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

The informational screens contain GSM dialer firmware version, modem type, etc.
9.4 PC connection

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

It is possible to define up to 16 different PC connections.

9.4.1.0 Add PC conn

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

INFO
PC conn added

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

9.4.1.n Select PC connection

Select the connection to configure.

Note: Particular options in this menu differ for specific transmission paths. For specific options, see:
• “PSTN specific options” on page 309
• “IP specific options” on page 309
• “GSM specific options” on page 310

9.4.1.n.1 Name

The connection name can consist of up to 16 characters.
9.4.1.n.2 Transm path

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

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

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:

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

The PC callback option defines which PC connection is used as a callback station.

If the PC call back option is set to Off (no connection assigned), then auto-answer is active.

**Note:** Callback is only possible for modem connection.

9.4.2.1 Primary

9.4.2.2 Backup

These menus allow you to configure the primary and the backup callback destination respectively.

Choose a PC connection for a callback, or 0 to disable it.

0>Off
1 PC conn 1

Upon a callback request Advisor Advanced attempts to connect to the primary callback destination. The number of attempts is defined in “9.4.1.n.5 Retry limit” on page 307. 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

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 00000000000000000000000000000000 (24 zeroes).

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

**Note:** A PC connection via IP transmission path is always encrypted. An encryption of PSTN and ISDN connection is optional. It is set via menu “9.3.n.9 Encryption” on page 293. USB communication is never encrypted.

9.4.5 Listening port

Listening port is an IP port that is used for receiving uploading/downloading requests from the remote PC. The default listening port is 32000.
Caution: Incoming requests via GPRS are accepted only if the GPRS connection is permanent and never closes automatically. See “9.3.n.7.8 Disconn.time” on page 304 for more details.

9.4.6 Panel ID

6 Panel ID
> <

Use Panel ID to distinguish between a few panels when using them in one facility with Downloader connection.

PSTN specific options

9.4.1.n.3 Modem protocol

3 Modem protocol
> V.21<

The Modem protocol option allows you to select one of the following modem protocols: Bell-103, V.21, V.22 or V.22bis.

IP specific options

9.4.1.n.4 Destination/IP

l>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 127.

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

The Ping host command allows you to send a ping to the selected PC. This command is used to check if the PC is present and accessible from the panel in the network.

The Tx/Rx value indicates a number of packets sent and received.

GSM specific options

9.4.1.n.3 Conn. type

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.

9.5 UltraSync

The menu allows you to configure the UltraSync cloud communication.

See “UltraSync” on page 117 for details.

9.5.1 Connectivity

Enable or disable the UltraSync cloud connection.

9.5.2 SID number

The informational screen that shows the panel serial number.

9.5.3 Settings

The menu contains UltraSync connection settings.
9.5.3.1 Password

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

9.5.3.2 FW Upgrade

Enable or disable remote firmware upgrade.

9.5.3.3 Remote configuration

Enable or disable remote panel programming.

9.5.3.4 Notifications

Enable or disable smartphone push notifications.

Push notifications are configured in “9.5.4 Notification list” below.

9.5.4 Notification list

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

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

9.5.4.n Select notification

Select a notification to configure it.

9.5.4.n.1 Notification name

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

Use the menu to enter or change the push notification name. The push notification name can contain up to 16 characters.
9.5.4.n.2 Identifier

The informational screen that shows the smartphone notification identifier.

9.5.4.n.3 Assigned user

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

9.5.4.n.4 Notification events

The menu allows you to select event types that will generate the selected push notification.

If the option is enabled, any alarm is sent via push notification to the assigned user.

The following options are available:

- 1 Alarms
- 2 Set/unset
- 3 Power
- 4 System
- 5 Video
- 6 Fault
- 7 Access

Enable or disable the selected push notification for particular event types.

9.5.4.n.5 Delete notification

Use the menu to remove the selected push notification from the system. To remove the notification, select OK and press Enter again. The notification is deleted.
Chapter 6
Software

Summary
The chapter describes how to connect Advisor Advanced control panel to PC for programming and firmware upgrading.

Content
Programming Advisor Advanced via configuration software 314
Upgrading Advisor Advanced firmware 316
  Installing AAFlash on the PC 316
  Connecting Advisor Advanced to the PC 316
  Archiving current firmware and settings 317
  Upgrading Advisor Advanced firmware 317
  Upgrading bootloader 318
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 308 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 259). 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 257) expires, a new user authorization is required.
Upgrading Advisor Advanced firmware

The Advisor Advanced panel firmware is upgradeable via USB DFU (device firmware upgrade) interface. Use the AAFlash software to do that.

Access level 4 (manufacturer) applies when changing the operating program software and needs to be executed at the local programming site.

Downgrading is not permitted.

To receive the AAFlash software as well as the latest firmware, contact your supplier.

Installing AAFlash on the PC

If AAFlash is not installed on the PC, follow the steps below to install it.

To install AAFlash:

1. Ensure that Microsoft .Net 3.5 required by AAFlash has been installed on the PC. If not, use Microsoft Update to install it, or download it from the Microsoft web page and install manually.
2. Run Setup.exe from the AAFlash installation package.
3. Choose the installation directory and proceed with the installation by clicking Next, and then Install.
4. Finish the installation process by clicking Finish.

Connecting Advisor Advanced to the PC

To connect the panel to the PC for an upgrade:

1. Disconnect the mains power supply from the panel.
2. Open the panel housing and disconnect the battery.
3. Put on the T2 jumper.
4. Reconnect mains supply.
   - RX and TX diodes must start blinking. If they don’t, disconnect the power and then reconnect again.
5. Plug a USB cable plug into the Advisor Advanced PCB main board.
   - See “General installation information” on page 8 for more information.
After that, the USB LED turns on, the TX LED turns off, and the RX LED continues blinking.

If this is the first DFU connection, the system prompts you to find Advisor Advanced USB DFU drivers to install. Choose the driver located in the subdirectory “Driver” or the AAFlash program directory (C:\Program Files\AAFlash\driver by default).

A new USB controller, STM Device in DFU Mode, has been installed in the system.

The panel is ready for the firmware upgrade.

Archiving current firmware and settings

Caution: To prevent any potential failure during programming, installing or initializing new firmware or new feature, take care that the actual firmware (including settings) is archived, and can be reprogrammed.

To archive the panel firmware:

1. While connected to the 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.

Caution: If firmware upgrade procedure fails, restore the latest archived firmware.

4. Disconnect the USB cable from the panel main board, and then remove the T2 jumper.

The TX LED stops blinking. The panel is automatically restarted.
Upgrading bootloader

Particular panels with older bootloader firmware cannot be upgraded to a new firmware. In this case an upgrade of bootloader firmware to a newer version is required. Upgrade bootloader firmware as described below.

**Caution:** Bootloader is a crucial part of the Advisor Advanced panel. Make sure that the procedure is performed in the right order (steps 5 to 7), and the power supply is not removed while step 7 is in progress, otherwise the system can be damaged.

**To upgrade bootloader firmware:**

1. Install AAFlash version 2.3.0 or higher.
   
   See “Installing AAFlash on the PC” on page 316.
2. Run the panel in DFU mode.
   
   a. Disconnect the mains power and batteries from the panel.
   
   b. Put in the T2 jumper and plug a mini-B USB cable into the panel PCB.
   
   c. Reconnect mains power supply.

   The panel is running in DFU mode now, RX LED is blinking.

   If RX and TX LEDs are blinking alternately, the connected PC does not have the required driver installed. In this case, the system prompts you to find Advisor Advanced USB DFU drivers to install. Choose the driver located in the AAFlash program directory (“C:\Program Files(x86)\AAFlash\driver” by default).
3. Run AAFlash (version 2.3.0 or higher), click “...” (Browse), and open *.dfu file with bootloader provided.
4. Click Upgrade Bootloader.
5. **The program prompts to create backup of the existing application firmware and the database. Click Yes and create a new file for the backup, or No to skip this step.**

   If you click Yes, you are prompted to enter a name for a dfu file for the backup. Enter a file name and wait for the instructions to display.
6. Remove T2 jumper and unplug the USB cable.
7. Ensure that both mains power supply and the battery are connected.

   The image version is compared with the current bootloader version. If it is the same or older, the upgrade does not perform.

   Sectors of internal flash allocated for bootloader are erased and checked.

   New bootloader is flashed.

   After the operation is completed, the heartbeat LED starts blinking.
8. Insert T2 jumper and plug USB cable.
The panel restarts. It is now running in DFU mode with new bootloader firmware.

If the backup was created in the step 5, the panel starts to restore the existing application firmware and the database. Otherwise, it is now ready for a new firmware upgrade. See also “Upgrading Advisor Advanced firmware” on page 317.
Chapter 7
Troubleshooting

Summary
The chapter contains information on resolving known hardware and configuration problems. It also describes how to recover the system when the installer access is lost.

Content
Recovery procedure 322
Device troubleshooting 323
   Advisor Advanced control panel 323
   LCD keypads 324
   Remote expanders — Models ATS1201, ATS1210, ATS1211, ATS1220 324
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 161 and “2.2.1.n.3.5 Control areas” on page 162 for more details.
## Device troubleshooting

### Advisor Advanced control panel

<table>
<thead>
<tr>
<th>Condition</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>The LCD keypad has all LEDs flashing, and displays the “System Fault” message</td>
<td>The system data bus line may be connected incorrectly.</td>
</tr>
<tr>
<td></td>
<td>The address links on the keypad may be incorrectly set.</td>
</tr>
<tr>
<td>The panel is not communicating with keypads or expanders</td>
<td>The system data bus line may be connected incorrectly.</td>
</tr>
<tr>
<td></td>
<td>Keypad or expander numbers to be polled may not be programmed, or may not match the addresses set on the units.</td>
</tr>
<tr>
<td></td>
<td>There is an earth loop in cabling.</td>
</tr>
<tr>
<td>The keypads or expanders appear to be going offline and online (indicated by keypad or expander fail LED’s)</td>
<td>The system data bus line may be connected incorrectly.</td>
</tr>
<tr>
<td></td>
<td>The termination may be incorrect. TERM links may not have been removed where necessary. See “Cabling” on page 23.</td>
</tr>
<tr>
<td>Zone goes into alarm while the area is unset</td>
<td>The zone is wired incorrectly causing a tamper condition (open circuit or short circuit) instead of active condition. EOL resistors may be installed incorrectly.</td>
</tr>
<tr>
<td></td>
<td>See “Cabling” on page 23.</td>
</tr>
<tr>
<td>The panel is not reporting to the central station</td>
<td>The telephone line connections may be wired incorrectly. See “Cabling” on page 23.</td>
</tr>
<tr>
<td></td>
<td>The central station receiver does not support the programmed protocol.</td>
</tr>
<tr>
<td></td>
<td>The account number in “9.1.n.5 Accounts” on page 282 may be programmed incorrectly.</td>
</tr>
<tr>
<td></td>
<td>The phone number for the central station receiver is wrong.</td>
</tr>
<tr>
<td></td>
<td>No central station is programmed to report the event. See “9.1 Central station” on page 280.</td>
</tr>
<tr>
<td></td>
<td>The zone is not programmed to be reported. See “4.1.n.6.24 CS report” on page 197.</td>
</tr>
</tbody>
</table>
# LCD keypads

<table>
<thead>
<tr>
<th>Condition</th>
<th>Possible cause</th>
</tr>
</thead>
</table>
| All the LEDs on the keypad are flashing       | The DIP switches may be incorrectly set (the address set on the keypad may be incorrect and therefore polling to the keypad is not being acknowledged).  
                                            | The system data bus line may be connected incorrectly.  
                                            | The keypad is not being polled (it may not have been included in keypads to be polled when programming keypads). |
| LEDs do not appear to be indicating the correct condition | The keypad type may have been defined incorrectly:  
                                            | LCD keypad must be set to Yes.                                                                                                                   |
| The keypad appears to be going off-line and on-line (indicated by the "Keypad fail" message on the LCD) | The termination may be incorrect. See “Cabling” on page 23.                                                                                     |
| 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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Possible cause</th>
</tr>
</thead>
</table>
| 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.  
<pre><code>                                        | The system data bus cable may be connected incorrectly or the power supply is faulty (mains or battery).                                        |
</code></pre>
<p>| The expander appears to be going off-line and on-line (indicated by “Expander fail” on a LCD keypad) | The termination may be incorrect. See “Cabling” on page 23.                                                                                 |</p>
<table>
<thead>
<tr>
<th>Condition</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some or all expander zones are permanently in tamper (or permanently in alarm if “8.6.1 Input mode” on page 270 is set to Single NO or Single NC).</td>
<td>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 31. The end-of-line resistors are wrong or the wrong resistor value is programmed in “8.6.2 EOL” (see page 270). There is a problem with wiring the zones. To check the voltage or resistor values, see “Zone connection” on page 24. The ATS1202 expansion modules (if fitted) have the DIP switches incorrectly set.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expansion module:</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIP switch 1</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>DIP switch 2</td>
<td>Off</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DIP switch 3</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>DIP switch 4</td>
<td>not used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-way relay modules (ATS1811) or 16-way open collector modules (ATS1820) connected to the expander do not function</td>
<td>DIP switch B on the expander has not been set to On.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 8
Regulations

Summary
These pages describe settings and actions required by particular regulations and norms.

Content
Options affected by EN 50131 regulations  328
   EN 50131 Grade 2  328
   EN 50131 Grade 3  329
   EN 50136 policy  331
   Transmitter polling interval requirements  331
   EN 50131 Grade 3 certified components  332
   EN 50131 compliance precautions  333
Options affected by other regulations  334
   ACPO policy  334
   INCERT policy  334
   SES policy  334
   SBSC policy  335
Options affected by EN 50131 regulations

EN 50131 Grade 2

Required settings
The following options and values are mandatory for EN 50131-1 Grade 2 regulations.

- 1.2.6.n.3 Period, see “Transmitter polling interval requirements” on page 331.
- 2.2.1.n.3.3 View areas and 2.2.1.n.3.5 Control areas settings are identical
- 2.2.1.n.3.10 Buzzer silent, never
- 2.2.1.n.3.11 Quick set, off
- 2.2.1.n.3.12 Function keys, all set to None
- 2.2.1.n.3.17 ACK on keypad, set to None for non-LCD keypads
- 3.1.n.7.3 SMS control, disabled for all users
- 3.2.n.6 User group options, 25. No OP/CL reports option set to No
- 4.1.n.6.1 Inhibit, set to No for all zones with type 5. Panic, 6. 24H
- 4.1.n.6.6 Swinger shunt, set to Yes for all zones
- 4.1.n.6.26 ACK on keypad, set to None for all zones with type 9. Keyswitch
- 4.2.n.3 Entry time, 45 s maximum
- 4.2.n.5.1 Entry alarms, Instant
- 7.2.n.2 Active, set to No for all schedules.
- 8.1.2.1 Activation, external siren 90 to 900 s
- 8.1.2.2 Delay time, external siren 600 s maximum
- 8.1.3.1 Armed display, 30 s maximum
- 8.1.3.4 Mains reporting delay, 3600 s maximum
- 8.2.1 User code required, enabled
- 8.3.1 Armed display, always
- 8.3.3 Alarm list, disabled
- 8.4.1 RTS options, all enabled except zone technical alarm, which is optional
- 8.4.2 Inhibit includes, all allowed except engineer reset, which must be disabled
- 8.4.6 Pending alarms, enabled
- 8.6.4 Swinger shunt ≥ 3
- 8.6.5 Report restore, on ACK
- 8.7.8.1 Remote config, No
- 9.3.n.2 Line fault, enabled per path used
- 9.3.n.3 Line fault delay, 0 s

It is required to apply the following supervision settings for wireless DGPs:

- Short supervision: 20 minutes
- Long supervision: 2 hours
- Smoke supervision: 4 hours
Refer to appropriate sections and manuals.

**Caution:** When any option, any additional function or any additional zone type in this section does not comply with the EN 50131 requirements, the EN 50131 Grade 2 label must be removed from the system.

### Additional functions

The Wireless PIR Camera functionality brings along video verification feature, this additional function is fully available without compromise to standards the system complies to.

The Wireless PIR camera system consists of the following:

- Advisor Advanced series control panel
- ATS1238 Advanced Wireless DGP
- TX-2344-03-1 Wireless PIR Camera
- ATS73X0 GSM/GPRS Module

These PIR camera settings have no influence on EN 50131 compliance:

- 2.2.2.n.4.9.1.1.2 Frame rate for all event types
- 2.2.2.n.4.9.1.1.3 Pic resolution for all event types
- 2.2.2.n.4.9.3 Pic auto deletion
- 4.5 Cameras
- 9.1.n.4.5 Vid dest port
- 9.3.n.10 Max Pics 24h, 9.3.n.7.9 Max Pics 24h

### EN 50131 Grade 3

### Required settings

The following options and values are mandatory for EN 50131-1 Grade 3 regulations:

- All Grade 2 required settings (see “EN 50131 Grade 2” on page 328).
- PIN length should be 6 digits minimum. See also “8.7.4 PIN length”.
- 3.2.n.6 User group options, set (6) Isolate, (22) SMS reporting, (23) SMS control to No for all user groups except Installer.
- 4.1.n.6.7 Anti mask, set to Yes for all I&HAS movement detectors
- 8.1.3.1 Armed display, set to 00’00
- 8.3.5 View EE timer, set to Off
- 8.4.1 RTS options, set Zone masking condition to Yes
- 8.4.2 Inhibit includes, set Zone masking condition to Access Level 2
- Battery test should be performed daily. See “1.2.9 Battery test” on page 151 for details.

The following features are not allowed (not evaluated):

- Keyswitch zone types to set and unset the system. See “Zone types” on page 47.
- Presetting indication and any automatic override of set prevention.
Refer to Table 29 below for all supported options for notification requirements.

<table>
<thead>
<tr>
<th>Notification equipment (Alarm reporting)</th>
<th>Grade 3 options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Remotely powered audible WD</td>
<td>2</td>
</tr>
<tr>
<td>Self-powered audible WD</td>
<td>Optional</td>
</tr>
<tr>
<td>Main ATS [1]</td>
<td>ATS 4</td>
</tr>
<tr>
<td>Additional ATS [1]</td>
<td>Optional</td>
</tr>
</tbody>
</table>

[1] Requirement according to EN 50136:2010
[3] Primary Path — SP4, backup path — SP2

Legend:
- ATS: Alarm transmission system
- SP: Single path alarm transmission system
- DP: Dual path alarm transmission system

The key variations of cards and keys are the following:

Both
- ATS1471 (1 pc.) and ATS1477 (10 pcs.) tags as well as
- ATS1475 (10 pcs.) card badges

have a number of key variations of 67 million minimum.

Both make use of 26 bit (to 48 bit) Hitag protocol.

The installer (user level 3) commissions the system with appropriate additional functions.

The end-user (user level 2) is able to make use of all these functions.

The Installer can only make use of these functions when he has an access granted by end-user.

**RAS required setting**

The keypad/RAS must be mounted within the secure premises, on the entry/exit route.

Each arming scenario described below meets EN 50131 requirements.

- 2.2.1.n.3.7.1 Card&PIN mode: Card and PIN always
  - Note: This setting must be applied manually by the installer after the appropriate cards are defined in the system.
- 2.2.1.n.3.7.3 1 x set/unset: Off
- 2.2.1.n.3.7.4 3 x badge set: Set
- 2.2.1.n.3.11 Quick set: Off
- 4.1.n.6.18 Key unset: Off
• 8.4.4 Forced set: Off
• 8.4.7 AS fault retry: 15 minutes
• 8.4.8 AS user retry: Disable

See also the appropriate RAS manual for more details.

EN 50136 policy

Required settings:
• “9.1.n.7 Retry count”: 1
• “9.1.n.8.3.2 Heartbeat time”: According Table 30 below.
• “9.1.n.8.3.5 Freq. HB time”: According Table 30 below.
• “9.3.n.7.1 Firewall”: Yes
• “9.3.n.7.2 Reply on PING”: No
• “9.3.n.7.6.1 Firewall”: Yes
• “9.3.n.7.6.2 Reply on PING”: No
• “9.3.n.9 Encryption”: Yes
• “9.4.3 Encryption key 1” must be set.

See also “Transmitter polling interval requirements” below.

Transmitter polling interval requirements

Transmitter polling interval must be set according to specified requirements for different alarm transmission systems (ATS). Table 30 below lists all required settings for the appropriate standards and diallers.

Table 30: Transmitter polling settings

<table>
<thead>
<tr>
<th>Standard and category</th>
<th>Required polling interval</th>
<th>Comm. path and dialler</th>
<th>Option</th>
<th>Required value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 50136:2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP2</td>
<td>25 h</td>
<td>PSTN via ATS7700 and GPRS (backup) via ATS73X0</td>
<td>1.2.6.n.3 Period</td>
<td>24</td>
</tr>
<tr>
<td>SP3</td>
<td>30 min</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:29'00</td>
</tr>
<tr>
<td>SP4</td>
<td>3 min</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:02'30</td>
</tr>
<tr>
<td>SP5</td>
<td>90 s</td>
<td>IP built-in</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:01'00</td>
</tr>
<tr>
<td>SP6</td>
<td>20 s</td>
<td>IP built-in</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:00'10</td>
</tr>
<tr>
<td>EN 50136:2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATS2 (T2), ATS3 (T2)</td>
<td>25 h</td>
<td>PSTN via ATS7700 and GPRS (backup) via ATS73X0</td>
<td>1.2.6.n.3 Period</td>
<td>24</td>
</tr>
<tr>
<td>ATS4 (T3)</td>
<td>300 min</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>04:55'00</td>
</tr>
</tbody>
</table>
### EN 50131 Grade 3 certified components

The Advisor Advanced EN 50131 Grade 3 system exists out the following components.

#### Intrusion control panels

- **ATS3500A(-IP):** Control panel

**Note:** In case of ATS1500A(-IP) panel, the system with peripherals listed below will be Grade 2 certified.

#### Keypads / readers (RAS, remote arming station)

Panel can support up to 8 or 16 RAS devices at the same time, depending on intrusion panel, regardless of type (independent of other expanders).

- **ATS1135:** LCD keypad
- **ATS1190/1192:** Smart Card reader
- **ATS1151/ATS1156:** Keypad

#### Remote expanders (DGP, data gathering panel)

Panel can support up to 7 or 15 DGP devices, depending on intrusion panel, regardless of type (independent of other expanders).

- **ATS1201E:** 8 to 32 zone DGP expander with 3 A PSU, small enclosure, EN 50131 Grade 3
- **ATS1203E:** 8 to 32 zone DGP expander with 3 A PSU, medium enclosure, EN 50131 Grade 3
- **ATS1204E:** 8 to 32 zone DGP expander with 3 A PSU, large enclosure, EN 50131 Grade 3

#### I/O expanders

Panel can support up to 3 I/O devices depending on the type.

- **ATS608:** Plug in 8-zone expander
- **ATS624:** 4 relay board
- **ATS626:** 16 open collector output board

---

<table>
<thead>
<tr>
<th>Standard and category</th>
<th>Required polling interval</th>
<th>Comm. path and dialler</th>
<th>Option</th>
<th>Required value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATS5 (T4)</td>
<td>180 s</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:02'30</td>
</tr>
<tr>
<td>ATS6 (T6)</td>
<td>20 s</td>
<td>IP built-in</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:00'10</td>
</tr>
<tr>
<td>LPS1277: Issue 3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATS4Plus</td>
<td>10 min</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:09'00</td>
</tr>
</tbody>
</table>
Reporting devices
Panel can support 1 GSM device connected onto MI bus.

- ATS7310: GSM communication device
- ATS7320: GSM communication device
- ATS7440: IP/GPRS alarm dialer
- ATS7700: PSTN interfance board

When any option, any additional function or any additional zone type in this section does not comply with the EN 50131 requirements, the EN 50131 Grade 3 label must be removed from the system. See also “EN 50131 compliance precautions” below.

EN 50131 compliance precautions

Installation
In order to install an EN 50131 compliant system, please make sure that all system components are EN 50131 compliant. See “EN 50131 Grade 3 certified components” on page 332 for more details.

Programming
Make sure that all system settings are in line with regulatory compliance guidelines. See “EN 50131 Grade 3” on page 329 for more details.

Size of log / event history
For full EN 50131 Grade 3 compliance, the system must store at least 500 events.

Marking
It is only allowed to mark the system with the EN 50131 Grade 3 label, if the following requirements are met:

- All system components are EN 50131 compliant. Refer to “EN 50131 Grade 3 certified components” on page 332.
- All settings are done according to “EN 50131 Grade 3” on page 329.

If any of these two items is not valid, the EN 50131 Grade 3 label must be removed from the system.
Options affected by other regulations

ACPO policy

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

- 4.2.n.5.1 Entry alarms, Delayed
- 8.2.4 Engineer reset, tamper enabled
- 8.7.6 Alarm confirm:
  - AB mode, enabled for all relevant areas
  - AB time, 30 min minimum, 60 min maximum
  - EE Confirm, enabled
  - TA confirm, enabled

Note: ACPO policy allows a higher level manager to become a level 3 user. Also, level 3 user menu access may be allowed without level 2 user authorization if it is provided by appropriate written agreement from the customer.

INCERT policy

Required settings:

- Isolate for End Users option disabled in 3.2.n.6 User group options
- Full Set/Part Set/Unset/Forced Set for Installer disabled in 3.2.n.6 User group options
- 8.2.4 Engineer reset, tamper enabled
- 8.4.1 RTS options, all enabled except FTC, Pending Alarms, and Zone technical alarm, that are optional
- RTS for Battery Fault enabled in 8.4.1 RTS options
- Inhibit for Battery Fault disabled in 8.4.2 Inhibit includes
- PIN length should be 6 digits minimum. See also “8.7.4 PIN length”.

SES policy

Depending on the SES default chosen, the following SES settings are required on top of EN 50131 Grade 2 / Grade 3.

- Take care that a proper dedicated panic button is used (which cannot be pushed by accident).
- Automatic unsetting is not allowed.
• For SES Grade 3 is not allowed to program GPRS communication as primary CS, it is only allowed in Grade 2.

• The table below indicates the required polling intervals for SES Grade 2 and Grade 3.

<table>
<thead>
<tr>
<th>Primary CS (IP)</th>
<th>AÜA-B25 25 h</th>
<th>AÜA-B5 5 h</th>
<th>AÜA-S180 180 sec</th>
<th>AÜA-S20 20 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back-up CS (GPRS)</td>
<td>AÜA-B25 25 h</td>
<td>2</td>
<td>2, 3</td>
<td>2, 3</td>
</tr>
<tr>
<td></td>
<td>AÜA-B5 5 h</td>
<td>2</td>
<td>2, 3</td>
<td>2, 3</td>
</tr>
</tbody>
</table>

* 2, 3: EN-CH Grade of the system

• The following options must be set:

<table>
<thead>
<tr>
<th>Standard and category</th>
<th>Required polling interval</th>
<th>Comm. path and dialler</th>
<th>Option</th>
<th>Required value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SES CHD.07 (V3 / 01.01.2011)</td>
<td>AÜA-B25 25 h</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>AÜA-B5 5 h</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>AÜA-S180 180 s</td>
<td>IP built-in, or GPRS via ATS73X0</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:02'30</td>
</tr>
<tr>
<td></td>
<td>AÜA-S20 20 s</td>
<td>IP built-in</td>
<td>9.1.n.8.3.2 Heartbeat time</td>
<td>00:00'10</td>
</tr>
</tbody>
</table>

SBSC policy

Larmklass 1

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

• 4.2.n.5.1 Entry alarms: Instant
• 8.7.6.9 Reporting delayed: No

See also “EN 50131 Grade 2” on page 328.

Larmklass 2

Required settings are all EN 50131 Grade 3 settings with the following modifications:

• 4.2.n.5.1 Entry alarms: Instant
• 8.7.6.9 Reporting delayed: No

See also “EN 50131 Grade 3” on page 329.
Appendix A
Advisor Advanced events

For Advisor Advanced system events, see Table 31 below. For access control events, used to program door controllers, see Table 32 on page 349.

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>ACTIVE</td>
<td>1</td>
<td>Zone active</td>
<td>Zone in active state</td>
</tr>
<tr>
<td>TAMPER</td>
<td>2</td>
<td>Zone tamper</td>
<td>Zone in tamper state</td>
<td></td>
</tr>
<tr>
<td>AM</td>
<td>3</td>
<td>Zone masking</td>
<td>Zone in anti-mask alarm state</td>
<td></td>
</tr>
<tr>
<td>BATTFAULT</td>
<td>4</td>
<td>Zone battery fault</td>
<td>Zone in battery fault state</td>
<td></td>
</tr>
<tr>
<td>FAULT</td>
<td>5</td>
<td>Zone fault</td>
<td>Zone in fault state</td>
<td></td>
</tr>
<tr>
<td>DIRTY</td>
<td>6</td>
<td>Zone dirty</td>
<td>Zone in dirty state</td>
<td></td>
</tr>
<tr>
<td>SVSHORT</td>
<td>7</td>
<td>Zone supervision short</td>
<td>Zone in short supervision state</td>
<td></td>
</tr>
<tr>
<td>SVLONG</td>
<td>8</td>
<td>Zone supervision long</td>
<td>Zone in short supervision state</td>
<td></td>
</tr>
<tr>
<td>INHIBIT</td>
<td>9</td>
<td>Zone inhibited</td>
<td>Zone state changed to inhibited</td>
<td></td>
</tr>
<tr>
<td>ISOLATE</td>
<td>10</td>
<td>Zone isolated</td>
<td>Zone state changed to isolated</td>
<td></td>
</tr>
<tr>
<td>SOAK</td>
<td>11</td>
<td>Zone in soak test</td>
<td>Soak test is active</td>
<td></td>
</tr>
<tr>
<td>SET</td>
<td>12</td>
<td>Zone set</td>
<td>Zone in Part set or Full set mode</td>
<td></td>
</tr>
<tr>
<td>ALARM</td>
<td>13</td>
<td>Zone in alarm</td>
<td>Zone in alarm. Restores after alarm acknowledgement.</td>
<td></td>
</tr>
<tr>
<td>RF learned</td>
<td>14</td>
<td>Wireless device programmed</td>
<td>Active for 3 seconds after a successful programming</td>
<td></td>
</tr>
<tr>
<td>RF signal accept</td>
<td>15</td>
<td>Wireless device found</td>
<td>Active for 3 seconds after device response</td>
<td></td>
</tr>
<tr>
<td>Held Open</td>
<td>16</td>
<td>Zone is open too long</td>
<td>Zone is held open</td>
<td></td>
</tr>
<tr>
<td>Inactive days</td>
<td>17</td>
<td>Zone inverted walk test failed</td>
<td>Zone has been inactive for longer than inactive day limit</td>
<td></td>
</tr>
<tr>
<td>SHUNT</td>
<td>18</td>
<td>Zone shunted</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix A: Advisor Advanced events

#### SHUNT FAULT
- **Event #:** 19
- **Event Description:** Zone shunt fault
- **Notes:** Fault — zone is active when unshunt

#### DOOR SHUNT
- **Event #:** 20
- **Event Description:** Door shunt
- **Notes:** Zone shunt by door shunt

#### DSHUNTWARN
- **Event #:** 21
- **Event Description:** Door shunt warning
- **Notes:** Zone in shunt warning time by door shunt

## Group | Event | # | Event description | Notes
---|---|---|---|---
Area | FULLSET | 1 | Area full set | Area is in full set state
| PARTSET1 | 2 | Area part set 1 | Area is in part set 1 state
| UNSET | 3 | Area unset | Area is in unset state
| ALARM | 4 | Intrusion alarm | Area Intrusion alarm is active
| FSALARM | 5 | Alarm during full set | Area alarm while in full set
| PSALARM | 6 | Alarm during part set | Area alarm while in part set
| USALARM | 7 | Alarm during unset | Area alarm while unset
| FTCALARM | 8 | Alarm and FTC | Area alarm while FTC present
| FIREDOOR | 9 | Fire door active | A fire door local alarm is active
| FSFIREDOOR | 10 | Fire door during full set | A fire door active while area full set
| PSFIREDOOR | 11 | Fire door during part set | A fire door active while area part set
| USFIREDOOR | 12 | Fire door during unset | A fire door active while area unset
| FTCFIREDOOR | 13 | Fire door and FTC | A fire door active while FTC present
| FIRE | 14 | Fire alarm | A fire alarm active
| FSFIRE | 15 | Fire alarm during full set | A fire alarm active while area full set
| PSFIRE | 16 | Fire alarm during part set | A fire alarm active while area part set
| USFIRE | 17 | Fire alarm during unset | A fire alarm active while area unset
| FTCFIRE | 18 | Fire alarm and FTC | A fire alarm active while FTC present
| PANIC | 19 | Panic alarm | A panic alarm active
| FSPANIC | 20 | Panic during full set | A panic alarm active while area full set
| PSPANIC | 21 | Panic during part set | A panic alarm active while area part set
| USPANIC | 22 | Panic during unset | A panic alarm active while area unset
<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTCPANIC</td>
<td>Panic and FTC</td>
<td>23</td>
<td>A panic alarm active while FTC present</td>
<td></td>
</tr>
<tr>
<td>MEDICAL</td>
<td>Medical alarm</td>
<td>24</td>
<td>A medical alarm active</td>
<td></td>
</tr>
<tr>
<td>FSMEDICAL</td>
<td>Medical during full set</td>
<td>25</td>
<td>A medical alarm active while area full set</td>
<td></td>
</tr>
<tr>
<td>PSMEDICAL</td>
<td>Medical during part set</td>
<td>26</td>
<td>A medical alarm active while area part set</td>
<td></td>
</tr>
<tr>
<td>USMEDICAL</td>
<td>Medical during unset</td>
<td>27</td>
<td>A medical alarm active while area unset</td>
<td></td>
</tr>
<tr>
<td>FTCMEDICAL</td>
<td>Medical and FTC</td>
<td>28</td>
<td>A medical alarm active while FTC present</td>
<td></td>
</tr>
<tr>
<td>TECHNICAL</td>
<td>Technical alarm</td>
<td>29</td>
<td>A technical alarm active</td>
<td></td>
</tr>
<tr>
<td>FSTECHNICAL</td>
<td>Technical during full set</td>
<td>30</td>
<td>A technical alarm active while area full set</td>
<td></td>
</tr>
<tr>
<td>PSTECHNICAL</td>
<td>Technical during part set</td>
<td>31</td>
<td>A technical alarm active while area part set</td>
<td></td>
</tr>
<tr>
<td>USTECHNICAL</td>
<td>Technical during unset</td>
<td>32</td>
<td>A technical alarm active while area unset</td>
<td></td>
</tr>
<tr>
<td>FTCTECHNICAL</td>
<td>Technical and FTC</td>
<td>33</td>
<td>A technical alarm active while FTC present</td>
<td></td>
</tr>
<tr>
<td>TAMPER</td>
<td>Tamper alarm</td>
<td>34</td>
<td>A tamper alarm active</td>
<td></td>
</tr>
<tr>
<td>FSTEMPER</td>
<td>Tamper during full set</td>
<td>35</td>
<td>A tamper alarm active while area set</td>
<td></td>
</tr>
<tr>
<td>PSTEMPER</td>
<td>Tamper during part set</td>
<td>36</td>
<td>A tamper alarm active while area part set</td>
<td></td>
</tr>
<tr>
<td>USTEMPER</td>
<td>Tamper during unset</td>
<td>37</td>
<td>A tamper alarm active while area unset</td>
<td></td>
</tr>
<tr>
<td>FTCTEMPER</td>
<td>Tamper and FTC</td>
<td>38</td>
<td>A tamper alarm active while FTC present</td>
<td></td>
</tr>
<tr>
<td>CHIME</td>
<td>Chime</td>
<td>39</td>
<td>Active for 2 sec when zone with chime option is active</td>
<td></td>
</tr>
<tr>
<td>PSCHIME</td>
<td>Chime during part set</td>
<td>40</td>
<td>Active for 2 sec when zone with chime option is active during part set</td>
<td></td>
</tr>
<tr>
<td>USCHIME</td>
<td>Chime during unset</td>
<td>41</td>
<td>Active for 2 sec when zone with chime option is active during unset</td>
<td></td>
</tr>
<tr>
<td>ZNACTIVE</td>
<td>Zone active</td>
<td>42</td>
<td>At least one zone in the area is in active state</td>
<td></td>
</tr>
<tr>
<td>ZNINHIBIT</td>
<td>Zone inhibit</td>
<td>43</td>
<td>At least one zone in the area is inhibited</td>
<td></td>
</tr>
<tr>
<td>ZNISOLATE</td>
<td>Zone isolate</td>
<td>44</td>
<td>At least one zone in the area is isolated</td>
<td></td>
</tr>
<tr>
<td>ZNFAULT</td>
<td>Zone fault</td>
<td>45</td>
<td>At least one zone in the area is in fault state</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Event</td>
<td>#</td>
<td>Event description</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>----</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>ZNAM</td>
<td>Zone masking</td>
<td>46</td>
<td>At least one zone in the area is in anti-mask alarm state</td>
<td></td>
</tr>
<tr>
<td>ZNTAMPER</td>
<td>Zone tamper</td>
<td>47</td>
<td>At least one zone in the area is in tamper state</td>
<td></td>
</tr>
<tr>
<td>KEYPADTAMPER</td>
<td>Keypad tamper</td>
<td>48</td>
<td>A keypad assigned to the area is in tamper state</td>
<td></td>
</tr>
<tr>
<td>KEYPADFAULT</td>
<td>Keypad fault</td>
<td>49</td>
<td>A keypad assigned to the area is in fault state</td>
<td></td>
</tr>
<tr>
<td>EXPANDERTAMPER</td>
<td>Expander tamper</td>
<td>50</td>
<td>An expander assigned to the area is in tamper state</td>
<td></td>
</tr>
<tr>
<td>EXPANDERFAULT</td>
<td>Expander fault</td>
<td>51</td>
<td>An expander assigned to the area is in fault state</td>
<td></td>
</tr>
<tr>
<td>DURESS</td>
<td>Duress</td>
<td>52</td>
<td>Duress code used in the area</td>
<td></td>
</tr>
<tr>
<td>FSDURESS</td>
<td>Duress during full set</td>
<td>53</td>
<td>Duress code used while area full set</td>
<td></td>
</tr>
<tr>
<td>PSDURESS</td>
<td>Duress during part set</td>
<td>54</td>
<td>Duress code used while area part set</td>
<td></td>
</tr>
<tr>
<td>USDURESS</td>
<td>Duress during unset</td>
<td>55</td>
<td>Duress code used while area unset</td>
<td></td>
</tr>
<tr>
<td>FTCDURESS</td>
<td>Duress and FTC</td>
<td>56</td>
<td>Duress code used while FTC present</td>
<td></td>
</tr>
<tr>
<td>CODETAMPER</td>
<td>Code tamper</td>
<td>57</td>
<td>Active when a keypad assigned to the area is locked for 2 minutes due to 3 wrong PIN entries</td>
<td></td>
</tr>
<tr>
<td>ENTRY</td>
<td>Area entry</td>
<td>58</td>
<td>Area entry time is active</td>
<td></td>
</tr>
<tr>
<td>EXIT</td>
<td>Area exit</td>
<td>59</td>
<td>Area exit time is active</td>
<td></td>
</tr>
<tr>
<td>EXITFAULT</td>
<td>Exit fault</td>
<td>60</td>
<td>Alarm detected during exit state before changing to part or full set state</td>
<td></td>
</tr>
<tr>
<td>RTS</td>
<td>Ready To Set</td>
<td>61</td>
<td>Active when all configured RTS conditions are valid</td>
<td></td>
</tr>
<tr>
<td>SETOK</td>
<td>Area set OK</td>
<td>62</td>
<td>Active for 2 s when area set successfully</td>
<td></td>
</tr>
<tr>
<td>SETFAULT</td>
<td>Area set failed</td>
<td>63</td>
<td>Active during 30 s after unsuccessful area setting</td>
<td></td>
</tr>
<tr>
<td>UNSETOK</td>
<td>Area unset OK</td>
<td>64</td>
<td>Active for 2 sec when area has been unset</td>
<td></td>
</tr>
<tr>
<td>ALARMACK</td>
<td>Alarms to ACK</td>
<td>65</td>
<td>Alarms present waiting for acknowledge</td>
<td></td>
</tr>
<tr>
<td>FIRERESET</td>
<td>Fire reset</td>
<td>66</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Event</td>
<td>#</td>
<td>Event description</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
<td>----</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>WALK</td>
<td>Walk test</td>
<td>67</td>
<td>User/Installer Walk test is active</td>
<td></td>
</tr>
<tr>
<td>WALKZNACTV</td>
<td>Walk test zone</td>
<td>68</td>
<td>Zone in walk test is activated</td>
<td></td>
</tr>
<tr>
<td>A-ALARM</td>
<td>A-Alarm</td>
<td>69</td>
<td>A-alarm active (unconfirmed alarm), reset after unset or expiration of AB timer and no B-alarm.</td>
<td></td>
</tr>
<tr>
<td>B-ALARM</td>
<td>B-Alarm</td>
<td>70</td>
<td>B-alarm active (confirmed alarm). Reset after unset</td>
<td></td>
</tr>
<tr>
<td>ISIREN</td>
<td>Internal siren</td>
<td>71</td>
<td>Internal siren. Activated on alarm during the internal siren time. Activation may be delayed by Siren delay time. Can be retriggered by next alarm.</td>
<td></td>
</tr>
<tr>
<td>ESIREN</td>
<td>External siren</td>
<td>72</td>
<td>External siren. Activated on alarm during the external siren time. Activation may be delayed by Siren delay time. This flag can not be retriggered.</td>
<td></td>
</tr>
<tr>
<td>STROBE</td>
<td>Strobe output</td>
<td>73</td>
<td>Strobe output. Activated by alarm during Set. Deactivated after unset.</td>
<td></td>
</tr>
<tr>
<td>BUZZER</td>
<td>Buzzer output</td>
<td>74</td>
<td>Buzzer output flag</td>
<td></td>
</tr>
<tr>
<td>AMRESET</td>
<td>AM reset</td>
<td>75</td>
<td>Activated during set procedure to reset AM detectors</td>
<td></td>
</tr>
<tr>
<td>PARTSET2</td>
<td>Area part set 2</td>
<td>76</td>
<td>Area is in part set 2 state.</td>
<td></td>
</tr>
<tr>
<td>AS_WARNING</td>
<td>Autoset warning</td>
<td>77</td>
<td>Area in warning state prior to autoset</td>
<td></td>
</tr>
<tr>
<td>AUTO_SET</td>
<td>Autoset</td>
<td>78</td>
<td>Autoset procedure is in progress</td>
<td></td>
</tr>
<tr>
<td>HA-ALARM</td>
<td>A hold-up alarm</td>
<td>79</td>
<td>Reset after unset</td>
<td></td>
</tr>
<tr>
<td>HB-ALARM</td>
<td>B hold-up alarm</td>
<td>80</td>
<td>Reset after unset</td>
<td></td>
</tr>
<tr>
<td>ZNINH LIMIT</td>
<td>Inhibit limit</td>
<td>81</td>
<td>Zone inhibit limit is reached</td>
<td></td>
</tr>
<tr>
<td>ZNISOL LIMIT</td>
<td>Isolation limit</td>
<td>82</td>
<td>Zone isolation limit is reached</td>
<td></td>
</tr>
<tr>
<td>ZNSHT LIMIT</td>
<td>Shunt limit</td>
<td>83</td>
<td>Zone shunt limit is reached</td>
<td></td>
</tr>
<tr>
<td>ZNISOL FAULT</td>
<td>Faulty zone</td>
<td>84</td>
<td>Faulty zone isolated</td>
<td></td>
</tr>
<tr>
<td>UNSETDELAY</td>
<td>ATM unset delay</td>
<td>85</td>
<td>ATM unset delay is active</td>
<td></td>
</tr>
<tr>
<td>UNSETTIME</td>
<td>ATM unset time</td>
<td>86</td>
<td>ATM unset time is active</td>
<td></td>
</tr>
<tr>
<td>UNSETWARNTIME</td>
<td>ATM unset warning</td>
<td>87</td>
<td>ATM unset warning time is active</td>
<td></td>
</tr>
<tr>
<td>UNSETTEXTTIME</td>
<td>ATM extended unset time</td>
<td>88</td>
<td>Extended ATM unset time is active</td>
<td></td>
</tr>
<tr>
<td>AREA DSHUNT</td>
<td>Door shunt</td>
<td>89</td>
<td>A zone in the area is shunted</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Event</td>
<td>#</td>
<td>Event description</td>
<td>Notes</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------</td>
<td>----</td>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>AREA DSHUNTWARN</td>
<td>90</td>
<td>Door shunt warning</td>
<td>A zone in the area is in shunt warning time</td>
<td></td>
</tr>
<tr>
<td>UNSETDELAYED</td>
<td>91</td>
<td>Unset delayed</td>
<td>Area unset delayed</td>
<td></td>
</tr>
<tr>
<td>PROHIBITUNSET</td>
<td>92</td>
<td>Prohibit unset</td>
<td>User unset prohibited</td>
<td></td>
</tr>
<tr>
<td>ZNSHUNT</td>
<td>93</td>
<td>Zone shunted</td>
<td>A zone in the area is shunted</td>
<td></td>
</tr>
<tr>
<td>SHUNTFault</td>
<td>94</td>
<td>Faulty zone shunted</td>
<td>A zone in the area is in the shunt fault state</td>
<td></td>
</tr>
<tr>
<td>SENSRESET</td>
<td>95</td>
<td>Sensor reset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCH ACTIVE</td>
<td>96</td>
<td>Schedule active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIOTAMPER</td>
<td>98</td>
<td>Audio device tamper</td>
<td>An audio device assigned to the area is in tamper state</td>
<td></td>
</tr>
<tr>
<td>AUDIOFAULT</td>
<td>99</td>
<td>Audio device fault</td>
<td>An audio device assigned to the area is in the fault state</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keypad</td>
<td>OFFLINE</td>
<td>1</td>
<td>Keypad is offline</td>
<td>Active if a keypad is offline</td>
</tr>
<tr>
<td></td>
<td>RTE</td>
<td>2</td>
<td>RTE triggered</td>
<td>Keypad RTE input triggered</td>
</tr>
<tr>
<td></td>
<td>CODETAMPER</td>
<td>3</td>
<td>Code tamper</td>
<td>Active when a keypad is locked for 2 minutes due to 3 wrong PIN entries</td>
</tr>
<tr>
<td></td>
<td>TAMPER</td>
<td>4</td>
<td>Keypad tamper</td>
<td>Keypad tamper</td>
</tr>
<tr>
<td></td>
<td>DURESS</td>
<td>5</td>
<td>Duress code</td>
<td>Duress code entered on this keypad</td>
</tr>
<tr>
<td></td>
<td>ACTIVE CARD</td>
<td>6</td>
<td>Badged card</td>
<td>A card is badged on this keypad, active for 3 s</td>
</tr>
<tr>
<td></td>
<td>PIN</td>
<td>7</td>
<td>Valid PIN</td>
<td>Valid PIN entered on this keypad, active for 3 s</td>
</tr>
<tr>
<td></td>
<td>DOORACC</td>
<td>8</td>
<td>Valid PIN or card</td>
<td>Valid PIN or card entered on this keypad, active for 3 s</td>
</tr>
<tr>
<td></td>
<td>LOCKED</td>
<td>9</td>
<td>Keypad is locked</td>
<td>Code tamper. It restores after the timeout has expired.</td>
</tr>
<tr>
<td></td>
<td>ISOLATED</td>
<td>10</td>
<td>Keypad is isolated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHIME</td>
<td>11</td>
<td>Keypad chime active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VALID CARD</td>
<td>12</td>
<td>Valid card</td>
<td>Valid card entered on this keypad, active for 3 s</td>
</tr>
<tr>
<td></td>
<td>EXIT STARTED</td>
<td>13</td>
<td>Exit time started</td>
<td>Exit time started during set from the selected keypad</td>
</tr>
<tr>
<td></td>
<td>ENTRY STOPPED</td>
<td>14</td>
<td>Entry time stopped</td>
<td>Entry time stopped during unset from the selected keypad</td>
</tr>
<tr>
<td></td>
<td>UNKNOWN CARD</td>
<td>15</td>
<td>Card is not recognized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCH ACTIVE</td>
<td>16</td>
<td>Schedule active</td>
<td></td>
</tr>
</tbody>
</table>
### Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expander</td>
<td>OFFLINE</td>
<td>1</td>
<td>Expander is offline</td>
<td>Active if device is offline</td>
</tr>
<tr>
<td></td>
<td>MAINSFAULT</td>
<td>2</td>
<td>Mains fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BATTERYFAULT</td>
<td>3</td>
<td>Battery fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TAMPER</td>
<td>4</td>
<td>Expander tamper</td>
<td>Device tamper</td>
</tr>
<tr>
<td></td>
<td>FUSEFAULT</td>
<td>5</td>
<td>Fuse fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIRENFAULT</td>
<td>6</td>
<td>Siren fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCVFAULT</td>
<td>7</td>
<td>Receiver fault</td>
<td>Wireless expander receiver fault</td>
</tr>
<tr>
<td></td>
<td>ISOLATED</td>
<td>8</td>
<td>Expander isolated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BATTLOW</td>
<td>9</td>
<td>Battery low</td>
<td>Expander battery is low</td>
</tr>
<tr>
<td></td>
<td>BTESTACTV</td>
<td>10</td>
<td>Battery test active</td>
<td>Expander battery test is active</td>
</tr>
<tr>
<td></td>
<td>BTESTFAIL</td>
<td>11</td>
<td>Battery test failed</td>
<td>Expander battery test failed</td>
</tr>
<tr>
<td></td>
<td>POWER UNIT FA</td>
<td>12</td>
<td>Expander PSU fail</td>
<td></td>
</tr>
<tr>
<td>Panel</td>
<td>MAINSFAULT</td>
<td>1</td>
<td>Mains fault</td>
<td>Panel mains fault detected</td>
</tr>
<tr>
<td></td>
<td>BATTERYFAULT</td>
<td>2</td>
<td>Battery fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TAMPER</td>
<td>3</td>
<td>Panel tamper</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FUSEFAULT</td>
<td>4</td>
<td>Panel fuse fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIRENFAULT</td>
<td>5</td>
<td>Panel siren fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LF</td>
<td>6</td>
<td>Line fault</td>
<td>A line fault is detected</td>
</tr>
<tr>
<td></td>
<td>LFPSTN</td>
<td>7</td>
<td>PSTN line fault</td>
<td>PSTN line fault detected</td>
</tr>
<tr>
<td></td>
<td>LFISDN</td>
<td>8</td>
<td>ISDN line fault</td>
<td>ISDN line fault detected</td>
</tr>
<tr>
<td></td>
<td>LGSM</td>
<td>9</td>
<td>GSM line fault</td>
<td>GSM line fault detected</td>
</tr>
<tr>
<td></td>
<td>FTC</td>
<td>10</td>
<td>Failed To Communicate</td>
<td>Failed to deliver an alarm message</td>
</tr>
<tr>
<td></td>
<td>MIFAULT</td>
<td>11</td>
<td>Line fault PSTN</td>
<td>MI Bus communication fault</td>
</tr>
<tr>
<td></td>
<td>MIFISDN</td>
<td>12</td>
<td>Line fault ISDN</td>
<td>ISDN dialler fault</td>
</tr>
<tr>
<td></td>
<td>MIFGSM</td>
<td>13</td>
<td>Line fault GSM</td>
<td>GSM dialler fault</td>
</tr>
<tr>
<td></td>
<td>MIFVOICE</td>
<td>14</td>
<td>Failed To Communicate</td>
<td>Voice module fault</td>
</tr>
<tr>
<td></td>
<td>NTPFAULT</td>
<td>15</td>
<td>NTP server connection fault</td>
<td>NTP server connection fault</td>
</tr>
<tr>
<td></td>
<td>LFETH</td>
<td>16</td>
<td>Ethernet line fault</td>
<td>Ethernet connection fault</td>
</tr>
<tr>
<td></td>
<td>LFIP</td>
<td>17</td>
<td>IP fault</td>
<td>Ethernet IP is not configured</td>
</tr>
<tr>
<td></td>
<td>LGPRS</td>
<td>18</td>
<td>GPRS line fault</td>
<td>GPRS connection fault</td>
</tr>
<tr>
<td></td>
<td>LFIPGPRS</td>
<td>19</td>
<td>GPRS IP fault</td>
<td>GPRS IP is not configured</td>
</tr>
<tr>
<td></td>
<td>LFTDA</td>
<td>20</td>
<td>TDA line fault</td>
<td>TDA module line fault</td>
</tr>
<tr>
<td></td>
<td>LFTDAGPRS</td>
<td>21</td>
<td>TDA GPRS fault</td>
<td>TDA module line fault (GPRS)</td>
</tr>
</tbody>
</table>
## Appendix A: Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LFTDAETH</td>
<td>22</td>
<td>TDA ETH fault</td>
<td>TDA module line fault (ETH)</td>
</tr>
<tr>
<td></td>
<td>MIFTDA</td>
<td>23</td>
<td>TDA MI fault</td>
<td>Panel MI device fault (TDA)</td>
</tr>
<tr>
<td></td>
<td>GSMJAMMING</td>
<td>24</td>
<td>GSM jamming</td>
<td>GSM jamming detected</td>
</tr>
<tr>
<td></td>
<td>POWER UNIT FA</td>
<td>25</td>
<td>Panel PSU fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BTESTACTV</td>
<td>26</td>
<td>Panel battery test active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BTESTFAIL</td>
<td>27</td>
<td>Panel battery test fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DLRBATTFAULT</td>
<td>28</td>
<td>Dialer battery fault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MODRESET</td>
<td>29</td>
<td>Dialer module reset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEVTAMPERINH</td>
<td>30</td>
<td>Panel tamper inhibited</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIRTAMPERINH</td>
<td>31</td>
<td>Siren tamper inhibited</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>CARDPIN</td>
<td>1</td>
<td>Card or PIN presented</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SMSCONTROL</td>
<td>2</td>
<td>SMS control active</td>
<td>SMS control is active</td>
</tr>
<tr>
<td></td>
<td>SMSCONTROLLOCK</td>
<td>3</td>
<td>SMS control locked</td>
<td>SMS control is disabled by invalid attempts</td>
</tr>
<tr>
<td></td>
<td>SMSREPORTING</td>
<td>4</td>
<td>SMS reporting active</td>
<td>SMS reporting is active</td>
</tr>
<tr>
<td></td>
<td>SMSREPAFTERSET</td>
<td>5</td>
<td>SMS reporting after set</td>
<td>SMS reporting will be activated after set</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>ACTIVE</td>
<td>1</td>
<td>Output active</td>
<td>Specified output activates</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>2</td>
<td>Output on</td>
<td>Physical output activates</td>
</tr>
<tr>
<td></td>
<td>FORCED</td>
<td>3</td>
<td>Door forced output</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>ACTIVE</td>
<td>1</td>
<td>Condition true</td>
<td>The selected filter condition is true / valid.</td>
</tr>
<tr>
<td>Group</td>
<td>Event</td>
<td>#</td>
<td>Event description</td>
<td>Notes</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>---</td>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>User group</td>
<td>CARDPIN</td>
<td>1</td>
<td>Card or PIN presented</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SCH ACTIVE</td>
<td>2</td>
<td>Schedule active</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>ALLSET</td>
<td>1</td>
<td>All set</td>
<td>All areas in the system are set</td>
</tr>
<tr>
<td></td>
<td>AUTOANS</td>
<td>2</td>
<td>Auto Answer</td>
<td>Auto answer procedure started (1 min)</td>
</tr>
<tr>
<td></td>
<td>RCONACTV</td>
<td>3</td>
<td>Remote connection</td>
<td>Remote connection active</td>
</tr>
<tr>
<td></td>
<td>RCONNFAIL</td>
<td>4</td>
<td>Remote connection fail</td>
<td>Remote connection fail (1 min)</td>
</tr>
<tr>
<td></td>
<td>LPRGACTV</td>
<td>5</td>
<td>Local programming</td>
<td>Local programming active</td>
</tr>
<tr>
<td></td>
<td>RPRGACTV</td>
<td>6</td>
<td>Remote programming</td>
<td>Remote programming active</td>
</tr>
<tr>
<td></td>
<td>TIMECHG</td>
<td>7</td>
<td>Time Changed</td>
<td>System time changed</td>
</tr>
<tr>
<td></td>
<td>SSAVER</td>
<td>8</td>
<td>Armed display</td>
<td>Armed display active</td>
</tr>
<tr>
<td></td>
<td>ISIREN</td>
<td>9</td>
<td>Internal siren</td>
<td>Internal siren event flag (system flag)</td>
</tr>
<tr>
<td></td>
<td>ESIREN</td>
<td>10</td>
<td>External siren</td>
<td>External siren event flag (system flag)</td>
</tr>
<tr>
<td></td>
<td>STROBE</td>
<td>11</td>
<td>Strobe output</td>
<td>Strobe event flag (system flag)</td>
</tr>
<tr>
<td></td>
<td>SYSFAULT</td>
<td>12</td>
<td>Global fault</td>
<td>Global system fault flag</td>
</tr>
<tr>
<td></td>
<td>SYSTAMPER</td>
<td>13</td>
<td>Global tamper</td>
<td>Global system tamper flag</td>
</tr>
<tr>
<td></td>
<td>SERVICEIN</td>
<td>14</td>
<td>Service in active</td>
<td>Service in is active for the installer</td>
</tr>
<tr>
<td></td>
<td>WT MODE ON</td>
<td>15</td>
<td>Walk test mode on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detector Test</td>
<td>16</td>
<td>Detector test active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DT FAILED</td>
<td>17</td>
<td>Detector test failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AR HRCHY 1</td>
<td>18</td>
<td>Hierarchy 1</td>
<td>All hierarchy 1 areas are set</td>
</tr>
<tr>
<td></td>
<td>AR HRCHY 2</td>
<td>19</td>
<td>Hierarchy 2</td>
<td>All hierarchy 2 areas are set</td>
</tr>
<tr>
<td></td>
<td>AR HRCHY 3</td>
<td>20</td>
<td>Hierarchy 3</td>
<td>All hierarchy 3 areas are set</td>
</tr>
<tr>
<td></td>
<td>POWERUPREPFAIL</td>
<td>21</td>
<td>System power up reporting failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LIS-IN ACTIVE</td>
<td>22</td>
<td>Audio listen-in session is active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud avl.</td>
<td>23</td>
<td>The panel is ready for UltraSync cloud connection</td>
<td>The panel has serial number</td>
</tr>
</tbody>
</table>
## Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud reg.</td>
<td>24</td>
<td>The panel is registered in UltraSync cloud</td>
<td></td>
</tr>
<tr>
<td>UltraSync SIM</td>
<td>25</td>
<td>UltraSync SIM card is present in the GSM module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>DISABLED</td>
<td>1</td>
<td>Door disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UNLOCKED</td>
<td>2</td>
<td>Door unlocked</td>
<td>Door unlocked until locked manually or by a schedule</td>
</tr>
<tr>
<td></td>
<td>UNLOCKED PRD</td>
<td>3</td>
<td>Door unlocked period</td>
<td>Door unlocked automatically</td>
</tr>
<tr>
<td></td>
<td>TUNLOCKED</td>
<td>4</td>
<td>Door timed unlock</td>
<td>Door unlocked for a specified time</td>
</tr>
<tr>
<td></td>
<td>OPEN</td>
<td>5</td>
<td>Door open</td>
<td>Door is unlocked for the time configured in its config.</td>
</tr>
<tr>
<td></td>
<td>OPENED</td>
<td>6</td>
<td>Door opened</td>
<td>Door zone is in active/tamper state</td>
</tr>
<tr>
<td></td>
<td>FORCED</td>
<td>7</td>
<td>Door forced</td>
<td>Door zone has been activated without unlocking</td>
</tr>
<tr>
<td></td>
<td>DOTL</td>
<td>8</td>
<td>Door DOTL</td>
<td>Door zone active after shunt time</td>
</tr>
<tr>
<td></td>
<td>SHUNTING</td>
<td>9</td>
<td>Door shunting</td>
<td>Door zone has been shunted</td>
</tr>
<tr>
<td></td>
<td>LIS</td>
<td>10</td>
<td>Door listen-in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LIS-FLAG1</td>
<td>11</td>
<td>Door listen-in flag 1</td>
<td>A programmable flag, which can be activated for 3 s by a DTMF code</td>
</tr>
<tr>
<td></td>
<td>DOOR INPUT</td>
<td>13</td>
<td>Door input</td>
<td>Door zone is in active/tamper state</td>
</tr>
<tr>
<td>CS</td>
<td>FTC</td>
<td>1</td>
<td>Failed To Communicate</td>
<td>Failed to deliver an alarm message</td>
</tr>
<tr>
<td></td>
<td>HB fault</td>
<td>2</td>
<td>OH heartbeat fault</td>
<td>OH protocol heartbeat fault</td>
</tr>
<tr>
<td></td>
<td>BUSY</td>
<td>3</td>
<td>CS busy</td>
<td>CS is busy (in use)</td>
</tr>
<tr>
<td></td>
<td>LIS-IN ACTIVE</td>
<td>4</td>
<td>Listen-in active</td>
<td>Active when listen-in session with the selected central station is active</td>
</tr>
<tr>
<td></td>
<td>LIS-IN FLAG1</td>
<td>5</td>
<td>Listen-in flag 1</td>
<td>A programmable flag, which can be activated for 3 s by a DTMF code</td>
</tr>
</tbody>
</table>
### Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIS-INV FLAG2</td>
<td>6</td>
<td>Listen-in flag 2</td>
<td>A programmable flag, which can be activated for 3 s by a DTMF code</td>
<td></td>
</tr>
<tr>
<td>LIS-INV FLAG3</td>
<td>7</td>
<td>Listen-in flag 3</td>
<td>A programmable flag, which can be activated for 3 s by a DTMF code</td>
<td></td>
</tr>
<tr>
<td>LIS-INV FLAG4</td>
<td>8</td>
<td>Listen-in flag 4</td>
<td>A programmable flag, which can be activated for 3 s by a DTMF code</td>
<td></td>
</tr>
</tbody>
</table>

### Trigger

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger</td>
<td>S1 1230/34</td>
<td>1</td>
<td>Fob button 1</td>
<td>Toggle state when fob button 1 is pressed</td>
</tr>
<tr>
<td></td>
<td>S2 1230/34</td>
<td>2</td>
<td>Fob button 2</td>
<td>Toggle state when fob button 2 is pressed</td>
</tr>
<tr>
<td></td>
<td>S1S2 1230/34</td>
<td>3</td>
<td>Fob buttons 1 and 2</td>
<td>Set state when fob button 1 is pressed, reset state when fob button 2 is pressed</td>
</tr>
<tr>
<td>REMOTEOUT</td>
<td></td>
<td>4</td>
<td>Remote control</td>
<td></td>
</tr>
<tr>
<td>FUNCTION KEY</td>
<td></td>
<td>5</td>
<td>Function key control</td>
<td></td>
</tr>
<tr>
<td>SCHEDULE</td>
<td></td>
<td>6</td>
<td>Schedule control</td>
<td></td>
</tr>
<tr>
<td>FOB (ATS1235)</td>
<td></td>
<td>7</td>
<td>Trigger is activated by a fob</td>
<td></td>
</tr>
</tbody>
</table>

### Calendar

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>CALHOUR</td>
<td>1</td>
<td>Every hour</td>
<td>The event flag is toggled every hour at 00 min</td>
</tr>
<tr>
<td></td>
<td>CALDAY</td>
<td>2</td>
<td>Every day</td>
<td>The event flag is toggled every day at 00:00</td>
</tr>
<tr>
<td></td>
<td>Monday</td>
<td>3</td>
<td>Monday</td>
<td>Active on Mondays</td>
</tr>
<tr>
<td></td>
<td>Tuesday</td>
<td>4</td>
<td>Tuesday</td>
<td>Active on Tuesdays</td>
</tr>
<tr>
<td></td>
<td>Wednesday</td>
<td>5</td>
<td>Wednesday</td>
<td>Active on Wednesdays</td>
</tr>
<tr>
<td></td>
<td>Thursday</td>
<td>6</td>
<td>Thursday</td>
<td>Active on Thursdays</td>
</tr>
<tr>
<td></td>
<td>Friday</td>
<td>7</td>
<td>Friday</td>
<td>Active on Fridays</td>
</tr>
<tr>
<td></td>
<td>Saturday</td>
<td>8</td>
<td>Saturday</td>
<td>Active on Saturdays</td>
</tr>
<tr>
<td></td>
<td>Sunday</td>
<td>9</td>
<td>Sunday</td>
<td>Active on Sundays</td>
</tr>
</tbody>
</table>

### Fob

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fob ATS1235+</td>
<td>Fob learned</td>
<td>1</td>
<td>Fob programmed</td>
<td>Active for 3 seconds after a successful programming</td>
</tr>
<tr>
<td></td>
<td>Button 1</td>
<td>2</td>
<td>Button 1 pressed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Button 2</td>
<td>3</td>
<td>Button 2 pressed</td>
<td></td>
</tr>
</tbody>
</table>
# Appendix A: Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button 3</td>
<td>4</td>
<td>Button 3 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 4</td>
<td>5</td>
<td>Button 4 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 1+2</td>
<td>6</td>
<td>Buttons 1 and 2 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 1+3</td>
<td>7</td>
<td>Buttons 1 and 3 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 1+4</td>
<td>8</td>
<td>Buttons 1 and 4 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 2+3</td>
<td>9</td>
<td>Buttons 2 and 3 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 2+4</td>
<td>10</td>
<td>Buttons 2 and 4 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button 3+4</td>
<td>11</td>
<td>Buttons 3 and 4 pressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOBBATTLOW</td>
<td>12</td>
<td>Fob battery low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Pic captured</td>
<td>1</td>
<td>Picture has been taken</td>
<td>Active for 3 seconds</td>
</tr>
<tr>
<td></td>
<td>Pic limit exc</td>
<td>2</td>
<td>Picture limit has been exceeded</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area group</td>
<td>SET</td>
<td>1</td>
<td>All areas set</td>
<td>All areas in area group are set</td>
</tr>
<tr>
<td></td>
<td>PSET1</td>
<td>2</td>
<td>All part set 1</td>
<td>All areas in area group are part set 1</td>
</tr>
<tr>
<td></td>
<td>PSET2</td>
<td>3</td>
<td>All part set 2</td>
<td>All areas in area group are part set 2</td>
</tr>
<tr>
<td></td>
<td>RTS</td>
<td>4</td>
<td>All ready to set</td>
<td>All areas in area group are in Ready to Set state</td>
</tr>
<tr>
<td></td>
<td>UNSET</td>
<td>5</td>
<td>All unset</td>
<td>All areas in area group are unset</td>
</tr>
<tr>
<td></td>
<td>FULLSET</td>
<td>6</td>
<td>All full set</td>
<td>All areas in area group are in full set state</td>
</tr>
<tr>
<td></td>
<td>ALARM</td>
<td>7</td>
<td>An alarm state</td>
<td>At least one area is in alarm</td>
</tr>
<tr>
<td></td>
<td>EXIT</td>
<td>8</td>
<td>An exit state</td>
<td>At least one area is in exit state</td>
</tr>
<tr>
<td></td>
<td>NRTS</td>
<td>9</td>
<td>Not ready to set</td>
<td>At least one area in area group is in not Ready To Set state</td>
</tr>
<tr>
<td></td>
<td>AREAASET</td>
<td>10</td>
<td>An area has been set</td>
<td>Active for 3 s</td>
</tr>
<tr>
<td></td>
<td>AREAUNSET</td>
<td>11</td>
<td>An area has been unset</td>
<td>Active for 3 s</td>
</tr>
</tbody>
</table>
### Appendix A: Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>SCH ACTIVE</td>
<td>1</td>
<td>Schedule active</td>
<td></td>
</tr>
<tr>
<td>Special</td>
<td>SP DAY ACTIVE</td>
<td>1</td>
<td>Special day is active</td>
<td></td>
</tr>
<tr>
<td>Reader</td>
<td>OFFLINE</td>
<td>1</td>
<td>Reader is offline</td>
<td></td>
</tr>
<tr>
<td>Reader</td>
<td>TAMPER</td>
<td>2</td>
<td>Reader tamper</td>
<td></td>
</tr>
</tbody>
</table>

### Table 32: Door controller events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door</td>
<td>Door open</td>
<td>1</td>
<td>Door open command is active (to unlock / start shunt)</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Door unlocked</td>
<td>2</td>
<td>Unlock output is active to unlock the door</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Door locked</td>
<td>3</td>
<td>Unlock output is deactivated to lock the door</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Door override</td>
<td>4</td>
<td>The low security schedule assigned to the door is valid</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>D.ovr.inhibit</td>
<td>5</td>
<td>Door override inhibit</td>
<td>The low security schedule is inhibited</td>
</tr>
<tr>
<td>Door</td>
<td>Door disabled</td>
<td>6</td>
<td>Door is disabled completely (from keypad or computer)</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Door enabled</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reader</td>
<td>Reader disabled</td>
<td>8</td>
<td>Door reader is disabled</td>
<td></td>
</tr>
<tr>
<td>Reader</td>
<td>Reader enabled</td>
<td>9</td>
<td>Door reader is enabled</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>2 card inside</td>
<td>10</td>
<td>Two Card access is required at the &quot;IN&quot; reader</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>2 card outside</td>
<td>11</td>
<td>Two Card access is required at the &quot;OUT&quot; reader</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Low sec.inside</td>
<td>12</td>
<td>Door low security inside</td>
<td>Card or PIN required to access at the &quot;IN&quot; reader</td>
</tr>
<tr>
<td>Door</td>
<td>Low sec.outs.</td>
<td>13</td>
<td>Door low security outside</td>
<td>Card or PIN required to access at the &quot;OUT&quot; reader</td>
</tr>
<tr>
<td>Door</td>
<td>Anti-passback</td>
<td>14</td>
<td>Anti-Passback is active</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Door shunting</td>
<td>15</td>
<td>Shunt timer is running</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>Shunt warning</td>
<td>16</td>
<td>Shunt warning timer is running</td>
<td></td>
</tr>
<tr>
<td>Door</td>
<td>D. Area armed</td>
<td>17</td>
<td>Area assigned to the door is armed. As a macro output, this event</td>
<td>Area assigned to the door is armed. As a macro output, this</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>disables a door when &quot;Deny access when set&quot; is set to Yes.</td>
<td>event disables a door when &quot;Deny access when set&quot; is set to</td>
</tr>
</tbody>
</table>

Advisor Advanced ATSx500A(-IP) Installation and Programming Manual 349
### Appendix A: Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Keypad duress</td>
<td>18</td>
<td>Duress PIN entered at door keypad</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOTL</td>
<td>19</td>
<td>Door contact is active after shunt timer has expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forced</td>
<td>20</td>
<td>Door contact is active with no valid door command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LED 1</td>
<td>21</td>
<td>LED 1 output is active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LED 2</td>
<td>22</td>
<td>LED 2 output is active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Buzzer</td>
<td>23</td>
<td>Door buzzer output is active</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door access</td>
<td>Interlock</td>
<td>1</td>
<td>Interlock zones are active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intlck.overrid</td>
<td>2</td>
<td>Interlock has been overridden</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denied</td>
<td>3</td>
<td>Door access has not been allowed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted</td>
<td>4</td>
<td>Door access has been allowed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted traced</td>
<td>5</td>
<td>Door access has been granted to a user with trace On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted 1badge</td>
<td>6</td>
<td>Door access has been granted when badged once</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted 2badge</td>
<td>7</td>
<td>Door access has been granted when badged twice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted 3badge</td>
<td>8</td>
<td>Door access has been granted when badged three times</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted IN btn</td>
<td>9</td>
<td>Door access has been granted and IN button pressed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granted OUTbtn</td>
<td>10</td>
<td>Door access has been granted and OUT button pressed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fire override</td>
<td>11</td>
<td>Secondary override is active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Normal</td>
<td>12</td>
<td>The door is locked and closed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-psbck dis</td>
<td>13</td>
<td>Disable anti-passback for selected door</td>
<td>Disable anti-passback for selected door</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Limit</td>
<td>1</td>
<td>Region limit</td>
<td>Active when the number of people in any region reaches the present limit (255 events, 1 per region)</td>
</tr>
<tr>
<td></td>
<td>Usr to Outside</td>
<td>2</td>
<td>Move users in region to outside region 1</td>
<td>Move users from selected region (1 to 255) to outside region 1 (255 events)</td>
</tr>
<tr>
<td></td>
<td>All to Outside</td>
<td>3</td>
<td>Move all users to outside region 1</td>
<td>Move all users to outside region 1</td>
</tr>
</tbody>
</table>
## Appendix A: Advisor Advanced events

### Usr to No Reg

<table>
<thead>
<tr>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usr to No Reg</td>
<td>4</td>
<td>Reset users in region to region 256 (no region)</td>
<td>Region value of users in the selected region (1 to 255) is reset to 256 (255 events, 1 per region)</td>
</tr>
</tbody>
</table>

### All to No Reg

<table>
<thead>
<tr>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>All to No Reg</td>
<td>5</td>
<td>Reset all users regions to 256 (no region)</td>
<td>Region value of all users is reset to 256</td>
</tr>
</tbody>
</table>

### Schedule activ

<table>
<thead>
<tr>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule activ</td>
<td>6</td>
<td>Schedule active</td>
<td>Activated if selected schedule is active (24 events, 1 per schedule)</td>
</tr>
</tbody>
</table>

### Faults

<table>
<thead>
<tr>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>D.reader fault</td>
<td>1</td>
<td>Door reader fault</td>
<td></td>
</tr>
<tr>
<td>D.lock fault</td>
<td>2</td>
<td>Door lock fault</td>
<td></td>
</tr>
<tr>
<td>RAS offline</td>
<td>3</td>
<td>RAS on door controller local databus is offline (16 events, 1 per RAS address)</td>
<td></td>
</tr>
<tr>
<td>DGP offline</td>
<td>4</td>
<td>DGP on ATS1260 local databus is offline</td>
<td></td>
</tr>
<tr>
<td>DGP mains fail</td>
<td>5</td>
<td>Mains fail condition exists on the door controller</td>
<td></td>
</tr>
<tr>
<td>DGP low batt</td>
<td>6</td>
<td>Low battery condition exists on the door controller</td>
<td></td>
</tr>
<tr>
<td>DGP fuse flt</td>
<td>7</td>
<td>Fuse Fail condition exists on the door controller</td>
<td></td>
</tr>
<tr>
<td>DGP siren flt</td>
<td>8</td>
<td>Siren fail (siren tamper) condition exists on this door controller</td>
<td></td>
</tr>
<tr>
<td>DGP tamper</td>
<td>9</td>
<td>Cabinet tamper condition exists on this door controller</td>
<td></td>
</tr>
<tr>
<td>DGP offline</td>
<td>10</td>
<td>DGP offline</td>
<td>door controller is not communicating with the Advisor Master</td>
</tr>
</tbody>
</table>

### Other

<table>
<thead>
<tr>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area disarmed</td>
<td>1</td>
<td>Area disarmed</td>
<td>Area disarmed (16 events, 1 per area)</td>
</tr>
<tr>
<td>Area alarm</td>
<td>2</td>
<td>Area alarm</td>
<td>Zones in alarm in area (16 events, 1 per area)</td>
</tr>
<tr>
<td>DGP out.active</td>
<td>3</td>
<td>DGP outputs</td>
<td>System output assigned to this DGP is active (16 events, 1 per outputs). First 16 on DGP can also be activated by physical output function</td>
</tr>
<tr>
<td>DGP zone active</td>
<td>4</td>
<td>Zones</td>
<td>Zone on this DGP active (16 events, 1 per zone)</td>
</tr>
</tbody>
</table>
## Appendix A: Advisor Advanced events

<table>
<thead>
<tr>
<th>Group</th>
<th>Event</th>
<th>#</th>
<th>Event description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phys. out activ</td>
<td>5</td>
<td>Physical outputs</td>
<td>Output connected to this DGP is active (255 events, 1 per output). Outputs above 16 are only activated by door macro.</td>
<td></td>
</tr>
<tr>
<td>DGP bat. t. act</td>
<td>6</td>
<td>Door controller battery test active</td>
<td>The battery test on this door controller is running</td>
<td></td>
</tr>
<tr>
<td>DGP bat. t. fail</td>
<td>7</td>
<td>Door controller battery test fail</td>
<td>The battery test failed on this door controller</td>
<td></td>
</tr>
<tr>
<td>DGP siren act</td>
<td>8</td>
<td>Door controller siren active</td>
<td>The siren output (16th relay) is active</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B
Advisor Advanced reporting codes

Table 33 below shows descriptions of SIA, CID, and VdS reporting codes used in Advisor Advanced.

Table 34 on page 358 lists allowed values for the appropriate reporting codes.

### Table 33: SIA, CID, and VdS reporting code descriptions

<table>
<thead>
<tr>
<th>#</th>
<th>SIA code</th>
<th>VdS code</th>
<th>CID code</th>
<th>Function</th>
<th>Note</th>
<th>Reporting priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>AN</td>
<td>0xB0</td>
<td>R393</td>
<td>Detector dirty restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>2.</td>
<td>AR</td>
<td>0xB2</td>
<td>R301</td>
<td>AC restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>3.</td>
<td>AS</td>
<td>0x30</td>
<td>E393</td>
<td>Detector dirty</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>4.</td>
<td>AT</td>
<td>0x32</td>
<td>E301</td>
<td>AC trouble</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>5.</td>
<td>BA</td>
<td>0x22</td>
<td>E130</td>
<td>Burglary alarm</td>
<td>Alarm / input in mask / trouble when set</td>
<td>Medium</td>
</tr>
<tr>
<td>6.</td>
<td>BB</td>
<td>0x51</td>
<td>E570</td>
<td>Burglary bypass</td>
<td>Alarm inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>7.</td>
<td>BC</td>
<td>0x52</td>
<td>E406</td>
<td>Burglary cancel</td>
<td>Cancel alarm by user / key / remotely</td>
<td>Low</td>
</tr>
<tr>
<td>8.</td>
<td>BJ</td>
<td>0xB0</td>
<td>R381</td>
<td>Detector supervision restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>9.</td>
<td>BR</td>
<td>0xA2</td>
<td>R130</td>
<td>Burglary restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>10.</td>
<td>BT</td>
<td>0x30</td>
<td>E380</td>
<td>Burglary trouble</td>
<td>Input in mask / trouble when unset</td>
<td>Low</td>
</tr>
<tr>
<td>11.</td>
<td>BU</td>
<td>0xD1</td>
<td>R570</td>
<td>Burglary unbypass</td>
<td>Alarm uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>12.</td>
<td>BV</td>
<td>0x00</td>
<td>E139</td>
<td>Alarm confirm</td>
<td>ACPO</td>
<td>Medium</td>
</tr>
<tr>
<td>13.</td>
<td>BW</td>
<td>0x80</td>
<td>R139</td>
<td>Restore confirmed alarm</td>
<td>ACPO</td>
<td>Low</td>
</tr>
<tr>
<td>14.</td>
<td>BZ</td>
<td>0x30</td>
<td>E381</td>
<td>Detector supervision</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>15.</td>
<td>CF</td>
<td>0x51</td>
<td>E408</td>
<td>Forced closing</td>
<td>Set by user / by key</td>
<td>Low</td>
</tr>
<tr>
<td>16.</td>
<td>CG</td>
<td>0x62</td>
<td>E456</td>
<td>Part set</td>
<td>Part set by user / by key / remotely</td>
<td>Low</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>VdS code</td>
<td>CID code</td>
<td>Function</td>
<td>Note</td>
<td>Reporting priority</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>17</td>
<td>CL</td>
<td>0x61</td>
<td>R401</td>
<td>Closing normal</td>
<td>Set by user</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R407</td>
<td>Closing normal</td>
<td>Set remotely</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R409</td>
<td>Closing normal</td>
<td>Set by key</td>
<td>Low</td>
</tr>
<tr>
<td>18</td>
<td>EE</td>
<td>0x30</td>
<td>E374</td>
<td>Exit error</td>
<td>Exit fault</td>
<td>Medium</td>
</tr>
<tr>
<td>19</td>
<td>ER</td>
<td>0xB0</td>
<td>R143</td>
<td>Expansion restore</td>
<td>Expander / keypad / audio trouble restore</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R300</td>
<td>Expansion restore</td>
<td>Expander fuse restore</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R330</td>
<td>Expansion restore</td>
<td>Expander / keypad / audio communication restore</td>
<td>Low</td>
</tr>
<tr>
<td>20</td>
<td>ET</td>
<td>0x30</td>
<td>E143</td>
<td>Expansion trouble</td>
<td>Expander / keypad / audio trouble</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E300</td>
<td>Expansion trouble</td>
<td>Expander fuse failure</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E330</td>
<td>Expansion trouble</td>
<td>Expander / keypad / audio communication fault</td>
<td>Low</td>
</tr>
<tr>
<td>21</td>
<td>FA</td>
<td>0x10</td>
<td>E110</td>
<td>Fire alarm</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>22</td>
<td>FB</td>
<td>0x51</td>
<td>E570</td>
<td>Fire bypass</td>
<td>Fire inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>23</td>
<td>FJ</td>
<td>0xA3</td>
<td>R373</td>
<td>Fire trouble restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>24</td>
<td>FR</td>
<td>0x90</td>
<td>R110</td>
<td>Fire restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>25</td>
<td>FT</td>
<td>0x23</td>
<td>E373</td>
<td>Fire trouble</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>26</td>
<td>FU</td>
<td>0xD1</td>
<td>R570</td>
<td>Fire unbypass</td>
<td>Fire uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>27</td>
<td>FW</td>
<td>0x30</td>
<td>–</td>
<td>Fire long supervision</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>28</td>
<td>HA</td>
<td>0x24</td>
<td>E121</td>
<td>Holdup alarm</td>
<td>Duress</td>
<td>High</td>
</tr>
<tr>
<td>29</td>
<td>HR</td>
<td>0xA4</td>
<td>R121</td>
<td>Holdup restore</td>
<td>Duress restore</td>
<td>Low</td>
</tr>
<tr>
<td>30</td>
<td>JP</td>
<td>0x63</td>
<td>E466</td>
<td>Service in</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>31</td>
<td>JR</td>
<td>0xE3</td>
<td>R466</td>
<td>Service out</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>32</td>
<td>JT</td>
<td>0x55</td>
<td>E625</td>
<td>Time changed</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>33</td>
<td>LB</td>
<td>0x01</td>
<td>E627</td>
<td>Local programming begin</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>34</td>
<td>LR</td>
<td>0xBA</td>
<td>R351</td>
<td>Line restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>35</td>
<td>LS</td>
<td>0x81</td>
<td>R628</td>
<td>Local programming stop</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>36</td>
<td>LT</td>
<td>0x3A</td>
<td>E351</td>
<td>Line fault</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>37</td>
<td>MA</td>
<td>0x48</td>
<td>E100</td>
<td>Medical alarm</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>38</td>
<td>MB</td>
<td>0x51</td>
<td>E570</td>
<td>Medical bypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>39</td>
<td>MJ</td>
<td>0xB0</td>
<td>–</td>
<td>Medical long supervision restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>40</td>
<td>MR</td>
<td>0xC8</td>
<td>R100</td>
<td>Medical restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>41</td>
<td>MS</td>
<td>0x30</td>
<td>–</td>
<td>Medical long supervision</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>VdS code</td>
<td>CID code</td>
<td>Function</td>
<td>Note</td>
<td>Reporting priority</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>42.</td>
<td>MU</td>
<td>0xD1</td>
<td>R570</td>
<td>Medical unbypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>43.</td>
<td>OP</td>
<td>0xE1</td>
<td>E401</td>
<td>Unset normal</td>
<td>Unset by user</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E407</td>
<td>Unset normal</td>
<td>Unset remotely</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E409</td>
<td>Unset normal</td>
<td>Unset by key</td>
<td>Low</td>
</tr>
<tr>
<td>44.</td>
<td>OR</td>
<td>0xE1</td>
<td>E406</td>
<td>Unset from alarm</td>
<td>Unset by user / key / remotely</td>
<td>Low</td>
</tr>
<tr>
<td>45.</td>
<td>PA</td>
<td>0x21</td>
<td>E120</td>
<td>Panic alarm</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>46.</td>
<td>PB</td>
<td>0x51</td>
<td>E570</td>
<td>Panic bypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>47.</td>
<td>PJ</td>
<td>0xA1</td>
<td>R375</td>
<td>Panic trouble restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>48.</td>
<td>PR</td>
<td>0xA1</td>
<td>R120</td>
<td>Panic restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>49.</td>
<td>PT</td>
<td>0x21</td>
<td>E375</td>
<td>Panic trouble</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>50.</td>
<td>PU</td>
<td>0xD1</td>
<td>R570</td>
<td>Panic unbypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>51.</td>
<td>RB</td>
<td>0x74</td>
<td>E416</td>
<td>Remote programming begin</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>52.</td>
<td>RP</td>
<td>—</td>
<td>E602</td>
<td>Automatic test / ring-in test</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>53.</td>
<td>RR</td>
<td>0x53</td>
<td>E305</td>
<td>Power up</td>
<td>System power-up</td>
<td>Low</td>
</tr>
<tr>
<td>54.</td>
<td>RS</td>
<td>0xF4</td>
<td>R416</td>
<td>Remote programming success</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>55.</td>
<td>RU</td>
<td>0x55</td>
<td>R416</td>
<td>Remote programming fail</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>56.</td>
<td>RX</td>
<td>—</td>
<td>E601</td>
<td>Manual CS test</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>57.</td>
<td>TA</td>
<td>0x23</td>
<td>E144</td>
<td>Tamper alarm</td>
<td>Zone tamper</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E145</td>
<td>Tamper alarm</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E320</td>
<td>Tamper alarm</td>
<td>Expander siren tamper</td>
<td>Medium</td>
</tr>
<tr>
<td>58.</td>
<td>TB</td>
<td>0x51</td>
<td>E570</td>
<td>Tamper bypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>59.</td>
<td>TR</td>
<td>0xA3</td>
<td>R144</td>
<td>Tamper restore</td>
<td>Zone tamper restore</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R145</td>
<td>Tamper restore</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R320</td>
<td>Tamper restore</td>
<td>Expander siren restore</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R370</td>
<td>Tamper restore</td>
<td>KeyBox tamper restore</td>
<td>Low</td>
</tr>
<tr>
<td>60.</td>
<td>TT</td>
<td>0x23</td>
<td>E370</td>
<td>KeyBox zone active</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>61.</td>
<td>TU</td>
<td>0xD1</td>
<td>R570</td>
<td>Tamper unbypass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>62.</td>
<td>UB</td>
<td>0x51</td>
<td>E570</td>
<td>Expander / keypad / audio / zone bypassed</td>
<td>Expander / keypad / audio / zone isolated</td>
<td>Low</td>
</tr>
<tr>
<td>63.</td>
<td>UU</td>
<td>0xD1</td>
<td>R570</td>
<td>Expander / keypad / audio / zone bypassed</td>
<td>Expander / keypad / audio / zone de-isolated</td>
<td>Low</td>
</tr>
<tr>
<td>64.</td>
<td>WF</td>
<td>0xF6</td>
<td>E612</td>
<td>Walk test fail</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>65.</td>
<td>WP</td>
<td>0x76</td>
<td>E611</td>
<td>Walk test pass</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>VdS code</td>
<td>CID code</td>
<td>Function</td>
<td>Note</td>
<td>Reporting priority</td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>----------</td>
<td>---------</td>
<td>-------------------------------</td>
<td>-------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>66.</td>
<td>XH</td>
<td>0xB0</td>
<td>R344</td>
<td>RF jamming restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>67.</td>
<td>XQ</td>
<td>0x30</td>
<td>E344</td>
<td>RF jamming</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>68.</td>
<td>XR</td>
<td>0xB0</td>
<td>R384</td>
<td>Detector or fob low battery restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>69.</td>
<td>XT</td>
<td>0x30</td>
<td>E384</td>
<td>Detector or fob low battery</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>70.</td>
<td>YC</td>
<td>0x37</td>
<td>E350</td>
<td>Communications fail</td>
<td>ISDN / GSM / voice / audio device fail</td>
<td>Low</td>
</tr>
<tr>
<td>71.</td>
<td>YK</td>
<td>0xB9</td>
<td>R354</td>
<td>Communications restore</td>
<td>ISDN / GSM / voice / audio device restore</td>
<td>Low</td>
</tr>
<tr>
<td>72.</td>
<td>YR</td>
<td>0xB3</td>
<td>R302</td>
<td>System battery / fuse restore</td>
<td>Expander / dialler battery / fuse restore</td>
<td>Low</td>
</tr>
<tr>
<td>73.</td>
<td>YS</td>
<td>0x39</td>
<td>E354</td>
<td>Communication trouble</td>
<td>Fail To Communicate (FTC)</td>
<td>Low</td>
</tr>
<tr>
<td>74.</td>
<td>YT</td>
<td>0x33</td>
<td>E302</td>
<td>System battery / fuse trouble</td>
<td>Expander / dialler battery low / fuse fault</td>
<td>Low</td>
</tr>
<tr>
<td>75.</td>
<td>ZA</td>
<td>0x40</td>
<td>E152</td>
<td>Technical alarm — low temperature</td>
<td>Low temperature detector alarm</td>
<td>Medium</td>
</tr>
<tr>
<td>76.</td>
<td>ZB</td>
<td>0x51</td>
<td>E570</td>
<td>Technical bypass — low temperature</td>
<td>Low temperature detector inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>77.</td>
<td>ZJ</td>
<td>0xB0</td>
<td>R381</td>
<td>Technical long supervision restore — low temperature</td>
<td>Low temperature detector long supervision restore</td>
<td>Low</td>
</tr>
<tr>
<td>78.</td>
<td>ZR</td>
<td>0xC0</td>
<td>R152</td>
<td>Technical restore — low temperature</td>
<td>Low temperature detector restore</td>
<td>Low</td>
</tr>
<tr>
<td>79.</td>
<td>ZS</td>
<td>0x30</td>
<td>E381</td>
<td>Technical long supervision — low temperature</td>
<td>Low temperature detector long supervision alarm</td>
<td>Low</td>
</tr>
<tr>
<td>80.</td>
<td>ZU</td>
<td>0xD1</td>
<td>R570</td>
<td>Technical un bypass — low temperature</td>
<td>Low temperature detector uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>81.</td>
<td>YA</td>
<td>0x23</td>
<td>E321</td>
<td>Siren fault</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>82.</td>
<td>YH</td>
<td>0xA3</td>
<td>R321</td>
<td>Siren restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>83.</td>
<td>NC</td>
<td>0x34</td>
<td>E356</td>
<td>CS polling fail</td>
<td>Heartbeat inactive</td>
<td>Low</td>
</tr>
<tr>
<td>84.</td>
<td>NR</td>
<td>0xB4</td>
<td>R356</td>
<td>CS polling restore</td>
<td>Heartbeat active</td>
<td>Low</td>
</tr>
<tr>
<td>85.</td>
<td>CP</td>
<td>0x61</td>
<td>R403</td>
<td>Auto set</td>
<td>Set by schedule</td>
<td>Low</td>
</tr>
<tr>
<td>86.</td>
<td>OA</td>
<td>0xE1</td>
<td>E403</td>
<td>Auto unset</td>
<td>Unset by schedule</td>
<td>Low</td>
</tr>
<tr>
<td>87.</td>
<td>OT</td>
<td>0x61</td>
<td>E608</td>
<td>Late close</td>
<td>Postponed auto set</td>
<td>Low</td>
</tr>
<tr>
<td>88.</td>
<td>OK</td>
<td>0x61</td>
<td>R608</td>
<td>Early open</td>
<td>Manually unset before auto unset</td>
<td>Low</td>
</tr>
<tr>
<td>89.</td>
<td>IA</td>
<td>0x63</td>
<td>E313</td>
<td>Engineer reset request</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>90.</td>
<td>IR</td>
<td>0xE3</td>
<td>R313</td>
<td>Engineer reset restore</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>91.</td>
<td>GA</td>
<td>0x73</td>
<td>E151</td>
<td>Technical alarm — gas</td>
<td>Gas detector alarm</td>
<td>High</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>VdS code</td>
<td>CID code</td>
<td>Function</td>
<td>Note</td>
<td>Reporting priority</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>92</td>
<td>GR</td>
<td>0xF3</td>
<td>R151</td>
<td>Technical restore — gas</td>
<td>Gas detector restore</td>
<td>High</td>
</tr>
<tr>
<td>93</td>
<td>GB</td>
<td>0x51</td>
<td>E570</td>
<td>Technical bypass — gas</td>
<td>Gas detector inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>94</td>
<td>GU</td>
<td>0xD1</td>
<td>R570</td>
<td>Technical unbypass — gas</td>
<td>Gas detector uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>95</td>
<td>GS</td>
<td>0x30</td>
<td>E381</td>
<td>Technical long supervision — gas</td>
<td>Gas detector long supervision alarm</td>
<td>Low</td>
</tr>
<tr>
<td>96</td>
<td>GJ</td>
<td>0xB0</td>
<td>R381</td>
<td>Technical long supervision restore — gas</td>
<td>Gas detector long supervision restore</td>
<td>Low</td>
</tr>
<tr>
<td>97</td>
<td>KA</td>
<td>0x12</td>
<td>E158</td>
<td>Technical alarm — high temperature</td>
<td>High temperature detector alarm</td>
<td>Medium</td>
</tr>
<tr>
<td>98</td>
<td>KR</td>
<td>0x92</td>
<td>R158</td>
<td>Technical restore — high temperature</td>
<td>High temperature detector restore</td>
<td>Medium</td>
</tr>
<tr>
<td>99</td>
<td>KB</td>
<td>0x51</td>
<td>E570</td>
<td>Technical bypass — high temperature</td>
<td>High temperature detector inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>100</td>
<td>KU</td>
<td>0xD1</td>
<td>R570</td>
<td>Technical unbypass — high temperature</td>
<td>High temperature detector uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>101</td>
<td>KS</td>
<td>0x30</td>
<td>E381</td>
<td>Technical long supervision — high temperature</td>
<td>High temperature detector long supervision alarm</td>
<td>Low</td>
</tr>
<tr>
<td>102</td>
<td>KJ</td>
<td>0xB0</td>
<td>R381</td>
<td>Technical long supervision restore — high temperature</td>
<td>High temperature detector long supervision restore</td>
<td>Low</td>
</tr>
<tr>
<td>103</td>
<td>WA</td>
<td>0x75</td>
<td>E154</td>
<td>Technical alarm — water</td>
<td>Water detector alarm</td>
<td>Medium</td>
</tr>
<tr>
<td>104</td>
<td>WR</td>
<td>0xF5</td>
<td>R154</td>
<td>Technical restore — water</td>
<td>Water detector restore</td>
<td>Medium</td>
</tr>
<tr>
<td>105</td>
<td>WB</td>
<td>0x51</td>
<td>E570</td>
<td>Technical bypass — water</td>
<td>Water detector inhibit</td>
<td>Low</td>
</tr>
<tr>
<td>106</td>
<td>WU</td>
<td>0xD1</td>
<td>R570</td>
<td>Technical unbypass — water</td>
<td>Water detector uninhibit</td>
<td>Low</td>
</tr>
<tr>
<td>107</td>
<td>WS</td>
<td>0x30</td>
<td>E381</td>
<td>Technical long supervision — water</td>
<td>Water detector long supervision alarm</td>
<td>Low</td>
</tr>
<tr>
<td>108</td>
<td>WJ</td>
<td>0xB0</td>
<td>R381</td>
<td>Technical long supervision restore — water</td>
<td>Water detector long supervision restore</td>
<td>Low</td>
</tr>
<tr>
<td>109</td>
<td>ES</td>
<td>0x23</td>
<td>E145</td>
<td>Tamper alarm</td>
<td>Expander / keypad / audio tamper alarm</td>
<td>Medium</td>
</tr>
<tr>
<td>110</td>
<td>EJ</td>
<td>0xA3</td>
<td>R145</td>
<td>Tamper restore</td>
<td>Expander / keypad / audio tamper restore</td>
<td>Medium</td>
</tr>
<tr>
<td>111</td>
<td>HV</td>
<td>0x21</td>
<td>E129</td>
<td>Hold-up alarm confirm</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>112</td>
<td>HW</td>
<td>0xA1</td>
<td>R129</td>
<td>Confirmed hold-up alarm restore</td>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>
### Advisor Advanced reporting codes

<table>
<thead>
<tr>
<th>#</th>
<th>SIA code</th>
<th>VdS code</th>
<th>CID code</th>
<th>Function</th>
<th>Note</th>
<th>Reporting priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>UA</td>
<td>0x20</td>
<td>E150</td>
<td>Technical zone — general alarm</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>114</td>
<td>UR</td>
<td>0xA0</td>
<td>R150</td>
<td>Technical zone — general alarm restore</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>115</td>
<td>TS</td>
<td>0x71</td>
<td>E607</td>
<td>Single zone walk test start</td>
<td>Start of single zone test, also for multiple zones selected</td>
<td>High</td>
</tr>
<tr>
<td>116</td>
<td>TE</td>
<td>0xF1</td>
<td>R607</td>
<td>Single zone walk test end</td>
<td>End of single zone test, also for multiple zones selected</td>
<td>Low</td>
</tr>
<tr>
<td>117</td>
<td>LU</td>
<td>0x55</td>
<td>R628</td>
<td>Local programming fail</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>118</td>
<td>YP</td>
<td>0x32</td>
<td>E301</td>
<td>Power Supply Trouble</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>119</td>
<td>YQ</td>
<td>0xB2</td>
<td>R301</td>
<td>Power Supply Restored</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>120</td>
<td>CI</td>
<td>—</td>
<td>E455</td>
<td>Autoset fail</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>121</td>
<td>DD</td>
<td>—</td>
<td>E421</td>
<td>Access denied</td>
<td>Card is unknown</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Table 34: SIA and CID reporting code values

<table>
<thead>
<tr>
<th>#</th>
<th>SIA code</th>
<th>Subevent type and range</th>
<th>CID code</th>
<th>Group range</th>
<th>Point range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AN</td>
<td>Zone (1–128, 257–368)</td>
<td>R393</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>2</td>
<td>AR</td>
<td>Expander (299–307)</td>
<td>R301</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>3</td>
<td>AS</td>
<td>Zone (1–128, 257–368)</td>
<td>E393</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>4</td>
<td>AT</td>
<td>Expander (299–307)</td>
<td>E301</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>5</td>
<td>BA</td>
<td>Zone (1–128, 257–368)</td>
<td>E130</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>7</td>
<td>BC</td>
<td>System (0), User (1–50)</td>
<td>E406</td>
<td>Area (1–8)</td>
<td>User (0), User (1–50)</td>
</tr>
<tr>
<td>8</td>
<td>BJ</td>
<td>Zone (1–128, 257–368)</td>
<td>R381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>9</td>
<td>BR</td>
<td>Zone (1–128, 257–368)</td>
<td>R130</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>12</td>
<td>BV</td>
<td>Zone (1–128, 257–368)</td>
<td>E139</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>14</td>
<td>BZ</td>
<td>Zone (1–128, 257–368)</td>
<td>E381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>15</td>
<td>CF</td>
<td>User (1–50)</td>
<td>E408</td>
<td>System (0)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td>16</td>
<td>CG</td>
<td>User (1–50), Zone (1–128, 257–368)</td>
<td>E456</td>
<td>System (0)</td>
<td>User (1–50)</td>
</tr>
</tbody>
</table>

---

358 Advisor Advanced ATsx500A(-IP) Installation and Programming Manual
<table>
<thead>
<tr>
<th>#</th>
<th>SIA code</th>
<th>Subevent type and range</th>
<th>CID code</th>
<th>Group range</th>
<th>Point range</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>CL</td>
<td>Keypad (401–408)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User (1–50)</td>
<td>R401</td>
<td>Area (1–8)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System (0)</td>
<td>R407</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>ER</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>R143</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander fuse (316–324)</td>
<td>R300</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander poll (332–340), keypad poll (465–472)</td>
<td>R330</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td>20</td>
<td>ET</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>E143</td>
<td>System (0)</td>
<td>Keypad (1–8), Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander fuse (316–324)</td>
<td>E300</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander poll (332–340), keypad poll (465–472)</td>
<td>E330</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td>21</td>
<td>FA</td>
<td>System (0)</td>
<td>E110</td>
<td>System (0)</td>
<td>Keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>26</td>
<td>FU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>27</td>
<td>FW</td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>HA</td>
<td>User (1–50)</td>
<td>E121</td>
<td>Area (1–8)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>29</td>
<td>HR</td>
<td>Keypad (401–408)</td>
<td>R121</td>
<td>System (0)</td>
<td>Keypad (1–8)</td>
</tr>
<tr>
<td>30</td>
<td>JP</td>
<td>System (0)</td>
<td>E466</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>JR</td>
<td>System (0)</td>
<td>R466</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>JT</td>
<td>User (1–50)</td>
<td>E625</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>LB</td>
<td>System (0)</td>
<td>E627</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>LR</td>
<td>Communication path (0–6) [1]</td>
<td>R351</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>LS</td>
<td>System (0)</td>
<td>R628</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>LT</td>
<td>Communication path (0–6) [1]</td>
<td>E351</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>MA</td>
<td>System (0)</td>
<td>E100</td>
<td>System (0)</td>
<td>Keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>39</td>
<td>MJ</td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>MR</td>
<td>Zone (1–128, 257–368)</td>
<td>R100</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>Subevent type and range</td>
<td>CID code</td>
<td>Group range</td>
<td>Point range</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>-------------------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>41.</td>
<td>MS</td>
<td>Zone (1–128, 257–368)</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>42.</td>
<td>MU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>43.</td>
<td>OP</td>
<td>User (1–50)</td>
<td>E401</td>
<td>Area (1–8)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System (0)</td>
<td>E407</td>
<td>System (0)</td>
<td></td>
</tr>
<tr>
<td>44.</td>
<td>OR</td>
<td>User (1–50)</td>
<td>E406</td>
<td>System (0)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>45.</td>
<td>PA</td>
<td>System (0)</td>
<td>E120</td>
<td>System (0)</td>
<td>Keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User (1–50)</td>
<td></td>
<td>Area (1–8)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>46.</td>
<td>PB</td>
<td>Zone (1–128, 257–368)</td>
<td>E570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>47.</td>
<td>PJ</td>
<td>Zone (1–128, 257–368)</td>
<td>R375</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>49.</td>
<td>PT</td>
<td>Zone (1–128, 257–368)</td>
<td>E375</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>50.</td>
<td>PU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>51.</td>
<td>RB</td>
<td>Unused (0)</td>
<td>E416</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>52.</td>
<td>RP</td>
<td>Unused (0)</td>
<td>E602</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>53.</td>
<td>RR</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>E305</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td>54.</td>
<td>RS</td>
<td>System (0)</td>
<td>R416</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>55.</td>
<td>RU</td>
<td>System (0)</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>56.</td>
<td>RX</td>
<td>System (0)</td>
<td>E601</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>57.</td>
<td>TA</td>
<td>Zone (1–128, 257–368)</td>
<td>E144</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander (299–307), keypad (401–408)</td>
<td>E145</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander (316–324)</td>
<td>E320</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>59.</td>
<td>TR</td>
<td>Zone (1–128, 257–368)</td>
<td>R144</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander (299–307), keypad (401–408)</td>
<td>R145</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expander (316–324)</td>
<td>R320</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>60.</td>
<td>TT</td>
<td>Zone (1–128, 257–368)</td>
<td>E370</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>62.</td>
<td>UB</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>E570</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>Subevent type and range</td>
<td>CID code</td>
<td>Group range</td>
<td>Point range</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>-------------------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>63</td>
<td>UU</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>R570</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>WF</td>
<td>Area (1–8)</td>
<td>E612</td>
<td>Area (1–8)</td>
<td>Area (1–8)</td>
</tr>
<tr>
<td>65</td>
<td>WP</td>
<td>Area (1–8)</td>
<td>E611</td>
<td>Area (1–8)</td>
<td>Area (1–8)</td>
</tr>
<tr>
<td>66</td>
<td>XH</td>
<td>Expander (299–307)</td>
<td>R344</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication path (0–6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>XQ</td>
<td>Expander (299–307)</td>
<td>E344</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication path (0–6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fob (1–112)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fob (1–112)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>YC</td>
<td>System (0)</td>
<td>E350</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>71</td>
<td>YK</td>
<td>System (0)</td>
<td>R354</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>72</td>
<td>YR</td>
<td>Expander (299–307)</td>
<td>R302</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>73</td>
<td>YS</td>
<td>System (0)</td>
<td>E354</td>
<td>System (0)</td>
<td>–</td>
</tr>
<tr>
<td>74</td>
<td>YT</td>
<td>Expander (299–307)</td>
<td>E302</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone (1–128, 257–368)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>ZA</td>
<td>Zone (1–128, 257–368)</td>
<td>E152</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>76</td>
<td>ZB</td>
<td>Zone (1–128, 257–368)</td>
<td>E570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>77</td>
<td>ZJ</td>
<td>Zone (1–128, 257–368)</td>
<td>R381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>78</td>
<td>ZR</td>
<td>Zone (1–128, 257–368)</td>
<td>R152</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>79</td>
<td>ZS</td>
<td>Zone (1–128, 257–368)</td>
<td>E381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>80</td>
<td>ZU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>81</td>
<td>YA</td>
<td>Expander (316–324)</td>
<td>E321</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>82</td>
<td>YH</td>
<td>Expander (316–324)</td>
<td>R321</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>83</td>
<td>NC</td>
<td>CS (1–16)</td>
<td>E356</td>
<td>System (0)</td>
<td>CS (1-16)</td>
</tr>
<tr>
<td>84</td>
<td>NR</td>
<td>CS (1–16)</td>
<td>R356</td>
<td>System (0)</td>
<td>CS (1-16)</td>
</tr>
<tr>
<td>85</td>
<td>CP</td>
<td>System (0)</td>
<td>R403</td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>OA</td>
<td>System (0)</td>
<td>E403</td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>OT</td>
<td>User (1–50)</td>
<td>E608</td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>OK</td>
<td>User (1–50)</td>
<td>R608</td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>IA</td>
<td>System (0)</td>
<td>E313</td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>IR</td>
<td>User (1–50)</td>
<td>R313</td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>GR</td>
<td>Zone (1–128, 257–368)</td>
<td>R151</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>#</td>
<td>SIA code</td>
<td>Subevent type and range</td>
<td>CID code</td>
<td>Group range</td>
<td>Point range</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>-------------------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>93</td>
<td>GB</td>
<td>Zone (1–128, 257–368)</td>
<td>E570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>94</td>
<td>GU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>95</td>
<td>GS</td>
<td>Zone (1–128, 257–368)</td>
<td>E381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>96</td>
<td>GJ</td>
<td>Zone (1–128, 257–368)</td>
<td>R381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>100</td>
<td>WU</td>
<td>Zone (1–128, 257–368)</td>
<td>R570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>102</td>
<td>WJ</td>
<td>Zone (1–128, 257–368)</td>
<td>R381</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>103</td>
<td>KA</td>
<td>Zone (1–128, 257–368)</td>
<td>E158</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>105</td>
<td>KB</td>
<td>Zone (1–128, 257–368)</td>
<td>E570</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>109</td>
<td>ES</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>R145</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td>110</td>
<td>EJ</td>
<td>Expander (299–307), keypad (401–408)</td>
<td>E145</td>
<td>System (0)</td>
<td>Expander (65–72), keypad (1–8)</td>
</tr>
<tr>
<td>113</td>
<td>UA</td>
<td>Zone (1–128, 257–368)</td>
<td>E150</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>114</td>
<td>UR</td>
<td>Zone (1–128, 257–368)</td>
<td>R150</td>
<td>Area (1–8)</td>
<td>Zone (1–128, 257–368)</td>
</tr>
<tr>
<td>115</td>
<td>TS</td>
<td>Area (1–8)</td>
<td>E607</td>
<td>Area (1–8)</td>
<td>Area (1–8)</td>
</tr>
<tr>
<td>116</td>
<td>TE</td>
<td>Area (1–8)</td>
<td>R607</td>
<td>Area (1–8)</td>
<td>Area (1–8)</td>
</tr>
<tr>
<td>117</td>
<td>LU</td>
<td>System (0)</td>
<td>R628</td>
<td>Area (1–8)</td>
<td>Area (1–8)</td>
</tr>
<tr>
<td>118</td>
<td>YP</td>
<td>Expander (299–307)</td>
<td>E301</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>119</td>
<td>YQ</td>
<td>Expander (299–307)</td>
<td>R301</td>
<td>System (0)</td>
<td>Expander (65–72)</td>
</tr>
<tr>
<td>120</td>
<td>CI</td>
<td>User (1–50)</td>
<td>E455</td>
<td>Area (1–8)</td>
<td>User (1–50)</td>
</tr>
<tr>
<td>121</td>
<td>DD</td>
<td>Keypad (401–408)</td>
<td>E421</td>
<td>System (0)</td>
<td>Keypad (1–8)</td>
</tr>
</tbody>
</table>

[1] Communication path is one of the following:
- 1: PSTN
- 2: ISDN
- 3: GSM
- 4: IP
- 5: TDA9xx
- 6: TDA74xx
• 7: TDA75xx
• 61: TDA74xx GPRS virtual port
• 62: TDA74xx ETH virtual port
• 71: TDA75xx GPRS virtual port
• 72: TDA75xx ETH virtual port

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

<table>
<thead>
<tr>
<th>Access control</th>
<th>The control of entry to, or exit from, a security area through doors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Action is a user programmed function, which can be done automatically according to the programmed schedule.</td>
</tr>
<tr>
<td>Action list</td>
<td>Action lists are used to group configured actions. They can be done automatically according to the programmed schedule.</td>
</tr>
<tr>
<td>Active</td>
<td>See Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault.</td>
</tr>
<tr>
<td>Alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Alarm control</td>
<td>The control over alarm functions.</td>
</tr>
<tr>
<td>Alarm reporting</td>
<td>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.</td>
</tr>
<tr>
<td>Anti-passback</td>
<td>Anti-passback function enables users to transfer from one region to another. Entering a region twice in succession is either not possible, or will result in an event being logged and reported to the operator.</td>
</tr>
<tr>
<td>Area</td>
<td>A section of premises that has specific security requirements. The Advisor Advanced system allows any premises to be divided into different areas having different security requirements. Each area has its zones. Each area is identified by a number or a name. For example, area 1, Workshop, etc.</td>
</tr>
<tr>
<td>Armed</td>
<td>See Set.</td>
</tr>
<tr>
<td>Armed display</td>
<td>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.</td>
</tr>
<tr>
<td>Arming station (RAS)</td>
<td>See Keypad.</td>
</tr>
<tr>
<td>Audio device</td>
<td>Audio devices are used for two-way audio alarm verification.</td>
</tr>
<tr>
<td>Autoset</td>
<td>An automatic setting of the premises started by a schedule. See Schedule.</td>
</tr>
<tr>
<td>Burglar alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Card</td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Central station</td>
<td>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.</td>
</tr>
<tr>
<td>Condition filter</td>
<td>A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.</td>
</tr>
<tr>
<td>Control panel</td>
<td>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.</td>
</tr>
<tr>
<td>Cursor</td>
<td>A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.</td>
</tr>
<tr>
<td>Detector test</td>
<td>Alarm system function for detectors with a dedicated test input. After the detector test input is activated, the panel checks if proper alarm signal is provided by the detector to the system. This functionality allows testing detectors that are difficult to access.</td>
</tr>
<tr>
<td>DGP</td>
<td>Data gathering panel. See Expander.</td>
</tr>
<tr>
<td>Dialler</td>
<td>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.</td>
</tr>
<tr>
<td>Disarmed</td>
<td>See Unset.</td>
</tr>
<tr>
<td>Door contact</td>
<td>A magnetic contact used to detect if a door or window is opened.</td>
</tr>
<tr>
<td>Door control</td>
<td>The control of doors. Part of access control features.</td>
</tr>
<tr>
<td>Door controller</td>
<td>A four-door expander is an access control panel, which extends the ATS system with advanced access control functions.</td>
</tr>
<tr>
<td>Door group</td>
<td>Door groups specify when access to a specific door is granted. Door groups are assigned to users. Each Door group may have a different time period (schedule) when access to the door may be granted.</td>
</tr>
<tr>
<td>DTMF</td>
<td>Dual-tone multi-frequency signaling. DTMF allows the central station operator to send specific commands to the control panel using an active audio session.</td>
</tr>
<tr>
<td>Dual</td>
<td>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.</td>
</tr>
<tr>
<td>Duress</td>
<td>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.</td>
</tr>
<tr>
<td>Engineer</td>
<td>Personnel from an installer that is able to install and service the control panel.</td>
</tr>
<tr>
<td>Expander</td>
<td>A device that collects data from other security devices within an area, and transfers it to the Advisor Advanced control panel.</td>
</tr>
<tr>
<td>Fire alarm</td>
<td>An alarm triggered by fire or smoke detectors indicating a fire.</td>
</tr>
<tr>
<td>Fob</td>
<td>A personal wireless device, which is used to perform programmed functions, for example, set or unset premises, open doors.</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>High Security Region (HSR)</td>
<td>High security regions (HSR) require a certain number of high security users (HSU) present in them to allow any normal users inside. If a high security user leaves the region causing too few HSU present in it, an alarm is raised, preceded by prewarning time. The system does not allow the normal user to stay in the HSR without HSU inside, therefore the last high security user will not be permitted to leave the high security area if there are normal users inside.</td>
</tr>
<tr>
<td>History</td>
<td>A list of past alarm and access control events stored in memory that can be viewed on an LCD keypad or through PC connections.</td>
</tr>
<tr>
<td>Hold-up</td>
<td>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.</td>
</tr>
<tr>
<td>Inhibit</td>
<td>See Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault.</td>
</tr>
<tr>
<td>Installer</td>
<td>A company that installs and services security equipment.</td>
</tr>
</tbody>
</table>
| Intelligent door | There are two types of doors in the ATS system:  
- Intelligent door: A door controlled by a door controller. This door can be used for advanced access control.  
- Standard door: A door controlled by the control panel. It only allows basic access control functions. |
| Inverted walk test | A test based on counting days of inactivity for each zone. |
| Key switch | A device using a switch to arm or disarm areas. The switch needs a key to switch. |
| Keypad | A device that is the user control panel for security options for areas or for access points (doors). The keypad can be a console (LCD keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as set/unset, open doors, etc. |
| LCD | Liquid crystal display. The part of a keypad where messages are displayed. |
| LED | Light emitting diode. A light indicator on a keypad which conveys a condition. For example, area in alarm, communication fault, etc. |
| Listen-in | See Two-way audio. |
| Normal / Active / Tamper / Inhibited / Isolated / Masked / Fault | Describes the condition of a zone.  
- Normal: The zone is 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. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuisance alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Online / offline</td>
<td>Operational/non-operational. A device may be offline due to a malfunction in the device itself or it may be disconnected from the control.</td>
</tr>
<tr>
<td>Output expander</td>
<td>A PCB module that connects to the Advisor Advanced control panel or an expander to provide relay or open collector outputs.</td>
</tr>
<tr>
<td>Panic button</td>
<td>See hold-up.</td>
</tr>
<tr>
<td>Part set</td>
<td>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.</td>
</tr>
<tr>
<td>PIN</td>
<td>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.</td>
</tr>
<tr>
<td>PIR</td>
<td>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.</td>
</tr>
<tr>
<td>Poll</td>
<td>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.</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote arming station. See Keypad.</td>
</tr>
<tr>
<td>Reader</td>
<td>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.</td>
</tr>
<tr>
<td>Region</td>
<td>A region is a defined access control area having doors acting as boundaries. Regions are used by the anti-passback functions to monitor in which regions users are present. Transfers from one region to another may be prohibited by the anti-passback settings.</td>
</tr>
<tr>
<td>Remote expander</td>
<td>See Expander.</td>
</tr>
<tr>
<td>Remote keypad</td>
<td>See Keypad.</td>
</tr>
<tr>
<td>Reporting</td>
<td>See Alarm reporting.</td>
</tr>
<tr>
<td>Request to Exit zone</td>
<td>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.</td>
</tr>
<tr>
<td>Schedule</td>
<td>A timed set of actions.</td>
</tr>
<tr>
<td>Screen saver</td>
<td>See Armed display.</td>
</tr>
<tr>
<td>Set</td>
<td>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.</td>
</tr>
<tr>
<td>Shunt</td>
<td>A procedure that automatically inhibits a zone from generating an alarm when it is activated. E.g. shunts stop a door generating an alarm when opened for a short time.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Special day</td>
<td>A date when alternative time frames in an active schedule are valid.</td>
</tr>
<tr>
<td>Tamper</td>
<td>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.</td>
</tr>
<tr>
<td>Trigger</td>
<td>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.</td>
</tr>
<tr>
<td>Two-way audio</td>
<td>Two-way audio allows the central station operator to listen to the live audio from the protected premises in alarm, and speak back.</td>
</tr>
<tr>
<td>Unset</td>
<td>The condition of an area when it is occupied and normal activity does not set off an alarm.</td>
</tr>
<tr>
<td>Up/Download</td>
<td>A protocol providing means to view the status of an Advisor Advanced system or change parameters in the system either local or remote.</td>
</tr>
<tr>
<td>User</td>
<td>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.</td>
</tr>
<tr>
<td>User group</td>
<td>User groups define the options and permissions available to users.</td>
</tr>
<tr>
<td>Virtual zone</td>
<td>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.</td>
</tr>
<tr>
<td>Walk test</td>
<td>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.</td>
</tr>
<tr>
<td>Wireless expander</td>
<td>An expander that collects data from wireless sensors and fobs, and transfers it to the control panel.</td>
</tr>
<tr>
<td>Wireless PIR camera</td>
<td>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.</td>
</tr>
<tr>
<td>Wireless PIR camera expander</td>
<td>A wireless expander that collects data from wireless PIR cameras and transfers it to the control panel.</td>
</tr>
<tr>
<td>Zone</td>
<td>An electrical signal from a security device or a group of devices (PIR detector, door contact) to the Advisor Advanced system. Each device is identified by a zone number or a name. For example, zone 14, Fire Exit Door.</td>
</tr>
</tbody>
</table>
Index

A

access control, 74
   reporting, 230
access denied, 221, 229
access options, 268
access zone, 47
account, 300
action, 83, 246, 250
   creating, 250
   deleting, 251
   name, 250
action list, 83
actions
   view, 246
active walk test, 90, 145
add
   action, 250
   audio device, 180
   central station, 280
door, 217
door group, 235
event, 239
expander, 168
filter, 238
fob, 104, 211
keypad, 160
macro, 176
output, 240
PC connection, 306
reader, 178
region, 237
schedule, 248
special day, 251
time frame, 249
trigger, 244
user, 182
user group, 189
zone, 191
adding a central station, 280
adding a door group, 235
adding a door to the system, 217
adding a filter to the system, 238
adding a macro to the system, 176
adding a PC connection, 306
adding a region, 237
adding a schedule, 248
adding a special day, 251
adding a time frame, 249
adding a trigger, 244
adding a user group, 189
adding a user to the system, 182
adding an action, 250
addressing, 32, 276
alarm, 142
   restore, 271
alarm confirmation, 273
alarm control, 220
alarm history, 136
alarm reporting, 92
alarm restore, 271
anti-mask, 194
anti-passback, 75, 234
APN, 303
area, 52, 193, 206
   entry/exit time, 206, 207
   hierarchy, 52, 210
   prealarm time, 208
   selection mode, 186
   unset delay, 208
   warning time, 208
area group, 52, 211
   assign areas, 211
   name, 211
area indicator, 165
area modifier, 282, 284
area selection mode, 186
area shunt, 224
area status, 166
arm, 54
armed display, 263
   timeout, 256
ATM, 114, 279
   delay, 279
   extended unset time, 279
   unset time, 279
   unset warning time, 279
audio device, 115, 179
   isolate, 181
   name, 180
   settings, 180
audio session, 289
test, 91
auto configuration, 4, 132
auto test, 201
automatic battery test, **152**
autoset, **101, 208, 209**

**B**
battery
status, 151
battery replacement, 17, 153
battery test, **151**
automatic test, 152
battery replacement, 153
duration, 152, 153
frequency, 152
bus device, 62
bus devices, **159**
buzzer, 278

**C**
calendar, **83, 246**
callback, 308
camera, **109, 214**
filter, 215
isolate, 216
taking picture, 216
zone list, 214
camera diagnostics, 111
camera range test, 139
card
assign, 184
check, 154
remove, 184
card & PIN mode, 163
card and PIN, 226
card and PIN timeout, 256
card format, 226
card reader, **14**
card to PIN time, 268
central station, 280
backup, 94
creating, 280
deleting, 285
mapping, 92
primary, 93
challenge code, 262
change PIN, 183
changing a door, 218
changing a user, 183
changing user group, 189
check card, 154
chime, 195, 277
CID codes, 353
classic addressing scheme, 276
cloud, 310
cloud solution, 117
code tamper, 58, 122
combined reporting, 93

communication, **280**
account code, 282
auto-answer, 308
callback, 308
central station, 280
cloud, 310
destination name, 286, 309
destination port, 286, 309
Downloader, 314
encryption, 287
events, 290
frequent heartbeat, 287
GSM, 297
GSM network, 298, 299
heartbeat, 287
line number, 287
PC connection, 306
phone number, 285
protocol, 281, 283
receiver number, 287
subevents, 284
test, 91
Titan, 314
transmission path, 281, 291
UltraSync, 310
video port, 287
condition filter, 80, 252
condition filters, **238, 241**
configuration software, 314
configure
area, 206
area group, 211
audio device, 180
condition filter, 238
door, 218
event, 177, 239
expander, 168
fob, 212
input, 270
keypad, 160
macro, 176
macro output, 178
output, 240
part set, 265
reader, 179
user, 183
zone, 192, 270
confirmed alarm test, 90, 145
creating a central station, 280
creating a door, 217
creating a door group, 235
creating a filter, 238
creating a macro, 176
creating a PC connection, 306
creating a region, 237
creating a schedule, 248
creating a special day, 251
creating a time frame, 249
creating a trigger, 244
creating a user, 182
creating a user group, 189
creating an action, 250
credit, 300
custom LCD message, 263

date, 254
daylight saving time, 254
default, 158
default values, 31
defaulting panel, 31
defaults, 130, 272
de-isolate, 193
delayed unset, 55
delete
  audio device, 181
door, 225
  expander, 170
  filter, 239
  keypad, 168
  macro, 178
  notification, 312
  output, 244
  reader, 179
  zone, 203
deleting a central station, 285
deleting a door group, 236
deleting a PC connection, 307
deleting a region, 237
deleting a schedule, 252
deleting a special day, 252
deleting a time frame, 249
deleting a trigger, 245
deleting a user, 186
deleting a user group, 190
deleting an action, 251
demo, 154
deny access, 229
detector test, 140
  auto test, 201
  duration, 140
  manual test, 140
  time, 140
device states, 159
DHCP, 294
dialler
  battery, 151
disable door, 155
disable duress, 228
disarm, 54
DNS, 295

door, 74, 217
  alarm control, 229
  anti-passback, 234
  area groups, 221
  areas, 220
  changing, 218
  control, 155
  creating, 217
  delete, 225
deny access, 221, 229
disable RTE, 230
DOTL output, 233
DOTL reporting, 231
DOTL zone, 228
EE PIN lock, 222
extend unlock time until opened, 228
extended time, 219
forced door, 231, 233
group, 75, 235
indication, 225, 233
intelligent door, 74
interlock, 231
location, 218
lock, 221
lock when closed, 228
low security, 221, 232
move, 224
name, 218
open and close reporting, 231
output, 219, 235
outside user, 234
pulsed lock and unlock, 77, 229
reader options, 225
readers, 218
region, 234
reporting, 230
RTE, 222
RTE control, 230
RTE reporting, 231
RTE schedule, 232
RTE zone, 230
schedule, 222
second zone, 228
shunt, 75, 222
standard door, 74
time, 219
unlock, 221, 222
user group, 229
warning output, 233
zone, 220
door control, 155
door controller, 74
  options, 269
  outputs, 233
door group, 75, 235
  creating, 235
  deleting, 236
door group
  name, 236
door held open, 225
door shunt, 75, 222, 225
   entry/exit, 225
   extended time, 223
time, 223
warning, 223
zones, 232
door shunt time, 223
door shunt warning, 223
DOTL
   output, 233
DST, 254
DTMF control, 116, 289
dual loop, 170
dual unset, 209
duress
   disable, 228

E
earthing, 21
EN 50131 requirements, 65
enable door, 155
encryption, 287, 293
   key, 308
end time, 249, 252
engineer lockout, 259
engineer reset, 113, 259
   auto reset, 261
   disable when service in, 261
engineer walk test, 88, 143, 195
entry
   extend time, 196
entry alarms, 209
entry time, 196, 207
entry timer, 264
entry/exit, 47, 49, 200
   access, 266
   full set, 266
   PIN lock, 164
entry/exit door shunt, 225
entry/exit time, 206, 207
entry/exit zone, 166, 167
EOL, 25, 170, 270
event, 86
   event list, 337
events, 290
   mapping, 290
exit terminator, 48, 196, 257
exit time, 206
exit timer, 264
expander, 63, 159, 168
dual loop, 170
EOL, 170
input mode, 170
isolate, 170
name, 169
resistor values, 170
settings, 169
single zone, 170
troubleshooting, 324
extend entry timer, 196
extend test call, 147
extended door shunt time, 223
extended time, 219
extended unset time, 279

F
failed to communicate, 94
fault, 142
fault indication, 264
filter, 238
   creating, 238
   delete, 239
final door, 196
final set, 257
firewall, 296
firmware, 316
firmware upgrade
   remote, 311
flash, 316
flexible addressing scheme, 276
fob, 184, 211
   add, 104, 211
   assigned user, 212
   buttons, 212
   name, 212
   remove, 214
forced set, 266
formula, 177, 238
frame rate, 174
frequent heartbeat, 287
frequent test call, 147
FTC, 94
function key, 60, 165

G
gateway, 295
glossary, 365
GPRS, 303
   disconnection time, 304
   line fault, 304
   password, 303
   picture limit, 297
   user name, 303
GPRS network
   registration, 150
   state, 150
gross level, 204
GSM, 297
  battery status, 151
  reporting, 288
GSM network, 298
  availability, 298
  code, 150
  diagnostic, 149
  PIN status, 149
  registration, 149
  scan, 299
  signal strength, 150

H
HDR, 138
heartbeat, 287
  frequent, 287
held open alarm, 199
  time, 258
hierarchy, 210
high current output, 278
high security, 210
high security region, 76, 235
high security user, 76, 235
  prewarning time, 235
housing, 8
HSR, 76, 235
HSU, 76, 235

I
IN reader, 218
inactive days, 139, 258
inhibit, 56, 193
inhibit limit, 210
input, 191
  delay, 258
  options, 270
  resistance, 139
  test, 137
input mode, 170
input state, 137, 142
inspection, 262
  date, 262
installation, 130
installer, 64
  in-time, 257
  user confirmation, 259
installer code, 132
installer in, 262
intelligent door, 74
interlock, 231
invert output, 241
inverted walk test, 139
  timer, 258
IP
  picture limit, 297
IP address, 294
IP diagnostic, 147
IP interface, 148
IP statistics, 148
ISDN
  point to point, 294
isolate, 56, 193
  camera, 216
  keypad, 164
  isolation limit, 210
K
key, 58, 196
key box
  time, 258
key switch, 48, 196
keypad, 13, 63, 159, 160
  buzzer, 278
  troubleshooting, 324
keypad layout, 128
keypad lockout, 58, 122
L
LAN device, 62
LCD
  EE timer, 264
  LCD backlight, 166
  LCD message, 263
  LCD options, 263
  LCD reader, 179
LDR, 138
learn card, 184
LED, 227
LED test, 141
limit reports, 201, 271
line number, 287
link speed, 297
listen-in, 155, 167, 179, 201, 213, 288
  test, 155
listing open zones, 137
lock door, 155, 221
lock user data, 65
lock when closed, 228
lockout, 58, 122
log, 136
logic, 80
logout, 158, 262
low security, 221
M
MAC, 297
macro, 176
  creating, 176
  delete, 178
mains fail reporting delay, 256
manual test, 140, 147
map door controller relays, 269
map panel LEDs, 270
Index

menu entries, 263
  accessing, 124
  confirmation of changes, 127
  exit, 127
  explanation of the LCD display, 125
  how to edit host address, 127
  how to edit list, 126
  how to edit text, 126
  how to program values, 125
  how to program Yes/No options, 126
  programming, 125
  scrolling the list of menus, 125
  unauthorized access, 122
  using PIN, 122
menu tree, 380
MMS, 304
  limit, 305
  proxy, 305
Mobile App, 120
monitor output 3, 278
move a door, 224
multiple badge time, 269

N
need acceptance, 124
need to set, 144
notification, 311
  delete, 312
  event, 312
  identifier, 312
  name, 311
  user, 312
NTP, 149, 296

O
OH 2000, 286
omit first call, 292
open door, 155
open zones, 137
OUT reader, 218
output, 31, 73, 235, 238
  active time, 243
  add, 240
  alarm, 235
  delay, 243
  delete, 244
  DOTL, 233
  edit, 240
  forced door, 233
  mode, 241
  name, 240
  siren, 278
  test, 141
  warning, 233
outside user, 234

P
panel diagnostics, 153
panel ID, 309
panel information, 156
panel lid, 157
panel status, 142
panel version, 156
panic alarm, 167, 276
part set, 54, 200
  name, 266
  options, 265
PC connection, 306, 314
  creating, 306
  deleting, 307
  host, 309
  port, 309
PCB, 12
picture auto deletion, 175
picture frame rate, 174
picture options, 173
picture quality, 174
picture settings, 173
PIN, 71, 183, 298
ping, 148, 286, 296, 310
point to point, 294
prealarm time, 208
predefined user, 64
prepaid, 300
privilege limitation, 68
programmable functions, 97
programming, 80, 380
programming cameras, 109
programming map, 380
programming users, 182
programming wireless devices, 102
protocol, 281, 283
pry-off tamper, 10
PUK, 149, 298
pulse count, 203
pulsed lock and unlock, 77
  door lock procedure, 78
  door open procedure, 78

Q
quick installation, 2
quick programming, 4
quick set, 164

R
range test, 139
reader, 178, 218
  card and PIN, 226
  card format, 226
  LED, 227
  schedule, 226
  two cards, 226
reader options, 225
Index

ready to set, 264
receiver number, 287
reduced walk test, 145
region, 75, 234
  count limit, 176
  creating, 237
  deleting, 237
  name, 237
region count limit, 176
regulations, 328
reinstall, 158
re-lock delay, 269
remote configuration, 275, 311
  supervisor, 275
remote firmware upgrade, 311
remote login, 184
remote options, 275
remote PIN, 183
remove
  fob, 214
  RF device, 206, 213
replacing battery, 17
reporting, 92
  account code, 282
  limit reports, 201, 271
  phone numbers, 285
request to exit, 199
resistance, 139
resistor values, 170, 270, 271
resolution, 174
RF device
  configuration, 204, 213
  remove, 206, 213
  supervision, 205
RF state, 138
ring setup, 292
RSSI, 138
RTE, 199, 222
  control, 230
  disabled when areas set, 230
  schedule, 232
RTE zone, 230
RTS, 264

S
schedule, 83, 226
  action list, 250
  active schedule, 248
  condition filter, 252
  creating, 248
  date, 248
  deleting, 252
  door unlock, 222
  name, 248
  RTE, 232
  special day, 251
  time, 248
  time frame, 249
scheme, 32, 276
secure cloud, 117
sensor type, 198
serial number, 310, 311
service, 136
  time, 257
  user confirmation, 259
service in, 124, 158, 262
set, 54
set options, 264
shielding, 22
shock sensor, 141, 195, 203
sensitivity, 204
shunt, 49, 56, 140, 201
door, 75, 222
time, 223
type, 223
zone, 56
shunt limit, 210
shunt zones, 232
SIA codes, 353
SIA frequency, 284
silent set, 209
SIM, 298
single zone, 170
single zone walk test, 145
siren, 29
siren EOL, 271
siren output, 278
siren timers, 255
SMS, 301
  center, 302
  charset, 303
  control, 69, 187
  counter, 151
  forwarding, 302
  header, 302
  messages limit, 302
  PIN, 303
  reporting, 69, 187
soak test, 195
time, 258
software revision, 156
special day, 246, 251
  creating, 251
  deleting, 252
  end time, 252
  name, 252
  start time, 252
special walk test mode, 145
standard door, 74
standard walk test, 143
start filter, 241
start time, 249, 252
status, 142
stop filter, 241
stop voice reporting, 201
subevents, 284
supervision, 205
suppress FTC, 284
swinger shunt, 194, 271
system bus, 23
system code, 261
system options, 254

t tamper area, 161
technical alarm, 197
technical zone sensor, 198
telephone number, 285
test, 137
  audio session, 91
  battery, 151
  communication, 91
  listen-in, 155
  two-way audio, 155
test call, 146, 147
  extend test call, 147
  frequent test call, 147
  FTC, 147
test duration, 140
test time, 140
testing system, 88
time and date, 254
time frame, 246
  creating, 249
  deleting, 249
  end, 249
  start, 249
  week days, 249
time zone, 254
timed open, 155
timed unset, 279
  delay, 279
  extended time, 279
  time, 279
  warning time, 279
timers, 254
Titan, 314
transmission path, 281, 291
trigger, 82, 238
  creating, 244
  deleting, 245
  name, 244
  state, 142
troubleshooting, 323
  data gathering panels, 324
  LCD keypads, 324
two cards, 226
two cards time, 268
two-way audio, 115, 155, 167, 179, 201, 213, 288
  test, 155
U
UltraSync, 117, 310
  channel, 289
uninhibit, 193
unlock door, 155, 221
  output, 219
unset, 54
  delayed unset, 55
  unset delay, 208
upgrade, 316
user, 64, 182
  area selection mode, 186
  card, 184
  changing, 183
  creating, 182
  deleting, 186
  language, 185
  PIN, 183
  programming, 182
  user group, 189
user card, 184
user confirmation, 259
user data lock, 65
user group, 66, 189, 229
  changing, 189
  creating, 189
  deleting, 190
  functions, 66
  name, 189
  options, 190
  privilege limitation, 68
  type, 189
user group type, 66
user LCD message, 263
user management, 182
user name, 183
user phone, 186
user privilege, 189
user programmable functions, 97
user walk test, 143, 144, 195
using cameras, 109
V
VdS codes, 353
version, 316
video port, 287
virtual zone, 199
W
walk test, 88, 90, 143, 145, 195
  active walk test, 90, 145
  confirmed alarm, 90, 145
  frequency, 144
  reduced walk test, 145
  single zone, 145
  standard walk test, 143
timeout, 256
walk test mode, 90, 145
warning time, 208, 279
week days, 249
wireless device, 102, 204, 213
  supervision, 205
wireless sensor, 102

Z
zone, 47, 191
  access, 200
  area, 193
  auto test, 201
  connection, 24
  copy, 202
  de-isolate, 193
  delete, 203
  entry/exit, 200
  entry/exit time, 206, 207
  held open alarm, 199
  inhibit, 193, 265
  isolate, 193, 201
  limit reports, 201
  move, 203
  name, 192
  open too long, 199, 258
  options, 193, 270
  part set, 54
  prealarm time, 208
  report as duress, 200
  report as panic, 200
  reporting, 197
  resistance, 139
  RTE, 230
  shunt, 49, 56, 140, 201
  stop voice reporting, 201
  type, 47, 192
  uninhibit, 193
  warning time, 208
  zone acknowledgement, 198
  zone delay, 197
  zone expansion, 31
  zone options, 193
  zone pairing, 195
  zone shunt, 224
  zone type, 47, 192
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
1.2.1.8 Detector test
1.2.1.8.1 Duration
1.2.1.8.2 Test time
1.2.1.8.3 Test when Set
1.2.1.8.4 Manual test
1.2.1.9 Shunt zones
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 Panel status
1.2.4.1 View open ZN
1.2.4.2 Alarms
1.2.4.3 Faults
1.2.5 Walk test
1.2.5.1 Start
1.2.5.2 Walk test opts
1.2.5.3 Single zone WT
1.2.5.4 Test No Bells
1.2.5.5 Active walk test
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
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.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 Jamming menu
    2.2.2.n.4.8.1 Jamm detection
    2.2.2.n.4.8.2 Jamming Sec
    2.2.2.n.4.8.3 Jamm thresh
  2.2.2.n.4.11 Default 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
Four-door expander specific options

2.2.2.n.4.6 Output modules
2.2.2.n.4.7 Region count limit
2.2.2.n.4.8 Macro Logic
   2.2.2.n.4.8.0 Add macro
   2.2.2.n.4.8.m Select macro
      2.2.2.n.4.8.m.1 Macro name
      2.2.2.n.4.8.m.2 Formula
         2.2.2.n.4.8.m.2.x Select event
         2.2.2.n.4.8.m.2.y Select Operator
      2.2.2.n.4.8.m.3 Macro output
         2.2.2.n.4.8.m.3.1 Output Func.
         2.2.2.n.4.8.m.3.2 Duration
         2.2.2.n.4.8.m.3.3 Activate
      2.2.2.n.4.8.m.4 Delete macro

2.2.2.n.4.9 Local Devices

2.2.3 DC/LC Exp Rdrs
   2.2.3.0 Add reader
   2.2.3.n Select reader
      2.2.3.n.2 Reader address
      2.2.3.n.3 Reader options
         2.2.3.n.3.1 Reader name
         2.2.3.n.3.2 LCD
      2.2.3.n.5 Delete reader

2.2.4 Audio devices
   2.2.4.0 Add audio
   2.2.4.n Select audio device
      2.2.4.n.1 Audio type
      2.2.4.n.2 Audio address
      2.2.4.n.3 Audio settings
         2.2.4.n.3.1 Audio name
         2.2.4.n.3.2 Tamper area
         2.2.4.n.3.3 Isolate audio
   2.2.4.n.4 Delete audio
3 User menu

3.1 Users

Common options:

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.4 RF fobs
3.1.n.5 Language
3.1.n.6 User groups
3.1.n.9 Select mode
3.1.n.10 Delete user

Mobile phone options:

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

Access control options:

3.1.n.8 Access options
3.1.n.8.1 Door group
3.1.n.8.2 Trace
3.1.n.8.3 Privileged
3.1.n.8.4 Extended access
3.1.n.8.5 Acc. user type

3.2 User groups

3.2.0 Add UG
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 AG
3.2.n.5 User group filter
3.2.n.6 User group options
3.2.n.7 Schedule
3.2.n.8 Remove user group
4 Zones and areas

4.1 Zone menu

4.1.0 Add zone
4.1.n Select zone

Common options

4.1.n.1 Zone name
4.1.n.2 Zone type
4.1.n.3 Isolated
4.1.n.4 Zone location
4.1.n.5 Zone areas
4.1.n.6 Zone options

4.1.n.6.1 Inhibit
4.1.n.6.2 Isolate
4.1.n.6.3 Excl. in PS1
4.1.n.6.4 Excl. in PS2
4.1.n.6.5 Double knock
4.1.n.6.6 Swinger shunt
4.1.n.6.7 Anti mask
4.1.n.6.8 Zone pairing
4.1.n.6.9 Chime
4.1.n.6.10 Soak test
4.1.n.6.11 Engineer walk test
4.1.n.6.12 User walk test
4.1.n.6.13 Shock sensor
4.1.n.6.14 Extend EE
4.1.n.6.15 Final door
4.1.n.6.16 Key latch
4.1.n.6.17 Key set
4.1.n.6.18 Key unset
4.1.n.6.19 Technical full set
4.1.n.6.20 Technical unset

4.1.n.7 Grs&Pls options
4.1.n.7.1 Pulse count
4.1.n.7.2 Gross level

4.1.n.7 RF details
4.1.n.7.1 Sensor ID
4.1.n.7.2 Sensor type
4.1.n.7.3 Sensor mode
4.1.n.7.4 Supervision
4.1.n.7.5 Sensor opt
4.1.n.7.6 Remove RF dev

4.1.n.8 Listen-in
4.1.n.8.1 Listen mode
4.1.n.8.2 Link audio

4.1.n.9 Copy
4.1.n.9.1 Copy par. from
4.1.n.9.2 Block assign

4.1.n.10 Move zone
4.1.n.11 Delete zone

Shock sensor options

4.1.n.6.21 Technical part set
4.1.n.6.22 Keypad LCD
4.1.n.6.23 Log
4.1.n.6.24 CS report
4.1.n.6.25 Delay timer
4.1.n.6.26 ACK on keypad
4.1.n.6.27 ACK by user
4.1.n.6.28 Sensor type
4.1.n.6.29 Virtual zone
4.1.n.6.30 Held open
4.1.n.6.31 EE set check
4.1.n.6.32 Alarm in PS1
4.1.n.6.33 Alarm in PS2
4.1.n.6.34 Report as
4.1.n.6.35 Auto test
4.1.n.6.36 Shunt
4.1.n.6.37 View isolated
4.1.n.6.38 Stop report
4.1.n.6.39 Limit reports

Wireless sensor options:

4.1.n.9.3 Sensor mode
4.1.n.9.4 Supervision
4.1.n.9.5 Sensor opt
4.1.n.9.6 Remove RF dev
### 4.2 Areas

#### 4.2.1 Area name

- 4.2.2 Exit time
  - 4.2.2.1 Exit time 1
  - 4.2.2.2 Exit time 2
  - 4.2.2.3 PS Exit time 1
  - 4.2.2.4 PS Exit time 2

- 4.2.3 Entry time
  - 4.2.3.1 Exit time 1
  - 4.2.3.2 Exit time 2
  - 4.2.3.3 PS Entry time 1
  - 4.2.3.4 PS Entry time 2

#### 4.2.4 Other timers

- 4.2.4.1 Warning time
- 4.2.4.2 Prealarm time
- 4.2.4.3 Unset delay

#### 4.2.5 Set/unset options

- 4.2.5.1 Entry alarms
- 4.2.5.2 Set retry
- 4.2.5.3 Silent autoset
- 4.2.5.4 Dual unset

#### 4.2.6 Hierarchy

#### 4.2.7 Limits

- 4.2.7.1 Inhibit limit
- 4.2.7.2 Isolate limit
- 4.2.7.3 Shunt limit

#### 4.2.8 Schedule

### 4.3 Area groups

#### 4.3.1 AG name

#### 4.3.2 Areas

### 4.4 RF fobs

#### 4.4.1 Fob name

#### 4.4.2 Assigned user

#### 4.4.3 Buttons

#### 4.4.4 RF details

#### 4.4.5 Listen-in

#### 4.4.6 Remove fob
4.5 Cameras
   4.5.n Select camera
      4.5.n.1 Camera name
      4.5.n.2 Pics by zone
      4.5.n.3 Pics by filter
          4.5.n.3.m Select filter
          4.5.n.3.m.1 Choose filter
          4.5.n.3.m.2 Event type <n>
          4.5.n.3.m.3 Report as
      4.5.n.4 Pics by rep ev
          4.5.n.4.m Select event
      4.5.n.5 Isolated
      4.5.n.6 Max pics 24h
      4.5.n.7 Remote pics
      4.5.n.8 Test pic to CS
### Intelligent door specific options

#### 5.1.n.3 Door readers
- **5.1.n.3.5 Readers opts**
  - 5.1.n.3.5.1 Card and PIN
  - 5.1.n.3.5.2 Two cards
  - 5.1.n.3.5.3 NoSchedule req
  - 5.1.n.3.5.4 Card format
  - 5.1.n.3.5.5 LEDs option
  - 5.1.n.3.5.6 Time&Attendance
  - 5.1.n.3.5.7 Disable Duress

#### 5.1.n.6 Door options
- **5.1.n.6.1 Door zones**
  - 5.1.n.6.1.2 DOTL zone
- **5.1.n.6.2 Door unlocked**
  - 5.1.n.6.2.1 Until closed
  - 5.1.n.6.2.2 Until opened
- **5.1.n.6.3 Alarm control**
  - 5.1.n.6.3.5 User group
  - 5.1.n.6.3.6 Control type
  - 5.1.n.6.3.7 If PIN sets
  - 5.1.n.6.3.7.1 Deny access
- **5.1.n.6.4 RTE options**
  - 5.1.n.6.4.2 RTE zone
  - 5.1.n.6.4.3 Dis. when set
- **5.1.n.6.5 Reporting**
  - 5.1.n.6.5.1 CL & Locked
  - 5.1.n.6.5.2 OP&Unl as Unl
  - 5.1.n.6.5.3 Open/Close
  - 5.1.n.6.5.4 Forced door
  - 5.1.n.6.5.5 DOTL
  - 5.1.n.6.5.6 RTE
- **5.1.n.6.6 Interlocking**
- **5.1.n.7 Schedule opts**
  - 5.1.n.7.1 Door unlocked
  - 5.1.n.7.2 Low Security
  - 5.1.n.7.3 RTE Schedule
- **5.1.n.8 Shunt options**
  - 5.1.n.8.1 Zones
  - 5.1.n.8.4 Indication
  - 5.1.n.8.5 Until door CL
  - 5.1.n.8.6 CancelAfterCL
- **5.1.n.9 Regions & AP**
  - 5.1.n.9.1 Regions
  - 5.1.n.9.2 Anti-passback
  - 5.1.n.9.3 Inh Reg 1 Usr
  - 5.1.n.9.4 HSU options
  - 5.1.n.9.4.1 Req HSU Nr
  - 5.1.n.9.4.2 Prewarn. time
  - 5.1.n.9.4.3 HS alarm out
5.2 Door groups
- 5.2.0 Add Door Gr
- 5.2.n Select door group
  - 5.2.n.1 Door Gr name
  - 5.2.n.2 Door Gr data
  - 5.2.n.3 Delete Door Gr

5.3 Regions
- 5.3.0 Add region
- 5.3.n Select region
  - 5.3.n.1 Region name
  - 5.3.n.2 Delete region

6 Outputs and filters
6.1 Condition filters
- 6.1.0 Add filter
- 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
  - 6.1.n.4 Delete filter

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

6.3 Triggers
- 6.3.0 Add trigger
- 6.3.n Select trigger
  - 6.3.n.1 Trigger name
  - 6.3.n.2 Schedule
  - 6.3.n.3 Delete trigger

6.1.0 Add filter
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
- 6.1.n.4 Delete filter

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

6.3.0 Add trigger
6.3.n Select trigger
- 6.3.n.1 Trigger name
- 6.3.n.2 Schedule
- 6.3.n.3 Delete trigger
### 7 Calendar

#### 7.1 View
- **7.1.n Date**
  - 7.1.n.1 Auto setting
  - 7.1.n.2 By object
  - 7.1.n.3 Special day
    - 7.1.n.3.1 Day type
    - 7.1.n.3.2 Recurring
    - 7.1.n.3.3 Until date

#### 7.2 Schedules
- **7.2.0 Add schedule**
- **7.2.n Select schedule**
  - 7.2.n.1 Schedule name
  - 7.2.n.2 Active
  - 7.2.n.3 Date
  - 7.2.n.4 Time
    - 7.2.n.4.0 Add time frame
    - 7.2.n.4.m Select time frame
      - 7.2.n.4.m.1 Start time
      - 7.2.n.4.m.2 End time
      - 7.2.n.4.m.3 Week days
  - 7.2.n.5 Action list
    - 7.2.n.5.0 Add action
    - 7.2.n.5.m Select action
      - 7.2.n.5.m.1 Action name
      - 7.2.n.5.m.2 Object type
      - 7.2.n.5.m.3 Function
      - 7.2.n.5.m.4 Parameters
  - 7.2.n.6 Special days
    - 7.2.n.6.0 Add special day
    - 7.2.n.6.m Select special day
      - 7.2.n.6.m.1 Special day name
      - 7.2.n.6.m.2 Start time
      - 7.2.n.6.m.3 End time
    - 7.2.n.6.m.4 Delete special day
  - 7.2.n.7 Filter
  - 7.2.n.8 Delete schedule
    - 7.2.n.8.m Delete schedule
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 Service in
  8.2.6 Challenge code
  8.2.7 Inspection
    8.2.7.1 Date
    8.2.7.2 Custom msg

8.3 LCD display options
  8.3.1 Armed display
  8.3.2 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 Part set
  - 8.4.3.1 Report BA
  - 8.4.3.2 Access to EE
  - 8.4.3.3 EE full set
  - 8.4.3.4 PS1 name
  - 8.4.3.5 PS2 name
- 8.4.4 Forced set
- 8.4.5 Forced set options
- 8.4.6 Pending alarms
- 8.4.7 AS fault retry
- 8.4.8 AS user retry

### 8.5 Access options
- 8.5.1 Access timers
  - 8.5.1.1 Card to PIN
  - 8.5.1.2 Two cards
  - 8.5.1.3 Multiple badge
  - 8.5.1.4 Re-lock delay
- 8.5.2 DGP options
  - 8.5.2.1 Map relays
  - 8.5.2.2 Map panel LEDs

### 8.6 Zone options
- 8.6.1 Input mode
- 8.6.2 EOL
- 8.6.3 Siren tamper EOL
- 8.6.4 Swinger shunt
- 8.6.5 Report restore
## Communication

### 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

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

- **IP and GSM/GPRS specific options:**
  - 9.1.n.4 Destination/IP

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

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

- **Audio specific options**
  - 9.1.n.10 Listen-in

- **Delete CS**

- **IP and GSM/GPRS specific options:**
  - 9.1.n.8.3 OH 2000

- **9.1.n.8 Protocol opt**
  - 9.1.n.8.1 XSIA
  - 9.1.n.8.2 VOICE
    - 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.8.2.1 Suppress FTC
  - 9.1.n.8.2.2 Without ACK

- **9.1.n.9 OP/CL report**

- **9.1.n.10 OP/CL report**

- **9.1.n.11 Delete CS**

### 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.8.2 VOICE
    - 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.8.2.1 Suppress FTC
  - 9.1.n.8.2.2 Without ACK

- **9.1.n.9 OP/CL report**

- **9.1.n.10 OP/CL report**

- **9.1.n.11 Delete CS**

### 9.1.n.4 Destination

- **9.1.n.4.1 Type**

- **9.1.n.4.2 Phone/User/UG**

### 9.1.n.4.4 Encryption

- **9.1.n.4.5 Vid dest port**

### 9.1.n.5.m Select area

- **9.1.n.5.1.1 Dest name**

- **9.1.n.5.1.2 Dest port**

- **9.1.n.5.1.3 Ping host**

### 9.1.n.6 Mode

- **9.1.n.6.1 Type**

### 9.1.n.7 Retry count

- **9.1.n.7.1 Type**

### 9.1.n.8 Protocol opt

- **9.1.n.8.1 XSIA**

- **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.9.1 Type**

### 9.1.n.10 OP/CL report

- **9.1.n.10.1 Enable**

- **9.1.n.10.2 Time**

- **9.1.n.10.3 DTMF control**

### 9.1.n.11 Delete CS

- **9.1.n.11.1 Type**

### 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
- 9.2.4 Lis-in events

### 9.3 Path options

- **9.3.n Select path**

  **Common options:**
  - 9.3.n.1 Path name
  - 9.3.n.2 Line fault
  - 9.3.n.4 Expander menu
  - 9.3.n.8 Ring setup
  - 9.3.n.8.1 Ring count
  - 9.3.n.8.2 Omit 1st call
  - 9.3.n.9 Encryption

  **PSTN specific options:**
  - 9.3.n.3 Line fault delay
  - 9.3.n.4 Transm path
  - 9.3.n.5 Dial tone
  - 9.3.n.6 Dialing

  **ISDN specific options**
  - 9.3.n.6 Point to Point
  - 9.3.n.7 MSN

  **IP specific options**
  - 9.3.n.3 Transm path
  - 9.3.n.4 IP config
    - 9.3.n.4.1 IP config
    - 9.3.n.4.2 IP address
    - 9.3.n.4.3 Subnet mask
    - 9.3.n.4.4 Gateway
  - 9.3.n.5 DNS config
    - 9.3.n.5.1 DNS config
    - 9.3.n.5.2 DNS server
  - 9.3.n.6 NTP config
    - 9.3.n.6.1 NTP config
    - 9.3.n.6.2 NTP server
  - 9.3.n.7 Firewall
    - 9.3.n.7.1 Firewall
    - 9.3.n.7.2 Reply on PING
  - 9.3.n.8 Link speed
  - 9.3.n.9 MAC address
  - 9.3.n.10 Max Pics 24h
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.6 SMS Setup
  9.3.n.6.1 SMS Center num
  9.3.n.6.2 SMS forwarding
  9.3.n.6.3 Max Msg 24h
  9.3.n.6.4 SMS header msg
  9.3.n.6.5 User PIN req.
  9.3.n.6.6 Ext.charset

9.3.n.7 GPRS Setup
  9.3.n.7.1 APN
  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.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 conn
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 Modern protocol

GSM specific options:

9.4.1.n.3 Conn. type

IP 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

9.4.5 Listening port
9.4.6 Panel ID

9.5 UltraSync

9.5.1 Connectivity
9.5.2 SID number
9.5.3 Settings

9.5.3.1 Password
9.5.3.2 FW Upgrade
9.5.3.3 Remote configuration
9.5.3.4 Notifications

9.5.4 Notification list

9.5.4.n Select notification

9.5.4.n.1 Notification name
9.5.4.n.2 Identifier
9.5.4.n.3 Assigned user
9.5.4.n.4 Notification events
9.5.4.n.5 Delete notification