JABLOTRON
CREATING ALARMS

USER MANUAL
JABLOTRON 10

EN Grade 2 certified

For questions and further information contact your installer.

Manufacturer:
JABLOTRON ALARMS
Pod Skalkou 33
466 01 Jablonec nad Nisou
Czech Republic
www.jablotron.com

MNX501001

Thank you for choosing the JA-10 security system. This manual is intended for the set of the JA-14K control panel and JA-10E or JA-15E keypads. This system is a unique indoor solution for commercial, home and personnel security which offers the use of wireless and wired devices. The JA-10 is very easy to control. Simplicity of control consists of two steps, authorization with a code or an RFID tag followed by pressing an individual function button on a keypad. The alarm system can be also controlled just by authorization. The JA-10 offers a wide range of detectors with timeless design and can be operated from anywhere owing to complete remote control access via our application for smart phones.

The JA-10 system is designed for up to 16 users and it can be divided into 4 separate sections. Up to 32 devices can be connected and the system offers 4 multi-purpose programmable outputs (e.g. home automation).

WARNING:
The JA-10 alarm system is intended to be installed and programmed by professionals. A user can only administrate user functions and access rights to the alarm system.

The alarm system can be programmed to utilize various ways of control which are selectable during installation as system profiles such as:

- o Default Jablotron
- o EN 50131, gr.2

Some of the user functions will be limited depending on the selected profile. Request a detailed function list from your service technician.

2. OPERATING THE JA-10 SYSTEM

The alarm system can be controlled by a system keypad and a few other ways. To unset the alarm, authorization in the form of user identification is always required. The system detects the identity of the users and allows them to operate those parts of the system which they have been assigned to control. You can choose from different ways of setting with or without authorization. When setting without authorization is used, you don't have to authorize yourself because it is possible to set the system just by pressing a function button on a keypad. The control panel may be configured to be controlled simply by authorization. The user name, date, and time are recorded and stored in the system's memory every time the system is accessed. This information is available indefinitely. Any user can also cancel a triggered alarm (stop sounding sirens) just by authorization in any part of the system (depending on their access rights). However, that does not automatically unset the system (unless the system's default setting is changed).

Note: Depending on the configuration of the installation and system settings, some of the options described below may not be available. Consult the configuration of the installation with your service technician.

WARNING: The alarm system monitors the number of incorrectly typed user codes and use of incorrect access cards. A tamper alarm will be triggered after 10 incorrect attempts at authorization and the control panel will be temporarily blocked depending on the alarm system configuration (a selected system profile).

Users and Their Access Rights

CODE AUTHORIZATION	TYPE DESCRIPTION
ARC code	This code has the highest level of authorization to configure the system's behaviour and is exclusively allowed to perform the system unblock after a triggered alarm. It can enter Service mode, access all tabs with options including ARC communication to which it can deny access to a Service technician (Service code). As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the ARC code can control all sections and PG outputs used in the system. This code enables to add more Administrators and other users with a lower level of authorization, assign them with codes or RFID tags. It also has a permission to erase alarm and tamper alarm memory. The number of ARC codes is limited only by remaining capacity of the control panel.
Service code (Service)	It can enter Service mode and configure the system's behaviour. It has access to all tabs with options including ARC communication unless the access is limited by a superior ARC technician. As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the Service code can control all sections and PG outputs used in the system. It can create a user with ARC permission, other Service technicians, Administrators and other users with a lower level of authorization and assign them with access codes or RFID tags. It also has a permission to erase alarm and tamper alarm memory. The number of Service codes is limited only by remaining capacity of the control panel. By the factory defaults, the code is 1010 and it cannot be erased.
Administrator (Main)	This code has always full access to all sections and is authorized to control all PG outputs. The Administrator can create other Administrator and other codes with a lower level of authorization, assign them with access to sections, PG outputs, access codes or RFID tags. It has permission to erase the alarm and tamper memory. There can be only one main Administrator code which cannot be erased. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized as to confirm access. By the factory defaults, the code is 1234.
Administrator (Other)	This type of Administrator code has access to sections selected by the main Administrator to which the other Administrator can add new users with the same or lower level of authorization in order to control sections and PG outputs, assign them with access codes or RFID tags. It has permission to erase the alarm and tamper memory in assigned sections. When "Administrator-restricted Service/ARC rights" is enabled, the administrator code must be authorized as to confirm access. The number of Administrator codes (other) is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
User	This code has access to sections and PG control rights assigned by an Administrator. Users can add/delete their RFID tags and change their telephone numbers. It has a permission to erase the alarm memory in assigned sections. Selected user may have time-limited access to their sections. The number of User codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
Set	This code is allowed only to set a designated section and is allowed to control (ON/OFF) PG outputs which require authorization. Users with this level of authorization are not allowed to change their code and are not allowed to erase the alarm memory. The number of Set codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
PG only	Allows the user to control programmable outputs with authorization only. This applies to both switching on and off. Users with this level of authorization are not allowed to change their codes. The number of PG only codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
Panic	This code is allowed only to trigger Panic alarm. A user of this code is not allowed to change it or erase the alarm memory. The number of Panic codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
Guard Code	This is a code for a security agency. This level of authorization allows to set the whole system. However the guard code can unset the system only during alarm or after it has expired as long as the alarm memory is still active. A user of this code is not allowed to change it or erase the alarm memory. The number of Guard codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
Unblocking code	This code is designated only to unblock the system after System blocking by alarm. A user of this code is not allowed to control the control panel, change this code or erase the alarm memory. The number of Unblocking codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.

2.1　KEYPAD CODE AUTHORIZATION

Authorization with a user code is done by typing a valid code into a keypad or with an RFID tag.
It is possible to use 4 or 6-digit codes in the system (depends on the selected profile).

CCCC

Meaning:
CCCC is a 4 or 6-digit code. Allowed codes… from 0000 to 9999 (000000 to 999999)

Default control panel code　　**Administrator: 1234; 123456;**

WARNING: It is recommended to change the Administrator code when the alarm system is powered on for the first time.

The security of access codes and contactless RFID tags:

A control panel enables user to be assigned with one 4 or 6-digit code and one RFID tag for system authorization. User authorization is required during each system operation via keypad, voice menu, web or mobile apps. Code length affects number of possible combinations and therefore code security.

The number of code combinations depends on the configuration:

CONTROL PANEL PARAMETERS	4 DIGITS	6 DIGITS
"Duress access control" disabled, **"Standard authorization"** enabled	$= 10^4$ – (Number of users)	$= 10^6$ – (Number of users)
"Duress access control" enabled, **"Standard authorization"** enabled	$\leq 10^4$ – (Number of users * 3)	$\leq 10^6$ – (Number of users * 3)
"Duress access control" disabled; **"Double authorization"** enabled	$= 10^8 * (10^4$ – Number of users)	$= 10^8 * (10^6$ – Number of users)
"Duress access control" enabled; **"Double authorization"** enabled	$\leq 10^8 * (10^4$ – (Number of users * 3))	$\leq 10^8 * (10^6$ – (Number of users * 3))
Using only an **RFID card** without an access code	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$

WAYS TO IMPROVE PROTECTION AGAINST GUESSING THE VALID CODE:

- o　Using a code with more digits (6-digit codes)
- o　More advanced types of authorization, such as "Double authorization".

Remote control safety:

The control panel can use remote controls. Safety of these controls is provided by more than 1 000 000 combinations of identification codes and special floating encryption transmission.

Ways of operating the JA-14K control panel:

On-site:
- o System keypad
- o System keyfob

Remotely:
- o MyJABLOTRON smart phone application
- o Mobile phone – via SMS
- o Mobile phone – using the voice menu

WARNING: Remote control may be limited depending on the range of security and the selected System profile.

2.2   USING THE SYSTEM KEYPAD

SYSTEM
INDICATOR

STATUS INDICATORS
A, B,C, D

LCD DISPLAY

THE KEYPAD
AND THE RFID
READER

FUNCTION BUTTONS
A, B, C, D

A House   13:16
B Garage
C Garage doors
Welcome home

The JA-10 system may be controlled by system keypads which let you not just control but also display statuses of individual sections. Statuses of individual sections are indicated by status indicators A, B, C, D above the LCD display and by the functions buttons. The control panel can be operated directly (setting or unsetting the alarm and other automation functions) using function buttons on the keypad. The function buttons and the status indicators A, B, C, D are colourfully backlit in order to clearly indicate the section status.

GREEN – Unset   **YELLOW** – Partially Set   **RED** – Set
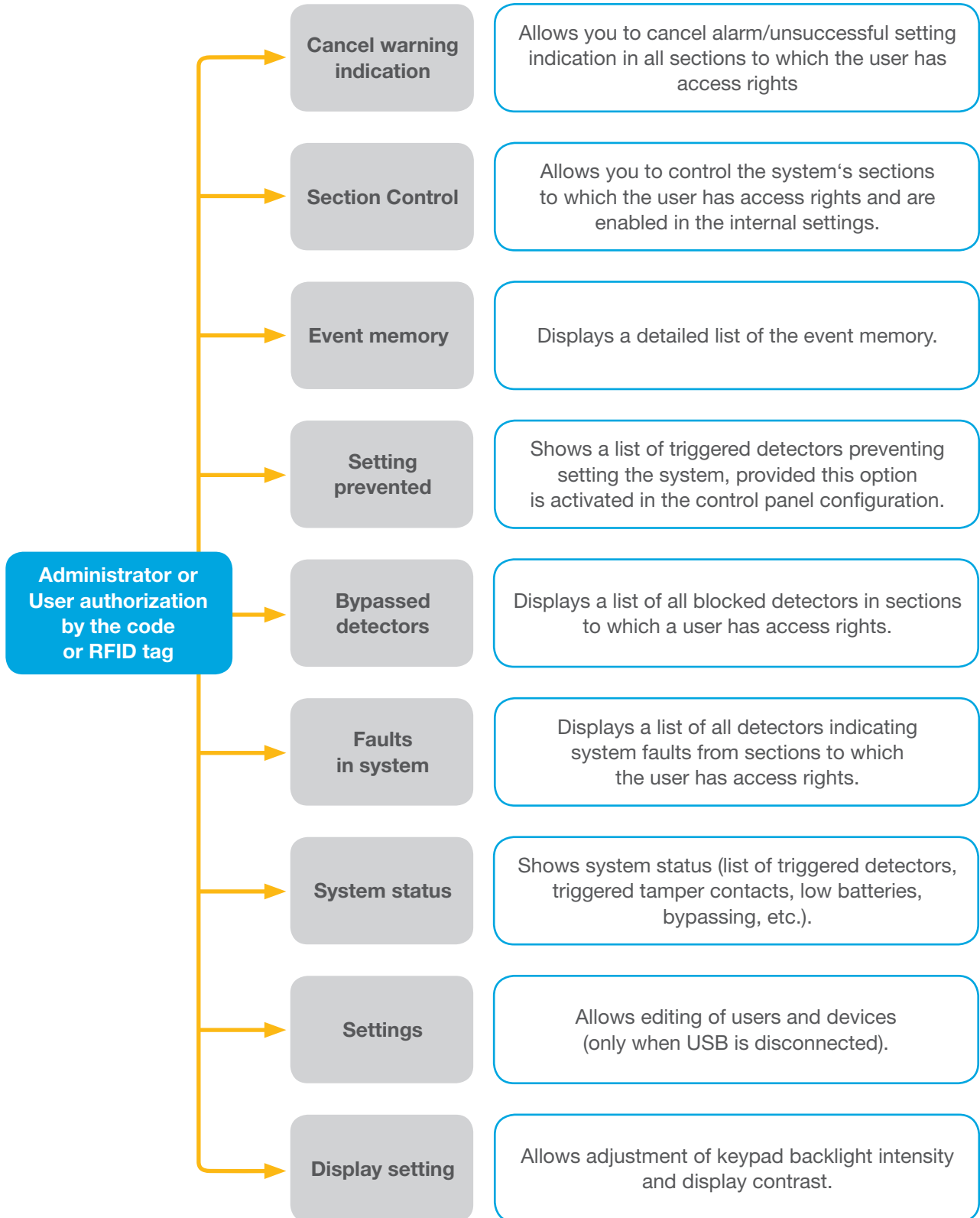

Authorization

Authorization can be done by entering an access code on the keypad or using an RFID tag assigned to a particular user. Each user can have one code and one RFID tag.

The control panel supports RFID tags compatible with 125 kHz EM Unique technology. If higher security is required the alarm system can be set up to use Double authorization using RFID tags and codes (an optional function).

If the user wants to control multiple sections simultaneously, he must authorize himself and then press function buttons of the particular sections subsequently. This way the user can unset all sections (for example the house and the garage) within one single authorization.

Structure and description of the internal LCD keypad menu

Administrator or User authorization by the code or RFID tag

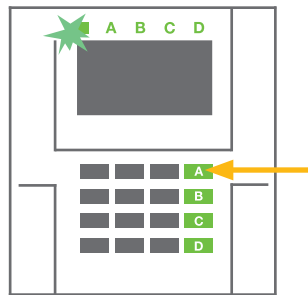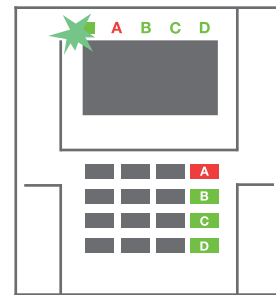| Menu Item	Description
Cancel warning indication	Allows you to cancel alarm/unsuccessful setting indication in all sections to which the user has access rights
Section Control	Allows you to control the system's sections to which the user has access rights and are enabled in the internal settings.
Event memory	Displays a detailed list of the event memory.
Setting prevented	Shows a list of triggered detectors preventing setting the system, provided this option is activated in the control panel configuration.
Bypassed detectors	Displays a list of all blocked detectors in sections to which a user has access rights.
Faults in system	Displays a list of all detectors indicating system faults from sections to which the user has access rights.
System status	Shows system status (list of triggered detectors, triggered tamper contacts, low batteries, bypassing, etc.).
Settings	Allows editing of users and devices (only when USB is disconnected).
Display setting	Allows adjustment of keypad backlight intensity and display contrast.

2.2.1 ALARM SETTING

1. **Authorize yourself using the keypad.** Function buttons A, B, C, D will light up and the system indicator starts flashing green.

2. **Press the function button to set a particular section.** It is possible to set more sections subsequently. The delay between sections selection must not be longer than 2 seconds.

3. **The command is executed** and the keypad acoustically indicates the exit delay. The section is set now, only the detectors with a "Delay" reaction provide time to leave the guarded area during the Exit delay. The status indicator and a function button of the set section will turn red.
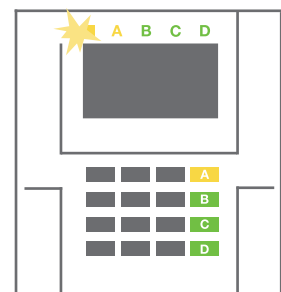
While setting the alarm, if any detector is triggered (e.g. an open window) the system will react (based on the system configuration) in one of the following ways:

- The control panel will set itself. Triggered detectors will be blocked automatically.*)

- The system will optically indicate triggered detectors with a function button flashing red for 8 seconds and the control panel will set automatically once this period has expired (triggered detectors will be blocked). *)

- Setting the section with triggered detectors is also possible by pressing the function button repeatedly. The user must confirm an intention to set the section with a triggered detector (e.g. an opened window). Otherwise the system will not set.

- A triggered detector will prevent the section from being set. This status is optically indicated by a function button flashing red. The detector preventing setting will be shown on the LCD display menu.

*) WARNING: Options a) and b) are not supported by EN 50131, gr.2 (selected control panel system profile).

If a detector with the "Instant zone alarm" reaction is triggered during an exit delay or if a detector with the "Delay" reaction stays triggered after the exit delay has expired, then the control panel will unset again. Unsuccessful setting is indicated by a system indicator flashing yellow, reported to the ARC and indicated by an external siren (applies to the security Grade 2).
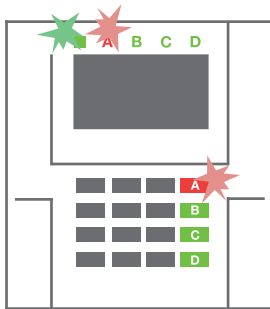

If the control panel is configured to be set without authorization then it is not necessary to authorize yourself. All you have to do is press a function button of a particular section. It is also possible to configure the control panel to be set simply by authorization.
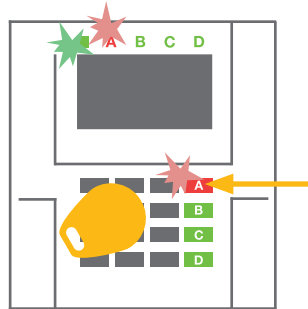
WARNING: Setting without authorization automatically lowers the maximum security level to Grade 1. Consider all possible risks related to using this function.

Consult the installation with a project consultant or a service technician in order to program the desired behaviour of the alarm system.
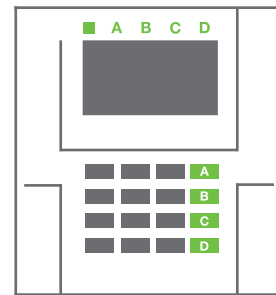
2.2.2 ALARM UNSETTING

1. **When you enter the building** (triggering a detector with a "Delay" reaction), the system starts indicating an entrance delay with a continuous tone, the system indicator and a function button, both flashing red, of the section in which the delayed entrance has been triggered.

2. **Authorize yourself** using the keypad – the system indicator will start flashing green.

3. **Press the function buttons** of the sections you want to unset.

4. **The command is executed.** The function buttons and the system indicator turn green to indicate unset sections.

Note: If the "Unset section by authorization only during entrance delay" parameter is enabled, then mere authorization will unset a section where the entrance delayed has been triggered. This option should be used with caution when using multiple sections.
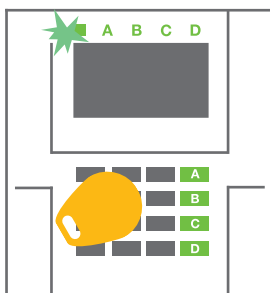
Consult the installation with a service technician in order to program the desired behaviour of the system.
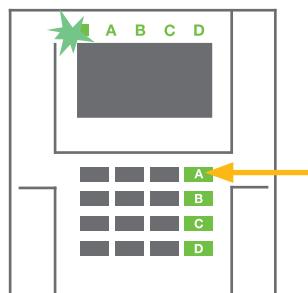
2.2.3 PARTIAL ALARM SETTING

WARNING: This is an additional function of the alarm system.

The system can also be configured to be partially set which allows guarding only by certain detectors in a section.

Example: At night, it is possible to set the door and window detectors only, while selected motion detectors will not trigger the alarm when somebody moves inside the section.

1. **Authorize yourself using the keypad** (enter a code or hold an RFID tag up to the reader). The system indicator button will start flashing green.

2. **Press the function button** of the selected section.

3. **The command is executed** and the function button turns permanently yellow to indicate a partially set section.

To set the entire premises in which partial setting is enabled, hold down the button to set the control panel for 2 seconds or press it twice. After the button is pressed once it shows continuous yellow light, after it is pressed a second time it shows continuous red light.

If the system is partially set already – the function button shows a continuous yellow light – the entire system can be fully set by authorization and pressing the yellow button for a longer time. Once the button is pressed, the system will be fully set and the button turns red.

Partial setting can be configured in a way that authorization is not required. In order to unset the control panel when it is partially set, press the yellow button. The control panel will unset and the button turns green.

2.2.4 DURESS ACCESS CONTROL

Provides unsetting of the control panel in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is reported to selected users (including ARC).
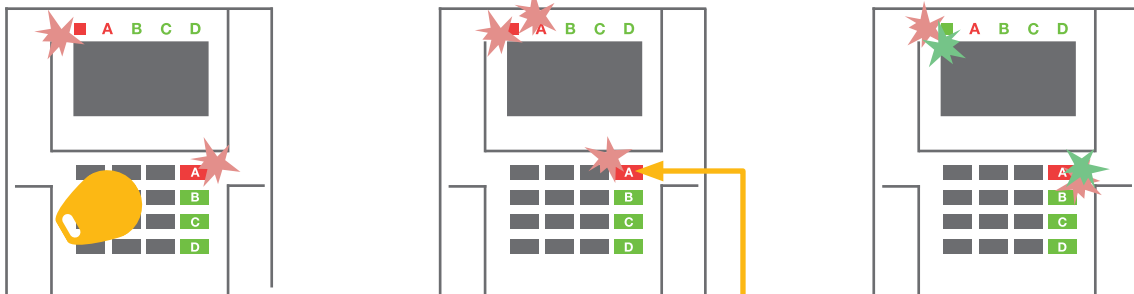
Unsetting under duress is executed by adding 1 to the last number in a valid code. Contact your service technician if you want to use this feature.

Example:
Valid code: 9999   **Code for unsetting under duress: 9990**

2.2.5 TERMINATING A TRIGGERED ALARM

1. **Authorize yourself using the keypad** (enter a code or hold a tag up to the reader).	**2.** **Press the function button** of the section in which the alarm has been triggered.	**3.** **Unsetting is finished** and sirens are silenced. Rapidly alternately flashing function buttons (green/red) and the status indicators indicate the alarm memory.

A triggered alarm in progress is indicated by the status indicator and the function button rapidly flashing red. You need to authorize yourself using the keypad in order to terminate the alarm. The section remains set, a rapidly flashing red function button indicates the alarm memory. Indication will continue flashing even after the system has been unset.

WARNING: If the alarm memory indication was activated during your absence, always enter the building with caution, search for the cause of the alarm in the event history and be very careful when checking the premises or wait until the security agency arrives (provided your system is connected to an Alarm Receiving Centre).

The alarm memory indication remains on until the system is set once again. Alternatively, it can be also cancelled from the keypad menu: **Main menu – Cancel warning indication**.

Indication of a triggered **tamper alarm** can be terminated only by a Service technician and Administrator.

Note: When using the "Default" system profile, it is possible to select a particular action by pressing a function button first and then confirm it by authorization using the keypad.

Terminating an alarm using a remote control will also unset the corresponding section.

2.2.6   SECTION CONTROL BY AUTHORIZATION

The service technician can configure the control panel to be controlled just by authorization. This way the status of all sections can change by authorization on a keypad (by typing an access code or using an RFID tag).

2.2.7   SECTION CONTROL FROM THE KEYPAD'S MENU

Control from the keypad menu:

- o Authorize yourself using a valid code or an RFID chip
- o Enter the menu by pressing **ENT**
- o Section Control → **ENT**
- o Select the desired section using arrows
- o Pressing **ENT** repeatedly will change between section statuses (partially set / set / unset)

Partial setting: | 1 |

Fully set: | **1** |

- o Press **ESC** to exit the menu.

2.3   OPERATING THE CONTROL PANEL WITH A KEYFOB

Keyfobs must be enrolled into the control panel by the installer. In order to control the alarm system, keyfobs must be linked to specific users, which will ensure their identification and prevent sending SMS notifications to the user who is interacting with the control panel at the moment (if notification parameters are set up in this way). The keyfobs provide one-way communication without any confirmation. Keyfobs control and indicate battery status and are equipped with optical and acoustic indication.

The button functions are differentiated by lock icons. The closed lock icon sets programmed sections; the opened lock icon unsets them. The buttons with symbols of full and empty circles can control another section. Buttons of the keyfob can also be configured to control PG outputs in different modes: the first button switches on, the second switches off, each button can have an individual function when hange state is used. For more functions, it is possible to press two buttons at the same time. This way a 4-button keyfob can have up to 6 individual functions. For example, to control an assigned section, one PG status output (e.g. turn the lights on and off), alternatively two impulse PG outputs (e.g. a garage door and door lock).

The keyfob buttons can be blocked to prevent accidental pressing (child safety lock). A command will be sent out when a button is pressed repeatedly.

A low battery is indicated by a red LED light and acoustically (3 fast beeps).
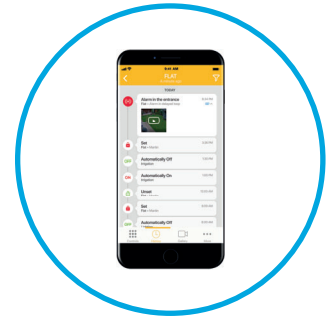
For more information, consult configuration of the remote control with your service technician. More detailed information is available in manuals to particular keyfobs.

2.4 OPERATING THE CONTROL PANEL USING THE MyJABLOTRON SMARTPHONE APP

If the user account is created in the MyJABLOTRON the alarm system can be monitored and controlled remotely using MyJABLOTRON app for smart phones running either on Android (ver. 4.0.3 or higher) or iPhone (ver. 9 or later). The application can be downloaded free of charge from Google play and App Store.

Usernames and login credentials for the MyJABLOTRON smartphone app are created when the system is registered by service technician.

2.5 OPERATING THE CONTROL PANEL BY SMS

If there is a GSM installed in the control panel then it is possible to use SMS commands to control Individual sections and programmable outputs just like the keypad function buttons. The form of text message to operate the system is: CODE_COMMAND. The actual commands are predefined (SET/UNSET) with an additional numeric parameter which identifies a specific section.

One SMS can control multiple sections at the same time. In this case, added numbers in the command define sections.
Example of an SMS command used to set sections 2 and 4.
The underscore "_" sign stands for a space between words.

CODE_SET_2_4

The commands to control the programmable outputs can be programmed by a service technician. For example, you may choose GARAGE DOOR as your command to open garage door. It is also possible to configure the system not to require a code before a command. In such case the command is automatically identified when the system recognizes the user's phone number from which the SMS was sent.

WARNING: It is necessary to use this function with caution. Remote setting and unsetting may cause unwanted alarms or prevent setting when there are other people still present in the building.

2.6 OPERATING THE CONTROL PANEL USING THE VOICE MENU

If there is a GSM or a PSTN communicator installed in the control panel, the system can be controlled from a mobile phone or land line through a simple voice menu, which guides the user through a series of options in the preconfigured language. To access the voice menu, you just dial the control panel's phone number.

Access to the voice menu can be enabled either to all telephone numbers without restrictions or only to authorized phone numbers stored in the control panel. Depending on the configuration, authorization by entering a valid code on a phone keypad may be required. When the user enters the menu, the system will give an update of the current status of all sections assigned to the user. The caller then can control these sections, either individually or collectively, using phone keypad and available menu options.

WARNING: It is necessary to use this function with caution. Remote setting and unsetting may cause unwanted alarms or prevent setting when there are other people still present in the building.

By default, the system is set up to answer incoming calls after three rings (approximately 15 seconds).

2.7 PG OUTPUTS CONTROL

PG output control is intended for non-alarm functions related to simple home automation.

2.7.1 KEYPAD FUNCTION BUTTONS

A PG output switches on by pressing a function button (A, B, C, D) and switches off by pressing the button again. If the output is configured as an impulse output, it will switch off according to the preset time.

Whether authorization is or is not demanded depends on the system configuration.

2.7.2 USER KEYPAD AUTHORIZATION

It is possible to activate a PG output by user authorization (entering a code or using an RIFD tag). The PG output must be configured to activate from a designated keypad.

2.7.3 REMOTE CONTROL

By pressing an assigned remote control button.

2.7.4 DIALLING-IN

Each telephone number stored in the control panel (one user can have one telephone number) can control a PG output just by dialling-in (i.e. without establishing a call). Dialling-in consists of dialling the phone number of the SIM card used in the security system and hanging up before the system answers the call. By default, the system will answer the call after the third ring (approximately 15 seconds).

WARNING: It is possible to control to the PG output only if the GSM or PSTN communicator installed in the control panel.

2.7.5 SMS MESSAGE

Sending an SMS can switch on/off a particular PG. Whether authorization is or is not demanded depends on the system configuration.

Example: **CODE_CONFIGURED TEXT**   ("_" character = space)

WARNING: It is possible to control to the PG output only if the GSM communicator installed in the control panel.

2.7.6 MyJABLOTRON

By clicking on the ON/OFF button in the "Automation" tab.

3. BLOCKING IN THE SYSTEM

3.1 BLOCKING USERS

Any user can be temporarily blocked (e.g. when a user loses a tag or his access code is revealed). When user's access is blocked the user access code or a tag will no longer be accepted by the control panel. The blocked user will also not receive any text message alerts or voice reports to a mobile phone.

Only the system administrator or service technician can block a user by choosing Settings / Users / User / Bypass and selecting "Yes" on the LCD keypad.

3.2 BLOCKING DETECTORS

A detector can be temporarily blocked in a similar way a user can be blocked. A detector is blocked when its activation is temporarily not desirable (for example a motion detector in a room with a pet or disable a siren sounding). Only the alarm function is deactivated however the system still performs diagnostics of tamper contacts and sends tamper alarm and service events.

Only the system administrator or service technician can block a detector. It can be achieved by choosing Settings / Devices / Bypass and selecting Yes on the LCD keypad. A device can be also blocked from MyJABLOTRON smartphone app in the "More/Devices" roll up menu.

WARNING: This function is limited by the selected System profile of the control panel. Always consult blocking detectors with your service technician. If the premises are guarded by a security agency, consult them as well.

4. CONTROL PANEL USER SETTINGS

4.1 CHANGING USER ACCESS CODE

Only the system administrator and the service technician can change the security codes. These changes are done after authorization on keypad by selecting Settings / Users / User / Code. To enter a new code, you must enter edit mode by pressing ENT (the line will start to flash). Now you can edit the code. The new code will be confirmed by pressing ENT again. After the changes are complete the change must be saved by selecting Save when the control panel prompts with "Save Settings?

Codes can be also changed in the MyJABLOTRON smartphone app in the "More/Change the user code" roll up menu.

4.2 CHANGING, DELETING OR ADDING AN RFID TAG

Only the administrator and the service technician can add, change or delete RFID tags from the LCD menu on the keypad. These changes are done after authorization by selecting Settings / Users / User / Access card. To enter a new RFID tag, you must enter edit mode by pressing ENT (access card line will start to flash). Then the RFID tag must be placed on to the reader (in front of keys) or the serial number under a bar code must be entered manually. After confirming by pressing ENT again, the RFID card/tag is added. To delete an access card enter "0" into the serial number field. After the changes are complete the change must be saved by selecting Save when the control panel prompts with "Save Settings?

4.3   CHANGING A PHONE NUMBER

Only the administrator and the service technician can add, change or delete telephone numbers of the users from the LCD menu on the keypad. This can be done after authorization by selecting Settings / Users / User / Phone. The user must be in edit mode to make changes. This is done by pressing ENT.
After making the changes, they must be confirmed by pressing ENT again. To delete a phone number enter "0" into the phone number field. After the changes are complete the change must be saved by selecting Save when the system prompts with "Save Settings?"

4.4   ADDING/ DELETING A USER

Only the service technician can add new users to the system (or delete them). New users can be added to the system (or deleted from it) only via the N-Link (the service technician). When creating new users, it is necessary to assign them with access permissions (rights) to individual sections and programmable outputs control with required authorization.

5. EVENT HISTORY

The security system stores all performed operations and events (setting, unsetting, alarms, faults, messages sent to users and ARCs) in the micro SD card in the system's control panel. Each entry includes the date, time (start and end), and source (cause / origin) of the event

The different ways of browsing the system's event history:

5.1   USING THE LCD KEYPAD

Accessing the event history using the keypad requires user authorization. Once authorized, the available options (based on user permissions) are displayed by choosing Event Memory. Records can be viewed from the most recent to the oldest using arrows.
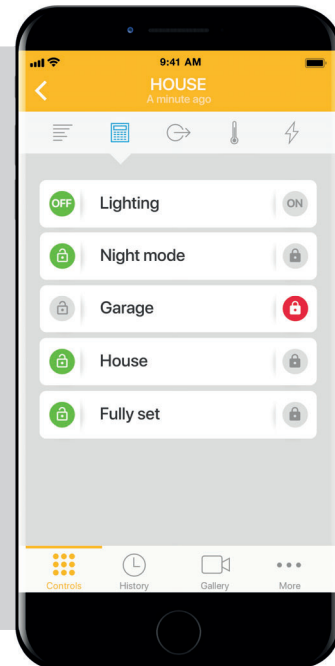
5.2   LOGGING INTO MYJABLOTRON (THE SMARTPHONE APP)

All system events can be viewed using after logging in the MyJABLOTRON smartphone app. The account shows history in a range which corresponds with the user's permissions.

MyJABLOTRON is a service which provides on-line access to JABLOTRON devices. It is intended for the end users and allows them to monitor and control the system.

MYJABLOTRON ALLOWS USERS TO:

o   View the current system status.

o   Set/unset the entire system or part of it.

o   Control programmable outputs.

o   View the event history.

o   Send reports to selected users via SMS, e-mail
     and PUSH notifications

o   Capture images from verification detectors and browse through
     them in the Photo gallery tab or directly in Recent events

o   And other useful features.

7. PERIODICAL MAINTENANCE

It is necessary to have regular and timely maintenance checks performed in order to secure reliable functioning of the system. Most of the maintenance is carried out by an installation company at least once a year during periodical maintenance inspections.

User maintenance consists of keeping the individual devices clean.

Some devices may require regular testing which is always described in the individual manual of such device (e.g. fire detectors).

PARAMETER	JA-100K
Type of installation	Fixed installation
Nominal control panel voltage / frequency / fuse	~ 230 V / 50 Hz, T200 mA fuse 250 V 5 x 20 mm ~ 115 V / 60 Hz, T400 mA fuse 250 V 5 x 20 mm
Operation voltage range	~ 195 V ÷ 250 V ~ 110 V ÷ 120 V
Electric power / current	Max 23 VA / 0.1 A
Protection class	II.
Back-up battery	12 V; 2.6 Ah max. (lead-acid)
Low battery voltage (fault indication)	≤ 11 V
Maximum battery charging time	48 ÷ 72 h
BUS voltage / max. voltage ripple (red-black)	12,0 ÷ 13,8 V DC / ± 100 mV
Max. continuous consumption from the control panel BUS +RJ	400 mA permanently (1000 mA for 5 minutes)
@ 12 hours backup (2.6 Ah)	LAN OFF: 125 mA – consumption of external modules LAN ON: 85 mA – consumption of modules
Max. number of devices	32
Alarm connection	JABLOTRON BUS – dedicated wired connection Wireless connection (with JA-111R) – unspecified wireless co-nnection, JABLOTRON wireless protocol
Alarm system classification	Security grade 2 / environmental class II
@ according to standards	EN50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN 50131-10, EN 50136-1, EN 50136-2
@ environment	Indoor general
@ operational temperature / humidity	-10 °C to +40 °C, relative humidity 75%, no condensation
@ power	Type A – primary supply with a charged backup battery
@ event history	approx. 7 million latest events, incl. date and time
@ system reaction to communication loss	Fault or tamper – according to the pre-set profile @ BUS - up to 10 s @ wireless communication - in 2 hrs (report) @ wireless communication - in 20 min block system to be set
@ reaction to invalid code entry	After 10 wrong code entries a tamper alarm is triggered and according to the selected profile it blocks all control devices for 10 min
@ ATS classification	Supported ATS classes : SP2 – SP 5, DP2 – DP3 SPT: type Z Operation type: Pass-Through Built-in LAN: SP2 – SP5 (with IP protocol) JA-190Y SP2 – SP5 (with IP protocol) JA-190X SP2 (with Contact ID protocol) LAN + JA-190Y DP2 – DP3 (with IP protocol) LAN + JA-190X DP2 (with IP / CID protocol)
@ ATS transferring protocols	JABLO IP, SIA IP, Contact ID, JABLO SMS
@ ATC protection against substitution and data protection	JABLOTRON protocol: Proprietary AES encryption with minimum 128 bit key ANSI SIA DC-09.2012 protocol with 128 bit AES encryption
LAN communicator	Ethernet interface CAT 5 (RJ-45)
Dimensions	268 x 225 x 83 (mm)
Weight	1450 g
Basic parameters of the JA-111R module	868.1 MHz, < 25 mW, GFSK < 80 kHz
Radio emissions	ETSI EN 300 220-2 (the JA-111R module)
EMC	EN 50130-4, EN 55032, ETSI EN 301 489-1, ETSI EN 301 489-3
Electric safety	EN 60950-1
Operational conditions	ERC REC 70-03, ERC DEC (98) 20
Certification body	TREZOR TEST

JABLOTRON ALARMS a.s. hereby declares that the JA-14K control panel meets the basic requirements and other relevant provisions of the EU directive no.2014/35/EU, 2014/30/EU and 2011/65/EU. You will find the original Declaration of Conformity at **www.jablotron.com**, section **Downloads**.

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

9. GLOSSARY OF TERMS

BUS / Wireless Devices:
The main hub of the security system is its control panel. It can communicate with all devices in two ways: using the BUS, i.e. using data cables within the guarded premises or part thereof; or wirelessly using radio communication. BUS devices are powered by the control panel. Wireless devices require batteries whose longevity depends on intensity of use. Some of the wireless devices are supplied by 230V from the electric grid (see the manual of the particular device).

RFID Tag
The RFID tag allows the user to operate the system and is used for contactless authorization by simply placing the tag on to the keypad reader. It replaces or complements numerical code entries. The RFID tag can be attached to a key ring.

Section
The alarm system can be divided into several smaller, independently functioning parts, called sections. Each section can have its assigned detectors, keypads, as well as sirens, users and their telephone numbers. There can be up to 4 sections per system.

Programmable Outputs PG
The security system can be used to switch on/off or control other electrical devices or appliances. This is done using programmable outputs that can be controlled by the user (an SMS message, using the keypad) or can be automated based on the system status (following the system status, alarm status, fault, etc.).

Home Automation
In addition to providing an intrusion alarm system, the JA-10 offers a number of other features. Among the most popular functions are: electrical door locks, automated light switches using motion detectors, and the remote control of appliances (heating, garage doors, gates, entry barriers, etc.).

Panic Alarm
When a user is in danger and in need of urgent assistance, the panic alarm can be triggered. The panic alarm can be set up as a designated function button on the keypad, a special code or as a specific combination of buttons on a keyfob. If connected to a security centre, triggering the panic alarm creates an immediate response (vehicle dispatch) that cannot be cancelled by phone.

Security Centre, ARC
An Alarm Receiving Centre, a continuously manned security agency (24/7/365), is able to immediately react to information received from the guarded premises and respond with an appropriate action or proceed according to internal rules.

NOTES:

NOTES: