Contents

USER FEATURES **2**

CAN REMOTE CONTROL BE SECURE? **2**

HOW THE SYSTEM WORKS **2**

REMOTE CONTROL BY PHONE **3**

1. GENERAL RULES FOR REMOTE CONTROL VIA SMS INSTRUCTIONS ✉ 3
2. SETTING (ARMING) BY SMS ✉ XXXX_SET 3
3. UNSETTING (DISARMING) BY SMS ✉ XXXX_UNSET 4
4. STATUS INTERROGATION ✉ XXXX_STATUS 4
5. LAST EVENT INTERROGATION ✉ XXXX_MEMORY 4
6. CONTROLLING APPLIANCES BY SMS ✉ 5
7. SIM CARD CREDIT INTERROGATION ✉ XXXX_CREDIT 5
8. REMOTE CONTROL VIA A TELEPHONE KEYPAD 5
9. REMOTE CONTROL BY DIALLING-IN 6
10. VOICE MENU FLOWCHART 7

PROGRAMMING IN MAINTENANCE MODE **8**

REMOTE ACCESS BY INTERNET **8**

User features

The JA-82Y GSM communicator offers many useful features. Its main purpose is **reporting events** directly **to you** and **to an ARC** (**A**larm **R**eceiving **C**entre).
In addition, the communicator allows you **remote system control and programming by phone or Internet and the remote control of appliances** in a house (e.g. heating).

Can remote control be secure?

There are several mechanisms for protection to ensure that remote system control is secure:

Using a phone:

- The communicator's **SIM card number gives basic protection**. This number is not explicitly referenced anywhere in the system, and we recommend keeping it private.
- As a second level of protection, every SMS instruction is required to contain a **valid access code – the same code as the one used for system operation from** the keypad. This code is also used when you request system access via a phone call – for so-called connection authorization.
- The third level can be realised by naming instructions with your own texts. We recommend recording these texts and keeping them in a safe place.

How the system works

Alarm triggering is processed by the communicator as follows:

- If enabled, **reporting to ARCs** (Alarm Receiving Centres) is started first.
- **SMS reports** are sent to pre-programmed phone numbers in the order they are stored.
- As a sort of **acoustic signalling**, pre-programmed phone numbers are called (again in the order that they are stored). Each phone number is dialled only once, regardless of whether the call is answered or not. Calling the next telephone number can be stopped by pressing # on your mobile phone. Calling the next numbers are then cancelled and your phone keypad is switched to alarm keypad simulation. Now you can remotely control the system like you are standing next to it.

If an alarm is cancelled by a user (by presenting a valid code/card) while it is being reported, any unsent SMSes and unperformed call reports are cancelled. However, the ARC still gets a complete set of reports about events in the system.

Remote control by phone

For a mobile phone, there are two ways to control the system remotely. You can either send SMS instructions or establish an authorized connection (protected by an access code) to the system. In this case the system is controlled by a voice menu. Press 9 to switch the phone to alarm keypad simulation. The phone keypad can be used the same way as the system keypad. Using a fixed line phone, you can only operate the system by dialling the communicator's number and establishing an authorized connection.
The below described way of remote control corresponds to the communicator's factory default setting. The configuration can be modified during installation. The installer should clearly explain any changes to the default setting.

1. General rules for remote control via SMS instructions ✉

- More than one instruction can be used in a single SMS message. It has to be separated by a comma.
- SMS instructions are not case-sensitive. Only standard English (ASCII) characters are accepted.
- All SMS instruction words (parameters) must be separated by a space. In this document a space in an SMS instruction will also be denoted by the underline character '_'.
- SMS instructions can be sent from a mobile phone or from a GSM gateway.
- If the % character is used, all preceding text will be ignored. The %% symbol ends processing when used in SMS text – i.e. all the following text will be ignored. It is recommended to use this symbol at the end of the instruction if the provider sends some additional text after your message (advertisements etc.).
- **Warning: If any extra text is not separated from a valid SMS instruction text by % or %% symbols, the SMS message will not be recognized and no instruction will be executed.**
- Performance of the instruction is confirmed by an SMS reply.
- The default instruction texts can be customized by an installer or administrator. E.g. the command PGX ON can be changed to SWITCH ON HEATING etc.

2. Setting (arming) by SMS ✉ xxxx_SET

The SET instruction allows you to put the system in to a set (armed) state, fully or partially. If the system is already set, it will not change its status.
Send an SMS message containing: **xxxx_SET**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: Sending **4321 SET** will set the system the same way as if the code 4321 had been entered on the system keypad.

Notes:
- As a factory default, setting (arming) by a SET instruction is confirmed by the system via an SMS reply.
- When the current system status does not allow system operation (e.g. when in programming mode), you will be notified about the situation via an SMS reply.
- In a split system, an xxxx_SET instruction will only have an effect on the section to which the code xxxx belongs.

3. Unsetting (disarming) by SMS

✉ xxxx_UNSET

The UNSET instruction allows you to unset (disarm) the system, fully or partially. If the system is already unset, it will not change its status.
Send an SMS message containing: **xxxx_UNSET**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: Sending **4321 UNSET** will unset the system the same way as if the code 4321 had been entered on the system keypad.

Notes:

- As a factory default, unsetting (disarming) by an UNSET instruction is confirmed by the system via an SMS reply.
- When the current system status does not allow system operation (e.g. when in programming mode), you will be notified about the situation via an SMS reply.
- In a split system, an xxxx_UNSET instruction will only have an effect on the section to which the code xxxx belongs.

4. Status interrogation

✉ xxxx_STATUS

The STATUS instruction allows you to get information about the current system status. The communicator will reply with an SMS reporting the current set/unset status, GSM signal strength, GPRS connection status and transmission success/failure status for each ARC involved.

Send an SMS message containing: **xxxx_STATUS**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: If the system is set, an SMS instruction **4321 STATUS** will be replied by the system via an SMS message which might look like the following:
Report from your alarm: System status: Set, GSM: 80%, GPRS OK, MS1 OK, MS2 OK, MS3 OK.

where GSM: 80% means the GSM signal strength, GPRS OK means communication via GPRS has been successfully established and MS1 OK, MS2 OK, MS3 OK means that all relevant data has been transmitted to monitoring stations MS1, MS2 and MS3.

5. Last event interrogation

✉ xxxx_MEMORY

On receiving a MEMORY instruction, the communicator will reply by reporting the last 3 events recorded in the control panel memory.

Send an SMS message containing: **xxxx_MEMORY**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: If an alarm has been triggered, the communicator will reply to the SMS instruction **4321 MEMORY** by reporting:
Report from your alarm: Last events: Unsetting, Master code, Alarm cancelled by user, Master code, Delayed alarm, 02: Device

6. Controlling appliances by SMS ✉

You can send SMS instructions to switch on/off communicator or control panel outputs. Up to 2 appliances can be attached (device X and device Y – see the corresponding table in the control panel user manual). The communicator will reply with an SMS message to confirm performance of the instruction.

To switch device X on send the following SMS:	**xxxx_PGX_ON**
To switch device X off send the following SMS:	**xxxx_PGX_OFF**
To switch device Y on send the following SMS:	**xxxx_PGY_ON**
To switch device Y off send the following SMS:	**xxxx_PGY_OFF**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: If the heating in your house is operated as the X device, you can switch the heating on by sending **xxxx PGX ON.**

7. SIM card credit interrogation ✉ xxxx_CREDIT

If a prepaid SIM card is used in the communicator you can check the credit balance.
Send an SMS message containing: **xxxx_CREDIT**

where:	**xxxx**	is a valid access code (user or master)
	_	is a space character

Example: The **xxxx_CREDIT** request is responded to by the following message:
Report from your alarm: Credit: Current balance is 26.35€.

Notes:

- **This instruction has to be pre-configured by the installer according to GSM provider requirements**
- **The user is responsible for the credit balance being sufficient!**
- **The GSM provider may have a time-limit after which the credit validity will expire!**
- **You can find more details on this function in the communicator installation manual**

Owing to the above facts, using pre-paid SIM cards is <u>not recommended</u>.

8. Remote control via a telephone keypad

If you want to operate the alarm system via a phone (mobile or landline), perform the following:

- Dial the GSM communicator number.
- The system will answer in 15 seconds. Listen to the voice menu introduction, the system asks you to key in your access code
- On your phone keypad, enter a valid access code (user, master or service code). Listen to the answer (current system state) and the system offers to change its status.
- You can press 9 to open keypad simulation mode; switching back to voice menu mode is not possible dial again.
- From this moment on, the telephone keypad will work as a system keypad.
- System status is signalled in these ways:
    - **1** beep = **set** (armed)
    - **2** beeps = **unset** (disarmed)
    - **3** beeps = **programming mode**
    - **siren sound** = **alarm**
    - **voice message** during a type of event = intruder alarm, tamper alarm, fault,..
- Any subsequent change to the system status is again indicated acoustically. For instance, after unsetting the system, you will hear two beeps. (see above)
- You can operate devices X or Y via the phone keypad the same way as from a system keypad. This means ***81**/***80** will control **device X** and ***91**/***90** will control **device Y.**
- To terminate the connection simply hang up. Connection is automatically terminated if there is no entry within 60 seconds.

Note: Remote access from a landline is only possible from a phone using tone dialling (DTMF).

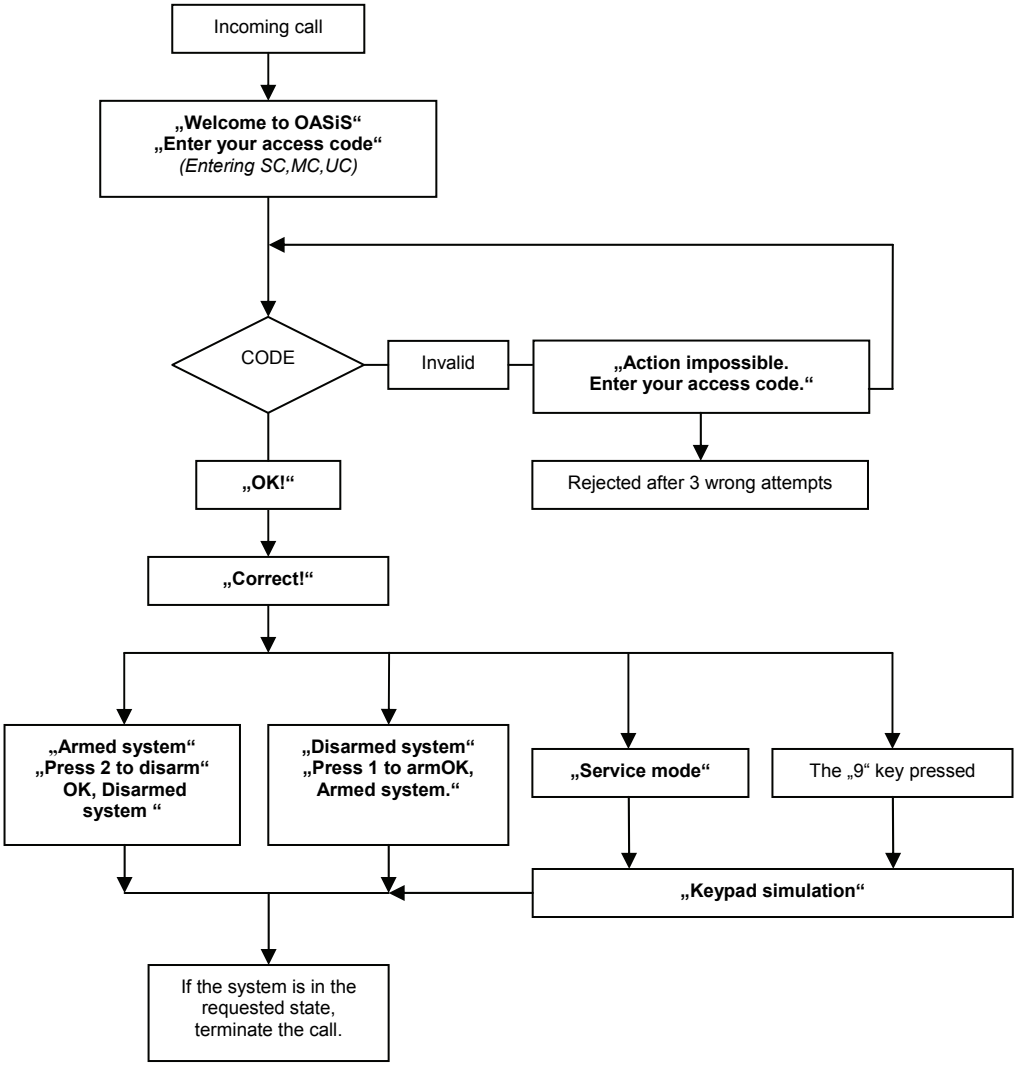
9. Remote control by dialling-in

With some limitations, the communicator allows you to operate the system by ringing the communicator. This operation requires your phone number to have been pre-authorized by being stored in the communicator memory

Notes:

- Dialling-in operation is not enabled for phones having hidden numbers.
- If you control by dialling-in without remote access privileges, the system performs the command and establishes the connection, it's for free.
- A phone which is pre-authorized for dialling-in remote control can also by used for normal remote control – just let it ring until the control panel answers the call by voice menu. Naturally, a pre-programmed function will be performed first.

10. Voice menu flowchart



Tab.1

Programming in maintenance mode

Programming in maintenance mode requires access to be enabled by a service technician. Otherwise, no programming is possible – any instruction sequence will be rejected by the system and the keypad will beep four times.

The following description is intended for a system administrator, who knows the control panel master code. All the settings can be performed via keying-in on a system keypad. An unfinished sequence can be cancelled by pressing the # key. A sequence is only stored in control panel memory (or executed) after the sequence has been completely entered. All the settings are only applicable if the control panel is in **maintenance** mode. To enter maintenance mode, first make sure, that the system is completely unset. Then enter the following sequence on the system keypad:

*** 0 master code (card)** The keypad will display **Maintenance mode**.

In maintenance mode it is possible to set transmission parameters, measure the GSM signal strength, enable/disable remote access, set the forwarding of incoming messages, record voice messages and so on. More details with descriptions can be found in the installation manual.

Wrongly set parameters could limit or cancel some of the functions (alarm reporting, faults,..). When you change any parameters, test that the system works properly.

Remote access by Internet

The system can be accessed remotely via Olink software version 2.0 and higher, which allows complete programming by installers and also operating the system by end users. The GPRS service (or, alternatively, SMS) is used for data transfer.

Remote access is provided by Jablotron Alarms free-of-charge (only the data transfer from the premises is charged). The installation technician can set up remote access according to the desired arrangement.

Accessing the communicator remotely requires its **SIM card to be enabled for GPRS data transfer**. Only then can the device work properly.

You can **operate the system** directly **using a virtual keypad by entering a programming sequence, Olink can open a command line** where the sequences can be entered the same way as if they were entered from a system keypad. By pressing the submit button you send the instruction via the internet network to the communicator where it will be processed. More details with descriptions can be found in the installation manual.

The **list of events** can be opened in any control panel state, therefore it is not necessary to put the control panel into a specific mode (like unsetting or switching to Maintenance Mode). The events list records the last 255 events.