Contents:

1  Control panel architecture .................................. 3
    1.1  Required system configuration 3
2  Preparing the control panel for installation ........ 3
3  Control panel main board................................... 3
    3.1  Main board terminal description: 3
    3.2  Hard-wired inputs on the main board 4
    3.3  Installation of additional hard-wire input modules 4
    3.4  Radio module installation 4
    3.5  Y,X,V communicator module installation 4
    3.6  Control panel memory chip 4
    3.7  Wired keypad connection 4
    3.8  Control panel resetting 5
4  Control panel power supply ............................... 5
    4.1  Backup battery connection 5
    4.2  Power supply connection 5
    4.3  Powering-up the control panel for the first time 5
5  Oasis wireless devices..................................... 6
    5.1  Enrolling wireless devices to the control panel 6
    5.2  Testing enrolled wireless devices 6
    5.3  Signal strength measuring 6
    5.4  Erasing enrolled devices 6
    5.5  Enrolling the control panel to UC and AC modules 6
6  Control panel programming ............................... 6
    6.1  Exit delay time 7
    6.2  Entrance delay time 7
    6.3  Alarm duration time 7
    6.4  PGX and PGY functions 7
    6.5  Changing telephone numbers in maintenance mode 7
    6.6  Radio interference indication 7
    6.7  Radio communications supervision 7
    6.8  RESET enabled 7
    6.9  Enrollment to a sub control panel for setting control 7
    6.10  Master code reset 8
    6.11  Enrollment to other devices (UC, AC) 8
    6.12  Setting (Arming) without an access code 8
    6.13  Triggered-detector indication 8
    6.14  Confirmation of intruder alarms 8
    6.15  Exit delay beeps 8
    6.16  Exit delay beeps while partially setting (arming) 8
    6.17  Entrance delay beeps 8
    6.18  Setting (arming) confirmed by wired-siren chirp 8
    6.19  Sirens always sound during audible alarms 9
    6.20  Wireless siren alarm enabled (IW and EW) 9
    6.21  Bypass user approval 9
    6.22  Final-door detectors 9
    6.23  Partial setting (arming) or system splitting 9
    6.24  Automatic summer time (daylight saving time) 10
    6.25  Pulse reaction of tamper sensors 10
    6.26  Operating the PG outputs using *8 and *9 10
    6.27  Permanent alarm status display 10
    6.28  Tamper alarm if unset 10
    6.29  Recording PG output activation to memory 10
    6.30  Engineer reset 10
    6.31  Social alarm feature 10
    6.32  Annual check notification 10
    6.33  Only single alarm indication 11
    6.34  Setting (arming) by service code 11
    6.35  Audible panic alarm 11
    6.36  Higher control-panel receiver-sensitivity 11
    6.37  Access by code plus card 11
    6.38  Audible 24 hour intruder alarm 11
    6.39  Service mode only with service and user code 11
    6.40  Device reactions and section assignment 11
    6.41  Code/card reactions and section assignment 12
    6.42  Enrollment by keying in production codes 12
    6.43  Automatic setting / unsetting schedule 12
    6.44  Changing the service code. 12
    6.45  Go to maintenance mode 12
    6.46  Setting the internal clock 12
    6.47  Editing keypad text 13
    6.48  Recommended settings 13
7  Operating the system...................................... 13
    7.1  The system keypad 13
    7.1.1  Keypad indicators........................................ 13
    7.1.2  LCD display .............................................. 13
    7.1.3  Keypad display sleep-mode .......................... 13
    7.1.4  Keys ..................................................... 13
    7.1.5  Functions beginning with the * key ............. 13
    7.2  Programming access codes and cards 13
    7.3  Setting and unsetting (arming/disarming) the system 14
    7.4  Maintenance Mode 14
    7.4.1  Displaying which user/card positions are occupied 14
    7.4.2  Bypassing devices .................................... 14
    7.4.3  Protecting a car near the system ............. 14
8  Operating/programming the system by PC ............. 14
    8.1  Programming access codes and cards ............ 20
    9  Basic guidance for installers .......................... 14
    10  Trouble-shooting ........................................ 15
    11  Control panel technical specifications ........... 16
    12  Control panel programming sequences ............ 17
    13  Programming access codes and cards............. 20

This manual is valid for control panel JA-82K
The control panel can be configured by a PC running OLInk software.
1 Control panel architecture

The JA-82K control panel is a modular unit, with 50 addresses (marked 01 to 50). The heart of the unit is the JA-82K main board with 4 wired inputs. The following additional modules can be plugged into this board:

- **JA-82R** – a radio module which makes it possible to enrol up to 50 wireless devices of the JA-8x and RC-8x range to the control panel.
- **JA-82C** – an extension module which provides 10 additional wired inputs, thus extending the total capacity to 14 wired inputs. (addresses 05 to 14)

A communicator can also be used with the control panel:

- **JA-8xY** – a GSM communicator which the control panel uses for transmitting alarm reports to the user and which communicates with the ARC (alarm receiving centre) via the GSM band. It also enables remote access via a phone keypad, or system administration via the GSMLink website (JA-80Y only) or via Olink software running on an internet enabled computer (JA-82Y only).
- **JA-80V** – a LAN (Ethernet) computer network communicator combined with a phone-line communicator. It allows communication with the ARC via LAN and transmission of reports via a telephone line. It also enables system administration via the GSMLink application.
- **JA-80Q** – must be used in combination with JA-80Y or JA-80V for handling the pictures from the JA-84P (not needed when the JA-82Y communicator is used).
- **JA-80X** – a phone-line communicator which is able to communicate with an ARC and which allows voice-reporting to the user pursuant to the type of alarm. This module can be used in combination with a JA-80Y – a GSM phone-line backup.

The JA-68 outputs module can also be used with the control panel – e.g. to provide a link to the transmitter for communication with the surveillance centre.

The control panel box also houses the power supply and space for a backup battery (up to 2.2 Ah). For a view of the control panel case see fig. 17.

1.1 Required system configuration

The requirements of technical standards (namely of the EN 50131 series) should be observed when planning the system structure. The Oasis control panel complies with safety grade 2. It must have one of the following configurations as a minimum:

- at least two non-backup-battery sirens (JA-80L or SA-105) + ATS2 class communicator (JA-8xY, JA-80V or JA-80X)
- at least one backup-battery siren (JA-80A or OS-360/365/300) + ATS2 class communicator (JA-8xY, JA-80V or JA-80X)

**Note:** the above-recommended configurations are based on the EU standard EN-50131-1 valid at the time of issuing this manual

2 Preparing the control panel for installation

The control panel can be attached to the wall using 3 screws. If the control panel communicates via radio, it should not be installed near any large metal objects capable of shielding radio communication. Route cables (power supplies, telephone leads etc.) inside the control panel before tightly screwing in the screws.

3 Control panel main board

1. Connector for a JA-82R wireless module.
2. Memory chip – for more information see 3.6.
3. Connector for communicators JA-8xY, and possibly a JA-8Q for the manipulation of pictures from detector type JA-84P.
4. Connector for the JA-82C wired input module – it is designed for an input module using addresses from L5 to L14.
5. Digital bus connector.
6. The heart beat LED.
7. The internal wiring connector.
8. RESET link – normally open and serves for resetting the system (if it is short-circuited when the control panel power supply is being switched on). This link can also be used to enter control panel enrollment mode by briefly shorting the link while the control panel is powered.
10. Switch enabling/disabling L1 ... L4 wired inputs.
11. Terminals for transformer output (AC power).
12. Terminals.

3.1 Main board terminal description:

01 to 04 and COM are hard-wired inputs for the control panel. The reactions to triggering inputs 01 to 04 are determined by the settings of addresses 01 to 04. The factory set natural reaction for these hard-wired inputs is a delayed alarm in section C.

**EW**

External warning output, (max. 0.5A). This output is grounded during an alarm. The EW output status is also transmitted for the wireless EW siren.

**IW**

Internal warning output. This output is grounded during an alarm. A hardwired siren can be wired between +U and IW terminals (max. 0.5A). The IW output status is also transmitted for the wireless IW siren.

The difference between the internal warning (IW) output function and the external warning (EW) one lies in their behaviour during the entrance delay period. If any instant reaction detectors are triggered during the entrance delay period, (e.g. by a child running straight to the living room during disarming), only an internal warning is triggered and then the external warning follows only if the entrance delay has been exceeded (but no longer than 30 seconds).

**PGX, PGY**

A pair of programmable outputs. When activated, the outputs switch to GND, with a maximum load of 0.1A/12V. The factory-default setting of PGX is the ON/OFF function (operated by the instruction +81 / +80 or using ON and #OFF keys). PGY is activated if any part of the system is armed. The status of PG outputs is also transmitted to AC and UC wireless output modules by the control panel.

**GND, A,B**

Common ground connection
digital bus data signals

back-up power supply (10 to 14 V). 1A fuse. Max. Continuous load 0.4A (max. Intermittent load 1A, for 15 minutes, once an hour). If the 1A fuse is blown, the control panel will indicate a power supply fault and if armed the alarm is triggered.

Device installation shall only be undertaken by qualified technicians holding a training certificate issued by an authorized distributor. The manufacturer cannot be held responsible for any damage or consequences related to the improper or incorrect installation of this product.
### 3.2 Hard-wired inputs on the main board

There are hard-wired input terminals for 01-04 device addresses on the main board. All hard-wired inputs act identically: double balanced loops which sense loop stand-by, activation or tampering as follows:

- **Stand-by** connected to COM via a 1 kΩ resistor (EOL resistor)
- **Activation** connected to COM via a 2kΩ to 6kΩ resistor
- **Tampering** connected to COM via a less than 700 Ω resistor (short-circuit) or connected to COM via a more than 6kΩ resistor (loop termination)

![fig. 2 SA-200 magnetic detector connection](image)

![fig. 3 JS-20 Largo detector connection](image)

![fig. 4 One-loop connection of JS-25 Combo](image)

![fig. 5 Two-loop connection of JS-25 Combo (01 GBS, 02 PIR)](image)

- **Notes:**
  - The used input zone must be terminated by a 1kΩ resistor in stand-by state.
  - When connecting a trigger contact to the zone, always use a parallel 1kΩ resistor. Thus it is possible to connect up to 5 trigger contacts in series.
  - Tamper contacts should be connected in series (without resistors). They therefore interrupt the whole loop. You can use an unlimited amount of tamper contacts which can be combined with trigger contacts (with parallel resistors).
  - The loop (input) reaction can be set. The NATURAL = delayed loop reaction is set as the factory default.
  - If you enrol a wireless device to the hard-wired input address, the corresponding terminal will be disabled (it will not affect the system).
  - If you do not intend to use the hard-wire input or enrol a wireless device to its address, switch the corresponding DIP switch to the OFF position (switch off the input).

### 3.3 Installation of additional hard-wire input modules

By adding the JA-82C module it is possible to extend the amount of inputs to fourteen. (addresses 01-14).

All hard-wire inputs behave identically: they are double balanced inputs which are able to sense stand-by, activation and tampering and for which examples of connection and conditions stated in Chapter 3.2 apply in full scope.

When you install the module, relabel the terminal description with a sticker from the module package (inputs 05-14). Insert plastic spacing posts on the openings in the module on the connector side and insert the prepared module to the selected position in the main board.

### 3.4 Radio module installation

The JA-82R radio module is installed in position 1 (see fig. 1). The antenna is included in the JA-82R package and it should be screwed on a plastic post (see fig. 17, pos 5). The antenna connector connects to the pins on the JA-82R radio module. The module installation enables the system to enroll up to 50 wireless devices.

### 3.5 Y,X,V communicator module installation

Screw the selected communicator into position using the supplied screws as shown in the picture fig. 17.

If you are installing a GSM communicator (Y) and there is a strong GSM signal in the place of installation, the self-adhesive antenna can be attached directly to the bottom of the plastic box (see fig. 17). If there is a weak GSM signal we recommend using one of the available rod antennas.

If you use the combination of a GSM communicator (Y) and a telephone line communicator (X), install the phone line communicator above the GSM communicator using the supplied posts.

### 3.6 Control panel memory chip

The control panel memory chip plugs into its own socket. If you take the memory unit from the control panel and plug it into another control panel main board of the same type, the control panel settings (enrolled detectors, codes, set functions, etc.) are transferred.

**Notes:**

- communicator settings are not stored in this memory
- do not plug or unplug the memory when the control panel is powered
- when you take the memory unit from a damaged control panel, its contents may be corrupted. It is therefore highly recommended to back-up the settings in a PC using OLink software

### 3.7 Wired keypad connection

The control panel can be operated and programmed by a JA-81E hard-wired keypad. A screened four-cord flat cable connecting the corresponding...
A double-insulated power supply cable should be used with a minimum cross-sectional area of 0.75 to 1.5 mm². The power cable should be fixed and secured in the terminals. The control panel power supply voltage networks: ~ 230 V / 50 Hz.

- Ensure that the battery is correctly connected (Polarity: RED = positive +, BLACK = negative -).

The average backup battery lifetime is up to 5 years after which it must be replaced. Checking its capacity during regular maintenance is recommended. The control panel automatically recharges the backup battery and monitors its condition. When the system runs only on the backup battery, the battery status is monitored and a technical alarm is triggered before its complete depletion. The backup battery is then disconnected. Once the power supply has been restored, the battery reconnects and is recharged. Ensure that the battery is correctly connected (Polarity: RED = positive +, BLACK = negative -).

The control panel power supply is double-insulated (safety class II) and does not incorporate a protective grounding wire.

The control panel power supply cable should only be installed by a person holding a sufficient electro-technical qualification.

The control panel power supply should be used with a minimum cross-sectional area of 0.75 to 1.5 mm². The power cable should be fixed and secured in the terminals. The control panel power supply voltage networks: ~ 230 V / 50 Hz.

- A double-insulated power supply cable should be used with a minimum cross-sectional area of 0.75 to 1.5 mm². The power cable should be fixed and secured in the terminals.

- The control unit JA-101K (-LAN) provides power supply terminals to select from 2 type of power supply voltage networks: ~ 230 V / 50 Hz and ~110 V / 60 Hz. According to the type of power supply voltage system, the control panel connects the main power supply and the corresponding fuse must be used in comply with chapter no. 15 Technical parameters. Fix the cable firmly to the cable holder in the control panel making sure that the wire ends are properly secured and connected in the terminals.

4.2 Power supply connection

The control panel power supply is double-insulated (safety class II) and does not incorporate a protective grounding wire.

ATTENTION – the backup battery is sold charged, avoid shorting out its terminals!

2. Check the backup battery connection
3. Switch the power supply on – a green LED starts flashing on the control panel board.
4. If a hard-wired keypad is connected it indicates “Service” mode
5. The control panel can also be set up via the interface using OLink software – (A virtual keypad can be used in OLink to indicate system status).
6. If you have neither the wired keypad, nor OLink, enrol a wireless keypad by the following means:
   a) have an opened keypad and its battery ready,
   b) check that the green LED in the control panel is flashing,
   c) short the RESET link in the control panel for 1 second (enrollment mode opens),
   d) install batteries into the keypad not far from the control panel

**Table: Power consumption of individual components**

<table>
<thead>
<tr>
<th>device</th>
<th>mA</th>
<th>note</th>
</tr>
</thead>
<tbody>
<tr>
<td>JA-82K control panel</td>
<td>30</td>
<td>without a communicator</td>
</tr>
<tr>
<td>JA-82R module</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>JA-82C module</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>JA-81E keypad</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-81E RGB keypad</td>
<td>up to 100</td>
<td></td>
</tr>
<tr>
<td>JA-80H (N) keypad</td>
<td>60</td>
<td>including WJ-80 interface</td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>JA-80V communicator</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

Wireless devices are not powered from the control panel.

4.3 Powering-up the control panel for the first time

1. First check all the wiring, and if a GSM communicator is installed, insert its SIM card (PIN code disabled).
2. Check the backup battery connection
3. Switch the power supply on – a green LED starts flashing on the control panel board.
4. If a hard-wired keypad is connected it indicates “Service” mode
5. The control panel can also be set up via the interface using OLink software – (A virtual keypad can be used in OLink to indicate system status).
6. If you have neither the wired keypad, nor OLink, enrol a wireless keypad by the following means:
   a) have an opened keypad and its battery ready,
   b) check that the green LED in the control panel is flashing,
   c) short the RESET link in the control panel for 1 second (enrollment mode opens),
   d) install batteries into the keypad not far from the control panel

**Table: Power consumption of individual components**

<table>
<thead>
<tr>
<th>device</th>
<th>mA</th>
<th>note</th>
</tr>
</thead>
<tbody>
<tr>
<td>JA-82K control panel</td>
<td>30</td>
<td>without a communicator</td>
</tr>
<tr>
<td>JA-82R module</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>JA-82C module</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>JA-81E keypad</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-81E RGB keypad</td>
<td>up to 100</td>
<td></td>
</tr>
<tr>
<td>JA-80H (N) keypad</td>
<td>60</td>
<td>including WJ-80 interface</td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>JA-80V communicator</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

Wireless devices are not powered from the control panel.

4.3 Powering-up the control panel for the first time

1. First check all the wiring, and if a GSM communicator is installed, insert its SIM card (PIN code disabled).
2. Check the backup battery connection
3. Switch the power supply on – a green LED starts flashing on the control panel board.
4. If a hard-wired keypad is connected it indicates “Service” mode
5. The control panel can also be set up via the interface using OLink software – (A virtual keypad can be used in OLink to indicate system status).

**Table: Power consumption of individual components**

<table>
<thead>
<tr>
<th>device</th>
<th>mA</th>
<th>note</th>
</tr>
</thead>
<tbody>
<tr>
<td>JA-82K control panel</td>
<td>30</td>
<td>without a communicator</td>
</tr>
<tr>
<td>JA-82R module</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>JA-82C module</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>JA-81E keypad</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-81E RGB keypad</td>
<td>up to 100</td>
<td></td>
</tr>
<tr>
<td>JA-80H (N) keypad</td>
<td>60</td>
<td>including WJ-80 interface</td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>JA-80V communicator</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

Wireless devices are not powered from the control panel.

4.3 Powering-up the control panel for the first time

1. First check all the wiring, and if a GSM communicator is installed, insert its SIM card (PIN code disabled).
2. Check the backup battery connection
3. Switch the power supply on – a green LED starts flashing on the control panel board.
4. If a hard-wired keypad is connected it indicates “Service” mode
5. The control panel can also be set up via the interface using OLink software – (A virtual keypad can be used in OLink to indicate system status).
6. If you have neither the wired keypad, nor OLink, enrol a wireless keypad by the following means:
   a) have an opened keypad and its battery ready,
   b) check that the green LED in the control panel is flashing,
   c) short the RESET link in the control panel for 1 second (enrollment mode opens),
   d) install batteries into the keypad not far from the control panel

**Table: Power consumption of individual components**

<table>
<thead>
<tr>
<th>device</th>
<th>mA</th>
<th>note</th>
</tr>
</thead>
<tbody>
<tr>
<td>JA-82K control panel</td>
<td>30</td>
<td>without a communicator</td>
</tr>
<tr>
<td>JA-82R module</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>JA-82C module</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>JA-81E keypad</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-81E RGB keypad</td>
<td>up to 100</td>
<td></td>
</tr>
<tr>
<td>JA-80H (N) keypad</td>
<td>60</td>
<td>including WJ-80 interface</td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>JA-80V communicator</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>JA-80X communicator</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

Wireless devices are not powered from the control panel.
e) the keypad emits a beep and enrols to the first free address. After that it displays “Enrollment” and offers another free address for enrollment.

f) Pressing the # key exits enrollment mode and the “Service” *) message appears on the keypad.

g) check whether the keyboard functions in the place where you intend to install it and then install its plastic rear part.

*) The keypad comes with English texts from production – these can be changed to other languages – see the manual.

Note: If the “Service” message fails to appear on the connected wired keypad or if the wireless keypad is not enrolled, the control panel settings are not the factory-defaults – perform a reset (see 3.8.)

5 Oasis wireless devices

The control panel had 50 addresses (01 to 50), allowing the enrollment of up to 50 wireless devices (detectors, keypad, key fobs, sirens, etc.). A device can be assigned to an address either by enrollment or by typing its serial number while in Service mode (see 6.42).

Wireless devices can be installed at their intended locations and then enrolled to the control panel or vice versa. If there are any doubts as to the suitability of devices for communication, temporarily attach the devices (e.g. using adhesive tape) in the selected place and test radio communication before finalizing installation. Follow the manuals of the particular devices during their installation.

5.1 Enrolling wireless devices to the control panel

1. The control panel must be in Service mode. If this is not the case, enter *0 service code (factory default: 8080). The control panel must be disarmed.

2. Press the “+1” key to enter enrollment mode. The first vacant address is then offered.

3. You can select the desired address using the +1 and +7 keys (If the address is already occupied, the A indicator is lit).

4. The device can be enrolled to the selected address by connecting its battery (power).

5. Enrollment to the given address is confirmed by the A indicator and the next vacant address is then offered,

6. Enrol all devices to the control panel one after another by connecting batteries to them. Press the # key to exit enrollment mode.

Notes:
• Enrolment of a wireless device to a hard-wire input address disables the corresponding terminal (when the wireless device is erased, the terminal is enabled again).

• RC-8x type key fobs are enrolled to the control panel by pressing and holding two buttons at the same time: +0 или +1. This means that a 4-button key fob can be enrolled to the control panel as two different pairs of buttons and different features can be assigned to them – see 6.40.

• Only a single device can be enrolled to each address,

• When an address is occupied (the A indicator lights), no more new devices can be enrolled to it.

• If a device has already been enrolled to an address, and it is then re-enrolled to another address, the device’s address assignment changes from the original address to the new one.

• If a device cannot be enrolled to the control panel, it does not have a good connection to the control panel (the device must be at least 2 m away from the control panel and an antenna must be connected to the control panel during enrollment).

• To re-enroll a device, first disconnect its battery. Then wait about 10 minutes after closing their cover. After that the detectors ignore frequent movements (see the detector manual). Test mode can be extended by opening and closing its cover.

• Devices can also be tested in Maintenance mode – see 7.4.

5.3 Signal strength measuring

1. The control panel must have its antenna connected and it must be in Service mode (If this is not the case, enter *0 service code (factory default: 8080). The control panel must be disarmed).

2. Key in 298, and the lowest enrolled device address is displayed

3. Trigger this device. The keypad (its cover should be flipped open) displays signal quality ranging from 1/4 to 4/4.

4. Use +1 and +7 keys to select other enrolled devices and measure their signal strength.

5. Exit signal measuring by pressing the # key.

Notes:
• The JA-80P and JA-85P motion detectors can be tested max. 15 minutes after closing their cover. After that the detector ignores frequent movements (see the detector manual).

• Measuring the signals from the JA-80L internal siren can be activated by pressing its button. The JA-80A outdoor siren and wireless keypad signal can be measured by triggering the IN input or triggering its cover tamper switch.

• Each installed device should have the minimum signal strength of 2/4. If the signal is too weak, the device should be relocated or higher control panel sensitivity can be selected. (see 6.36) Alternatively, the control panel can be equipped with an external antenna.

• This measurement allows the strength of the signal received from the device by the control panel.

• The wireless keypad can be carried during device testing, its tamper contact can be disabled via the jumper (near the tamper contact – do not forget to re-enable the tamper upon finishing the servicing) – i.e. the keypad usually has a slightly shorter communication range than the detectors. Therefore, if carried to more-distant detectors the triggering of the detectors might not be shown.

• The most convenient way of measuring is via a computer using OLink SW.

5.4 Erasing enrolled devices

1. The control panel must be in Service mode. If this is not the case, enter *0 service code (factory default: 8080). The control panel must be disarmed.

2. Key in “+1” to enter enrollment mode and select the desired address of the device you wish to erase using the arrow keys.

3. Press and hold the “2” key until a beep is heard and the A indicator turns off.

4. When all the desired devices have been erased press #.

Notes:
• To erase all wireless devices, press and hold the “4” key in enrollment mode.

• If a wireless keypad is erased by the above mentioned means, it stops communicating with the control panel and you must re-enroll it again (see 3.4).

5.5 Enrolling the control panel to UC and AC modules

If you wish to transmit PGX and PGY programmable output signals to the UC-82 and AC-82 output modules, you must enrol the control panel to these modules as follows:

1. The control panel must be in Service mode. If this is not the case, enter *0 service code (factory default: 8080). The control panel must be disarmed.

2. Enter the control panel enrollment mode on the UC or AC module (see 3.4).

3. Key in 299 on the control panel keypad – the LEDs on the module will flash a few times.

Notes:
• we recommend locating the module close to the control panel during enrollment or carry the wireless keypad close to the module.

• the control panel can be enrolled to the desired number of UC/AC modules (each PG output can thus have an output at an arbitrary number of places in the house).

• PG outputs are enrolled to UC and AC module relays individually (PGX output to the X relay, PGY output to the Y relay). This means that either one or both modules can be enrolled to the module if requested.

• Only one control panel can be enrolled to a UC or AC receiver (a control panel repeats its PG signal every 9 minutes).

6 Control panel programming

The most convenient way to program the system is to use a PC running OLink software. However, the system can also be programmed by keying in the below mentioned sequences. The sequence summary table can be found at the end of this manual.
6.1 Exit delay time

An exit delay time occurs while setting (arming) the system. During this time period delayed or next-delayed detectors can be triggered without an alarm occurring. To program the delay time, enter:

\[ 2 \times \]

where \( x \) is a number from 1 to 9 determining the duration in steps of tens of seconds (1=10 s, 2=20 s, ...,).

If there is a final-door detector in the system then the exit delay is multiplied by 30 s instead (1=30 s, 2=60 s, ...).

**Example:** To program a 20 seconds exit delay, use the sequence 202 (if there is a final-door detector, a 60 seconds delay will result).

**Factory default setting:** \( x = 3 \)

6.2 Entrance delay time

The entrance delay time is provided to unset (disarm) the system after a first delayed detector has been triggered. To program this time, enter:

\[ 2 \times \]

where \( x \) is a number from 1 to 9 determining the delay in multiples of 5 seconds (1=5 s, 2=10 s, ...,).

If the entrance delay is triggered by a final-door detector, then parameter \( x \) is multiplied by 30 s instead. (1=30 s, 2=60 s, ...) – in this case it means that the entrance delay would be six times longer than if it had been triggered by an ordinary detector.

**Example:** To program a 20 seconds entrance delay, enter the sequence 214 (if the delay has been activated by a final-door detector, a 120 seconds delay will result instead).

**Factory default setting:** \( x = 4 \)

6.3 Alarm duration time

This parameter limits the duration of a triggered alarm. After the alarm state expires, the control panel will return to its previous state, i.e. as before the alarm occurred. The alarm state can also be terminated by an authorised user. To program the alarm duration enter:

\[ 2 \times \]

where \( x \) is a number from 0 to 9 determining the alarm duration: 0 = 10 s, 1 = 1 min., 2 = 2 min. up to 8 = 8 min., 9 = 15 min.

**Note:** There can be up to 5 different alarms in the system: intruder, tamper, fire, panic, and technical alarm.

**Example:** Alarm duration of 5 min. = sequence 225

**Factory default setting:** 4 minutes

6.4 PGX and PGY functions

The functions of PGX and PGY can be programmed by entering sequences:

\[ C X \] for PGX
\[ 2 4 X \] for PGY

where \( x \) determines the PG function or the event which triggers a change of PG state:

<table>
<thead>
<tr>
<th>( x )</th>
<th>Unsplit system</th>
<th>Split system</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Completely (ABC) set = PG on</td>
<td>Alarm A = PG on</td>
</tr>
<tr>
<td>1</td>
<td>Anything set = PG on</td>
<td>Alarm B = PG on</td>
</tr>
<tr>
<td>2</td>
<td>AB set (not ABC) = PG on</td>
<td>Entrance delay A = PG on</td>
</tr>
<tr>
<td>3</td>
<td>Fire alarm = PG on</td>
<td>Entrance delay B = PG on</td>
</tr>
<tr>
<td>4</td>
<td>Panic = PG on</td>
<td>A set = PGX on, B set = PGY on</td>
</tr>
<tr>
<td>5</td>
<td>Any alarm = PG on (excluding Panic)</td>
<td>Panic A = PGX on, Panic B = PGY on</td>
</tr>
<tr>
<td>6</td>
<td>AC dropout = PG on</td>
<td>Fire = PGX on, dropout =PGY on</td>
</tr>
</tbody>
</table>

**7** ON/OFF

**8** 2 seconds pulse

Fig. 9 PG outputs settings

* The ON / OFF and 2 second pulse functions can be controlled from the keypad by keying in * 8, * 9 or using the arrow keys ON and OFF see 6.20) or they can be operated by a code or card. These PG output functions can also be controlled by signals from keyfobs or detectors (see 6.40).

**Notes:**
If it is desired to control a sub control panel from a master control panel (i.e., setting/unsetting), it is possible to enroll a JA-80 Oasis master control panel to a sub control panel as a remote control as follows:

1. First enroll the sub control panel to the desired address in the master control panel by entering 299 on the sub control panel's keypad in Service Mode – see 5.1 for full details.
2. Switch the master control panel to Service Mode.
3. In the sub control panel, enter enrollment mode by keying in “1” in Service Mode and select the desired address.
4. In the master control panel enter 290. This way the control panel will enroll to the sub control panel to the desired address as a remote control.
5. Switch both control panels to maintenance mode and check that all section setting of the master control panel also sets the sub control panel and unsetting the master control panel unsets the sub control panel too. Expect approximately 2 seconds of delay between control panels.

Notes for operating the sub control panel:
- The sub control panel can still be operated independently via its keyfob or keypad e.g. it can be set while the master control panel is unset. If the master control panel changes its status later on, it will then control the sub control panel to achieve synchronisation.
- To disable the master control panel’s ability to control the sub control panel, enter the sub control panel’s enrollment mode, select the address where the master control panel is enrolled and erase the master control panel from this address by pressing and holding key 2.
- The status of the sub control panel is not displayed on the master control panel.

6.10 Master code reset
If the master code has been forgotten or a card lost, it is possible to use the following sequence to reset the master code to the factory-default 1234:

2 9 1

Note: Resetting the master code has no effect on other codes and cards. Resets are recorded in the control panel memory and sent to the ARC.

6.11 Enrollment to other devices (UC, AC)
Keying in 299 sends an enrollment signal to enroll the control panel to UC-82 or AC-82 receiving modules (see 5.5). This sequence can also be used to enroll a sub control panel to a master control panel (see 6.9).

6.12 Setting (Arming) without an access code
“Hot” setting keys (short-cut keys for setting) A, B, ABC or entering “* number” can be enabled for use without a valid access code or card. If disabled, then hot key use or entering “* number” has to be followed by a valid access code or card to have any effect:

Function/sequence 301 300
---
All-section setting ABC key Code/card
Setting of A A key A key, code/card
Setting of AB (or B) B key B key, code/card
Event memory recall #4 #4 code/card

fig. 10 setting / arming with or without code

If you remotely operate the system by mobile phone, you can press ∗1 for the ABC key, ∗2 for key A, and ∗3 for key B.
- Controlling the PG outputs by keying in +8 or +9 or pressing +ON and +OFF is unaffected by these settings. These keys can however be disabled by a special sequence (see 6.26).

Factory default setting: Setting (arming) without an access code enabled.

6.13 Triggered-detector indication
Pressing the ? key checks if any detectors are permanently triggered, e.g. if any doors or windows are open.

3 1 1 indication enabled
3 1 0 indication disabled

Factory default setting: indication enabled

6.14 Confirmation of intruder alarms
To reduce the risk of false alarms and to comply with British standard BSI DD243, the control panel allows alarm confirmation logic to be enabled as follows:

3 2 1 confirmation logic enabled
3 2 0 confirmation logic disabled

Confirmation logic:
- If the system is set (armed) and any intruder detector gets triggered, i.e. a detector with an instant, delayed, or next-delayed reaction, an alarm will not be caused but the control panel will record a so-called unconfirmed alarm.
- If any other intruder detector is triggered in a set section within 40 minutes of the above event, an intruder alarm will be triggered. If no other detector is triggered during this period, the control panel will stop waiting for confirmation.
- The alarm must be confirmed by another detector than the first one. If the same type of detector is used for confirmation then their detection area must not cover the same area. This must be ensured by the proper location of detectors.
- An unconfirmed alarm is recorded in control panel memory but can also be sent to the ARC, or to the user by SMS report.
- If the first triggered detector has a delayed reaction, it will start a so-called unconfirmed entrance delay. This delay is indicated the same way as an ordinary entrance delay. If no other delayed detector is triggered during this delay, there will be no alarm. If the entrance delay is exceeded the unconfirmed alarm is recorded in the control panel memory. If there is any other delayed or next-delayed detector triggered during the entrance delay period, it will confirm the entrance delay, and if this delay is exceeded (due to no unsetting being done) it will trigger an intruder alarm at the end of the delay.
- If a delayed detector is triggered within 40 minutes after the triggering of an unconfirmed alarm or the moment the unconfirmed entrance delay is exceeded, the confirmed entrance delay starts running and when it times out (due to no unsetting being done), an intruder alarm is triggered.
- If the unconfirmed entrance delay is confirmed by an instant detector it will trigger an internal warning (IW) alarm immediately (e.g. an internal siren) and if the entrance delay times out then an external alarm (EW) will be triggered.
- An unconfirmed alarm can be confirmed by any other intruder detectors in the system as long as the detectors are assigned to a set (armed) section.
- The confirmation of intruder alarms concerns only detectors with instant, delayed, or next-delayed reactions. It has no effect on fire, panic, 24-hour, tamper, or technical alarms. These alarms are triggered immediately without confirmation.

Note: When the first detector is triggered it begins a process which waits 40 minutes for any possible confirmation of the alarm (unconfirmed alarm status) during which the system works exactly the same way as if the confirmation function had not been enabled.

Warning: If intruder alarm confirmation is enabled, it is necessary to install enough detectors in the building to detect an intruder even if he/she is only moving in one particular place.

Factory default setting: confirmation disabled

6.15 Exit delay beeps
The exit delay can be indicated by beeps from the keypad and internal wireless siren. The beeps get faster in the last 5 seconds.

3 3 1 Beeps enabled
3 3 0 Beeps disabled

Factory default setting: Beeps enabled.

6.16 Exit delay beeps while partially setting (arming)
The exit delay caused by partial setting, e.g. using the A or B key, can also be indicated by keypad beeps and internal-siren beeps. The beeps get faster in the last 5 seconds. The feature is linked to 331 parameter setting.

3 4 1 Beeps enabled
3 4 0 Beeps disabled

Factory default setting: Beeps disabled.

6.17 Entrance delay beeps
The entrance delay can be indicated by keypad beeps and internal-siren beeps:

3 5 1 Beeps enabled
3 5 0 Beeps disabled

Factory default setting: Beeps enabled.

6.18 Setting (arming) confirmed by wired-siren chirp
A hard-wired siren connected to the IW terminal of the control panel can audibly indicate setting by one beep, unset by two beeps and unsetting after an alarm by three beeps. Four beeps mean an invalid attempt at setting the system has occurred.

3 6 1 Chirps enabled
3 6 0 Chirps disabled

Note: In JA-80L wireless sirens, this function can be individually enabled for each siren. (see the siren manual).

Factory default setting: Hard-wired siren chirps disabled
6.19 Sirens always sound during audible alarms

Using this sequence it is possible to disable internal and external sirens (IW and EW) if any part of the system is unset (partial setting), i.e. when someone is home.

3 7 1 Sirens always sound during audible alarms
3 7 0 Sirens only sound during audible alarms when all sections are set, i.e. no one is at home

Factory default setting: Sirens always sound during audible alarms.

6.20 Wireless siren alarm enabled (IW and EW)

This setting is for enabling and disabling wireless sirens in the system:
3 8 1 wireless sirens enabled
3 8 0 wireless sirens disabled

Note: This setting applies both to internal and external wireless sirens.

Factory default setting: Wireless sirens enabled

6.21 Bypass user approval

This setting can change the function of the system when it is being set (armed) and if there is:
- any detector triggered
- any tamper alarm
- any trouble in the power source
- Keypad communication with any wireless device (for more than 20 minutes)
- any panic button triggered

If bypass user approval is set (391), then during setting (arming), the system notes which problems mentioned above are active and displays informative text on the keypad and only bypasses them if the user approves the bypassing by keying in a * within 6 seconds of being notified.

The system has a built-in auto-bypass function (setting 390) so that if any number of detectors are being triggered during setting (arming) then they will be bypassed and ignored automatically without consulting the user.

3 9 1 Approval by pressing the * key is requested from the user
3 9 0 Bypassing occurs automatically without user approval

Notes regarding setting the system with (a) triggered detector(s) or problems as mentioned above:
- Details can be viewed by pressing the ? key (e.g. open doors or windows).
- If a wireless keyfob is used to set the system and auto-bypass user approval is enabled, the system will set without bypass approval, i.e. setting by keyfob does not trigger an approval request.
- The automatic bypass of a detector will end after the detector has been de-triggered (for example if a door is closed) or the problem disappears.
- If auto-bypass user approval is enabled and Service mode is being exited while a detector is being triggered, the installer will be notified about the bypass. The installer can then approve the bypass by pressing # twice.
- To comply with the EN-50131-1, 3 standards 391 should be set.

Factory default setting: Bypassing occurs automatically without user approval.

6.22 Final-door detectors

In this mode, up to 5 detectors can be defined as final-door detectors and assigned to addresses 01 to 05 or 46 to 50 in order to make leaving a building much easier, especially via a garage:

6 5 x

Where
- x = 0 none
- x = 1 detectors on addresses 01 to 05
- x = 2 detectors on addresses 46 to 50

Description of final-door detector mode:
- If a final-door detector is used in the system then the value of x for exit delay programming is multiplied by 30 s (see 12) thereby extending the delay, and if an entrance delay is triggered by a final-door detector then the value of x for the entrance delay is also multiplied by a larger value of 30 s.
- A final-door detector should be programmed to have a natural reaction, otherwise it works as it is set (e.g. instant reaction).
- Only door/window detectors, hard-wired control panel inputs or hard-wired inputs in the wireless keypad unit to whose alarm input the final-door detector is connected should be assigned to the addresses which you set with this sequence as belonging to final-door detectors.
- If a final-door detector is used for a garage door, no instant detectors should be inside the garage. Next-delay detectors would however be acceptable.

Setting (arming) the system with a final-door detector:
- After entering a request to set the system, an exit delay of between 30 and 270 seconds will begin and be indicated.
- If a final-door detector is triggered during the exit delay, the exit delay will be extended by the time in which the detector is still triggered. So, if for example, the door is left continuously open, the exit delay will never end.
- If a final-door detector is de-triggered, the system will wait five more seconds during which beeping gets faster, and if the door is not opened again during this short period, the exit delay will terminate and the system will be set immediately.
- The duration of the exit delay therefore depends on the time the final door detector stays open. For instance, in winter if the driveway in front of a garage needs to be cleared of snow there will be plenty of time to do it, and in summer when garages can be exited easily and therefore quickly, the exit delay can be rather shorter. The exit delay only depends on the length of time the garage door is left open.
- If no final-door detectors are triggered during the exit delay, the system will provide an exit delay and then set.
- If the final door detector stays continuously triggered, an endless exit delay will result with the system never being set. This means all delayed and next-delayed detectors will not be set (armed).
- If there are multiple final-door detectors in the system, the exit delay is extended if any of them is triggered and ends after all final-door detectors have been de-triggered.

Unsetting (disarming) the system with a final door detector:
- If a final-door detector gets triggered in a set (armed) system, an entrance delay will begin with a duration of between 30 and 270 seconds.
- If a normal delayed detector gets triggered while the user enters a building, the system starts an ordinary entrance delay of between 5 and 45 seconds.
- If a final-door detector is triggered first, a longer entrance delay will begin. If during this delay an ordinary delayed detector is then triggered, the remaining entrance delay will then be shortened to the delay associated with detectors of this kind.

Note: Only use status-reporting detectors such as the JA-81M or JA-82M, or the hard-wired inputs of wireless keypads, or the hard-wired inputs of JA-81E hard-wired keypads which also have a pulse reaction.

Factory default setting: No final-door detectors in the system.

6.23 Partial setting (arming) or system splitting

The control panel can be configured in three ways as follows:
- the entire system sets and unsets together or,
- the system partially sets and unsets to protect only certain parts of a house during the day, while people are still present in the unset parts and,
- the system can be split into two independently set/unset sections for two separate users and also with a common section if desired.

Program as follows to configure the system as desired:

6 6 x

Where
- x = 0 unsplitted system (setting/unsetting as an entire system)
- 1 = partial setting (for setting sections A, AB, or ABC)
- 2 = split system (sections A and B can be set/unset independently by separate users, with section C only being automatically set when both A and B are manually set)

Notes:
- For an unsplitted system, all intruder detectors are set/unset immediately after the user sets/unsets the system. Assigning wireless devices, access codes and keyfobs to various sections of the system has no effect in this mode.
- Partial setting is especially suitable for homes and apartments where the user wishes to protect different parts of the premises during the day. Detectors can be set to three sections, A, B and C. Using setting (arming) key A on the system keypad, you can set section A, e.g. setting the garage area in the afternoon. Using setting key B you can set sections A and B simultaneously e.g. in the evening before going to sleep to protect the garage (section A) and the ground floor of the house (section B). The ABC total-setting button is used when leaving the house and setting all sections, A, B and C. If you then use a valid access code or card for unset (disarming), all sections will be unset. The assignment of codes or cards to sections has no effect in this mode. A and B keypad buttons are used for partial setting.
- A keyfob can also be used for partial setting control. Buttons and 0+O can be programmed to set and unset the entire system, and buttons can be programmed for setting (arming) sections A and AB respectively to partially set the system (this pair of buttons must be assigned to section A or B if it is to be used for partial setting. See 6.40 for details on partial setting by keyfob).
6.24 Automatic summer time (daylight saving time)

If enabled, this feature automatically offsets the system time to that of summer time, or daylight saving time as it is also known:

- **6 8 0 1**: automatic summer time enabled
- **6 8 0 0**: automatic summer time disabled

**Note**: If automatic summer time is enabled, the control panel's internal clock is automatically offset by +1 hour on March 31st at midnight. The offset is then removed on October 31st at midnight to return to winter time.

**Factory default setting**: automatic summer time disabled

6.25 Pulse reaction of tamper sensors

This feature allows permanently triggered tamper sensors to be ignored:

- **6 8 1 1**: ignore permanently triggered tamper sensors, i.e. only react to an increase in the number of triggered tamper sensors.
- **6 8 1 0**: react with a tamper alarm to all triggered tamper sensors

**Note**: Ignoring permanently triggered tamper sensors is useful for example when carrying a detached wireless keypad around with you during installation as this avoids unnecessary tamper indication. If you choose to ignore permanently triggered tamper sensors, their de-triggering is not reported to the ARC.

**Factory default setting**: react with a tamper alarm to all triggered tamper sensors

6.26 Operating the PG outputs using *8 and *9

Using this feature the PGX and PGY outputs can be controlled from the keypad by pressing the *8 and *9 keys (or keys ON and OFF).

- **6 8 2 1**: control enabled
- **6 8 2 0**: control disabled

**Notes**: The PG outputs can only be operated from the keypad if they have their ON/OFF or pulse functions enabled.

- In addition to controlling the PG outputs using keys *8 and *9, PG outputs can also be controlled by access codes, access keys, keyfobs and detector signals (see 6.40 and 6.41 for details).
- If a PG output should only be operated by a valid access code or card, then control by *8 and *9 should be disabled and the codes and cards should be programmed to control the PG outputs instead (see 6.41).

**Factory default setting**: control enabled

6.27 Permanent alarm status display

The below sequence enables the permanent display of alarm status on the keypad unit.

- **6 8 3 1**: permanent status display enabled
- **6 8 3 0**: display a maximum of 3 minutes after last event

**Notes**: European legislation requires status displaying to be suppressed within three minutes of last event in the display (keypad, visual, entry alarm, status indication). This feature can be used to ignore this requirement if appropriate.

- The wireless keypad can continuously display the status if powered by an external power supply. If powered by internal batteries the keypad will turn off its display after 20 seconds of not being used (in Service Mode the display turns off after 15 minutes of no use by the installer).

**Factory default setting**: only 3 minutes of display time

6.28 Tamper alarm if unset

According to EU legislation an unset (disarmed) system should not audibly sound a tamper alarm if tampering occurs. If the audible indication of tamper alarms is required while the system is unset (disarmed) then this can be enabled by the following sequence:

- **6 8 4 1**: audible tamper alarm even for an unset system
- **6 8 4 0**: silent tamper alarm for an unset system

**Notes**: Even if tamper alarms are silent, they are still recorded in the control panel memory and reported to the end user by SMS, and also to the ARC if used.

- If the sequence 370 has been programmed, then tamper alarms will be silent if the system is unset or partially set.

**Factory default setting**: silent tamper alarms for an unset system

6.29 Recording PG output activation to memory

The activation of PGX and PGY outputs can be recorded in the control panel's memory (for example if the outputs are used for access control). This can be enabled by the following sequence:

- **6 8 5 1**: enabled
- **6 8 5 0**: disabled

**Factory default setting**: recording enabled

6.30 Engineer reset

This is a special function requested by the DD243-2004 standard. It can only be used when the alarm system is connected to an alarm-receiving centre. When a confirmed alarm is activated the control panel is completely blocked – it cannot be operated by any user, master or service code until an engineering reset is performed by an ARC code. This function is required in some countries only and you can enable it by the following sequence:

- **6 8 6 1**: Engineer reset enabled
- **6 8 6 0**: Engineer reset disabled

**Factory default setting**: Engineer reset disabled

**Notes**: To enable the confirmation of intruder alarms (requires two detectors to be triggered in different zones within a definite period) – use sequence 3 2 1

- Reporting to ARCs must be locked by a digital code.
- The keypad shows the text “Eng. reset req’d” and the system stays blocked until the ARC code is used via the communicator (see the communicator manual).
- The feature is supported when a JA-80Y version XA61008 or higher, or a JA-80V version XA64005 or higher is installed.

6.31 Social alarm feature

If this function is enabled the signals from delayed, next delayed and instant detectors are regularly checked in disarmed mode. If there is no active signal (no movement inside) for more than 16 hours a panic alarm is triggered.

- **6 8 7 1**: social alarm enabled
- **6 8 7 0**: social alarm disabled (default)

**Note**: This feature can be used to alert the user that the system is unintentionally disarmed.

6.32 Annual check notification

This sequence enables the user and installer to be notified of the necessary time for an annual technical check:

- **6 9 0 0**: notification disabled
- **6 9 0 1**: notification enabled

**Notes**: An annual technical inspection notification is displayed as text on the keypad display and can also be sent as an SMS to the end user and/or installer and/or as a report code to an ARC, if used.

- Annual technical inspection notification text appears on entering Service Mode.
- When this notification is enabled, exiting Service Mode will cause a notification to occur on the next year on the first day of the month in which it was set. (e.g. if you set the annual check notification on the 15th October 2007, the notification is displayed on the 1st October 2008.)
- When this notification is enabled, exiting Service Mode will cause a notification to occur every twelve months later (the same day and month).
- If you wish to receive a notification earlier than a year later, change the annual check settings to the day and month you prefer before exiting Service Mode by entering 4hhmmDDMMYY, and then re-adjust the clock to the correct time in maintenance mode. By tricking the system this way, you can be notified on the desired date. (see 6.45, entering and exiting maintenance mode does not change the notification date).

**Example**: If the date is 10 January 2007 and you wish to receive a notification 6 months later on 10 July 2007, while still in Service Mode change the system clock to 10 July 2007, i.e. the day and month of the
6.33 Only single alarm indication

If this function is enabled, then only one intruder alarm may be indicated at a time. Once an intruder alarm has been triggered and has not ended yet, then no more alarms can be indicated no matter how many more times triggering occurs. When the alarm ends, the system is then ready to indicate the next single intruder alarm.

This is to limit the number of SMS reports sent if hard-wired PIR detectors capable of being frequently triggered are installed in the system and the system is not unset (disarmed) properly when someone enters the building.

6 9 1 0 multiple simultaneous intruder alarms allowed
6 9 1 1 single intruder alarm allowed only

Note:
- A panic alarm can always be triggered with no limits (except when in service and maintenance modes).
- Apart from this limitation the system also checks if any detector is triggering multiple alarms during one arm period. If any detector has caused at least three alarms in a row it is then automatically bypassed. This bypass lasts until another detector triggers an alarm or until the next arming of the system.

6.34 Setting (arming) by service code

Normally, it is not allowed to control the system via the service code. Using this sequence, the installer can be authorized to set and unset the system by means of a valid service code. This feature should only be enabled with the explicit approval of the master code holder (system administrator):

6 9 2 0 disabled
6 9 2 1 enabled

Factory default setting: disabled

6.35 Audible panic alarm

If enabled, panic alarms can be indicated by internal and external warning devices (sirens on W and EW):

6 9 3 0 silent panic alarm
6 9 3 1 audible panic alarm

Note: If the sequence 370 is used, panic alarms are silent if any section of the system is unset.

Factory default setting: silent panic alarm

6.36 Higher control-panel receiver-sensitivity

If enabled, this feature can extend the communication range between the control panel and its wireless devices if there is no radio frequency interference in the premises.

6 9 4 0 standard control panel sensitivity
6 9 4 1 higher control panel sensitivity

Note: The sensitivity of the control panel receiver should only be increased if there is no RF interference as the radio range would only be reduced if interference was present.

Factory default setting: standard control panel sensitivity

6.37 Access by code plus card

This feature increases security against unauthorised setting/unsetting (arming/disarming):

6 9 5 0 system access by code or card
6 9 5 1 system only accessed by code and card if both are assigned to the same user position

Notes:
- The system has up to 50 user positions (01 to 50) each capable of having an access code and an access card assigned to it. If both a code and a card are assigned to a user then the above sequences (6950 and 6951) determine whether the user can use a code or a card or whether he must present both a card and a code to gain control over the system. If both, a card and a code have to be presented, the order in which they are done is unimportant.
- If only a card or only a code is assigned to a user, then the above settings have no effect on users like this.

Factory default setting: system operated by code or card

6.38 Audible 24 hour intruder alarm

The 24-hour intruder alarm which can be triggered whether the system is set or not, and can also be silent or audible (IW and EW) according to the following sequences:

6 9 6 0 silent 24-hour intruder alarm
6 9 6 1 audible 24-hour intruder alarm

Note: If sequence 370 is programmed, the intruder alarm will be silent if any section in the system is unset.

Factory default setting: audible 24-hour intruder alarm

6.39 Service mode only with service and user code

To prevent the installer from accessing Service Mode without a user's permission, this feature (if enabled) makes it compulsory for the any user code (or master code) to be entered directly after entering the service code to access Service Mode. Service Mode can then be entered by keying in the service-code user-code (or master-code).

6 9 7 0 Only service code needed.
6 9 7 1 Service code and user-code (or master-code) needed.

Factory default setting: Only service code needed.

6.40 Device reactions and section assignment

The following sequence programs the characteristics of system devices:

6 1 nn rs

where

- nn is the device address from 01 to 50 (01 to 04 … 14 can either be the hard-wired input terminals in the control panel or enrolled wireless devices)
- r is the reaction index from 0 to 9 – see table
- s is the section 1 = A, 2 = B, 3 = C (only has an effect if partial setting or system splitting is used – except for PG output control – See 6.23)

<table>
<thead>
<tr>
<th>R</th>
<th>Reaction</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disabled (none)</td>
<td>For temporarily disabling codes or devices including tamper sensors</td>
</tr>
<tr>
<td>1</td>
<td>Natural</td>
<td>For detectors = instant, delayed or fire (selectable in detectors by DIP switch)</td>
</tr>
<tr>
<td>2</td>
<td>Panic</td>
<td>Triggers a panic alarm (audible or silent, see 6.35)</td>
</tr>
<tr>
<td>3</td>
<td>Fire</td>
<td>Triggers a fire alarm</td>
</tr>
<tr>
<td>4</td>
<td>24 hours</td>
<td>Triggers an intruder alarm even if the system is unset (audible or silent – see 6.38)</td>
</tr>
<tr>
<td>5</td>
<td>Next delay</td>
<td>Always provides an exit delay. An entrance delay is only provided if it is triggered shortly after a delayed detector.</td>
</tr>
<tr>
<td>6</td>
<td>Instant</td>
<td>If activated in a set (armed) section, it triggers an immediate alarm instantly.</td>
</tr>
<tr>
<td>7</td>
<td>Set</td>
<td>Sets its own section of the system</td>
</tr>
</tbody>
</table>
| 8 | PG output control | The value of the s parameter determines which PG output is controlled: s=1=PGX, s=2=PGY: keyp, s=3=PGX & PGY. To use this function the PG output involved has to be programmed to the ON/OFF or pulse functions. If the reaction is triggered by:
- a code (card) – the PG output changes its state (ON,OFF,ON,OFF……) or a pulsed switching event is generated after a valid code or card is used. If a code or card is programmed this way, it cannot be used for setting (arming) control. One or more (up to 50) different codes can be programmed to operate PG outputs, if desired.
- a keyfob – one button in a pair is used to switch a PG output ON, the second one to switch it off or each of them generates a pulsed switching event. If a keyfob is programmed this way, it cannot be used for setting (arming) control. Each PG output can have as many associated keyfobs as desired. A detector – the PG output copies the status of the detector or it generates a pulsed switching event when the detector is triggered. Only one detector should be programmed to a PG output ON/OFF reaction and should not be combined with keyfob or keypad control as the detector repeats its status every 9 minutes and it would override the signal from the keypad or keyfob. |

fig. 11 Device reactions

JA-82K control panel installation manual

MKHS2204
### Assigning keyfobs with natural reactions to sections

<table>
<thead>
<tr>
<th>s</th>
<th>button</th>
<th>Unsplit system</th>
<th>Partial setting</th>
<th>Split system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 (or 1)</td>
<td>set</td>
<td>set A</td>
<td>set A</td>
</tr>
<tr>
<td></td>
<td>1 (or 0)</td>
<td>unset</td>
<td>set AB</td>
<td>unset A</td>
</tr>
<tr>
<td>2</td>
<td>1 (or 1)</td>
<td>set</td>
<td>set B</td>
<td>unset B</td>
</tr>
<tr>
<td></td>
<td>1 (or 0)</td>
<td>unset</td>
<td>set AB</td>
<td>unset B</td>
</tr>
<tr>
<td>3</td>
<td>1 (or 1)</td>
<td>set</td>
<td>set ABC</td>
<td>set ABC</td>
</tr>
<tr>
<td></td>
<td>1 (or 0)</td>
<td>unset</td>
<td>unset ABC</td>
<td>unset ABC</td>
</tr>
</tbody>
</table>

fig. 12 Buttons to section

**Guidance on assignment to sections:**

- If partial setting is programmed then detectors can be assigned to sections: A (s=1), B (s=2) or C (s=3).
- If the selected reaction is PG output control then the s parameter defines which PG output is controlled: s=1 PGX, s=2 PGY, s=3 PGX and PGY.

**Guidance on programming reactions:**

- The reaction selected in a detector by its internal DIP switches is only obeyed by the control panel if the reaction programmed in the detector's address is a natural one (n=1).
- Keyfobs always enrol a pair of buttons (1 or 1) or (1 or 1). The natural reaction of such a pair of buttons is shown in the table above. If any other reaction is selected for a keyfob, this reaction will only apply to the first button of the pair, i.e. 1 or 1, or to double buttons 1 + 1 or 1 + 1. The 1 (1) button has no effect (can still be used for controlling UC/AC receivers).

**Factory default setting:** All addresses from 01 to 50 have a natural reaction (n=1) and are assigned to section C (s=3).

### 6.42 Enrollment by keying in production codes

This sequence allows the enrollment of devices by keying in their production codes:

```
6 0 nn xx...x
```

where:

- `nn` is the address of the device from 01 to 50
- `xx...x` is the production code of the device (the last eight digits of the bar code, see the label on the PCB inside the device)

**Notes:**

- If the address `nn` is already occupied, the current device will be erased, and the new device will then be enrolled instead.
- If a device with production code `xx...x` has already been enrolled to another address in the past, and if the device is now enrolled to a new address, then it will be moved to the new address, releasing the old address.
- If you enter `nn = 01 to 4 (1...4)`, the device will enroll instead of the corresponding hard-wired input in the control panel (the terminal will be disabled).
- If eight zeros are entered as a production code, the device already assigned to the address `nn` will be erased

### 6.43 Automatic setting / unsetting schedule

This can be used to program an automatic sequence of daily setting/unsetting events. Up to 10 daily events can be programmed. Events will occur every day of the week:

```
6 4 n a hh mm
```

where:

- `n` is the event number from 0 to 9
- `a` is the type of event from 0 to 6 (see the following table)
- `hh` hours (time of event)
- `mm` minutes (time of event)

**Erase the automatic schedule setting by:**

```
6 4 n 0
```

<table>
<thead>
<tr>
<th>a</th>
<th>Unsplit system</th>
<th>Split system</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No event</td>
<td>No event</td>
</tr>
<tr>
<td>1</td>
<td>Set all (ABC)</td>
<td>Set all (ABC)</td>
</tr>
<tr>
<td>2</td>
<td>Unset all (ABC)*</td>
<td>Unset all (ABC)</td>
</tr>
<tr>
<td>3</td>
<td>Set X**</td>
<td>A</td>
</tr>
<tr>
<td>4</td>
<td>Set AB**</td>
<td>B</td>
</tr>
<tr>
<td>5</td>
<td>Unset all (ABC)*</td>
<td>A</td>
</tr>
<tr>
<td>6</td>
<td>Unset all (ABC)*</td>
<td>B</td>
</tr>
</tbody>
</table>

* the same event in an unsplit system
** only possible if partial setting (arming) is programmed (see 6.23)

**Notes:**

- The automatic setting/unsetting event schedule can also be programmed in maintenance mode.
- It is not possible to use the same instant of time for two events. Use t+1 minute for the second event.

**Factory default setting:** All automatic events switched off.

### 6.44 Changing the service code.

The service code is used to switch into Service mode. To change the service code, enter:

```
5 NC NC
```

where:

- `NC` new code (4 digits), the new code has to be entered twice.

**Example:** The code 1276 can be programmed by entering: 5 1276 1276

**Factory default setting:** 8080

### 6.45 Go to maintenance mode

By entering 292 while in Service Mode the system switches to maintenance mode. In maintenance mode it is possible to program the devices to be bypassed and to adjust the control panel internal clock (see 7.4).

### 6.46 Setting the internal clock

The control panel has a built in real-time clock which is used to timestamp all recorded events in the control panel memory. Adjust the clock after installation by entering:

```
4 hh mm DD MM YY
```

where:

- `hh` is the time in hours (00 to 23)
- `mm` is the time in minutes (00 to 59)
- `DD` is the day (01 to 31)
- `MM` is the month (01 to 12)
- `YY` is the year (00 to 99)

**Note:** The internal clock can also be adjusted in maintenance mode.
Example: On 30 June 2012 at 17:15 enter: 4 17 15 30 06 12
After the control panel is powered up, the clock is set to 00 00 01 01 00.

6.47 Editing keypad text

The names of devices and programmable outputs as displayed on the keypad unit can be edited as follows:

- The menu can be entered in Service mode by holding the ? key. Then the internal keypad menu will be displayed. Using the arrows or keys 1 and 7 you can scroll through the menu to Edit text. Press ●. Editing mode and the name of the device enrolled to address 01 is then displayed with a flashing cursor on the first text character.
- Key functions:
  1 and 7 text scrolling (see table)
  3 and 9 character-selection (A,B,C,D,...,8,9,0)
  4 and 6 cursor control (left/right)
  2 delete selected character
  8 space
  # exit editing (& save changes)

List of editable text:

<table>
<thead>
<tr>
<th>text</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01: to 50: Devices</td>
<td>Names of devices in addresses 01 to 50</td>
</tr>
<tr>
<td>Control panel</td>
<td>Name of control panel (e.g. displayed if its cover is opened)</td>
</tr>
<tr>
<td>Keypad</td>
<td>Name of hard-wired keypad</td>
</tr>
<tr>
<td>Communicator</td>
<td>Name of the communicator in the control panel</td>
</tr>
<tr>
<td>Master code</td>
<td>Name of the master code</td>
</tr>
<tr>
<td>ARC Code</td>
<td>Names of user codes</td>
</tr>
<tr>
<td>Service code</td>
<td>Name of the service code</td>
</tr>
<tr>
<td>PGX and PGY</td>
<td>Names of programmable outputs</td>
</tr>
<tr>
<td>Oasis JA-80</td>
<td>The default text displayed in operating mode if no other text needs to be displayed. If erased then nothing will be displayed.</td>
</tr>
</tbody>
</table>

Notes:
- Be sure that the capital or small letters can switch by key.
- The length of the text is limited to the length of the display.
- The text is only stored in the keypad used for editing (different keypads in the system can show different text if desired).
- Text is stored in the non-volatile memory of keypads, so power disconnection will not erase any stored text.
- Convenient text editing is possible using a PC running OLink software. (texts can be edited in the Text synchronization \ Comparison window (F11)).
- Besides device names, keypads also use so-called internal text such as “service”, “maintenance mode” etc, and this text can also be edited via OLink software by selecting “Central” on the menu and then “Text synchronization \ Comparison” or F11.
- After editing keypad text using OLink software, all keypads (including wireless ones) must be connected to the digital bus to save the changes to the keypad units by clicking on the OK button in the software. (It is recommended to connect JA-81F wireless keypads to the bus in order to save the text into them as well)
- The texts can also be uploaded directly into the JA-81F wireless keypad from the Olink.

Factory default setting: in addresses 01 to 50 there is the text “Device”. Other default text: “Control panel”, “Keypad”, “Communicator”, “Master code”, users 01 to 50 “Code”, “ARC Code”, “Service code”, “PGX”, “PGY” and “Oasis JA-80”.

6.48 Recommended settings

Recommended settings for the following parameters according to the standards:

<table>
<thead>
<tr>
<th>Code</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>261</td>
<td>radio interference indication (see 6.6)</td>
<td></td>
</tr>
<tr>
<td>271</td>
<td>radio communications supervision (see 6.7)</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>setting (arming) without an access code disabled (see 6.12)</td>
<td></td>
</tr>
<tr>
<td>391</td>
<td>auto-bypass user approval (see 6.21)</td>
<td></td>
</tr>
<tr>
<td>6841</td>
<td>tamper alarm if unset (see 6.28)</td>
<td></td>
</tr>
<tr>
<td>6830</td>
<td>keypad displays status for 3 min. if any button pressed (see 6.27)</td>
<td></td>
</tr>
<tr>
<td>6920</td>
<td>not allowed to control the system via the service code (see 6.34)</td>
<td></td>
</tr>
<tr>
<td>6951</td>
<td>system only accessed by code and card (see 6.37)</td>
<td></td>
</tr>
<tr>
<td>6971</td>
<td>service mode only with service and user (master) code (see 6.39)</td>
<td></td>
</tr>
</tbody>
</table>

7. Operating the system

The Oasis system can be operated locally using a keypad or a keyfob and it can also be operated remotely by mobile phone or the Internet (if equipped with a suitable communicator).

7.1 The system keypad

Indoor keypads model JA-81F (wireless) or JA-81E (wired) can be used to operate the system. Both keypad types provide the same functionality. There also can be connected the JA-80H outdoor keypad via the WJ-80 interface – see the manual for more info.

7.1.1 Keypad indicators:

- APC setting (arming) status of sections – if all sections are set then all these indicators (A & B) are lit.
- Flashing = alarm, with the simultaneous display of alarm details on the LCD, e.g.:
  - Alarm
  - Constantly lit = fault – details are displayed by pressing the “?” key
- Power. Constantly lit = mains and back-up battery ok.

7.1.2 LCD display

The 1st line displays the status: triggered detector, Service mode etc. In standby mode, it shows the text “JABLOTRON”. A picture of size 128x48 pixels can be loaded into the keypad. (Olink 1.4 or a higher version is needed).

The 2nd line displays the name of a device (e.g. 01: Main Door etc.). In standby mode, it shows the text “Oasis JA-80” (editable, see 6.47). The text can be edited, see 6.47.

Displaying the status of devices and programmable outputs:

- Details on permanently triggered detectors (e.g. open windows) and the status of the PGX and PGY outputs can be displayed by pressing the ? key.

7.1.3 Keypad display sleep-mode

In operating mode, the wireless keypad unit displays the system status for 20 seconds (if battery-powered) after the last interaction with a user, and then goes into sleep mode. Pressing any key, triggering the keypad input, pressing or opening the keypad’s flip cover re-activates the display.

7.1.4 Keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–9</td>
<td>digital code entry</td>
</tr>
<tr>
<td>*</td>
<td>function sequences</td>
</tr>
<tr>
<td>#</td>
<td>escape</td>
</tr>
<tr>
<td>ABC</td>
<td>hot key for setting the entire system (all sections A, B &amp; C)</td>
</tr>
<tr>
<td>A</td>
<td>hot key for setting section A (e.g. partial setting of the garage)</td>
</tr>
<tr>
<td>B</td>
<td>hot key for setting sections A and B (e.g. partial night-setting of the garage and the ground floor)</td>
</tr>
<tr>
<td>?</td>
<td>in a split system: hot key for setting section B (C is only set if both sections A and B are set)</td>
</tr>
<tr>
<td>0</td>
<td>display of triggered detectors (e.g. open windows), fault details and PGX / PGY status.</td>
</tr>
</tbody>
</table>

Notes:
- The A and B keys only have a function if partial setting or splitting are enabled.

7.1.5 Functions beginning with the * key

The following functions are available to the user via the keypad:

- * sets the entire system (the same as key ABC)*
- + sets section A (the same as key A)*
- # sets A and B, or just B (the same as key B)*
- @ event memory recall (key 4 scrolls backwards) – the control panel records max. 255 of the latest events
- # new Master Code/Card (+5 MC NC NC)
- $ access code/card programming (+6 MC nn NC)
- % for operation while under duress (should be entered before the access code to secretly signal distress)
- ^ PGX control (ON/OFF = +81/+80 or enter +8 to trigger if a pulsed switching reaction is programmed)*
- _ PGY control (ON/OFF = +91/+90 or enter +9 to trigger if a pulsed switching reaction is programmed)*
- 0 to enter Service Mode (+0 SC – factory default 8080) or to enter maintenance mode (+0 MC – factory default 1234)

The * functions allow the system to be operated from a mobile phone keypad (if the control panel is equipped with the relevant communicator).

7.2 Programming access codes and cards

The system can be controlled by 4-digit codes and by access cards, of the types PC-01 and PC-02 (EM UNIQUE 125kHz standard).

- Sequences for programming access codes and cards are described in fig. 19. They should only be programmed in the DISARMED state.
- The control panel has 1 service, 1 master and 50 user codes.

JA-82K control panel installation manual   - 13 -
7.3 Setting and unsetting (arming/disarming) the system

The system can be set and unset from a keypad, a keyfob or remotely by phone or from a PC running OLink software.

To set the system from a keypad:

- Press key ABC, A or B.
- Enter a code (or present a card)

If the system is partially set (section A is set), and you wish to extend the system to section B, the keypad would then be used to control the alarm system. If the outdoor electric door lock (known as an outdoor bypass feature), i.e. an indoor keypad or card reader will always open the electric door lock.

If the system is equipped with a JA-80H outdoor keypad or a JA-80N 80T, JA-82T interface or a JA80-BT wireless Bluetooth interface. The control panel allows a maximum of 10 unsuccessful attempts in a row to enter a valid code or card. If exceeded, a tamper alarm starts.

7.4 Maintenance Mode

Maintenance mode can be entered using a master code or master card by entering:

- 0 MC

where MC = master code (card) – factory default 1234 or use card.

In maintenance mode it is possible to:

- Test devices (an alarm cannot be triggered).
- Display which code/card positions are currently occupied.
- Bypass individual devices (for one setting/unsetting cycle or indefinitely) - see 7.4.2.
- Program the real-time system clock – see 6.4.6.
- Program the automatic setting/unsetting schedule – see 6.4.3.
- Program telephone numbers for event reports to the end user (see 6.5).
- Exit maintenance mode by pressing the # key.

7.4.1 Displaying which user/card positions are occupied

Which positions in the range 01 to 50 are occupied by codes or cards can be displayed in maintenance mode as follows:

1. The control panel must be in maintenance mode – if not then enter +0 master master code or card (factory default: 1234) while the system is totally unset.
2. Press key 5 (the display indicates “Codes 01: Code”).
3. Using the arrow keys all user positions (01 to 50) can be scrolled through, with the A indicator showing whether a code is programmed or not, and the B indicator showing whether a card is programmed or not.
4. To exit this code/card display mode press the # key.
5. To exit maintenance mode press the # key.

Change access codes and cards use sequence 1 MC nn NC (see fig. 19). (The system must be disarmed).

The most convenient way to administer codes is by using a PC running OLink software (in the Codes window).

7.4.2 Bypassing devices

In maintenance mode it is possible to bypass (disable) individual system devices (permanently or only for one setting/unsetting cycle):

1. The control panel must be in maintenance mode – if it is not, then enter +0 master code (factory default: 1234) while the system is totally unset.
2. Press key 1, to display the control panel’s bypass menu.
3. Using the 1 and 7 keys you can scroll through all the devices able to trigger alarms.
4. To bypass a device use key:
   - 2 to bypass the device for one setting/unsetting cycle (the indicator will start flashing)
   - 3 to permanently bypass a device (the indicator will light continuously)
5. To cancel the bypassing of a device use the same button as was originally used for bypassing (2 or 3). Using key 4 will cancel all device bypasses in the system.
6. If the desired device is a PC can be programmed by repeating step 3 and 4.
7. Press the # key to exit the bypass menu. Pressing # again exits maintenance mode.

If a system with bypasses programmed is being set, then bypass text will be displayed on the keypad unit. Bypassing is canceled when leaving Service mode.

7.4.3 Protecting a car near the system

The Oasis system can also protect a car (cars) parked in the proximity of the house.

1. If the car has a built-in car alarm then an RC-85 transmitter unit can be connected to the car alarm output. The RC-85 can be enrolled to a free address in the Oasis control panel. (See the RC-85 manual). An alarm triggered in the car can be indicated as an Oasis panic alarm (or a 24-hour reaction can be set), regardless of whether the system is set or not. Note: If the car alarm confirms setting (arming) by sirens chirps appearing on the alarm output, then these should be disabled to avoid false alarms.
2. If the car has no built-in car alarm then JA-85P or JA-85B detectors can be installed in the car. The car detectors can be assigned to their own dedicated section in the system, e.g. a split system section where section A could be for the car detectors, and section B for the house detectors, with no detectors assigned to section C, and the entry codes/cards assigned to section C to access the whole house. So when the user enters the house he can set section A to protect the car, and unset section B to be able to enter the house. Radio communication supervision should be disabled for the car detectors to avoid fault notifications when the car is driven away from the house (see the detector manual).

8 Operating/programming the system by PC

The Oasis system can be operated and programmed locally using a PC running OLink software. To connect the control panel to the PC use a JA-80T, JA-82T interface or a JA80-BT wireless Bluetooth interface.

OLink software can be used by installers and end users. The software only allows access to features allowed by the access code (service or user).

If the control panel is equipped with a suitable communicator such as the JA-80Y (GSM/GPRS) or JA-80V (LAN/telephone line) then the system can also be accessed from a PC connected to the Internet. For this remote access it is first necessary to register at www.GSMOlink.cz or directly by Olink v. 2.0 and higher (JA-82Y only).

9 Basic guidance for installers

- Create an installation plan that sufficiently covers the building to be protected.
- If the customer requests changes to the suggested configuration in order to reduce the price, especially reducing the number of detectors, ask for his request to be given to you in writing. (You will avoid future disputes if the insufficient protection is overcome by intruders.)
- Perform the installation in a very professional and conscientious manner and always tidy up the site afterwards.
- It is very important to teach the end user how to use and test the system and to check his level of understanding.
- Get the customer to sign a written statement that the system was installed according to the customer’s specifications and that the customer understands how to operate the system.
- Explain the importance of the annual technical inspection of the system to the customer and offer him this service. For more details see the relevant EN standards.

For further information see EN 50131-1 and other standards.
## Trouble-shooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible causes</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The control panel is not in service mode after being powered up.</td>
<td>The control panel does not have factory-default settings.</td>
<td>Reset the control panel.</td>
</tr>
<tr>
<td>It is impossible to enroll a wireless device to the control panel.</td>
<td>The device’s location is unsuitable, the control panel antenna is disconnected, the device’s battery was incorrectly installed, the control panel is not in enrollment mode, the device is too near to the control panel (it should be at least 2 meters away).</td>
<td>Check and fix the mentioned problems.</td>
</tr>
<tr>
<td>The keypad unit indicates a fault</td>
<td>Press the ? key to see the cause.</td>
<td>React according to the cause displayed.</td>
</tr>
<tr>
<td>A motion detector triggers false alarms for no apparent reason.</td>
<td>Animals are moving in the protected area (mice etc), sudden changes in temperature, significant air movements, movement of objects having a temperature close to 37°C (e.g. curtains moving above a radiator)</td>
<td>Change the location of the detector, select a higher immunity in the detector, use an optional pet lens in the detector, program alarms confirmed by two detectors in the control panel.</td>
</tr>
<tr>
<td>The wireless keypad does not indicate entrance delays by beeping.</td>
<td>If the keypad is only battery-powered, then it turns off 20 seconds after the last time a key was pressed. To indicate entrance delays, first wake it up.</td>
<td>Install an ordinary magnetic sensor to the entrance door, wiring it to the keypad input so that opening the door wakes up the keypad and reports to the control panel. Alternatively, power the keypad with an AC adaptor to prevent sleep mode or install an indoor wireless siren type JA-80L to generate entrance delay beeps.</td>
</tr>
</tbody>
</table>

fig. 15 Trouble-shooting
11 Control panel technical specifications

External power source:
- 230 V / 50Hz, max. 0.1 A, together with T200 mA fuse
- 110 to 120 V / 60Hz, max. 0.2 A, together with T400 mA fuse

CLASS PROTECTION II

Power supply: type A (EN 50131-6)

Backup battery: 12 V, 1.3 to 2.6 Ah, typical battery lifetime approx. 5 years

Maximum recharge time: 72 hours

Backup power output (+U terminal) maximum continuous load 0.4 A

intermittent load 1 A for 15 min’s max.

Number of combination (51 users) - code + card: 1 075 970

Number of wireless device addresses: 50 (requires a JA-82R module)

Communications frequency (JA-82R): 868 MHz ISM band

Number of hard-wired inputs: 4 (up to 14 if the JA-82C is plugged in)

double balanced inputs, with triggering and tamper functions

each wireless detector blocks the hard-wired input to which it is assigned

External warning output EW*: switching to GND, max. 0.5 A

Internal warning output IW*: switching to GND, max. 0.5 A

Programmable outputs: PGX, PGY max. 0.1 A, switching to GND

Event memory: 255 latest events, including date and time stamping

Intruder alarm signal or message: after 1 or 2 events (adjustable)

Tamper signal or message: after 1 event

Wrong authorization code alarm signal or message: after 10 events

Fault signal or message: after 1 event

Security grade: 2 according to EN 50131-1, EN 50131-6, and EN 50131-5-3

Environmental class: II. indoor-general (-10 to +40°C) compliant with EN 50131-1

EMC: EN 50950-1

JA-82R radio module

Communications frequency (JA-82R): 868 MHz ISM band

Can be operated according to ERC REC 7003

Radio emissions: ETSI EN 300220

* These signals are also transmitted wirelessly to wireless sirens and AC and UC receiver modules.

JABLOTRON ALARMS a.s. hereby declares that the JA-82K is in compliance with the relevant Union harmonisation legislation: Directives No: 2014/35/EU, 2014/30/EU, 2011/65/EU.
The original of the conformity assessment can be found at www.jablotron.com - Section Downloads.

Note: Although this product does not contain any harmful materials we suggest you return the product to the dealer or directly to the manufacturer after use.

fig. 16 Control panel box dimensions

Description: 1. antenna connector; 2. wireless module; 3. the heart beat LED; 4. wired-zone module; 5. antenna for wireless module; 6. AC power terminals; 7. terminals; 8. back up battery; 9. digital bus connector; 10. GSM antenna; 11. mains fuse (T200 mA); 12. transformer; 13. box cover tamper contact; 14. GSM communicator; 15. GSM communication LED; 16.SIM Card

fig. 17 Control panel box layout
### Control panel programming sequences

<table>
<thead>
<tr>
<th>Function</th>
<th>Sequence</th>
<th>Options</th>
<th>Factory default</th>
<th>Setting to comply with EN-50131-1</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entering enrollment mode</td>
<td>1</td>
<td>Keys:</td>
<td>nothing</td>
<td></td>
<td>• devices enroll by connecting their power (battery) except keyfobs which enroll by pressing &amp; holding a pair of their buttons</td>
</tr>
<tr>
<td></td>
<td></td>
<td>① and ⑦ address scrolling</td>
<td></td>
<td></td>
<td>• an occupied address is indicated by the A indicator being lit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>holding 2 erases the displayed</td>
<td></td>
<td></td>
<td>• enrolling a device to a new address will move it there</td>
</tr>
<tr>
<td></td>
<td></td>
<td>address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>holding 4 erases all addresses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td># exiting enrollment mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit delay time</td>
<td>20 x</td>
<td>x = 1 to 9 (x10 s =10 to 90 s)</td>
<td>30 s</td>
<td></td>
<td>if a final door detector is used, then x is multiplied by 30 s instead (i.e. from 30 to 270 s)</td>
</tr>
<tr>
<td>Entrance delay time</td>
<td>21 x</td>
<td>x = 1 to 9 (x 5 s = 5 to 45 s)</td>
<td>20 s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm duration time</td>
<td>22 x</td>
<td>x = 1 to 8 (min.), 9=15min</td>
<td>4 min.</td>
<td>0=10s (for testing)</td>
<td></td>
</tr>
<tr>
<td>PGX function</td>
<td>23 x</td>
<td>x in an unsplilt system:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>24 x</td>
<td>0 whole system set (ABC) = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 any system part set = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 AB set (not C) = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Fire alarm = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Panic alarm = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Any alarm = PG on (excluding Panic)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 AC dropout = PG on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 PG on/off (by +80 /+81 for PGX and +90/+91 for PGY)</td>
<td>7 on/off +80/+81</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 Single 2 s pulse</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(keys +X, +9 = Y)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling of telephone number changes in maintenance mode</td>
<td>25 x</td>
<td>251 = YES 250 = NO</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio interference indication</td>
<td>26 x</td>
<td>261 = YES 260 = NO</td>
<td>NO</td>
<td>YES 30 s or longer</td>
<td></td>
</tr>
<tr>
<td>Radio communication supervision</td>
<td>27 x</td>
<td>271 = YES 270 = NO</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>RESET enabled</td>
<td>28 x</td>
<td>281 = YES 280 = NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master control panel enrollment to a sub control panel for setting (arming) control</td>
<td>290</td>
<td>The sequence triggers enrollment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Un)setting the master control panel will (un)set the sub control p. The sub c. panel must be in enrollment mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master code reset</td>
<td>291</td>
<td>Returns master code to 1234</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measuring signal strength</td>
<td>298</td>
<td>Activates measurement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enrolling the control panel to UC, AC or a sub control panel</td>
<td>299</td>
<td>The sequence triggers enrollment.</td>
<td>see 6.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting (arming) without an access code</td>
<td>30 x</td>
<td>301 = YES 300 = NO</td>
<td>YES</td>
<td>NO</td>
<td>by keying: A, B, ABC, +1, +2, +3, +4</td>
</tr>
<tr>
<td>Triggered detector indication by text on the keypad display</td>
<td>31 x</td>
<td>311 = YES 310 = NO</td>
<td>YES</td>
<td></td>
<td>allows the display of open windows &amp; doors, to view details press ?</td>
</tr>
<tr>
<td>Confirmation of intruder alarms</td>
<td>32 x</td>
<td>321 = YES 320 = NO</td>
<td>NO</td>
<td></td>
<td>An alarm can be confirmed by any other intruder detector in any section which is set (armed).</td>
</tr>
<tr>
<td>Exit delay beeps</td>
<td>33 x</td>
<td>331 = YES 330 = NO</td>
<td>YES</td>
<td></td>
<td>The last 5 s faster</td>
</tr>
<tr>
<td>Exit delay beeps while partially arming</td>
<td>34 x</td>
<td>341 = YES 340 = NO</td>
<td>NO</td>
<td></td>
<td>The last 5 s faster (linked to 33x setting)</td>
</tr>
<tr>
<td>Entrance delay beeps</td>
<td>35 x</td>
<td>351 = YES 350 = NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting (arming) confirmation by wired-siren chirp</td>
<td>36 x</td>
<td>361 = YES 360 = NO</td>
<td>NO</td>
<td></td>
<td>IW terminal only</td>
</tr>
<tr>
<td>Siren always sounds during audible alarms</td>
<td>37 x</td>
<td>371 = YES 370 = NO</td>
<td>YES</td>
<td></td>
<td>NO = siren only sounds if the system is completely set (armed)</td>
</tr>
</tbody>
</table>

Fig. 18 Summary of the programming sequences

JA-82K control panel installation manual - 17 - MKH52204
### Function Sequence Options Factory default Setting to comply with EN-50131-1 Notes

<table>
<thead>
<tr>
<th>Function</th>
<th>Sequence</th>
<th>Options</th>
<th>Factory default</th>
<th>Setting to comply with EN-50131-1</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless-siren alarms enabled (IW &amp; EW)</td>
<td>38x</td>
<td>381 = YES 380 = NO</td>
<td>YES</td>
<td></td>
<td>NO = siren disabled</td>
</tr>
<tr>
<td>Auto-bypass user approval via the * key</td>
<td>39x</td>
<td>391 = YES 390 = NO</td>
<td>NO</td>
<td>YES</td>
<td>to confirm auto-bypass while exiting Service mode press # twice</td>
</tr>
<tr>
<td>Final-door detectors</td>
<td>65x</td>
<td>0 none 1 detectors 01 to 05, 2 detectors 46 to 50 x = 0</td>
<td></td>
<td>If multiple F. door detectors are used, then triggered state=any of them, non triggered state=all of them</td>
<td></td>
</tr>
<tr>
<td>Partial setting (arming) or system splitting</td>
<td>66x</td>
<td>0 unsplit system 1 partial setting (A, AB, ABC) 2 split system A, B &amp; common section C (set if A &amp; B are set)</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic Summer Time (Daylight Saving Time)</td>
<td>680x</td>
<td>6801 = YES 6800 = NO</td>
<td>NO</td>
<td>Changes internal clock + 1h on Apr.1 &amp; -1h on Nov.1</td>
<td></td>
</tr>
<tr>
<td>Pulse reaction of tamper sensors</td>
<td>681x</td>
<td>6811 = ignore permanently triggered tamper sensors, i.e. only react to an increase in the number of triggered tamper sensors 6810 = react with a tamper alarm to all triggered tamper sensors x = 0</td>
<td></td>
<td>Suppresses the indication of permanently triggered tamper sensors</td>
<td></td>
</tr>
<tr>
<td>Operating the PG outputs using *8 and *9</td>
<td>682x</td>
<td>6821 = YES 6820 = NO</td>
<td>YES</td>
<td></td>
<td>if yes then arrow keys can also operate PGX</td>
</tr>
<tr>
<td>Permanent alarm status display for a set system</td>
<td>683x</td>
<td>6831 = YES 6830 = NO</td>
<td>NO</td>
<td>suppresses the 3min. display timeout</td>
<td></td>
</tr>
<tr>
<td>Tamper alarm if unset (disarmed)</td>
<td>684x</td>
<td>6841 = YES 6840 = NO</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Recording PG output activation to memory</td>
<td>685x</td>
<td>6851 = YES 6850 = NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engineer reset</td>
<td>686x</td>
<td>6861 = YES 6860 = NO</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social alarm</td>
<td>687x</td>
<td>6871 = YES 6870 = NO</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annual check requirement display</td>
<td>690x</td>
<td>6901 = YES 6900 = NO</td>
<td>NO</td>
<td></td>
<td>Another time period can be selected by changing the system date before exiting service mode</td>
</tr>
<tr>
<td>Only single alarm indication</td>
<td>691x</td>
<td>6911 = YES 6910 = NO</td>
<td>NO</td>
<td>YES</td>
<td>6911 = no other alarms are reported during an intruder alarm</td>
</tr>
<tr>
<td>Setting (arming) by service code</td>
<td>692x</td>
<td>6921 = YES 6920 = NO</td>
<td>NO</td>
<td>only with the master code holder's approval</td>
<td></td>
</tr>
<tr>
<td>Audible panic alarm</td>
<td>693x</td>
<td>6931 = YES 6930 = NO</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Higher control-panel receiver-sensitivity</td>
<td>694x</td>
<td>6940 = normal 6941 = higher</td>
<td>normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access by Code plus Card</td>
<td>695x</td>
<td>6951 = Code+Card 6950 = Code or Card</td>
<td>code or card</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Audible 24h intruder alarm</td>
<td>696x</td>
<td>6961 = YES 6960 = NO</td>
<td>YES</td>
<td>0= silent 24h intruder alarm</td>
<td></td>
</tr>
<tr>
<td>Service mode only with service + user (master) code</td>
<td>697x</td>
<td>6971 = YES 6970 = NO</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>
Device reactions and section assignment (detectors, key fobs, control panel and keypad inputs)
- A detector’s natural reaction can be INS, DEL or Fire (selectable in the detector)
- The natural reaction of Control panel & Keypad wired inputs is DEL

Keyfob natural reactions: 🕔 ( [, ] = SET (arm), 🕒 (,), [ ] = UNSET (disarm) and both simultaneously = Panic. If a reaction from 2 to 8 is selected (see opposite), only the key 🕒 ( [ ] ) button has no effect (can still be used for controlling UC/AC receivers).
- Assignment to sections will only have an effect on partial arming or if the system is split (except PG output control)
- For partial arming, a pair of keyfob buttons assigned to section:
  - A has the effect: 🕒 ( [, ] ) = SET A, 🕒 (, ) = SET AB
  - B has the effect: 🕒 ( [, ] ) = SET A, 🕒 (, ) = SET AB
  - C has the effect: 🕒 ( [, ] ) = SET ABC, 🕒 (, ) = UNSET ABC
- In a split system, a keyfob button pair assigned to section: A=SET/UNSET A, B=SET/UNSET B, C=SET/UNSET ABC

Code (card) reactions and section assignment
- A code (card) may have the same kind of reaction as devices
- Assignment of the code to sections is useful for split systems only. In a split system, a code (card) assigned to C will SET/UNSET all ABC sections.

Enrollment by keying in production codes

Automatic Daily Setting/Unsetting schedule (arming/disarming)

Changing the service code
5 NC NC = new code (4 digits) 8080 enter NC twice

Go to maintenance mode
292 switches to maintenance mode -

Setting the internal clock
4 hh mm DD MM YY 00:00 1.1.00

Editing keypad text
Text for device names, code names and PG output names are stored in each individual keypad.
- The menu can be entered in Service mode by holding the ? key. Then the internal keypad menu will be displayed. Using the arrows or keys 1 and 7 you can scroll through the menu to Edit text. Press
- Editing mode and the name of the device enrolled to address 01 is then displayed with a flashing cursor on the first text character.
- Key functions:
  1 and 7 text scrolling (see table)
  3 and 9 character-selection (A,B,C,D,......,8,9,0)
  4 and 6 cursor control (left/right)
  2 delete selected character
  8 space
  # exit editing (& save changes)
13 Programming access codes and cards

<table>
<thead>
<tr>
<th>Code name</th>
<th>Amount</th>
<th>Sequence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Service** | 1 | 5 NC NC | - Only programmable in Service Mode.  
- NC = new code (must be entered twice) – a card cannot be used.  
- Factory-default service code: 8080  
- This code can be changed but not erased.  
*Example*: 5 4567 4567 |
| **Master** | 1 | +5 MC NC NC | - Only programmable if the system is totally unset (disarmed)  
- MC = master code or card (factory default 1234)  
- NC = new code or card entry – a numerical code has to be entered twice, but a card only presented once  
- Either a code or a card can be programmed as a master code (to have both is impossible).  
- The Master Code can be changed but not erased.  
- The Master Code’s reaction is set/unset and it is assigned to all sections.  
- To reset the Master Code to the factory default 1234, enter 291 in Service Mode (this will only affect the Master Code).  
- To make handing over the system to the end user easier, we recommend programming the system card (provided with the control panel) to the master code.  
*Example*: +5 1234 and then presenting the card to the keypad’s RFID reader |
| **User** | 50 | +6 MC nn NC | - Only programmable if the system is totally unset  
- MC = Master Code or card.  
- nn = user code or card position from 01 to 50.  
- NC = new code or card entry.  
- Factory default: all user codes and cards are erased.  
- Each user position can have both a card and a code programmed to it (by using the sequence nn NC twice)  
- Each user code can have its own reaction programmed by an installer in Service Mode, and with a split system, codes can be assigned to different sections.  
*Example*: +6 1234 12 4345 (code 4345 will be programmed to user position 12)  
To erase codes/cards enter:  
+6 MC nn 0000 erases the code and the card in user position nn.  
+6 MC 00 UC erases the code UC (or card UC) if programmed to any user position.  
+6 MC 00 0000 erases all user codes and cards in user positions 01 to 50. |

fig. 19 Programming access codes and cards (only in the disarmed state)