The JA-107K, JA-103K and JA-103K-7 Ah Control Panels of the JABLOTRON Security System

A control panel is a fundamental part of the JABLOTRON series alarm system and is designed to protect small, medium or large premises and complies with security grade 2 requirements. The control panel has BUS and/or wireless device (when the system is equipped with a radio module) compatibility. It is recommended that only JABLOTRON devices are used with the system. Proper functionality cannot be guaranteed when using third party devices.

Caution: The JABLOTRON security system can only be installed by a trained technician with a valid certificate issued by an authorized distributor.

The manual is intended for trained technicians.

Some features described in this manual require the installation of additional communicators:

- ***Voice menu for remote control, ringing control, voice reports, ringing reports, special reports, SMS reports, SMS control, GPDS communication – The JA-19xY-ZZZZ GSM communicator.***

Contents

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

1 Basic description and definitions

Modular architecture – allows the system to be configured for specific installations, sizes and user needs.

Firmware (FW) update – procedure for uploading a new FW version into the system containing new functions, improvements and adaptations. We recommend you check that FW is up-to-date during any installation as well as during regular service checks. Besides the control panel FW, it is necessary to update FW in all devices if required (keypads, radio modules, motion detectors with a camera etc...).

Access module (keypad) – is the basic modular element of a control keypad and its task is to identify users. The simplest version only contains a reader of contactless RFID tags/cards. A version with a keypad and an LCD display is also available. Access modules are produced both in a BUS and in a wireless version. Each access module contains one control segment (expandable to 20 segments per device). There is also an RFID card reader and a keypad with a built-in RFID card reader for outdoor use in our product portfolio.

Control segment – is a modular element of an indoor control keypad. A segment has 2 buttons (left = OFF, right = ON). By installing the required number of segments to an access module you can create a keypad that will fulfil all required functions. The segments clearly indicate the system status and enable its intuitive operation. The installed segments allow the user to clearly see what functions are provided by the system (rather than being hidden inside the menu only) and what access rights the user has assigned.

Control keypad – consists of an access module and control segments.

Alarm types – the system is able to react to intrusion, panic, tamper, fire, gas leak and water flooding. The use of suitable detectors makes it possible to report other dangers as well (somebody moving in the garden, handling of a guarded object, high temperature, risk of freezing etc.). To reduce the occurrence of false alarms the detectors' reaction can be set in way that their activation must be confirmed (the same detector must be activated repeatedly or confirmation by another detector).

Visual verification of an alarm – photo verification devices (camera detectors, photo verification cameras) are able to automatically take and send photos or video sequences corresponding to events in the system.

Personal protection – in case of a robbery, health problem or fire the user can call for assistance (pressing the button on a keypad, entering a panic code, by activating a panic button or using a wireless remote control).

Duress access control – serves for triggering a silent alarm by authorization only, or by system control (setting, unsetting, PG control, …) when a user is threatened (in the presence of a criminal). A panic alarm is triggered during system control when a code is entered with 1 mathematically added to the last digit of the code.

Delayed panic – a function for triggering a panic alarm with a time delay during which the alarm can be cancelled. The function is designed for users afraid of opening the entrance door to an unknown visitor, who may attack them. Thus, the user activates delayed panic before opening the door and if he/she is sure that he/she is safe, he/she must cancel the function before expiration of the pre-set delay time. The panic delay time can be set in the specific device's internal settings used for triggering the panic alarm (keypad segment, panic button, etc.).

Event reporting – reporting of all events to an Alarm Receiving Centre (ARC) may ensure timely intervention of professionals. The reports are sent to the ARC via the built-in LAN communicator. After installing the GSM communicator the reports can also be directly sent to users by means of SMS messages or voice calls.

Special reports – are SMS messages or voice calls. Their meaning can be sent independently of other functions. Sending a report can be linked to activation of a device. This way, the status of other devices or technologies with an error output can be monitored etc.

Remote control – authorized users may make a phone call to the system and use a voice menu to control or check the setting status. Statuses of individual sections can be remotely controlled by means of defined SMS commands. SMS commands can also be used to switch programmable PG outputs ON and OFF. They can also be activated by simply ringing (without establishing a call) from authorized phone numbers. There is the F-link software meant for service technicians for remotely management of the system. For the system administrator a software is also available called JA-100-Link with limited functions. The system can be also remotely controlled via web service at www.myjablotron.com or also by smartphone application.

MyJABLOTRON – a unique service that provides online access to JABLOTRON devices. It is designed for both end users and installation technicians. A **JABLOTRON Security SIM card** is required in order to use the MyJABLOTRON service. For more information about the registration of control panels and service availability in your country please contact your distributor.

Users' access rights – defines the user authorization access level. You can modify user access rights to which part of the protected premises and also which programmable PG outputs the user can control. The users prove their identity by applying their RFID tag or entering their code using a keypad. The system allows you to individually set a time restriction to disable the access of selected users to guarded sections.

Administrator – a required number of administrators can be defined in the system, they can assign access rights to standard users. Different sections in the building may have different administrators. In the default setting there is one main (master) administrator of the system, who is always authorized to access to all section, PG outputs and set access rights for all users (default code 1234).

Service technician – there can be more than one authorized service technician to manage the system (default code 1010). With this code the technician is authorized to adjust all features of the system. The access of a service technician may be conditional on the administrator's approval by the authorisation. A special case of service authorization is a technician of the ARC. This technician can use his code to lock the access to settings of the parameters of communication with the Alarm Receiving Centre.

F-Link (JA-100-Link) – to program the system, a computer with a Windows operating system is required. The control panel can be connected to the computer locally using a USB cable or remotely from a computer connected to the Internet (in this case some functions of program are not available e.g. language change or update FW of control panel). All features are set using the computer and the F-Link software. This software is exclusively designed for trained technicians. Access to it cannot be granted to an administrator or end user of the system. For this purpose, a simplified version of this software (JA-100-Link) is designed, which gives system administrators access to some settings (user management, diagnostics, setting of calendar actions, reading the event history).

Service mode – is the mode in which complete configuration of the system can be modified. Only a service technician (or an ARC technician) can enter the system into service mode. This can be done by using the F-Link software while locally or remotely connected control panel to the PC (with a USB cable or via the Internet). In the SERVICE mode the system is completely out of operation and the PG outputs are switched off (it does not guard and does not provide any user functions, e.g. control of programmable PG outputs). The SERVICE mode is indicated by the keypad system indicator flashing yellow (2 x each 2 seconds).

Maintenance mode – is the mode meant primarily for Administrator. It allows to perform a maintenance (e.g. changing batteries) in the section (sections) according to the Administrator's access rights. The system can be switched to the maintenance mode by Administrator using the keypad or the JA-100-Link software (the Service technician can enter the Maintenance mode using the F-Link software). The maintenance mode in one section does not affect the status and functionality of other sections or the status of programmable PG outputs. The Service technician may restrict the Administrator access to the Maintenance mode in the Parameters tab in the F-Link. The MAINTENANCE mode is indicated by the keypad system indicator flashing green (2 x each 2 seconds) and by the segment buttons of the particular section lighting off.

Day / night mode – the control panel allows you to set a different behaviour for day and night time. For example, a different keypad backlight intensity, PG output activation according to day/night (blocking lights during the day), etc. The day/night can be switched by a selected device (e.g. twilight switch) or by sunrise and sunset time according to the astronomical calendar. For this option, it is necessary to set the coordinates of the location where the system is installed.

Control of appliances – the system has programmable PG outputs that can be used to switch various devices ON and OFF. PG outputs represent a logic programmed in the system that controls required output modules (system devices). An output can be controlled using the keypad segments, by activation of detectors, remote controls, by an event in the system (e.g. setting a section, alarm triggering…), by a calendar action, using an SMS command, by ringing from an authorized user or through the MyJABLOTRON application. Activation of a PG output can also be blocked by a status of a section, by detector or by other PG. Activation and deactivation of an output can be reported to users using an SMS or to the MyJABLOTRON service by data transfer (push notifications).

Door lock control – an electric door lock (connected to a PG output) can be opened by applying a tag or entering of a code using a keypad. Each user can be assigned to a door he / she is authorized to open. An output can be blocked by a set section so there is no danger of somebody entering an area if it is guarded (set). Opening of a door by user authorization can be recorded in the system event history.

Calendar – using the calendar you can program automatic calendar actions – guarding (setting / partial setting / unsetting) of sections and control of PG programmable outputs (activation / deactivation, blocking / unblocking). Each action can be set to a day and a month in which it is performed. There can be up to 4 times or repeats in set intervals for the selected day. The yearly schedule can be used to set deviations from the weekly schedule (e.g. public holidays, personal holidays).

BUS devices – are connected to the system using a BUS cable (4-wire). The BUS ensures power supply as well as communication. BUS devices (detectors, keypads, sirens etc.) require enrollment to a position (address) in the system for their function. However, there are also devices that are only connected and work without being enrolled on a position (some PG output modules, status indicators, BUS isolators etc.).

Wireless devices – to ensure communication, the control panel must be equipped with a radio module and the wireless devices (detectors, keypads, sirens etc.) must be enrolled to a position (address) in the system. However, there may also be devices in the system that do not occupy system positions (they are used for reception only and do not report to the control panel), e.g. modules of PG outputs. To cover the area of a larger site up to 3 radio

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

modules can be installed in the system (connected with a BUS cable). The control panel regularly checks the activity of selected wireless devices (the Supervision parameter) and also checks current state of batteries. If communication with a wireless device is lost, the control panel indicates communication fault. Radio modules check RF jamming / interference on the JABLOTRON system communication band. If the band is jammed, the system triggers a Fault.

Intrusion detectors – a group of detectors designed to identify the intruder. It includes detectors of motion, opening, glass breaking, tilt or shock detectors. The detectors are set to a desired reaction to its triggering (activation). It determines how the detector is going to react to its activation. Fire, gas, flood or panic reaction detectors do not belong to the group of intrusion detectors.

GSM communicator – can be installed to the control panel as a supplementary module and provides connection to a mobile phone network and the Internet. Thus, the system may transmit data to the alarm receiving centre (ARC). The communicator provides remote access to the control panel with the use of the F-Link (JA-100-Link) software, reporting events to users, remote control of the system.

LAN communicator – is included in the control panel and it provides connection to the Internet. It allows fast remote access by F-Link and JA-100-Link software and it can also transmit data to an alarm receiving centre (ARC) that is equipped with reception technology for the JABLOTRON protocol. In the control panel settings, you can select which communication type will be primary and which will be used as a backup.

Section – a system can be split into parts (sections) which can be set and unset independently. A section may also be a separate apartment in an apartment building, a store in a shopping mall or department in a company or an office building. Section interdependency can be set in the way it reminds you it is protected by your own control panel (access rights, reports, displaying things on the keypad, acoustic indication, the MyJABLOTRON service…).

Common section – is a separate section designed to be a superior section for a selected group of other sections. When the last subsection is set, the common section is then set automatically. When a first subsection is unset then the common section is unset as well. The purpose is to secure areas such as halls, toilets, kitchens in companies, etc. We do not recommend to directly control the common section.

Common segment – is a function of a keypad segment, that allows you to control multiple sections simultaneously with only one segment. These sections must be set to separate segments on the particular keypad. Each keypad can have up to two segments with the common segment function and therefore to control two different groups of sections.

Partial set – is adjustable for each section separately. If partial set is on, the system does not react to intrusion detectors with the parameter “internal” set (i.e. monitor the indoor space). Thus, for example movement is allowed in the residential part of the house, but the system triggers an alarm or entrance delay when there is entry through a door or motion in a garage, cellar, etc. If a section is set completely, it reacts to activation of all detectors that are assigned to it.

Bypass – active status of devices or a fault present in the system is confirmed during system setting. The status of active inputs is ignored after a bypass until they go to stand-by (deactivated). When inputs go to standby (are deactivated) they are included with guarding. By bypassing system faults the user confirms that it has been recognized, but it doesn’t change its status (a fault is still present in the system). The function depends on the option given by the parameter Ways of setting.

Blocking – it blocks an active device input to activate a PG output or to perform any reaction activation. Perform blocking manually by an LCD keypad, JA-100-Link or F-Link or via the MyJABLOTRON app. This way it is possible to block a device input anytime and not only during the setting procedure. The function depends on the option given by the parameter Ways of setting.

Autobypass – automatic bypass of the system reaction to a device according to options. Input activation after 3x activations or 3x alarms (optional). Faults after 3rd fault triggered.

Disabling – this option serves for temporarily manual disabling selected sections, devices, users, programmable outputs (PG) or calendar actions. The section to which the control panel is assigned cannot by disabled and this is true for the Service code at position 0 and Administrator’s code at position 1 too. For devices we distinguish Blocking (it is only about input activation), disabling the device at all and tamper alarm detection, for more information see chapter 9.16 Disabling and blocking options.

Ways of setting – selection of the level of the system setting procedure. Options are from the lowest level where the system doesn’t check anything (always sets) up to the highest level where the system doesn’t allow you to set if any device is activated (for example an open window), see chapter 9.11 Obstacles preventing setting the system.

Event history – the system records occurring events in its memory. The contents of the memory can be viewed from the F-Link (JA-100-Link) software, from an LCD keypad or from the MyJABLOTRON app. The beginning of an event is usually registered as Activation (status of a device, fault, tampering etc.) and the end of an event as Deactivation. Statuses of sections are registered as Set / Unset, alarm statuses as Alarm / Alarm expiration, Alarm silencing or Alarm Cancellation.

ID	Time	Source	Section	Event	Channel
2172	1/21/2022 1:14:56 PM	Detector 6: Device 6	1: Section 1	Delay activation	6: Device 6
2173	1/21/2022 1:14:59 PM	Detector 6: Device 6	1: Section 1	Delay deactivation	6: Device 6
2174	1/21/2022 1:15:00 PM	Detector 6: Device 6	1: Section 1	Delayed alarm	0: Control panel
2175	1/21/2022 1:15:59 PM	Detector 0: Control panel	1: Section 1	Alarm expired	0: Control panel

Magnet activation and deactivation

Alarm Beginning and End

Some events may only have an activation record (e.g. New Picture, Panic Alarm, Configuration changed).

MicroSD memory card – the control panel uses a microSD card as a memory medium. After connecting the control panel to a PC using a USB cable two drives will be displayed in the File Manager. FLEXI_CFG and FLEXI_LOG. The capacity of supplied card can be up to 4GB (SD / SD-HC). Before using a brand new SD card perform the control panel reset to get default settings see chapter 12 Reset of the control panel. And then perform upgrade firmware, see chapter 11.13 Firmware updates This procedure saves all required files (default texts, voices, etc..) to the SD card.

FLEXI_CFG – with hidden directories and files that contain system settings. Do not alter the contents of the drive, there is a risk of loss of functionality of the system. This drive also contains the JA-100-Link directory with the JA-100-Link.exe software, which may be run and used by the System Administrator.

FLEXI_LOG – contains the PHOTO directory and the FLEXILOG.TXT file, where all system events are recorded. Selected data from the file can be viewed in F-Link / Event History. The PHOTO directory is used to store image files that have been sent to the control panel from camera devices (e.g. from motion detectors with a camera). Both file types (txt and jpg) are stored in an encrypted form and their contents cannot be normally viewed with text and picture viewers. PHOTO content can only be viewed if the F-Link (JA-100-Link) software is also run in the PC at the same time and the authorization level Service or Administrator is confirmed by entering of the respective code. Events are recorded in the FLEXILOG.TXT file up to the size of 10 MB, then the file is renamed to FLEXILOG.OLD and a new file is created.

SIMLock – a function of the control panel that can be activated by the respective ARC on registration of the control panel to MyJABLOTRON. If this function is activated, then after replacement of the used SIM card with another one the system will automatically delete the ARC setting (the registration of the system to MyJABLOTRON will have to be renewed). This step is used to prevent undesired transmission of information to the ARC from a different card than the one that was registered for it and from which the setting was done.

1.1 Basic system configuration requirements

Mind the requirements of the valid norms when designing the system. The JA-107K / JA-103K / JA-103K-7Ah control panels can be set to have behaviour according to a pre-set **System profile** to comply with all the following conditions (profiles):

1. Default – Factory pre-set profile, all system parameters are optional.
2. EN50131-1, Grade 2 – Profile pre-sets some specific system parameters (valid for control panel, keypads, sirens etc.) according to the given norm requirements valid for security grade 2. The parameters can't be changed.
3. INCERT, Grade 2 – Profile pre-sets some specific system parameters (valid for control panel, keypads, sirens etc.) according to the given norm requirements valid for security grade 2. The parameters can't be changed.

In relation to alarm reporting, valid for security grade 2, the control panel has to be installed according to one of following configurations as a minimum:

– At least one siren with a backup battery (e.g. JA-111A or JA-163A RB) and a LAN* communicator or a GSM communicator.
– Two independent communicators, for instance LAN* + GSM communicators.

***Caution:** Ensure that all LAN devices providing connection to the Internet network have their power backed up!*

During system designing it is necessary to take into account splitting into sections and pre-set entrance delays to be able to set the definition of delay zones. There can be 3 kinds of delayed zones (Delay A, Delay B and Delay C), each of them has its own timer to pre-set entrance and exit times.

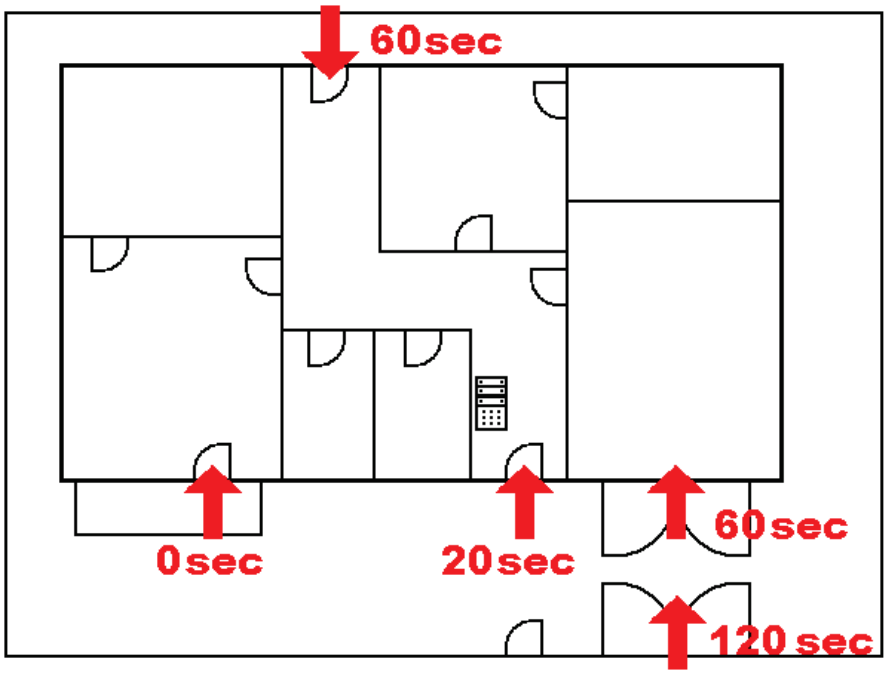
Example: A typical family house with a garage with a perimeter protected by outdoor detectors:

The main gate or entrance gate and also the main door are protected by a magnetic contact. The garage door and rear door as well. The whole building with perimeter and garage is protected by one section only and the system keypad is placed at the entrance hall*.

*It is recommended to use multiple keypads always near the entrance door to protected premises and ensure that the state of the system and the entered code cannot be recognized by a potential trespasser.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Position and name of the detector	Reaction	Entrance time	Exit time
1.Magnetic contact – Main gate outdoors	Delay C	120 s	360 s
2.Movement detector – Outdoor movement	Delay C	120 s	360 s
3.Magnetic contact – Garage door	Delay B	60 s	120 s
4.Magnetic contact – Rear door	Delay B	60 s	120 s
5.Movement detector – PIR garage	Next delay (Delay B)	60 s	120 s
6.Magnetic contact – Main door	Delay A	20 s	60 s
7.Movement detector – PIR hall	Next delay (Delay A)	20 s	60 s
9.Magnetic contact – Balcony door	Instant	0 s	0 s
9.Movement detector – PIR room	Instant	0 s	0 s



Variant 1:

- Entrance to the protected premises (system is SET) through the main door triggers Delay A (**20 s**) and the system starts counting time for unsetting the system (entrance delay).
- Entering a valid code on the keypad and pressing the green button on the keypad segment is a system unset. When authorisation and unsetting of the system is not performed during the entrance delay then an alarm from the delay zone will be triggered (Delay A).

Variant 2:

- Entrance to the protected premises (system is SET) through the rear door or garage door triggers Delay B (**60 s**) and the system starts counting time for unsetting the system (entrance delay).
- Next detected movement by detectors with a Delay A reaction shortens the entrance delay according to Delay A (20 s) if the delay is shorter than Delay B.
- Entering a valid code on the keypad and pressing the green button on the keypad segment is a system unset. When authorisation and unsetting of the system is not performed during the entrance delay then an alarm from the delay zone will be triggered – from the zone in which the time expires first (Delay A, Delay B).

Variant 3:

- Entrance to the protected premises (system is SET) by activation of any outdoor detectors (Main gate opening, entrance gate or outdoor PIR activation) triggers the Delay C zone entrance time (**120 s**) and the system starts counting the time for unsetting the system (entrance delay).
- On opening the garage door and activation of a magnetic detector the system starts counting the Delay B time (60 s) and it shortens the time of the Delay C zone already activated (if delay C is not shorter than Delay B).
- Going through the Main door activates the Delay A time (20 s) and it shortens the entrance time (if delay B or delay C are not shorter than delay A).

– Entering a valid code on the keypad and pressing the green button on the keypad segment is a system unset. When authorisation and unsetting the system is not performed during the entrance delay then an alarm from the delay zone will be triggered - from the zone in which the time expires first (Delay A, delay B, delay C).

1.2 Access codes and their default settings

Authorization is necessary by a valid (4, 6 or 8-digit) code or by applying the RFID card or tag to the authorization module (keypad) to be able to operate the system (setting, unsetting or to check the status of some section or device). According to the authorization level of the specific user the system shows you all information and allows system control appropriate to your access rights.

The authorization to control the system with a keypad or to use F-Link (JA-100-Link) software, the MyJABLOTRON application or the voice menu must be performed by entering a numeric code. The code can be entered with a prefix or without a prefix (default setting).

Enter a code without a prefix in the following format:

cccc

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

The control panel is delivered with 2 default codes:

Default codes without a prefix	4-digit	6-digit	8-digit
Service	1010	101010	10101010
Administrator	1234	123456	12345678

*The default codes are filled in automatically by the F-Link software, so from the first activation until a code change the software does not request them. However, for security reasons immediately after installation is finished, it is imperative to change all default codes. If both codes are not changed, when the Service mode is exited an SMS is sent to the service phone number, reporting **"Warning, default codes, Section 1"** (it can be cancelled in the Parameters "Default codes warning").*

For systems with a higher number of users the prefix can be enabled. With the prefix enabled, users can change their codes themselves from the LCD keypad. The prefix can be enabled in the Initial setup tab in F-Link.

Enter a code with a prefix in the following format:

ppp*cccc

where: **ppp** is the sequential number (position **0 to 600**) of the user (called a prefix)

***** is a separator (* key)

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

In that case the Service and Administrator codes are set as follows:

Default codes with a prefix	4-digit	6-digit	8-digit
Service	0*1010	0*101010	0*10101010
Administrator	1*1234	1*123456	1*12345678

Caution: *The **service code** has to always begin with a prefix **0.***
*The **administrator code** has to always begin with a prefix **1.***

Warning: *When the Prefix is disabled, the codes will always be changed to the default values and all other codes are erased (all access RFID cards / tags remain). When the Prefix is enabled, all the codes and cards / tags will remain set and the prefixes will only be added.*

1.2.1 Change of access codes

When the option "Code with prefix" is enabled then the control panel allows the arbitrary digit combination of a 4 – 8-digit code for every user (they can even have the same code with a different prefix). Every user with a "User" authorization and the checked parameter "Code change allowed" has an option to edit his own code.

Access codes can be changed by:

– LCD keypad (PC has to be disconnected from the control panel, no remote or local connection).

- JA-100-Link (user) software available in the control panel disk unit (it appears when you connect a USB cable) or F-Link (service technician) software which can be downloaded from MyCOMPANY.
- MyJABLOTRON smartphone application (from version 3.5).

When the option “Code with a prefix” is disabled then the control panel allows the combination of a 4 – 8-digit code for every user, but the control panel restricts using the same code value for another user which has already been used in the system. Only system Administrator(s) is/are fully responsible for editing already existing user codes and assigning new codes.

Access codes can only be changed by an Administrator:

- LCD keypad (PC has to be disconnected from the control panel, no remote or local connection).
- JA-100-Link (administrator) software available in the control panel disk unit (it appears when you connect a USB cable) or F-Link (service technician) software which can be downloaded from MyCOMPANY.
- MyJABLOTRON smartphone application (version 3.5 and higher).

1.2.2 Security access codes and RFID devices

The control panel allows you to assign one 4, 6 or 8-digit code and up to two RFID tags to every user to be authorised. Authorisation is required when the system is operated with a keypad, voice menu, by PC, web or smart app. The security level is adequate for this fact and it can be represented by numbers.

Calculating code combinations according to 1 user is shown in the following examples:

Control panel parameters	4-digit	6-digit	8-digit
“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”** disabled	= $\mathbf{10^4}$ – (no. of users in the system – 1)	= $\mathbf{10^6}$ – (no. of users in the system – 1)	= $\mathbf{10^8}$ – (no. of users in the system – 1)
“Code with a prefix” disabled and **“Duress access control”** enabled	≤ $\mathbf{10^4}$ - ((no. of users in the system – 1) * 3)	≤ $\mathbf{10^6}$ - ((no. of users in the system – 1) * 3)	≤ $\mathbf{10^8}$ - ((no. of users in the system – 1) * 3)
Using an **RFID card** with 14 characters only (6 fixed + 8 variable)	=$\mathbf{10^8}$ = (100,000,000)	=$\mathbf{10^8}$ = (100,000,000)	=$\mathbf{10^8}$ = (100,000,000)
“Code with prefix” and **“Card confirmation with a code”** enabled	= ($\mathbf{10^8}$ * $\mathbf{10^4}$) = $\mathbf{10^{12}}$ = (1,000,000,000,000)	= ($\mathbf{10^8}$ * $\mathbf{10^6}$) = $\mathbf{10^{14}}$ = (100,000,000,000,000)	= ($\mathbf{10^8}$ * $\mathbf{10^8}$) = $\mathbf{10^{16}}$ = (1,000,000,000,000,000)
“Code with a prefix” disabled and **“Card confirmation with a code”** enabled	= $\mathbf{10^8}$ * ($\mathbf{10^4}$ – (no. of users in the system – 1))	= $\mathbf{10^8}$ * ($\mathbf{10^6}$ – (no. of users in the system – 1))	= $\mathbf{10^8}$ * ($\mathbf{10^8}$ – (no. of users in the system – 1))

Example: Using a standard 4-digit access code with an enabled function called “Codes with a prefix” it reaches 104 (10.000) code combinations for every user. The number of combinations is reduced by disabling prefixes and with increasing the number of users. It also depends on the “Duress access control” parameter because it adds one more code to each user.

A solution to how to reduce the risk of code breaking can be the following:
- Using 6 or 8-digit code(s).
- Select a higher level of authorization such as “Card confirmation with a code” or “Double authorization”.
- Using JABLOTRON contactless RFID cards / tags (JA-19xJ).

The control panel counts the attempts at wrongly entered codes and if the **10th attempt** is reached, the system triggers the tamper event “Code breaking attempt” and reports this event to predefined numbers. No additional blocking of entering other codes into the system is applied. After a valid code entry, the counter of wrongly entered codes is reset and the triggered alarm terminated. This counter is pre-set to 10 attempts and it cannot be changed.

1.2.3 Regular system check (maintenance)

The whole security system requires periodical testing of its correct functioning and that of all its parts but also cleaning, external visual checks (dust and dirt, usually performed by the system user) and internally (spider webs, insects, battery status, etc… performed by service technician). Some specific parts of the system are able to perform a self-test and a possible fault report to the control panel and it informs about this status according to the settings. Almost all maintenance steps are required to be done by a service technician during the annual system check.

The main backup battery is tested periodically a few times per minute by the control panel using a load test. Wireless device batteries (in detectors, keypads, sirens, remote controls) are automatically tested with every periodical test transmission. The system reports a low battery from every enrolled device from the moment when it appears until its replacement on the LCD keypad, eventually also via a pre-set SMS report. Replacement of the batteries can be performed by a service technician in a Service mode or by an administrator in a Maintenance mode. When a battery is removed it is necessary to wait a few moments (at least 20 s) for discharging any internal capacitors and then insert a new battery.

Overview of recommended maintenance / function control:

Device type	Description	Who does the action	Frequency of the action
Fire detectors	Test of functions; inform the ARC agency before you proceed!	Administrator	Once per month
	Clean up the dust and dirt.	Administrator	Once per year
	Battery check (BUS and wireless devices).	Service technician	Once per year
Panic buttons	Test of functions; inform the ARC agency before you proceed!	Administrator	Once per month
	Battery check, measuring the voltage, physical state.	Service technician	Once per year
Detectors	Clean up the dust and dirt.	Administrator	Once per year
	Test of functions; test of RF range for wireless detectors. For detectors with a built-in camera test by taking a picture.	Service technician	Once per year
	Battery check, measuring the voltage of every battery, physical state, etc.	Service technician	Once per year
Keypads	Clean up the dust and dirt.	Administrator	Once per year
	Test every button, segments and RFID sensor; test the RF range for wireless keypads.	Service technician	Once per year
	Battery status check and their physical state, measuring the voltage of every battery, etc.	Service technician	Once per year
Sirens	Clean up the dust and dirt, insects, check water penetration to PCB, etc.	Service technician	Once per year
	Test of functions; test the RF range for wireless sirens.	Service technician	Once per year
	Check batteries or backup batteries, measuring, physical state, measuring the voltage of every battery, etc.	Service technician	Once per year
Remote controls (RC)	Test of functions; RF range, low batt indication check. Cleaning up or plastic housing replacement.	Administrator or Service technician	Once per year
Alarm state	Test of communication to ARC, voice calls and SMS reporting.	Administrator or service technician	Once per year
Backup battery in the control panel	Test during mains (AC) disconnection and measuring the voltage of a backup battery after 5 minutes of no mains power.	Service technician	Once per year
Programmable outputs (PG)	Test of functions; RF range of wireless modules.	Service technician	Once per year

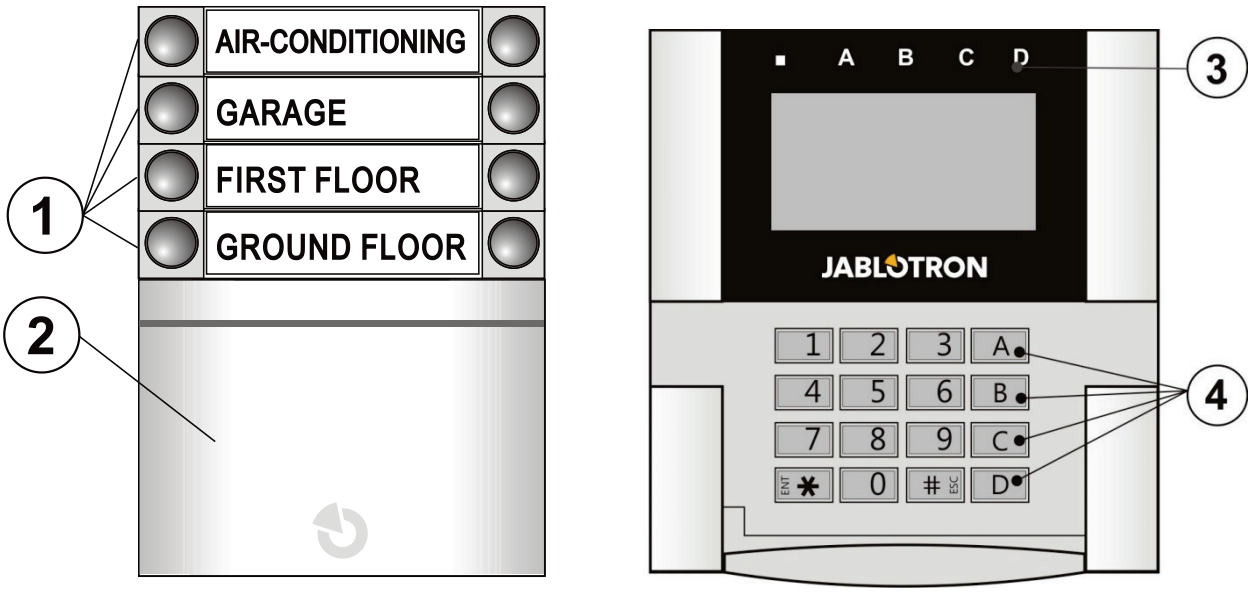
All operations are recommended by the manufacturer but are not superior to local regulations.

2 System size

The system range can be set regarding the premises size and user needs.

2.1 External size

The external size of the system as seen by its users can be defined by the access module (segment keypad) assembly. The JA-110E/JA-150E keypads have 4 functional buttons and it cannot be changed. They can be set for controlling of sections and PG outputs.



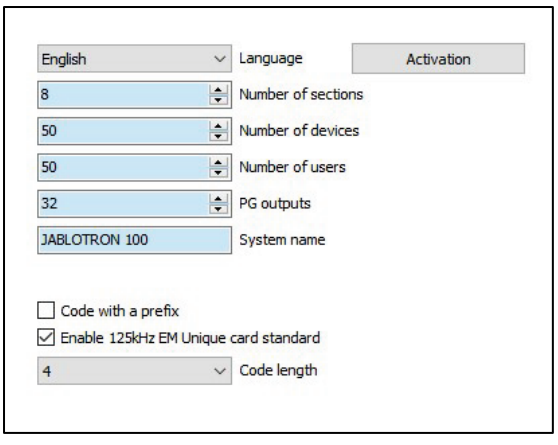
1 – Control segments; 2 – Access module; 3 – Section indicators; 4 – Functional buttons

A keypad can have up to 20 **control segments**. Each segment has two buttons (OFF – on the left and ON – on the right). A segment is used to control a section (Set / Unset), to control appliances or to call assistance. A segment can also be used to indicate the status of a section or PG output (it can indicate the active status both with a red LED as standard and with a green LED – "Inverted indication" segment function). For instance, on the keypad it is possible to monitor and indicate segment activation/deactivation of a magnetic detector installed on a door if it is open or closed. It can be pre-set as a "Common Segment" for simultaneous control of more sections.

An **access module** verifies authorization of users. The authorization method is determined by the module selection (RFID card/tag reader, keypad + RFID reader, keypad with an LCD display + RFID reader). The module also enables opening of a door-lock by application of a card/tag (code entry). Modules are available in a wireless and BUS version. Functions apply to both.

Configuration of the control keyboard is described in chapter 10.5.1 Keypad configuration.

2.2 Internal size (system range)

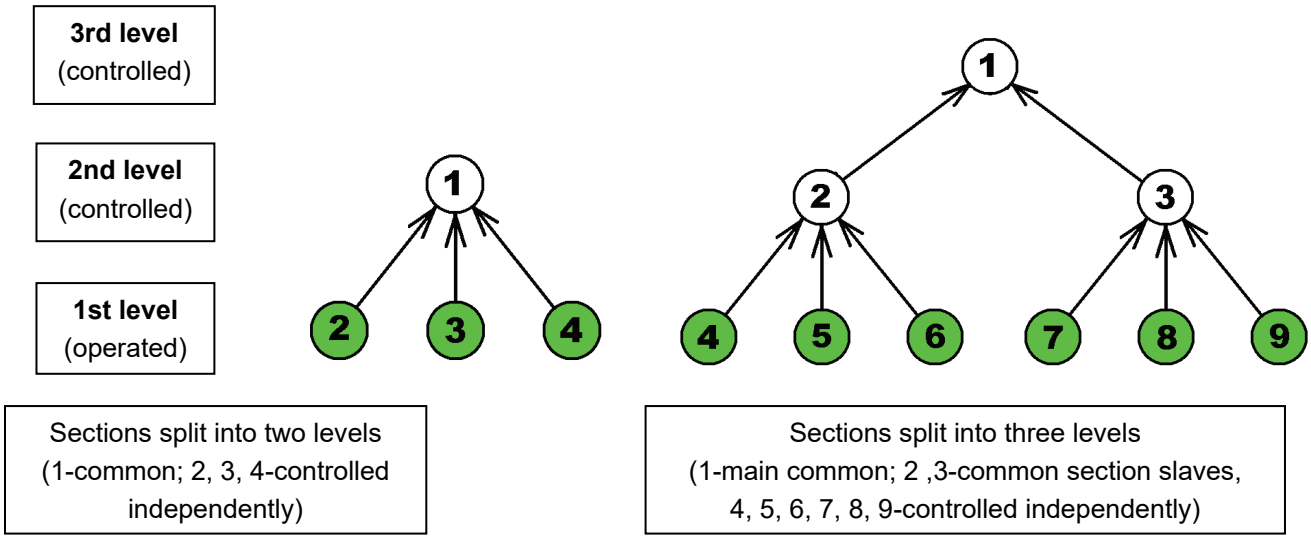


The control panel can be split into 15 sections (independently adjustable parts). Every device has its own address (keypads, detectors, sirens) and has to be enrolled to a section. Each user can have set an authorisation to access required sections only. The number of sections is set using the F-Link software, Initial setup tab. It makes programming more organised. Their quantity can be increased or reduced (unless links are made that would make it impossible to reduce the number of sections).

The number of devices, sections, users and programmable outputs is set using the F-Link software. You can create a system both for a small apartment with one section and some devices and for a large building making the most of the JABLOTRON system with independently controlled sections. A section can be linked to other sections to control them and their statuses in common.

2.2.2 Configuration and splitting

The JA-103K security system control panel is meant to be used for protecting small premises. The JA-103K–7Ah is suitable for medium premises. And large premises, the JA-107K system is more suitable; thanks to its range, dimensions and number of sections it offers a great variability to fit the given installation. A section is a part of the system to which devices related to a protected area are assigned. Small premises may have one basic section (flat, small family house) and in this case all devices are assigned to the same section. Medium systems can have multiple sections (for instance flats in a block of flats, company building) and also its own 2nd level common section (common hall, cellars, etc.). Larger premises can have many more sections (offices), 2nd level common sections (for instance such as multi-storey buildings) and common premises like reception or a lobby as a 3rd level common section (see the picture). Very important for operation of such systems is setting the users authorisation to the lowest control level of the sections they have assigned. Not for 2nd and 3rd levels of common sections. When all sections assigned to the 2nd or 3rd level of common section are set then every common section is set automatically and automatically unset if at least one of the basic sections is unset. Users can only control 1st level sections. See the following figure:



It is recommended for higher levels of common premises (2nd and 3rd level) to use keypads with a specific number of segments equal to the sections used, to determine which section is set / unset after entering the protected premises.

For 1st level keypads it is quite enough to equip them with control segment(s) assigned to a specific section(s).

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

3 Types of control panels, utility parameters

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	Note
Maximum number of devices	50	50	230	JA-107K
Maximum number of users	50	50	600	Max. 120 wireless devices on positions 1 – 120 and max. 60 devices per 1 BUS terminal
Maximum number of independent sections (Partitions)	8	8	15	
Maximum number of programmable outputs	32	32	128	
GSM / GPRS communicator	No	No	No	Only PGs 1 – 32 can be used for wireless transmission
IP LAN (Ethernet) communicator	Yes	Yes	Yes	The JA-19xY supplementary GSM module
Maximum number of radio modules	3	3	3	
SMS reports	Up to 8 users	Up to 8 users	Up to 50 users	5 reports per 1 event
Voice reports	Up to 8 users	Up to 8 users	Up to 15 users	5 reports per 1 event
Recommended 12 V backup battery	2,6 Ah	≤ 7 Ah	7 to 18 Ah	
Maximum possible short-term current consumption	1000 mA	1000 mA	2000 mA permanent 3000 mA for 60 min. (max. 2000 mA for one BUS)	
BUS terminals	BUS 1 + 4 pin connector (I-BUS) for radio module	BUS 1 + 4 pin connector (I-BUS) for radio module	BUS 1, BUS 2 + 4 pin connector (BUS 3) for radio module or the JA-110Z-D splitter	The JA-107K terminals are isolated, i.e. short-circuiting of one branch does not have any influence on the other branch.
Maximum BUS cable length	500 m	500 m	3 x 500 m	Can be extended using the JA-110T or JA-120Z modules.

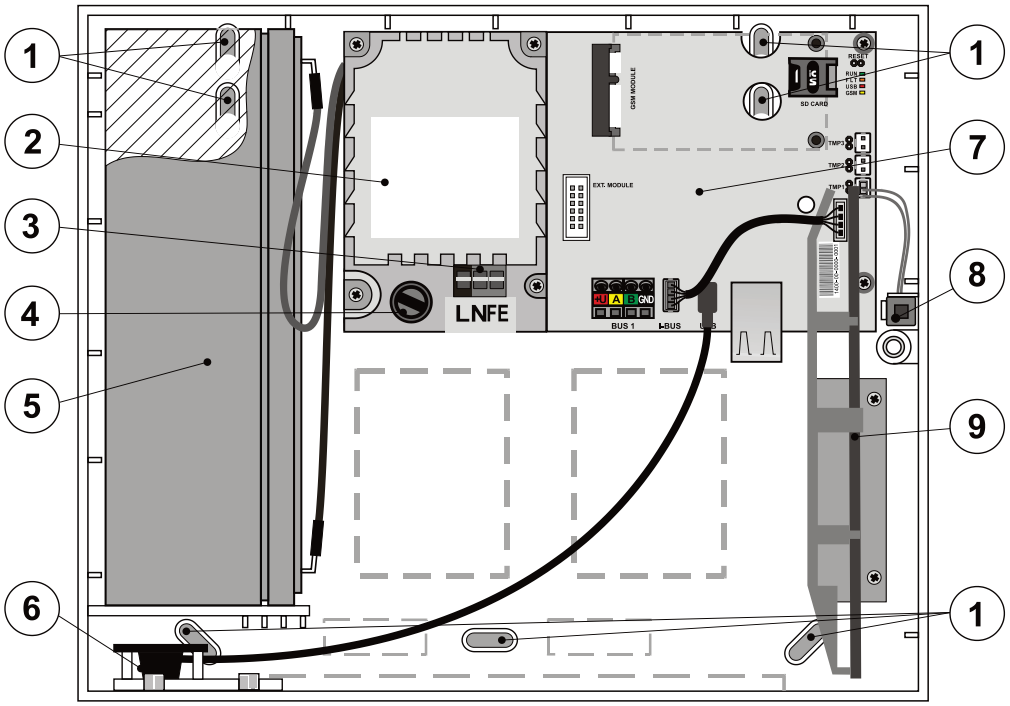
	JA-103K – akumulátor 2,6 Ah		JA-103K-7Ah – akumulátor 7 Ah		JA-107K – akumulátor 18 Ah	
Maximum continuous current consumption for 12-hours backup supply	Without GSM communicator	LAN – OFF: 115 mA LAN – ON: 88 mA	Without GSM communicator	LAN – OFF: 328 mA LAN – ON: 304 mA	Without GSM communicator	LAN – OFF: 1135 mA LAN – ON: 1107 mA
	Without GSM communicator	LAN – OFF: 80 mA LAN – ON: 53 mA	Without GSM communicator	LAN – OFF: 296 mA LAN – ON: 272 mA	With GSM communicator	LAN – OFF: 1100 mA LAN – ON: 1072 mA
Maximum continuous current consumption for 24-hours backup supply	Without GSM communicator	LAN – OFF: 21 mA	Without GSM communicator	LAN – OFF: 136 mA LAN – ON: 112 mA	Without GSM communicator	LAN – OFF: 535 mA LAN – ON: 499 mA
	Without GSM communicator	LAN – OFF: 17 mA	Without GSM communicator	LAN – OFF: 104 mA LAN – ON: 80 mA	With GSM communicator	LAN – OFF: 530 mA LAN – ON: 494 mA

3.1 Description of the JA-103K control panel

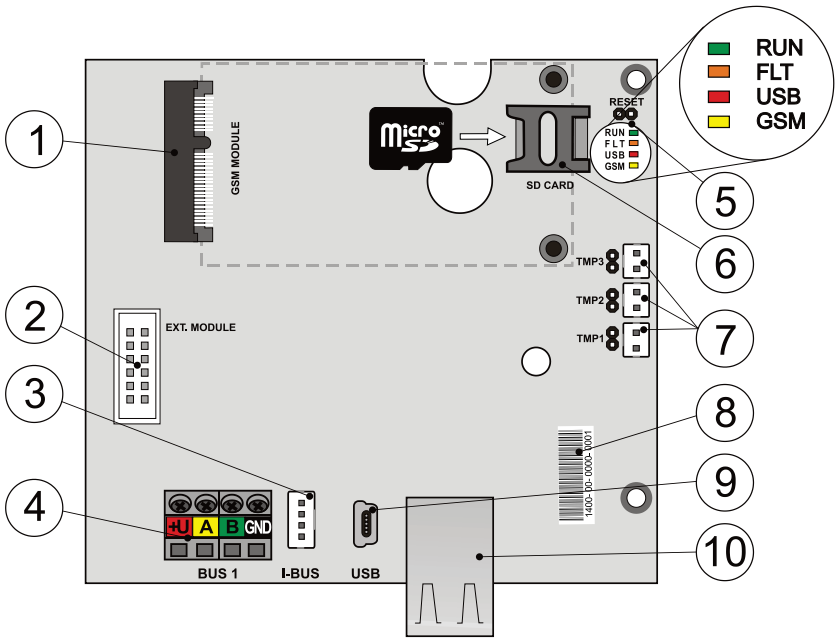
The JA-103K control panel is designed for **small BUS systems** (limited by the output of the power supply) and for **medium-sized systems** with wireless communication. The control panel is equipped with a LAN communicator which can be connected to the Internet and with the ability to send data to servers (images taken by photo verification devices), JABLOTRON Cloud services or to the server of security agencies with technical equipment for this data to be received. When connected to the Internet via the LAN communicator remote access is also possible using the F-Link (JA-100-Link) software.

The control panel can be expanded with additional communicator:

The JA-19xY – GSM communicator for GSM/GPRS or LTE communication. It allows communication with ARC, Jablotron Cloud Services and remote connection via SW F-Link / JA-100-Link



1 – Wall mounting holes; 2 – Power supply module; 3 – Mains power terminals; 4 – Mains fuse; 5 – Backup battery; 6 - USB connector for PC connection; 7 – Control panel PCB; 8 – Housing tamper contact; 9 – The JA-11xR radio module holder



1 - GSM communicator connector; 2 – Connector for additional modules; 3 – BUS terminal for the JA-11xR internal radio module; 4 – BUS terminals; 5 – LED indicators and RESET jumper; 6 – MicroSD card holder; 7 – Connectors of the housing tamper contacts, 8 – Production code; 9 - MiniUSB connector; 10 – LAN connector

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Parts of the JA-103K control panel (changeable parts) are:

– MicroSD card

To extend control panel options use:

– The JA-11xR radio module
– The JA-19xY-zzzz GSM communicator

Control panel accessories include:

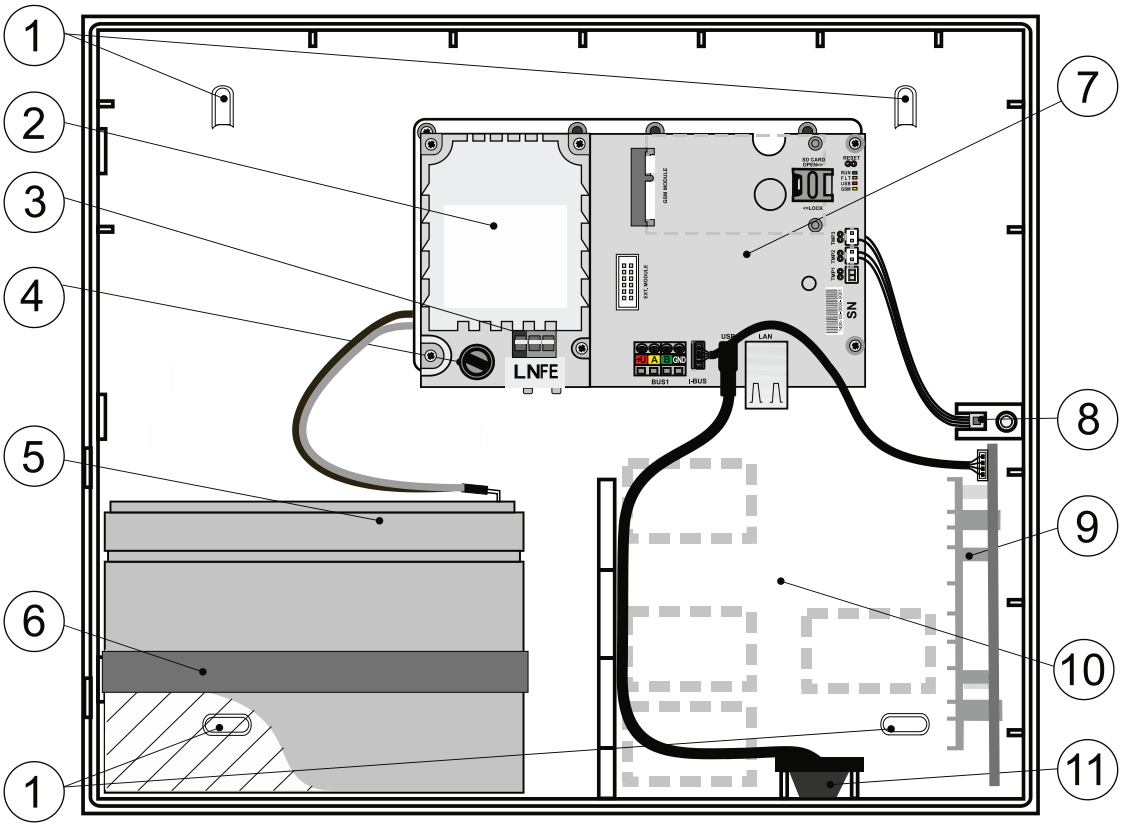
– 1pc USB cable (180 cm)
– 1pc Connection cable for the JA-11xR radio module
– 1pc Extension USB cable (20 cm) installed in the control panel
– 1pc Fuse T 1.6 A; 250 V
– 4pcs Jumpers (for jumper pins connection)
– 6pcs Warning stickers
– 4pcs Fasteners 8 mm
– 4pcs Screws 40 mm
– 3pcs Ties 100 mm
– Drilling template A4
– CZ / EN Installation manual (short version)

3.2 Description of the JA-103K 7Ah control panel

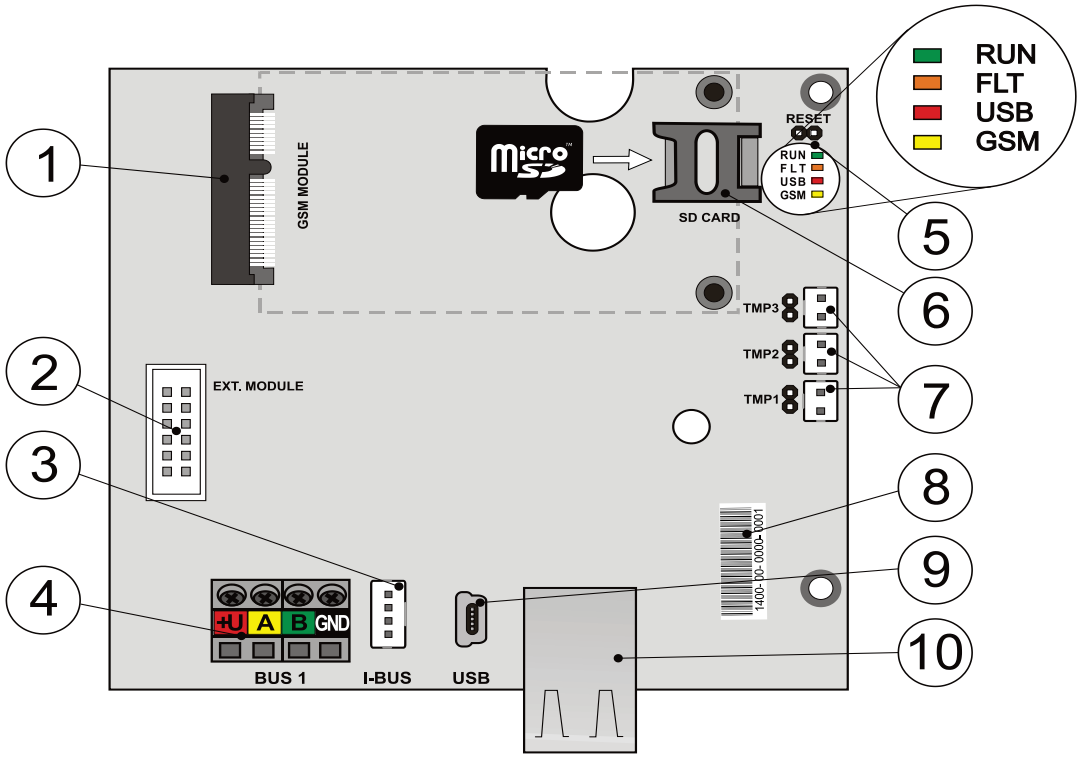
The JA-103K-7Ah control panel is designed for medium-sized and large installations, both BUS and wireless systems. The control panel is equipped with a LAN communicator which can be connected to the Internet and with the ability to send data to servers (images taken by photo verification devices) or to the server of security agencies with technical equipment for this data to be received. When connected to the Internet via the LAN communicator remote access is also possible using the F-Link (JA-100-Link) software.

The control panel can be expanded with additional communicator:

The JA-19xY-zzzz – GSM communicator for GSM/GPRS or LTE communication. It allows communication with ARC, Jablotron Cloud Services and remote connection via SW F-Link / JA-100-Link



1 – Wall mounting holes; 2 – Power supply unit; 3 – Mains power terminals; 4 – Mains fuse; 5 – Backup battery; 6 – Attachment strap of the backup battery; 7 – Control panel PCB; 8 – Housing tamper contact; 9 – The JA-11xR radio module holder; 10 – Cabling space; 11 – USB connector for PC connection



1 – GSM communicator connector; 2 – Connector for additional modules; 3 – I-BUS connector for radio module JA-11xR; 4 – BUS Terminal 5 – LED indicators and RESET jumper; 6 – MicroSD card holder; 7 – Connectors of the housing tamper contacts; 8 – Serial number; 9 – MiniUSB connector; 10 – LAN connector

Parts of the JA-103K control panel (changeable parts) are:

– MicroSD card

To extend control panel options use:

– The JA-11xR radio module
– The JA-19xY GSM communicator

Control panel accessories include:

– 1pc USB cable (180 cm)
– 1pc Connection cable for the JA-11xR radio module
– 1pc Extension USB cable (20 cm) installed in the control panel
– 1pc Fuse T 1.6 A; 250 V
– 4pcs Jumpers (for jumper pins connection)
– 6pcs Warning stickers
– 4pcs Fasteners 8 mm
– 4pcs Screws 40 mm
– 3pcs Ties 100 mm
– Drilling template A4
– CZ / EN Installation manual (short version)

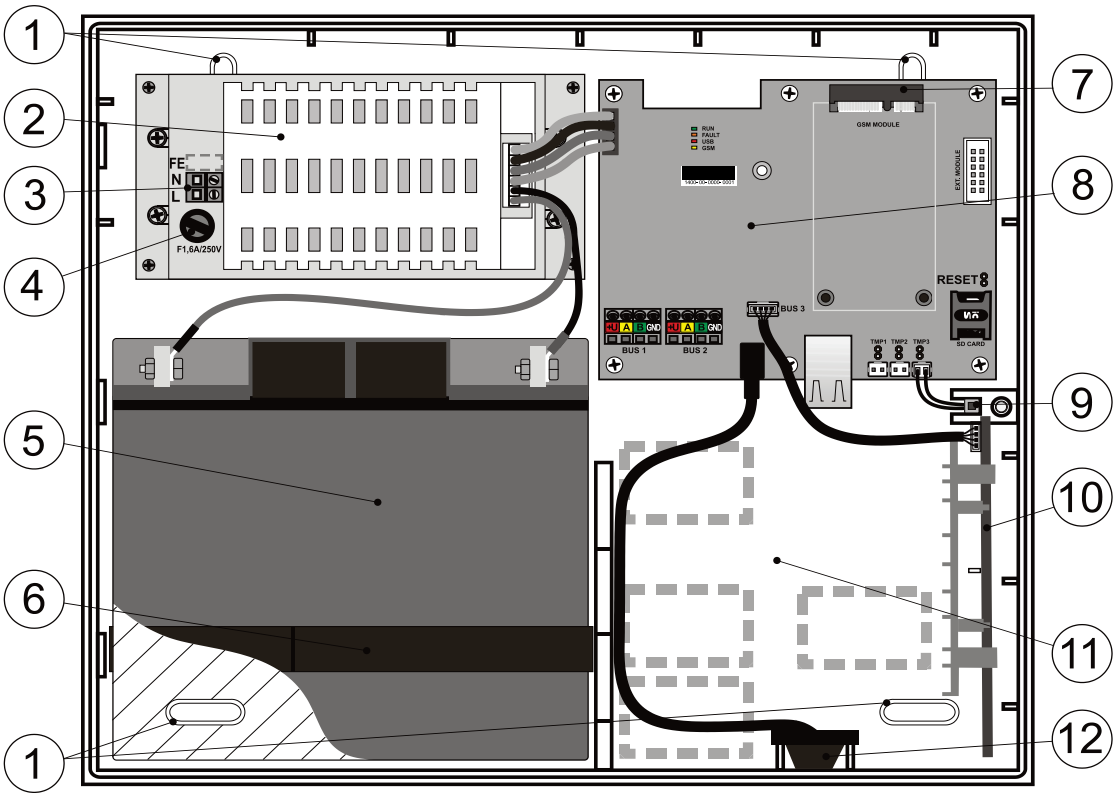
JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

3.3 Description of the JA-107K control panel

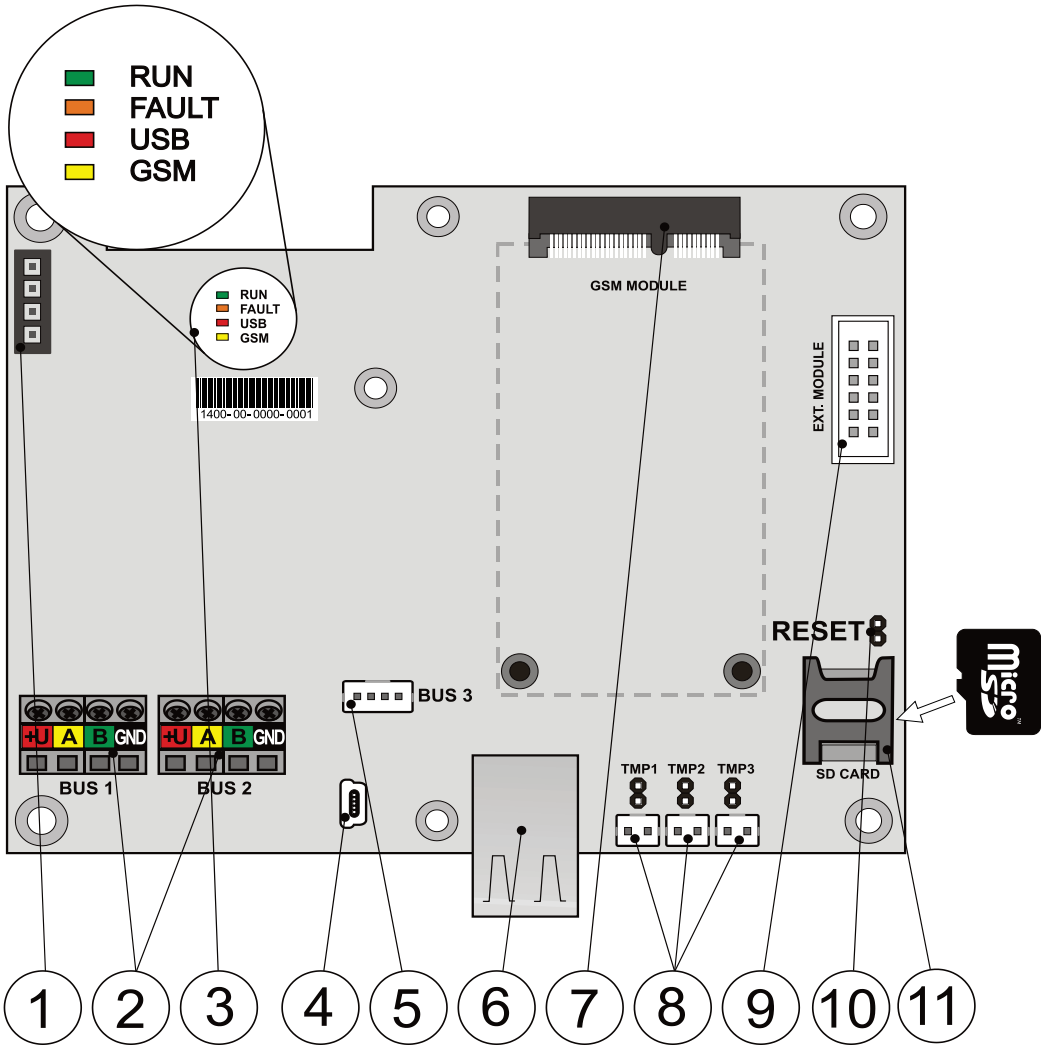
The JA-107K control panel is designed for **medium-sized and large installations, both BUS and wireless systems.** The control panel is equipped with a LAN communicator which can be connected to the Internet and with the ability to send data to servers (images taken by photo verification devices) or to the server of security agencies with technical equipment for this data to be received. When connected to the Internet via the LAN communicator remote access is also possible using the F-Link (JA-100-Link) software.

The control panel can be expanded with additional communicator:

The JA-19xY-zzzz – GSM communicator for GSM/GPRS or LTE communication. It allows communication with ARC, Jablotron Cloud Services and remote connection via SW F-Link / JA-100-Link



1 – Wall mounting holes; 2 – Control panel power supply; 3 – Mains power terminals; 4 – Mains fuse; 5 – Backup battery; 6 - Attachment strap of the backup battery; 7 – GSM communicator connector; 8 – Control panel PCB; 9 – Housing tamper contact; 10 – The JA-11xR radio module holder; 11 – Cabling space; 12 - USB connector for PC connection)



1 – Power supply terminal; 2 – Independent BUS terminals; 3 – LED indicators; 4 – MiniUSB connector; 5 – BUS terminal for the radio module or a 3rd BUS terminal; 6 – LAN connector; 7 – GSM communicator connector; 8 – Connectors of the housing tamper contacts; 9 – Connector for additional modules; 10 – RESET jumper; 11 – MicroSD card holder

Parts of the JA-107K control panel (changeable parts) are:

– MicroSD card

To extend control panel options use:

– The JA-11xR radio module
– The JA-19xY-zzzz GSM communicator

Control panel accessories include:

– 1 pc USB cable (180 cm)
– 1 pc Connection cable for the JA-11xR radio module
– 1 pc Extension USB cable (20 cm) installed in the control panel
– 1 pc Fuse T 1.6 A; 250 V
– 4 pcs Jumpers (for jumper pins connection)
– 6 pcs Warning stickers
– 4 pcs Fasteners 8 mm
– 4 pcs Screws 40 mm
– 2 pcs Ties 150 mm
– Drilling template A3
– 2 pcs Screws 3 x 8 mm
– 2 pcs Reduction for connecting the FASTON terminals to the battery
– CZ / EN Installation manual (short version)

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

3.4 Indication LEDs on the control panel board

All versions of control panels feature the following indication LEDs on the main board:

Description	Colour	Meaning
RUN	green	Flashing during operation of the communication BUS indicates correct functioning.
FAULT	yellow	Permanently lit indicates a general error in the system (more information provided by F-Link or a keypad with a display).
USB	yellow	Indicating USB connection to a PC.
GSM	red	If GSM communication is installed: – Permanently lit after power supply connection when searching for a GSM network (for 1 min at the most). – OFF if GSM is OK and no communication is going on. – Flashing in 1s/1s ON/OFF intervals if no GSM network is available. *Note: Flashing during communication, with a short repeated flash indicates the parameter setting: GSM communicator OFF.*

3.5 Additional Connectors on the control panel PCB

All control panels have a RESET jumper on their PCBs, thanks to which the system can be set to factory default settings (if enabled by the parameter “Reset enabled”). The procedure is described in chapter 12 Reset of the control panel.

There is a flat connector on the control panel PCB for the JA-19xY GSM communicator and a 10-pin connector for an additional module also.

There is also 4-pin connector:

- JA-103K, JA-103K-7Ah – I-BUS – designed exclusively for connecting the JA-11xR radio module placed inside
  the control panel housing. No other device can be connected to this connector.
- JA-107K – it is a 3rd BUS with the same parameters as BUS 1 and 2. It allows you to connect the JA-11xR radio module or to expand the system for a 3rd BUS by connecting the JA-110Z-D BUS splitter.

There are 3 connectors for a special tamper contact on the control panel PCB (a front cover tamper contact, a rear tamper contact and one supplementary tamper contact to increase the level of protection. Next to every connector is a jumper and by removing it you switch ON the tamper contact. If any of the contacts is not used, a jumper has to be connected, however, this degrades the system and does not compliance for certification to security grade 2.

3.6 Connection terminals on the control panel PCB

The control panel of a security system has the requirement to be connected to the mains ~110 – 230 V power permanently. The mains power is connected via terminals equipped with a replaceable fuse. The control panel is a protection class 2 device with double isolation. That´s why a 2-wire cable is enough (just a live wire and a neutral wire). The earth wire (if used) can be connected to the FE terminal (for JA-107K you need to remove the cover cap). Internal communication between the control panel and connected devices is performed via the BUS. It is realized for the JA-103K (JA-103K-7Ah) panel by a single four-colour terminal (red, yellow, green and black) and for the JA-107K panel there are two of these BUS terminals.

A built-in USB connector is placed on control panel PCB, connected to a USB connector located on the control panel housing. This makes it is possible to establish a connection with a PC via the USB cable without opening the control panel.

4 Before system installation

Select a hidden place for the control panel (inside the protected area) where mains supply is available. We recommend protecting the room with the control panel by a detector with immediate reaction. If the control panel is equipped with a GSM communicator, there must be good GSM signal reception in the location (check with a phone). Caution, if a possible intruder knows where the control panel is located, there is a risk of the system being damaged without sending information about the intrusion.

The mains supply of the control panel may only be installed by a person with the required electrical qualifications. The power supply of the control panel has double safety separation of the circuits. During the installation and connection of the BUS components of the control panel all the power supply of the control panel must be completely off or the BUS must be switched off in the F-Link software.

The control panel provides the option of connecting a power supply in a range of ~110 – 230 V / 50 – 60 Hz.

1. First consider the arrangement and target setting of the system. Clarify the required control method with the customer. It is recommended to prepare a project documentation for a more complex system.
2. When setting up the devices follow their manuals, the general design principles of fire alarm systems and instructions provided by the manufacturer during the certification training. If you have any unclear points, phone the Jablotron consultant. **The manufacturer declines any liability for damage if the system is installed or set improperly.**
3. Prepare the power supply of the control panel – use a suitable cable with double insulation and a cross-section of 0.75 to 1.5 mm². Voltage surge protection on the control panel mains supply is recommended. It is also recommended to use a single cable with a circuit breaker (2 A–6 A) which also functions as a main switch.
   Warning: *Don't connect any other electrical appliance to this specific circuit, not even power for external PG outputs or a heating system or any other device related to control panel functions.*
4. Attach the control panel straight onto the wall or any other incombustible surface. Ensure there are no metal constructions (e.g. elevator shaft) which could negatively influence transmitting or receiving radio signals (radio module and GSM communicator) next to the control panel. Use the supplied template to prepare holes for fasteners. Put the screws through the upper holes in the plastic housing to keep it 1 cm from the wall, then hang the control panel housing on it. Also put an additional screw through the lower hole(s) and screw it in as well to stabilize the position of the control panel. Tighten all the screws.

5 Installation of BUS devices

Connect only BUS devices of the JA-1xx JABLOTRON series to the system. Proceed with the following procedure:

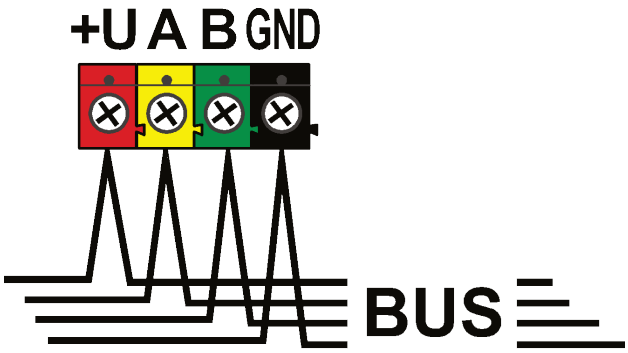
1. During the connection of any BUS modules the power supply of the control panel must be completely off or the BUS must be switched off in the F-Link software.
2. Follow the installation manuals of individual devices.
3. The BUS cable must be installed inside the area that is protected by the system. If the cable is outside the protected area, this part must be separated with a JA-110T BUS isolator.
4. For line branching use a JA-110Z BUS splitter (and the JA-110Z-B, JA-110Z-C, JA-110Z-D).
5. During the connection of BUS devices pay attention to the colour of wires (red, yellow, green, black).

Connection of third-party devices or a device of a different producer is possible via an appropriate module (the JA-111H, JA-116H, JA-114HN, JA-110M, JA-112M, JA-118M etc.). When such device is used, the producer (JABLOTRON) cannot guarantee proper functioning of the connected device and the system security grade.

5.1 The JABLOTRON BUS

The BUS of the JABLOTRON system consists of four wires (4-wire). The BUS is intended for the JABLOTRON system only and it cannot be shared with another system, not even to power different devices. For powering other systems by BUS (smart home automation) use the JA-121T interface or the JA-110T BUS isolator.

Terminal	Colour	Note
+U	red	positive power supply terminal; it can only be used to supply devices of the JABLOTRON series
A	yellow	data A
B	green	data B
GND	GND	common terminal (negative power supply terminal)



BUS terminal board

5.2 BUS cables

Resistance of the pair of power supply wires (there and back)		
CC-01	resistance of the pair per 1 m	0.0754 Ω
	resistance of the pair per 10 m	0.754 Ω
	resistance of the pair per 100 m	7.54 Ω
CC-02	resistance of the pair per 1 m	0.1932 Ω
	resistance of the pair per 10 m	1.932 Ω
	resistance of the pair per 100 m	19.32 Ω
CC-03	resistance of the pair per 1 m	0.0705 Ω
	resistance of the pair per 10 m	0.705 Ω
	resistance of the pair per 100 m	7.05 Ω
CC-11	resistance of the pair per 1 m	0.0754 Ω
	resistance of the pair per 10 m	0.754 Ω
	resistance of the pair per 100 m	7.54 Ω

Connect BUS devices using a JABLOTRON CC-01, CC-02, CC-03 or CC-11 cable.

The JABLOTRON CC-01 cable is designed for the main BUS line, or the connection of elements with a high consumption (siren) or remote elements. The cable has 4 wires (the colours corresponding to the BUS colour).

The power supply wires (black and red) have a bigger cross-section of the core (0.5 mm²) as compared to the communication wires (0.2 mm²). The cable is supplied in packs per 300 m.

The JABLOTRON CC-02 cable is designed for branches from the main BUS line or for the connection of elements with a low consumption (detectors) or for short distances. The cable has 4 wires (the colours correspond to the BUS colour). All the wires of the CC-02 cable have the same core cross-section (0.2 mm²). The cable is supplied in packs per 300 m.

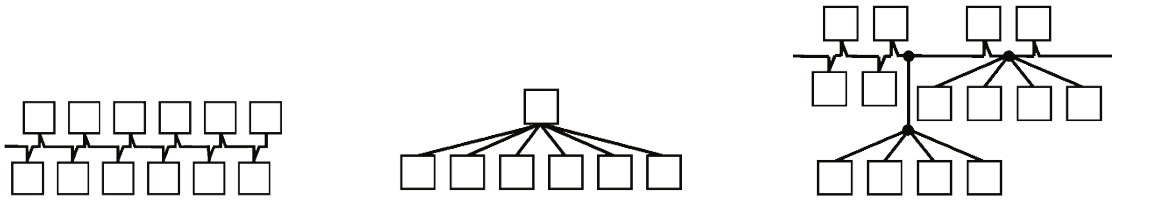
The JABLOTRON CC-03 cable is designed for the main BUS line, or the connection of elements with a high consumption (siren) or remote elements. The cable has 8 wires (8-wire) that are split as follows: The power supply conductors (red and black) have a bigger cross-section of 0.7 mm², the communication wires (green and yellow) for the system BUS and auxiliary wires (brown and grey, white and blue) have the cross-section of 0.3 mm². The auxiliary wires can be used as loops of magnetic detectors or tamper contacts. The cable is supplied in packs per 250 m.

The JABLOTRON CC-11 cable is designed for the main BUS line, or the connection of elements with a high consumption (siren) or remote elements. The cable has an external insulation of an orange colour, it has 4 wires (the colours correspond to the BUS colour). The power supply wires (black and red) have a bigger cross-section of the core (0.5 mm²) as compared to the communication wires (0.2 mm²). The cable is supplied in packs per 200 m. It has the B2CA increased fire protection certification.

5.3 BUS layout

When interconnecting individual parts of the system – detectors, keypads, sirens, output modules etc. you can route the BUS cable in the shortest possible direction regardless of the system parts that the used elements belong to. The BUS can branch as necessary. It can have a linear (Daisy-chain), Star or tree structure (Daisy-chain & Star). In real-life installation a combination of these three options is usually the most convenient choice.

Examples of possible wiring layouts of the BUS:



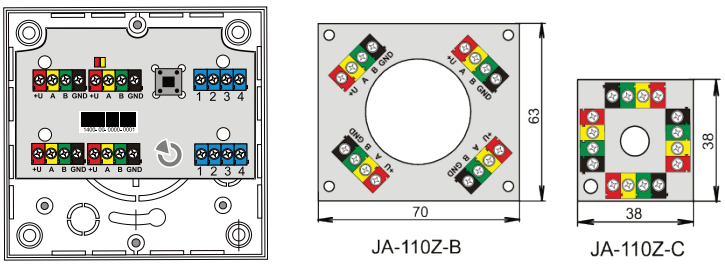
Daisy-chain (linear BUS structure) *Star BUS structure* *Daisy-chain & Star (tree BUS structure)*

The BUS cable **must not** be connected in such a way to create a **closed loop** of any wire (the ends of individual branches must never be interconnected and the common GND wire must not be interconnected either.

5.4 BUS branching and splitting

For branching and splitting of the BUS you can conveniently use a **JA-110Z BUS splitter**. It is produced in four variants: the JA-110Z, JA110Z-B, JA110Z-C and JA110Z-D. The JA-110Z is supplied in an installation box meant to be installed on a surface and equipped with front and rear tamper contacts to detect unwanted manipulation. It occupies one position in the system. All the terminals of the same colour are interconnected on the splitter PCB. Variant B is prepared with its dimensions for installation in the JA-190PL versatile assembly box. Variant C is prepared with its dimensions for installation in a standard KU-68 electric installation box.

Variants of interconnection terminal boards:



JA-110Z-B JA-110Z-C

5.5 BUS length and numbers of connected devices

The maximum length of one BUS without boosting (separation) is 500 m. The length is calculated as the sum of the length of all the cables between all the connected devices. The JA-107K control panels can have up to 3

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

separate BUS branches, i.e. the total length of both the BUS lines can be 3x500 m. You are recommended to distribute its addressed BUS devices equally between both the BUS lines, i.e. maximum 60 devices per either BUS.

For use of more than 60 peripherals on a single bus, it is necessary to use the JA-120Z bus booster unit is required.

The number of connected BUS devices is limited by the capacity of the backup battery of the control panel. To meet the standard for security level 2, in case of a 230 V mains failure the system must reliably work for at least 12 hours being powered by the backup source. Thus, the total consumption of all the BUS devices must not exceed the maximum continuous consumption of current from the control panel, see chapter 5.8 Example of calculation of BUS consumption to back-up the system. To calculate the total continuous consumption of connected elements summarize their **backup consumption** (Chapter 5.8).

Another limiting parameter for the max. length of a BUS can be the voltage loss along the line (shown clearly by the System Diagnostics in F-Link software).

5.6 Calculation of line losses

Voltage losses along the line depend on the line resistance, which results from the used conductor (cable) and consumed current. Current consumption values of devices can be found in individual manuals. These values can be used to calculate the line voltage loss and to find out whether there will be sufficient voltage available for the last installed device. The calculation is based on Ohm's law **U = I * R.**

CC-01 cable (power supply pair)		**CC-02 cable**		**CC-03 cable (power supply pair)**		**CC-11 cable (power supply pair)**	
Total current	Max. length	Total current	Max. length	Total current	Max. length	Total current	Max. length
50 mA	400 m	25 mA	200 m	70 mA	400 m	50 mA	400 m
100 mA	300 m	50 mA	150 m	140 mA	300 m	100 mA	300 m
200 mA	150 m	100 mA	100 m	280 mA	150 m	200 mA	150 m
300 mA	100 m	200 mA	50 m	420 mA	100 m	300 mA	100 m
500 mA	50 m	300 mA	30 m	800 mA	50 m	500 mA	50 m
The data in the table assume the worst possible case i.e. that the total consumption is at the end of the cable.							

In the normal operation state, the voltage of the +U and GND terminals is nearly 14 V. For the calculation consider a situation when the control panel is only powered by the battery and the voltage approximates 12 V. A higher voltage than the minimum allowed voltage of 10 V must be available for all the devices. For proper functioning of the connected devices the **maximum allowed voltage loss is 2.0 V.**

Unexpected voltage loss can be caused by terminal connections with a poor contact (transitional resistances).

Voltage losses of individual devices can be approximately verified using the F-Link software in the Diagnostics card for addressed devices. Non-addressed devices (e.g. output modules) do not provide this possibility; they must be checked with a measuring device.

In a real-life installation we always recommend you verify the calculation and connection by terminal measurement. In the case of high-consumption devices (siren, keypad, relay output) carry out this measurement during increased consumption periods (active siren, backlit keypad, engaged relay).

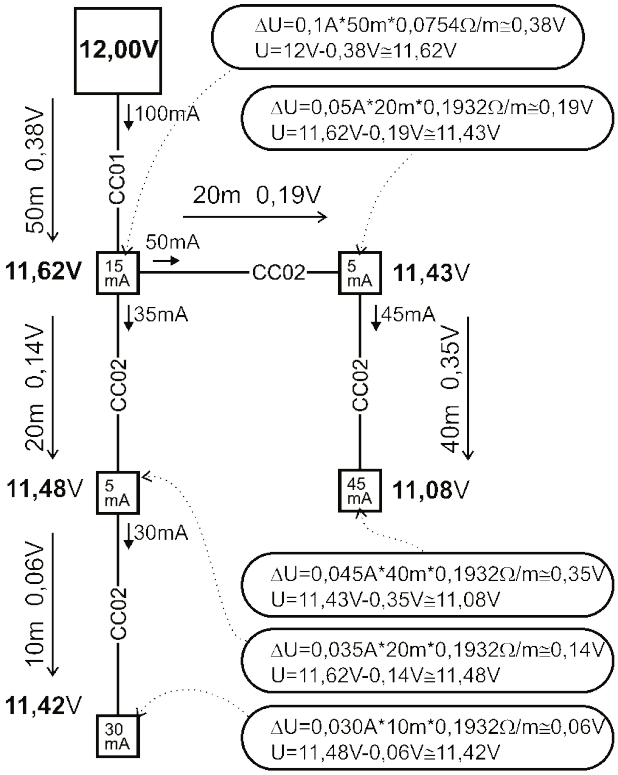
The limitations specified in the table are generally valid.

For the calculation of the total load of cables calculate the **consumption for cable selection** (you will find it in the manuals of devices).

5.7 Example of a voltage loss calculation

1. Find the values of current consumption of individual devices (in the technical parameters of the products - Current consumption for cable selection).
2. Get information about cable lengths. You need to know the cable length as exactly as possible from node to node.
3. Draw a plan with cable lengths and consumption of individual branches.
4. Calculate the electric current flowing through individual branches.
5. Use the assumed line length and the estimated values of current of individual branches in accordance with the tab above to compare suitability of cable selection.

Deduct individual losses from the supply voltage to determine the voltage at the line end. Always consider the voltage of 12 V from the control panel during mains supply failure operation.



5.8 Example of calculation of BUS consumption to back-up the system

The table presents an example of a small system. The total idle consumption in the backup mode is 78 mA. Thus, you can use the JA-103K control panel with a GSM communicator and a switched off LAN communicator, which enables maximum permanent loading of 80 mA.

Device	Description	No. of pieces	Consumption in backup mode
JA-11xR	module for radio communication	1	25 mA
JA-114E	control panel 15 mA + 3x 1 mA segments	1	18 mA
JA-110M	module for magnetic sensors 5 mA	1	5 mA
JA-110P	PIR motion detector 5 mA	2	10 mA
JA-110ST	fire detector 5 mA	2	10 mA
JA-110A	internal siren 5 mA	1	5 mA
JA-111A	external backed-up siren 5 mA	1	5 mA
		TOTAL	**78 mA**

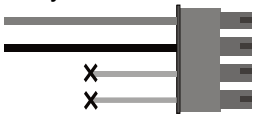
The JA-103 type is more suitable for wireless systems where devices are powered by batteries. When planning the configuration of a wireless control panel, do not forget to include the radio module(s) in the consumption.

For larger BUS systems use the JA-107K control panel.

5.9 Power supply requirements

The control panel requires to be powered permanently by protected AC power in a range 110 – 230 V, see Technical Specifications The control panel is a device with double isolation so its connection is usually performed by a cable with double insulation and a cross-section of 0.75 to 1.5 mm². The control panel has a protective small glass fuse. It is a part of the mains power terminals. The JA-103K and JA-103K-7Ah cannot be powered from alternative sources such as high-capacity batteries charged by solar panel, etc.

The JA-107K control panel makes it possible to utilize an external power supply which is in conformity with EN 50131-6. The power supply must be within the range of 10 to 15 V (DC) and intended for use in remote system installations and/or objects without a constant 230 V (AC) power supply. In order to connect the external power supply, we recommend the use of a VOD-JA-107K cable. It is comprised of a conductor, a fuse box containing a fuse (F 6,3 A) and a connector.



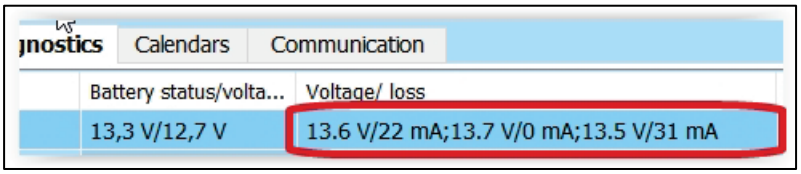
5.10 Backup requirements

A security system which has to comply with security grade 2 has to backed up by backup battery for 12 hr during a mains power disconnection and it also has to be fully charged 48 hr after mains power recovery and be ready to back the system up again. To meet this requirement, it is necessary not to exceed the maximum current consumption from the BUS.

Example of maximum permanent current taken from system BUS according to the backup battery capacity:

	JA-103K 2.6 Ah battery		JA-103K-7Ah 7 Ah battery		JA-107K 18 Ah battery	
Maximum continuous current consumption from the BUS	BUS 1 – 1000 mA I-BUS – 200 mA		BUS 1 – 1000 mA I-BUS – 200 mA		2000 mA permanent 3000 mA for 60 min. (max. 2000 mA for one BUS)	
Maximum continuous current consumption for 12-hours backup supply	Without GSM communicator	LAN – OFF: 115 mA LAN – ON: 88 mA	Without GSM communicator	LAN – OFF: 328 mA LAN – ON: 304 mA	Without GSM communicator	LAN – OFF: 1135 mA LAN – ON: 1107 mA
	With GSM communicator	LAN – OFF: 88 mA LAN – ON: 53 mA	With GSM communicator	LAN – OFF: 296 mA LAN – ON: 272 mA	With GSM communicator	LAN – OFF: 1100 mA LAN – ON: 1072 mA
Maximum continuous current consumption for 24-hours backup supply	Without GSM communicator	LAN – OFF: 21 mA	Without GSM communicator	LAN – OFF: 136 mA LAN – ON: 12 mA	Without GSM communicator	LAN – OFF: 535 mA LAN – ON: 499 mA
	With GSM communicator	LAN – OFF: 17 mA	With GSM communicator	LAN – OFF: 104 mA LAN – ON: 80 mA	With GSM communicator	LAN – OFF: 530 mA LAN – ON: 494 mA

The current taken from each BUS output terminal is shown in the F-Link software in the Diagnostics tab on line 0 where the control panel is. For the JA-107K control panel it is necessary to sum the values of all BUS outputs. This current is compared with the current stated in the table above. This way you can check if the backup battery capacity is adequate to norm requirements for system backup time. If the measured current is higher than the one stated in the table, it is necessary to solve the system power supply with e.g. adding the JA-120Z booster unit.

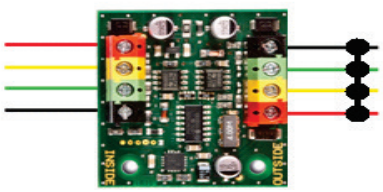


5.11 BUS isolation

Parts of the BUS routed in unprotected areas must be protected from possible short-circuit or another attempt to disable the system by isolation using a JA110T BUS isolator. This module can be incorporated in a JA-190PL multipurpose installation box. The isolator also improves the signal quality of the BUS. It is connected to and powered by the BUS, it does not occupy any position in system and makes it possible to extend the maximum BUS length up to next 500 m. Avoid using 2 or more BUS isolators on one BUS leg – devices cannot communicate through 2 or more of them.

An application example may be routing of the BUS to relay modules controlling for example blinds or a siren to which the BUS is routed in such a way that it could be potentially attacked or disabled from outside. You will find more information in the JA-110T manual.

BUS from the control panel



Possible BUS damaging behind the module caused for instance by short circuit, doesn't influence the BUS in front of the module!

5.12 Use of existing cabling in refurbishment projects.

- For the installation of new lines, you should preferentially use the CC-01, CC-02, CC-03 and CC-11 cables.
- In case of connection to cables of the SYKFY 3x2x0.5 type the data wires of the BUS (A, B) must be connected to one selected twisted pair. For the power supply (+U12, GND) you can connect the respective wires together in the remaining two pairs (doubling within a pair).
- In case of connection to cables of the UTP the data wires of the BUS (A, B) must be connected to one selected twisted pair. For the power supply (+U, GND) it is suitable to connect together (double) the respective wires of the remaining wire pairs.

If a shielded cable is used, do not connect the shield to the BUS terminals! We recommend bonding all the shields (tinning) in the control panel to an auxiliary terminal and not to connect this bonding anywhere else. Also leave the other end of shielding at the device side unconnected.

6 Use of wireless devices

In the JABLOTRON system you can use wireless device of the JA-15x, JA-16x and JA-18x series. The JA-11xR radio module must be used for a communication with the wireless devices. There can be up to 3 radio modules in the system.

When installing individual devices, follow the instructions in their manuals.

Caution: *Up to 120 wireless devices can be enrolled into the JA-107K control panel, they can be enrolled to positions 1 to 120 only. The positions 121 to 230 are for BUS devices only. If the JA-11xR radio module is installed after the JA-120Z BUS booster unit, it must be enrolled in a position within the position range 1 – 120.*

6.1 Installation of a JA-11xR radio module

1. The JA-11xR radio module can be in a holder in a bottom right corner of the control panel.
2. If the JA-103K/103K-7Ah/107K control panel t is installed in a place with poor GSM signal reception, the GSM module increases its transmission power, which can have a negative impact on the radio module communication range in the system. In such a case it is recommended to place the radio module outside the control panel, namely at least 2 m from it, where it will not be negatively influenced anymore and will have higher-quality radio reception from the devices, which will allow for longer ranges and consequently installation distances.

   Note: *The JA-111R taken out from the control panel must be inserted into the PLV-JA111R plastic housing (sold separately).*

   The radio module connector on the JA-103K and JA-103K-7Ah control panel PCB is exclusively designed for the connection of a one radio module installed inside the control panel housing.

3. You can cover a larger area with radio signal by installing up to 3 radio modules in different places (e.g. each one on a different floor). Signals from a wireless device (hereinafter device) can be received by more radio modules simultaneously. The control panel communicates in a cycle with individual radio modules, so it will get information sent by a device from the radio module that was the first to receive an intact signal and reacts to it. Then, it will not get the same information from the other radio modules any more even though it was received with a stronger signal. As regards to bi-directional devices, the control panel "reserves" the once used channel (communication with the first radio module) and after that it communicates with the particular device via this radio module only (shown in Diagnostics, the Channel column) until the device stops responding. Then, it looks for the connection signal in the other radio modules. If you need to verify the quality of connection of individual devices to individual radio modules, check it by the RF signal graph in the F-Link software (button on the upper toolbar). There you can select the radio module for which communication should be checked and the activate devices you want to check. A graph of radio communication shows the RF signal strength measured by a specific radio module. It is also possible to have several RF signal windows open so you can very simply monitor the RF coverage in that premises.
4. Install a radio module vertically on a wall. It must not be situated near objects that shield or interfere with communications (metals, electronic devices, cables, pipelines etc.).
5. After switching the system on you must **enroll the radio modules first.** It is only then that you can enroll wireless.

Recommendation: It is recommended to enrol the wireless devices after they have been installed into their final position in the premises. Although this makes the installation procedure less comfortable, it offers the advantage of a more reliable connection of the wireless devices with the radio module once the alarm system is put into operation. The radio module has implemented a mechanism of measuring the RF signal while in service mode. This mechanism provides a safety margin in case of a deterioration of the radio transmission conditions when the system is in full operation. More information can be found in the EN 50131-5-3 norm.

6.2 Installation of wireless devices – enrollment mode

Wireless devices have to be enrolled to the system for instance by a production code. The enrollment procedure can be performed in Enrollment mode only using a PC with installed F-Link software, see chapter 8.4.1 Enrolling and erasing devices.

6.3 Extending the range of wireless devices

If the standard range of the radio module is not sufficient enough or if it is not possible to shorten the distance between the radio module and the wireless devices, it is possible to extend the signals of the one-was wireless devices (detectors, remote controls, PG module) with the JA-150R radio signal repeater, which requires only a permanent power supply for its installation. The location of the JA-150R signal repeater is chosen in such a way that both the control panel (radio module) and the wireless devices are in its range, see the figure below.

First signal repeater range | Radio module range | Second signal repeater range

7 Switching the system ON

1. Check connection of the BUS cables.
2. Verify whether a microSD card is present in its holder on the control panel board.
3. Check whether the mains supply cable is correctly connected to the control panel and that the supply cable is firmly fixed.
4. Insert a battery in the control panel and fix it in the housing using a strap.
   Caution – the backup battery is delivered in a charged condition, it must not be short-circuited!
5. Connect the supply leads of the battery. Mind the correct polarity (red +, black -).
   a. Switch on power from the mains and check the LED indicators on the control panel:
   b. The green LED starts flashing (BUS function).
   c. The red LED flashes – logging in to the GSM network.
   d. The red GSM LED goes out – the control panel has established connection to the mobile network.
   e. The red LED permanently lit – the control panel has not logged in to the GSM network.
   (points c, d, e applies only with installed GSM communicator).
6. When the connected BUS devices start flashing yellow, assign them to the system, see chapter 8.4.1 Enrolling and erasing devices.
7. Perform configuration of the keypads, see chapter 10.5.1 Keypad configuration.
8. Set the required functions and test the system, see chapter 10.9 Parameters tab.
9. In order to comply with the EN50131-1 or INCERT norms, grade 2, disconnect the extending USB cable from the PCB of the control panel.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

8 System configuration

The security system (protected premises – building) can be split into independent parts – sections. Every section can also be guarded as a whole section or only part of it. This is called partial setting. Detectors with the enabled parameter “Internal” do not guard in such a mode.

The basic part is **perimeter protection**. It protects main doors, garage doors, windows, balcony doors, and rear and roof entrances. Among the devices assigned to perimeter protection you can find magnetic detectors, glass-break detectors, shake / tilt detectors and also infrared barriers. The only specific thing is that main doors or garage doors are usually delayed and the rest of the zones are defined as having an instant reaction.

The following part is about **motion detectors**. It follows movement in protected premises using motion detectors (PIR) or their combination with other detectors. Detectors placed in a premises entrance usually have pre-set delay reaction or next delay reaction. The rest of the motion detectors are in most cases pre-set to instant reactions. You can select from up to 3 timers to make the entrance paths (for instance, a longer delay during entry through a garage).

Premises protection serves to protect safes or valuables but also for the detection of intrusion using brute force. Garage doors can be damaged with any opening. Shake and tilt detectors are included in premises protection but also the usual magnetic detectors for the detection of opening the doors can be included–typically as a delayed sensor.

Protection of individual security components is realized by tamper contacts indicating unauthorized operation of the device.

Environmental protection includes mostly fire detectors, detectors for the detection of combustible and poisonous gases and flooding detectors. All the mentioned detectors have usually an adjustable reaction as permanently independent of system status or simply said a 24hr reaction.

8.1 The system profiles

System profile selection allows you to globally pre-set the following system parameters to modify system behaviour to comply with the given norm and the required security grade. These options could be blocked when a specific profile is selected for changes.

Caution: *Setting individual parameters by selection of a system profile does not guarantee that the installed system complies with security grade 2. Only correct system design (using the right devices) and correct installation with CLC/TS 50131-7 requirements and ARC service implementation can ensure security grade 2.*

System parameter overview when the “DEFAULT” system profile is set (default settings):

Device	Parameter	Option	Blocking (limitation)
Control panel	Codes with a prefix	NO	NO
Control panel	Enable 125kHz EM UNIQUE card standard	YES	NO
Control panel	Code length	4	NO
Control panel	Automatically check time in the connected PC	YES	NO
Control panel	Siren when partially set	NO	NO
Control panel	Sirens enabled	YES	NO
Control panel	Warning about default codes	YES	NO
Control panel	Administrator – restricted Service/ARC rights	NO	NO
Control panel	Service and ARC controls the system	YES	NO
Control panel	Trial operation	NO	NO
Control panel	Service requirement	NO	NO
Control panel	Enable Maintenance mode	YES	NO
Control panel	Duress access control	YES	NO
Control panel	Alarm confirmation within one section	NO	NO
Control panel	Siren (IW output) when a tamper is triggered	NO	NO
Control panel	Tamper alarm indication reset by Service	NO	NO

Control panel	Reset enabled	YES	NO
Control panel	Daily reset of device autobypass	YES	NO
Control panel	Blocking when setting	NO	NO
Control panel	Unsetting cancels alarm	NO	NO
Control panel	Unsuccessful setting	NO	NO
Control panel	Device trouble autobypass	YES	YES
Control panel	Delayed report to ARC	NO	NO
Control panel	Ways of setting	Set with warning	NO
Control panel	Authorization type	Standard	NO
Control panel	System blocking by alarm	NO	NO
Control panel	Loss of a BUS module	Fault	NO
Control panel	Fault autobypass	3rd activation	YES
Control panel	Alarm length	260 s	90…1200 s
Control panel	Entrance delay	30 s	5…120 s
Control panel	Exit delay	30 s	5..120 s
Radio module	RF jamming detection	Disabled	NO
Keypad	Optical indication setting	1.Permanently (BUS) or 4.Segment status change (RF)	NO
Keypad	Indicate Unset status	YES	NO
Keypad	Indicate Set status	YES	NO
Keypad	Alarm acoustic indication	YES	NO
Keypad	Entrance delay acoustic indication	YES	NO
Keypad	Exit delay acoustic indication	YES	NO

By setting the “Default” system profile, all the mentioned parameters are pre-set back to the factory settings and all inaccessible parameters are accessed for changes to be performed. The alarm system then doesn’t comply with the requirements of security grade 2, which might violate the requirements given by the insurance company or local regulations. In the case of a harmful event, the insurance company doesn’t have to pay for the damage because of broken regulations and an incorrectly programmed system caused by the installation company.

System parameter overview when “EN50131-1, grade 2”, “INCERT”, „SSF 1014“ are set:

Device	Parameter	Option	Blocking (limitation)
Control panel	Codes with a prefix	YES	YES
Control panel	Enable 125 kHz EM UNIQUE card standard	YES	NO
Control panel	Code length	4 (INCERT 6)	NO, (INCERT YES)
Control panel	Automatically check time in the connected PC	YES	NO
Control panel	Siren when partially set	NO	NO
Control panel	Sirens enabled	YES	YES
Control panel	Warning about default codes	YES	YES
Control panel	Administrator – restricted Service/ARC rights	YES	YES
Control panel	Service and ARC controls the system	NO	YES
Control panel	Trial operation	NO	NO
Control panel	Service requirement	NO	NO
Control panel	Duress access control	YES	NO
Control panel	Alarm confirmation within one section	NO	NO

Control panel	Siren (IW output) when a tamper is triggered	YES	YES
Control panel	Tamper alarm indication reset by Service	YES	YES
Control panel	Reset enabled	NO	YES
Control panel	Daily reset of device autobypass	NO	YES
Control panel	Blocking when setting	YES	YES
Control panel	Unsetting cancels alarm	YES	YES
Control panel	Unsuccessful setting	YES	YES
Control panel	Disable device trouble autobypass	NO	NO
Control panel	Delayed report to ARC	YES (SSF 1014 ON)	NO (SSF 1014 YES)
Control panel	Ways of setting	According to system profile	YES
Control panel	Authorization type	Standard	NO
Control panel	System blocking by alarm	No	NO
Control panel	Loss of a BUS module	Tamper always	NO
Control panel	Device autobypass	3rd activation	NO
Control panel	Alarm length	260	90…900 s
Control panel	Entrance delay	30	5…30 s
Control panel	Exit delay	30	5..60 s
Radio module	RF jamming detection	LOW	NO
Keypad	Optical indication setting	2.Section status change (BUS) or 4.Segment status change (RF)	YES
Keypad	Indicate Unset status	NO	NO
Keypad	Indicate Set status	NO	NO
Keypad	Alarm acoustic indication	YES	YES
Keypad	Entrance delay acoustic indication	YES	YES
Keypad	Exit delay acoustic indication	YES	YES
Remote controls	Control functions limitation	NO	YES
Calendar	Control function limitations	NO	YES

Global overview of reasons preventing setting according to the pre-set system profile:

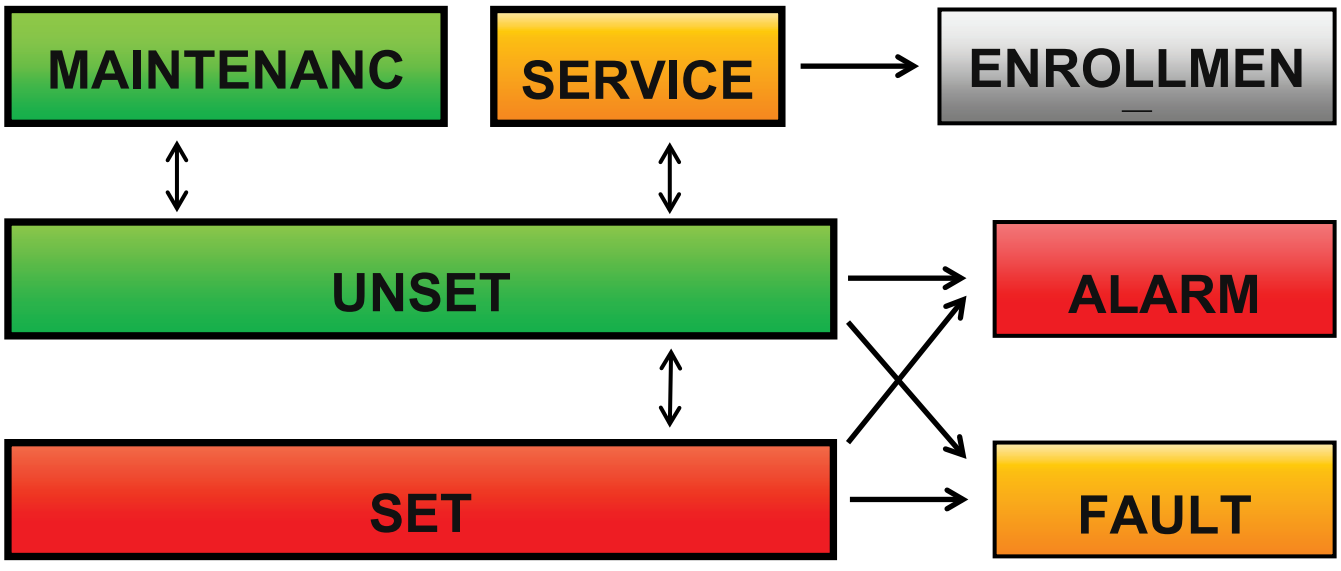
Event \ Profile	Default		EN50131-1, grade 2		INCERT, grade 2 SSF 1014	
	Passable	Impassable	Passable	Impassable	Passable	Impassable
Active tamper	☑		☑			☑
Active input (any input)					☑	
Active instant input	☑		☑		☑	
Active alarm memory indication			☑			☑
RF device 20 min. no response			☑		☑	
Siren fault				☑		☑
Fault	☑		☑			☑
Loss of a device	☑		☑			☑
Blocked detectors						
Low Batt in device	☑		☑			☑
Low Batt in control panel	☑		☑			☑
Failure of battery in control panel	☑			☑		☑
AC fault			☑		☑	
AC fault for 30 minutes	☑		☑			☑
System in configuration				☑		☑
GSM fault	☑		☑			☑
LAN fault	☑		☑			☑
PSTN fault	☑		☑			☑
Fault of all ARCs				☑		☑

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

8.2 Control panel operation modes

Security system has a few operation modes. Switching between modes depends on users' authorisation levels.

Mode	Description
Service (+ Enrollment mode)	A mode in which no alarm can be triggered. It is only meant for a service technician or an ARC technician and it is for enrolling new devices and system configuration. No control is available in this mode (locally nor remotely). Segments on keypads are switched off and the mode is indicated by yellow flashing of the backlit button (2x flashes each 2 s) and signals from remote controls or other devices are ignored. Entering or leaving service mode can be performed from an LCD keypad or from a PC using F-Link software. When a PC is connected online, service mode cannot be entered or left from the keypad.
Maintenance mode	A mode meant primarily for Administrator. It allows to perform a maintenance in the section (sections) according to the administrator's access rights (e.g. changing batteries in detectors). The administrator can switch the system to the maintenance mode using the keypad or the JA-100-Link software. The maintenance mode in one section does not affect the status and functionality of other sections or the status of programmable PG outputs. The maintenance mode is indicated by the green flashing of the backlit button (2x flashes each 2 seconds) and by the segment buttons of the particular section lighting off. Entering or leaving service mode can be performed from an LCD keypad or from a PC using F-Link (JA-100-Link) software
Unset	A normal mode in which intrusion detectors don't guard. Free movement is possible through the premises, opening windows and doors is allowed. Smoke / temperature detectors, gas leak detectors, flood detectors or panic buttons can trigger an alarm all the time. Also tamper contacts of all devices always protect and when they are activated the system triggers a tamper alarm. Unset mode is indicated on the keypad by a green light on the specific segment.
Set (fully or partially)	All detectors are active and guard (except Internal detectors when partially set) and when they are activated then an alarm is triggered (next point). Set mode is indicated on the keypad by a red light (yellow light when partially set) on the specific segment.
Alarm	Alarm is a state when for a pre-set time (alarm length) the IW and EW outputs are activated and the internal and external sirens sound. The Alarm state is indicated on the keypad by rapid flashing of the red backlit button. For a description of differences in EW and IW output behaviour see chapter8.5 Types of alarms.
Fault	Fault is a warning signal of the system which indicates some abnormal state of the control panel, communicators or devices and their power problems (mains power or battery) or communication troubles. Optical indication can be viewed on keypad backlit indication segment.



8.3 Authorisation of users

Everyone who can control a security system or perform any setting is called a User of the system. The first preset user with almost the highest authority and who cannot be erased is called the Service code. The second preset code which cannot be erased is the Main Administrator. Other users, who can be added and erased, have adjustable authorisation.

Authorization of users can be as follows:

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, 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.
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 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 a user 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. 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 from the system.
Administrator (Main)	It can enter the Maintenance mode. 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. 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 as to confirm access. By the factory defaults, the code is 1234 and it cannot be erased from the system.
Administrator (Other)	It can enter the Maintenance mode in assigned sections. 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. Has permission to erase the alarm memory in assigned sections. 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 access cards and change their telephone numbers. It has permission to erase the alarm memory in assigned sections. Users can change their codes provided that the system uses Codes with prefixes. 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	This code is allowed only to set a designated section. 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 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	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 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.

Creating new users and the administration of their authorization level is done by F-Link or JA-100-Link software.

8.4 System optional parameters

Code with prefix – this function determines the way of entering all access codes during user´s authorization. When enabled the system requires entering of a 1 or 3-digit prefix followed by * before you enter your 4, 6 or 8-digit valid access code (for instance. 12*3456). In this case it is allowed for users to enter their own 4-digit codes from an LCD keypad and to edit them arbitrarily. Disabling the function causes the system not to require a prefix to be entered and only a valid access code is required. In this case only the system administrator can add and edit the codes of all users. The administrator has to avoid the situation of code duplication (2 users should not have the same code).

Caution: *Disabling this parameter causes the irreversible erasing of all user codes and pre-set service and administrator codes to default values. User authorization and RFID cards and tags of already set up users remain the same.*

Code length – to increase the alarm system security level during authorization, it is possible to pre-set the **user code length** regardless of the prefix function. There can be 4, 6 or 8-digit codes. When the code length is changed, then Service and Administrator codes are set to the default values (1010 and 1234) and all other codes are erased. Default codes are:

Default codes without a prefix	4-digit	6-digit	8-digit
Service:	1010	101010	10101010
Administrator:	1234	123456	12345678

Default codes with a prefix	4-digit	6-digit	8-digit
Service:	0*1010	0*101010	0*10101010
Administrator:	1*1234	1*123456	1*12345678

Enable 125 kHz EM UNIQUE card standard – if disabled, identification RFID cards / tags (JA-190J, JA-191J, JA-192J, JA-193J, JA-194J, JA-195J, JA-196J) recommended by the manufacturer may only be used. If enabled, cards of other manufacturers working at the above-mentioned frequency are also allowed.

Siren when partially set IW – this function which allows the activation of internal sirens during an intrusion alarm (it is not related to Fire or 24hr alarms) when the system is partially set.

Warning about default codes – when service mode is left the system sends an SMS (position 0) to the service technician about the remaining codes still set to default.

Administrator – restricted Service / ARC rights – administrator authorisation is required to access the system for the ARC or service technician. In the case of remote access by a service technician to the system via F-Link the administrator may get authorised using a keypad in the building. In the case of a local connection by a service technician to the control panel using a USB cable the administrator may get authorized remotely using the voice menu.

Service and ARC controls the system – this is for the service and ARC technicians to control (Set / Unset) all sections and all PG outputs (ON / OFF) which require authorisation.

Trial operation – a special mode used after system installation when, regardless of the real setting of alarm length, it shortens to 60 s and all alarm event are reported by means of an SMS to defined users and the service technician (position 0) even though alarm reports are not activated for them. Trial operation is automatically terminated after 7 days after leaving Service mode.

Service requirement – if enabled, 12 months after you have left service mode there appears on the LCD keypad a message namely “System check requirement” and by pressing the “I” button it shows “call service technician” with his telephone number (if pre-set). A message on the LCD disappears automatically when a service technician locally accesses the system. The annual check counter performs a reset. The service requirement can be also set to an exact date as a calendar action in the Calendar tab *(the Calendar “Service requirement” function can be combined with the automatic “Service requirement” one year after leaving Service mode)*.

Duress access control – this function is to trigger a silent panic alarm by authorization only or during system control (setting, unsetting, PG) when a user is under a threat from an intruder. A panic alarm is triggered during system control by adding the number “1” to the last digit of the code. It is supported for a code with or without a prefix as well. When a user code has the number 9 as the last digit then during access control enter 0 as the last digit.

Alarm confirmation within one section – if confirmation reaction by another detector is set for a detector, this confirmation option can be used to limit confirmation to the same section only (otherwise a detector from any section can confirm an alarm). This is equally valid for intrusion detectors and for fire detectors.

Siren (IW output) when tamper is triggered – the sirens with an IW reaction acoustically indicate a tamper alarm if the zone is unset or partially set. Sirens always indicate when the system (section) is set fully.

Tamper alarm indication reset by Service – the tampering memory indication can only be reset by a service or ARC technician. If this option is not checked, the indication may also be reset by the Administrator (but not a User).

Reset enabled – possibility to lock resetting the control panel with a jumper on the board. If the reset option is disabled and the service code is lost, the control panel can only be unlocked by the manufacturer. Reset of the control panel is described in chapter 12 Reset of the control panel.

Daily reset of device autobypass – the option only relates to activation inputs (not tamper and fault inputs). If this option is enabled, the system will automatically reset autobypassed devices, namely every day at 12:00. If the option is disabled, the autobypass of the device will only be reset with a status change in the section. This selection is suitable e.g. for the use of detectors with a 24hr reaction or flood detectors that are found in a section where setting/unsetting is not necessary.

Blocking when setting – if enabled then all active inputs will be blocked during setting the section and they cannot trigger an alarm in this guarding period anymore. If disabled, all active inputs will be bypassed (autobypass) temporarily until they go to standby and detectors start guarding again (risk of false alarm triggering – e.g. improperly closed window).

Unsetting cancels alarm – a function which determines if an alarm will be cancelled by the authorization of a valid code only or by unsetting the section with an alarm. If enabled, an alarm can be cancelled by unsetting the section where the alarm has been triggered or from an LCD keypad menu by pressing on “Cancel warning indication”.

Unsuccessful setting – a function processed during every setting procedure. If an instant zone is triggered within the exit time or a delayed zone stays open when the exit time expires, the system is not set and triggers an “Unsuccessful setting” event and records it in the history. It is also reported by an SMS to a pre-set user if the event “SMS about unsuccessful setting” is enabled to be sent. It is indicated by keypads and also by an outdoor siren. To cancel the indication about unsuccessful setting it is necessary to press “Cancel warning indication” in the LCD keypad menu.

Fault autobypass – it is only available when one of the system profiles “EN50131-1” or “INCERT” is chosen. It is meant for disabling the limited number of triggered faults from 3 faults maximum to no limit.

Ways of setting – selection of the way the system gets through setting the system with an active device or fault in the system. From the lowest level the system always sets regardless of active devices or faults to the highest level where it cannot be set with active device (instant zone).

Authorization type – selection of the way the system processes user authorization. From Standard authorization (only a code or a card) through to RFID card confirmation by a code (if the user has assigned both) to double authorization, which means obligatory applying of the card and code. User code confirmation by a card to reduce the risk of unauthorized access or control by a third party.

System blocking by alarm – the parameters allow blocking the system after first alarm triggering (intrusion or tamper) to avoid next alarms being triggered. Unblocking can be performed by a special code for Unblocking or by authorized access from an ARC (meant for Great Britain). Unblocking after tamper alarm triggering can be performed also by a user with service authorization (meant for the Benelux area).

Loss of a BUS device – the control panel processes the loss of a device or a short circuit on the system BUS. According to the selected option it will react by triggering a Fault, or a tamper alarm with every device loss, or the last option by triggering a tamper alarm after confirmation that any other device is lost.

Device autobypass – the option only relates to activation inputs, not tamper and fault inputs. If the function is enabled and set to “3rd activation”, the control panel allows 3 activations of the device during one alarm period. The second option is “3rd alarm”, that means the particular device is only bypassed after 3 alarm periods, i.e. the device can be activated up to 9 times in one guarding period.

8.4.1 Enrolling and erasing devices

An installed device (detector, keypad, siren, tag etc.) will only work after being enrolled on a position (address) in the system. After the enrollment some devices occupy more positions (multiple magnet inputs, input expanders). There are also devices (PG output modules, status indicators, BUS separators and splitters) that are not enrolled on any position. You will find details in the manual of the particular device.

1. Device enrollment is performed through the F-Link software, the Devices tab, **Enroll** button Enrolling is **only possible in the Service mode**.
2. You can enroll a device in several ways:

a. **By pressing the tamper switch of a BUS device = closing the cover** (some devices can be enrolled by the pressing of a key – see the manual of the particular device).
b. **By connecting the battery to a wireless device** – however, at least one radio module must be enrolled first. In the case of remote controls of the JA-186Jx type the battery connection can be replaced by pressing and holding two buttons (forming a pair). Remote controls of the JA-154Jx and JA-16xJ type are enrolled by pressing of any button. Wireless access modules (keypads) can be enrolled by pressing of the backlit activation button.
c. **By entering the serial number in the SN production code field** (it is found under the barcode on the board inside the device, e.g. 1400-00-0000-0123). The number can also be read with an optical barcode reader. Subsequently, you should activate the detector to verify its enrollment.
d. **By selectively loading not enrolled BUS devices** – if one or more devices that have not been enrolled yet are connected to the BUS, after pressing of **Enroll** in the **Device** the **Enroll not enrolled** button will be displayed, which will offer enrollment of the BUS device. You will enroll the device by double clicking on the selected item.
e. **By collectively loading not enrolled BUS devices** – if one or more devices that have not been enrolled yet are connected to the BUS, after pressing of the **Scan/add new BUS devices** button all the BUS devices will be enrolled collectively. This procedure does not allow you to determine the sequential positions for individual devices.

3. You can delete a device by deleting its production code (just the entire device will be deleted) or by selecting the respective line in the Devices tab and the Delete option in the menu or under the right mouse button or by merely pressing the Delete key, which will delete the whole line of the device (with its settings of the section, reaction, PG output control, notes and other options). This way, after marking more devices (click + Shift or click + Ctrl) you can delete all of them or you can just change a common parameter.

Notes:

- BUS devices that have not been enrolled flash with yellow light. If a not enrolled device does not start flashing with the yellow LED within approx. 180 s after enabling of the power supply of the control panel (in the course of initialization) check whether the device is properly connected.
- Wireless devices with one-way communication do not have any means of signalling the enrollment request.
- If you enroll a device in the system using the above-mentioned procedure, the next position will be offered automatically. You do not need to take any steps; you just need to enroll devices in the selected order. Automatic movement to the next position can be cancelled in the device enrollment window.
- If you enroll an already enrolled device on another position, it will move to that position.
- If a device occupies more than one position, it will automatically occupy the respective number of consecutive position by one enrollment (e.g. the JA-110M module, which has two alarm inputs, will occupy two positions). Caution, inadvertent deletion of device enrolled on other position can occur!
- If you enroll a device on the highest possible position, the process of gradual enrollment will be completed.
- Free positions are set in section 1 by default. The selection of a section can be changed later.
- For multi-position devices such as JA-116H, JA-118M, JA-150M etc. you can limit the number of occupied positions by erasing specific lines when the module is enrolled. Perform erasing by clicking on the particular line on required position (not the button in the column Type!) and press the Delete key on the PC keyboard.

8.4.2 List of applicable reactions

In the Devices tab you can set the reaction of the system activation of an enrolled device. Only such types of reactions are offered for individual devices that make sense for the particular product. There are some devices that cannot be assigned any reaction (e.g. an external siren).

Instant	Immediate intrusion alarm if it is set. If an entrance delay is set, an IW alarm is released. An EW alarm is only released after expiration of the entrance delay time (for more information about EW and IW see chapter 8.5 Types of alarms).
Delayed A	Intrusion alarm with entrance / exit delay, timer A.
Delayed B	Intrusion alarm with entrance / exit delay, timer B.
Delayed C	Intrusion alarm with entrance / exit delay, timer C. Setting of timers A, B, C – see Parameters tab. In the Parameters tab you can set for this reaction that the exit delay will be extended by an active detector with the delay C (e.g. for the time of opening of the garage gate).

Next delayed	Intrusion alarm. A detector provides the same exit delay as the delayed detectors in the same section. This detector will only provide the entrance delay if it is activated after a detector for which a delayed reaction has been set. If it is the first one to be activated, it will release an alarm immediately. This setting makes sense if a delayed detector is set in the same section.
Shortened exit A	Intrusion alarm with entrance / exit delay, timer A. The exit delay is shortened to 5 s after an activated detector goes standby.
Shortened exit B	Intrusion alarm with entrance / exit delay, timer B. The exit delay is shortened to 5 s after an activated detector goes standby.
Shortened exit C	Intrusion alarm with entrance / exit delay, timer C. The exit delay is shortened to 5 s after an activated detector goes standby.
Instant always	Instant intrusion alarm if set. Both EW and IW alarm warnings are activated together and immediately also during exit delay time.
Instant / Delayed A	The system reacts to triggering a detector (alarm, entrance delay) when partially set as an Instant zone, and when fully set as a Delayed A zone.
Instant confirmed	Instant intrusion alarm – see 8.4.3 Confirmed intrusion reaction below.
Delayed A confirmed	Intrusion alarm with an entry and exit delay, timer A – see 8.4.3 Confirmed intrusion reaction below.
Repeated instant	Instant intrusion alarm – see 8.4.3 Repeated reaction below.
Repeated delayed A	Intrusion alarm with an entry and exit delay, timer A – see 8.4.3 Repeated reaction below.
Tampering	Tamper alarm any time (the section does not need to be set).
24 hours	Immediate intrusion alarm (the section does not need to be set).
Silent Panic	Silent Panic alarm: 1) EW and IW not activated (see chapter 8.5 Types of alarms); 2) the keypad does not beep although otherwise it is set like this; 3) if the system can distinguish who triggered the Panic alarm (e.g. through a tag with adopted user's identity or entering of the panic code by the user), it does not send Panic SMS to this user.
Audible Panic	Audible panic alarm (the behaviour is the same as a Silent panic, the only difference is that an alarm is signalled by the used siren according to the table in chapter 8.5 Types of alarms).
Fire alarm	Fire alarm any time (the section does not need to be set).
Fire confirmation	Fire alarm any time (the section does not need to be set), see 8.4.3 Confirmed fire reaction below.
Fire instant	Fire alarm only if the respective section is set.
Gas	Gas leakage alarm any time (the section does not to be set).
Health troubles	Sends a health trouble report.
Flooding	Sends a flood alarm.
Set / Partial Set	Setting (partial setting) of a section. If the section is a common one, all sections that belong to it will be set at the same time. This reaction also has the Unset function.
Mute	Silencing of the internal siren with a subsequent report of the presence of a person in the building.
Report A / B / C / D	A special report is sent (special reports A, B, C and D are set in the Reports to Users tab), which may be accompanied by a voice message call. If saving of special reports in the event history is enabled, reports are also sent to the ARC.
Key-Box	A special reaction designed for sealed key in case of emergency, etc the opening of which will send a report to the ARC without activating the alarm with a siren.
Instant always	Instant zone reaction. If set, then based on activation, instant including EW and IW alarm warnings is activated also during exit delay time.
None	Without any impact for intrusion alarm; however, the device may be used to activate PG outputs.
None with no tamper	The system reacts to detector triggering by PG output control only. None of the alarm types are triggered (even a tamper alarm), fault detection is kept.

8.4.3 Limitation of false alarms

In installations with an increased risk of false alarms special reaction types can be used:

Confirmed intrusion reaction – if in a set section a detector with confirmed reaction is activated, the system only reports an unconfirmed alarm to the ARC and waits for confirmation by another detector. The alarm may be confirmed by any intrusion detector in a set section. In the Parameters tab you can define whether the confirmation can come from any set section or it must be from the same section. You can also set the time for which the system waits for confirmation by another detector in the Parameters tab (up to 60 min). If the alarm is not confirmed within the pre-determined period of time, no alarm is released. If a confirmed delayed reaction is set, activation of a detector only initiates sending of an unconfirmed alarm after expiration of the entrance delay. Confirmed reaction can only be used if a higher number of intrusion detectors are installed in the building (to enable confirming). This reaction is only available if the "Default" system profile is used.

Confirmed fire reaction – if a fire detector with this reaction is activated, only an unconfirmed fire alarm is reported to the ARC and the system waits for confirmation of the fire by another fire detector. In the Parameters tab you can define whether the confirmation can come from any section or it must be from the same section. The time period of waiting for confirmation of a fire alarm is set in the Parameters tab. If fire is not confirmed within the pre-determined period of time, no fire alarm is released. Confirmed reaction can only be used if a higher number of fire detectors are installed in the building (to enable confirming).

***Warning**: This function and its use have to be taken seriously in accordance with local requirements and norms.*

Repeated reaction – if a detector with this reaction type is activated, the system waits whether activation of the same detector will be repeated. In the Parameters tab you can set the time period for which the system waits for repeated activation and also the time for which the detector is disregarded. If activation of the detector is not repeated within the pre-set time period (adjustable from 6 to 120 s), the system will cancel the first activation. The repeated reaction is used in environment with an increased risk of occasional false alarms e.g. caused by rodents, small insects, drafts etc.

Three-strikes function (3x and STOP!) – all detectors with an activated alarm reaction of the intrusion and fire type are limited to three possible activations of the control panel during one monitoring period at the most. After three activations (on the fourth intrusion) a bypass is activated for the respective alarm input and the corresponding sensor is excluded from further activity. If these three activations occur during an alarm, three alarm SMS messages are generated altogether and then the detector is disabled. If these three activations occur in time intervals that are longer than the duration of an alarm, three alarm SMS messages are generated, three alarms are triggered and then the detector is disabled.
This function can be extended by the "Device autobypass" parameter, you can find it on the Parameters tab and the selection "3rd alarm" – now it can reach up to 3 activations from every device during all of a maximum of 3 alarms. It means that up to nine (3x3) alarm SMS messages can be sent. A bypass can be cancelled by unsetting and subsequently setting the section, then the detector is back in guarding mode again. The bypass for the fire and flooding reaction is also cancelled automatically on the next day at 12:00 (according to the parameter "Daily reset of device autobypass" on the Parameters tab). The bypass mechanism of 3x and stop is not applied to devices where the Panic reaction has been set. The number of triggered faults can be limited a similar way (see "Fault autobypass" on the Parameters tab).

Delayed report to ARC – according to the EN50131-1 norm requirement to reduce the number of false alarms caused by end user invalid operation of the system and security agency intervention. When enabled, an Internal alarm (sirens, keypad indication) will be triggered after the entrance delay has timed out, but the system waits for 30 s to send an alarm report to the ARC. A user has 15 s more to unset the system without triggering an alarm reported to the ARC. If he does it in time, nothing will be reported. This delay is only related to an alarm triggered by a delay zone. Other alarm types (instant, fire, tamper, etc..) are reported immediately with no delay regardless of this function.

8.5 Types of alarms

The main reason for the security system is to report events to its owner and users or a professional security agency to inform about threats. It could be intrusion by a burglar but also some environmental effect such as smoke, fire, gas leakage, flooding in the protected premises. Indication of every type of alarm can be different according to its cause. For sirens alarms are split into internal (IW) and external (EW).

In the following table is an overview of IW and EW outputs according to the type of alarms and section status:

Section status	Alarm type					System Settings – Parameters		Activates	
	Intrusion	Tampering	Audible Panic	Fire	24h./Flood	Siren IW during partial set	IW siren on case of tampering	EW	IW
Unset		X				*N/A*	NO		
		X				*N/A*	YES		X
			X			*N/A*	*N/A*	X	X
				X	X	*N/A*	*N/A*		X
Partially set		X				*N/A*	NO		
		X				*N/A*	YES		X
	X					YES	*N/A*		X
	X					NO	*N/A*		
			X			*N/A*	*N/A*	X	X
				X	X	*N/A*	*N/A*		X
Set	X	X	X	X	X	*N/A*	*N/A*	X	X

All types of system sirens sound with an intermittent tone (optional continuous or intermittent) and outdoor siren flashing is done by a red or blue light (flasher). Indication length is given by the alarm length time parameter in the control panel. Every siren has its own settings like alarm length limitation, thanks to this you can pre-set a shorter time of alarm indication by the external siren than by the internal one. Every alarm (except panic alarm) has a beginning and an end (expiration or cancelling by user) and with the cause of event it is recorded to the events with a time and date stamp.

On all system keypads, all alarms (except panic alarm) are indicated by red flashing of the backlit indication button with a continuous acoustic indication.

8.5.1 Intrusion alarm

It is a control panel alarm state which can be triggered by detectors with delay or instant reactions (and their variations) and it is valid for a partially or a fully set system. It is indicated by internal and external sirens see the table above. The alarm length is given by settings in the control panel system parameters. When an alarm expires keypads and sirens stop indication. When a user is authorized, it mutes the acoustic indication of all sirens and keypads but it doesn't cancel the system alarm state nor it's unsetting. It has to be performed as a following action by a control segment or the LCD keypad menu.

8.5.2 Tamper alarm

The control panel supervise all devices enrolled to the system regardless of the system status (set / unset). Most devices have a built-in tamper contact for the detection of opening their cover and tearing from the wall. An activation triggers a tamper alarm and it is indicated by an internal siren (according to the parameter Siren IW when tamper triggered) in an unset system, but in a set system by both sirens (internal and external as well) see table above. A tamper alarm can also be the loss of BUS devices (by short circuit for instance), or by a code breaking attempt (10x) on the keypad, remotely and via a phone call using DTMF, an SMS message or using the MyJABLOTRON application (WEB + smartphone).

8.5.3 Fire alarm

A fire alarm is triggered by triggering the detectors with a set Fire reaction. The following detectors are all taken as fire detectors (smoke, high temperature, detector of combustible gases or detector of poisonous CO). A fire alarm is indicated by internal sirens when the system is unset or set partially, and when the system is set fully, then it is indicated by internal and external sirens too.

There are different types of alarms such as:

1. **Fire** – basic reaction for all fire detectors.
2. **Fire confirmed** – option for higher reliability. A minimum of 2 fire detectors have to be installed in every room with the same settings.
3. **Fire instant** – used especially for premises where there is smoke normally (restaurants, welding shops etc.) and detection is only performed when the system is set.
4. **Gas** – A special reaction of fire detectors with the identification of combustible, poisonous or explosive gas for specific reporting of this event to the ARC.

8.5.4 Panic alarm

A panic alarm is a special event which can be triggered as 2 different events, **Silent panic** and **Audible panic**. Each of them has different behaviour.

1. **Silent panic** – a special event not assigned to a group of intrusion alarms, which would be indicated by a siren or keypad. A silent panic has no timer and there is no end to this event. So it cannot be used for the status control of a PG output. It is only for triggering a silent panic alarm and call help under duress without the awareness of the attacker. A silent panic can be triggered from a particular (hidden or portable button) panic button. Usually by a button pre-set to a silent panic, by a combination of keys on the remote, by a keypad with a special control segment pre-set to a silent panic (in this case a panic alarm can be delayed with an optional timer), by pressing the button on the internal siren, by an input on the BUS module meant for wired devices or by entering a special code for silent panic triggering. A silent panic can also be triggered when Duress access control is performed (see chapter 9.10 System control by Duress access control) where the standard user code is modified.
2. **Audible panic** – is a usual alarm event with a beginning and an end so it is indicated acoustically by siren and keypad. It can be used for the status control of a PG output. And mostly it is used for triggering a panic alarm with an optical indication requirement or for blocking electric door locks etc. An audible panic alarm can be triggered from a particular (hidden or portable button) panic button. Usually by a button pre-set to a silent panic, by a pre-set key on the remote control, by a keypad with a special control segment pre-set to a silent panic (in this case a panic alarm can be delayed with an optional timer), by pressing the button on the internal siren, by an input on the BUS module meant for wired devices.

Caution: *Both Panic alarm types are specific thanks to the fact that they could be triggered repeatedly with no limitation or automatic blocking.*

8.5.5 24hr alarm

Detectors which ensure permanent protection regardless of the system status (set or unset) can have a pre-set reaction of 24 hours or flooding. This type of alarm is assigned to the group of intrusion alarms, but regardless of this fact it can be triggered when the system is unset. According to the system status an alarm is indicated by internal and external sirens as well, see the table above. Alarm reporting is performed the same way as other alarms.

8.5.6 Alarm cancelling

When an alarm in the system is triggered, its duration is counted by the timer meant for alarm length, see F-Link, Parameters tab. If there is an authorized user present in the protected premises, the alarm can be cancelled in time. Alarm cancelling causes immediate silencing of all sirens and terminates alarm voice reporting to all pre-set telephone numbers. The way of alarm cancelling depends on the parameter in the Parameters tab:

Unsetting cancels alarm

- If enabled, the currently running alarm is cancelled by unsetting the section with an alarm or after authorization on an LCD keypad and by pressing the option “Cancel warning indication”.
- If disabled, a currently running alarm can be cancelled only by valid user authorization with access rights to that section with no requirement to unset that section.

8.6 System faults

A fault is a warning signal from the system which indicates some abnormal state of the control panel, communication or devices. The problem can be related to radio, GSM and LAN communication, masking the detectors (with an antimasking function), problems with power (mains power or battery) or the back-up power supply. Fault(s) is/are optically indicated on system keypads by the backlit indication button. Fault reporting is

taken from every source and with the 4th fault activation the source of the fault is bypassed which means that the 4th fault is not reported. This automatic fault blocking is an optional parameter, see the Parameters tab. If enabled, no faults are counted and there is no limitation of their reporting. The parameter is not available when the "Default" system profile is set.

In the following table there is an overview of general system faults:

Fault source	Cause
Control panel	Mains power disconnected more than 30 minutes
	Faulty or low back-up battery in the control panel
Communicator	Loss of LAN connection, or GSM signal minimum 15 minutes
	Event(s) not delivered to the ARC in a given time
Radio module	Jamming of 868 MHz radio band
	BUS communication loss
Keypads	Radio or BUS communication loss (see chapter 8.7 Fault caused by loss of a device below)
Sirens	
Modules	
Detectors	
	Masking of motion detectors (Antimasking) Internal detector fault (gas leakage detector) Fault cause by reducing IR ray intensity (infra barrier)

8.7 Fault caused by loss of a device

Every device (BUS or wireless) in the system is supervised by the control panel when the Supervision parameter is enabled (see Parameters tab, Supervision column) and communication with the control panel is lost (no response within a pre-set time) then the system triggers the event "Fault activation" and according to the "Loss of a BUS device" it can be followed by a tamper alarm. It is optional and can be triggered when the radio module detects RF jamming or some kind of RF interference which takes a minimum 30 s according to the detection level set in the radio module. And it can also trigger a tamper alarm when a short circuit occurs on the system BUS which avoids proper the communication of BUS devices. The communication time-out is a fixed time and cannot be changed. For BUS devices it is 8 s and for wireless 120 min from the last communication.

The **"Supervision"** function is optional for almost all wireless devices meant for guarding (detectors, sirens, keypads), for some of them it is disabled completely (remote controls and automation appliances) and for instance for some BUS devices it is always enabled with no option to be disabled.

An option which changes the control panel reaction to the loss of BUS devices is called **"Loss of a BUS device"**, see F-Link software, Parameters tab. It offers the following options:

- **Fault** – the control panel always processes the loss of a device on the BUS or a short circuit of the BUS just as a Fault.
- **Tamper always** – the control panel processes the loss of a device on the BUS or a short circuit of the BUS as a tamper alarm always when it occurs. If the radio module has RF jamming detection allowed and it is really detected, then it also triggers a tamper alarm. A tamper alarm is also followed by a fault and when the fault is restored, the system cancels the tamper alarm as well.
- **Tamper after confirmation** – the control panel processes the loss of the first device as a fault and if within a pre-set time given by the parameter "Period of waiting for alarm confirmation" another device loss occurs, then the system confirms it and triggers a tamper alarm. When the fault of all the lost devices is restored, the system cancels the fault and tamper alarm.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

9 System control options

The security system can be controlled a few ways. Basic control options are local or remote. Other options are mentioned by the following table:

Type	Way/mode	Device	Condition	Control description
Local	Keypad with control segment	JA-114E, JA-113E, JA-154E, JA-153E, JA-123E, JA-121E	The JA-11xR radio module for wireless devices	Operation can be performed after user authorization and pressing a specific control segment or also via the LCD keypad menu.
	Keypad	JA-110E, JA-150E	The JA-11xR radio module for wireless devices	Operation can be performed after user authorization and pressing a specific function button or also via the LCD keypad menu.
	RFID reader with control segment	JA-112E, JA-152E; JA-122E, JA-120E (PC control only)	The JA-11xR radio module for wireless devices	Operation can be performed after user authorization using an RFID tag and pressing a specific control segment.
	Remote control	JA-15xJ, JA-16xJ, JA-18xJ	The JA-11xR radio module for wireless devices	Setting and unsetting by pressing a pre-set remote control button.
	Calendar	Up to 64 calendar actions		Every calendar action has options to select: event, time of its performance, day of the week. It can control sections and PG outputs. PG outputs can be blocked.
	JA-100-Link (F-Link) software	PC with Windows	USB cable	Using a virtual keypad sections can be controlled and also PG outputs after authorization.
	Control module	JA-111H-AD TRB and JA-121T	BUS	System can be controlled using an arbitrary external device (by module wired input activation or data communication).
Remote	Voice menu	Telephone	GSM communicator	Calling the system telephone number and control system by DTMF tones after authorization.
	SMS message	Cell phone	GSM communicator	Authorized command for setting or unsetting sections and also control of PG outputs.
	Dialling in from authorized telephone number	Telephone (PG control only)	GSM communicator	For every authorized telephone number one specific PG output can be controlled.
	MyJABLOTRON web app	PC	JABLOTRON Security SIM card in GSM communicator	After authorization sections and PG outputs can be controlled, photos taken by photo-devices browsed thermometers and electricity meters.
	MyJABLOTRON smartphone app	Smart phone or tablet	JABLOTRON Security SIM card in GSM communicator	After authorization sections and PG outputs can be controlled, photos taken by photo-devices browsed, thermometers and electricity meters.
	JA-100-Link (F-Link) software	PC with Windows	GSM or LAN communicator	Sections and PG outputs can be controlled by virtual keypad after authorization.

All mentioned ways can be used for system control (setting, partial setting, unsetting) for PG output control (ON, OFF, timing). The only exceptions are JA-122E, JA-120E outdoor RFID readers and dialling in from an authorized telephone number which can control a PG output.

9.1 Way of authorization

Authorization is the key factor to control the system and to verify if the user is really authorized for operation. According to the authorization procedure the system decides if the user is authorized to control the required sections, PG outputs or if he can only browse the system status and history log using an LCD keypad menu. Every user can have the following options assigned to authorize himself:

- Access code (4, 6, or 8-digit number with or without a prefix).
- RFID card/tag (up to 2 positions for RFID identification elements).
- Telephone number for authorization during remote accessing by telephone call or by SMS.

To adjust the security level the authorization level can be pre-set at the following 3 levels:

1. **Standard** – authorization is performed by applying an RFID card or entering a valid access code.
2. **Card confirmation with a code** – a user code confirmed by an RFID card is required to be applied (their order doesn't matter). If users have either cards or codes, they will authorize themselves according to the Standard option so authorization by one of them is enough. When remote access is performed, the telephone number is verified first and as confirmation it is obligatory to enter a valid access code. In this case double authorization can be used for some users with a higher level of supervision and for some just standard authorization can be required.
3. **Double authorization** – entering a user code and using an RFID card will accomplish valid authorization (regardless of the order of authorization). During remote access the telephone number is always verified and entry of a valid access code as well. F-Link monitors whether a code and a card are assigned to a user in the Users tab (otherwise F-Link won't allow you to save the configuration).

Caution: *Confirmation of a user code by an RFID card reduces the risk of unauthorized operation or overcoming the system by a third party.*

9.2 System control by keypad

9.2.1 System control from segment keypads

The best way to control a security system and its monitoring is using a system keypad where thanks to a colour LED indicator of the main control button faults and alarms can be checked and using other control segments the status of sections and PG outputs can be controlled and also system options such as alarm memory indication, triggering a panic alarm or health troubles. Using an LCD keypad, you can browse through the internal menu to get information about faults, events, active or bypassed detectors or detectors preventing the system being set – everything after particular authorization. No authorization = no access to the keypad menu and according to the individual keypad settings visibility of particular segments can be supressed and it protects the system against unauthorised operation.

Setting and unsetting the sections is a very basic function of the system keypad. The system can be set fully or partially. The system can be controlled from the LCD keypad menu or by control segments. Using segments, you can perform setting according to their settings; fully or partially and with authorization (who performed setting a specific section is recorded in the event log) or also without it (no code required and in the event log it is not specified who set the system). For unsetting the system authorization is always required so in the event log it is recorded who unset the system.

The setting procedure can be performed in the following two ways:

1. **Full section setting before you leave the protected premises** (no one else in the premises)**:**

For system control from a keypad placed in protected premises it is necessary to ensure an exit and entrance path protected by detectors with a delayed reaction. Delay and Next delay zones are not included in guarding immediately after section setting but zones with an Instant reaction are included. The user has to be able to leave the protected premises after system setting before the exit delay time expires. And when the entrance delay is triggered by a delay zone the user has to be able go through the entrance path to the keypad from which to perform system unsetting. If the user doesn't unset the section in time (entrance time expired), the system triggers an alarm in the delayed zone. If intrusion is performed by a different path than the entrance path, the system triggers an alarm in an instant zone – it activates the siren immediately. A fully set system/section is indicated by a red coloured control segment or by a full square with the number of the section on the LCD keypad.

2. **Partial setting, user stays in the premises:**

When the system is set partially, the user stays in the protected premises and only perimeter protection is included for guarding (it ensures free movement inside the premises). There are 2 variants of control:

a) Control from a keypad placed inside the protected premises with perimeter protection (entrance hall, etc.). All detectors in the entrance hall have to be pre-set to a Delay reaction to ensure that when the system is set their activation triggers some time for entry to unset the system.

b) Control from a keypad placed outside protected premises with perimeter protection (internal hall, stairs, bedroom, etc.). This variant doesn't allow the entrance of any person without instant alarm triggering. The premises can be entered by previous unsetting by remote control, by voice menu, by SMS or via the MyJABLOTRON app. Detectors are pre-set to an Instant / Delay A reaction in this case.

Partial setting is indicated by a yellow colour on the segment or by a square around the digit on the LCD keypad display.

System control by keypad – procedure:

The system offers a few system profiles which comply with various norm requirements and it also changes the keypad´s behaviour and of course the method of their control. The system can be controlled in two ways:

1. **Variant 1 of system control (valid for all profiles)**

   Setting the system:

   Using **variant 1 requires your authorization first** because not all segments have to show their status according to their settings without authorization!

   1. Applying the RFID card / tag or entering the code performs authorization (when a code and card are both required then their order doesn't matter).
   2. An unset section is indicated by a green LED light on the left segment side.
   3. Pressing the red segment button on the right side gives a request for section setting. More requests can be selected considering the number of used segments.
   4. If after a selection the red or yellow LED flashing (8 s) remains, the system detects an obstacle preventing the setting (see chapter 9.11 Obstacles preventing setting the system).
   5. Successful setting or partial setting is confirmed by red or yellow segment LED lights.

   Unsetting the system:

   Authorization is required to control the system from a keypad **for variant 1**!

   1. Applying the RFID card / tag or entering a code performs authorization (when a code and card are both required then their order doesn't matter).
   2. A set section is indicated by a red or yellow LED light on the right segment side. When intrusion of protected premises is detected it triggers an entrance delay indicated by rapid flashing of the green LED.
   3. Pressing the green button (or several buttons gradually) on the left side gives a request for section unsetting.
   4. Successful unsetting is confirmed by green segment LED lights.
   5. If after unsetting the section the red LED remains rapidly flashing, it indicates the alarm memory in the section. Cancelling this indication can be performed by further pressing of the green button on the segment with authorization to cancel this indication or using the LCD keypad menu and selecting the option "Cancel warning indication".

2. **Variant 2 of system control ("Default" profile)**

   Setting the system:

   The way of controlling is based on the procedure: "select the required action and authorize yourself".

   1. An unset section is indicated by a green LED light on the left segment side.
   2. Pressing the red segment button on the right side gives a request for section setting. More requests can be selected considering the number of used segments.
   3. If the authorization is required for setting the section, a red (full setting) or yellow (partial setting) LED indicates the time-out when authorization is expected by slow flashing (8 s).
   4. Applying the RFID card / tag or entering a code performs authorization (when a code and card are both required then their order doesn't matter).
   5. If after a selection the red or yellow LED flashing (8 s) remains, the system detects an obstacle preventing the setting (see chapter 9.11 Obstacles preventing setting the system).
   6. Successful setting or partial setting is confirmed by red or yellow segment LED lights.

Unsetting the system:

1. A set section is indicated by a red or yellow LED light on the right segment side. When intrusion of the protected premises is detected it triggers an entrance delay indicated by rapid flashing of the specific LED.
2. Pressing the green button (or more buttons gradually) on the left side gives a request for section unsetting and the segment indicates the time-out when authorization is expected by slow flashing.
3. Applying the RFID card / tag or entering a code performs authorization (when a code and card are both required then their order doesn't matter).
4. Successful unsetting is confirmed by green segment LED lights.
5. If after unsetting the section the red LED remains rapidly flashing, it indicates the alarm memory in the section. Cancelling this indication can be performed by further pressing of the green button on the segment with authorization to cancel this indication or using the LCD keypad menu and selecting the option "Cancel warning indication".

9.2.2 System control from the JA-110E and JA-150E keypads

The best way to control a security system and its monitoring is using a system keypad where thanks to a colour LED system status indicator of the main control button faults and alarms can be checked and using other functional buttons the status of sections and PG outputs can be controlled and also system options such as alarm memory indication, triggering a panic alarm or health troubles. Using a keypad you can browse through the internal menu to get information about faults, events, active or bypassed detectors or detectors preventing the system being set – everything after particular authorization. No authorization = no access to the keypad menu and according to the individual keypad settings visibility of menu items can be supressed and it protects the system against unauthorised operation.

Setting and unsetting the sections is a very basic function of the system keypad. The system can be set fully or partially. Control can be comfortably performed in several ways:

1. By functional buttons – pressing the key can set fully or only partially or partially and fully. Setting can be followed by authorization (in the history is recorded who set which section) or without authorization (no code required so in the history is not specified who performed section setting). When unsetting the system by functional buttons authorization is always required so it records who performed the unsetting in the control panel memory.
2. From the keypad menu – press the "*" key after authorization and set partially, fully or unset.
3. By authorization only – considering the settings can be set fully (only) and unset by only authorization by a code or by applying the RFID card/tag. To enter the keypad menu press the "*" key before you authorize yourself.

The setting procedure:

1. Full section setting before you leave the protected premises (no one else in the premises):

A fully set system is indicated by a red coloured functional button or a fully highlighted number of the section on the keypad LCD display during control from the menu.

For system control from a keypad placed in protected premises it is necessary to ensure an exit and entrance path protected by detectors with a delayed reaction. Delay and Next delay zones are not included in guarding immediately after section setting but zones with an Instant reaction are included. The user has to be able to leave the protected premises after system setting before the exit delay time expires. And when the entrance delay is triggered by a delay zone the user has to be able go through the entrance path to the keypad from which to perform system unsetting. If the user doesn´t unset the section in time (entrance time expired), the system triggers an alarm in the delayed zone. If intrusion is performed by a different path than the entrance path, the system triggers an alarm in an instant zone – it activates the siren immediately.

2. Partial setting, user stays in the premises:

A partially set system is indicated by a yellow coloured functional button or a fully highlighted number of the section on the keypad LCD display during control from the menu.

When the system is set partially, the user stays in the protected premises and only perimeter protection is included for guarding (it ensures free movement inside the premises). There are 2 variants of control:

1. Control from a keypad placed inside the protected premises with perimeter protection (entrance hall, etc.). All detectors in the entrance hall have to be pre-set to a Delay reaction to ensure that when the system is set their activation triggers some time for entry to unset the system.
2. Control from a keypad placed outside protected premises with perimeter protection (internal hall, stairs, bedroom, etc.). This variant doesn´t allow the entrance of any person without instant alarm triggering.

The premises can be entered by previous unsetting by remote controller, when supplementary GSM module connected then by voice menu or by SMS. Detectors are pre-set to an Instant / Delay reaction in this case.

System control by keypad - procedure:

The system offers a few system profiles which comply with various norm requirements and it also changes the keypad´s behaviour and of course the method of their control.

Setting the system:

1. An unset section is indicated by a functional button which lights green.
2. Pressing the functional button makes a request for section setting. More requests can be selected considering the number of used functional buttons.
3. If the authorization is required for setting the section, a red (full setting) or yellow (partial setting) colour of the functional button indicates the time-out when authorization is expected by slow flashing (8 s).
4. Applying the RFID card / tag or entering a code performs authorization (when a code and card are both required then their order doesn´t matter).
5. If after a selection the functional button flashing red or yellow (8 s) remains, the system detects an obstacle preventing setting (see chapter 9.11 Obstacles preventing setting the system).
6. Successful setting or partial setting is confirmed by permanent lighting of the red or yellow coloured functional button.

Unsetting the system:

1. A set section is indicated by a functional button which lights red or yellow. When intrusion of the protected premises is detected it triggers an entrance delay indicated by rapid flashing of the specific functional button.
2. Pressing the desired functional button (or more buttons gradually) makes a request for section unsetting and the functional button indicates expected authorization by slow flashing.
3. Applying the RFID card / tag or entering a code performs authorization (when a code and card are both required then their order doesn´t matter).
4. Successful unsetting is confirmed by the permanent lighting of the green coloured functional button.
5. If after unsetting the section the red functional button remains rapidly flashing, it indicates the alarm memory in the section. Cancelling this indication can be performed by further pressing of this button with authorization to cancel the alarm memory or using the LCD keypad menu and selecting the option “Cancel warning indication”.

Keypad backlit indication button – overview of statuses:

Button lights green ON	Normal operation. Sections controlled from keypad are OK with no faults.
Button lights yellow ON	Normal operation and in some of the controlled sections a fault has been detected. From the LCD keypad menu, you can get more detailed information after user authorization according to their access rights. If the fault is followed by a rotating JABLOTRON logo on the LCD keypad it represents a fault of radio communication between the control panel and the keypad.
Button lights red ON	Keypad in BOOT mode, during a FW upgrade.
Button flashes green (2 Hz)	Authorization performed, the user can change the system status from segments or browse the menu of the LCD keypad. Authorization time-out takes 8 s from the last key pressing or cancel it by pressing ESC.
Button flashes yellow (8 Hz)	Unsuccessful setting warning indication.
Button flashes red (8 Hz)	Indication of a currently triggered alarm in a specific section on the keypad. The type of alarm, name of the section where an alarm has been triggered and the source of the triggered alarm are visible on the LCD keypad.
Flashes alternate red/yellow	Triggered alarm with an active fault.
Flashes alternate green/red	Authorization with a currently triggered alarm or an alarm memory.
Flashes alternate green/yellow	Authorization with an active fault.
Button flashes yellow (2x every 2 s)	Programming / Service mode. All control segment indication is disabled for users and the Administrator keypad menu too. The keypad menu is only available for a service technician until the PC is connected to the control panel.
Button flashes red (2x every 2 s)	Alarm memory indication.
Button flashes green (2x every 2 s)	Maintenance mode. Control segment indication is disabled for sections switched to the Maintenance mode.

Button flashes yellow (1x every 2 s)	Fault indication on keypad in sleep mode (valid for EN50131-1 profile only).
Button flashes red (1x every 2 s)	Alarm memory indication on keypad in sleep mode (valid for EN50131-1 profile only).
No indication	Keypad in sleep mode.

Keypad control segment optical indication overview:

Segment lights green	Section status is Unset or PG output OFF.
Segment flashes green (4 Hz)	Entrance delay running and the system waits for authorization to be unset.
Segment lights yellow	Section status is Partially set.
Segment lights red	Section status is Set or PG output ON.
Segment flashes yellow (4 Hz)	System expects authorization when partially set or it reports a fault during partial setting.
Segment flashes yellow (8 Hz)	Unsuccessful setting warning indication.
Segment flashes red (4 Hz)	System waits for authorization during setting or it reports a problem during setting.
Segment flashes red (8 Hz)	Alarm memory indication is indicated until it is cancelled.
Segment does not light at all	Switched off; Service or Maintenance mode; or blocked section after alarm.

9.3 System control by remote control

If there is a requirement to control the system before access to the protected premises (arriving by car at the garage) or building to be protected just by detectors with an instant reaction, it ensures no one can unset the system from a keypad inside the protected premises (no entrance path), this can be realized by remote control before you access the building. It requires the JA-11xR radio module to be enrolled to the system for communication with wireless devices. It has to be placed at the right place to ensure reliable communication with the remote in addition to the required working distance.

When using remote controls (JA-15xJ, JA-16xJ), its buttons behave the same way as the control segments of a keypad. Every button can control a selected section (the right one always sets and the left one always unsets). Remote controls respect rules on how the system should be set, so with any obstacles preventing the setting it will not be possible to set the system.

Keypad control segments and bidirectional remote controls have the same way of indication by a three colour LED. Descriptions of individual statuses are mentioned in the following table:

Bidirectional remote controls (JA-15xJ) status indication – shown after being pressed:

LED lights green	Section status Unset or PG output OFF
LED lights yellow	Section status Partially set
LED lights red	Section status Set or PG output ON
LED flashes red	There is an obstacle in the section which prevents setting
LED flashes yellow	Command status unknown (fault of communication, out of communication range etc.)

Using a unidirectional remote control (JA-16xJ, JA-18xJ) this controls the system the same way and indicates by its LED that button pressing is indicated and the command sent. There is no feedback from the control panel and the user should use a different type of status indication to confirm a section status change such as siren chirps, other optical indications or SMS reports about setting / unsetting.

9.4 System control by a calendar

Automatic system control can be performed by the control panel's internal calendar. The calendar can be pre-set to do up to 64 calendar actions – sections and PG outputs control. Via the calendar you can select the exact date of the service annual check which is independent on the "Service requirement" option in the Parameters tab.

For every action it is possible to pre-set the day of the week and month and month of the year when it will be performed. An action can therefore be set from one particular day of the year to a regular repetition on certain days (e.g. weekly or monthly). On the selected days, up to 4 times can be set when a calendar action is performed, or repeating at regular intervals can be chosen. The interval repetition can be additionally specified in a time "from–to". A typical application is the automatic setting of a section in shops, partial setting of a building at night or lights control in the night. Every automatic event is recorded in the history log with the name of the source being "Calendar".

Calendar control options related to guarding:

Unset	Unset pre-set section from any guarding level (fully or partially set).
Set partially	It sets pre-set section(s) partially and starts with an exit beeping time of 180 s (regardless of how long an exit time has been set in the control panel), within this time all alarm zones behave like delayed ones. A prolonged time for acoustic exit indication is meant for warning users who are in the protected premises to inform them about the fact that the system has been set partially by an automatic timer. Partial setting is not usually acoustically indicated (See Parameters tab to enable it). The control panel fully respects all ways of setting and checking the systems ready to be set rules.
Set	It sets pre-set section(s) and starts with an exit beeping time of 180 s (regardless of how long the exit time has been set in the control panel), within this time all alarm zones behave like a delayed zone. A prolonged time of acoustic exit indication is meant for warning users who is in the protected premises to inform them about the fact that the system has been set by an automatic timer. During this time the user has to go to the system keypad immediately and unset the section in the usual way or leave the protected premises. If he would ignore this warning and stays in the building and keeps moving then an alarm will be triggered. The control panel fully respects all ways of setting and checking the systems ready to be set rules.
Set immediately	It sets pre-set section(s) immediately without an exit delay or any acoustic indication. The system is set immediately so no movement is possible in the protected premises. If someone would keep moving in the premises after self-setting performance then an alarm would be triggered in the set section(s). The option is for fast and silent setting with no warning. The control panel fully respects all ways of setting and checking the systems ready to be set rules.
Set partially now	It sets pre-set section(s) partially and immediately without an exit delay or any acoustic indication. The system is set immediately in the pre-set time. The option is for fast and silent setting with no warning. The control panel fully respects all ways of setting and checking the systems ready to be set rules.
Set always	It sets pre-set section(s) and starts with an exit beeping time of 180 s (regardless of how long the exit time has been set in the control panel), within this time all alarm zones behave like a delayed zone. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
Always set partially	It sets pre-set section(s) partially and starts with an exit beeping time of 180 s (regardless of how long the exit time has been set in the control panel), within this time all alarm zones behave like a delayed zone. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
Always set immediately	It sets pre-set section(s) immediately without an exit delay or any acoustic indication. The system is set immediately so no movement is possible in the protected premises. The option is for fast and silent setting with no warning. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
Always set partially and immediately	It sets pre-set section(s) partially and immediately without an exit delay or any acoustic indication. The system is set immediately in a pre-set time. The option is for fast and silent setting with no warning. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
No	No control function pre-set.

PG output control options using calendar:

Activate PG	Activates programmable output(s) if they are not blocked (for instance by calendar, device or section).
Deactivate PG	Disable programmable PG outputs.
Block PG	Blocks pre-set PG outputs. Those outputs won't be possible to switch on at all until it will be unblocked by the calendar action "Unblock PG". Entering or leaving service mode don't unblock it.
Unblock PG	Unblocks pre-set PG output blocking.
No	No blocking function pre-set.
Service requirement	In a pre-set time, the "System requires service check" event is triggered in the system, which is, together with the Information icon, displayed on keypads with an LCD screen.

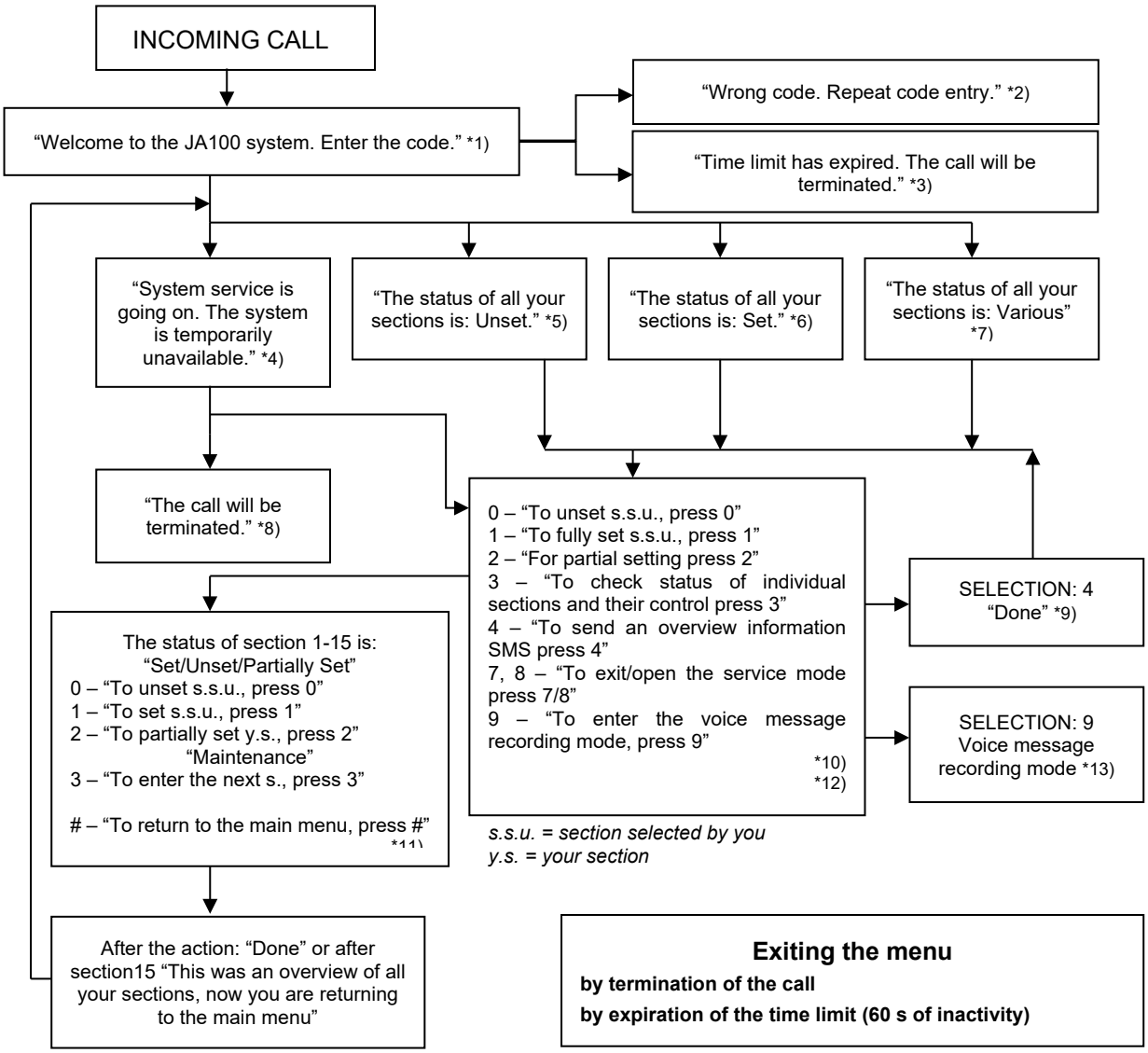
Function blocking action by the calendar: Every calendar action can be blocked by selected PG outputs. Blocking means: when a PG output is activated then a specific action won't be performed for a predefined time.

9.5 System control via communicator voice menu (GSM)

If the JA-19xY-zzzz GSM communicator is installed in the control panel, the security system can be controlled remotely thanks to the implemented voice menu and DTMF tones on the caller's cell phone. By calling to the used SIM card telephone number the system picks up the call after a pre-set number of rings (default is 3 rings), the control panel plays an introduction voice message and according to the settings maybe require a valid code entry. The caller has to authorize himself by his access code. When the code is successfully verified then the system tells you the status of the whole system and according to caller authorization offers other control options. The parameter "No code for voice menu and SMS" in the Communication tab the user can be authorized according to a pre-set telephone number stored in the Users list and then the code doesn't have to be required. The status of a section can be controlled via the voice menu, entering and leaving service mode and recording voice messages with the names of individual sections and special reports. Control of PG outputs is not possible via the voice menu.

Caution: *Make sure nobody is present in the protected premises before you set the system remotely.*

Voice menu overview:



*1) Answers after 3 ringing impulses. The number of ringing impulses until answering (1.10) is adjustable in the Communication tab and the tab of the respective communicator where entry in the voice menu without code can be allowed.
*2) Wrong code entry. After the third wrong entry the call will be terminated.
*3) 60 s time limit for code entry. Every 5s the "Enter code" request is repeated.
*4) The voice menu cannot be used during service.
*5) All sections that can be controlled on the basis of the authorization are unset.
*6) All sections that can be controlled on the basis of the authorization are set.
*7) The sections that can be controlled on the basis of the authorization are in various statuses.
*8) Valid for all authorizations except ARC / Service.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

*9) After sending of an INFO-SMS to the caller's number.
*10) Points in the menu that do not make sense are skipped (e.g. if everything is set, the selection 1, 2, 3 is not applicable).
*11) The menu is adapted to the current status of the section.
*12) If the user has been authorized with the service code, selection 9 is possible – "For the voice message recording mode press 9".
*13) Voice message recording mode **SELECTION 9**:
0 – "To record the installation name, press 0." and then "Press star (*)".
1 – "To record section names, press 1", then enter the number of section that you want to record and then "Press star (*)".
2 (3, 4, 5) – "To record messages of report A (B, C, D), press 2 (3, 4, 5)" and then "Press star (*)".
9 – "To delete all recorded messages, press 9".
– "To return to the main menu, press #".

Notes:

- 1 – "You are not authorized for this selection" – always if the user is not authorized to handle a section or check status.
- 2 – "Required report of an important message, the call will be terminated in 30 seconds" – reports / important messages to ARM have priority over the ongoing voice menu.
- Entry in the recording mode is indicated with a beep. A recorded message is replayed for listening immediately after recording.
- If you are not satisfied with the record, you can select re-recording immediately.
- It is suitable to start recording immediately after the beep signal and to press the end character* immediately after the end of your recording.
- The installation name may take 40 s at the most. Every other message may be 20 s long at the most.

9.6 SMS commands

If the JA-19xY GSM communicator is installed in the control panel, the system can be controlled with SMS commands. SMS commands can be used to control the setting statuses of individual sections or the whole system (setting, unsetting), or inquire about their statuses. PG outputs can be also controlled via the SMS commands. There are no factory commands to control PG outputs, it is necessary to set them first. The texts of the commands cannot be changed, except commands to control PG outputs

Command structure:

ppp*cccc_command

where: **ppp** is the position number of the user code (only if a code with a prefix is used);

***** is a separator (* is only necessary if a code with a prefix is used);

cccc is a user code;

_ is a separating gap (empty character);

command is the execution command (see list of commands below).

Query commands:

Information about the system status can also be obtained with the use of the following commands;

DINFO, STATUS, COM and GSM

Control command:

The control of setting the **system** as a whole or just its individual **sections** can be generated with the use of the following commands:

SET, UNSET, or SET x x x, UNSET x x x, where x are numbers of sections separated by a space.

The control commands for the control of **PG outputs** are pre-set by the manufacturer as **On PG output x** (x = 1 – 128).

Caution: *If control commands include accented diacritics (like with the languages GR and RU), then the Diacritics parameter on the Communication tab should be enabled for correct and reliable functioning. It is also necessary to mind small and capital letters when diacritics are enabled. With usual characters size doesn't matter.*

Commands overview:

Control command	Authorization	Answer (specimen)	Note
DINFO (basic information about the installation)	Service, Administrator	JABLOTRON: TYPE: JA-103K, SN: 14004026532523, SW: LJ60418, HW: LJ16117, RC: C5U6G-215CP-D2A6, GSM: 90%, GPRS: Ok, LAN: off Time 17:01 22.7.	Installation name as the Initial setup tab Control panel type Serial number Firmware version Hardware version Registration code of GSM communicator GSM signal, GPRS data availability LAN connection status (OK or OFF) Time and date of handing over the SMS to the GSM network
STATUS (status of sections)	Service, Administrator, User (If the user only has access to some sections, the status of the sections that are accessible for him/her will be returned)	JABLOTRON: Status: Section 1: Unset; Section 2: Set; Section 3: Unset; Section 4: Set, Error; Section 5: Set; Section 6: Set; Section 7: Unset; Section 8: Unset; GSM: 90%; Time 17:01 22.7.	Installation name as the Initial setup tab Status: Name and status of Section 1 Name and status of Section 2 Name and status of Section 3 Name and status of Section 4 Name and status of Section 5 Name and status of Section 6 Name and status of Section 7 Name and status of Section 8 GSM signal quality Time and date of handing over the SMS to the GSM network
COM (info about communication)	Service	JABLOTRON: GSM: 90%, DATA: ok, CELLID: 44905, OPID: 23003, LAN: ok, MAC: hh:hh:hh:hh:hh:hh, ARC: 1:ok, 2:ok, 3:off, 4:ok, 5:off, Time 17:01 22.7.	Installation name as the Initial setup tab GSM signal quality, GPRS data availability Number of the cell and operator providing the GSM connection LAN connection status and MAC address Activation status of transmissions to individual possible ARC's Time and date of handing over the SMS to the GSM network
GSM (restart GSM)	Service, Administrator, User	JABLOTRON: SMS processed OK: GSM; Time 17:01 22.7.	Installation name as the Initial setup tab Confirmation of SMS delivery (before restart) Time and date of handing over the SMS to the GSM network
SET (control of the whole system)	(According to the used code)	JABLOTRON: Status: Section 1: Set; Section 2: Set; Section 3: Set; Section 4: Set, Error; Section 5: Set; Section 6: Set; Section 7:Bypassed while being set, Section 8: Bypassed while being set; GSM: 90%; Time 17:01 22.7.	Installation name as the Initial setup tab Status: Name and status of Section 1 Name and status of Section 2 Name and status of Section 3 Name and status of Section 4 Name and status of Section 5 Name and status of Section 6 Name and status of Section 7 Name and status of Section 8 GSM signal quality Time and date of handing over the SMS to the GSM network
UNSET (control of the whole system)	(According to the used code)	JABLOTRON: Status: Section 1: Unset; Section 2: Unset;	Installation name as the Initial setup tab Status: Name and status of Section 1 Name and status of Section 2

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

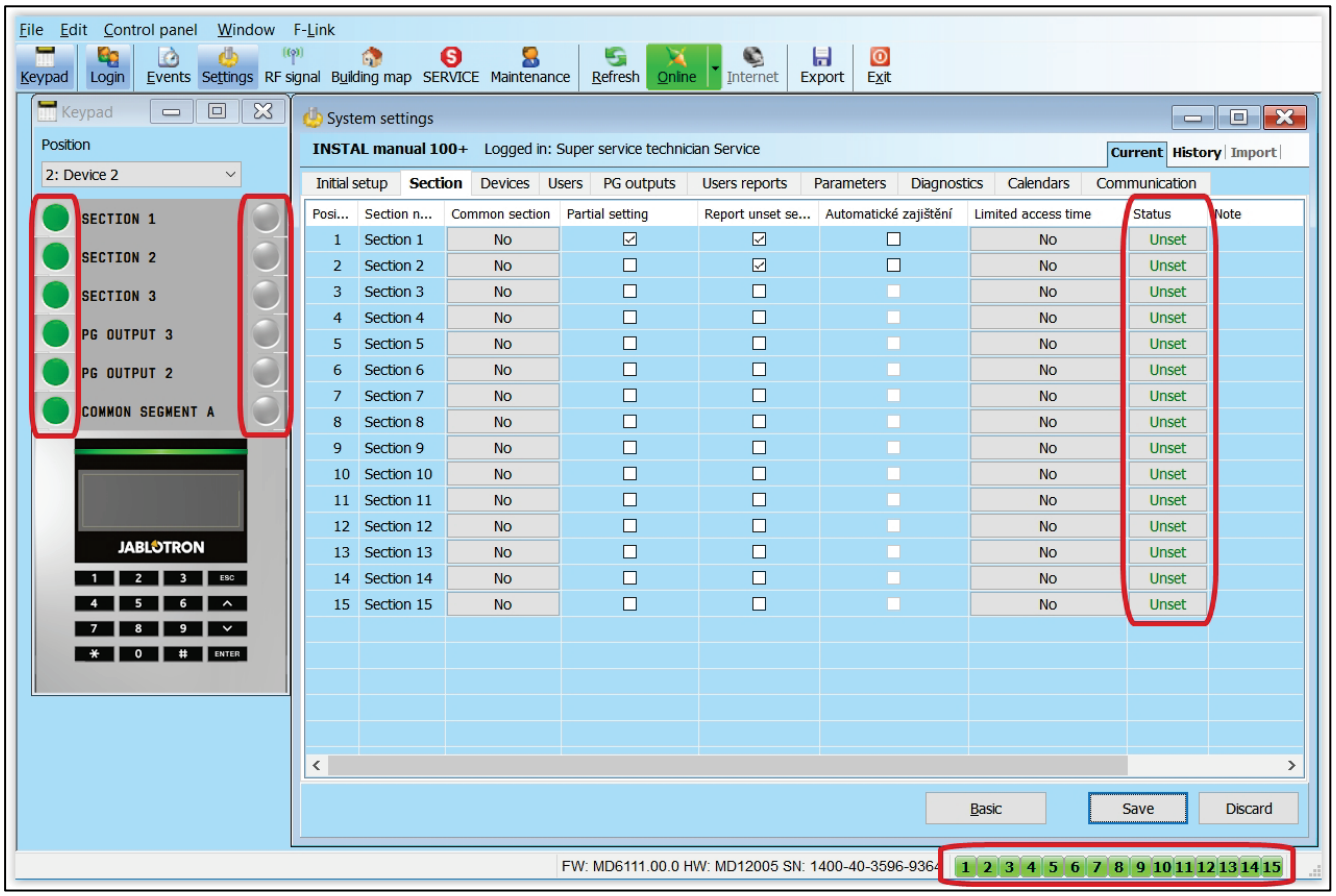
		Section 3: Unset; Section 4: Unset, Error; Section 5: Unset; Section 6: Unset; Section 7: Unset; Section 8: Unset; GSM: 90%; Time 17:01 22.7.	Name and status of Section 3 Name and status of Section 4 Name and status of Section 5 Name and status of Section 6 Name and status of Section 7 Name and status of Section 8 GSM signal quality Time and date of handing over the SMS to the GSM network
SET 1 3 5 7 (control of selected system sections)	(According to the used code)	JABLOTRON: Status: Section 1: Set; Section 3: Set; Section 5: Set; Section 7:Bypassed while being set, GSM: 90%; Time 17:01 22.7.	Installation name as the Initial setup tab Status: Name and status of Section 1 Name and status of Section 3 Name and status of Section 5 Name and status of Section 7 GSM signal quality Time and date of handing over the SMS to GSM
UNSET 2 4 6 8 (control of selected system sections)	(According to the used code)	JABLOTRON: Status: Section 2: Unset; Section 4: Unset; GSM: 90%; Time 17:01 22.7.	Installation name as the Initial setup tab Status: Name and status of Section 2 Name and status of Section 4 GSM signal quality Time and date of handing over the SMS to GSM

9.7 System control via the F-Link or JA-100-Link software

The F-Link and JA-100-Link software are used for local and remote programming of the whole system or user editing; provide an overview of section statuses and section control. It's possible to control sections and PG outputs using segments of the virtual keypad according to the configuration of keypads which are physically present in the system. Control is also possible from the "Section" tab in the "status" column or from the lower status bar. The system records system control according to authorization upon user authorization in the software.

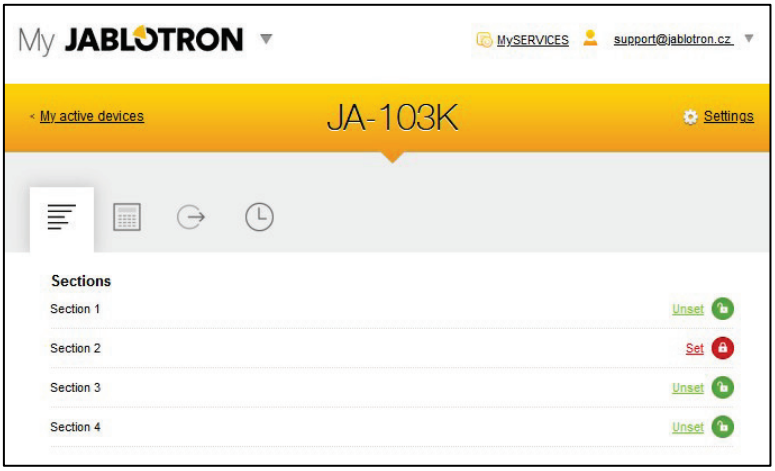
9.8 System control from the MyJABLOTRON web app

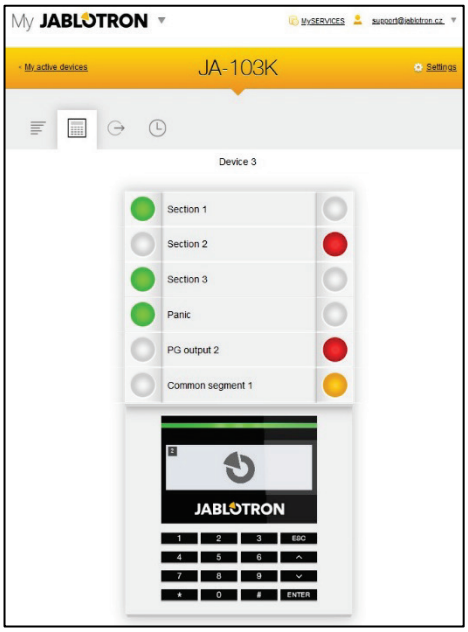
Remote control from the MyJABLOTRON web app is the most user-friendly way to control the security system from any Internet browser regardless of computer platform. Once logged in, the app enables you to control the system not just from the virtual keypad of every physical keypad present in the system, but also enables you to control all sections and PG outputs from an overall list. The user can also browse through a detailed event history including taken photos. New photos can be taken immediately by a user's request. Unlike with



the physical system, the user can see the current temperatures from thermometers, values from various meters and configure messages notifying you about system events or exceeded user-set values.

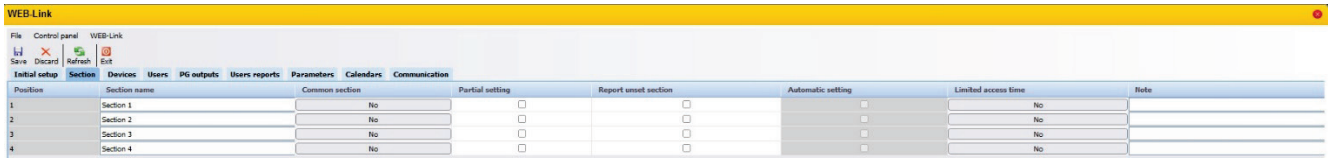
You must authorize yourself with a user code every time you sign in to control the system. Setting sections using segments is identical to their real setup. If the segments enable partial setting, it'll be possible to partially set the system remotely. In all other cases, controlling from the list will always set whole sections. For more info, see chapter 14 MyJABLOTRON web application.





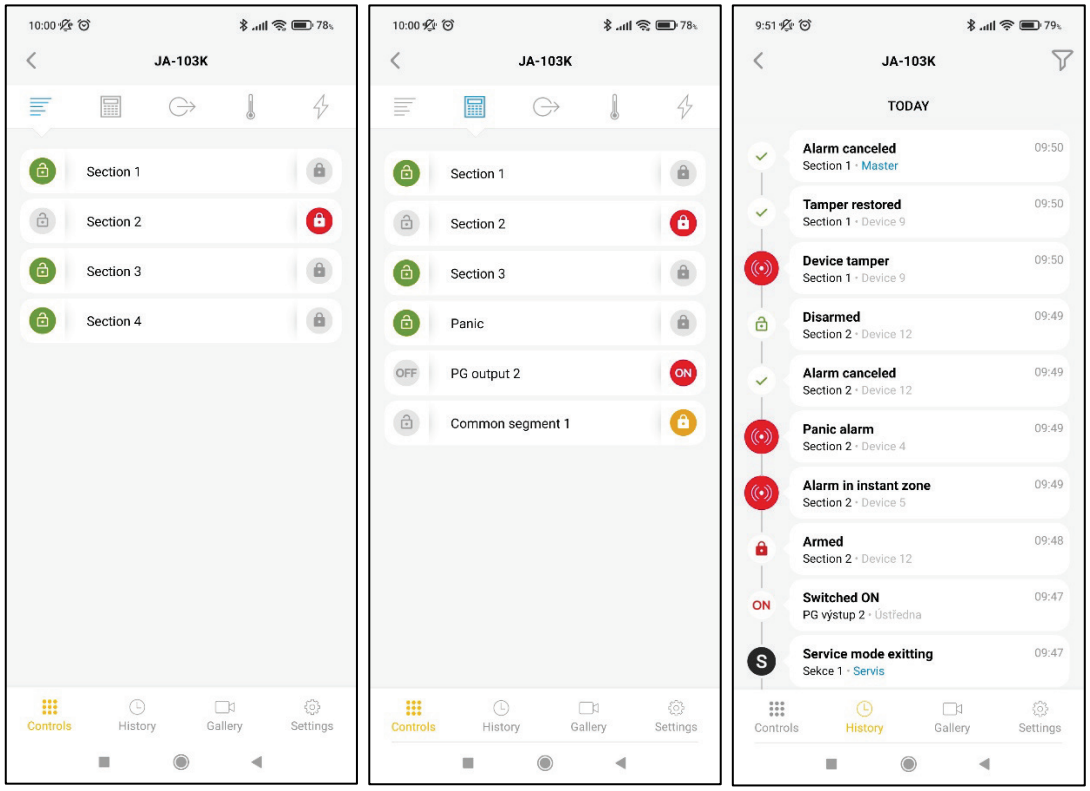
Part of remote programming from the website (regardless of the platform of the remote computer) is so called WEB-Link, which is available in MyCOMPANY app → Installation management → Configuration button. WEB-Link is available only for installer companies, which can use this tool to perform indirect remote access by changing parameters in a configuration file located on the server and save it immediately, in a specific time or after unsetting the system. The installation technician may be informed about a successful change in configuration by SMS or e-mail.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



9.9 System control via the MyJABLOTRON mobile app

Users of MyJABLOTRON can download an application for smartphones. Available for platforms iOS and Android. The mobile app is the most user-friendly way to control the security system which the user can even carry in a pocket thanks to almost unlimited Internet access. After once secured logging in, the app enables you to control the system not just from the virtual keypad of every physical keypad present in the system, but also enables you to control all sections and PG outputs from an overall list. So almost the same function range as in the MyJABLOTRON web application. For some platforms it offers something extra, for instance TouchID or FaceID instead of a code.



9.10 System control by Duress access control

This option enables users to control (set or unset) the system with a different code when they are threatened by another person. This code will unobtrusively draw attention to such a situation by triggering a **silent Panic alarm** without any acoustic or visual indication. A silent panic alarm is triggered by adding 1 to an existing user code. This function is supported by codes with or without a prefix.

Example:

User code with prefix = 4*4444. Duress access control code = 4*444**5**

User code without prefix = 4444. Duress access control code = 444**5**

Warning**: If the user code ends with the number 9 when using Duress access control, then the last number of the code will be **0.

9.11 Obstacles preventing setting the system

According to **Ways of setting** (see Parameters tab), the control panel may check for triggered or fault statuses of individual devices or a particular section while setting each section of the system. In line with this option, the control panel indicates some obstacles during setting (**passable obstacles**) and some of the statuses and may even prevent the system from setting when they occur (**impassable obstacles**).

One of the most common obstacles is any system fault (indicated by a yellow keypad backlight indication button), a loss of connection with a wireless detector or a triggered status detector (typically a magnetic detector) set with a delayed zone reaction (front door and garage door detectors), depleted system battery or a long-lasting power supply failure.

An impassable obstacle preventing setting the system is for example a **triggered status detector** (usually a magnetic door opening detector) set up to an **Instant reaction**. Devices which belong in this group are window opening, balcony or backdoor detectors but it can also be critical systems faults such as fault of backup power supply or fault of communication to the ARC. The reasons which prevent system settings are different according to the pre-set system profile. An exception in preventing the system from setting a section which doesn't check for any triggered detectors or faults is the automatic setting by a calendar using the option "Set Always". The calendar will always set each section provided it's configured to perform such an action (available only when the "Default" system profile is in use).

Pulse detector triggering (e.g. detectors: motion, glass-break, tilt, shock and suchlike) cannot prevent setting.

System informs you about setting with an active device by SMS report (to group of users with predefined alarm reports) with a detailed description.

Ways of setting – table overview

Ways of setting	System keypad	Via voice menu / SMS / calendar	MyJABLOTRON app	F-Link JA-100-Link
Set always	Will set always despite faults or triggered devices status.	Will set always despite faults or triggered devices status.	Will set always despite faults or triggered devices status.	Will set always despite faults or triggered devices status.
Set with warning	While attempting to set with a fault or a triggered device, the keypad flashes for 8 s after which the system will automatically set. It's possible to set the system by pressing the segment button again or by pressing the Enter key.	Will set always despite faults or triggered devices status.	Will set according to "Ways of setting" (Set with check / Set with no check) in the Service configuration tab.	Will set always despite faults or triggered devices status.
Set after confirmation	While attempting to set with a fault or a triggered device, the keypad flashes for 8 s. It's possible to set the system ONLY by pressing the segment button again or by pressing the Enter key.	Will set always despite faults or triggered devices status.	Will set according to "Ways of setting" (Set with check / Set with no check) in the Service configuration tab.	Will set always despite faults or triggered devices status.
Will not set with an active element	While attempting to set with a fault or a triggered device, the keypad flashes for 8 s. It's possible to set the system by pressing the segment button again or by pressing the Enter key ONLY when a detector set to an INSTANT zone reaction is NOT triggered.	Will not set when a triggered detector is set to an INSTANT zone reaction When "Set always" is selected, the Calendar it will set despite faults or triggered devices status.	Will not set when a triggered detector is set to an INSTANT zone reaction.	Will always set despite faults or a triggered devices status.

9.12 Unsuccessful setting

It is a security function thanks to which the control panel checks within the exit delay if setting the system can be executed and the security of the protected premises is not limited by the following cases. If the function is enabled, then **unsuccessful setting** can be caused by:

1. Instant detector activation anytime during the exit delay (someone enters to an already protected area).
2. Permanent activation of a detector with a delay reaction after the exit time has already expired (The user forgot to close the main door, garage or gate, etc.).

In the case when setting the system is prevented, an “Unsuccessful setting” event is triggered and indicated by rapid flashing of the yellow backlit indication button on the keypads and also by their beeping, and acoustically by an outdoor siren as well. Simultaneously it is reported to that particular user who tried to set the system or to the system administrator, provided the report “SMS about unsuccessful setting” is enabled, see F-Link software, Communication tab.

To cancel the indication of unsuccessful setting it is necessary to select in the LCD keypad menu an option called “Cancel warning indication” or if the “Default” system profile has been pre-set then by setting that section.

9.13 Events reported to users

All events which are sent to users are assigned to four basic groups. Every single group can be assigned to users arbitrary. Users to whom a group will be assigned will be sent reports from this group. When the basic settings of the groups are not enough then there are two special groups which can be used (User defined group 1 and 2). Events can be added to those groups and can be given to only specific users.

Overview table of Groups of Events reported to users:

Order	Event	Group
1	Setting	SMS about Setting / Unsetting (3)
2	Unsetting	SMS about Setting / Unsetting (3)
3	Partially setting	SMS about Setting / Unsetting (3)
4	30-minute mains fault	SMS alerts (1) / Alarm call (2)
5	Mains restored after 30 min	SMS alerts (1) / Alarm call (2)
6	Instant alarm	SMS alerts (1) / Alarm call (2)
7	Instant alarm cancelled	SMS alerts (1) / Alarm call (2)
8	Delay alarm	SMS alerts (1) / Alarm call (2)
9	Delay alarm cancelled	SMS alerts (1) / Alarm call (2)
10	Tamper alarm	SMS alerts (1) / Alarm call (2)
11	Tamper alarm cancelled	SMS alerts (1) / Alarm call (2)
12	Fire alarm	SMS alerts (1) / Alarm call (2)
13	Fire alarm cancelled	SMS alerts (1) / Alarm call (2)
14	Gas leak	SMS alerts (1) / Alarm call (2)
15	Panic alarm	SMS alerts (1) / Alarm call (2)
16	Panic alarm cancelled	SMS alerts (1) / Alarm call (2)
17	Health troubles	SMS alerts (1) / Alarm call (2)
18	Flooding	SMS alerts (1) / Alarm call (2)
19	Code breaking attempt	SMS alerts (1) / Alarm call (2)
20	Set with active zone (when confirmation enabled)	SMS alerts (1) / Alarm call (2)
21	Section without movement	SMS alerts (1) / Alarm call (2)
22	Overheating activation	SMS alerts (1) / Alarm call (2)
23	Overheating deactivation	SMS alerts (1) / Alarm call (2)
24	Freezing activation	SMS alerts (1) / Alarm call (2)
25	Freezing deactivation	SMS alerts (1) / Alarm call (2)
26	System start (out of service mode)	Fault and service SMS (4)
27	Device low battery	Fault and service SMS (4)
28	Device battery OK	Fault and service SMS (4)
29	Fault (device, communicator)	Fault and service SMS (4)
30	Fault end	Fault and service SMS (4)
31	Service mode entry	Fault and service SMS (4)
32	Service mode left	Fault and service SMS (4)
33	Maintenance mode entry	Fault and service SMS (4)
34	Maintenance mode left	Fault and service SMS (4)
35	Low BATTERY	Fault and service SMS (4)
36	BATTERY OK	Fault and service SMS (4)
37	ARC communication fault	Fault and service SMS (4)
38	ARC communication restored	Fault and service SMS (4)
39	RF jamming	Fault and service SMS (4)
40	RF jamming end	Fault and service SMS (4)
41	Low credit balance	Fault and service SMS (4)

The assignment of events distinguished by the system to groups is specified in the table. On occurrence of an event the system generates an SMS in the format: Installation name, Time, Event, Event source, Section, Time.

Example of a sent SMS:

JABLOTRON	*(installation name)*
17:01:10, Delayed alarm	*(event time, event)*
Door magnet, Ground floor	*(detector name, section name)*
17:01:25, Instant alarm	*(event time, event)*
Staircase movement, Upstairs	*(detector name, section name)*
Time 17:01 22.7.	*(time of sending)*

9.14 System acoustic indication

Acoustic indication of the system can indicate not only alarm status but also inform about other statuses or status changes. For an acoustic indication overview see the following tables:

Acoustic indication by keypad / reader:

Sound	Action description
One short beep	Button pressing confirmation
One long beep	Segment activation, setting a section or switching on a PG
Two long beeps	Segment deactivation, unsetting a section or switching off a PG
Two long repeated beeps	Unsuccessful setting
Three long beeps	Section unsetting with alarm memory indication
Permanent beeping	Exit delay
Continuous beeping	Entrance delay
	Alarm

Acoustic indication by indoor / outdoor sirens:

Sound	Action description
One short beep	Section setting
	PG output switching ON
Two short beeps	Section unsetting
	PG output switching OFF
Three short beeps	Section unsetting with alarm memory indication
	Unsuccessful setting
	Setting with an active zone (until FW 13 only)
Permanent rapid beeping	PG status indication – quick beeping
Permanent slow beeping	Exit delay
	PG status indication – slow beeping
Continuous squeaking	Entrance delay
	PG status indication – permanent squeaking
Whooping	Alarm in a section
Melody (1 – 4) *	PG status indication

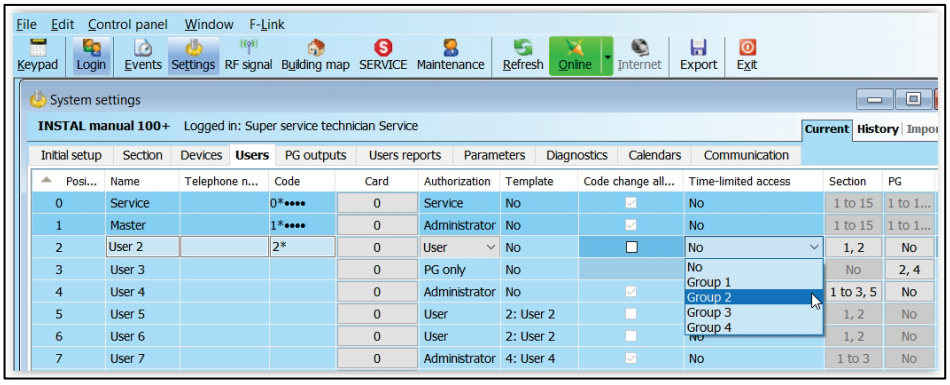
* Only valid for sirens supporting the Melody function

Acoustic indication of fire detectors (smoke, temperature, gas):

Sound	Action description
Permanent rapid beeping	Fire alarm
Permanent hooting	

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

9.15 Time limited access for users

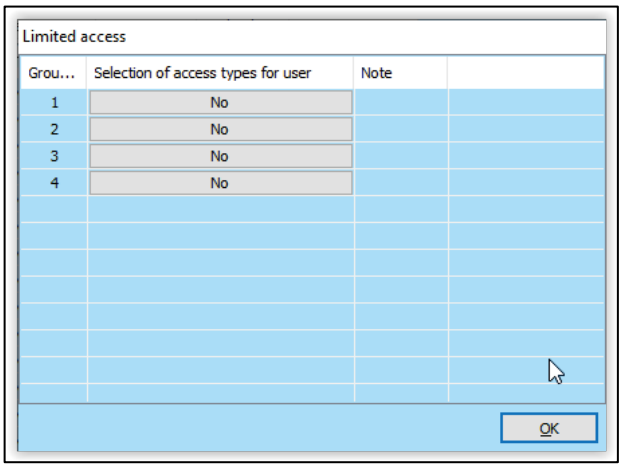


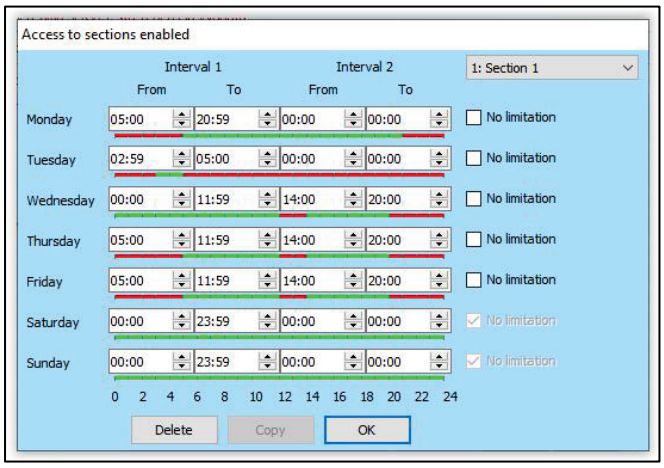
The time limited access function is meant for selected users split into up to 4 groups. To these groups they can be added various "time authorizations" for access to assigned areas (sections) according to the weekly calendar. That allows every group of users blocking or unsetting
a selected section in two-time frames (Interval 1 and Interval 2) for every day in a week. The main purpose of this is for larger companies when there could be workers, heads and managers or in a kindergarten, cleaning ladies, chefs, teachers and parents with their children.

Every system user whom should have limited access according to the pre-set calendar has an enabled option i.e. "Time limited access" by the option from "Group 1" to "Group 4" and it represents every single group of users.

Limitation is valid for "User authorisation" only. If the user with enabled time limitation tries to unset a section in the blocking period, the system will refuse it. And if the user was already inside the protected premises then after entrance delay time expiration an intrusion alarm would be triggered. The user has authorization to cancel the alarm but the system won't be unset within the blocking period.

In the following example there is a variant of settings for access allowed for a selected group of users "Group 1" where access is limited to "Section 1". On Monday and Tuesday access is allowed from 5:00 in the morning to 20:59 in the evening. From Wednesday to Friday access is allowed from 5:00 to 11:59 and then from 14:00 to 20:00 hr. On the weekend (Saturday and Sunday) access is blocked completely.





To program time limited access using F-Link software on the Users tab, the same name of the button which serves for setting the group of users for individual sections is used.

9.16 Disabling and blocking options

9.16.1 Disabling

Before you set the system, a situation can occur where a device is necessary to be intentionally bypassed from guarding (for instance a garage because of some construction activity or leaving a dog inside a usually protected room). This option is called **Device disabling**, it is available in an LCD keypad menu or by JA-100-Link software and it can be performed at two levels according to user authorization:

1. **Blocking of input (BLK)** – the function is for blocking a detector input (it blocks its activation). The system ignores any detector activation = an alarm is not triggered, nor reports PG activation. Tamper alarms, faults or depleted battery reports are supervised all the time. In the JA-100-Link software it is indicated by a yellow dot. Authorization for blocking to be performed belong to the Administrator and Service technician.
2. **Device disabling (DIS)** – this function is for disabling a detector. The system ignores all device functions = it doesn't trigger any alarms nor tamper alarms, reports or faults. In the JA-100-Link software it is indicated by red dot. Authorization for disabling is done by the Service technician only.

Not only a device but also a user can be **Disabled**, except users in position 0 (service technician) and 1 (Administrator), PG outputs or calendar actions. Disabling is permanent until it cancelled by the same procedure as its activation.

Caution: *It is not possible to* ***block*** *or* ***disable*** *a control panel or a device with a Panic reaction!*

9.16.2 Blocking

During section setting a situation can occur that some devices stay active (for example an open window or a balcony door, flooded detector in a cellar, etc.). The system reacts to this situation quickly during the setting of the section and informs about it, but after the confirmation the system will behave according to the parameter **Blocking during setting** one of the following ways:

1. **Blocking enabled** – enabling this option will make all active detectors blocked during setting, it means they cannot trigger an alarm at all in this setting period.
2. **Blocking disabled** – disabling this option will make all active detectors temporarily bypassed during setting only, it means that if they go back to standby then they can trigger an alarm (there is the risk of false alarm creation because of windows opened by draft for instance).

9.17 Non-alarm functions – Functions of PG outputs

The security system allows authorized users (according to the settings) to control the system functions – not just functions related to guarding the sections but also controlling PG programmable outputs (switching ON / OFF). Using relay modules or a module with special semiconductor outputs they can switch on devices (such as indicators, traffic lights, acoustic indicators), or other appliances related to the security system (such as movement lights, AC when entering a room, blocking the heating when a window is open or when a section is set), or a completely separate appliance, i.e. home automation (e.g. electric gate or garage door opening, heating, garden watering).

Function of PG output	Description	Example
ON / OFF	Bi-stabile output status, can be changed by arbitrary command or device.	Manually switching ON appliances using a control segment, SMS or also by some device with an option of manually switching off with no limitation. Typically heating control, air conditioning, lights.
Impulse	Mono-stabile output status with pre-set time.	Impulse switching of other additional control circuits such as gate control, rollers, jalousies, garden watering, door locks, etc.
Copy	Output status with OR logic. Output will be active if minimum one device at least will also be active, but deactivation occurs when all control devices will be inactive.	Useful for indication of some single or collective statuses (typically of open windows, garage doors, etc.) on the keypad control segment. In similar ways statuses of all sections, alarms, alarm memories, faults and many other events can also be indicated where the beginning and the end are given.
Delayed copy	Mono-stable output status with pre-set time of switching with an option to be prolonged repeatedly.	Typical output setting for control of lights when movement is detected by a motion detector, any motion detected then prolongs the pulse.
Extended copy	Delayed output status with pre-set time of that delay.	Mostly used for the indication of an opened door for longer than a predefined time because someone could have forgotten to close them (mains, door or garage door). Indication can be optical on a keypad control segment but also acoustic by keypad or indoor / outdoor siren.
Change	Bi-stabile output status.	Output meant for cyclical control (ON, OFF) for instance from an impulse device, by authorization or by dialling in from an authorized telephone number.

The system also offers user functions such as measuring the temperature using temperature detectors or thermostats, which can be shown on the LCD keypad and in the MyJABLOTRON application, measuring and monitoring electrical energy consumption, amount of water or any other utilities. The JA-150EM-DIN impulse counter is for this purpose in combination with some measuring device (electricity meter, gas meter, hydrometer, etc.). See our application studies and recommendations in MyCOMPANY, MySTORAGE section.

10 Setting the system through the F-Link software

The JABLOTRON system is exclusively programmed using a computer, through the F-Link software. F-Link checks the current version of the software from version 1.4.0 through updates from the JABLOTRON server and the latest version is automatically offered for download. Or after the login it can be downloaded from the MyCOMPANY web interface at www.myjablotron.com.

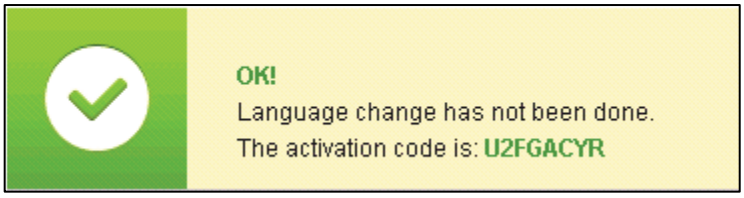
Immediately after opening the initial window for connection selection the F-Link software can be switched over to the desired language environment by clicking on a language change icon (flag). You can change the language at any time later. The initial window offers the following options:

1. **Connect locally** – for the connection of the computer to the control panel. A USB cable is necessary (with A-B connectors).
2. **Connect remotely** – offering selection from a file database allowing you to establish a remote connection. To establish remote communication with the control panel the computer must have access to the Internet and the used SIM card in the control panel must have active GPRS data transmission. For trouble-free connection other requirements must be met as e.g. enabled remote configuration in the control panel, proper registration code, service code and if LAN communicator is not used, then also sufficient GSM signal in the control panel location.
3. **Offline settings** – provides access to the setting data of the control panel. Here, you can e.g. get to the list of devices or records of the last battery replacement etc.

The F-Link software can also be used to change the language of the control panel for communication with users. The language does not only refer to displayed texts on the LCD screen or SMS messages sent to mobile phones of users, but also the voice menu of communicators that communicate with the user. By changing the language of the control panel you will delete all the texts in the system and therefore this selection should be made as the first step before the installation and assignment of names to devices, sections or users.

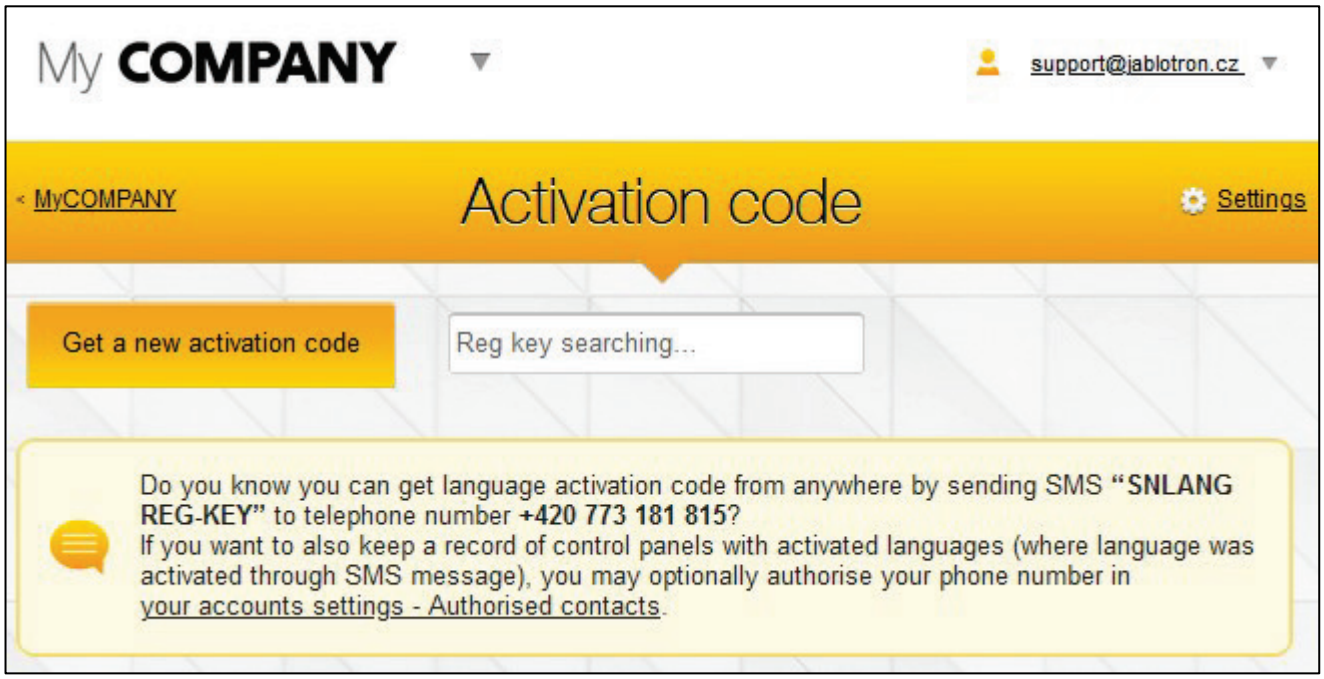
The JABLOTRON system is delivered ex works with the communication language option set to “English” with the possibility to select “Czech”. However, other language options of the control panel are limited by a narrower choice of language(s) per the country the control panel is designed for. The installation company that is registered in the MyCOMPANY web service www.myjablotron.com can request the “Activation key”, which will be bound to the unique equipment registration code. The “Activation Key”, will extend the available choice of languages designed by the manufacturer for the particular market. The Activation Key can be obtained in three ways:

1. From the web interface, which is only accessible for trained installation technicians:
    a. Login to the MyJABLOTRON web service www.myjablotron.com
    b. Open the MyCOMPANY section
    c. Select the Activation Codes service
    d. Click on the item + Get new activation code
    e. Enter the Registration Key of the control panel and select “Send”
    f. If an offer of more languages is displayed, select the requested languages and complete the selection with “Send”



    g. Make note of the Activation Code displayed in green and enter it in F-Link

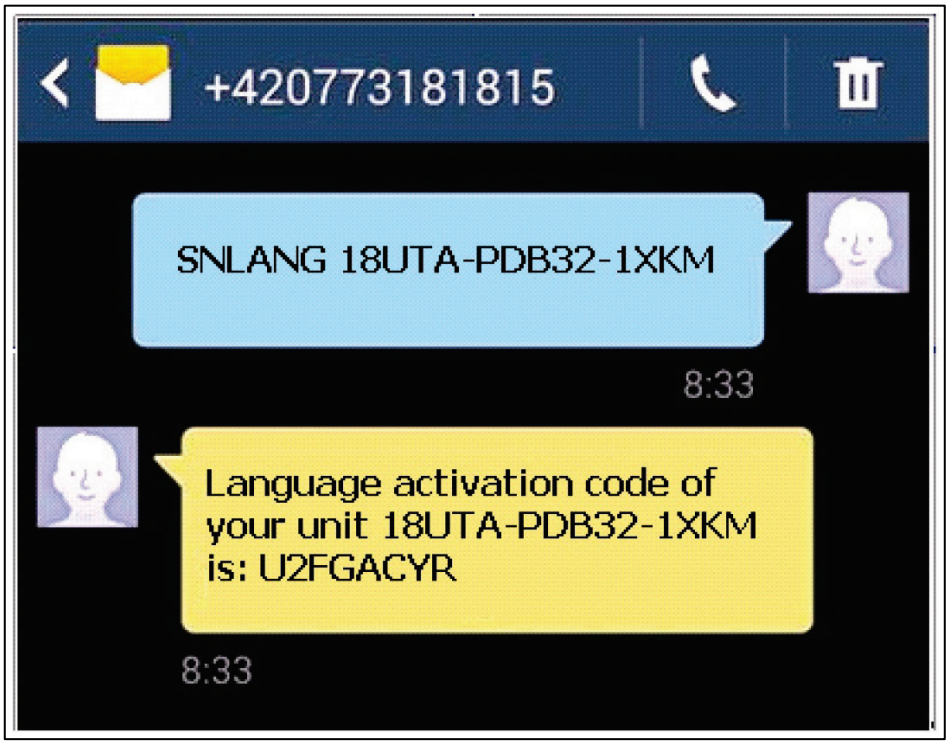
The list of generated Activation Codes will remain saved at the website for possible further use.



2. If the installation technician cannot access the Internet (the MyJABLOTRON web service) at the moment, the Activation Code can be requested with an SMS.

An SMS message in the format: "**SNLANG_registration code"** can be sent to the phone number **+420 773 181 815**. An answer with the activation code will be sent shortly after that. The activation code may contain 8 to 14 numerals and case-sensitive letters.

The received activation code should be entered in F-Link in the Initial setup tab, using the Activate button.

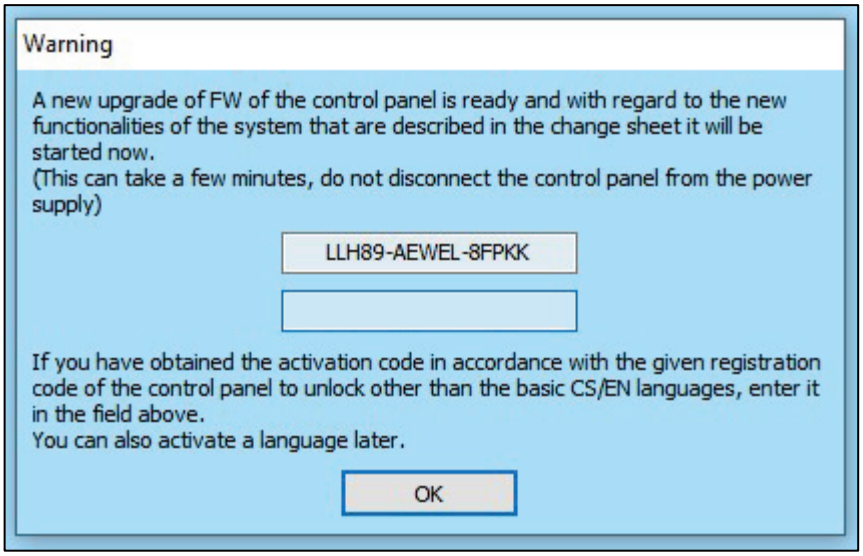


Example of sending a request using an SMS

3. Getting the Activation Code from your distributor. When asking for the Activation Code you will need to provide the registration code of the control panel. Depending on country, the activation code can be also found on the package box of the control panel.

10.1 Starting the F-Link software and setting the system size

1. Connect a computer to the control panel using a USB cable – the computer will initialize the new USB device (it may take a longer time if the control panel is being connected for the first time).
2. After the connection your computer will display two newly found drives: FLEXI_CFG and FLEXI_LOG. If displayed, you can close the window.
3. Start the F-Link software. If the control panel has default settings, the **Initial setup** tab will open and the system will automatically get into the Service mode. If the control panel has been configured before (its service code has been changed), the software will request entry of the code – it should be entered in the format **cccc** (the default setting of the service code is 1010). If the prefix is enabled (in the Initial setup tab in F-Link) it is 0*cccc (0*1010). You can use the **Remember** option to make the software to save the code until closing of the database. Use the **Display Code** option to check the entered code e.g. if you use an alphanumerical keyboard where a mistake can be made. Note: After establishing connection using the USB cable the possibility of programming changes of settings from the LCD keyboard will be disabled (menu item Settings will be disabled). After disconnection of the cable the item will re-appear in the menu in a few seconds.
4. After proper authorization the following window can appear:



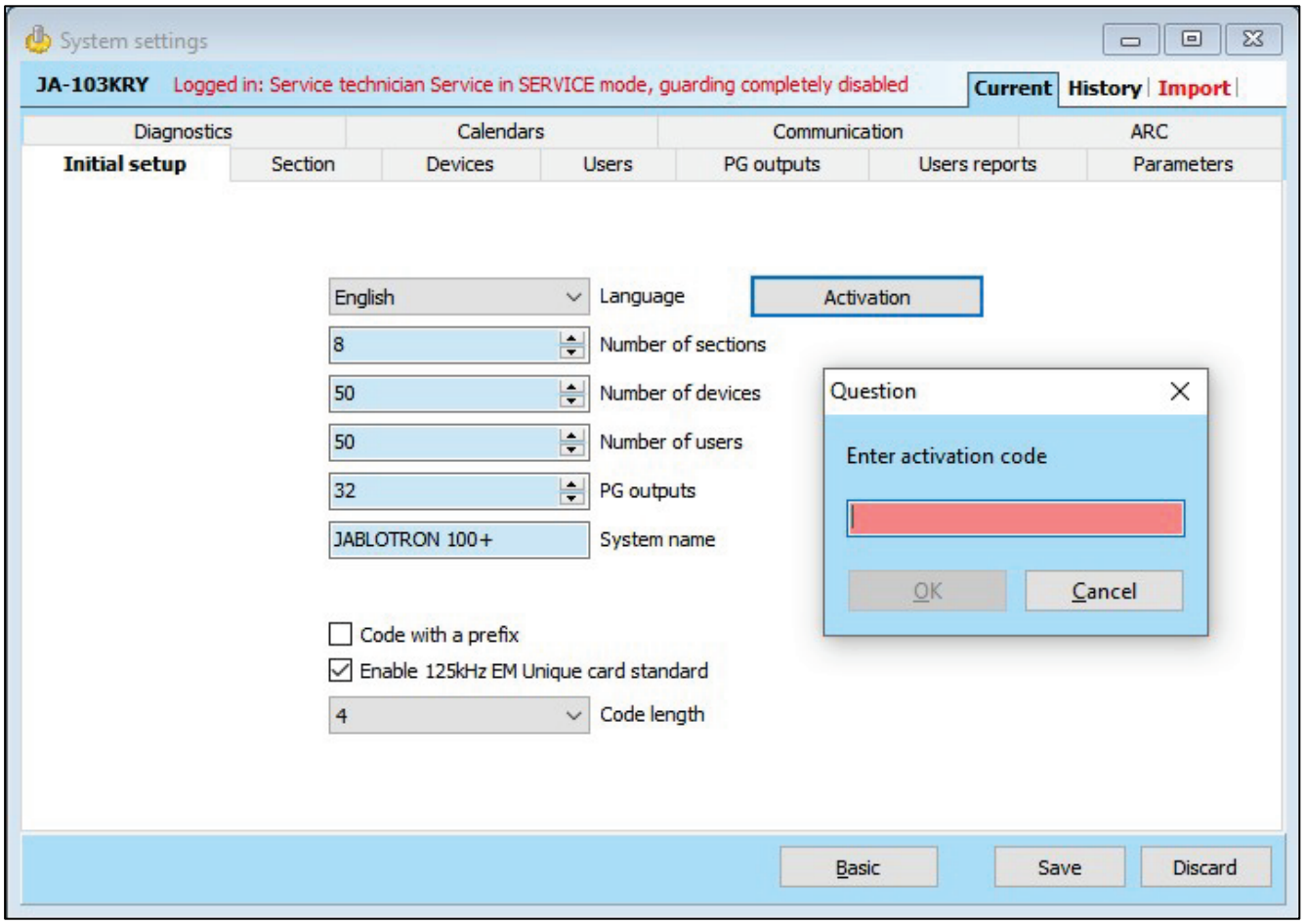
In such a case we recommend performing the update. After confirmation of the key the new firmware package will be downloaded, which may take a few minutes. After the completion of the update the first page of the Wizard (Initial setup tab) will be displayed.

10.2 Starting the Wizard

1. In every offered tab set the required parameter and click on the “Next” button. If you skip a setting by mistake, you can return to tab that have already been previously set in the Wizard.
2. After setting the last tab press “Save” and close the Wizard with the “Exit” button.
3. After exiting you will be asked whether you want to start the Installation Wizard when starting the F-Link software next time.
4. You can exit the Wizard any time during the setting process by pressing the “Exit” button.
5. You can start the Wizard independently and any time in the Control Panel / Installation Wizard menu.

10.3 Initial setup tab

This tab is used to set the basic size of the system. The set values can be changed any time. The range values influence the size of the database and thus the time required for loading and saving data (generally via remote access). To make changes in this tab you do not need to be in the Service mode. During the first start of the F-Link software the Wizard will gradually guide you through the setting of all parameters of the system.



Activation: by entering a special activation code you can add a language (languages) to the choice of languages that is (are) released for the country the control panel is designed for.

Notes:

- If one of the default languages (EN/CZ) is required, the Activate function will not be used.
- If you request another language, after entering the activation code you can select one of the available languages from the Language menu.
- You will also need to upgrade the firmware of the wireless components (specifically access modules with display to get selected language into them, too).

Initial setup tab description:

Codes with a prefix – this function determines the ways of entering all access codes for user authorization. When the function is enabled the system requires a 1 to 3-digit prefix (position of the code) ended by a * symbol before an access code entry (e.g. 12*3456). It allows users to change their own codes from the LCD. However, to be able to control the system, you must use a code with the sequential number of the code (prefix). If this parameter is disabled, only a 4-digit access code is required to be entered and the codes may only be changed by the system Administrator, who will assign codes and will be the only person authorized to change user rights (thus he/she will have a knowledge of them). The administrator is also responsible for avoiding code duplicity.

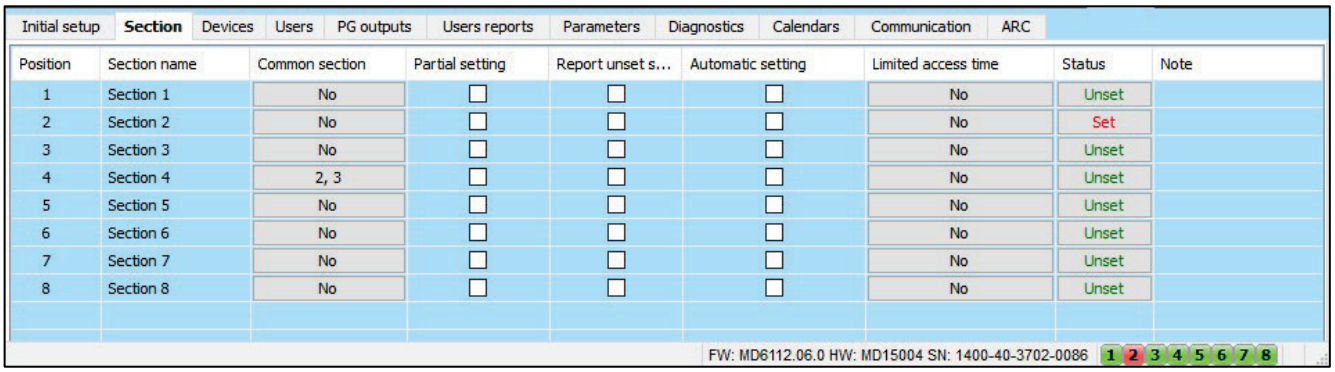
Warning: *Anytime this parameter is disabled, it will irreversibly delete all the user codes and settings of the Service Code and Administrator Code and restore the default values. Users' authorizations and the RFID card / tags of already existing users are not changed.*

Enable 125kHz EM UNIQUE card standard – if disabled, the identification RFID cards / tags (JA-190J, JA-191J, JA-192J, JA-194J) recommended by a manufacturer may only be used. If enabled, cards of other manufacturers working with the above-mentioned frequency are also allowed.

Code length – to increase the alarm system security level during authorization it is possible to pre-set the user code length regardless of the prefix function. There can be 4, 6 or 8-digit codes. When the code length is changed then Service and Administrator codes are set to the default values and earlier pre-set codes are erased.

10.4 Sections tab

Used to configure parameters of independently controlled monitored sections (zones). To make changes in this tab you do not need to be in the Service mode.



* Items described below marked * are only displayed if **Advanced Settings view** is enabled.

Section name – naming of sections is used to make textual event reports (SMS), showing on LCD keypad and memory readout, for a better recognition when reported (e.g. Ground Floor, Store, ...).

Common section – allows you to select that a section is automatically set if all the sections, for which it is a common one, are set (suitable for corridors, staircases and other common areas). Warning of limitation of possible use of the keypad segment for the common section: if any of the sections has been unset separately, the common section segment **cannot** be used to unset the remaining sections. These sections must be unset separately.

Partial setting* – allows you to set a section partly if somebody remains inside (detectors with selected reaction of the Internal type will not be active – see chapter 8 System configuration). Without activation of this parameter partial setting cannot be used in the section.

Report unset section* – if a section is unset and no detector is activated in it during a pre-determined period, the “Unset Section” report is used.” The time period is set in the tab Parameters / Report unset section after (60 – 2 880 min).

Automatic setting – it server for an automatic setting of a section, where the “Unset section” was reported. In the Parameters tab you can set a time interval in minutes after which the section will be set automatically. The time interval starts at the moment when the “Unset section” is reported. This function is a supplement of the “Report unset section” function and can be used only if the “Report unset section” function is enabled.

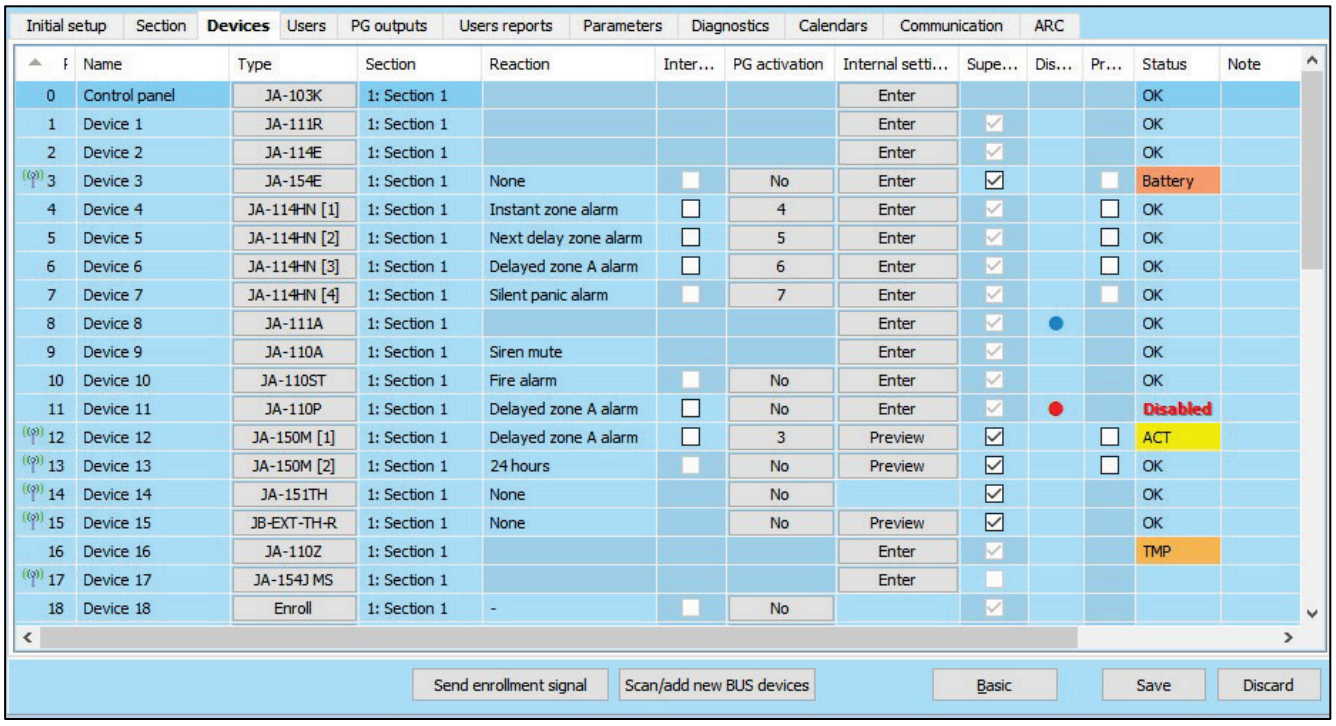
Limited access time* – allows you to set a weekly schedule permitting unsetting of a section for selected users. More details see chapter 9.15.

Status – indicates the current status of a section (Unset, Set, Exit Delay, Entrance Delay, Partially Set, Alarm, Alarm Memory, Disabled, Service mode). By pressing the button, the system can be controlled according to the authorization given by your login (it changes the section state – set / unset).

Note – it allows you to describe details of a section for easier orientation during annual inspections etc.

10.5 Devices tab

It is used to enroll an installed device in the system and to set its parameters. The tab will display as many positions as you have selected in the Initial setup tab. The control panel is automatically enrolled on Position 0 in Section 1 and it cannot be removed or deleted. To make changes in this tab you must be in the Service mode.



	Name	Type	Section	Reaction	Inter...	PG activation	Internal setti...	Supe...	Dis...	Pr...	Status	Note
0	Control panel	JA-103K	1: Section 1				Enter				OK	
1	Device 1	JA-111R	1: Section 1				Enter	☑			OK	
2	Device 2	JA-114E	1: Section 1				Enter	☑			OK	
3	Device 3	JA-154E	1: Section 1	None	☐	No	Enter	☑		☐	Battery	
4	Device 4	JA-114HN [1]	1: Section 1	Instant zone alarm	☐	4	Enter	☑		☐	OK	
5	Device 5	JA-114HN [2]	1: Section 1	Next delay zone alarm	☐	5	Enter	☑		☐	OK	
6	Device 6	JA-114HN [3]	1: Section 1	Delayed zone A alarm	☐	6	Enter	☑		☐	OK	
7	Device 7	JA-114HN [4]	1: Section 1	Silent panic alarm	☐	7	Enter	☑		☐	OK	
8	Device 8	JA-111A	1: Section 1				Enter	☑	●		OK	
9	Device 9	JA-110A	1: Section 1	Siren mute			Enter	☑			OK	
10	Device 10	JA-110ST	1: Section 1	Fire alarm	☐	No	Enter	☑			OK	
11	Device 11	JA-110P	1: Section 1	Delayed zone A alarm	☐	No	Enter	☑	●		Disabled	
12	Device 12	JA-150M [1]	1: Section 1	Delayed zone A alarm	☐	3	Preview	☑		☐	ACT	
13	Device 13	JA-150M [2]	1: Section 1	24 hours	☐	No	Preview	☑		☐	OK	
14	Device 14	JA-151TH	1: Section 1	None		No		☑			OK	
15	Device 15	JB-EXT-TH-R	1: Section 1	None		No	Preview	☑			OK	
16	Device 16	JA-110Z	1: Section 1				Enter	☑			TMP	
17	Device 17	JA-154J MS	1: Section 1				Enter	☐				
18	Device 18	Enroll	1: Section 1	-	☐	No		☑				

* Items described below marked * are only displayed if **Advanced Settings view** is enabled.

Name - it is used in textual reports of events and in the memory readout (example Main door).

Type – displays the type of the assigned device. An empty position allows you to enroll a new device. **Enrolling devices**, see chapter 8.4.1 Enrolling and erasing devices.

Section – determines to which monitoring section the device will report events (alarm, tampering, fault ...). ***Note**: Division of a building into sections – see chapter 10.4 Sections tab.*

Reaction – defines which reaction will be released by activation of the particular device. If a device does not have any alarm input (e.g. a BUS access module), it cannot be assigned a reaction. The complete list of reactions for devices is displayed if Advanced Settings are enabled. You will find a description of all the reactions in chapter 8.4.2 List of applicable reactions.

Internal* – this parameter is only available for intrusion detectors. Signals from devices with this indication are not evaluated as alarm signals if a section is partially set. Partial setting of a section – see chapter 10.4 Sections tab. If partial setting is not enabled for a section, the setting of this parameter is not applicable.

PG activation* – activation of a device can activate programmable PG outputs with their defined reactions. This option is linked to the item PG Outputs / Activation / by a device.

Internal settings – access to settings of internal parameters of perimeters that are connected to the BUS or feature bidirectional wireless communication. Individual devices have different internal parameters (some have none). The internal settings of a keypad are described in chapter 10.5.1 Keypad configuration. Settings of other devices are described in their manuals.

Supervision* – allows you to disable checking of regular communication with wireless devices (it cannot be disabled for BUS elements). By the default, setting of wireless devices (except remote controls and Panic buttons) is always enabled.

Disable – can be performed at 3 levels given by your authorization:

1. **Input blocking** (yellow dot), serves for the permanent blocking of the detector's input (BLK). The system ignores any device activation = an alarm is not triggered and the PG is not controlled but tamper alarms and faults are registered as usual.
2. **Device disabling** (red dot), serves for the device to be completely disabled (Disabled). The system ignores all connected device functions = no alarm, tampering, PG activation, Fault, report...
3. **Tamper detection disabling** (blue dot), serves to permanent blocking of the detector's tamper contacts (TMP). The system ignores detector opening and detachment from the back cover = no sabotage

You cannot disable the control panel or a device whose reaction is set to Panic.

Status – indicates the current status of the device. OK = everything all right, TMP = tampering, ACT = alarm input activated, BLK = blocked, Disabled = Disabled, ERR = error, ?? = no communication with the device, Mains supply

= supply failure, Battery = discharged or disconnected battery in the control panel, Charging = charging the backup battery in the device or control panel, BOOT = upgrading of the device is going on or upgrade failure (repeat upgrade), INIT = reading of the device configuration, Disabled = device is disabled. By moving the mouse cursor on the device STATUS, you will display detailed data.

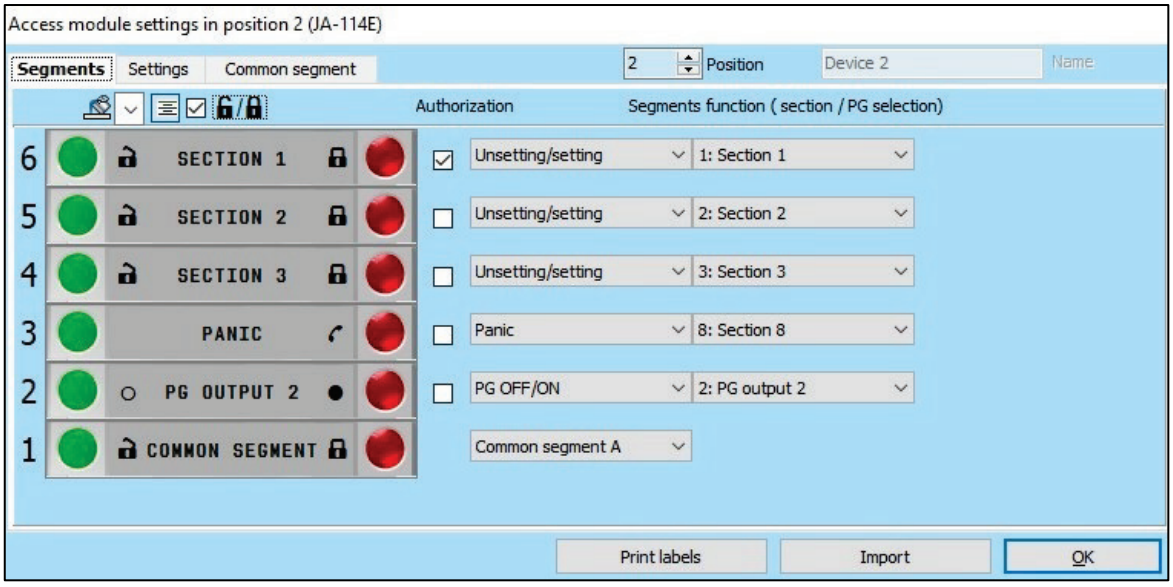
Note – it allows you to describe details of the device, e.g. location, last battery replacement date, mean RF signal strength during the last testing etc.

10.5.1 Keypad configuration

- First, assemble the control keypad mechanically. Attach the required number of control segments (max. 20) to the selected access module; their internal cables must be interconnected.
- Enroll the keypad on the selected position in the system (see chapter 5 Installation of BUS devices).
- On entering in the internal settings of the keypad (the Devices tab) the following window will open (the example refers to the JA-114E keypad), for other keypads the setting range may be smaller).

Example of keypad internal settings:

10.5.1.1 Segments tab



Background colour choice – serves for background colour choice of segment labels

Locks locked / unlocked – activates the display of the lock symbols for segment control buttons setting sections, and dot symbols (empty / full) for the control of PG outputs. The symbols are taken into consideration when printing the labels.

Texts of control segment labels – the Section Name (from the Sections tab) or PG Output Name (from the PG Outputs tab) is displayed. You can also edit the entire text to be printed right here by clicking on the respective text. The **Print labels** button (in the bottom bar of the card) is used to print segment labels.

Print labels – enables direct print of pre-set label texts using the installed printer. You can edit the texts by clicking on the segment and the changed texts will be saved in the database and they are uploaded to MyJABLOTRON app. You can conveniently use the PT-P700 label printer from JABLOTRON, which enables automatic cutting by the required label dimension.

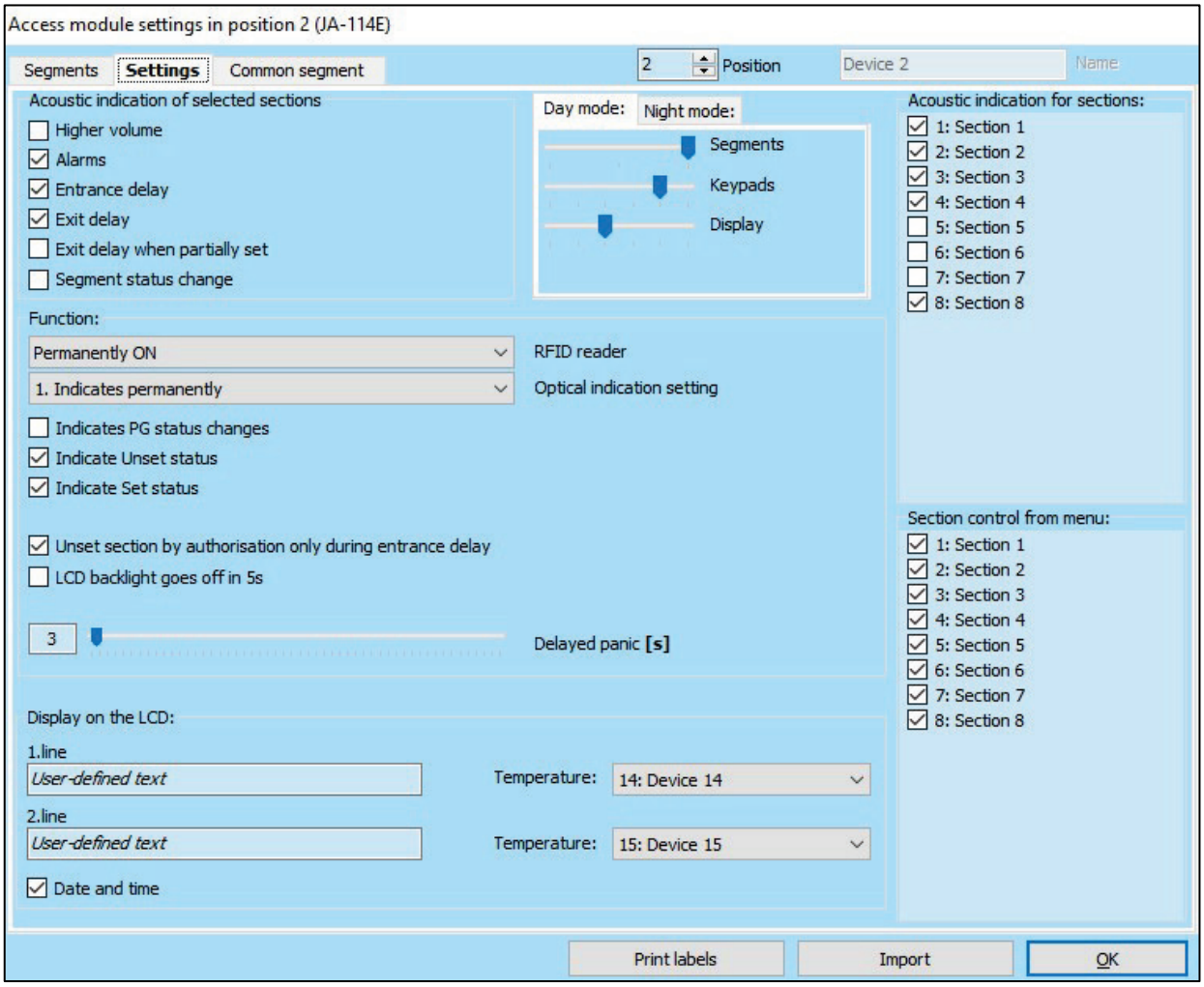
Import – allow the copying of current keypad settings to other keypads, for instance in the case when a protected building has a few more entrances and every entrance requires having a keypad with the same functions. Making a copy is possible for the same type of keypad. Or it can be used when a keypad is replaced with a new one. The Import button offers you the history of the last known settings of the keypad at that given position.

Authorization – the user's authorization is required for setting and unsetting. When this parameter is disabled, all segments can be controlled without authorization except the Unset Section function for which authorization is always required. As regards enabling and disabling PG outputs the setting of the Authorization / without Authorization function is valid for both the controls.

Segment functions – on the left the function of the segment is selected, on the right the section or PG output that the selected function is assigned to. The following functions can be assigned to a segment:

None	Segment off, used for segments prepared as a reserve for future used.
Unset / Set	Section control. Segment indication: section unset = green, set = red.
Unset / Partially set	Enables activation of partial setting mode of the section (if enabled in the Sections tab). Segment indication: section unset = green, partially set = yellow.
Unset / Partially set / Set	Allows you to select the setting level. After pressing of the right button (Set) partial setting is offered, after repeated pressing complete setting is offered. For this selection partial setting must be enabled for the section in the Sections tab. Segment indication: section unset = green, partially set = yellow, fully set = red.
Indicates section	The segment only shows the status of the section, but does not enable its control (suitable e.g. for indication of the status of common sections, staircase etc.) If an alarm is released, it allows you to cancel it by pressing the green button of the segment with subsequent valid authorization of the user.
Panic (silent)	The segment makes it possible to release a silent Panic alarm. After pressing the right button, a Panic report is sent from the section the function is assigned to, without acoustic indication. The Panic alarm may also be Delayed with adjustable time and possibility of cancellation before expiration of the set time (see Delayed Panic). If the section is set, it will not be unset.
Fire	The segment triggers the fire alarm. After pressing the right segment button if flashes red for 3 s (during this time it is possible to cancel the fire alarm by pressing the left segment button). Then, fire alarm is released from the section the segment is assigned to.
Audible Panic	The segment makes it possible to release a loud alarm. After pressing, loud Panic alarm is released from the section the segment is assigned to. The loud Panic alarm may also be Delayed with adjustable time and possibility of cancellation before expiration of the set time (see Delayed Panic). If the section is set, it will not be unset.
Medical troubles	The segment allows you to send a health troubles report (without activating a siren). After pressing the right segment button if flashes red for 3 s (during this time it is possible to cancel the Medical trouble report by pressing the left segment button). Then, the segment returns to the standby mode and the system sends the Medical trouble report from the section the segment is assigned to.
Disable PG / Enable PG	The segment allows you to control a PG output. Indication: PG inactive = green, PG active/enabled = red.
Enable PG	The segment can only be used to enable the PG output (e.g. switch on the lights for a pre-set time).
Disable PG	The segment can only be used to disable the PG output (e.g. function of an emergency STOP button).
Indicates PG	The segment only indicates the status of the PG output without the possibility to control it (red indicates the active status).
Indicates PG inversely	The segment only indicates the status of the PG output with the inversed logic (green indicates the active status) without the possibility to control it.
Common segment A / B	Enables simultaneous control of more sections that have their individual segments on the keypad with one segment. After pressing the button on the same segment the Unset/Set command is executed collectively for selected section segments. If some sections controlled from the Common Segment are set and the others unset, after using the Common Segment the remaining segments will be Unset/Set. If Partial Setting is enabled for one of the selected segments (details see chapter 9 System control options), the Common Segment will behave as follows: 1st pressing of Set = partial setting, 2nd pressing of Set = full setting. It is not suitable to combine the Common Segment function with the Section / Common for Sections functions. Common Segment indication: all sections unset = green, all sections fully set = red, any section set (partially set) = yellow. There may be max. 2 common segments on one keypad at the most. Sections are assigned to the Common Segment in the top Common Segment tab. Note: The “Common segment x” item is only offered if more than two segments for section control are connected to the module.
PG indicates / controls	The segment can control a different PG output from the one it optically indicates. In this menu the first parameter is used to select the PG output for indication and the other one (supplementary) the PG output to control. The function is e.g. used to control a garage gate with a PG output impulse while the control segment displays the actual status of the gate obtained from the gate detector.

10.5.1.2 Settings tab



Acoustic indication of selected sections:

Higher volume	Setting of indication volume except for an alarm
Alarms	Acoustic output in case of an alarm (siren sound)
Entrance delay	Continuous whistling tone during an entrance delay
Exit delay	Slow intermittent beeps (1 per s)
Exit delay when partly set	Slow intermittent beeps (off by default)
Segment status change	Acoustic indication with one beep at a change

Functions:

RFID reader	To save energy, the activity of the reader can only be limited to 3 s from pressing of its cover. The RFID reader can also be completely disabled. This setting applies to wireless keypads and access modules if they are permanently supplied with power from an external source, otherwise their RFID reader is always switched off automatically.	
	Permanently on	The RFID reader is permanently enabled. In the case of a BUS keypad it does not respect the wake-up setting.
	Activated by pressing	Waking up the RFID reader for 3 s after activation on the keypad.
	Off	The RFID reader is permanently disabled.
	Activated by pressing or authorization request	The RFID reader wakes up after activation on the keypad or by an authorization request.
Optical indication settings	1. Indicates permanently	A BUS keypad indicates permanently. A wireless keypad will only indicate permanently with external power supply. Without external power supply it behaves like in option 2.

	2. After a section status change – keypad	The keypad indicates **a change of the status of a section / PG**. A status change is only indicated on the concerned segment. An **entrance delay and alarm** are indicated by the whole keypad.
	3. After a section status change – segment	The keypad indicates a change of the status of a section / PG. A status change of a segment, entrance delay and alarm are only indicated on the concerned segment.
	4. After a segment status change	**Entrance delay and alarm** are just indicated acoustically. **A change of the status of a section / PG** is only indicated on the concerned segment. This option is the default setting.
	5. After an entry and alarm	The keypad indicates an **entrance delay and alarm** on the concerned segment. **A change of the status of a section / PG** is not indicated at all.
	6. Wake-up by pressing	The keypad only provides optical and acoustic indications after opening of the front cover; pressing of a key, segment or front cover.
Indicates PG status changes		Optical indication of a PG´s output status changes on a segment. It is related to the indication settings – options 2 – 4. If disabled, the PG output status changes are not optically indicated.
Indicates Unset status		Keypad segments indicate an unset status without valid authorization. When disabled, they indicate this status only during valid authorization.
Indicates Set status		Keypad segments indicate a set status without valid authorization. When disabled, they indicate this status only during valid authorization.
Unset section by authorization only during entrance delay		If enabled, then a section where the entrance delay has started is unset by a user valid RFID card/tag or code authorisation only. With wireless keypads authorization can be performed after the entrance delay is triggered. **Caution:** We strictly recommend you disable this function when the entrance delay usually runs for a common section, otherwise all sections assigned to the common section will be unset for a given authorisation.
LCD backlight goes off in 5 s		If enabled, the LCD backlight goes off 5 s after the last time of operation with a unit (pressing a key, segment or front cover). If disabled the backlight goes off at the same moment as the whole keypad. If enabled then the battery lifetime is increased.
Delayed panic		The function serves to postpone triggering of a silent or audible panic by a pre-set time. It is possible to determine the time interval when you can cancel the activation by repeated pressing of the same segment button with a pre-set to silent or audible panic. By pressing the right (red) button the timer is triggered and by pressing the left (green) button it is cancelled. When authorization is enabled then it is required for activation and deactivation as well. The delay is adjustable from 1 s to 255 s.

Display on the LCD:

1st line	Allows you to enter a text that will be displayed on the 1st line of the LCD screen of the keypad if no other more important information is displayed, e.g. the company name, building name, description for displayed temperature etc.
2nd line	Allows you to enter a text that will be displayed on the 2nd line of the LCD screen of the keypad if no other more important information is displayed, e.g. the company name, building name, description for displayed temperature etc.
Date and time	Possibility to display date and time of the control panel on the LCD screen of the keypad.
Temperature	Possibility to display the temperature of the 1st thermometer or thermostat on screen.
Temperature	Possibility to display the temperature of the 2nd thermometer or thermostat on screen.

Backlight intensity:

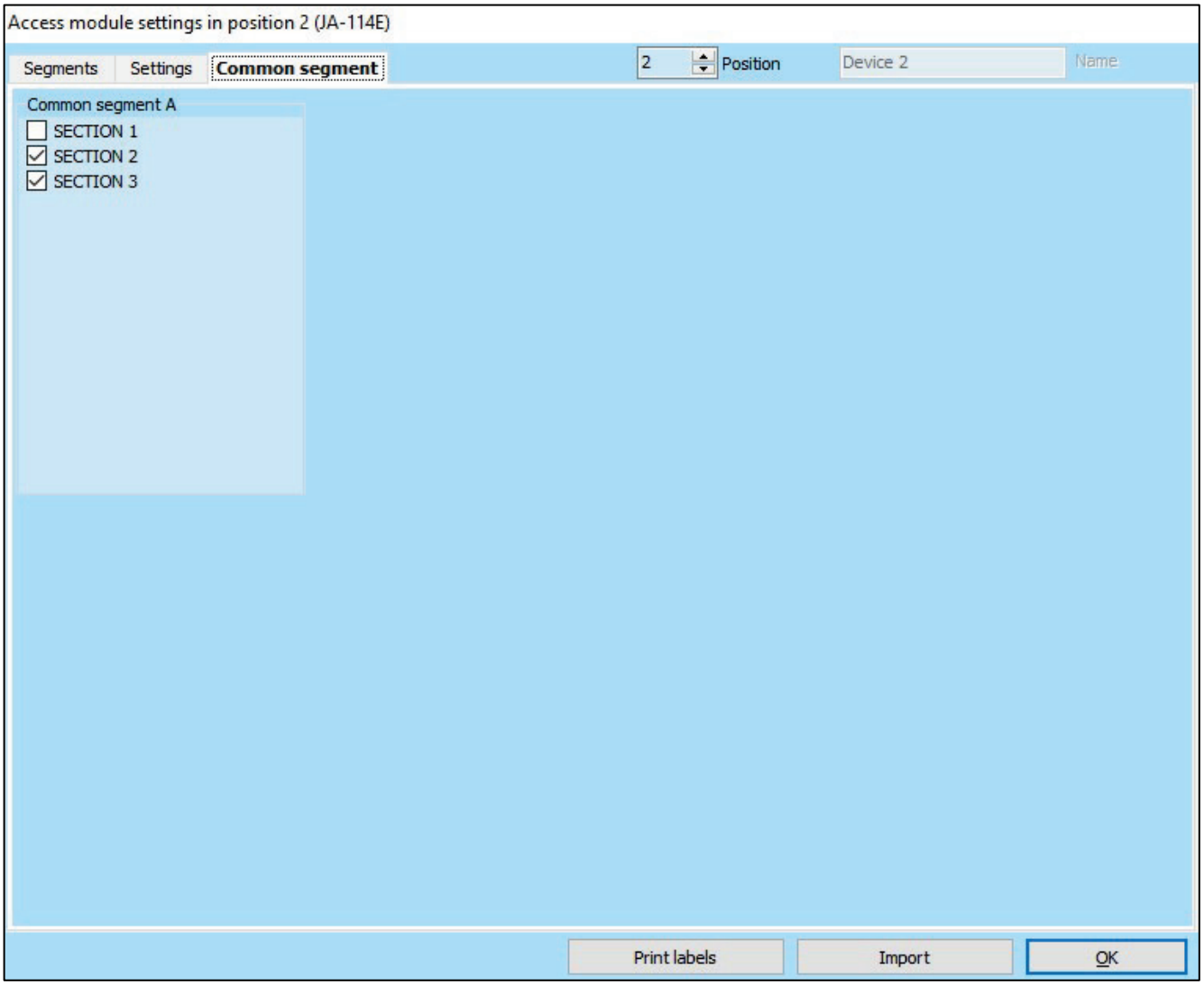
Segments	Adjustment of the LED illumination on the segments
Keypad	Adjustment of the keypad backlight
Display	Setting of the LCD display backlight

***Note**: Backlight intensity can be set differently for the day and night mode, also the keypad acoustic indication can be silenced.*

Acoustic indication for sections – allows you to select sections for which acoustic indication will be active (of alarms, entrance and exit delays, control of PG output etc.).

Sections control from menu – in a keyboard that contains an LCD screen you can define which sections can be enabled and disabled from the menu. This way you can e.g. create a keypad that normally controls 2 sections with the use of segments, but if necessary it can use the menu to control other parts of the house for which it does not have any installed segments.

10.5.1.3 Common segment tab



Enables the simultaneous control of several sections that have their individual segments on the keypad combined as one segment. After pressing the button on the same segment, the Unset / Set command is executed collectively for selected section segments. If some sections controlled from the Common Segment are set and the others unset, after using of the Common Segment the remaining segments will be Unset/Set. If Partial Setting is enabled for one of the selected segments (details see chapter 9.2 System control by keypad), the Common Segment will behave as follows: 1st pressing of Set = partial setting, 2nd pressing of Set = full setting. The Common Segment makes it possible to bypass an active detector in a section if its setting mode is “Sets with warning” or “Sets after confirmation” without influencing the other segments set to “Sets partially with one pressing and completely with the second one” with its second pressing.

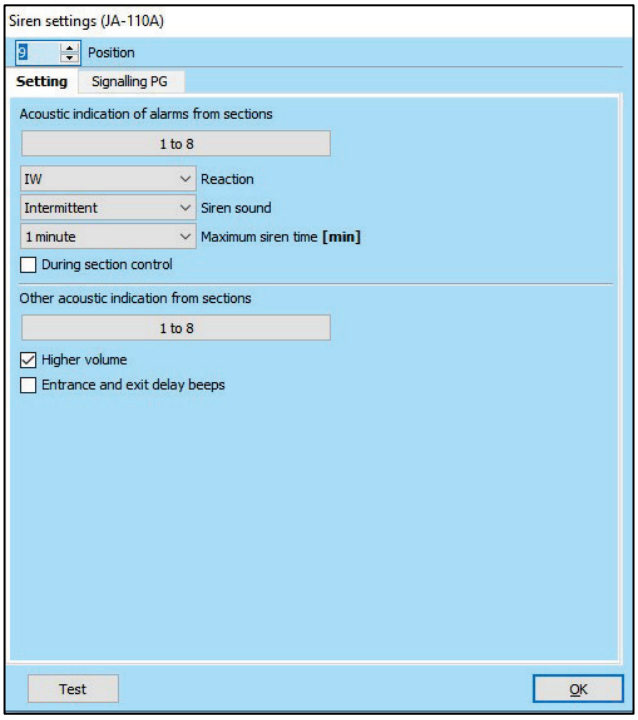
Common Segment indication: All sections unset = green, all sections fully set = red, any section set (partially set) = yellow. Sections are assigned to the Common Segment in the top **Common Segment** tab.

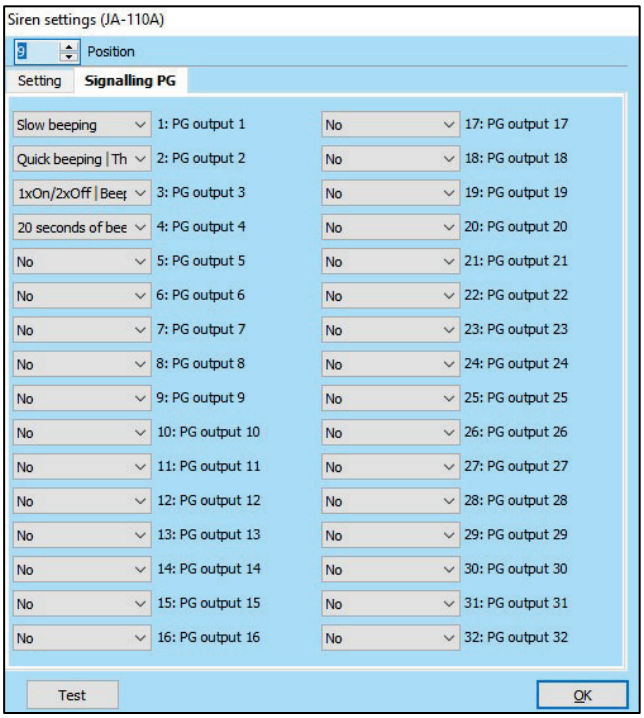
There may be max. 2 common segments on one keypad at the most. The selected section can be mutual for both common segments.

Notes:

- The “Common segment” is only offered if more than two segments for section control are connected to the module.
- It is not suitable to combine the Common Segment function with the Common Section function.

10.5.2 Example of settings of an internal siren





Acoustic indication of an intrusion alarm from sections – used to select sections for which alarm will be acoustically indicated by the sirens.

Reaction – selection for the alarm indication options EW (external warning indication) or IW (internal warning indication). The difference is described in table in a chapter 8.5 Types of alarms.

Siren sound – selection of the way of siren sound: Intermittent (50/50) / Continuous.

Maximum siren time – limitation of the maximum hooting time to 1 to 5 minutes (assuming the control panel alarm is longer; otherwise it stops together with the control panel alarm).

Higher loudness – possibility to set higher and lower loudness volume of indication of the entry and exit delay and indication of PG output control. It does not have any impact on alarm hooting, which is always set to the highest volume.

Beeps during section control – acoustic confirmation of section status changes.

Entrance and exist delay beeps – acoustic indication of an entrance / exit delay.

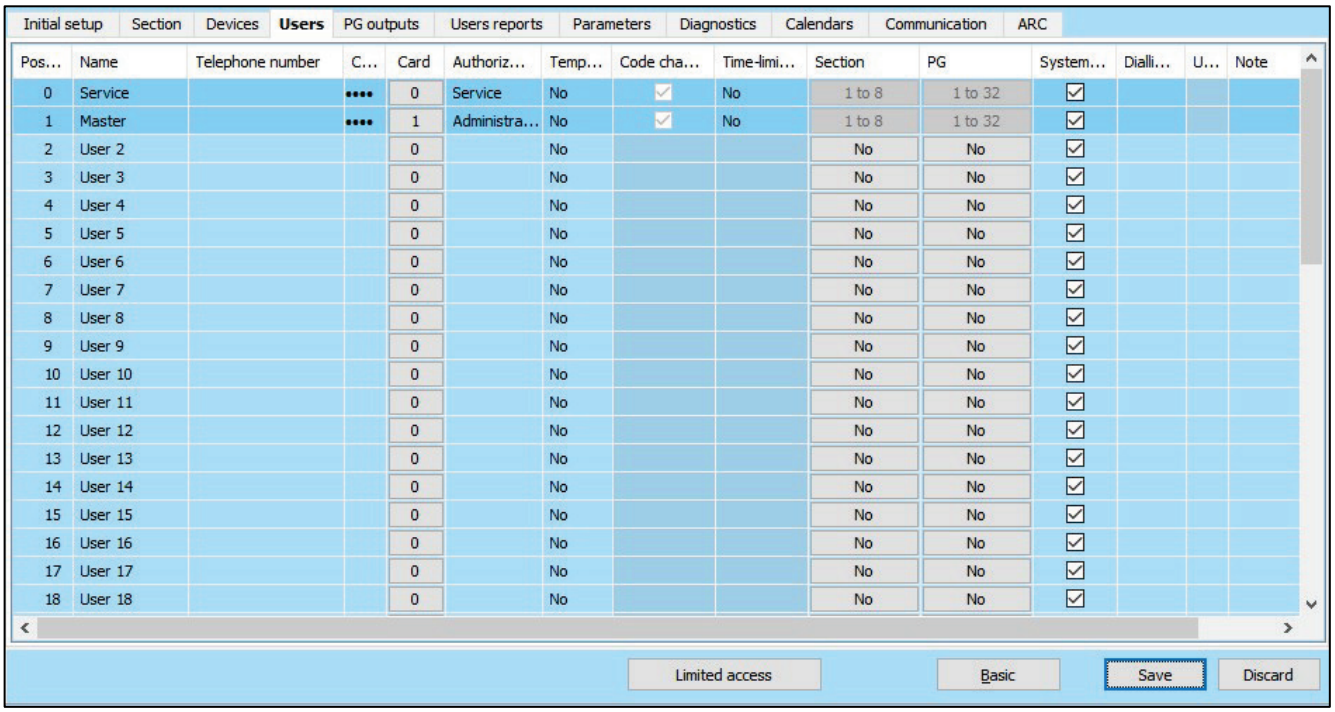
Signalling PG – acoustic confirmation of changes in the PG outputs of the used segments. Allows you to select sounds assigned to a specific PG output to distinguish them acoustically, for instance pressing the doorbell button has a different sound to the sound of a PG output triggered by opening the door.

Test – button for a 3 second test of acoustic and optical alarm indication.

10.6 Users tab

It is used to establish new system users and to set their rights. The tab will display as many positions as you have selected in the **Initial setup** tab. To make changes in this tab you do not need to be in the Service mode.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



* Items marked this way are displayed if **Advanced Settings** are on.

Name – names of users are used in textual event reports in the readouts of the event history, in tabs for reports, authorization settings or for authorization on a keypad with an LCD screen.

Telephone number – used for reporting events and for identification of users when the system is controlled by phone using a voice menu or for activation of PG outputs by ringing and SMS. The phone number must always be entered in the international format (e.g. +420777123456).

Code – the user access code is entered in the format **p*cccc (p = prefix (position number), * = separator, cccc = 4 code numerals)**. If the prefix is disabled (in the Initial setup tab in F-Link) it is **cccc** only. The code on positions 0 and 1 cannot be deleted (Service and main Administrator). Codes can be 4, 6 or 8-digit.

Card – used to assign RFID access cards (tags). Each user can be assigned 2 cards. Cards can be assigned:
- by entering the serial number (it can be read with a barcode reader from the RFID card/tag).
- **using the JA-190T reader** (connected to a USB port of the computer) by application of the RFID card/tag.
- using any keypad and applying an RFID card/tag.

Authorization – defines user rights. The authorizations on position 0 and 1 cannot be changed. Details – see chapter 8.3 Authorisation of users.

Model user – allows to copy all the settings according to the model user. Subsequent changes in the settings of the model user will apply to all users set according to the model user.

Code change allowed* – allows a user to change his/her code (not the position number). The option is only available when the parameter Codes with prefixes is enabled (Administrator, Service and ARC can change their code any time).

Time-limited access* – makes it possible to limit a user's access in accordance with the weekly schedule in the tab **Sections / Time Limited Access** see chapter 9.15 Time limited access for users. Access limitation can only be applied to users with the User authorization level.

Section – defines which sections may be defined by the user (administrator). The Administrator may also set codes and cards of users in the assigned sections. A section cannot be assigned to a user that is only authorized to control PG outputs.

PG – defines which PG outputs the user is authorized to control (if authorization is required for the output control).

Control reports – allows a user to enable sending SMS reports about Setting / Unsetting when controlled for keypad.

Dialling in activates PG – information window about assigned PG control by dialling in.

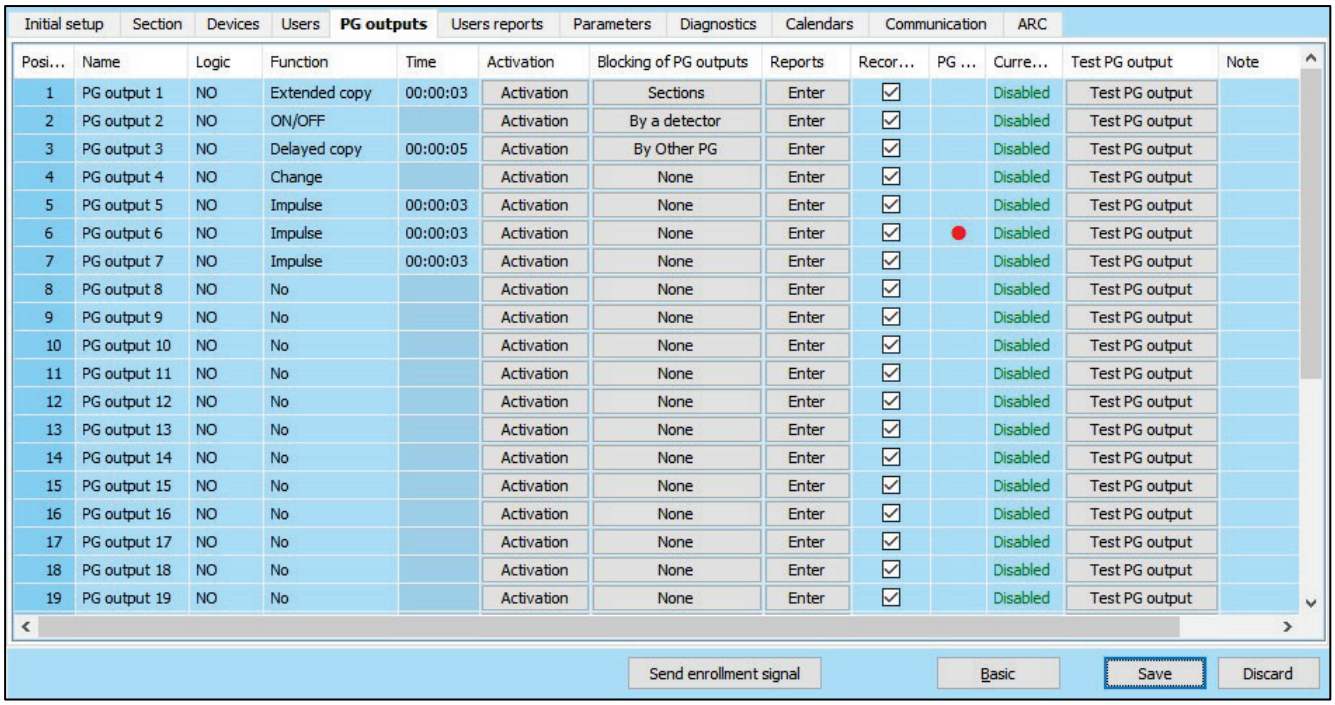
Disable – possibility to block a user. The user on position 0 (service technician) and 1 (chief administrator) cannot be disabled. Disabling of a user is indicated by a red dot. The Administrator (using the LCD keypad or JA-100-Link) and Service Technician (via F-Link) are authorized to disable users.

Note – makes it possible to describe a user's details, e.g. authorization of access outside working hours etc.

Time-limited access – the button serves for setting up time – limited access, see chapter 9.15 Time limited access for users.

10.7 PG outputs tab

It is used to set functions of the programmable outputs. The tab will display as many positions as you have selected in the **Initial setup** tab. To make changes in this tab you do not need to be in the Service mode.



Posi...	Name	Logic	Function	Time	Activation	Blocking of PG outputs	Reports	Recor...	PG ...	Curre...	Test PG output	Note
1	PG output 1	NO	Extended copy	00:00:03	Activation	Sections	Enter	☑		Disabled	Test PG output	
2	PG output 2	NO	ON/OFF		Activation	By a detector	Enter	☑		Disabled	Test PG output	
3	PG output 3	NO	Delayed copy	00:00:05	Activation	By Other PG	Enter	☑		Disabled	Test PG output	
4	PG output 4	NO	Change		Activation	None	Enter	☑		Disabled	Test PG output	
5	PG output 5	NO	Impulse	00:00:03	Activation	None	Enter	☑		Disabled	Test PG output	
6	PG output 6	NO	Impulse	00:00:03	Activation	None	Enter	☑	●	Disabled	Test PG output	
7	PG output 7	NO	Impulse	00:00:03	Activation	None	Enter	☑		Disabled	Test PG output	
8	PG output 8	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
9	PG output 9	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
10	PG output 10	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
11	PG output 11	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
12	PG output 12	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
13	PG output 13	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
14	PG output 14	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
15	PG output 15	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
16	PG output 16	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
17	PG output 17	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
18	PG output 18	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	
19	PG output 19	NO	No		Activation	None	Enter	☑		Disabled	Test PG output	

Name – identification of the output (e.g. Air-conditioning, Warehouse door...).

Logic – possibility to set the inverted logic of the output (NO = normally open, NC = normally closed).

Function – determines behaviour of the output after activation.

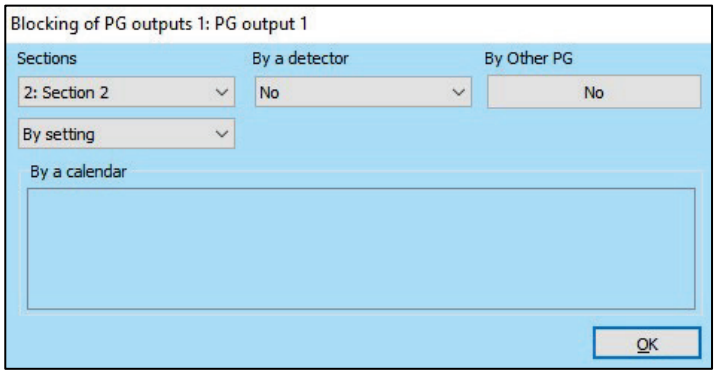
Impulse	Enables activation with a time limitation (the time is set in the Time column).
ON/OFF	The enabling command will cause activation, disabling command deactivation while the status of the source or duration is not checked, the last command always performs its request.
Copy	Copies activation of a detector or internal status; if there is a request from two devices, the OR logic is used.
Delayed copy	Only sends a command when the activation condition is valid longer than set in the Time column (suitable e.g. for indication of forgotten closing of a garage gate).
Extended copy	Copies activation of a device (or internal status) and extends it by the time set in the Time column (suitable e.g. for lighting of a corridor after door opening).
Change	By activation the current PG status is inverted to the opposite status (only suitable for impulse control, e.g. with a remote-control button).

Time – setting of time for the functions Impulse, Copy after delay and Copy with overlap. Time is set in the format *hh:mm:ss* in the range of 00:00:01 to 23:59:59.

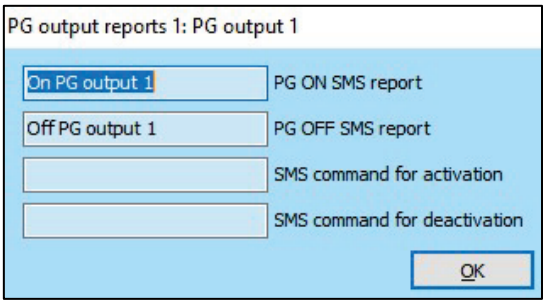
Activation – opening the Activation Map of the PG output – see chapter 10.7.1 Activation Map of a PG outputs.

Blocking of PG – makes it possible to block a PG output by a section status, detector or another PG. The blocking prevents the particular PG from being enabled and if it is already on, it will disable it. It is suitable e.g. to block a door lock if the respective section is set. In the case of blocking by a section status you can select whether the blocking is valid when the section is set or unset and in the case of blocking by a device or another PG output whether by its activation or deactivation. All the blocking options can be used at the same time.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



Reports – setting the texts of SMS reports sent on activation or deactivation of a PG output. The users that each of the reports is sent to are set in the Users reports tab. When the texts of the reports are changed, they are recorded in the log, so they cannot be completely deleted.



PG recording in the memory – enables registration of PG activation in the event history and thus also SMS reporting to users and communication to the ARC (e.g. for monitoring the entry of users to monitored doors, registration in the MyJABLOTRON app etc.).

Disable – possibility to block a PG output. Disabling (blocking) of an output is indicated by a red dot. Only the Service Technician (using F-Link) is authorized to disable an output.

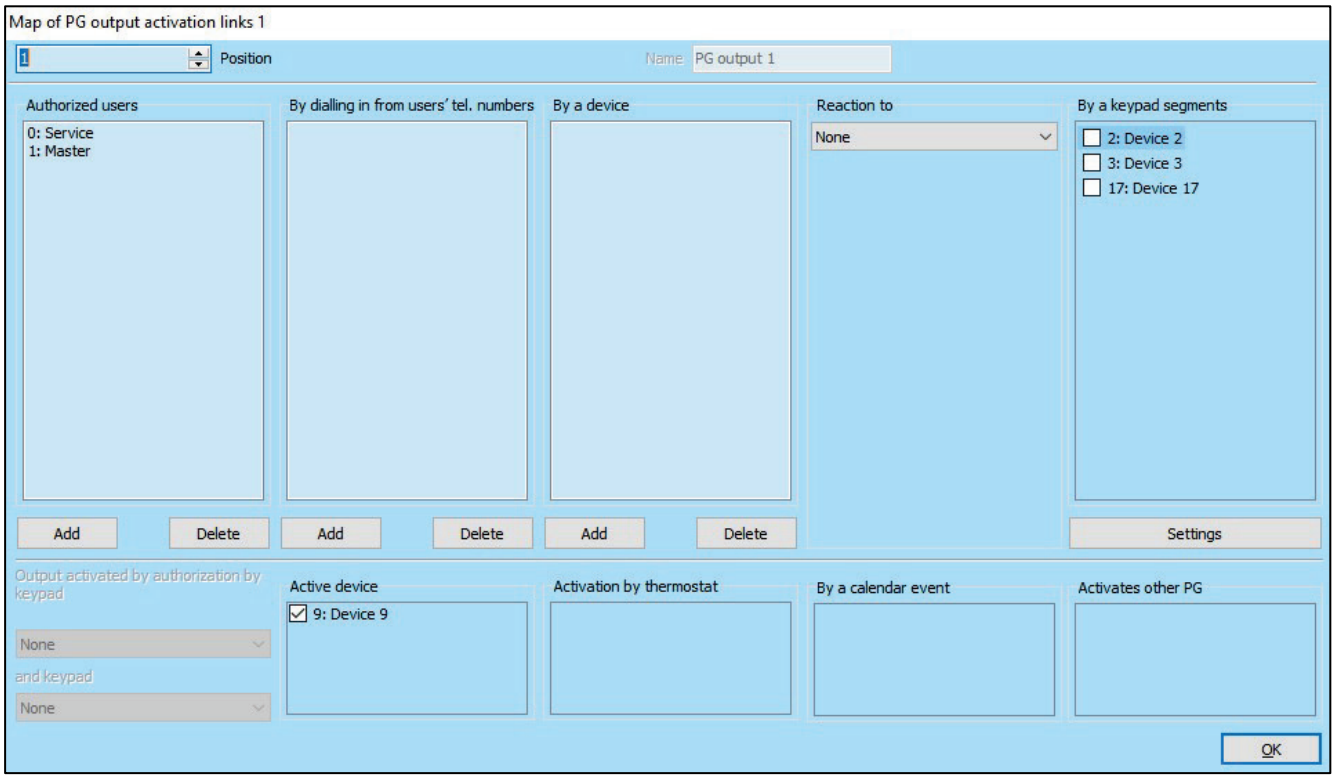
Current status – color-coded information about the current status of a PG output. Green description corresponds to the green light of the segment; red description corresponds to the red light of the segment.

Test – possibility to control an output manually from the computer. Depending on the selected function it will enable (or disable) the particular PG, if it´s not currently blocked.

Note – makes it possible to describe details of a PG output, its use, special behaviour, notification of activation together with other outputs etc.

10.7.1 Activation Map of a PG outputs

By selecting Activation in the PG outputs tab, you will enter the map of activation links. The map determines what action the output responds to.



Authorized users – defines users that are authorized to control the PG output with the requirement for authorization from a keypad (with segment buttons), from the MyJABLOTRON app or by an SMS command. The setting is linked to the Users tab.

By user's authorization by keypad – allows you to set up to 2 keypads that activate the PG output by mere authorization (application of a card/tag or code entry). This function is designed for opening of a door lock (i.e. no operation of the segment buttons is necessary). This function is only available if the output function is set to Impulse.

By dialling in from user's tel. numbers – defining users that are authorized to activate a PG output by calling from their phone (phone numbers are entered in the Users tab). Phone numbers used for the ringing activation must not be hidden (the CLIP service must not be deactivated for them). The term "ringing" means that after dialling the phone number the caller waits for at least one ringing tone (however, up to the answering setting, see the number of ringing tones of incoming calls in the communicator settings) and terminates the call. The PG output switches on when call hangs up. If the call is answered by the control panel, the output will not be activated.

By a device – enables activation of a PG output by a device (detector activation, pressing a tag etc.). The setting is linked to the Devices tab.

Reaction to – enables activation of an output by a selected internal status of the system (e.g. setting, alarm, power supply failure, error etc.). For an internal status (39 internal statuses altogether, see the following table) you can set the group of sections the signal will be accepted from (the OR logic). The concerned PG output may be set to copy the status of another PG output or several other outputs where the mutual logic is selectable (OR or AND). The last item in the menu "Event in system" allows you to set activation of an output and its deactivation in response to a completely different event (e.g. activation in case of an alarm, but deactivation by unsetting only).

By a keypad segment – shows a list of keypads and remote controls in the system. Using the Setting button (under the list of keypads) you can enter the internal menu of the selected keypad and adjust its settings, see chapter 10.5.1 Keypad configuration.

By SMS commands – allows you to set textual commands to activate and deactivate a PG output by phone. Reception of the respective SMS has a similar effect to pressing of the Set or Unset button on the control segment of the keypad. To control outputs, use SMS in the format **code_command**, e.g. **2*2345_enable_light** (Note: the _ character is a blank space). The code before the command is not obligatory if in the **Communication** tab the "Voice menu and control SMS without a code" item is enabled and the phone number of a user authorized to control the corresponding PG output is identified.

Active device – list of devices that are activated by the concerned PG output, for instance a photo from a PIR with a camera (only information window, the function must be set in the device's internal settings).

By a calendar action – list of calendar actions that activate or deactivate or block the concerned PG output (information window).

Warning 1: *The JA-107K control panel provides 128 PG outputs. Wireless PG outputs can only be assigned at outputs 1 to 32. All 128 PG outputs can be used for BUS modules.*

Warning 2: *The PG outputs are not functional if the system is in the Service mode. By pressing the Test button all PG outputs can be tested. On activation of the Service mode all the PG outputs get disabled. After exiting of the Service mode from F-Link their re-activation is offered except Warning 3.*

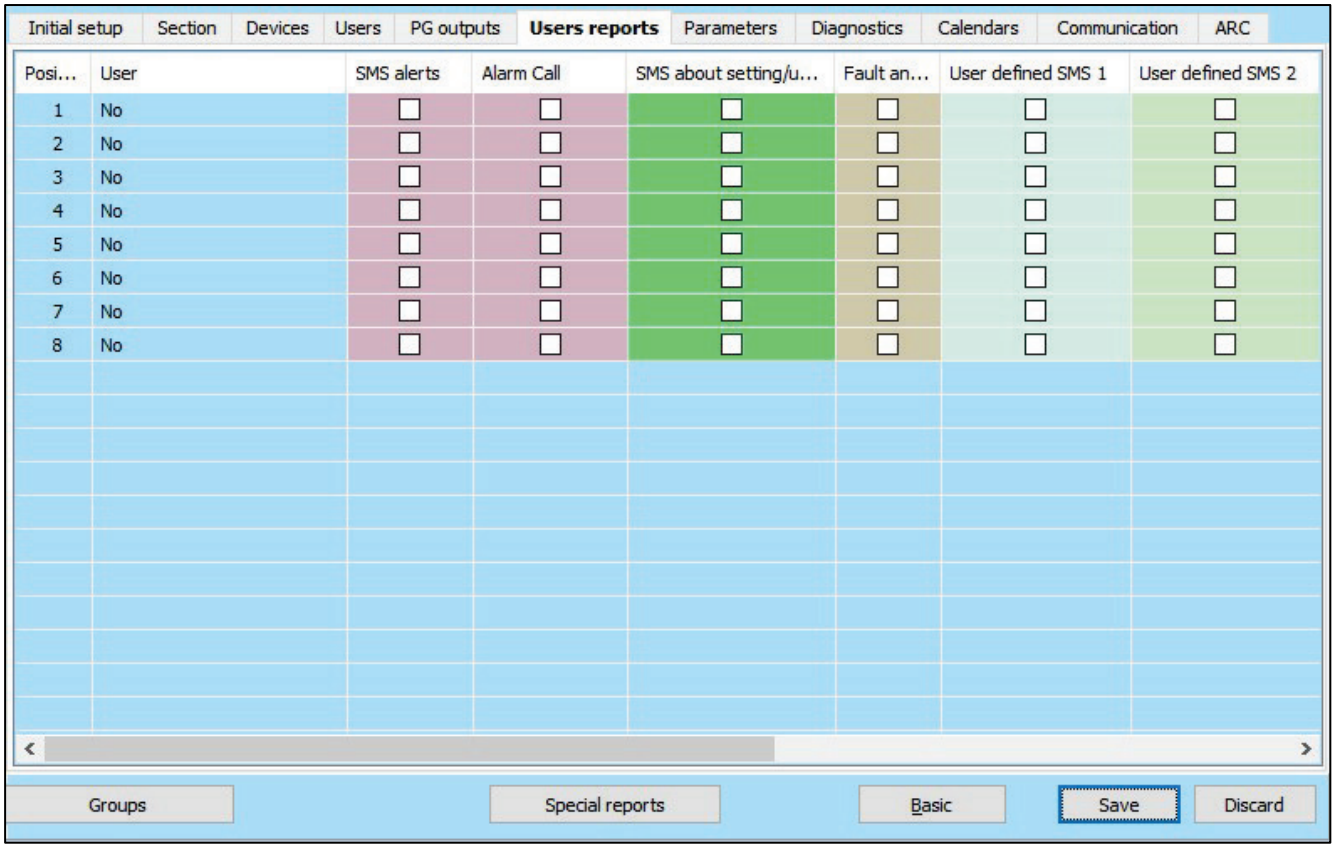
Warning 3: *If the setting Parameters / On F-Link start activate the Service mode automatically and if on connection of the control panel to F-Link the Unset item is selected in the Warning window, after this direct entry to the Service mode, F-Link does not register any possible PG outputs with impulse activation (e.g. activated by a keypad segment and the Enable / Disable function or setting in the schedule. This means that on exiting of the Service mode the question whether these PG outputs should be re-activated does not appear either.*

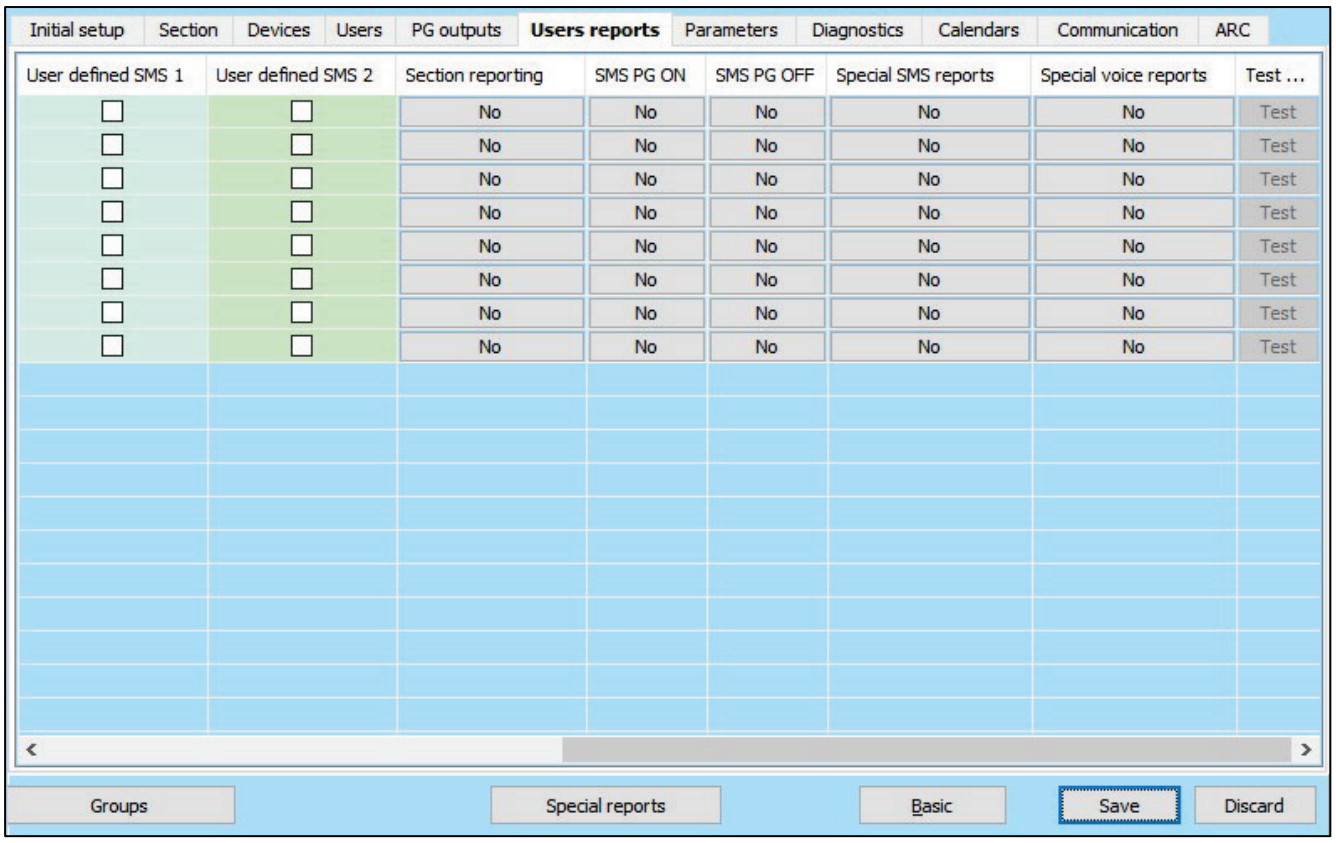
Internal statuses for control of PG outputs:

1. Unset	14. Exit delay	27. Device with tamper activated
2. Any set	15. AC fault	28. No movement in section
3. Partially set	16. AC fault for 30 minutes	29. Ready to be set
4. Completely set	17. Backup battery fault	30. Ready to be partially set
5. Any alarm	18. Internal warning (IW)	31. Unsuccessfull settings
6. Instant alarm	19. External warning (EW)	32. Annual check request
7. Delayed alarm	20. Fault	33. GSM fault
8. Fire alarm	21. Triggered detector	34. LAN fault
9. Panic alarm	22. Any detector triggered except a delayed one	35. PSTN fault
10. Tamper alarm	23. Delayed detector triggered	36. Night mode
11. Alarm memory	24. Bypass in a section	37. Maintenance mode
12. Unconfirmed alarm	25. Device lost 20 minutes	38. Other PG
13. Entrance delay	26. Device with a low battery	39. Event in system

10.8 Users reports tab

This tab is used to define users the system will report selected groups of events to in the form of SMS or voice calls to their phones. The groups and the SMS format are described in the table 9.13 Events reported to users. The basic structure of the voice menu is described in the attached table in a chapter 9.5 System control via communicator voice menu (GSM). To make changes in this tab you do not need to be in the Service mode.





User – enables selection of a user from the list of users.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

SMS alerts – group of selectable alarm reports in the case of which a textual report is sent about an alarm event in selected section, further about a failure or restoration of power supply longer than 30 minutes, setting with an open zone, or possibly a report about an unset section without motion (see the Sections tab).

Alarm call – a group of reports in the case of which (after sending of SMS reports) the system conveys an alarm voice message to the user. The call rings for approx. 30 s. If the call is not answered, the system calls the next user in sequence. If the call is answered, the voice message is sent repeatedly. The structure of the message is: Your alarm reports – Alarm type – Section no. After hanging up of the call by the user, however after 50 s at the latest, the call is terminated and the next user is called. The user can confirm the reception of the call by pressing the **# key** on the phone and after the voice message the user must enter a valid code. When a valid code has been entered, **the alarm is stopped and the next user is not called any more.** For the voice reports universal voice message are pre-set in the system. The voice messages can be re-recorded by replacing the names with the required ones in the voice menu. For Voice menu structure see chapter 9.5 System control via communicator voice menu (GSM).

SMS about setting / unsetting – group of reports for which a text message about setting and unsetting is sent. A setting report is sent with the fixed **delay of 60 seconds** after setting. Setting and unsetting is not reported to the user who has performed it (however it can be set to report in the Users tab). An exception is setting of a common section (done by the control panel, not user).

Fault and service SMS – sends text reports about errors (discharged batteries, entering the Service mode etc.).

User defined SMS 1 – special 1st group where the installation technician may transfer certain events to be reported (typically reports of failures and restoration of power supply, or possibly setting with an active device) only for selected users.

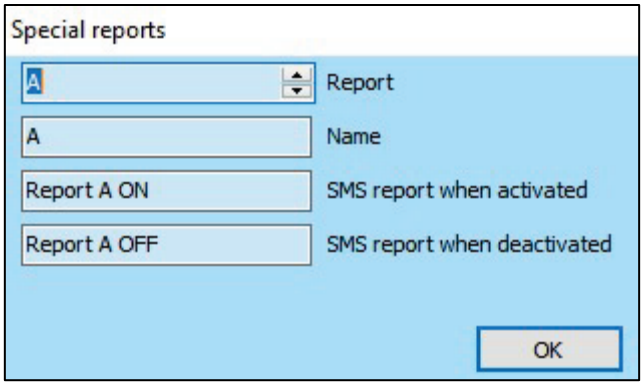
User defined SMS 2 – special 2nd group where the installation technician may transfer certain events to be reported (typically low batteries in devices or low charge level of the backup battery) only for selected users.

Reports from sections – determines which section the selected groups of events will be reported from. If Errors and Service SMS are checked and no section is selected, system errors and service are reported only (they are always assigned to the Section no. 1). There is no link between authorization and the ability of section control.

PG ON SMS* – possibility to report enabling of PG outputs to a user. The messages are sent with a fixed delay of 60 s. The texts of the SMS messages are set in the PG Outputs tab, see chapter 10.7 PG outputs tab.

PG OFF SMS* – possibility to report disabling of PG outputs to a user. The messages are sent with a fixed delay of 60 s. The texts of the SMS messages are set in the PG Outputs tab, see chapter 10.7 PG outputs tab.

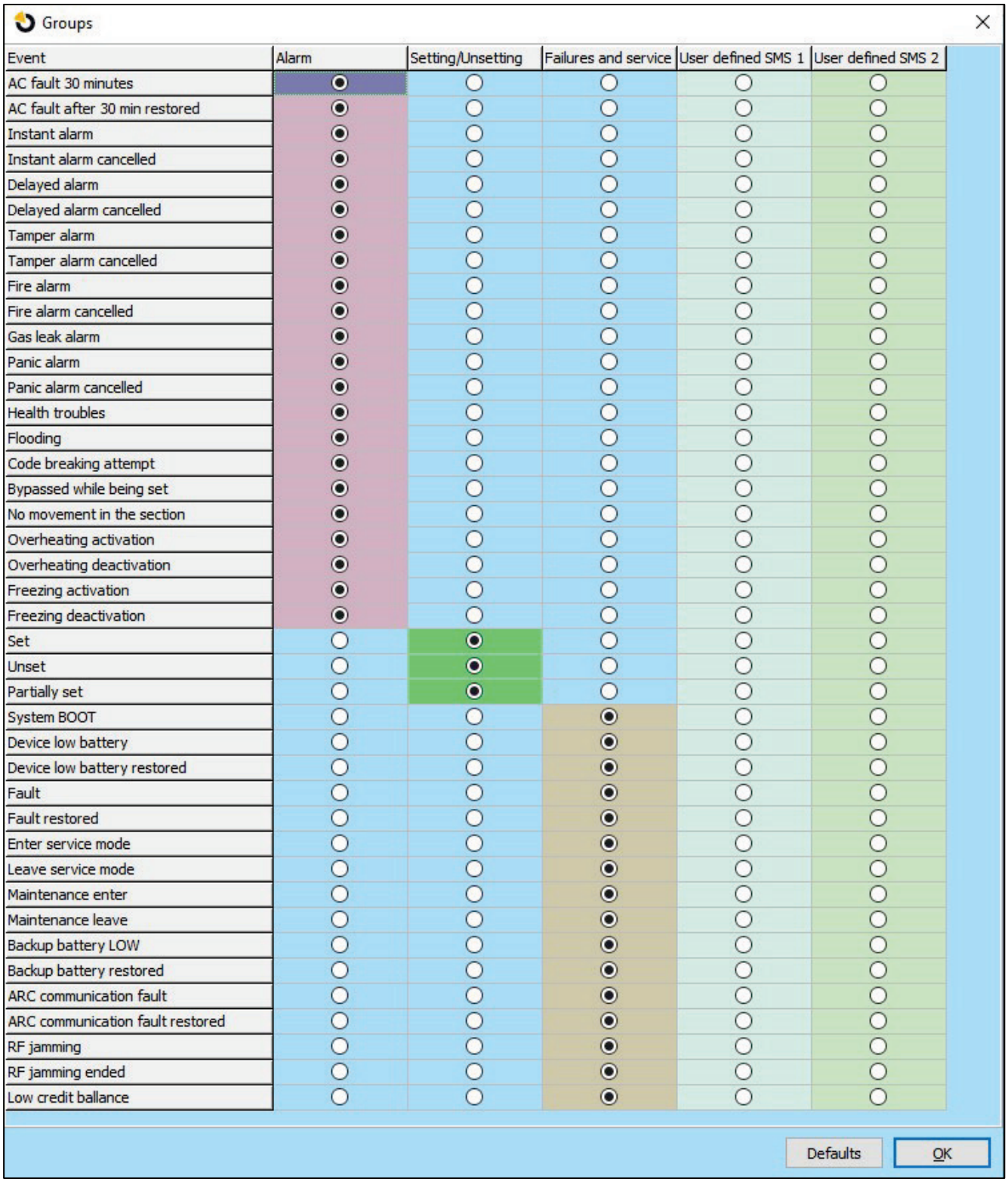
Special Reports SMS* – possibility to report activation of detectors for which the Special Report reaction (A, B, C or D) has been set to the user with an SMS. The texts of special reports are set using the **Special Reports** button on the right at the bottom of the Reports to users tab.



Special Reports by voice* – possibility to report activation of detectors for which the Special Report reaction (A, B, C or D) has been set to the user with a voice message. Voice messages can be re-recorded by calling to the phone number of the control panel where after answering of the call and authorization with the administrator's code you can use the key 9 to enter recording of voice messages, see chapter 9.5 System control via communicator voice menu (GSM).

Test – by pressing of this button the test SMS report will be sent to the user: "Test report, Control Panel, Section 1".

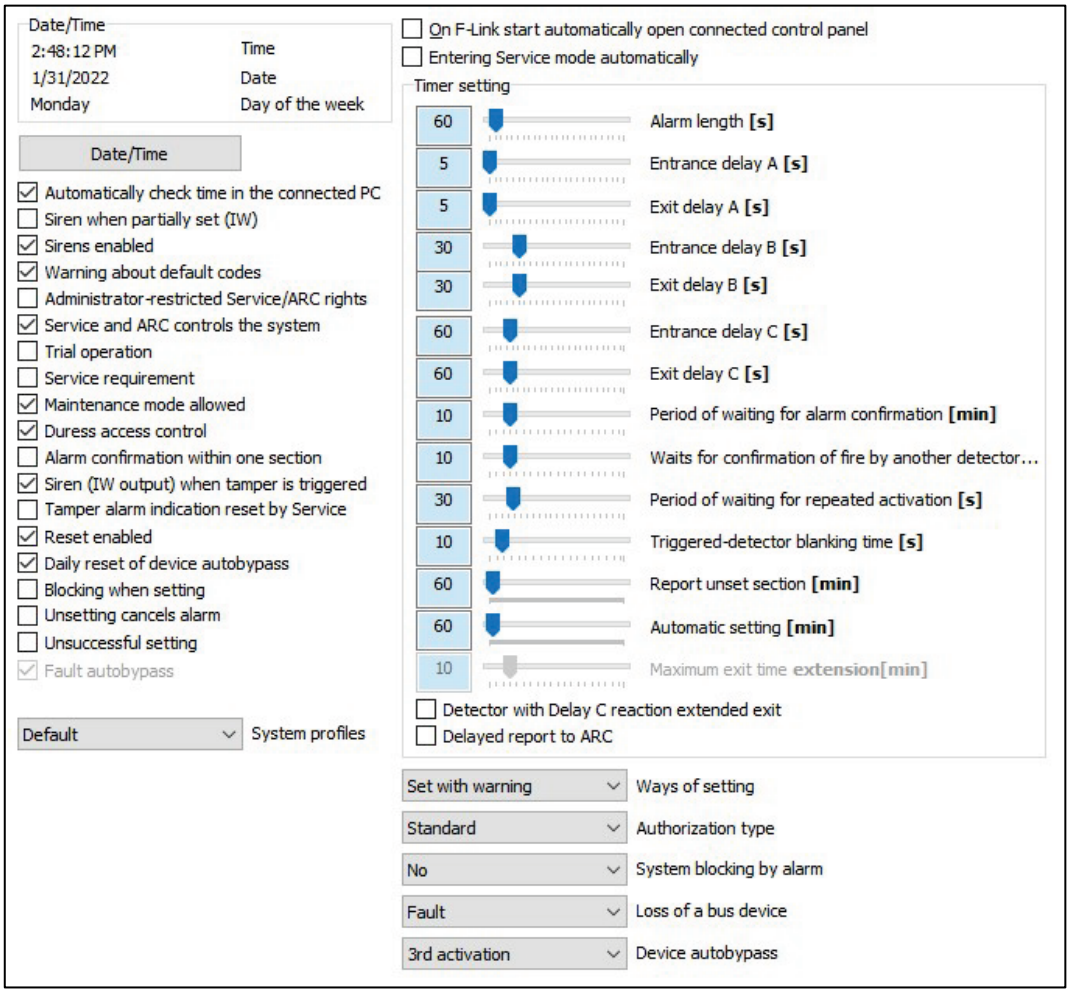
Table of events and pre-set groups:



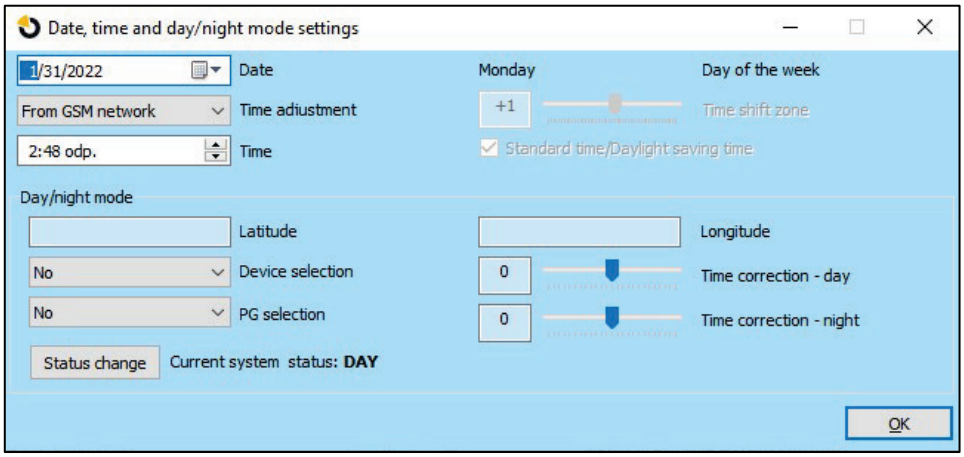
Special reports – The button on the open-programming-table lower toolbar for the setting of name, activation / deactivation SMS and an option for recording reports from A to D in the event memory used as a zone reaction, see chapter 8.4.2 List of applicable reactions.

10.9 Parameters tab

It is used to set parameters and selectable functions of the control panel. The tab is identical to Devices / Control Panel / Internal Settings. To make most of the changes in this tab you do not need to be in the Service mode.



After pressing the **Date/Time** button



* Items marked this way are displayed if **Advanced Settings** are on.

Date	Internal calendar setting.	
Day of the week	Displaying the day of the week.	
Time adjustment*	Internal time and date adjustment method:	
	Manually	Manual setting of the time and data (using the F-Link or JA-100-Link software).
	From the GSM network	Time and date are taken from the GSM provider with every logging in to the GSM network.
	From the JABLOTRON server	Time and date are adjusted automatically according to communication server (GMT 0). Option does nothing when the type of communication is set to “Without remote programming” (factory default setting).

Time shift		Setting the time shift from the GMT 0 time zone.
Time		Internal clock setting.
Standard time / Daylight saving time*		Automatic switching of the winter and summer time can only be selected for manual time adjustment. The change occurs on the last Sunday of March or October, respectively at 1:00 UTC (i.e. e.g. 2:00 CET, or 3:00 CEST).
Day / Night mode	**Latitude**	Input format xx.xxxxxxN (e.g. 50.729058N)
	Longitude	Input format xx.xxxxxxE (e.g. 15.176636E)
	Device selection	Activation of selected device switches the control panel to the Night mode.
	Time correction Day	Time correction option for switching to the Day mode.
	Time correction Night	Time correction option for switching to the Night mode.
Automatically check time in the connected PC*		If the clock of the computer and control panel differ by more than 1 min, F-Link will warn the user of this fact.
Siren IW when partially set		Allows you to set an acoustic alarm with the IW system if the section is partially set (does not apply to Fire and 24 hours alarms).
Sirens enabled*		Enables all BUS and wireless sirens of the system (designed for disabling the acoustic alarm during system testing).
Warning about default codes*		On completion of service an SMS message is sent to the service technician on position 0 that default codes have been left in the system.
Administrator restricted Service and ARC		It blocks independent access of service technicians and ARC to the system. Note: In case of remote access of a technician to the system via F-Link the administrator may get authorized using a keypad in the building. In case of local connection of a technician to the control panel using a USB cable the administrator may get authorized remotely using the voice menu.
Service and ARC control system*		This setting allows the service technician and ARC technician to control the system for all the sections. If this parameter is disabled, the technician is not authorized to control sections and will only be able to enter the Service mode after unsetting of all the sections by the Administrator or a user.
Trial operation		All alarms are limited to 60 s and reported by means of SMS to defined users and the service technician (position 0) although alarm reports are not activated for him. Trial operation is automatically terminated after 7 days from leaving the Service mode.
Service required		If this function is on, 12 months after the last closing of Service mode it initiates the "System requires service check" event in the system, which is, together with the Information icon, displayed on keypads with an LCD screen and registered in the event history. After pressing the "i" key the text "call the service technician" will be displayed together with his phone number. The message on LCD disappears automatically when the service technician locally accesses the system. Then the annual check counter performs a reset.
Maintenance mode		Allows the Administrator(s) to switch the system to the Maintenance mode.
Duress access control		Serves for triggering of a silent alarm by authorization only or by system control (setting, unsetting, PG control, …) when a user is in the presence of an intruder. A Panic alarm is triggered during system control when a code is entered with 1 mathematically added to the last digit's value. This function is available for codes with and without a prefix. **Example:** a user code with a prefix = 4*4444, for duress access control enter 4*444**5**; a user code without prefix = 4444, for duress access control enter 444**5**. **Caution:** When the user code's last digit is 9, for duress access control use **0** as a last digit.
Alarm confirmation within one section*		If confirmation reaction by another detector is set for a detector, this confirmation option can be used to limit confirmation **to the same** section only (otherwise a detector from any section can confirm an alarm). This is valid equally for intrusion detectors and for fire detectors.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Siren (IW output) when tamper is triggered*	A siren with the IW response acoustically indicates a tamper alarm if the zone is unset or partially set. If fully set, the siren indicates the tamper alarm always.	
Tamper alarm indication reset by Service*	The tampering memory indication can only be reset by a service or ARC technician. If this option is not checked, the indication may also be reset by the Administrator (but not User).	
Reset enabled*	Possibility to lock reset of the control panel with a jumper on the board. If reset is prohibited and the service code is lost, the control panel can only be unlocked by the manufacturer. Reset of the control panel is described in chapter 12 Reset of the control panel.	
Daily reset of device autobypass*	The option only relates to activation inputs (not tamper and error inputs). If this option is enabled, the system will automatically reset autobypassed devices every day at 12:00. If the option is disabled, autobypass of the device will only be reset with a status change of the section. This option is suitable e.g. for the use of detectors with a 24hr reaction or flood detectors that are found in a section where setting/unsetting is not necessary.	
Blocking when setting	If enabled then all active inputs will be blocked during setting the section and they cannot trigger an alarm in this guarding period anymore. If disabled, all active inputs will be bypassed temporarily until they go to standby and detectors start guarding again (risk of false alarm triggering – e.g. improperly closed window).	
Unsetting cancels alarm	A function which determines if an alarm will be cancelled by authorization of a valid code only or by unsetting the section with an alarm. If enabled, the alarm can be cancelled with unsetting of a section where an alarm has been triggered or from the LCD keypad menu by pressing on “Cancel warning indication”.	
Unsuccessful setting	The function is processed during every setting procedure. If an instant zone is triggered within the exit time or a delayed zone stays open when the exit time expires, the system is not set and triggers an “Unsuccessful setting” event and records it in the history. It is also reported by an SMS to a pre-set user if the event “SMS about unsuccessful setting” is enabled to be sent. It is indicated by keypads and also by an outdoor siren. To cancel the indication about unsuccessful setting it is necessary to press “Cancel warning indication” in the LCD keypad menu.	
Fault autobypass	It is only available when one of the system profiles “EN50131-1” or “INCERT” is chosen. It is meant for disabling of the limited number of triggered faults from 3 faults maximum to no limit.	
System profiles	Selection from pre-set system profiles according to requirements.	
	Default	Parameters set by factory default with the option to modify them according to needs.
	EN50131-1, Grade 2	Some parameters are pre-set automatically to comply with EN50131-1, grade 2 (low – middle risks) with no option to be modified.
	INCERT, Grade 2	Some parameters are pre-set automatically to comply with the INCERT norm, grade 2 with no option to be modified.
	SSF 1014, Grade 2	Some parameters are pre-set automatically to comply with the SSF 1014 norm, grade 2 with no option to be modified.
Ways of setting	Selection of the way the system manages the setting process. From the lowest level when the system can be set regardless of active devices and faults in system to the highest level when the system cannot be set at all with active devices (instant zone). Linked to the system profile option.	
	Set always	Set always regardless of the system status (faults, active devices...).
	Set with warning	Optically indicates (on segment and display) the system status (faults, active elements…) for 8 s and sets automatically once this period expires. Setting is also possible by repeatedly pressing the segment or by pressing the ENTER key.

	Set after confirmation	Optically indicates (segment and display) the system status (faults, active elements…) for 8 s. Can be set ONLY by repeatedly pressing the segment or by pressing the ENTER key.
	Don't set with an active element	Optically indicates (segment and display) the system status (faults, active elements…) for 8 seconds. Can be set by repeatedly pressing the segment or by pressing the ENTER key but only if the active detector is of the DELAYED or NEXT DELAYED reaction type. An active element with any other alarm reaction CANNOT be set this way. ATTENTION!!! this also applies to remote control (Voice menu, SMS, MyJABLOTRON, action through calendar except "Set always").
Authorization type	Selection of the way the system processes user authorization. Related to controlling a PG output with authorization.	
	Standard	Entering a user code or using an RFID card/tag will accomplish valid authorization. Just one of these options is necessary to control the system.
	Card confirmation with code	Users assigned with cards and codes must authorize themselves with both (regardless of the order of authorization). If users have either cards or codes, they will authorize themselves according to the Standard option. Remote phone access is enabled for authorized numbers only.
	Double authorization	Entering a user code and using an RFID card will accomplish valid authorization (regardless of the order of authorization). F-Link monitors whether a code and a card are assigned to a user in the Users tab (otherwise F-Link won't allow you to save the configuration). Remote phone access is enabled for authorized numbers only.
System blocking by alarm	The parameter allows blocking the system after first alarm triggering (intrusion or tamper) to avoid further alarms to be triggered. Unblocking can be performed by a special code for Unblocking or by authorized access from the ARC (meant for Great Britain). Unblocking after tamper alarm triggering can be performed also by a user with a service authorization (meant for the Benelux area).	
	No	No blocking
	By tamper alarm	The system is blocked when a tamper alarm is triggered (by opening the device, by RF jamming or by 10 incorrect code entries, etc.).
	Any alarm	The system is blocked by triggering any alarm (intrusion, fire alarm, flooding, 24hr alarm or panic alarm).
Loss of a BUS device	The control panel processes the loss of a device or a short circuit on the system BUS. According to the selected option system will react to occurred situation:	
	Fault	The control panel always processes the loss of a device on the BUS or a short circuit of the BUS as a Fault.
	Tamper always	The control panel processes the loss of a device on the BUS or a short circuit of the BUS as a tamper alarm always when it occurs. If the radio module has RF jamming detection allowed and it is detected then it also triggers a tamper alarm. A tamper alarm is also followed by a fault and when the fault disappears, it cancels the tamper alarm as well.

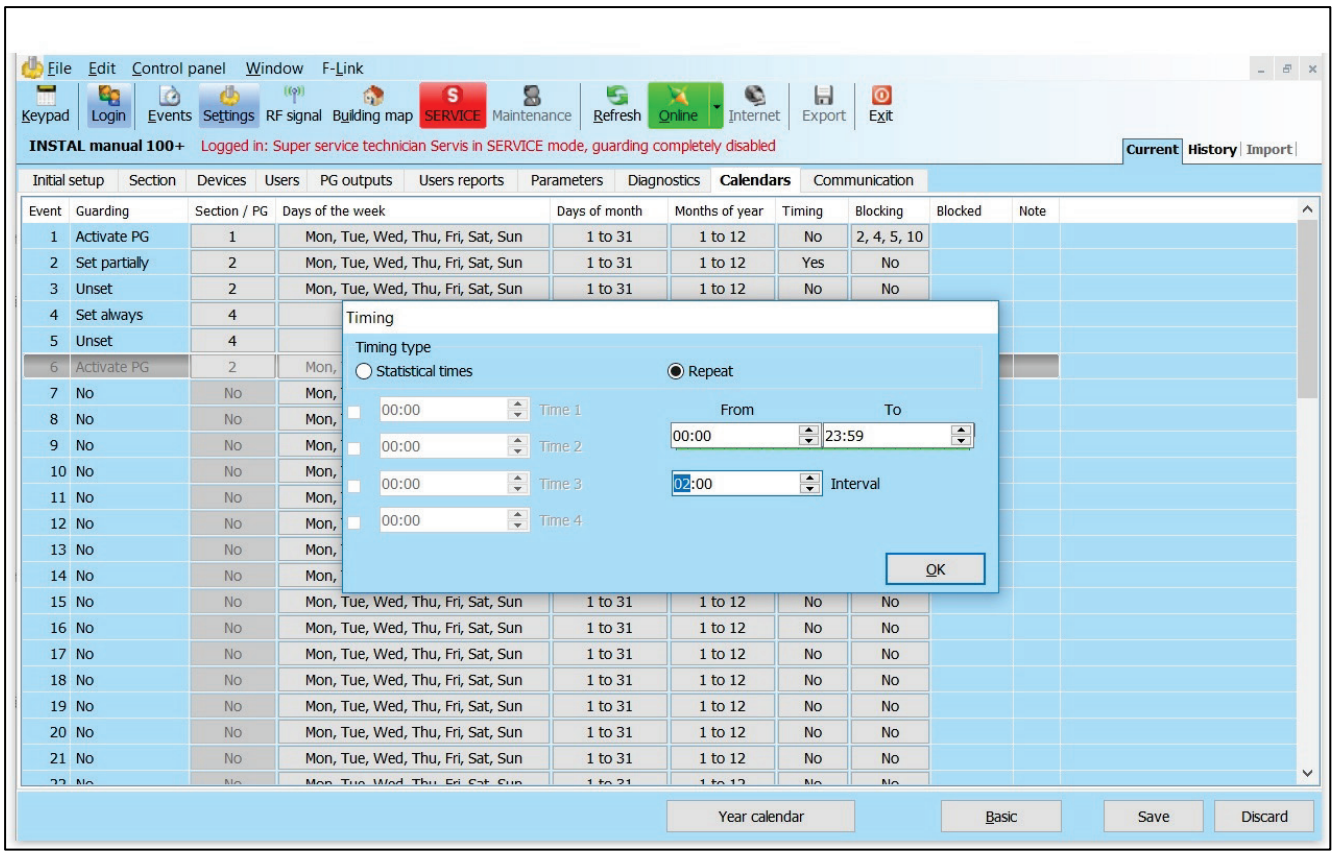
JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

	Tamper after confirmation	The control panel processes the loss of a first device as a fault and if within a pre-set time given by the parameter “Period of waiting for alarm confirmation” another device loss occurs, then the system confirms it and triggers a tamper alarm. When the faults of all the lost devices are restored then the system cancels the fault and tamper alarm.
Device autobypass	The option serves for the selection of the method of autobypassing.	
	3rd activation	The device will be bypassed after being triggered 3 times in one setting period regardless of the alarm length. Any other attempts to trigger the device will be ignored, until unsetting the section.
	3rd alarm	A device enables triggering 3 times during 1 alarm period. The particular device will be bypassed after 3 alarm periods, meaning after the device could have been triggered up to 9 times.
On F-Link start automatically open connected control panel	If the control panel is connected to a PC via the USB cable, the connection is established automatically when the F-Link software starts.	
Entering Service mode automatically	Automatically enters the Service mode when the control panel is connected to a PC via the USB cable. If some sections are set, you will be asked about unsetting with authorisation. If default codes are still in use, the authorisation is not required.	
Timer setting	In each section, the entrance and exit delays A, B and C are measured separately. If different exit delays are defined for detectors within one section the longest delay is measured. In case of different entrance delays the one that belongs to the activated detector is measured. If more detectors are activated, the shortest one of the defined entrance delays is measured. Detectors with delay C can extend the duration of the exit delay (see the option “Detector with the Delayed C reaction extends exit” in the Parameters tab).	
Alarm length	Alarm length – valid for all sections. Range 5 s – 20 min.	
Entrance delay A	Timer A. Range 5 s – 2 min.	
Exit delay A	Timer A. Range 5 s – 2 min.	
Entrance delay B	Timer B. Range 5 s – 2 min.	
Exit delay B	Timer B. Range 5 s – 2 min.	
Entrance delay C	Timer C. Range 5 s – 6 min.	
Exit delay C	Timer C. Range 5 s – 6 min.	
Waits for confirmation of intrusion by another detector	Waiting time for alarm confirmation by another detector of a set section. Valid for all detectors with the reaction Confirmed immediate / Confirmed delayed A (1 – 60 min.).	
Waits for confirmation of fire by another detector	Waiting time for fire alarm confirmation by another detector. Valid for all detectors with the reaction Fire confirmed. (1 – 60 min.).	
Waits for repeated activation of the detector	Waiting time for repeated activation of the same detector. The set time must be longer than minimum detector restoration before repeating. Valid for all detectors with the reaction Repeated immediate / Repeated delayed A (6 – 120 s).	
Triggered-detector blanking time	Minimum time for which the detector is not evaluated before it can repeat the activation. Valid for all detectors with the reaction Repeated immediate / Repeated delayed A (5 – 60 s).	
Report when unset after	Time after which an unset section reports unsetting if no detector has been activated in it (the reporting is enabled in the Section tab – Report unset section (5 – 2880 min.).	
Automatic setting	Time after which a section where an event “Unset section” was reported is set automatically (0 – 120 min.).	
Maximum exit time extension	Maximum time the exit delay is extended by an active delayed detector in the section. Only functional together with the option “Detector with the Delayed C reaction extends exit delay”. If the detector is activated for a longer time, the section is set and the detector is bypassed (1 – 60 min.).	

Detector(s) extend exit delay C	The “garage gate function” – an active detector with the Delayed C reaction (open gate) extends the exit delay in the respective section. Such an extension may only be caused by detectors with a status reaction (typically opening detectors). The maximum time of possible extension is set through the previous option.
Delayed report to ARC	When enabled, an Internal alarm will be triggered after the entrance delay has timed out, but the system waits for 15 s to send an alarm report to the ARC. A user has 15 s more to unset the system without triggering an alarm reported to the ARC.

10.10 Calendars tab

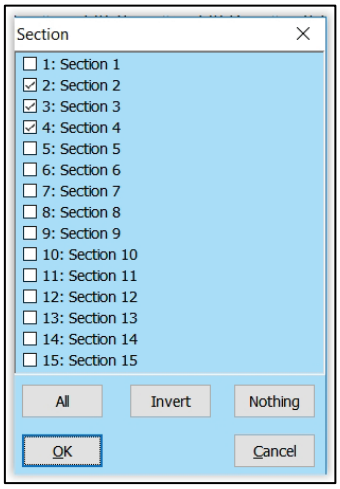
Here, you can set the time schedule of actions that the system will carry out automatically and regularly. To make changes in this tab you do not need to be in the Service mode.



Guarding – allows you to set, which action should be executed for section or PG output (Unset, Set, Partially set, PG control, Service requirement). Possible variants are “Immediately” (no exit delay) and “Always” (does not respect the pre-selected way of setting). The Service requirement action triggers the same event in the system as the Service requirement option in the Parameters tab.

Section/PG – specifies in which section(s) the action of the set type is executed or which PG output(s) are controlled.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



Days of the week – defines on which days in a week the action is executed (e.g. every Monday).

Days of the month – defines on which days in a month the action is executed.

Months of the year – defines in which months of a year the action is executed.

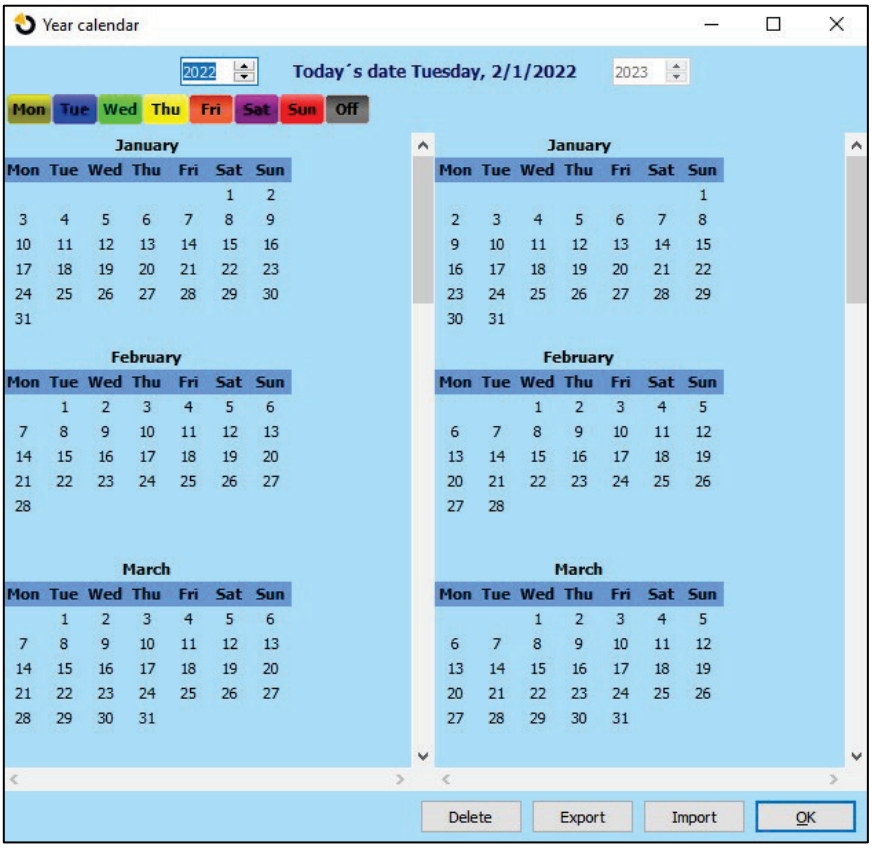
Timing – the system allows you to set up to 4 times in one day or a time interval of a regular repeating of the required action. The repeating can be defined as a time FROM – TO.

Blocking – PG outputs are offered here; their activation allows blocking a calendar action.

Disable – possibility to block a particular action. Disabling is indicated by a red dot. The Administrator (using JA-100-Link) and Service Technician (using F-Link) are authorized to disable the scheduler action.

Note – provides the possibility of customized description of scheduled actions.

Annual schedule – allows you to change the attribute of days (Mo, Tu, ...Su) for individual days of the current and next year. You can change the attributed by (repeated) clicking of the mouse button on the corresponding day. Application example: For a public holiday (non-working day) falling on Wednesday you can change the attribute of the day from Wednesday to Sunday. Actions that are automatically planned in accordance with the basic settings of the Schedule and valid for working days are not carried out on this day. However, the program valid for Sundays will be kept. This way you can adjust the control of Sections or PG Control e.g. also for company holidays etc. The “Off” attributed means disabled – on days indicated like this no scheduled action is executed.

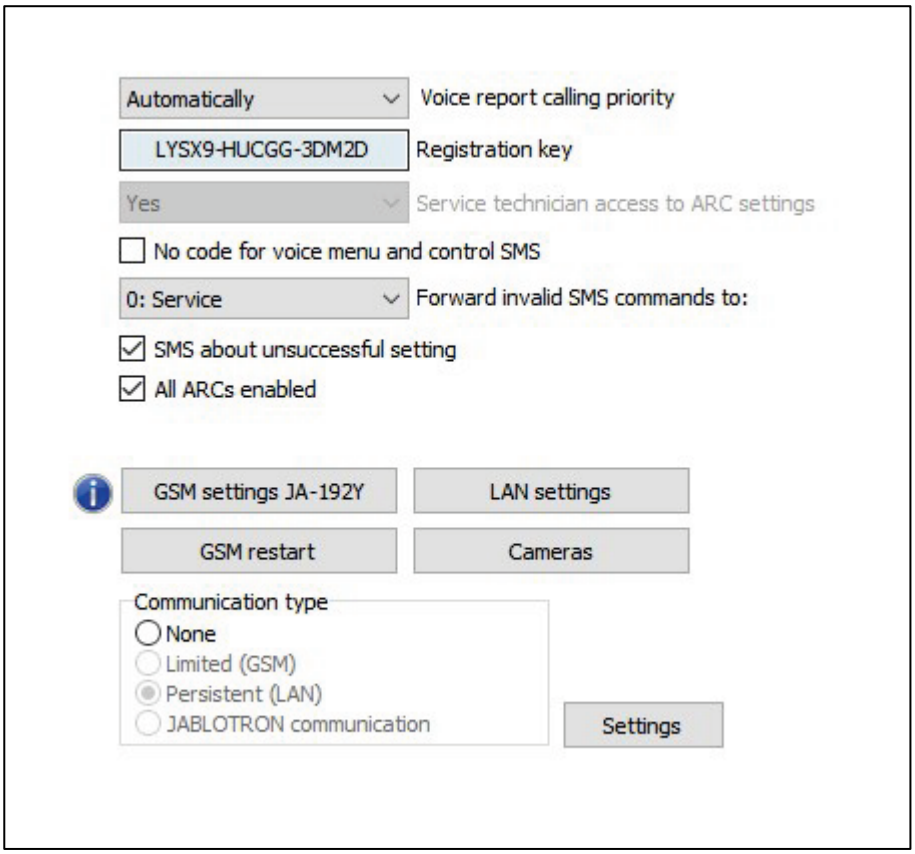


Notes:

- Switching an application on and off for a certain time is possible in 2 ways. You can either set an action for enabling and an action for disabling the PG output or only an action for enabling and set an impulse of the required length for the PG output.
- If you select Setting (Partial setting) of a specified section, at the specified time an exit delay with the fixed time of 3 min is first activated. All sensors in the specified sections with the Immediate reaction are readjusted to have the Delayed reaction during this 3 min period. If you select Set immediately, setting is executed immediately without an exit delay and all the loops are active immediately (including delayed detectors).

10.11 Communication tab

The tab is used to set the behaviour of communicators and the way of communication. To make changes in this tab you do not need to be in the Service mode.



Voice report calling priority – selecting the channel that the control panel will use to report voice events (options GSM).

Registration key – unique registration number of the control panel.

Service technician access to ARC settings – allows the ARC technician to limit the access of the Service technician to the ARC tab.

Voice menu without code – when using an authorized phone to control a function by calling, the user does not have to enter his/her code (he/she is authorized by calling from his/her phone). For this function the caller's identification (CLIP) must be activated.

Forward invalid SMS commands – selecting the user where SMS messages that are incomprehensible for the control panel will be forwarded (invoicing information from the operator etc.).

SMS about unsuccessful setting – the control panel sends SMS about unsuccessful setting. When unsuccessfully set with authorization (by an authorized user), the SMS is sent to this user When unsuccessfully set without authorization, the SMS is sent to the Administrator on position 1.

All ARCs enabled – option to disable all communication to ARC – unavailable it the ARC technician restricted the access.

Communication type – the system offers several methods of remote communication/configuration:

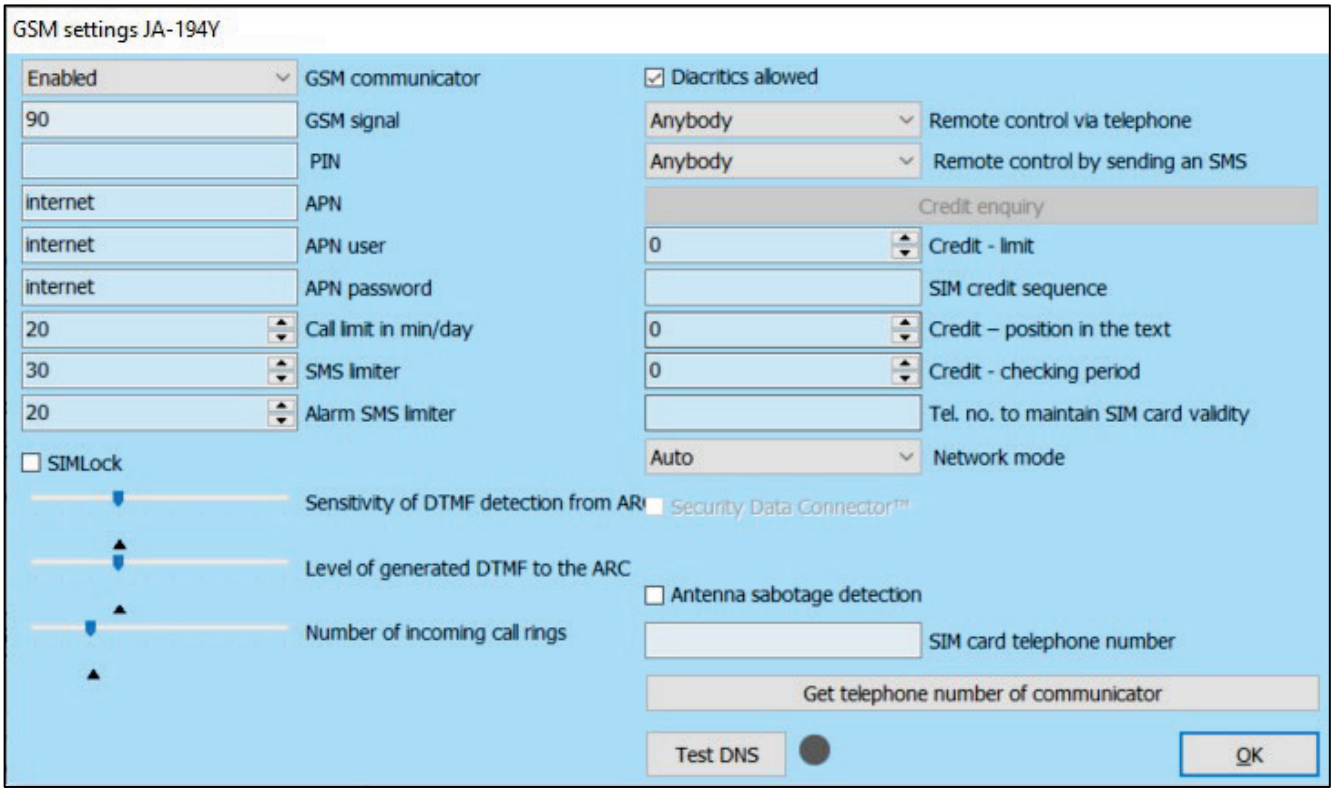
- **None** – it behaves like an autonomous device with its own SIM card. The device communicates outwards (sends SMS and voice messages) and receives command SMS and has a functional voice menu. Remote configuration with the F-Link software is not possible.
- **Limited (GSM)** – communicates like the previous type and in addition it supports remote configuration of the system. Remote configuration is possible from a computer with the F-Link (JA-100-Link) software with an Internet connection. To establish connection to the control panel F-Link connects to the manufacturer's server to provide it with the registration code and phone number of the SIM card inserted in the control panel communicator. There must be functional data communication in the control panel (LAN or GSM/GPRS).
- **Persistent (LAN)** – the control panel maintains a permanent data communication with the server, it allows remote connection with the F-Link software is possible.
- **JABLOTRON communication** – the device communicates with the manufacturer's server (MyJABLOTRON application) and continuously sends information about the device status to it. Thus, if the F-Link (JA-100-Link) sends a request for remote connection, the server is immediately ready to establish connection. In addition, this communication allows the user to use server services. Applications allowing the user to operate the system can be installed in mobile devices with the Android or iOS systems. For this option it is necessary to use the JABLOTRON Security SIM card.

Contact your distributor for information about the possibilities of using each communication type in your country.

Settings – the button serves for registering the system to CLOUD service MyJABLOTRON. When you fill in the form and send the data for confirmation then it creates a registration request. Confirmation of the filled in form will be done in a few moments.

10.11.1 GSM Settings

The button is used to set parameters and behaviour of the GSM communicator.



* An item marked like this is set automatically after activation of the control panel if a GSM communicator was installed and a functional SIM card was inserted into it before activation (service of the JABLOTRON server).

GSM communicator – possibility to switch off the communicator.

GSM signal – information about the signal strength in percent (it is measured once every minute). For proper function the signal should be at least 50%. If you encounter problems with GSM signal quality, you are recommended to test a SIM card of another operator. You are not recommended to use a directional or gain GSM antenna for the communicator (it only reduces connection of the module to 1 network cell = unstable communication). You can also get information about the signal quality using the SMS command STATUS (see chapter 9.6 SMS commands).

SIM Card PIN – we recommend using a SIM card with the PIN code disabled.

Network APN* – GPRS data communication settings. Data communication provides access to services of the JABLOTRON server, enables remote access of a service technician, communication with the ARC etc. Besides the APN settings the used SIM card must support data transmission.

Contact your JABLOTRON distributor for more information about the possibility of this communication.

APN User* – name (do not enter one unless the network uses it).

APN Password* – password (do not enter one unless the network uses it).

Call limit min./day – limits the range of actual calling to 5 to 250 minutes a day.

SMS limiter – the limiter limits the number of SMS sent per day from the control panel. It includes alarm and also non-alarm events (alarm events - alarm, tamper, fault, report, …; non-alarm – PG, service…). The range to be sent is from 5 to 250 SMS. The system can send maximum 250 SMS per day. This maximum is split between the *SMS limiter* and the *Alarm SMS limiter* (F-Link automatically checks that setting both limiters doesn't exceed 250).

Alarm SMS limiter – the limiter limits the number of alarm SMS per day from the control panel if the limit of sent SMS has already been reached (*SMS limiter*) It is related to alarm events (alarms, tampers, faults, reports, ...). The range to be set is from 0 to 245 SMS. **Example:** The *limiter of sent SMS* is set to 30, the *limiter of alarm SMS* is set to 20. The system behaviour will be like the following: When for one day any type of 30 SMS are sent (alarm and non-alarm), the system won't send any non-alarm SMS that day. But it can still send alarm SMS (but 20 is the maximum). This ensures that the system always has some reserve for the case of an alarm to be able to inform the user by SMS.

Allow diacritic – if international character accents (ICC) are allowed, reports can be sent from the system via more than one SMS text message. ICC must be enabled if you use e.g. Russian alphabet in your texts etc.

Remote control via telephone – setting the possibility to control the system remotely using the voice menu. If Users are selected, the menu can only be accessed from the phones of defined users (in the Communication tab you can even allow users to enter the voice menu without entering their user code – the Voice menu without code option). If "Anybody" is selected, the voice menu can be accessed from any phone. However, on accessing the menu the user is always requested to enter the user's code.

This function is directly dependent on the **Authorization type** settings on the **Parameters** tab. Choosing a different means of authorization besides **Standard**. **Prevents utilization** of GSM control by **anyone**, as the system needs to recognize an user with a specified phone number, and as a means of secondary authorization, their alarm code.

Remote control by sending SMS – setting the possibility to control the system remotely with the use of SMS commands. If Users are selected, the system only accepts SMS commands from the phones of defined users (in the Communication tab you can even allow users to use SMS commands without entering their user code – the Voice menu without code option). If "Anybody" is set, an SMS command can be set from any phone; however, it is conditional on entering the access code.

This function is directly dependent on the **Authorization type** settings on the **Parameters** tab. Choosing a different means of authorization besides **Standard**. **Prevents utilization** of GSM control by **anyone**, as the system needs to recognize an user with a specified phone number, and as a means of secondary authorization, their alarm code.

Credit enquiry – by pressing this button you can immediately get information about the credit balance from the operator's answer (it this function is support).

Credit - limit – possibility to set the lower limit for automatic checking of the limit of a pre-paid SIM card. If the established credit is below this limit, the system will send and information SMS to the person whom the reports SMS Errors and Service are assigned to. **Caution: You are not recommended to use a pre-paid card in the system – they increase the risk of a communication failure.**

SIM credit sequence – command for automatic checking of the credit balance of a pre-paid SIM card (if supported by the operator). You can obtain the command from your operator.

Credit - position in text – position (sequential number of the character) in the operator's credit balance report at which the numerical information about the credit balance starts (the communicator only looks for numerals in the report and ignores the other characters).

Credit - checking period – setting how often the system will check the credit balance (you can set 0 to 99 days where 0 is off).

Tel.no. to maintain SIM card validity – if the pre-paid SIM card requires maintaining calls, you can set a phone number which the system will dial automatically (e.g. the exact time service) if there has not been any outgoing call from the system for a period longer than 90 days (10 s after answering of the call by the called party the system will hang up).

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

SIMLock – function that links the phone number of the SIM card to the ARC settings. It means that if you replace the SIM card with another one and the SIM will be logged in to the GSM network, all the settings of the **ARC tab will be deleted.** The deletion is irreversible and other settings (registration to the MyJABLOTRON web service) must be performed by the ARC technician once again.

Sensitivity of DTMF detection from ARC – setting the sensitivity of reception of the signal generated by the ARC. The sensitivity is adjustable in 10 steps; the optimum default value is 4.

Level of generated DTMF to the ARC – setting the intensity of the transmitted tone dialling signal in DTMF generated by the control panel. The intensity is adjustable in 10 steps; the optimum default value is 4.

Number of incoming call rings – number of ringing impulses until automatic answering by the communicator. You can set answering after 1 to 10 ringing impulses (corresponding to 5 to 50 seconds). The default value is 3 (15 seconds).

SIM card telephone number – telephone number of the SIM card used in the communicator.

Get telephone number of communicator – the SMS request is sent when the button is pressed. After a successful response the phone number will be displayed in the “SIM card telephone number” box.

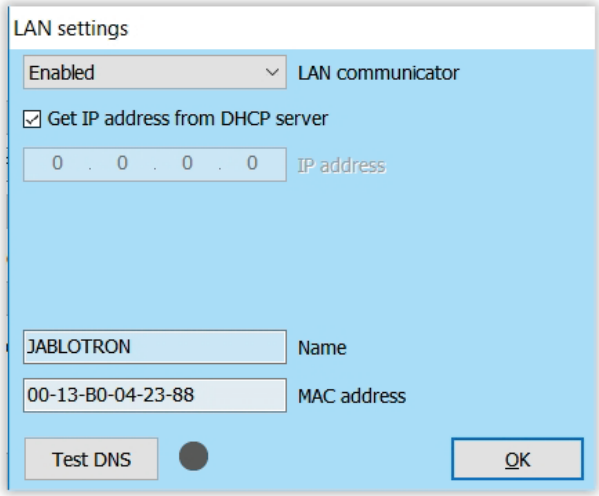
[1]**Security Data Connector ™** – The Security Data Connector ™ service is used in the control panel. All GSM parameters are pre-set automatically and cannot be modified.

[1]**GSM provider switching** – This option allows automatic switching between GSM providers

Network mode - Selection of the network that the control panel will use for communication (*Auto; 2G; 3G; 4G*). When the parameter is changed, the change will take effect 5 minutes after the F-link is disconnected from the control panel. If there are problems with *Auto* mode, we recommend selecting 2G, this will limit switching between other networks and reduce the time the control panel is out of signal.

[1] – Items marked like this are available when Security Data Connector ™ is used

10.11.2 LAN Settings



It is used to set the LAN communicator (if the control panel contains one).

LAN communicator – possibility to enable or disable LAN communication.

Get IP address from the DHCP server – automatic setting of network parameters. If this function is not supported by the network, the respective parameters must be entered manually. Manual entry is only possible if this option is unchecked.

IP address – setting for manual IP address assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.99.

Subnet mask – setting for manual subnet mask IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 255.255.255.0.

Gateway – setting for manual default gateway IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.1.

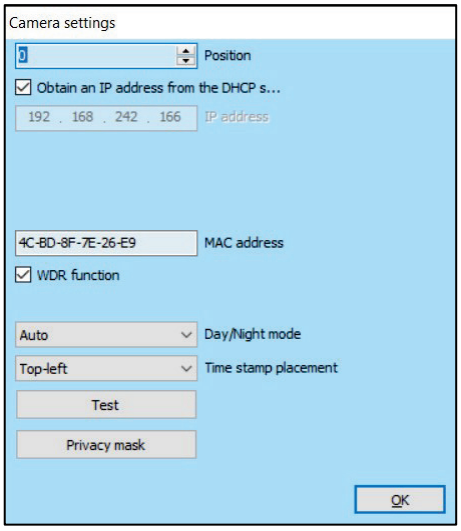
DNS server – setting for manual DNS server IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.1.

Name – device name for easier identification in the local network.

MAC address – unique address of every LAN device (identification of data source).

Test DNS – when the LAN communicator is connected to the Internet, the settings can be tested for correctness. If a green dot appears after pressing of the button, the connection to the server has been established, but if a red dot is displayed after a few seconds, the time for establishing the connection has expired, which indicates an incorrect setting or an error in the LAN communicator connection.

10.11.3 Cameras



The Cameras button allows you to perform a connectivity test (if the required ports are allowed) and a test of connection speed. After the test is successfully finished, a graph is displayed together with a proposition of how many cameras in which resolution can work in that particular network. If there is already an active camera connected in the network, in the F-Link you can set its basic parameters.

Position – position in the system

Get IP address from the DHCP server – automatic setting of network parameters. If this function is not supported by the network, the respective parameters must be entered manually. Manual entry is only possible if this option is unchecked.

IP address – setting for manual IP address assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.99.

Subnet mask – setting for manual subnet mask IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 255.255.255.0.

Gateway – setting for manual default gateway IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.1.

DNS server – setting for manual DNS server IP assignment that is only available if automatic assignment from the DHCP server is not enabled. The default setting is 192.168.1.1.

MAC address – unique address of every LAN device (identification of data source).

WDR function – disabling the WDR (Wide Dynamic Range – backlighting compensation) for e.g. areas with a high contrast of bright and dark places.

IR illumination – disabling the IR illumination for e.g. areas with permanent lighting.

Camera mode – selection of the camera mode, you can select between Day, Night and Automatic mode.

Time stamp placement – allows you to display time, date, and name of the camera in the saved record, the option declares in which corner are information displayed.

Test – tests camera functionality and displays the current view as a reference image.

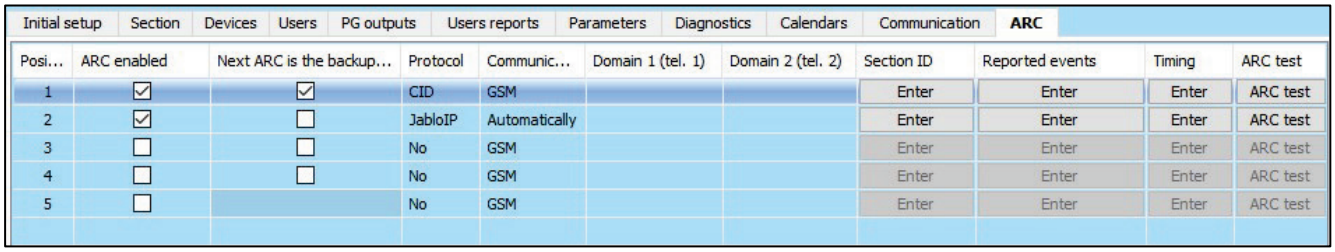
Privacy mask – allows to cover part of the image with a black pattern, e.g. to capture public areas

10.11.4 GSM Restart

Button for logging the communicator out and logging it in the network again. It may take tens of seconds to log the GSM communicator in the network again (depending on the current status of the system). GSM can also be restarted using the SMS command GSM (see chapter 9.6 SMS commands).

10.12 ARC tab

This tab is used to set communication for alarm receiving centres. If in the Communication tab the access of the service technician is restricted, this parameter can only be set by a person with the ARC Technician authorization level. The option is also unavailable if the JABLOTRON communication is selected, which considerably simplifies setting of the communication part of the system. To make changes in this tab you do not need to be in the Service mode.



ARC enabled – possibility to disable the set communication.

Next ARC is the backup - if enabled, the next position will only be used if data cannot be transmitted from the current one.

Protocol – transmission protocol setting.

Communicator – if the selected protocol can be transmitted to ARC in more ways, the communicator type is selected here. The options are GSM, LAN, Phone line and Automatically, but only the currently available options are visible. The Automatic option uses a combination of LAN/GSM communicators, which primarily uses LAN and in a case of unavailable LAN switches to backup GSM. In case of failure of transmission from both communicators the system reports a fault – data not transferred to ARC.

Domain 1 (phone 1) – setting of the main domain (using URL or IP address), or the main phone number depending on the used protocol. If IP communication is used, you must enter the communication port after the IP address, separated with a colon. You will obtain the communication port and IP address data from the ARC the communication is routed to. If no communication port is filled in, the event will not be transmitted.

Domain 2 (phone 2) – setting of a backup domain (using URL or IP address) or a backup phone number depending on the used protocol.

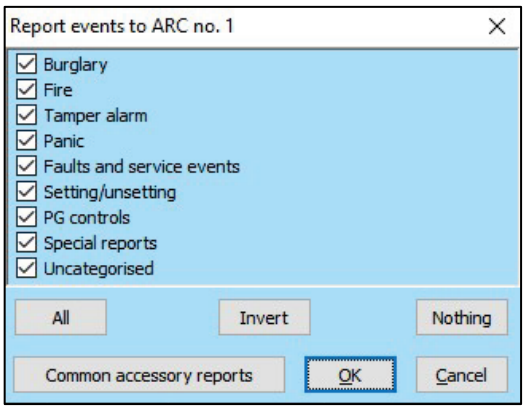
Section ID – setting of the building identification (common for the whole building or individually for sections). Warning: The default setting is zero, with which the communicator will not send any reports!

Reported events – selecting types of reported events and the possibility of setting codes of supplementary reports (PG outputs, special reports A to D).

Timing – setting the time limits for transmissions and setting the connection checking period.

ARC test – by pressing you will start a manual test to check connection with the respective protocol.

Note – here, you can note details of ARC settings, commencement date of the service etc.



10.12.1 JABLOTRON CID and SIA codes

CID	SIA	EN	Report category
		Activation events	
1101	QA	Health problem	Burglary
1110	FA	Fire alarm	Fire
1118	FG	Unconfirmed fire alarm	Fire
1120	PA	Panic alarm	Panic
1130	BA	Instant alarm	Burglary
1130	BA	Keybox	Faults and service events
1133	BA	24H alarm	Burglary
1134	BA	Delayed alarm	Burglary
1138	BG	Unconfirmed alarm	Burglary
1144	TA	Tamper of periphery	Tamper
1151	GA	Gas Leak	Fire
1154	WA	Flood alarm	Burglary
1158	KA	Overheating	Uncategorised
1159	ZA	Freezing	Uncategorised
1170	UA	Special Reaction A	Faults and service events
1171	UA	Special Reaction B	Faults and service events
1172	UA	Special Reaction C	Faults and service events
1173	UA	Special Reaction D	Faults and service events
1174	UA	Not used	Uncategorised
1300	ET	Fault	Faults and service events
1301	AT	AC loss	Faults and service events
6301	AT	AC loss longer then 30 min	PG controls
1302	YT	Low ACU control panel	Faults and service events
1305	RR	System boot	Faults and service events

1306	LB	Entering service	Faults and service events
1308	RE	System shutdown	Faults and service events
1313	YX	Bloceked after alarm -Engineer reset	Uncategorised
1314	YG	ARC setting has been resetted	Uncategorised
1344	XQ	RF interference	Faults and service events
1350	YC	Event to ARC not delivered	Uncategorised
1351	YD	LAN primary channel - fault	Uncategorised
1352	YD	GSM backup channel - fault	Uncategorised
1354	YS	Event to ARC was not delivered in preset time	Faults and service events
1384	XT	Low batt	Faults and service events
1389	YU	Test failed	Faults and service events
1401	OP	Disarmed	Setting / Unsetting
1402	OG	Disarmed partialy	Setting / Unsetting
1406	BC	Alarm canceled by user	Burglary
1407	OQ	Remotely disarmed	Setting / Unsetting
1412	LF	Remote access	Uncategorised
1416	LS	Configuration saved	Uncategorised
1454	NA	Section without movement	Faults and service events
1455	CI	Unsuccesfull arming	Uncategorised
1461	JA	Over code	Tamper
1521	BL	Siren mute	Uncategorised
1570	EB	Bypass periphery (turned off)	Uncategorised
1572	TB	Tamper bypass	Faults and service events
1573	BB	Activation bypass	Faults and service events
1574	UB	Bypass section (turned off), maitenance	Faults and service events
1578	UO	Fault bypass	Faults and service events
1601	RX	Manual test	Faults and service events
1602	RP	Periodic test	Uncategorised
1625	JT	Reset of time	Uncategorised
1661	RC	PG1 ON	PG controls
1662	RC	PG2 ON	PG controls
1663	RC	PG3 ON	PG controls
1664	RC	PG4 ON	PG controls
1665	RC	PG5 ON	PG controls
1666	RC	PG6 ON	PG controls
1667	RC	PG7 ON	PG controls
1668	RC	PG8 ON	PG controls
1669	RC	PG9 ON	PG controls
1670	RC	PG10 ON	PG controls
1671	RC	PG11 ON	PG controls
1672	RC	PG12 ON	PG controls
1673	RC	PG13 ON	PG controls
1674	RC	PG14 ON	PG controls
1675	RC	PG15 ON	PG controls
1676	RC	PG16 ON	PG controls
1677	RC	PG17 ON	PG controls
1678	RC	PG18 ON	PG controls
1679	RC	PG19 ON	PG controls
1680	RC	PG20 ON	PG controls
1681	RC	PG21 ON	PG controls
1682	RC	PG22 ON	PG controls
1683	RC	PG23 ON	PG controls
1684	RC	PG24 ON	PG controls
1685	RC	PG25 ON	PG controls
1686	RC	PG26 ON	PG controls
1687	RC	PG27 ON	PG controls

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

1688	RC	PG28 ON	PG controls
1689	RC	PG29 ON	PG controls
1690	RC	PG30 ON	PG controls
1691	RC	PG31 ON	PG controls
1692	RC	PG32 ON	PG controls
		Deactivation events	
3101	QR	Health problem	Burglary
3110	FR	Fire alarm	Fire
3118	FH	Unconfirmed fire alarm	Fire
3120	PR	Panic	Panic
3130	BR	Instant alarm	Burglary
3130	BR	Keybox	Faults and service events
3133	BR	24H alarm	Burglary
3134	BR	Delayed alarm	Burglary
3138	BH	Unconfirmed alarm	Burglary
3144	TR	Tamper	Tamper
3151	GR	Gas Leak	Fire
3154	WR	Flood alarm	Burglary
3158	KH	Overheating	Uncategorised
3159	ZH	Freezing	Uncategorised
3170	UR	Special Reaction A	Faults and service events
3171	UR	Special Reaction B	Faults and service events
3172	UR	Special Reaction C	Faults and service events
3173	UR	Special Reaction D	Faults and service events
3174	UR	Not used	Uncategorised
3300	ER	Fault	Faults and service events
3301	AR	AC recovery	Faults and service events
3302	YR	Control panel battery OK	Faults and service events
3306	LX	Service exit	Faults and service events
3313	YZ	Unblocked after alarm	Faults and service events
3344	XH	RF interference	Faults and service events
3350	YK	Comunication to ARC restored	Uncategorised
3351	YE	LAN primary channel - OK	Uncategorised
3352	YE	GSM backup channel - OK	Uncategorised
3354	YL	Event to ARC was not delivered in preset time	Faults and service events
3384	XR	Battery of periphery OK	Faults and service events
3389	YZ	Test OK	Faults and service events
3401	CL	Armed	Setting / Unsetting
3402	CG	Partialy armed	Setting / Unsetting
3407	CQ	Remotely armed	Setting / Unsetting
3412	LE	Remote access closed	Uncategorised
3570	EU	Remotely partialy armed	Setting / Unsetting
3572	TU	Tamper bypass end	Faults and service events
3573	BU	Activation bypass end	Faults and service events
3574	UU	End of section bypass	Faults and service events
3578	UP	Fault bypass	Faults and service events
3661	RO	PG1 OFF	PG controls
3662	RO	PG2 OFF	PG controls
3663	RO	PG3 OFF	PG controls
3664	RO	PG4 OFF	PG controls
3665	RO	PG5 OFF	PG controls
3666	RO	PG6 OFF	PG controls
3667	RO	PG7 OFF	PG controls
3668	RO	PG8 OFF	PG controls
3669	RO	PG9 OFF	PG controls
3670	RO	PG10 OFF	PG controls

3671	RO	PG11 OFF	PG controls
3672	RO	PG12 OFF	PG controls
3673	RO	PG13 OFF	PG controls
3674	RO	PG14 OFF	PG controls
3675	RO	PG15 OFF	PG controls
3676	RO	PG16 OFF	PG controls
3677	RO	PG17 OFF	PG controls
3678	RO	PG18 OFF	PG controls
3679	RO	PG19 OFF	PG controls
3680	RO	PG20 OFF	PG controls
3681	RO	PG21 OFF	PG controls
3682	RO	PG22 OFF	PG controls
3683	RO	PG23 OFF	PG controls
3684	RO	PG24 OFF	PG controls
3685	RO	PG25 OFF	PG controls
3686	RO	PG26 OFF	PG controls
3687	RO	PG27 OFF	PG controls
3688	RO	PG28 OFF	PG controls
3689	RO	PG29 OFF	PG controls
3690	RO	PG30 OFF	PG controls
3691	RO	PG31 OFF	PG controls
3692	RO	PG32 OFF	PG controls

	Sources for JA 100
001 – 249	Peripheries (devices)
251 – 850	User codes
250	Service code
901	Control panel
921	ARC1
922	ARC2
923	ARC3
924	ARC4
925	ARC5
911	GSM communicator
912	LAN communicator
914	GSM communicator external

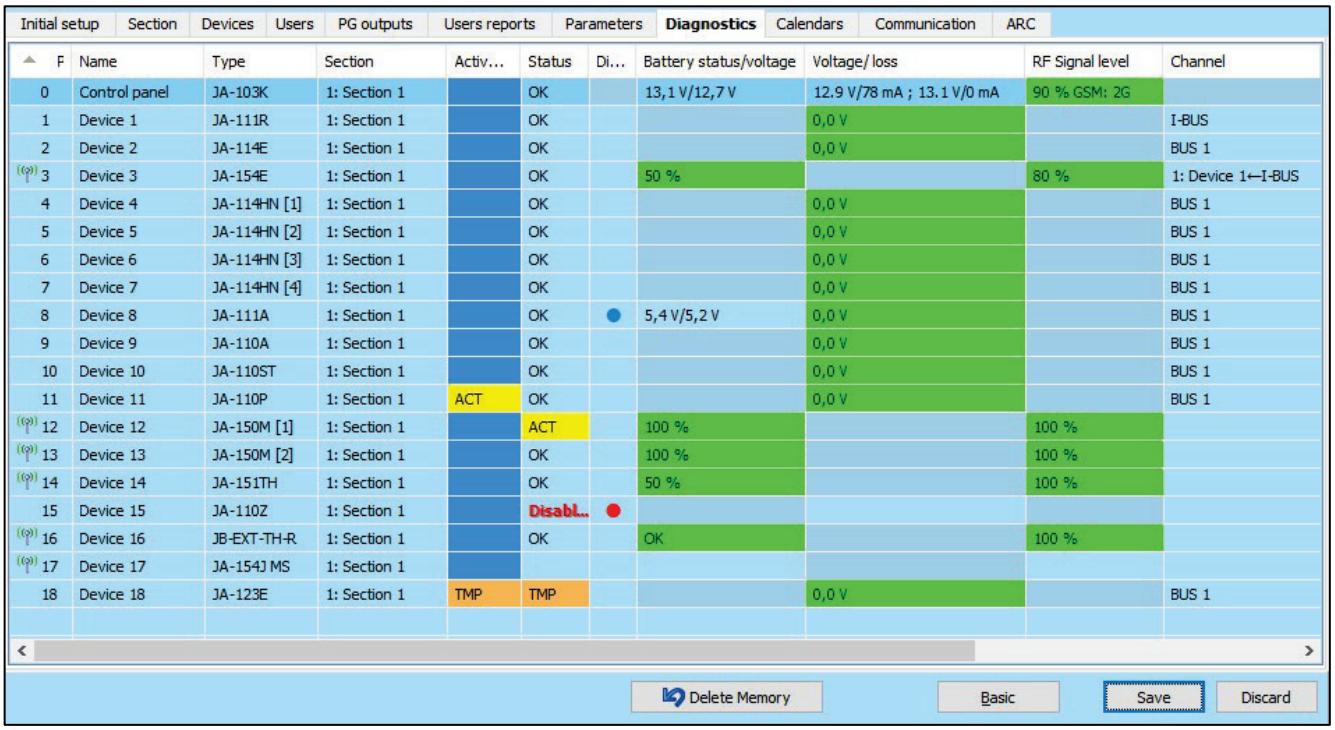
	PG	
	Range	**CID composition**
1. group	1 – 32 PG	Section 1 + 1661 – 1692 / 3661 -3692
2. group	33 – 64 PG	Section 2 + 1661 – 1692 / 3661 -3692
3. group	65 – 96 PG	Section 3 + 1661 – 1692 / 3661 -3692
4. group	97 – 128 PG	Section 4 + 1661 – 1692 / 3661 -3692
Example: Object ID 1234, 18 constant**, PG ON** no. **33**, 02 is a section, 901 is a event source control panel = **1234 18 1 661 02 901**		

10.12.2 Setting the transmission of photos to external storage

If in the region/country the MyJABLOTRON service is activated and the equipment user is going to use it, the required settings will be done completely automatically on registration of the control panel to the MyJABLOTRON web service.

10.13 Diagnostics tab

It is used to check and verify the status of devices and their properties.



P	Name	Type	Section	Activ...	Status	Di...	Battery status/voltage	Voltage/ loss	RF Signal level	Channel
0	Control panel	JA-103K	1: Section 1		OK		13,1 V/12,7 V	12.9 V/78 mA ; 13.1 V/0 mA	90 % GSM: 2G	
1	Device 1	JA-111R	1: Section 1		OK			0,0 V		I-BUS
2	Device 2	JA-114E	1: Section 1		OK			0,0 V		BUS 1
3	Device 3	JA-154E	1: Section 1		OK		50 %		80 %	1: Device 1←I-BUS
4	Device 4	JA-114HN [1]	1: Section 1		OK			0,0 V		BUS 1
5	Device 5	JA-114HN [2]	1: Section 1		OK			0,0 V		BUS 1
6	Device 6	JA-114HN [3]	1: Section 1		OK			0,0 V		BUS 1
7	Device 7	JA-114HN [4]	1: Section 1		OK			0,0 V		BUS 1
8	Device 8	JA-111A	1: Section 1		OK		5,4 V/5,2 V	0,0 V		BUS 1
9	Device 9	JA-110A	1: Section 1		OK			0,0 V		BUS 1
10	Device 10	JA-110ST	1: Section 1		OK			0,0 V		BUS 1
11	Device 11	JA-110P	1: Section 1	ACT	OK			0,0 V		BUS 1
12	Device 12	JA-150M [1]	1: Section 1		ACT		100 %		100 %	
13	Device 13	JA-150M [2]	1: Section 1		OK		100 %		100 %	
14	Device 14	JA-151TH	1: Section 1		OK		50 %		100 %	
15	Device 15	JA-110Z	1: Section 1		Disabl...					
16	Device 16	JB-EXT-TH-R	1: Section 1		OK		OK		100 %	
17	Device 17	JA-154J MS	1: Section 1							
18	Device 18	JA-123E	1: Section 1	TMP	TMP			0,0 V		BUS 1

* Items marked this way are displayed if **Advanced Settings** are on.

Activation memory – registers activations of the device that have occurred since the last deletion of this column. The memory of all devices activations can be deleted with the Delete memory button (bottom bar). You can delete the memory of a selected device using the right mouse button. Activation of a tamper sensor (TMP) has the highest priority when events are recorded in the memory.

Status – indicates the current status of the device. OK = everything all right, TMP = tampering, ACT = alarm input activated, ERR = error, ?? = no communication with the device, Mains supply = supply failure (or completely discharged battery), Charging = charging the backup battery in the device or control panel. Battery = discharged or disconnected battery in the control panel, BOOT = upgrading of the device is going on or upgrade failure (repeat upgrade), INIT = reading of the device configuration, Disabled = device is disabled. By moving the mouse cursor on the STATUS of the respective device you will display details.

Battery* – if the device contains a battery, its status is displayed. For the control panel (position 0) the voltage of the backup battery is displayed. If the voltage data of a wireless device are missing, the device has not communicated yet – activating its transmission (e.g. by means of the tamper sensor or in F-Link click on the Load button) or wait until automatic transmission occurs. If wireless keypads are powered by an external power supply source “Powered from external source” is indicated. For wireless devices (except devices of the JA-18x series) battery status is visible. Colour coding of the battery status: 10% red, 20% yellow, 30% and higher green.

Voltage* – on the position of the control panel (0) voltage of the control panel terminals and current that is drawn by the BUS devices from the control panel are displayed (individually for each BUS output). For BUS device the line voltage loss as compared to the control panel is displayed. The loss must not be higher than 2 V; otherwise the problem must be solved.

RF signal level* – on the position of the control panel it indicates quality of the GSM network signal. For a reliable communication the value should be at least 50 %. For wireless devices it indicates the quality of the RF signal, the value should be at least 50 %. If the indication is missing, the device has not communicated yet – activated its transmission (e.g. by means of the tamper sensor) or wait until automatic transmission occurs. About the interference between radio modules and the GSM module see also chapter 6.1 Installation of a JA-11xR radio module).
Colour coding of the GSM signal: 0-30 % red, 40-50 % yellow and over 50 % green.
Colour coding of the RF signal: 10 % red, 20 % yellow, 30 % and higher green.

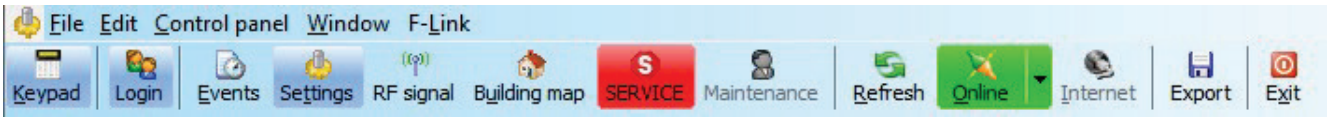
For bidirectional devices (supporting this function), when you position the mouse cursor over the signal level of the device, it will display both communication channels between the control panel and the device.

Channel* – informs about the BUS used by the device to communicate. Three directions are distinguished: BUS 1, BUS 2, 3 (only JA-107K) and the I-BUS connector designed for the JA-11xR radio module (JA-103K). For bidirectional wireless devices (sirens, keypads etc.) the “Channel” column displays the radio module through which the device currently communicates.

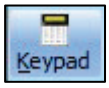
11 Other F-Link options

The F-Link version is always indicated in the top bar after the name.

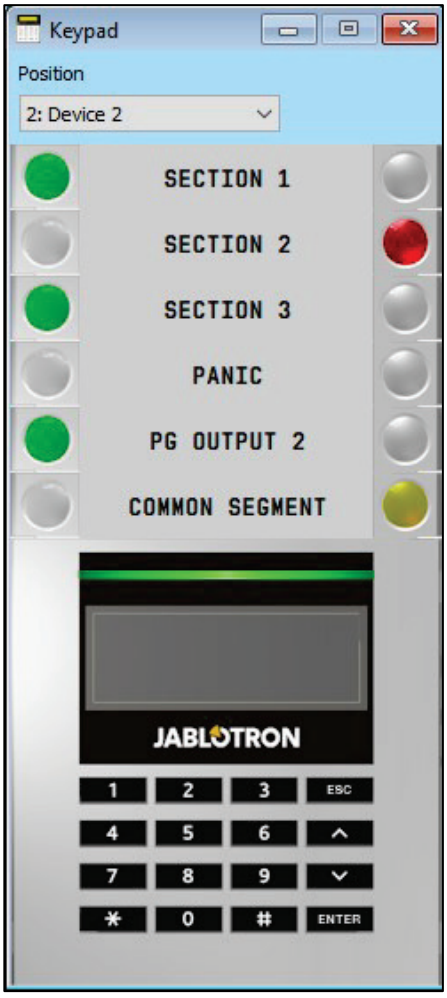
The toolbar provides immediate access to virtual keyboards, system events, settings, RF signal of radio modules, site map, mode changes, local and remote access to the control panel.



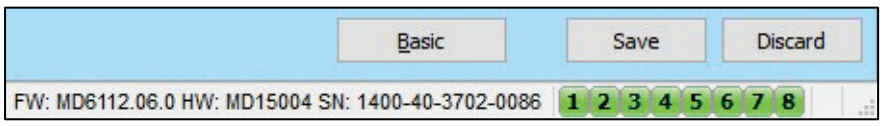
11.1 Keypad (virtual)



The virtual keypad in the F-Link (now in JA-100-Link as well) for all types of control modules enables control (of sections, PG outputs) with the use of segments (not numbered keys) of the person logged in to F-Link. This means that codes cannot be entered.

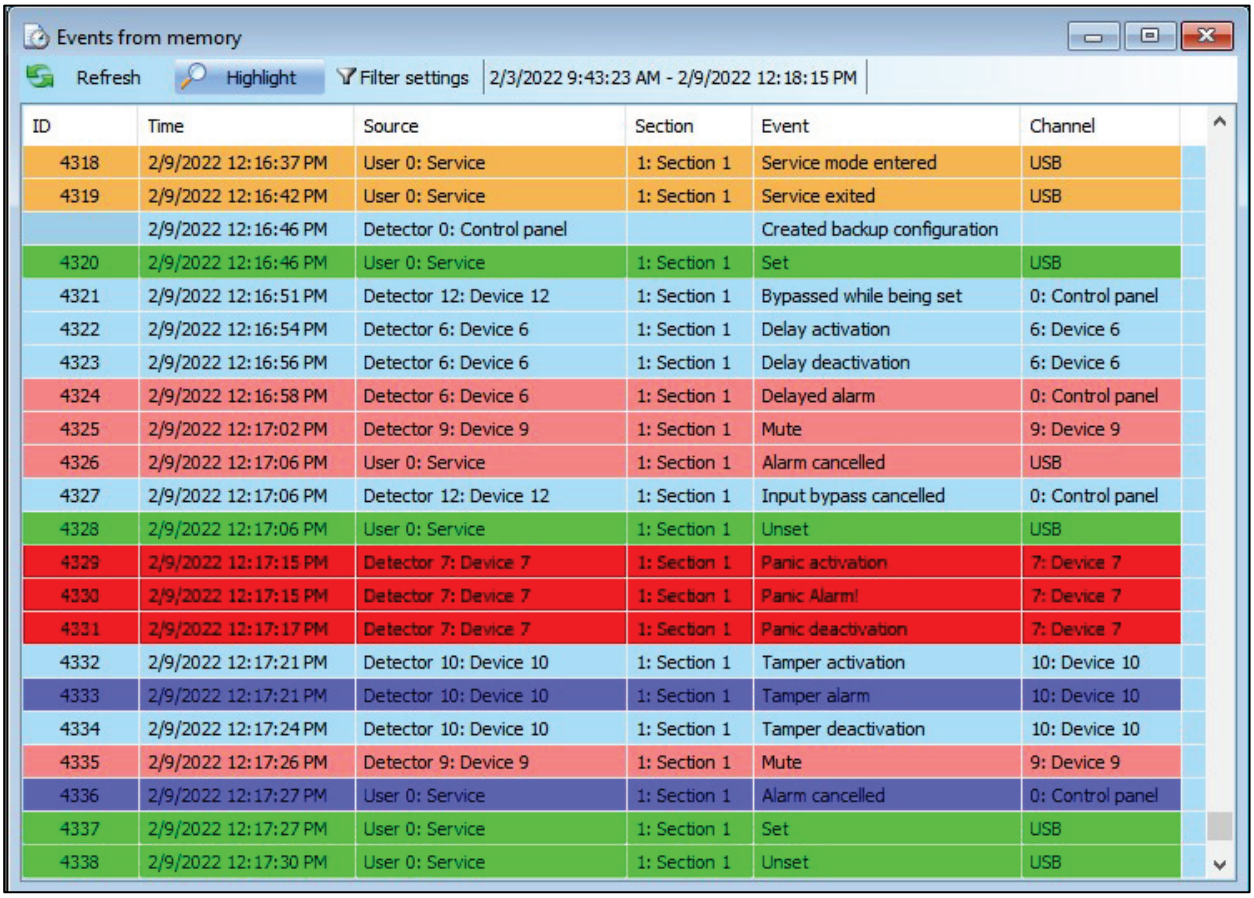


The system can be controlled locally and also remotely (set and unset) by clicking on the icons representing system status in the lower toolbar and in the Section tab by buttons there as well.



11.2 Event history

Event history is accessible in F-Link by pressing of the Events button and selecting “Event history”. In the memory of the control panel (microSD card) up to several millions of records may be stored with the sequential number, exact date and time and source of the event.



ID	Time	Source	Section	Event	Channel
4318	2/9/2022 12:16:37 PM	User 0: Service	1: Section 1	Service mode entered	USB
4319	2/9/2022 12:16:42 PM	User 0: Service	1: Section 1	Service exited	USB
	2/9/2022 12:16:46 PM	Detector 0: Control panel		Created backup configuration	
4320	2/9/2022 12:16:46 PM	User 0: Service	1: Section 1	Set	USB
4321	2/9/2022 12:16:51 PM	Detector 12: Device 12	1: Section 1	Bypassed while being set	0: Control panel
4322	2/9/2022 12:16:54 PM	Detector 6: Device 6	1: Section 1	Delay activation	6: Device 6
4323	2/9/2022 12:16:56 PM	Detector 6: Device 6	1: Section 1	Delay deactivation	6: Device 6
4324	2/9/2022 12:16:58 PM	Detector 6: Device 6	1: Section 1	Delayed alarm	0: Control panel
4325	2/9/2022 12:17:02 PM	Detector 9: Device 9	1: Section 1	Mute	9: Device 9
4326	2/9/2022 12:17:06 PM	User 0: Service	1: Section 1	Alarm cancelled	USB
4327	2/9/2022 12:17:06 PM	Detector 12: Device 12	1: Section 1	Input bypass cancelled	0: Control panel
4328	2/9/2022 12:17:06 PM	User 0: Service	1: Section 1	Unset	USB
4329	2/9/2022 12:17:15 PM	Detector 7: Device 7	1: Section 1	Panic activation	7: Device 7
4330	2/9/2022 12:17:15 PM	Detector 7: Device 7	1: Section 1	Panic Alarm!	7: Device 7
4331	2/9/2022 12:17:17 PM	Detector 7: Device 7	1: Section 1	Panic deactivation	7: Device 7
4332	2/9/2022 12:17:21 PM	Detector 10: Device 10	1: Section 1	Tamper activation	10: Device 10
4333	2/9/2022 12:17:21 PM	Detector 10: Device 10	1: Section 1	Tamper alarm	10: Device 10
4334	2/9/2022 12:17:24 PM	Detector 10: Device 10	1: Section 1	Tamper deactivation	10: Device 10
4335	2/9/2022 12:17:26 PM	Detector 9: Device 9	1: Section 1	Mute	9: Device 9
4336	2/9/2022 12:17:27 PM	User 0: Service	1: Section 1	Alarm cancelled	0: Control panel
4337	2/9/2022 12:17:27 PM	User 0: Service	1: Section 1	Set	USB
4338	2/9/2022 12:17:30 PM	User 0: Service	1: Section 1	Unset	USB

Events from the control panel memory (available also after pressing F8) – approx. 100 kB of events (from the microSD card) are loaded. If the loading range is insufficient, you can repeatedly select Load / Next 100(500) kB, range from – to, or All. Warning: If you select Load/All, in a control panel with a longer time of operation the loading may take a few minutes. The history does not record events that occur during service setting (just the opening and closing of the Service mode is registered). Loaded events can be saved in a file in the File menu using the Export item (Shift + Ctrl + S), namely in several formats (FDE, PDF, TXT, CSV, XML, HTM or HTML). The FDE suffix makes it possible for the F-Link to download the events again.

***Note**: The option to load a range from – to (date) is available only when connected remotely.*

Events online (available also after pressing F7) – in a temporary table all events are recorded that are saved in the event history and that occur after activation of this option, incl. events during service setting.

Signals online (available also after pressing of F6) – in a temporary table all signals are recorded that are registered by the BUS (e.g. also activation and deactivation of sensors).

Events from file – events from the event history saved in the FDE database file format can be opened (see Events from the control panel memory).

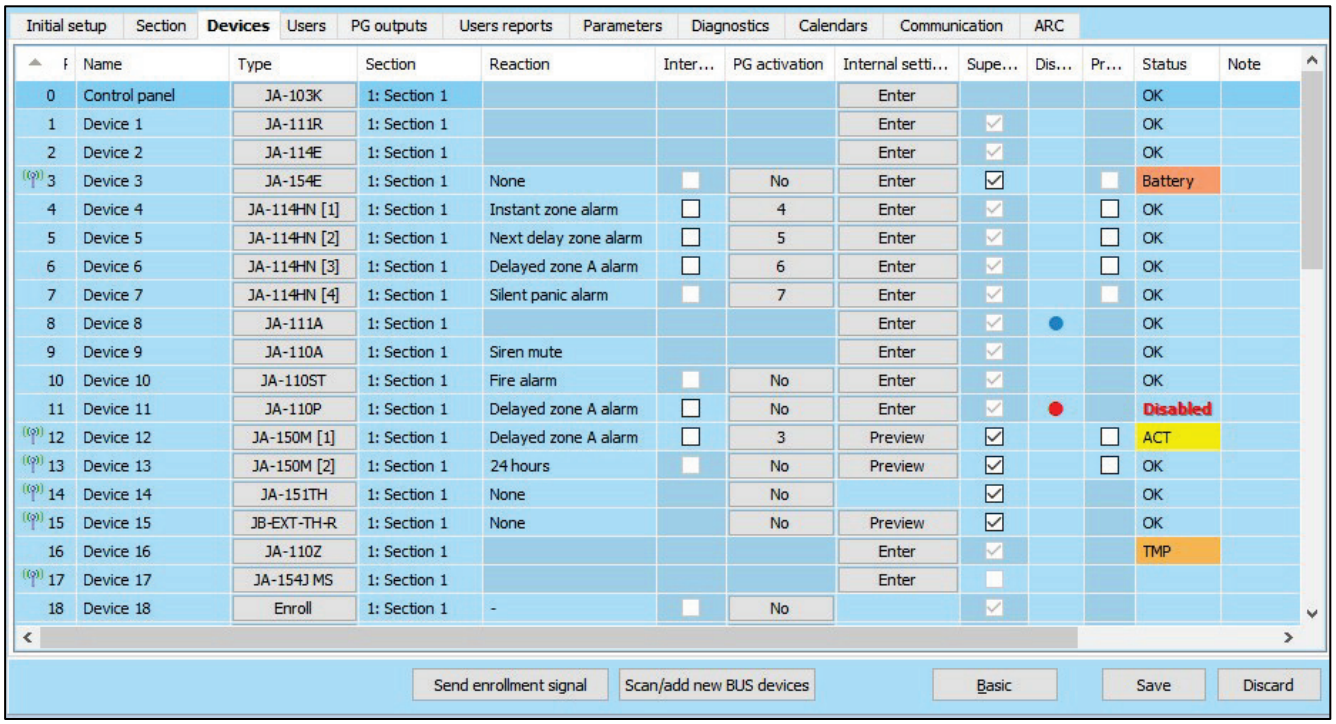
Load – makes it possible to load more events deeper from the history by 100 kB, 500 kB (100 kB corresponds to approx. 1200 events) or all.

Highlight – colour highlighting makes it possible to distinguish event types (alarm with red, control with green, error with orange, tampering with blue, neutral with light blue, automation or transmissions with grey etc.).

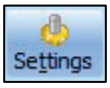
Filter Settings – the filter allows you to obtain only desired information by time, by event type, sections, users, devices or PG outputs in a very detailed way. Filters can be combined to increase searching efficiency in deep history.

11.3 System settings

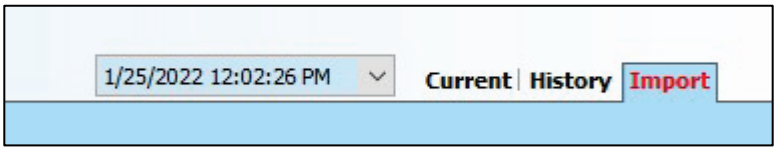
Window used to set behaviour of the system, all devices, sections, users, PG outputs, communicators and transmissions to ARC is available by pressing the Settings button on the basic top bar.



	Name	Type	Section	Reaction	Inter...	PG activation	Internal setti...	Supe...	Dis...	Pr...	Status	Note
0	Control panel	JA-103K	1: Section 1				Enter				OK	
1	Device 1	JA-111R	1: Section 1				Enter	☑			OK	
2	Device 2	JA-114E	1: Section 1				Enter	☑			OK	
3	Device 3	JA-154E	1: Section 1	None	☐	No	Enter	☑		☐	Battery	
4	Device 4	JA-114HN [1]	1: Section 1	Instant zone alarm	☐	4	Enter	☑		☐	OK	
5	Device 5	JA-114HN [2]	1: Section 1	Next delay zone alarm	☐	5	Enter	☑		☐	OK	
6	Device 6	JA-114HN [3]	1: Section 1	Delayed zone A alarm	☐	6	Enter	☑		☐	OK	
7	Device 7	JA-114HN [4]	1: Section 1	Silent panic alarm	☐	7	Enter	☑		☐	OK	
8	Device 8	JA-111A	1: Section 1				Enter	☑	●		OK	
9	Device 9	JA-110A	1: Section 1	Siren mute			Enter	☑			OK	
10	Device 10	JA-110ST	1: Section 1	Fire alarm	☐	No	Enter	☑			OK	
11	Device 11	JA-110P	1: Section 1	Delayed zone A alarm	☐	No	Enter	☑	●		Disabled	
12	Device 12	JA-150M [1]	1: Section 1	Delayed zone A alarm	☐	3	Preview	☑		☐	ACT	
13	Device 13	JA-150M [2]	1: Section 1	24 hours	☐	No	Preview	☑		☐	OK	
14	Device 14	JA-151TH	1: Section 1	None		No		☑			OK	
15	Device 15	JB-EXT-TH-R	1: Section 1	None		No	Preview	☑			OK	
16	Device 16	JA-110Z	1: Section 1				Enter	☑			TMP	
17	Device 17	JA-154J MS	1: Section 1				Enter	☐				
18	Device 18	Enroll	1: Section 1	-	☐	No		☑				

1. The System Settings Window is opened and closed by the **Settings** 

button in the top toolbar.
2. In the window you can switch between the following **tabs: Initial setting, Sections, Devices, Users, Reports**, …
3. The window will display the **current setting of the control panel** loaded on opening of the F-Link software. The **Load** button in the top toolbar can be used to load the current content of the control panel at any time.
4. If you want to view **older settings of the control panel, use the History tab** in the top right corner. The history cannot be changed, but it can be saved in the control panel (if you need to return to earlier settings). Max. 10 previous settings are recorded in the history (arranged by the date and time) and also all setting changes.
5. You can **import settings** from another installation to the system, e.g. after replacing an old control panel with a new one or using a default template. If the control panel is replaced with a new one, after the connection a completely new database will be created in the computer. To import settings from another database, in the top bar of the main menu select **File / Import** and select the file you want to import settings from. After this selection the **Import** button in the **System Settings** tab will be.



6. For simpler applications you can just set the **basic functions** of the system. If you need to set **all functions** of the system, use the “Advanced” button in the bottom right corner. By repeatedly pressing this button you can hide the advanced settings options (their settings remain valid even though they are hidden. The **Advanced/Basic** button is available in the other windows as well.

7. **If you make a change to a setting, it will be indicated with blue text** (the name of the tab will become blue too). The blue indication will disappear as soon as you save the changes.
8. You can **Save the Settings** using the **Save** button (at the bottom on the right). If you are saving settings in the control panel for the first time, the F-Link will ask you to **enter the file name**. In the computer, a file with the *FDB suffix will be created where the history of settings is gradually saved (every time the settings are saved in the control panel). If you do not want to save the changes, select the **Cancel** button and in the confirmation question select **Ignore**. Parameters can be changed in more tabs and you can then Save all changes.
9. The **Scan/add new BUS devices** button (Lower toolbar on the Devices tab) will open a dialog for collective enrollment (without the possibility to select positions) of devices that are connected to the BUS and have not been connected to the system in another way. See chapter 8.4.1 Enrolling and erasing devices.

10. The **Send enrolling signal** button (Devices and PG outputs tab) will release sending of the enrolling code of the control panel to wireless devices, e.g. to wireless output modules.
11. **Setting of all parameters is only possible in the Service mode** (the system does not guard). The Service mode is activated and deactivated with the **Service** button in the top toolbar.
12. **Some parameters can be changed during operation.** Therefore, the Settings tab can be opened without entering the Service mode. However, available options can only be set.
13. **The F-Link contains bubble help** – after placing the mouse cursor over an item the text description will be displayed. You can disable the bubble help in the F-Link roll-down menu.

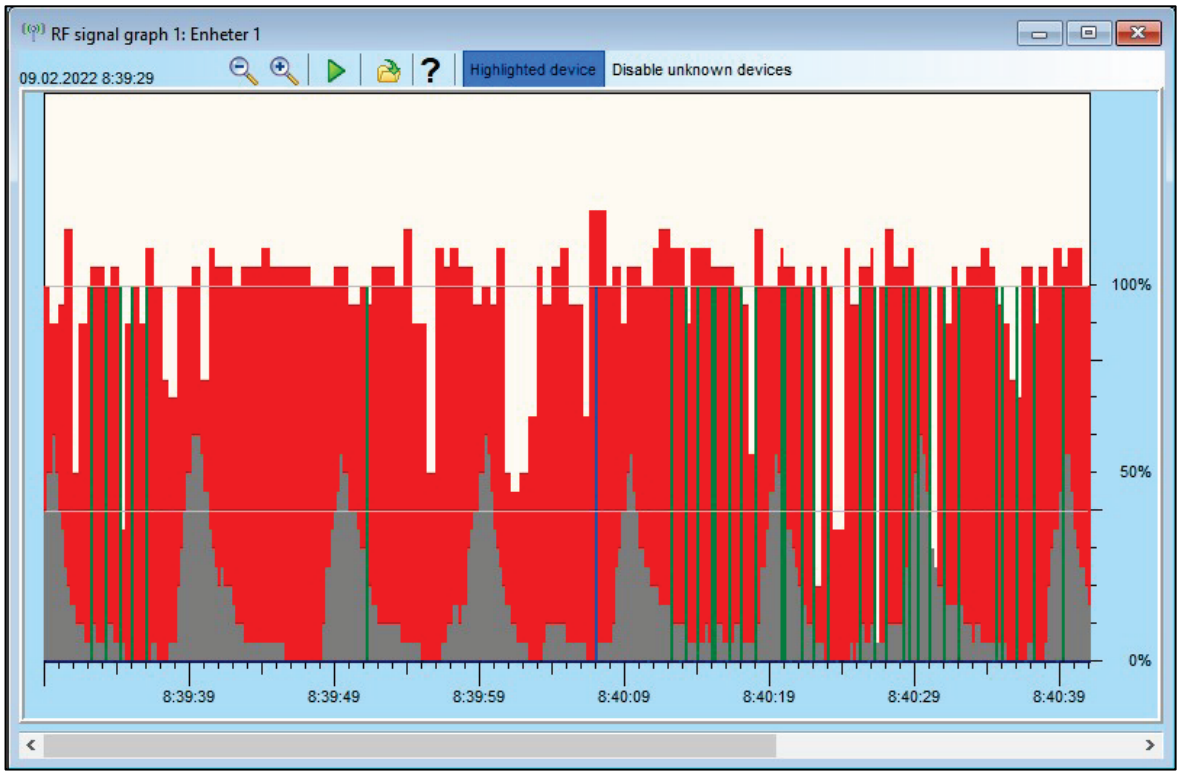
Possible problems during the use of the System Settings:

Problem	Possible cause
None or some of the displayed parameters cannot be changed	The system is not in the Service mode and you have selected a function that can only be changed in the Service code. On the start of the F-Link the Service Code was not entered and you do not have the authorization. This is a setting that cannot be changed (Service Technician's authorization, control panel position, the device does not support it etc.). The ARC setting has been blocked by the ARC technician. You are offline. You have enabled the parameter to fulfil the EN 50131 standard.
The requested parameter cannot be found	Only the basic options are displayed, use the Advanced button. You do not see the whole setting area on the screen – use a scroll button or enlarge the window. You are authorized by a code with a different access level.
The positions are arranged in a different way	By clicking on the title of a column you can select which column will be used as the criterion to arrange the positions; by clicking on the title repeatedly you can select ascending or descending order.
Some tabs are missing	If the PG Outputs tab is not available, check whether the number of PG outputs set in the Initial setting tab is not zero. The ARC tab is not available if you do not have sufficient authorization for it (it may be locked by the ARC technician). It may also be unavailable after registration of the system in the My-JABLOTRON application. You have an older version of the F-Link (JA-100-Link) software.
Internal settings cannot be modified in the Devices tab	Check whether the device is properly connected, enrolled and functional. The Service mode is not enabled. Some devices do not have internal settings. Older versions of F-Link may not have support for new types of devices. In the case of a wireless device check whether the radio module is enrolled and functional.
A device cannot be enrolled in the Devices tab	For wireless devices – you have not enrolled the JA-11xR radio module. In a BUS device the yellow signal LED must flash regularly. If it does not flash, the element is not properly connected or has not stabilized after activation of the power supply (it may take up to 180 s.). The Service mode is not on. Older versions of F-Link may not have support for new types of devices.
A PG output does not react to activation of a device	Make sure the system in not in the Service mode. In the Diagnostics tab check whether the device transmits information to the control panel. In the PG Outputs tab check whether the output is not blocked by a section status, device or calendar; check the Functions column for proper setting. In the JA-11xN, JA-15xN modules check the DIP switches for proper binary setting of the address and function of the module.

11.4 RF Signal

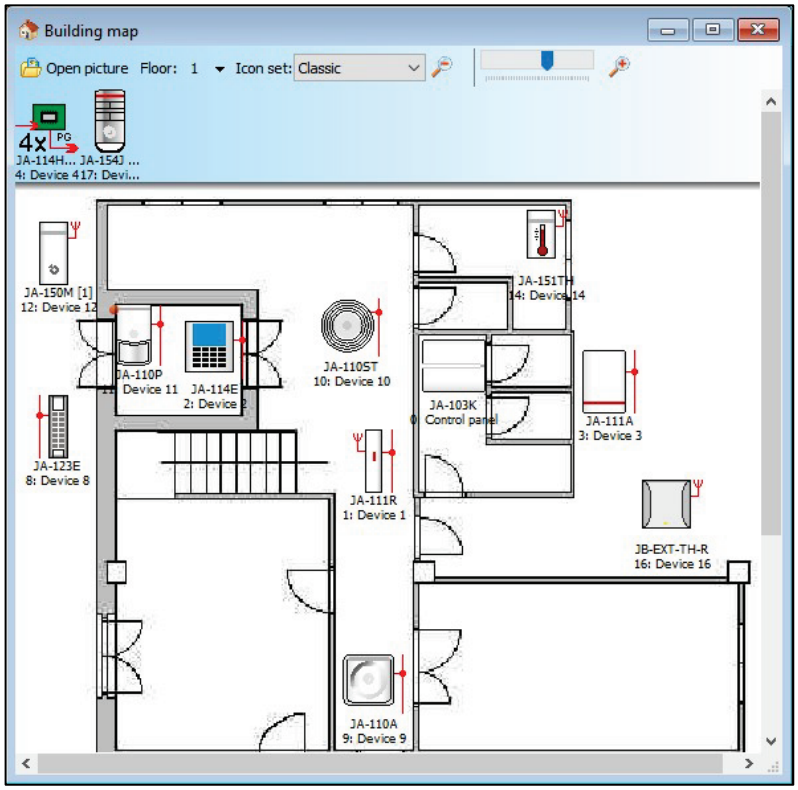
Window for graphic representation of radio band interference intensity with the possibility to select from the used radio modules. Presence of unknown signals in the band is indicated in red. Green colour identifies communication signals of the system (enrolled devices) and blue is used to display the selected device from the list of the **Highlighted device** item (see figure). Grey colour indicates a background (jamming). With the **Disable unknown devices** option, it is possible to filter out the unknown devices and to display only the devices enrolled in the system.

Monitored interference logging (when the RF Signal window is open) can be exported from the main menu to a file with the FDR suffix and the  button can be used to import it back for viewing.



11.5 Building map

You can insert a top view (jpg, gif, bmp, tif, png etc.) into the building map for each floor separately or you can use simple lines to draw your own plan. In each floor you can only insert icons of the enrolled devices from the icon panel by Drag & Drop. You can print the building map with the icons or you can save it as a BMP image using the Print or Export item in the main menu.



11.6 Service

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Switching the control panel mode between the Unset status (when changes of setting can be done in all tabs except the Settings tab) and the Service mode (changes can be done in the Devices tab, incl. enrolling, changes of internal settings and deletion of devices).

11.7 Maintenance

Switching the control panel mode between the Unset status and the Maintenance mode. In maintenance mode, the system cannot be controlled, it ignores all alarm including tamper alarms. Suitable e.g. for changing batteries in wireless detectors without intervention of a service technician.

11.8 Refresh

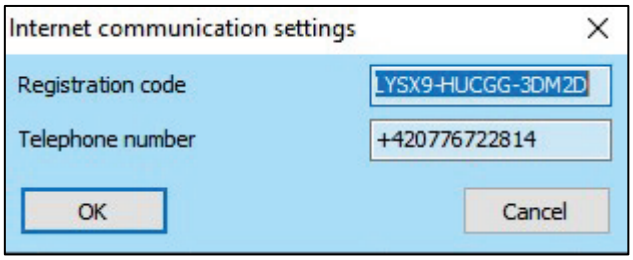
Updating the internal settings of devices after a hardware change, e.g. addition of segments to access modules or keypads.

11.9 Online

Connection or disconnection of F-Link from the control panel using a USB cable. After the connection the software will find the port the control panel uses for communication automatically.

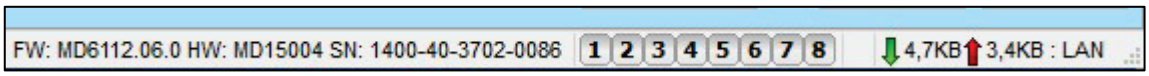
11.10 Internet

Remote connection or disconnection of F-Link from the control panel via the Internet. A precondition for establishing the connection is the properly entered registration code (it is automatically pre-entered from the database that was used to program the control panel), phone number of the SIM card in the control panel (also pre-entered from the Installation Information) and the computer connected to the Internet. Remote access can be disabled in the Communication tab / Communication Type = Without remote communication. If the Security SIM is in use, this option is disabled.



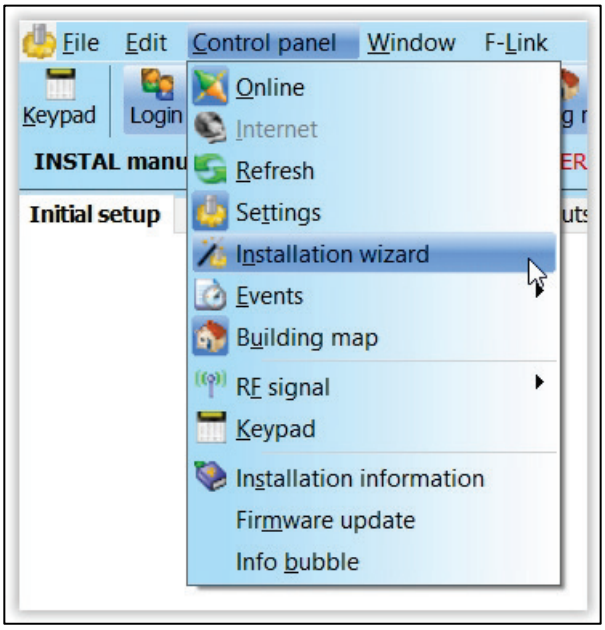
After clicking on the Internet button, a dialog window with pre-entered data is displayed. If you are connecting from a new “empty” database, the registration code and the phone number will have to be added. If the Security SIM and LAN connection is in use, the phone number doesn’t have to be entered. Establishing the connection only takes a few seconds, but the downloading of the configuration depends on the system size and it may usually take 1 to 2 minutes.

***Note**: Information about the way of establishing the GPRS / LAN connection and the sent and received amount of data is displayed in the bottom right corner.*



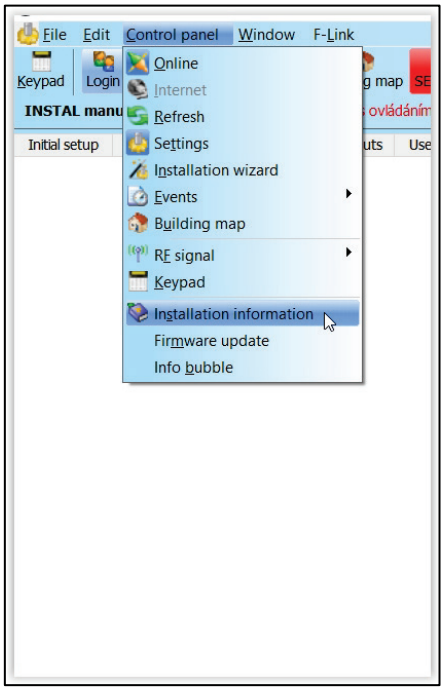
11.11 Installation wizard

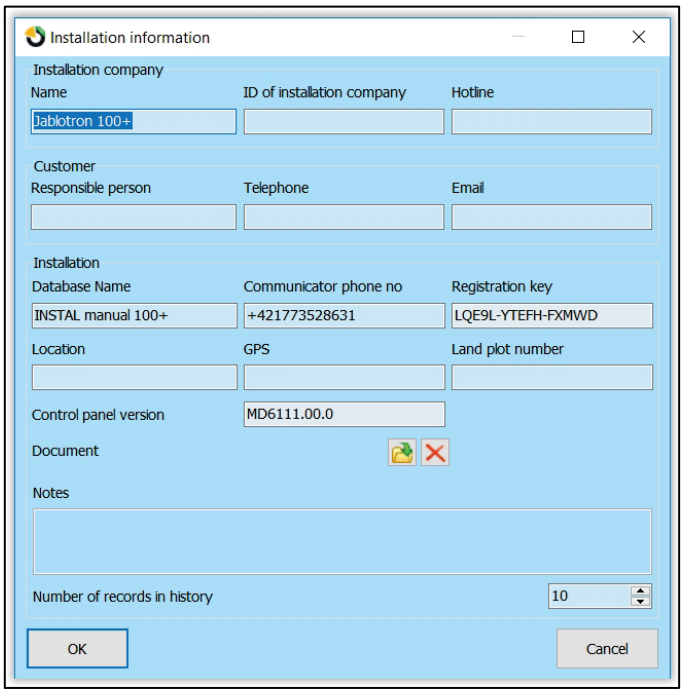
An assistant for gradual passing through the Settings tabs that facilitates the programming procedure of the system. The Wizard is enabled in the Control Panel main menu and disabled with the Close button in the bottom right corner of the Wizard window.



11.12 Installation information

The window contains items for the installation company to save important contact information about the system owner, the entire system and possibly an external document related to the building (offer, acceptance record, invoice etc.). In the ext. field the installation technician may fill in notes and information obtained during the assembly that may be useful e.g. in case of system extension.

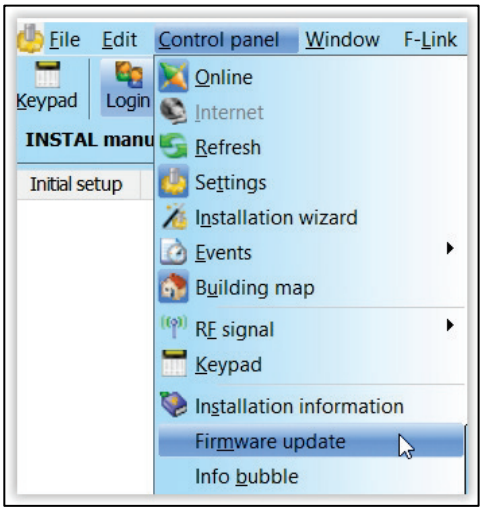




11.13 Firmware update

A firmware update or change makes it possible to change the behaviour of updatable devices (control panel, radio modules, keypads, detectors etc.) with a package that the manufacturer officially releases in the JABLOTRON sever. F-Link downloads from the JABLOTRON server automatically (after a query), if in the F-Link menu the Automatic Updates item is activated (in the default setting it is activated). If the item is not enabled F-Link will make it possible to find the way to the FWP files in the computer manually before the upgrade.

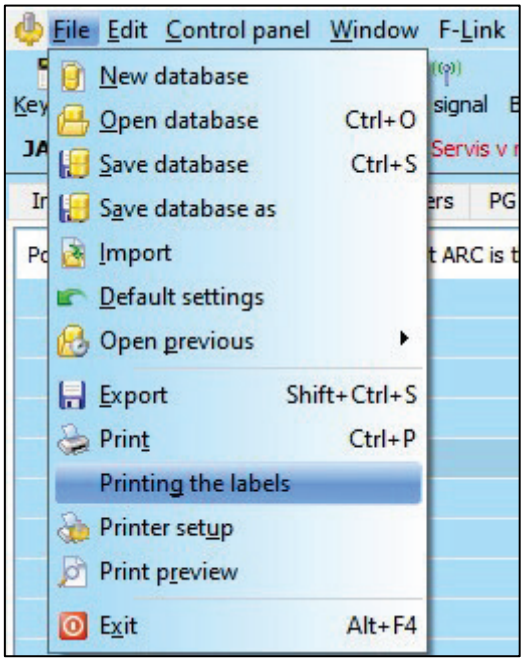
JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



11.14 Printing the labels

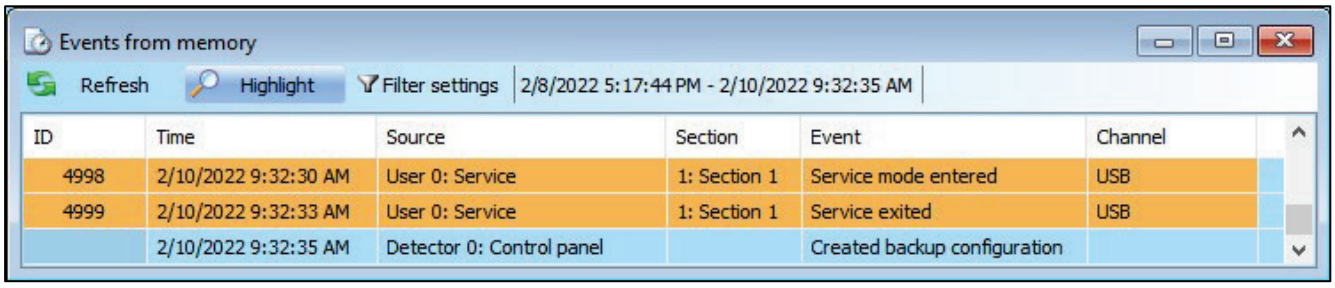
To print labels with names of the actually used segment of access modules it is convenient to use the Print Labels function in the internal settings window of each used access modules, see chapter 10.5.1.1 Segments tab.

You can enter your own text to be printed. Edited texts are not saved by the software after the print, so they are not available for possible repeated print. The text on the labels can be aligned to the left or centred.



11.15 History of settings

The control panel saves the settings of all devices with changes of their programming to the SD card. And it also records the event “Configuration backup created” in the history with information about the file name. It includes the configuration before change execution to ensure a way to get the previous configuration back, to browse through it and to check when that change was done. To browse through saved configuration changes, open Events from the control panel memory and search for the configuration change events according to the date and time and for comparing with the current system programming, load it, and look in the “History” tab available in the right upper corner of the “System settings” window. Changes in configuration are highlighted by blue italics letters. From the saved backup file, it is possible to accept the changes and by clicking on the “Save” button save it to the control panel or after browsing through the changes get back the current settings by clicking on the “Current” tab. All configuration modifications are saved to the folder called BACKUP, in the file CFGxxxxx.bak with a number according to the order of performed changes.



The F-Link software saves (3 to 10 in the Installation information window) the history of settings backwards in its own database. This history of settings is used by the software for upgrades of the control panel firmware as a change always causes the loss of the previous settings and this history can be used to restore it. The same option can be used in the case of a Reset of the control panel to the default settings, replacement of the SD card, language changes when texts are deleted, which can be restored this way or just in the case of an inadvertent change of a setting.

12 Reset of the control panel

You can only restore the default settings of the control panel in the following way if in the F-Link software in the Parameters tab the Reset allowed item is checked. If Reset is not allowed and you do not know the service code, you cannot reset the control panel and the control panel board must be sent to the distributor.

Procedure:

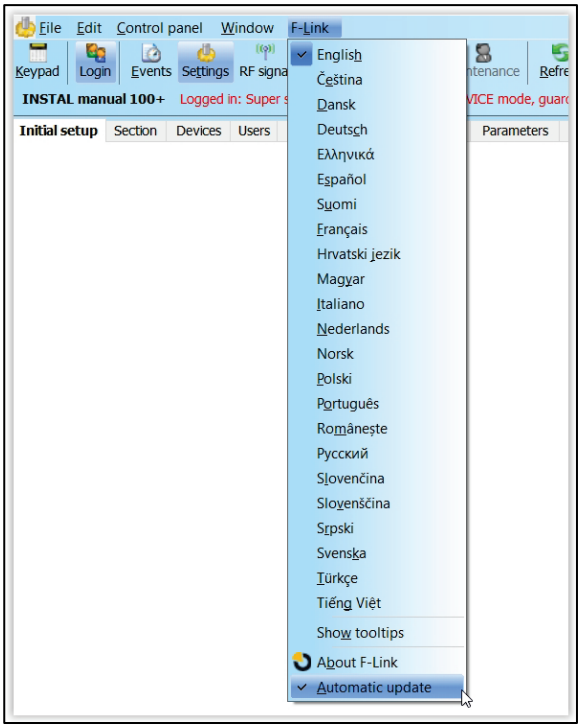
1. Switch the control panel to the Service mode (not obligatory).
2. Open the control panel cover: Reset requires that the tamper contact must be active. If the condition of point 1 was not fulfilled, an alarm will be triggered.
3. Disconnect the USB cable from the control panel.
4. Turn off the power supply (most easily by releasing the power supply fuse) and disconnect the battery.
5. Connect the pins on the control panel board marked RESET (using the jumper included in the package).
6. First connect the battery and then the power supply of the control panel and wait. The green, yellow and red LED indicators at the jumper will light up (if just the red LED indicator remains on, the setting Parameters / Reset Allowed is not enabled).
7. Wait for approx. 15 s and then disconnect the jumper.
8. After a few seconds all LED indicators will flash as a confirmation of completion of the control panel reset. Then, voltage restart of the control panel and BUS devices will occur, which will be confirmed by a flash of all segments on the keypads.
9. This way, the control panel has been reset to the default settings, incl. language selection. However, reset of the control panel does not cause deletion of the history of events saved on the memory SD card. If Reset was not executed correctly, the control panel will keep the original settings without changes.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

13 Firmware updates

The control panels and some other devices of the JABLOTRON system enable a firmware change. Firmware is usually changed to extend the useful parameters of the equipment.

13.1 General firmware update rules (FW)



1. A change can only be performed with a computer with the installed **F-Link** software either with the use of local access via a USB cable or remotely where the possibility to change firmware is limited to BUS devices.
2. Firmware (FW) can be changed by a user with the Service authorization.
3. Check whether you are using the up-to-date version of F-Link. The latest version is available at the website www.myjablotron.com, **MyCOMPANY / MySTORAGE / Software**, which is only accessible for authorized technicians after login. Or with already installed F-Link software and Internet access F-Link offers software updates after the start automatically and at the same time it downloads the current FW package by itself.
4. Connect the computer to the control panel with a USB cable, the cable is included in the control panel delivery.
5. Start the **F-Link** software with the control panel connected.
6. Switch the control panel over to the **Service** mode.
7. Start the **Control Panel / Firmware Update**
   If **Automatic Update** is allowed in the **F-Link** menu (enabled in the default setting), the list of updatable devices is displayed. This file is part of F-Link in the **F-Link x.x.x / Firmware** directory and its up-to-date status is only guaranteed at the time of the F-Link download. Its up-to date status is automatically guaranteed at the time when F-Link is downloaded.

Location of the Automatic Update parameter:

13.2 FW updates for the control panel and devices connected to the BUS

1. In the Firmware Update selection window updatable BUS devices and the control panel are only displayed. F-Link automatically selects devices for which an update is required (they have older FW than in the FW pack).
2. F-Link warns you when wireless devices can be updated. See the chapter 13.3 FW update for wireless devices for information about the update procedure of wireless devices.
3. More detailed information about the existing and new version of individual devices is displayed in the bubble help after moving the mouse cursor over each of the offered devices.
4. In the selection boxes check the devices for which you want to change FW. If in the offered options there is the control panel with the offer of a newer FW version, we recommend you leave it checked. Some items may be obligatory and thus unavailable (greyed) for update cancellation.
5. If the control panel update option is enabled, the possibility to keep the modified user voice menu is displayed. If the possibility to keep the menu is disabled, the default setting of the voice menu will be restored.
6. Click on OK to start the update of FW of all the selected devices. All the changes will be executed within a few minutes (depending on the number of devices). Finally, the control panel will restart the system.
7. After a change of FW, a part of the registration code will change. Its change will not have any impact on the possibility of remote access (using F-Link) or possible communication of the control panel with the MyJABLOTRON service.
8. If during the control panel update F-Link finds damaged files in the SD card, it will format it and after completion of the update it will offer the possibility of re-importing the original settings.
9. Although the FW update does not change the system behaviour, perform a check in accordance with the description in chapter Check after a FW change 13.4 Check after a FW update.

13.3 FW updates for wireless devices.

1. The FW update of the wireless devices is done the same way as of the BUS devices. Should this way of the update fail, proceed by following the steps below:
2. Open the updatable wireless device (e.g. JA-152E, JA-153E, JA-154E, JA-160PC, AC-160DIN etc.) by pushing the latch.
3. If it contains batteries, remove them and disconnect possible external power supply.
4. Start F-Link, open the database and connect a USB cable to the computer (miniUSB or microUSB depending on the used device).
   ***Warning**: USB cables are not included in the delivery of individual devices. We recommend you use direct USB connection to the PC, possible connection with a USB HUB may reduce reliability.*
5. The update of FW of wireless devices must be carried out gradually, it cannot be done simultaneously with more USB cables.
6. In the wireless device to be updated open the mode for loading new FW. In the case of other devices follow the instructions of the respective manuals.
7. Then continue as during system upgrade with the **F-Link software: Control Panel → Firmware Update.**
8. In the table of devices selection, select the USB item (typically in the first position).
9. More detailed information about the existing and new version of individual devices are displayed in the bubble help after moving the mouse cursor over each of the offered devices.
10. By pressing the OK button, you will upgrade all the devices.
11. After completion of the update disconnect the USB cable, reinsert batteries or connect the power supply and make the module complete.
12. Perform a check in accordance with the description in the chapter 13.4 Check after a FW .
13. Go on to upgrade the next wireless device.

13.4 Check after a FW update

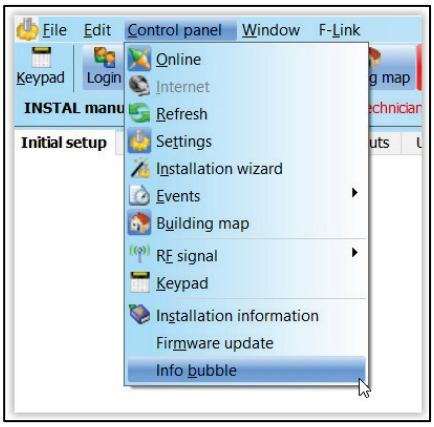
1. Check the settings of all the changed devices and control panel in **F-Link, Devices / Internal Settings** Depending on the range of changes implemented during the update the previous setting may be maintained or reset to the default production values. If reset to the default values has been done, you can use the Import button in the internal settings of individual devices to select from previous settings.
2. If new items were added within the update, they will have the default settings. Check them and adapt the settings as necessary for the installation.
3. Check the settings and test the activity of the updated devices.

13.5 Info bubble

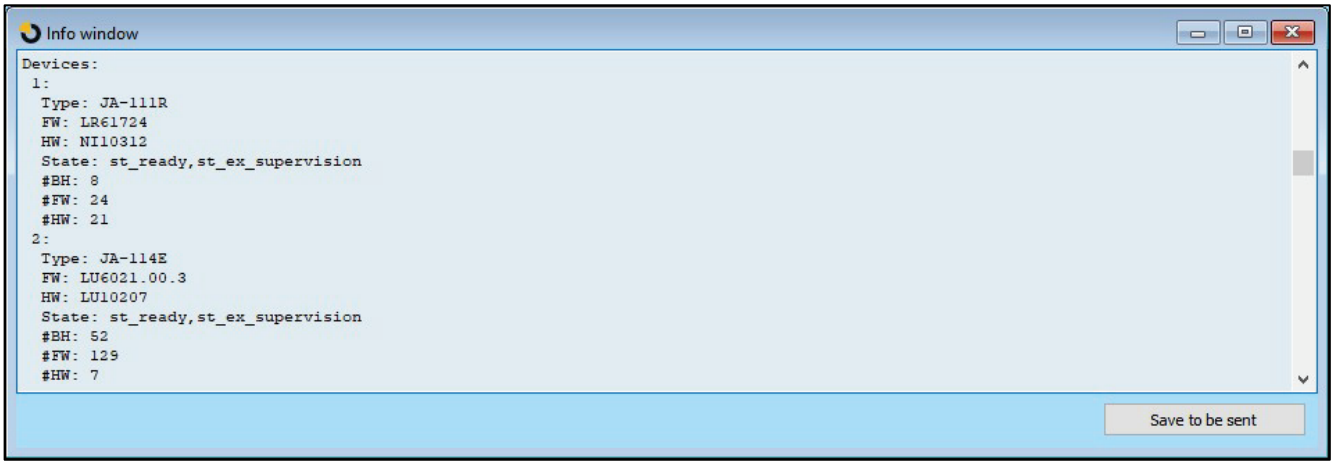
It is opened from the main menu **Control Panel / Info bubble** during generation of the Info bubble the control panel addresses all connected devices and wireless devices to ask for their current information.

The **Info bubble** offers a general overview of technical data of the entire system, incl. control panel (serial number, registration code, FW and HW version, voltage and current of the BUS, setting range of: devices, sections, PG outputs), all the used communicators (GSM: phone number, signal BTS number, LAN: status, MAC, IP, phone line status) as well as all BUS and wireless devices (uni and bidirectional): device type, identification of FW / HW versions of individual devices and their status. It is available in all statuses of the system (set / unset / service).

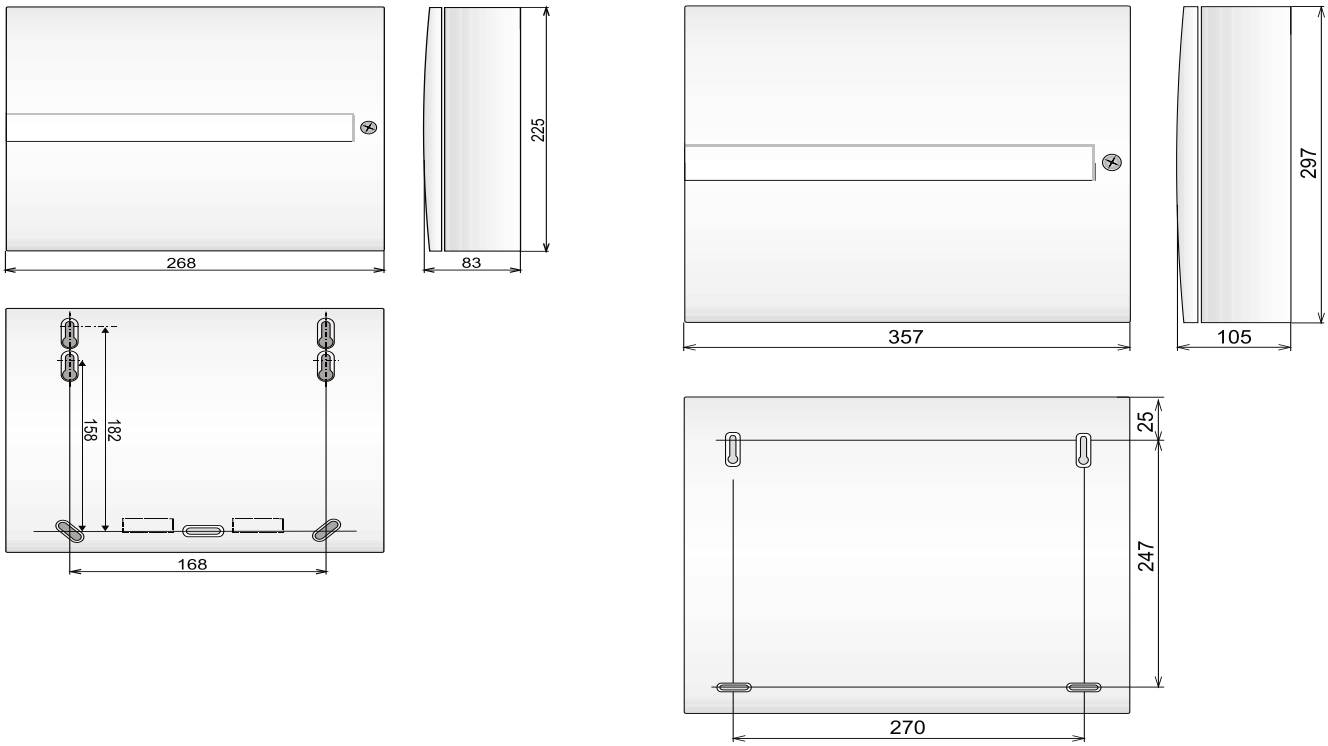
This data is necessary e.g. for communication with the technical consultant for which the Save for Sending button in the bottom right corner is designed for. The file is a ZIP compressed file and it contains numerical data of the installation, incl. a part of the event history (100 kB), but it does not contain any sensitive data as phone numbers of users or their access codes or other confidential data. The saved file achieves the size on the order of hundreds of KB and therefore it can be distributed using common means, e.g. e-mail.



JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



13.6 Control panels dimensions



14 MyJABLOTRON web application

The MyJABLOTRON web application is a unique service that provides users and installation technicians with online access to devices produced by Jablotron. Jablotron customers can use it for administration of their systems. End users of alarms can use it to control and monitor their device. It provides installation technicians with a powerful tool that allows them to monitor and administer all installed alarms and to comfortably create quotations for new installations.

Everything concerning your alarms or installation is available clearly in one application that is accessible from anywhere.

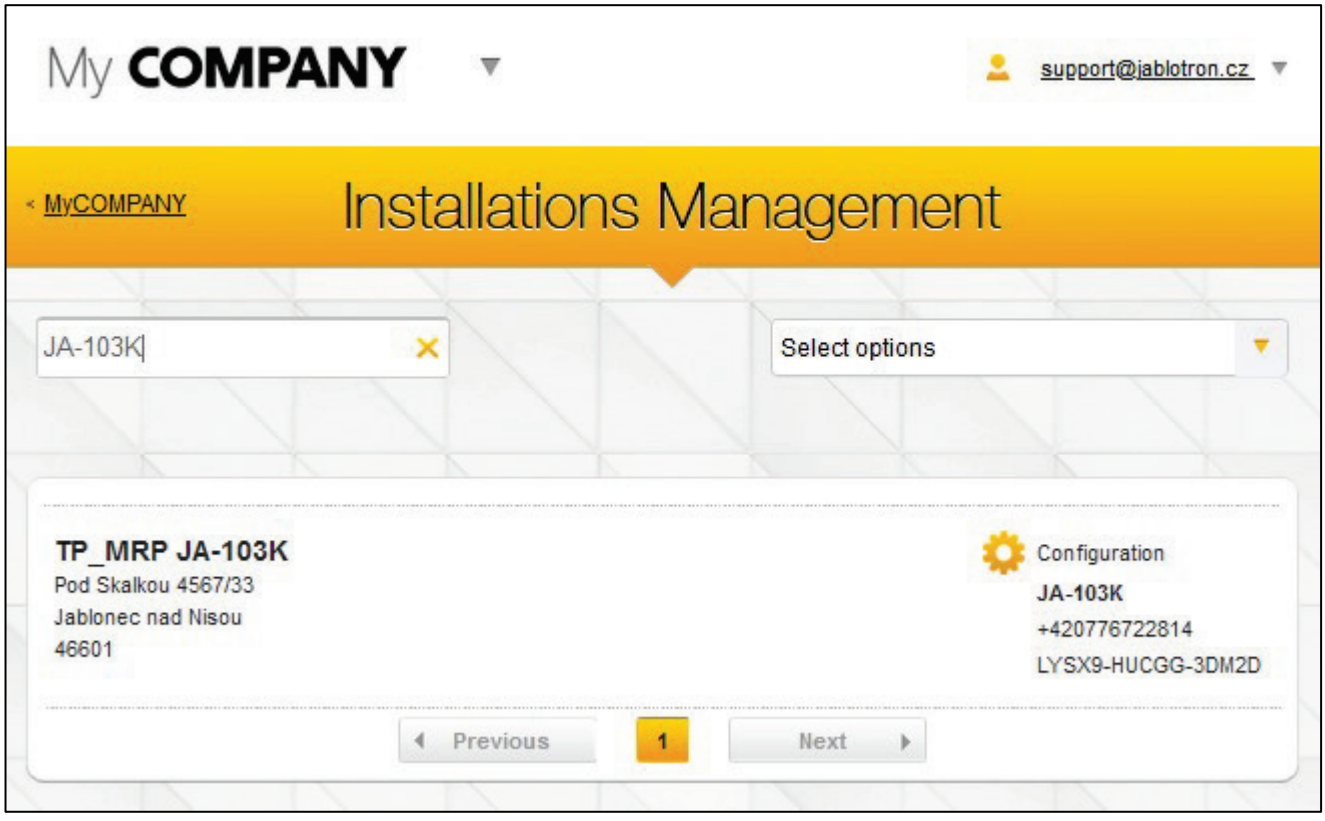
The MyJABLOTRON application enables users to:

- See the **current status of an alarm** (in the initial widget your registered devices are visible together with the last registered event and the number of sections in the unset and set status).
- **Set / unset an alarm** or its part.
- **Control** programmable **outputs** (most frequently for appliance control).
- View history of events with the possibility to export it to a file.
- **View and if allowed, take photos** from verification devices.
- **Monitor the course of temperature** in the building or outdoors (incl. notification of exceeding of the lower or upper limit of set temperatures at a defined time of the day).
- **Monitor consumption of electricity** (incl. setting of a notification in case of exceeding the hourly/daily/monthly consumption).
- **Send messages** to selected contacts by SMS, e-mail, using the standard PUSH notifications for mobile phones.
- And other useful functions.

14.1 Management of installations and offers for an installation technician

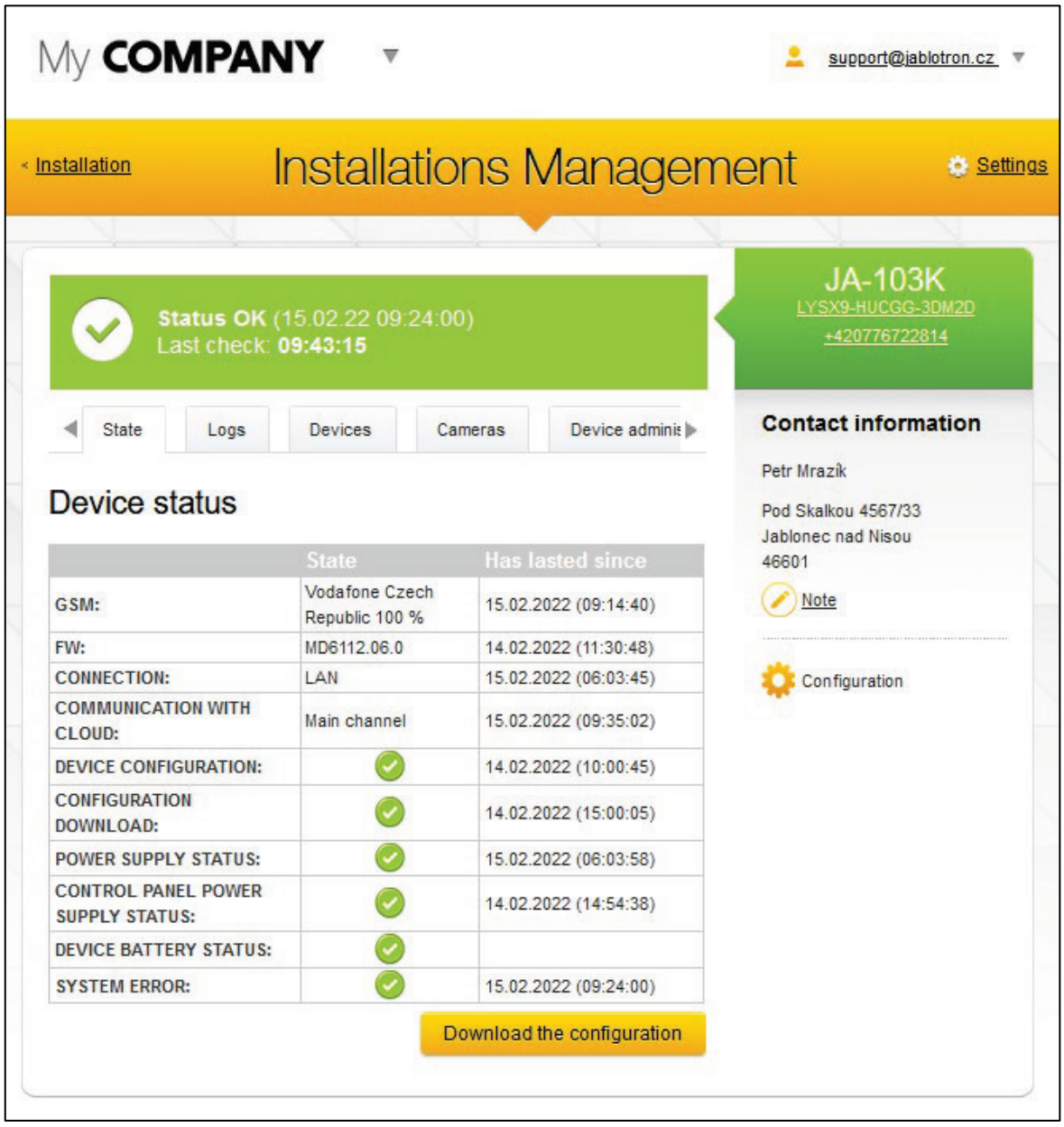
Overview of all installed devices registered in MyJABLOTRON – Installation Management module

This is a unique tool for installation technicians, who can manage all their installed systems in one place, incl. a complete overview of their current technical status, view of the history and operation diagnostics... You will find the **Installation Management** module in your account in the MyJABLOTRON application in the **MyCOMPANY** part (if supported in your region).



JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

You can filter your installations by the alarm type or based on their current status. Thus, you can pre-set notification for a technical problem and you can quickly respond to it with a service intervention. This way, you can provide your customer with an above-standard service as you will contact him/her before the customer starts to solve the system problem.



In the detail of every control panel the installation technician gets a general overview in the form of status display of individual groups of faults (states of power supply, communication, status of batteries in devices, interference or other faults, SIM card type in the device and current GSM signal quality, current FW version) with the date since when the status has been active. Besides, the technician gets overview of the complete event history – but it must be allowed by the building owner in his/her settings.

In the **Installation Management** application, you will also find a complete log of the technical events of the alarm with a graphic representation of the GSM connection quality, history of firmware changes or communication.

14.2 WEB-Link application (configuration)

A very useful application for an installation technician within the MyJABLOTRON web service is **WEB-Link**. It is application very similar to the F-Link software but with the difference that this application is running on the server and it is accessible from everywhere via any web browser. Start the application by clicking on the icon Configuration in Installation management in MyCOMPANY. The installer is able from any computer to change almost all settings in the system assigned to his profile regardless where he is and which platform does he use. Changes performed by installer are stored on the server and can be saved to the system immediately or at some time which can be set or after system unsetting by user. The installer can be informed of changes via SMS or e-mail.

15 System takeover by the user

When installation of the security system is finished it is generally recommended to create documentation (report about handing over the system, security system LOG, etc.) where there will be all information about the number and location of devices such as detectors, sirens, keypads, their segments and how they have been configured. System users should be trained how to use the system according to following points:

1. Control from system keypad. Setting and unsetting of sections (from control segments or from keypad menu).
2. Ensure that exit / entrance time is adequate and also valid for garage doors or other entrance routes.
3. Explain what authorization is, what it is for and options like codes with and without prefixes, RFIS tags, etc…
4. Partial setting at home. Difference in indication between partial and full setting.
5. Control of home automation using control segments and other functions (Panic, Fire, health troubles).
6. Triggering an alarm when the system is set included sirens, test of alarm call.
7. Explaining the difference between alarm cancelling by authorization and unsetting a section.
8. Section control (remotely via voice menu using cell phone keypad).
9. Section control and home automation (PG outputs) via SMS.
10. Control using the MyJABLOTRON application from smartphones or from a website.
11. Editing user codes by the user via the keypad and via JA-100-Link software.

Don't forget to offer annual system checking to your customer. It is very useful to check the system functions periodically, not only the control panel but also all installed devices. The technician creates a report about the annual check performance and this can serve the insurance company. The annual check being due can be indicated to the customer automatically by an LCD keypad.

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

16 Technical specifications

<table>
<tr><td>Parameter</td><td colspan="2">JA-103K</td><td colspan="2">JA-103K-7 Ah</td><td colspan="2">JA-107K</td></tr>
<tr><td>Control panel power supply</td><td colspan="2">~ 110–230 V / 50–60 Hz,
max. 0.28 A
with fuse F1.6 A/250 V
Protection class II</td><td colspan="2">~ 110–230 V / 50–60 Hz,
max. 0.28 A with fuse
F1.6 A/250 V
Protection class II</td><td colspan="2">~ 110–230 V / 50–60 Hz,
max. 0.85 A with fuse
F1.6 A/250 V
Protection class II</td></tr>
<tr><td>Back-up battery</td><td colspan="2">12 V; 2,6 Ah (lead gel)</td><td colspan="2">12 V; 7 Ah (lead gel)</td><td colspan="2">12 V; 7 to 18 Ah (lead gel)</td></tr>
<tr><td>Maximum battery charging time</td><td colspan="2">48 h</td><td colspan="2">48 h</td><td colspan="2">48 h</td></tr>
<tr><td>BUS voltage (red - black)</td><td colspan="2">12,0 to 13,8 V</td><td colspan="2">12,0 to 13,8 V</td><td colspan="2">12,0 to 13,8 V</td></tr>
<tr><td>Maximum continuous current consumption from the control panel</td><td colspan="2">1000 mA</td><td colspan="2">1000 mA</td><td colspan="2">2000 mA permanent
3000 mA for 60 minutes
(max. 2000 mA for one BUS)</td></tr>
<tr><td rowspan="3">Max. continuous current consumption for back-up
12 hours</td><td colspan="2">JA-103K – 2.6 Ah back-up battery</td><td colspan="2">JA-103K – 7 Ah back-up battery</td><td colspan="2">JA-107K – 18 Ah back-up battery</td></tr>
<tr><td>Without GSM communicator</td><td>LAN – OFF: 115 mA
LAN – ON: 88 mA</td><td>Without GSM communicator</td><td>LAN – OFF: 328 mA
LAN – ON: 304 mA</td><td>Without GSM communicator</td><td>LAN – OFF: 1135 mA
LAN – ON: 1107 mA</td></tr>
<tr><td>With GSM communicator</td><td>LAN – OFF: 80 mA
LAN – ON: 53 mA</td><td>With GSM communicator</td><td>LAN – OFF: 296 mA
LAN – ON: 272 mA</td><td>With GSM communicator</td><td>LAN – OFF: 1100 mA
LAN – ON: 1072 mA</td></tr>
<tr><td rowspan="2">Max. continuous current consumption for back-up
24 hours</td><td>Without GSM communicator</td><td>LAN – OFF: 21 mA</td><td>Without GSM communicator</td><td>LAN – OFF: 136 mA
LAN – ON: 112 mA</td><td>Without GSM communicator</td><td>LAN – OFF: 535 mA
LAN – ON: 499 mA</td></tr>
<tr><td>With GSM communicator</td><td>LAN – OFF: 17 mA</td><td>With GSM communicator</td><td>LAN – OFF: 104 mA
LAN – ON: 80 mA</td><td>With GSM communicator</td><td>LAN – OFF: 530 mA
LAN – ON: 494 mA</td></tr>
<tr><td>Maximum number of devices</td><td colspan="2">50</td><td colspan="2">50</td><td colspan="2">230</td></tr>
<tr><td>LAN communicator</td><td colspan="2">Ethernet interface, 10/100BASE</td><td colspan="2">Ethernet interface, 10/100BASE</td><td colspan="2">Ethernet interface, 10/100BASE</td></tr>
<tr><td>Dimensions (mm)</td><td colspan="2">268 x 225 x 83 mm</td><td colspan="2">357 x 297 x 105 mm</td><td colspan="2">357 x 297 x 105 mm</td></tr>
<tr><td>Weight with/without AKU</td><td colspan="2">1844 g / 970 g</td><td colspan="2">3755 g / 1665 g</td><td colspan="2">7027 g / 1809 g</td></tr>
<tr><td>Reaction to invalid code entry</td><td colspan="6">Alarm after 10 wrong code entries</td></tr>
<tr><td>Event memory</td><td colspan="6">Approx. 7 million latest events, including date and time</td></tr>
<tr><td rowspan="2">Power supply unit</td><td colspan="6">Type A according to EN 50131-6</td></tr>
<tr><td colspan="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.</td></tr>
<tr><td>Classification</td><td colspan="6">Security grade 2 according to EN 50131-1</td></tr>
<tr><td>Operational environment</td><td colspan="6">Environmental class II (indoor general) according to EN 50131-1</td></tr>
<tr><td>Operational temperature range</td><td colspan="6">-10 °C to +40 °C</td></tr>
<tr><td>Average operational humidity</td><td colspan="6">75 % RH, non-condensation</td></tr>
<tr><td>Complies with</td><td colspan="6">EN 50131-1, -3, -5-3, -6, -10, EN 50136-1, -2, EN IEC 63000, T 031</td></tr>
</table>

Radio operating frequency (with the JA-11xR module)	868.1 MHz
Radio emissions	ETSI EN 300 220-1, -2 (module R), ETSI EN 301 489-7, ETSI EN 301 511 (GSM)
EMC	EN 50130-, EN 55032
Safety conformity	EN 62368-1
Caller identification (CLIP)	ETSI EN 300 089
Operational conditions	ERC REC 70-03
Certification body	Trezor Test s.r.o. (no. 3025), Kiwa Nederland b. v.

JABLOTRON a.s. hereby declares that the devices JA-103K, JA-103K-7Ah, JA-107K are designed and manufactured 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.

NOTES:

JABLOTRON a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com