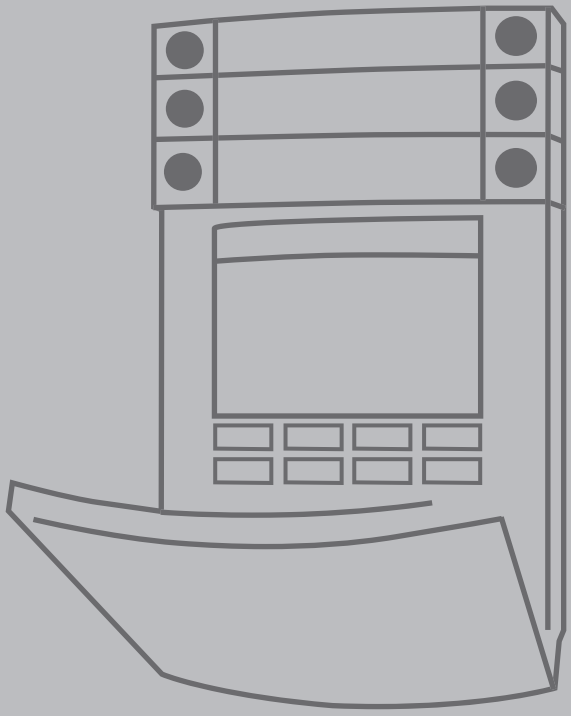
ekirja Használati Utasítás Gebruikershandleiding Bruke
de Utilizador Užívateľský návod Användarmanual Man
ti Utasítás Gebruikershandleiding Brukermanual Instru
vateľský návod Manuál Användarmanual Brugermanua
uikershandleiding Brukermanual Instrukcja użytkownik
nvändarmanual Manuál Brugermanual Käyttöohjekirja
rukermanual Instrukcja użytkownika Manual de Utiliza
l Brugermanual Käyttöohjekirja Használati Utasítás Ge
użytkownika Manual de Utilizador Užívateľský návod A
töohjekirja Használati Utasítás Gebruikershandleiding
de Utilizador Užívateľský návod Manuál Användarman

JABLOTRON 100+



EN

TABLE OF CONTENTS

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 mainly of keeping the individual devices clean. The ADMINISTRATOR of the system can switch se system to a MAINTENANCE mode in order to be able to open the detectors (change batteries) or to remove them from the installation. Consult the request to set the MAINTENANCE mode with the installation company. If the system is configured to the "EN 50131-1, grade 2" system profile, the MAINTENANCE mode is not available.

:: The system can be switched to the maintenance mode via the JA-100-Link software or from the menu of the keypad with LCD display. After authorization a "Maintenance mode" can be selected with a selection of sections where the maintenance is needed. In the maintenance mode no alarms will be triggered in the selected sections, including opening or removing the detectors from the installation.

:: The maintenance mode is indicated by the activation button flashing green (2 flashes each 2 seconds) and by the two segment buttons of the particular section lighting off.

:: When handling with the devices a care must be taken to avoid damage to the plastic and mechanisms of the detectors.

:: The cover is usually secured with a tab that needs to me slightly pushed into the detector's body with a small tool (e.g. screwdriver) and then the cover can be taken off. In some cases, the tab is secured with a small locking screw that must be unscrewed first.

:: When changing batteries in the detector, always replace all batteries in the particular detector at the same time (use batteries of the same type and from the same manufacturer).

:: Some devices may require testing (e.g. fi re detectors). For more information please contact your service technician.

1. INTRODUCTION

The JABLOTRON 100+ system is designed for up to 600 users and it can be divided into 15 individual sections. Up to 230 devices can be connected and the system offers up to 128 multi-purpose programmable outputs (e.g. home automation).

2. OPERATING THE JABLOTRON 100+ SYSTEM

The security system can be controlled in a number of different 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 Standard authorization type is used, you don't have to authorize yourself because it is possible to set the system just by pressing the right segment button on a keypad. The user name, date, and time are recorded and stored in the system memory every time the system is accessed. This information is available indefinitely. Any user can also cancel a triggered alarm (stop sirens from sounding) 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.

Users and their access rights

CODE AUTHORIZATION	TYPE DESCRIPTION
ARC code	This code has the highest level of authorization to configure the system's behavior 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, RFID tags and cards. 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 and there is no code set by the factory defaults.**
Service code (Service)	This code can enter Service mode and configure the system's behavior. It has access to all tabs with options including ARC communication unless the access is limited by the 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 users with ARC permission, other Service technicians, Administrators and other users with a lower level of authorization and assign them with access codes, RFID tags and cards. 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. The Service user is always on position 0 in the control panel and it cannot be erased.**
Administrator code (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 and assign them with access to sections and PG outputs, access codes, RFID chips and cards. This code has permission to erase the alarm memory. There can be only one main Administrator code which can't be erased. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized to confirm access for ARC and Service technicians. **By the factory defaults, the code is 1234. The main Administrator user is always on position 1 and it cannot be erased.**
Administrator code (Other)	This 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 to control sections and PG outputs, assign them with access codes, RFID tags and cards. This code has permission to erase the alarm memory in assigned sections. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized to confirm access for ARC and Service technicians. 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.**

CODE AUTHORIZATION	TYPE DESCRIPTION
User code	This code has access to sections and PG control rights assigned by an Administrator. Users can add/delete their RFID tags and access cards and change their own telephone numbers. Users can change their codes provided that the system uses Codes with prefixes. It has permission to erase the alarm memory in assigned sections. Selected users may have their access to sections limited by a schedule. **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 code	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 code	This code 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 code and are not allowed to erase the alarm memory. **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 code	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 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 to unblock the system after System blocking by alarm. A user of this code is not allowed to change it 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.**

The security of access codes, contactless RFID devices and remote controls:

A control panel enables each user to be assigned with one 4, 6 or 8-digit code and up to two RFID tags for system authorization. User authorization is required during each manipulation operation via keypad, voice menu, a computer, 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	8 DIGITS
"Code with a prefix" enabled	= $\mathbf{10^4}$ = (10.000)	= $\mathbf{10^6}$ = (1.000.000)	= $\mathbf{10^8}$ = (100.000.000)
"Code with a prefix" and **"Duress access control"** both disabled	= $\mathbf{10^4}$ – (Number of users – 1)	= $\mathbf{10^6}$ – (Number of users – 1)	= $\mathbf{10^8}$ – (Number of users – 1)
"Code with a prefix" disabled; **"Duress access control"** enabled	≤ $\mathbf{10^4}$ – ((Number of users – 1) * 3)	≤ $\mathbf{10^6}$ – ((Number of users – 1) * 3)	≤ $\mathbf{10^8}$ – ((Number of users – 1) * 3)

Control panel parameters	4 DIGITS	6 DIGITS	8 DIGITS
Using only an **RFID card** with a range of 14 characters (6 constant + 8 variable)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
"Code with a prefix" and **"Card confirmation with a code"** both enabled	= (10^8 * 10^4) = 10^{12} = (1.000.000.000.000)	= (10^8 * 10^6) = 10^{14} = (100.000.000.000.000)	= (10^8 * 10^8) = 10^{16} = 1.000.000.000.000.000)
"Code with a prefix" disabled; **"Card confirmation with a code"** enabled	= 10^8 * (10^4 – (Number of users – 1))	= 10^8 * (10^6 – (Number of users – 1))	= 10^8 * (10^8 – (Number of users – 1))

Ways to improve protection against guessing the valid code:

:: Using a code with more digits (6 or 8-digit codes),
:: More advanced types of authorization (such as "Card confirmation with a code" or "Double authorization").

Ways of operating the JABLOTRON 100+

On-site:

:: System keypad
:: System keyfob
:: Computer using a USB cable and the JA-100-Link software

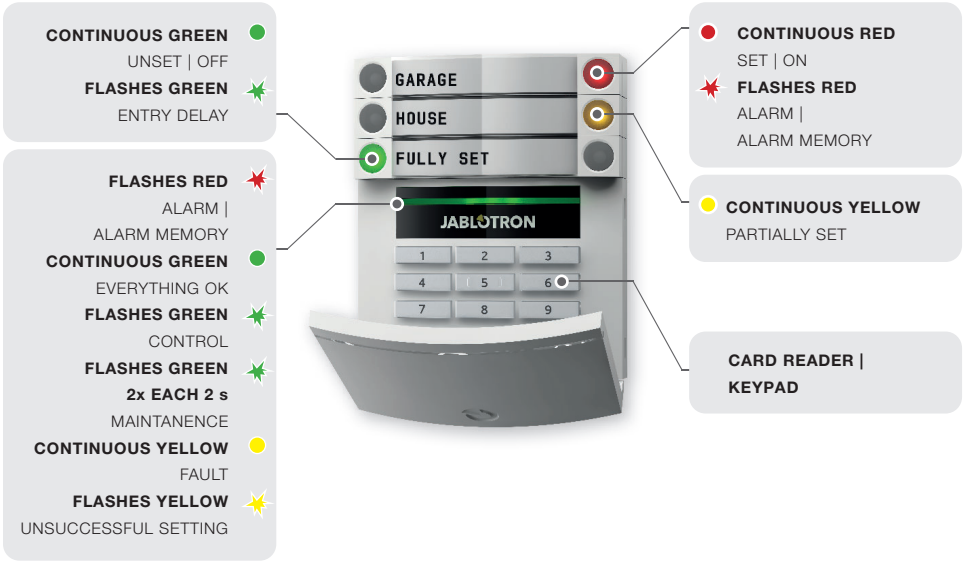
Remotely:

:: MyJABLOTRON smartphone application
:: Computer via the MyJABLOTRON web interface
:: Telephone using the voice menu
:: Telephone via SMS
:: Computer via the internet using the JA-100-Link software
:: Dialling-in from an authorized telephone number (only for operating programmable outputs)

2.1. ON-SITE OPERATING

2.1.1. USING THE SYSTEM KEYPAD

JABLOTRON 100+ system may be controlled by a variety of access modules which let you not just control but also display statuses of individual segments. The system can be operated directly (setting or unsetting the system and other automation functions) using two-button segments on the keypad. The segment buttons are clearly labelled and coloured (using traffic light logic) so that each segment status is distinctly indicated. A segment can also be used to indicate a status (e.g. opened garage door) or to control various automated devices (for example heating or window blinds). The maximum number of segments is 20 for one access module. A segment can also be set up to call for help in an emergency (medical or panic alarm).



The types of access modules and their combinations:

RFID card reader

allows control of the system using segments and user authorization using contactless method (RFID card/tag).

Keypad with a card reader

the user can control the system using segments and authorization, either by entering a code or the contactless method (RFID card/tag), or a combination of both for higher security.

Keypad with an LCD display and a card reader

the user can control the system using segments and authorization, using either a code, the contactless method (RFID card/tag), both code and card/tag for higher security, or by authorizing and using the options available on the keypad's LCD display.

When unsetting the alarm using the segment buttons,
user authorization is always required. When setting the alarm and controlling automated processes using the segment buttons, user authorization is optional for each segment.

Users can authorize
themselves by entering their assigned codes or using their RFID cards/tags. Each user can have one code and up to two RFID chips (cards or tags).

Recommended contactless chips: JABLOTRON 100+, Oasis or other third-party chips compatible with 125 kHz EM. If higher security is required the alarm system can be set up to use confirmed authorization using RFID chips and codes (optional). If the users want to control multiple segments simultaneously, they must authorize themselves and then press segments of the particular sections subsequently. This way the users can for example set the house and unset the garage within one single authorization. If the "Code with a prefix" parameter is enabled, the keypad authorization code can consist of up to eleven digits: a prefix (one to three digits), an asterisk * (which separates the prefix and main code), and a 4,6 or 8-digit code depending on configuration (for example: 123*12345678, or 1*12345678). All users can change their own codes which follow the prefix. The code can be changed from the keypad with the LCD display, the JA-100-Link software or MyJABLOTRON app.

If the "Code with a prefix" parameter is enabled, the users can be allowed to change their code.
If the "Code with a prefix" parameter is disabled, the codes can be changed only by the Administrator.

2.1.2. 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, 6 or 8-digit codes in the system.

The system can be configured to be used with prefix codes or without them (default settings). For alarm systems with a higher number of users the prefix can be enabled. To change this option, please contact the service technician of your alarm system.

Code without a prefix: CCCC

where:

cccc is a 4, 6 or 8-digit code, allowed codes are from 0000 to 99999999

Default control panel code Administrator: **1234; 123456; 12345678;**

Code with a prefix: nnn*cccc

where:

nnn is the prefix, which is the number of the user's position (position 0 to 600)
* is a separator (key *)
cccc is a 4, 6 or 8-digit code, allowed codes are from 0000 to 99999999

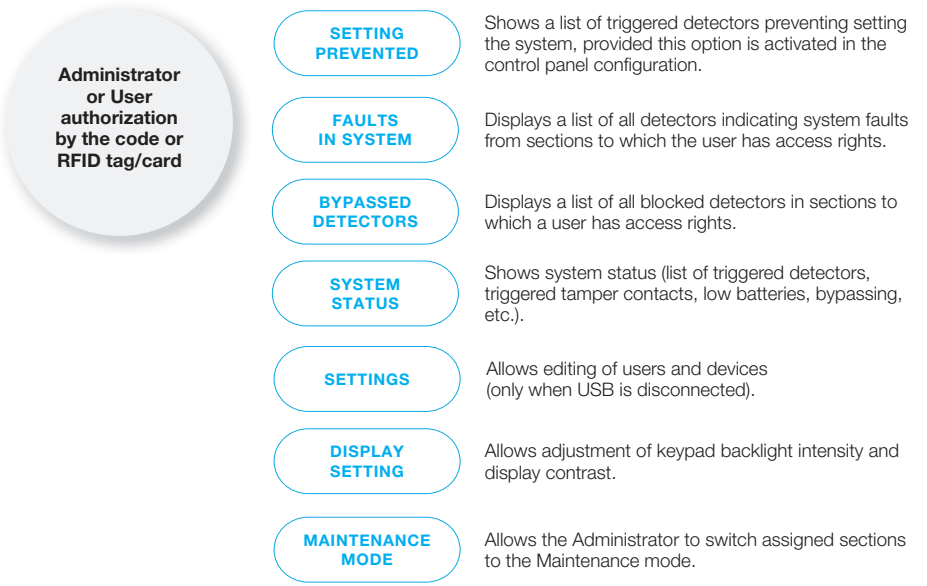
Default control panel code Administrator: **1*1234; 1*123456; 1*12345678;**

WARNING: The main Administrator code starts with the prefix **1**

The main Service code starts with the prefix **0**

To change the code type, please contact the service technician of your alarm system.

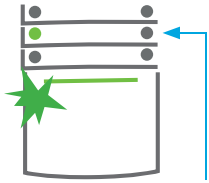
Structure and description of the internal LCD keypad menu:



2.1.2.1. ALARM SETTING

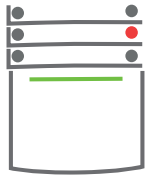
1. Authorize using the keypad.

Sections which can be controlled are lit up and the backlit indication button will start flashing green.



2. Press the right button

(the one which isn't lit up) 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 "Delayed Zone" reaction provide time to leave the guarded area during the exit delay. The segment button of the set section turns red.

While setting the alarm, if any detector is triggered (e.g. an open window) the system will react in one of the following ways (based on the system configuration):

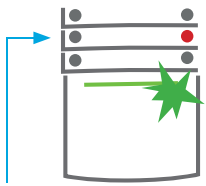
:: Detectors will guard automatically after they switch to a standby mode (default setting).
:: The system will optically indicate triggered detectors with a segment flashing red for 8 seconds and the system will set automatically once this period has expired.
:: Setting the section with triggered detectors is also possible by pressing the segment button on the right side repeatedly. This way a user confirms an intention to set the section with a triggered detector (e.g. an opened window). Otherwise the section with the triggered detector will not be set.
:: A triggered detector will prevent the section from being set. This status is optically indicated by a flashing red segment button. The detector preventing setting will be shown in the menu on the keypad's LCD display.

An unsuccessful setting is indicated by the indication button flashing yellow ("Unsuccessful setting" parameter must be enabled). Consult the installation with a service technician in order to program the desired behavior of the system.

2.1.2.2. ALARM UNSETTING

1. When you enter the building

(triggering a detector with a "Delayed zone" reaction), the system starts indicating entrance delay with a continuous tone and segment button of the section in which the delayed entrance has been triggered flashing green.

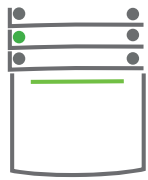


Authorize yourself using the keypad

– the green indication light of the authorization panel starts flashing.

2. Press the left segment button

of the section you want to unset.



3. The command is executed

and the segment buttons 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 such section where the entrance delay has been triggered.

2.1.2.3. DURESS ACCESS CONTROL

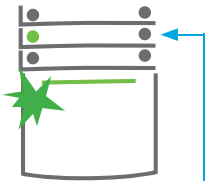
This function provides unsetting of the system in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is then reported to selected users (including ARC). Unsetting under duress is executed by adding 1 to the last number in a valid code.

Example for a code with the prefix: Valid code: 2*9999 Code for unsetting under duress: 2*9990

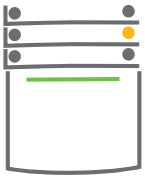
Example for a code without the prefix: Valid code: *9999 Code for unsetting under duress: 9990

2.1.2.4. PARTIAL ALARM SETTING

1. Authorize yourself using
the keypad (enter a code or hold a card or a tag up to the reader). The green backlit indication button will start flashing.



2. Press the right segment button
of the selected section.



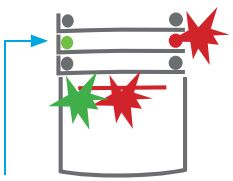
3. The command is executed,
and the segment button turns yellow to indicate a partially set section.

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 motion detectors inside a house do not react to anything.

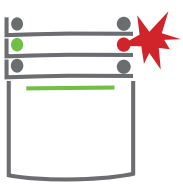
To fully set the premises in which partial setting is enabled, the button to set the system has to be pressed twice. After the button is pressed once it fl ashes yellow, when it is pressed a second time it fl ashes red. If the system is partially set – indicated by a continuous yellow light – the entire system can be fully set by authorization and pressing the yellow button. Once the button is pressed, the system will be fully set and the button turns red.

2.1.2.5. TERMINATING A TRIGGERED ALARM

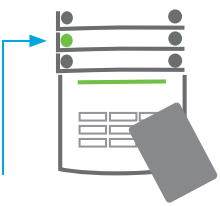
1. Authorize
yourself using the key-pad (enter a code; hold a tag up to the reader).



2. Press
the left segment button of the section where the alarm has been triggered.



3. Unsetting is finished
and sirens are silenced. The green flashing button indicates unsetting of the particular section. The red flashing light indicates alarm memory.



4. Authorize
yourself and press the green button again to cancel the alarm memory indication.

5. The segment
indicates the unset section with a continuously lit up green button.

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

If the alarm memory indication was activated during your absence, search for the cause of the alarm in the event history and be very careful when entering and checking the premises or wait until the security agency arrives (provided your system is connected to an ARC).

The segment alarm memory indication remains on until the system is set once again. Alternatively, it can be cancelled by unsetting the system one more time. Alarm indication can be also cancelled from the main menu from the keypad with an LCD display – Cancel warning indication.

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

Note: When using the "EN 50131-1, grade 2" system profile, it is always necessary to first authorize yourself and then perform the desired action.

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

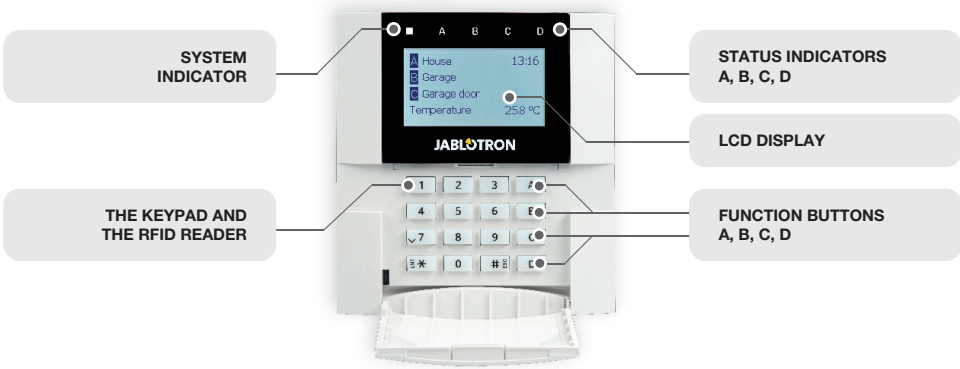
2.1.2.6. SECTION CONTROL FROM THE MENU OF THE KEYPAD WITH AN LCD DISPLAY

Statuses of sections are displayed in the left top part of the keypad's LCD display. A fully set section Is shown by a number in a rectangle filled with black colour 2; a partially set section is depicted by a framed number 4.

Control from the keypad menu:

:: Authorization by a valid code or an RFID chip.
:: Enter the menu by pressing ENTER.
:: Section Control → ENTER.
:: Select the desired section using arrows.
:: Pressing ENTER repeatedly will change between section statuses partially set / set / unset.
:: Press ESC to exit the menu.

2.1.3. USING THE JA-110E AND JA-150E SYSTEM KEYPADS



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 colorfully backlit in order to clearly indicate the section status.

:: GREEN – Unset :: YELLOW – Partially Unset :: RED – Set

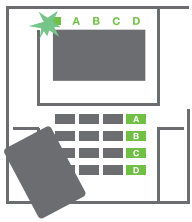
Authorization can be done by entering an access code on the keypad or using an RFID card/tag assigned to a particular user. Each user can have one code and one RFID chip (a card or a tag). If the users want to control multiple sections simultaneously, they must authorize themselves and then press function buttons of the particular sections subsequently. This way the users 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/card

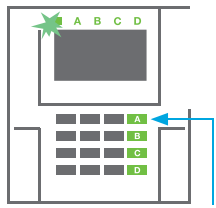
CANCEL WARNING INDICATION	Allows you to cancel alarm/unsuccessful setting indication in all sections to which the user has access rights.
SECTION CONTROL	Allows you to control the system's sections to which the user has access rights and are enabled in the internal settings.
PG CONTROL	Allows the user to control PG programmable outputs depending on the user's permissions and according to 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.
FAULTS IN SYSTEM	Displays a list of all detectors indicating system faults from sections to which the user has access rights.
BYPASSED DETECTORS	Displays a list of all blocked detectors in sections to which a 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.
MAINTENANCE MODE	Allows the Administrator to switch assigned sections to the Maintenance mode.

2.1.3.1. ALARM SETTING



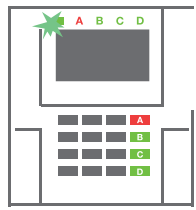
1. Authorize yourself using

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

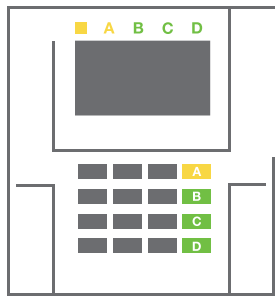
and the keypad acoustically indicates the exit delay. The section is set now, only the detectors with a "Delayed Zone" reaction provide time to leave the guarded area during the Exit delay. The status indicator and a function button of the set section will turn red.

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 "Delayed zone alarm" 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).

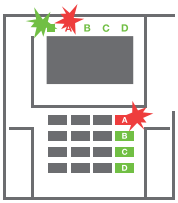


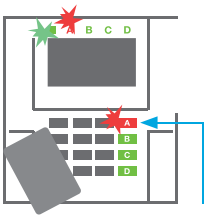
If the control panel is configured to be set without authorization then it is not necessary to authorize yourself. All you have to do is press a function button of a particular section. It is also possible to configure the control panel to be set simply by authorization.

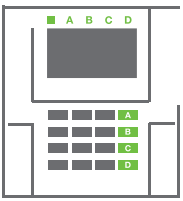
WARNING: Setting without authorization automatically lowers the maximum security level to Grade 1. Consider all possible risks related to using this function.

Consult the installation with a project consultant or a service technician in order to program the desired behavior of the alarm system.

2.1.3.2. ALARM UNSETTING







1. When you enter the building

(triggering a detector with a "Delayed zone" 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.

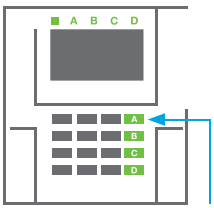
Consult the installation with a service technician in order to program the desired behavior of the system.

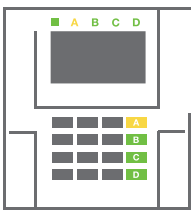
2.1.3.3. PARTIAL ALARM SETTING

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 card or 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.

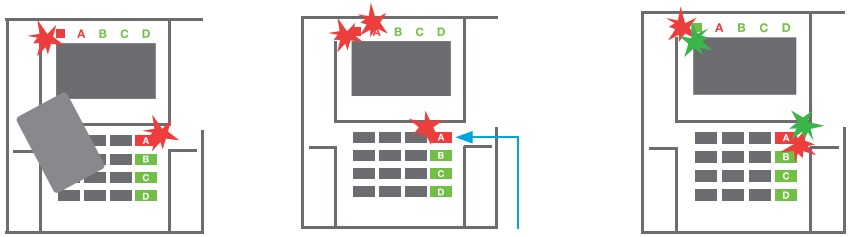
2.1.3.4. DURESS ACCESS CONTROL

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

2.1.3.5. 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.

2.1.4. OPERATING THE SYSTEM WITH A KEYFOB

Keyfobs must be enrolled into the system by the installer. The keyfob can be linked to specific users, which will prevent SMS text message notification to the user who is interacting with the system at the moment (if notification parameters are set up in this way). The keyfob can provide either bi-directional communication, confirming the execution of a command with a colored indicator light, or one-way without any confirmation. Keyfobs control and indicate battery status and are equipped with optical and acoustic indication.

BI-DIRECTIONAL KEYFOB

The button functions are differentiated by lock icons. The closed lock icon sets programmed sections; the opened lock icon unsets them. Correct command execution is confirmed by an LED light; unsetting – green, setting – red. A communication fault (out of the control panel's range) is indicated by a yellow LED light flashing once. 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 impulse or change functions are 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 or one PG status output (e.g. turn the lights on and off), alternatively two PG outputs (e.g. a garage door and door lock).

If the system is configured to Set after confirmation the detector will indicate unsuccessful setting with a green LED light if a device is triggered. It is necessary to confirm setting by pressing the lock button again. A set section will be confirmed by a red LED light.

The keyfob buttons can be blocked to prevent accidental pressing. A command will be sent out when a button is pressed repeatedly. A low battery is indicated acoustically (with 3 beeps) and optically with a yellow flashing LED after pressing a button.

For more information, consult configuration of the remote control with your service technician.

ONE-WAY KEYFOBS

One-way keyfobs send a signal every time a button is pressed without receiving feedback from the control panel. Sending a signal is confirmed only by a short fl ash of the red LED and alternatively with a beep.

2.2. REMOTE OPERATING

The highest comfort for remote operating and management of the system is provided by the MyJABLOTRON service. The MyJABLOTRON web interface is a unique service which allows on-line access to JABLOTRON devices. It allows end-users to monitor and control the system. It is available in a form of a smartphone app and as a web application. The MyJABLOTRON service allows users to:

:: View the current system status,
:: Set/unset the entire system or a part of it,
:: Control programmable outputs,
:: View the event history,
:: Send reports to selected users via SMS, e-mail or PUSH notifications,
:: Capture images from photo verification devices and browse through them in the Photo gallery tab or directly in Recent events,
:: Monitor current temperature or energy consumption, including a history overview on graphic charts,
:: And other useful features.

Depending on your country or region, a web account in MyJABLOTRON can be set up by an authorized JABLOTRON partner. The login name is the user e-mail address. The password for the first log in will be sent to this address. The password can be changed anytime in the user settings.

2.2.1. OPERATING THE SYSTEM USING THE MyJABLOTRON SMARTPHONE APP

Once a user account is created, the user can remotely monitor and control the system via the MyJABLOTRON app for Android and iOS smartphones.

2.2.2. OPERATING THE SYSTEM VIA THE MyJABLOTRON WEB INTERFACE

The JABLOTRON 100+ system can be easily and conveniently operated using your computer via the internet and the MyJABLOTRON web interface, which is accessible from **www.myjablotron.com**.

2.2.3. OPERATING THE SYSTEM USING THE VOICE MENU

The system can be controlled from a phone through a voice menu, which guides the user through a series of options in the preconfigured language. To access the voice menu, you just dial the alarm system's phone number.

Access to the voice menu can be enabled either to all telephone numbers without restrictions or alternatively 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.

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

2.2.4. OPERATING THE SYSTEM USING SMS COMMANDS

SMS commands can control individual sections and programmable outputs just like keypad segment 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.

CODE_SET_2_4

The commands to control the programmable outputs can be programmed by a system installer. For example, you may choose BLINDS DOWN as your command to close the blinds on your windows. It is also possible to configure the system not to require a code before a command. In such case the command is simply automatically identified when the system recognizes the user's phone number from which the SMS was sent. Configuration is done by a service technician.

2.2.5. OPERATING THE SYSTEM REMOTELY USING A COMPUTER (JA-100-LINK)

The JABLOTRON 100+ system can be operated remotely using a computer with an installed JA-100-Link software. It can be downloaded from the **www.myjablotron.com** website.

2.2.6. CONTROLLING THE PROGRAMMABLE OUTPUTS (PG)

2.2.6.1. KEYPAD SEGMENT

A PG output switches on by pressing the right button of the segment and switches off by pressing the left button. If the output is configured as a pulse output, it is switched off according to the pre-set time. PG control may or may not be stored in the control panel's event memory. Configuration is done by a service technician.

Authorization is/is not demanded based on the system configuration.

2.2.6.2. USER KEYPAD AUTHORIZATION

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

2.2.6.3. FROM THE MENU OF THE KEYPAD WITH AN LCD DISPLAY

After user authorization the programmable outputs can be controlled from the menu of the keypad with an LCD display. The user has access to programmable outputs depending on the user's permissions.

Control from the keypad menu:

:: Authorization by a valid code or an RFID chip.
:: Enter the menu by pressing ENTER.
:: PG Control → ENTER.
:: Select the desired PG group using arrows (1–32), (33–64), (65–96), (97–128) → ENTER.
:: Select the desired PG using arrows → ENTER.
:: Pressing ENTER repeatedly will change the PG statuses (active PG is shown by a PG number in a rectangle fi lled with black colour.
:: Press ESC to exit the menu.

2.2.6.4. REMOTE CONTROL

By pressing an assigned button of a remote control. Bi-directional remote controls confirm activation of PG outputs with an LED indicator.

2.2.6.5. MyJABLOTRON SMARTPHONE APP

By tapping on ON/OFF in the Automation (PG) tab.

2.2.6.6. MyJABLOTRON WEB INTERFACE

By clicking on ON/OFF in the Automation (PG) tab.

2.2.6.7. DIALLING-IN

Each telephone number stored in the system (one user can have one telephone number) can control one PG 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).

2.2.6.8. SMS MESSAGE

Sending an SMS can switch on/off a particular PG. Authorization is/is not demanded based on the system configuration.

Example: CODE_CONFIGURED TEXT

3. BLOCKING/DISABLING IN THE SYSTEM

3.1. BLOCKING USERS

Any user can be temporarily blocked (e.g. when a user loses a card/tag or his access code is revealed). When user's access is blocked their ID code or card/tag will no longer be accepted by the system. The users will also not receive any SMS alerts or voice reports to their phone.

Only the system administrator or service technician can block a user. One method of taking away access rights is by choosing Settings / Users / User / Bypass and selecting "Yes" on the LCD keypad. Another option is to locally or remotely block a user through the JA-100-Link software by clicking on the user in the Settings / Users / User blocking column.

A blocked (disabled) user will be marked with a red circle until the blocking is cancelled.

3.2. BLOCKING DETECTORS

A detector can be temporarily blocked in a similar way a user can be disabled. 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). The system still performs diagnostics of tamper contacts and sends service events however the alarm function is deactivated.

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. Another option is to use the JA-100-Link software by clicking on the detector in the Settings / Diagnostics / Disabled column. A blocked detector is marked with a yellow circle until it is turned back on using the same procedure. A device can be also blocked from MyJABLOTRON smartphone app.

3.3. DISABLING TIMERS

To temporarily disable automated scheduled events in the system, a timer can be disabled. Disabling a scheduled event (e.g. unsetting the system from night guarding at a predetermined time) will prevent execution of that event (e.g. while on vacation).

A timer can be disabled locally or remotely through the JA-100-Link software by clicking on the section in the Settings / Calendar / Blocked column. A disabled timer is marked with a red circle until it is turned back on using the same procedure.

4. CUSTOMIZING THE SYSTEM

4.1. CHANGING A USER ACCESS CODE

If the system is set up without prefixed codes, only the system administrator and the service technician can change the security codes. The system administrator can make changes from both the LCD keypad menu the JA-100-Link software and MyJABLOTRON smartphone app. The code can be changed after authorization by selecting Settings / Users / User / Code. To input a new code, you must enter edit mode (the code will start flashing) by pressing Enter, enter the new code and confirm by pressing Enter again. After completing the changes, they must be confirmed by choosing Save when the system prompts you with "Save Settings?".

If the system is set up with prefix codes, individual users can be allowed to change their codes from the LCD menu on the keypad.

4.2. CHANGING, DELETING OR ADDING AN RFID CARD/TAG

If the system is set up with prefixed codes, users can add, change or delete their RFID tags or cards from the LCD menu on the keypad. These changes are done after authorization by selecting Settings / Users / User / Access card 1 (or 2). To enter a new RFID card/tag, you must enter edit mode (access card 1 or 2 will start to fl ash) by pressing Enter. Then the RFID card/tag must be placed on to the reader or the serial number must be manually entered. After confirming by pressing Enter 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 system prompts with Save Settings?

The system administrator and the service technician can add, change and delete RFID cards/tags from both the LCD keypad menu and the JA-100-Link software.

4.3. CHANGING A USERNAME OR PHONE NUMBER

If the system is set up with prefix codes, users can add, change or delete their telephone numbers or change their name from the LCD menu on the keypad. This can be done after authorization by electing Settings / Users / User / Phone. The user must be in edit mode to make changes. This is done by pressing Enter. After making the changes, they must be confirmed by pressing Enter 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?”.

The system administrator and the service technician can add, modify or delete a user phone number or change a user name from both the LCD keypad menu and the JA-100-Link software.

4.4. ADDING/DELETING A USER

Only the system administrator or 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 through the JA-100-Link software, or the F-Link software in the case of a service technician.

When creating a new user, it is necessary to assign him with access permissions (rights), sections the user may operate, programmable outputs he may control, and what type of authorization will be required.

4.5. CALENDAR EVENTS SET UP

It is possible to configure calendar events (unsetting / setting / partial setting, controlling or blocking PG outputs).

The calendar events can be set up via the JA-100-Link software in the Calendar tab.

For each calendar event, action, section or PG output and event time can be set. Day can be defined by a day of week, month or year. For the selected day you can set up to 4 times to perform an action or to set repeating at regular intervals.

Therefore, calendar events can be customized not only for sections control but also for controlling various technologies in the object using PG outputs.

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 through 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 using arrows.

5.2. USING THE JA-100-LINK SOFTWARE AND A COMPUTER

The system memory can be browsed using the JA-100-Link software. Events can be downloaded from the control panel in small (about 1,200 events) or larger (about 4,000 events) batches. The events can be filtered in detail, colour-coded for easier orientation, or saved into a fi le in a computer.

5.3. LOGGING INTO MyJABLOTRON (WEB/SMARTPHONE)

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

6. TECHNICAL SPECIFICATIONS

PARAMETER	JA-103K	JA-103K-7 Ah	JA-107K
Control panel power supply	~ 110–230 V/50–60 Hz, max. 0.28 A with fuse F1.6 A/250 V, Protection class II	~ 110–230 V/50–60 Hz, max. 0.28 A with fuse F1.6 A/250 V, Protection class II	~ 110–230 V/50–60 Hz, max. 0.85 A with fuse F1.6 A/250 V, Protection class II
Back-up battery	12 V; 2,6 Ah (lead gel)	12 V; 7 Ah (lead gel)	12 V; 7 to 18 Ah (lead gel)
Maximum battery charging time	48 h	48 h	48 h
BUS voltage (red - black)	12,0 to 13,8 V	12,0 to 13,8 V	12,0 to 13,8 V
Maximum continuous current consumption from the control panel	1000 mA	1000 mA	2000 mA permanent 3000 mA for 60 minutes (max. 2000 mA for one BUS)
Max. continuous current consumption for back-up 12 hours	JA-103K – 2.6 Ah back-up battery	JA-103K – 7 Ah back-up battery	JA-107K – 18 Ah back-up battery
	Without GSM communicator: LAN – OFF: 115 mA; LAN – ON: 88 mA	Without GSM communicator: LAN – OFF: 334 mA; LAN – ON: 300 mA	Without GSM communicator: LAN – OFF: 1135 mA; LAN – ON: 1107 mA
	With GSM communicator: LAN – OFF: 80 mA; LAN – ON: 53 mA	With GSM communicator: LAN – OFF: 302 mA; LAN – ON: 270 mA	With GSM communicator: LAN – OFF: 1100 mA; LAN – ON: 1072 mA
Max. continuous current consumption for back-up 24 hours	Without GSM communicator: LAN – OFF: 21 mA	Without GSM communicator: LAN – OFF: 160 mA; LAN – ON: 125 mA	Without GSM communicator: LAN – OFF: 535 mA; LAN – ON: 499 mA
	With GSM communicator: LAN – OFF: 17 mA	With GSM communicator: LAN – OFF: 128 mA; LAN – ON: 110 mA	With GSM communicator: LAN – OFF: 530 mA; LAN – ON: 494 mA
Maximum number of devices	50	50	230
LAN communicator	Ethernet interface, 10/100BASE	Ethernet interface, 10/100BASE	Ethernet interface, 10/100BASE
Dimensions	268 x 225 x 83 mm	357 x 297 x 105 mm	357 x 297 x 105 mm

PARAMETER	JA-103K	JA-103K-7 Ah	JA-107K
Weight with/without AKU	1844 g/970 g	3755 g/1665 g	7027 g/1809 g
Reaction to invalid code entry	Alarm after 10 wrong code entries		
Event memory	Approx. 7 million latest events, including date and time		
Power supply unit	Type A according to EN 50131-6 T 031 note: In case of a main power failure is the system backed up for 24 hours and at the same time is a failure report sent to the ARC.		
Classification	Security grade 2 according to EN 50131-1		
Operational environment	Environmental class II (indoor general) according to EN 50131-1		
Operational temp. range	-10 °C to +40 °C		
Average operational humidity	75 % RH, non-condensing		
Complies with	EN 50131-1 ed. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 ed. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN IEC 63000		
Radio operating frequency (with the JA 11xR module)	868.1 MHz		
Radio emissions	ETSI EN 300 220-1,-2 (module R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)		
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7		
Safety conformity	EN IEC 62368-1		
Caller identification (CLIP)	ETSI EN 300 089		
Operational conditions	ERC REC 70-03		
Certification body	Trezor Test s.r.o. (no. 3025)		

Note: The parameters may differ if you use another type of control panel.

JABLOTRON a.s. hereby declares that the control panels JA-103K, JA-103K-7Ah and JA-107K are in a compliance with the relevant European Union harmonisation legislation: Directives No: 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU, when used as intended.
The original of the conformity assessment can be found www.jablotron.com – Downloads section.

Note: Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling. Please return the product to the dealer or contact your local authority for further details of your nearest designated collection point.

www.jablotron.com