JABLOTRON

CONTROL PANELS

JA-103K | JA-103K-7Ah | JA-107K | JA-108K
of the JABLOTRON security system

The control panel is the basic element of the JABLOTRON alarm system, which is designed to protect small, medium and large properties. The control panel can be operated in various configurations, which can be applied by selecting a configuration profile (the default setting is the "Default" profile). The control panel allows the connection of Bus devices and, when using the JA-11xR radio module, also the connection of wireless devices (except for JA-108K and profile settings for Security Grade 3 according to EN 50131).

- The JABLOTRON alarm system is intended exclusively for installation by a trained installation technician who has a valid JABLOTRON certificate.
- The JA-108K control panel supports profile settings for EN 50131 Security Grade 3 only as a Bus system. If it is necessary to use JABLOTRON wireless devices, it is possible to switch the control panel to Security Grade 2 and operate as a hybrid alarm system.
- It is recommended to use only JABLOTRON 100 series devices throughout the system, or devices recommended directly by the manufacturer JABLOTRON. When using other components, the correct functioning of the system and the achievement of the required security grade cannot be guaranteed.
- Some of the functions described in the manual require the installation of additional accessories.
- Connecting JA-100 control panels using LAN to the same network with active 48V PoE power supply may cause unreliable network communication. We recommend using a PoE splitter.

MMD20008

1 Introduction **6**
1.1 Terms and definitions 6

2 Control panel features **10**
2.1 Technical specifications 10
2.1.1 Mechanical dimensions 14
2.2 JA-103K 14
2.3 JA-103K-7Ah 15
2.4 JA-107K 16
2.5 JA-108K 17
2.6 Extension accessories for control panels 18
2.6.1 RJA-11xR radio module 19
2.6.2 GJA-19xY GSM communicators 19
2.6.3 JA-110Z-D Multi-position Bus splitter 19
2.7 Common parts of control panels 20
2.7.1 Control elements on the control panel 20
2.7.2 LED indicators on the control panel board 21
2.7.3 Micro SD card 21
2.7.4 Control panel Bus 21
2.7.4.1 Bus length and number of connected devices 22
2.7.4.2 Bus arrangement, branching 22
2.8 Functional characteristics of the system 22
2.8.1 System profiles 23
2.8.1.1 Overview of surmountable and insurmountable causes preventing security 25
2.8.2 Control panel operating modes 26
2.8.3 User authorisation 28
2.8.4 JABLOTRON system authorisation means 29
2.8.4.1 Access codes 30
2.8.4.1.1 Use of invalid codes 31
2.8.4.1.2 Factory default codes 31
2.8.4.2 Changing access codes 32
2.8.4.3 RFID cards and chips 32
2.8.4.4 Authorisation using a combination of codes and RFID devices 32
2.8.5 Object and division into sections and subsections 33
2.8.5.1 Common section 33
2.8.6 System reactions, statuses and reports 33
2.8.6.1 Overview of configurable device reactions 34
2.8.6.2 Types of alarms and their processing 36
2.8.6.2.1 Delayed A 37
2.8.6.2.2 Tamper alarm 37
2.8.6.2.3 Fire alarm 37
2.8.6.2.4 Panic 38
2.8.6.2.5 24-hour alarm 38
2.8.6.2.6 Ending an alarm 38
2.8.6.2.7 False alarm reduction 39
2.8.6.3 Fault states 39
2.8.6.3.1 Fault due to loss of device 40

3 System installation and commissioning . . . 41
3.1 Before installing the system . . . 41
3.1.1 System design . . . 42
3.1.1.1 System control . . . 42
3.1.1.2 Selection of control components . . . 45
3.1.1.3 Alarm output selection . . . 46
3.1.1.4 Choice of control panel, profile and system size . . . 46
3.2 Control panel installation . . . 47
3.2.1 Preparation and installation of the control panel . . . 47
3.2.2 System . . . 47
3.2.3 Example of determining consumption for system backup . . . 48
3.2.4 Installation of Bus devices . . . 48
3.2.4.1 CC-xx Bus cables . . . 48
3.2.4.2 Bus arrangement, branching . . . 49
3.2.4.3 Calculation of voltage drops and consumption . . . 49
3.2.4.3.1 Example of calculating voltage drop in a simple installation . . . 50
3.2.4.4 Bus separation . . . 51
3.2.4.5 Use of existing cabling during renovations . . . 51
3.2.5 Installation of wireless devices . . . 51
3.2.5.1 Installation of the JA-11xR radio module: . . . 52
3.2.5.2 Registration and placement of wireless devices . . . 53
3.3 Commissioning . . . 53
3.3.1 Handover of the system to the operator/user . . . 54

4 System configuration . . . 54
4.1 System activation . . . 55
4.1.1 Connecting the control panel to the system . . . 56
4.1.2 Starting the Wizard . . . 56
4.2 F-Link tabs . . . 56
4.2.1 Initial setup . . . 56
4.2.2 Sections . . . 57
4.2.3 Devices . . . 58
4.2.3.1 Enrolling or removing devices . . . 59
4.2.3.2 Keypad configuration . . . 60
4.2.3.2.1 Segments tab . . . 61
4.2.3.2.2 Settings tab . . . 63
4.2.3.2.3 Common segment . . . 65
4.2.3.3 Internal siren configuration . . . 66
4.2.4 Users . . . 68
4.2.5 PPG outputs and activation maps . . . 69
4.2.6 User reports . . . 72
4.2.7 Parameters . . . 74
4.2.8 Diagnostics . . . 80
4.2.9 Calendar . . . 81

4.2.10 Communication . . . 82
4.2.10.1 GSM settings . . . 83
4.2.10.1.1 GSM restart . . . 85
4.2.10.2 LAN settings . . . 85
4.2.10.3 Camera settings . . . 86
4.2.11 ARC and transmissions . . . 87
4.2.11.1 Transfer of photos to external storage . . . 88
4.3 Additional settings . . . 88
4.3.1 Keypad (virtual) . . . 88
4.3.2 UEvents . . . 89
4.3.3 Settings . . . 90
4.3.4 RF signal . . . 92
4.3.5 Buidling map . . . 92
4.3.6 Service . . . 93
4.3.7 Maintenance . . . 93
4.3.8 Refresh . . . 93
4.3.9 Online . . . 93
4.3.10 Internet . . . 93
4.3.11 Installation wizzard . . . 94
4.3.12 Installation information . . . 94
4.3.13 Firmware update . . . 95
4.3.14 Label printing . . . 95
4.3.15 Settings history . . . 95

5 System control . . . 97
5.1 User authorisation . . . 98
5.2 Keypad control . . . 98
5.2.1 System control from the keypad segment . . . 98
5.2.2 System control from the JA-114E, JA-115E and JA-116E keypads . . . 101
5.3 Remote control . . . 105
5.4 Calendar control . . . 105
5.5 Control from the communicator voice menu (GSM) . . . 107
5.6 SMS command control . . . 108
5.7 Control of F-Link or JA-100-Link software . . . 110
5.8 Duress access control . . . 111
5.9 Reporting events to users . . . 111
5.10 Acoustic signals . . . 112
5.11 System restrictions and blockages . . . 113
5.11.1 Time-limited access of users . . . 113
5.11.2 Reasons preventing system security . . . 114
5.11.3 Unsuccessful setting . . . 115
5.11.4 Non-alarm system functions . . . 116
5.11.5 Bypassing and blocking options . . . 116
5.11.5.1 Disabling a device . . . 116
5.11.5.2 Blocking when setting . . . 117

6 Maintenance and service **118**
6.1 Maintenance 118
6.2 Service 119
6.2.1 Resetting the control panel 119
6.2.2 Firmware updates 119
6.2.2.1 General rules 120
6.2.2.2 Updating the FW of the control panel and devices connected to the Bus 121
6.2.2.3 FW update for wireless devices 121
6.2.2.4 Check after FW update 122
6.2.2.5 Info window 122

7 Legislative information and declaration of conformity **123**

8 Overview of related documents **124**

1 Introduction

This manual serves as a basic technical specification and functional description of JABLOTRON control panels of the following types:

- JA-103K, and its variants JA-103K-7AH,
- JA-107K
- JA-108K

and a simplified manual for the design, installation and commissioning of the alarm system. It also describes how to configure the alarm system using the F-Link software, basic system operation and maintenance and service requirements.

1.1 Terms and definitions

This chapter briefly explains the basic concepts, terms and their definitions used throughout the manual.

Modular system – Allows you to create and develop a system that precisely matches the size of the building and the needs of users in terms of range and functions. The system can also be expanded by adding additional devices and modules.

Firmware (FW) update – A procedure in which a new version of FW containing new functions, improvements and modifications is uploaded to the system. It is recommended to check that the FW is up to date during each installation and during regular service checks. It is always necessary to update the FW of all devices that allow updates (keypads, radio modules, motion detectors with cameras, etc.).

Access module (keypad) – A basic component of the control keypad, used to identify the user. The simplest version contains only a contactless RFID chip/card reader. A version with a keypad and LCD display is also available. Access modules are available in bus and wireless versions. Each access module always includes one control segment. The range is complemented by an outdoor version of the RFID chip reader and a keypad with a reader.

Control segment – Component of the interior control keypad. The segment has two buttons (left = off, right = on). By installing the required number of segments to the access module, you can create a keypad that precisely matches the required functions. The segments clearly indicate the status of the system and allow for intuitive control. Thanks to the installed segments, the user can clearly see what functions their system provides (they are not hidden somewhere in the menu) and for which they have authorisation.

Control keypad – Consists of an access module and one or more control segments. It is used for normal system control and user authorisation.

Alarm types – The system is capable of responding to burglary, duress, sabotage, fire, gas leaks and flooding. By using appropriate detectors, other dangers can also be reported (movement in the garden, tampering with a guarded object, high temperature, danger of freezing, etc.). To reduce false alarms, advanced responses can be set for detectors (repeated activation of the detector or confirmation by another detector).

Visual alarm verification – Photo verification devices (camera detectors, verification cameras) can automatically take and send photos or video sequences of events in the system. This allows the user to look back and see what caused the alarm, etc.

Personal protection – In the event of a hold-up, health problems or fire, the user can call for help (using a button on the keypad, entering an emergency code, an emergency button or a wireless controller).

Duress access control – Used to trigger a silent/panic alarm by simply authorising or controlling (setting, unsetting, controlling PG, etc.) the system if the user is in danger. The silent/panic alarm is triggered when the system is controlled by entering the user code with 1 added to the last digit of the code (e.g. code 1234 becomes 1235).

Delayed panic – A function for triggering a silent/panic alarm with a time delay during which the alarm can be cancelled. It is intended, for example, for users who are afraid to open the entrance door to an unknown

person who could attack them. The user activates the delayed panic alarm before opening the door and, if they are sure they are safe, must cancel the function before the delayed panic alarm timer expires. The delay time is set on the device used to trigger the alarm (keypad segment, panic button, etc.).

Event reports – Reporting all events to the alarm receiving centre (ARC) can ensure timely intervention by professionals. Reports can be sent to the ARC via the built-in LAN communicator. With the addition of a GSM communicator, reports can also be sent directly to users via SMS messages or voice calls.

Special reports – SMS or voice messages whose meaning can be set independently of other functions. Sending a report can be linked to the activation of a device. This makes it possible, for example, to monitor the status of other devices or technologies with a fault output, etc.

Remote control – When the system is expanded with communication modules, authorised users can:

call into the system and use the voice menu to control or check the status of the security system, use defined SMS commands to control sections and PG outputs, control selected functions by calling from authorised telephone numbers, remotely manage the system using F-Link software (for service technicians) and JA-100-Link (for system administrators). The system can also be controlled remotely using the web service at www.myjablotron.com or smartphone applications.

MyJABLOTRON – A unique service that allows online access to JABLOTRON devices. It is intended for end users and also installation technicians. Use of the MyJABLOTRON service requires a JABLOTRON security SIM card (in the Czech Republic, it is supplied with the communicator; for information on using the MyJABLOTRON service abroad, contact distributors).

User access rights – Defines the level of user permissions. You can set which part of the property or which programmable outputs (PG) the user can control. The user proves their identity by attaching an RFID/NFC chip/card or entering a code on the keypad. The system allows you to selectively set time restrictions on user access to secured sections and control of PG outputs.

Administrator – The system allows you to specify the required number of administrators who set access rights for regular users. Different sections of the building can have different administrators. The system is factory-set with one main administrator who always has access rights to all sections and can control all PG outputs. At the same time, they also have the authority to set access rights for all users (the factory default code is 1234, but this code must be changed before the system is put into operation – the change is enforced by the F-Link software if necessary).

Service technician – The system allows you to set up multiple service technicians for administration and programming. The factory default service code is 1010 (however, this code must be changed before the system is put into operation – the change is enforced by the F-Link software if necessary). Logging into the system with the service code allows complete configuration of the system. Access to service mode can be conditional on administrator approval (authorisation). The ARC code is a special level of service authorisation. This code locks access to the settings for communication between the system and the alarm receiving centre (ARC).

F-Link (JA-100-Link) – Configuration software for system settings demands a computer with the Windows operating system. The control panel can be connected to a computer locally using a USB cable or remotely from a computer connected to the internet (some software functions are not available during remote connection, e.g. changing the control panel language or updating its firmware). F-Link is intended exclusively for trained service technicians. It cannot be provided to system administrators or end users. System administrators can use a simplified version of the JA-100-Link software, which allows for certain system settings (user management, diagnostics, calendar event settings, event log printout).

Service mode – System status in which the complete configuration can be changed. Only a service technician (or ARC technician) can put the system into service mode by connecting the control panel to the F-Link software (via a USB cable or remotely via the Internet). In SERVICE mode, the system is completely out of operation, the programmable PG outputs are switched off (it does not monitor and does not provide any user functions, e.g. control of programmable PG outputs). The SERVICE status is indicated on the keypads by the yellow system LED indicator flashing twice in 2 seconds.

Maintenance – Status intended primarily for system administrators. It allows maintenance to be performed in the section(s) for which the Administrator(s) has (have) authorisation (e.g. replacing batteries in detectors). The administrator can switch the system to Maintenance mode using the keypad or JA-100-Link software

(the service technician can enter maintenance mode from the F-Link software). Maintenance mode in a given section does not affect the status and functionality of other sections or the status of PG outputs. The service technician can restrict access to maintenance mode for Administrators in the system parameters. The MAINTENANCE status is indicated on the keypads by the segments of the relevant section going out and the green system LED indicator flashing twice in 2 seconds.

Day/night mode – Allows you to set different system behaviours for day and night times. For example, you can set different keypad backlight intensities or set PG output activation according to this system status (lighting blocking during the day). Day/night mode can be switched according to the selected devices (e.g. twilight sensor) or using sunrise and sunset data from the astronomical calendar. For this option, it is necessary to set the coordinates of the location where the system is installed.

Appliance control – The system has programmable PG outputs that can be used to switch various devices on and off. The PG represents the logic used in the system, which then controls the required number of output modules (system devices). Outputs can be controlled using segments on the keypad, by activating detectors or remote controls, by events in the system (e.g. section arming, alarm...), by a set automatic calendar action, by an SMS command, by ringing an authorised user or by accessing the MyJABLOTRON application. The PG output activation can be blocked by the section status, detector or other PG. Output activation and deactivation can be reported to users via SMS message or data transfer to the MyJABLOTRON service (push notification).

Door lock control – The electric door lock (connected to the PG output) can be opened by placing an RFID/NFC chip/card or entering a code on the keypad. Each user can be programmed to open specific doors. The output can be blocked by a set section, so there is no risk of entry into the area if it is guarded. Door opening by user authorisation can be recorded in the system event log.

Calendar – Allows you to program automatic time-based actions – guarding (setting/partial setting/unsetting) of sections and control of programmable PG outputs (switching on/off, blocking/unblocking). Each action can be set for the day and month in which it will be performed. On the selected day, it is possible to set up to 4 times or repetitions at set intervals.

Bus devices – They connect to the system using a bus cable (4 wires). The bus provides power and communication. Bus devices (detectors, keypads, sirens, etc.) require assignment to a position (address) in the system in order to function. There are also non-addressable devices that simply connect and function without being assigned a position (some PG output modules, status indicators, bus separators, etc.).

Wireless devices – For wireless communication, the control panel must be equipped with a radio module and wireless devices (detectors, keypads, sirens, etc.) must be assigned to a position (address) in the system. The system may also include non-addressable wireless devices that do not occupy a position in the system (they are only receivers and do not report to the control panel), e.g. PG output modules. To cover a larger area, up to 3 radio modules (connected to the bus via a cable) can be installed in the system to cover the area in a larger building. The control panel performs regular communication checks on selected wireless devices (Supervision parameter). This check also includes monitoring the status of the power supply batteries. If communication with a wireless device is lost, the control panel reports its failure. The radio modules monitor radio background interference from foreign signals on the JABLOTRON system communication frequency. If this occurs, the system can trigger a fault (this function is optional and disabled by default).

Intrusion detectors – A group of detectors used to identify the intruder. These include motion, opening, glass breakage, tilt and shock detectors. The desired response to activation is programmed for the detectors in the system. This defines how the system will respond to the activation of the detector. Intrusion detectors do not include fire, gas, flood or panic responses.

GSM communicator – An extension module for the control panel for communication via mobile networks and the Internet. This allows the system to transmit data to an alarm receiving centre (ARC). The communicator enables remote access to the control panel via F-Link (JA-100-Link) software, event reporting to users and remote control of system functions.

LAN communicator – An integrated part of the control panel providing an internet connection. It enables fast remote access to the F-Link and JA-100-Link software, data transmission to the MyJABLOTRON service and to the alarm receiving centre (ARC), which is equipped with reception technology for the JABLOTRON protocol. It is possible to select which communication path will be primary and which will be backup.

Sections – The system can be split into sections, in which setting and unsetting can be controlled independently. A section can be a separate flat in an apartment building, a shop in a shopping centre or a department in a company. The independence of a section can be set as if it were secured by a separate control panel (user access rights, reports, display on keypads, acoustic signalling, MyJABLOTRON service, etc.).

Common section – This is a separate section designated as subordinate to selected sections. If the last superior section is set, the common section is automatically set as well. When the first of the superior sections is unset , it is also unset. It is used to secure areas such as common corridors, sanitary facilities, company kitchens, etc. Direct control of the common section is not recommended.

Common segment – This is a keypad segment function that allows you to control multiple sections simultaneously with a single press. These sections must be assigned to separate segments on the keypad. Each keypad can have up to two segments with the common segment function, allowing you to control two different groups of sections simultaneously.

Partial set – Optional (independently adjustable) mode for each section. If partial setting is enabled, the system does not respond to intrusion detectors that have the "internal" parameter set (i.e. they guard the interior). This allows movement in the residential part of the house, but the system responds with an alarm or by activating the entry delay when someone enters through the door or moves in the garage or basement. If the section is completely secured, it responds to the activation of all detectors assigned to it.

Bypass – Confirmation of the triggered device input or an active fault in the system during setting. Active inputs after bypassing are not evaluated until they are deactivated (restored). After deactivation (restoration), the devices are again included in the guarding and are thus fully functional. If there is a fault in the system, such as a power failure, bypassing only confirms that the user is aware of it, but its status does not change (it still persists in the system). The function depends on the control mode parameter settings and is only a one-time bypass during the system setting (unlike blocking, which lasts until it is turned off by the user).

Blocking – Disabling the input of an active device, preventing it from causing any reaction, including control of PG outputs. Blocking can also be performed manually from the LCD keypad, JA-100-Link, F-Link or MyJABLOTRON software, making it possible to block devices even outside the arming process. The function depends on the control method parameter settings.

Autobypass – Automatic disabling of the system's response to devices according to the selection (when one device repeatedly causes an alarm in one period, the system automatically bypasses it until it is unset or the autobypass is reset (daily at 12:00). Activation of inputs after three activations or three alarms (optional). Fault conditions after three activations.

Disabling a device – Option to manually disable selected sections, devices, users, PG outputs or calendar events. It is not possible to disable a section where a control panel is assigned or a user (Service at position 0 and Administrator at position 1). For devices, we distinguish between Blocking (input activation only), complete Device disabling, and Sabotage detection disabling. The system therefore does not respond to the activation of any tamper contact of the given device.

Ways of setting – Choosing the level of how the system will respond when setting. The options range from the lowest level, where nothing is checked (always set), to the highest level, where it is not possible to set with an active element (e.g. an open window), see chapter 5.11.2.

Event memory – The system records events in its memory. The memory can be viewed using the F-Link software (JA-100-Link) software, from the keypad with LCD display or from MyJABLOTRON. Usually, the beginning of an event is recorded as Activation (device status, faults, sabotage, etc.) and the end of an event as Deactivation. Section statuses are recorded as Set / Unset, alarm statuses as Alarm / Alarm Delay, Alarm Silence or Alarm Cancellation. Some events may only have an activation record (e.g. New Image, Panic Alarm, Configuration Change).

Magnet activation and deactivation

Start and End of Alarm

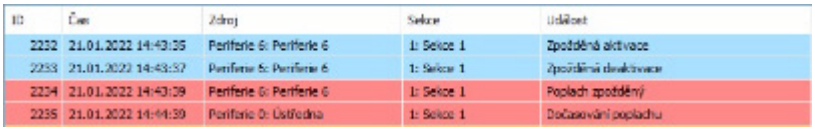


Figure 1 – Event memory

MicroSD memory card – The control panel uses a microSD card as a storage medium. After connecting the control panel to a PC using a USB cable, two drives will appear in the file manager: FLEXI_CFG and FLEXI_LOG. The SD cards supplied with the control panels can be up to 32 GB (SD/SD-HC). Before using a brand new SD card, it is necessary to first reset the control panel to factory settings, see chapter Resetting the control panel Resetting the control panel and then update the firmware, see chapter 6.2.2 Updating the firmware , which will save the necessary files (default settings and texts, audio recordings, etc.) to the memory card.

FLEXI_CFG – A disk with hidden directories and files containing system settings. Do not manipulate the contents of the disk, as this may cause the system to malfunction. This disk also contains the JA-100-Link directory with the JA-100-Link.exe software JA-100-Link.exe, which can be run and used by the System Administrator.

FLEXI_LOG – A disk containing the PHOTO directory and the FLEXILOG.TXT file, into which all events in the system are written. The selection of data from the file is displayed in F-Link / Event memory. The PHOTO directory stores files that have been sent to the control panel from camera devices (e.g. from motion detectors with cameras). Both types of files (txt and jpg) are stored in encrypted form, and their content cannot normally be viewed with text and image viewers. The PHOTO content can only be viewed if the F-Link (JA-100-Link) software is also running on the PC F-Link (JA-100-Link) is also running on the PC and authorisation has been granted with the Service or Administrator code. Events are written to the FLEXILOG.TXT file up to a size of 10MB, after which it is renamed to FLEXILOG.OLD and a new file is created a new file is created.

SIMLock – A control panel function that deletes the ARC tab settings when the SIM card is replaced with another one, if the control panel is registered with the MyJABLOTRON cloud service. If the SIM card is replaced (e.g. with another operator) before registering with MyJABLOTRON, nothing changes in the settings. This step prevents unwanted transfer of information to the ARC from a SIM card other than the one that was registered and for which the settings were made.

2 Control panel features

This chapter provides specifications and describes the functional features of JABLOTRON control panels, their design elements and other functions.

2.1 Technical specifications

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
Functional characteristics					
Max. number of devices	50	50	230 Max. 120 wireless devices at positions 1–120		Max. 60 devices per 1 Bus terminal
(I-)BUS outputs	1x Bus terminal 1x I-Bus onboard (JA-11xR only)	1x Bus terminal 1x I-BUS onboard (JA-11xR only)	2x Bus terminal 1x I-BUS onboard		
Maximum number of JA-11xR radio modules	3	3	3	0 for security level 3 3 for security level 2	Max. number of JA-11xR radio modules
Max. number of users	50	50	600		
Maximum number of independent monitoring sections	8	8	15		

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
Maximum number of programmable outputs	32	32	128		Only the following can be used for wireless transmission PG 1 - 32
Blocking of user inputs in case of incorrectly entered codes	No blocking			after 10 incorrectly entered codes, then every subsequent attempt	User input is, for example, a keypad or F-Link
Alarm Sabotage due to incorrect code entry / blocking time	after 10 incorrectly entered codes			Optional: 10 to 21 incorrect code entries	
Event memory	approx. 7 million recent events including date and time				
Alarm system features					
Compliant with standards	EN 50131-3, EN 50131-5-3, EN 50131-6, EN 50131-10 (EN 50136-2, EN 50136-1)				
	INCERT T 031			---	
Security classification	Degree 2			Security level 3 or 2	According to profile
Environment class	II Indoor general				
Power supply type	Type A according to EN 50131-6				
ATS classification	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP5 (LAN) SP5 (GSM) DP3 (LAN+GSM)	When using a GSM communicator, see the separate communicator manuals for more information.
Certification body	Trezor Test s.r.o. (No. 3025), Kiwa Nederland b. v.			Trezor Test s.r.o. (No. 3025)	
External communication					
LAN communicator	on board Ethernet 10/100 BASE	on board Ethernet 10/100 BASE	on board Ethernet 10/100 BASE		
GSM communicator	Yes, using accessories	Yes, using accessories	Yes, using accessories		Not included in the control panel.
- SMS reports	up to 8 users	up to 8 users	up to 50 users		5 reports per event
- Voice reports	up to 8 users	up to 8 users	up to 15 users		5 reports per event
- Caller identification (CLIP)	ETSI EN 300 089				
Control panel power supply					
Power supply voltage	110 ÷ 230 VAC 50 ÷ 60 Hz	110 ÷ 230 VAC 50 ÷ 60 Hz	110 ÷ 230 VAC 50 ÷ 60 Hz		

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
Maximum current consumption	max. 0.28 A	max. 0.28 A	max. 0.85 A		
AC power consumption	max 30 VA	max 30 VA	max. 55 VA		At maximum Bus load and with GSM module
Current protection	Fuse 5x20 F1.6 A/250 V	Fuse 5x20 F1.6 A/250 V	Fuse 5x20 F1.6 A/250 V		
Electrical protection class	II	II	II		
Electrical parameters for calculating battery backup					
Nominal DC current consumption of the control panel board with LAN	90 mA	90 mA	105 mA		Consumption measured from the battery
Nominal DC current consumption of the control panel board without LAN	60 mA	60 mA	70 mA		Current consumption measured from the battery
Low battery voltage fault notification voltage	11 V	11 V	11 V		
Voltage at the end of low battery voltage detection	12.2 V	12.2 V	12.2 V		
Deep discharge protection – Battery disconnect voltage	9.6 V	9.6 V	9.6 V		
Power outputs					
Bus voltage	12.0 to 13.8 V	12.0 to 13.8 V	12.0 to 13.8 V		Terminals (red – black)
Max. continuous consumption from the control panel	1000 mA	1000 mA	2000 mA (max. 3000 mA / 60 min)		JA-107K / JA-108K provides 2x Bus terminals and an I-BUS connector for expansion. The maximum consumption from the control panel must be divided between both outputs.
Max. continuous load of one Bus terminal	1000 mA	1000 mA	2000 mA		
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 connecting a radio module or hub JA-110Z-D		For JA-107K, the individual Buses are isolated from each other between , i.e. short-circuiting one branch will not affect another
Maximum Bus cable length	500 m	500 m	3 x 500 m		can be extended using JA-120Z modules
Operating characteristics					
Dimensions	268 x 225 x 83 mm	357 x 297 x 105 mm	357 x 297 x 105 mm		
Weight with battery/without battery	1844 g / 970 g	3755 g / 1665 g	7027 g / 1809 g		
Operating temperature range	-10 °C to +40 °C				

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
Average operating humidity	75% RH, non-condensing				
System and control panelbackup					
Recommended backup 12V battery	12 V / 2.6 Ah (lead-acid gel)	12 V / ≤7 Ah (lead gel)		12 V / 18 Ah (lead gel)	
Maximum time to recharge the battery to 80% capacity	48	48		48	

Table 1 – Technical Specifications table

Bus current consumption for different backup times and control panel configurations:

Required configuration			JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
Time backup	GSM	LAN	Battery 12 V / 2.6 Ah	Battery 12 V / 7 Ah	Battery 12 V / 18 Ah	Battery 12 V / 18 Ah	
12 hours	NO	OFF	113 mA	406 mA	1135 mA	1135 mA	
		ON	86 mA	379 mA	1100 mA	1100 mA	
	YES	OFF	93 mA	386 mA	1115 mA	1115 mA	
		ON	66 mA	359 mA	1080 mA	1080 mA	
24 h	NO	OFF	26 mA	173 mA	535 mA	535 mA	
		ON	NOT POSSIBLE	146 mA	500 mA	500 mA	
	YES	OFF	6 mA	153 mA	515 mA	515 mA	
		ON	NOT POSSIBLE	126 mA	480 mA	480 mA	
30 hours	NO	OFF	---	---	---	NOT PERMITTED	Only for JA-108K, Security Grade 3 profile
		ON	---	---	---	402 mA	
	YES	OFF	---	---	---	390 mA	
		ON	---	---	---	383 mA	
60 hours	NO	OFF	---	---	---	170 mA	Only for JA-108K, security grade 3 profile
		ON	---	---	---	135 mA	
	YES	OFF	---	---	---	160 mA	
		ON	---	---	---	125 mA	

Table 2 – Current consumption (backup) table

NOTE: Table 2 shows the maximum consumption from the control panel at maximum possible battery load; the control panel's own consumption is already included in the specified consumption.:

2.1.1 Mechanical dimensions

JA-103K
(268 x 225 x 83 mm)

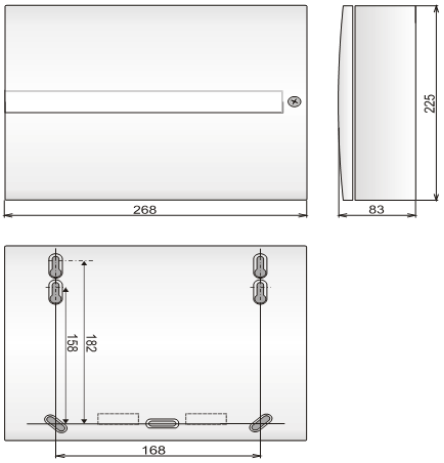


Figure 2 – JA-103K (dimensions)

JA-103K-7Ah, JA-107K and JA-108K
(357 x 297 x 105 mm.)

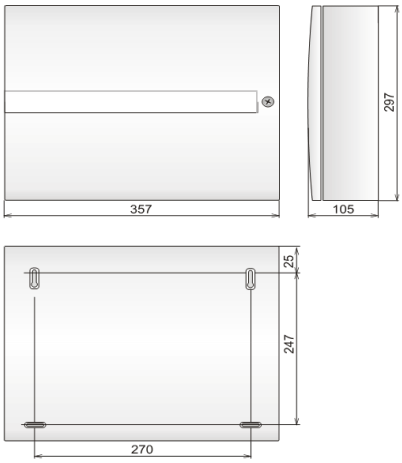


Figure 3 – JA-103K-7Ah, JA-107K and JA-108K (dimensions)

2.2 JA-103K

The JA-103K control panel is designed for small Bus systems (limited by the power and capacity of the backup power supply) and can be used for medium-sized systems communicating wirelessly (requires installation of the JA-11xR radio module).

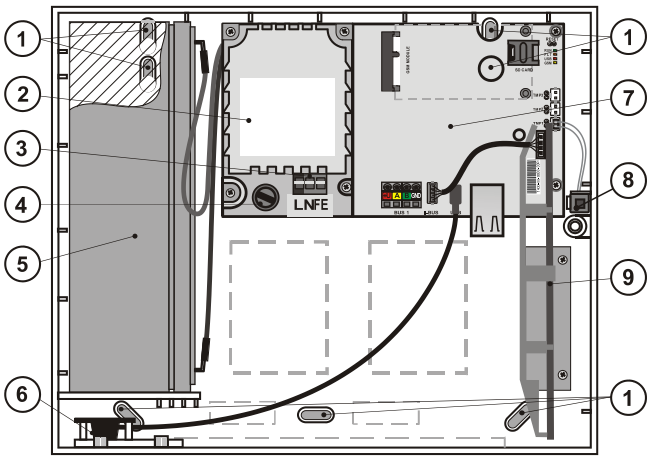
NOTE: Power and backup limits can be found in the chapter Technical specifications.

The control panel is equipped with a LAN communicator for connecting to the internet. It allows connection to the JABLOTRON cloud, establishing a connection to the ARC or remote management of the control panel using F-Link or JA-100-Link software. In addition to the LAN communicator, the control panel provides a slot for connecting an expansion GSM communicator from the JA-19xY series, which, depending on the type, can also provide voice and SMS services and extend the ARC connection with a backup channel.

Control panel expansion options (built-in):

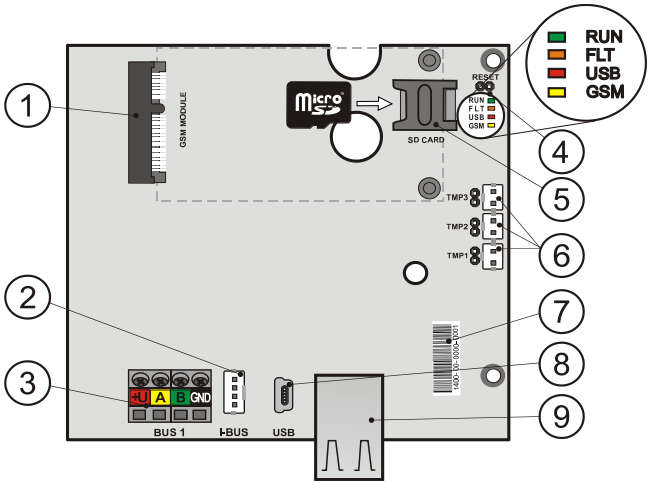
- 1x JA-11xR radio module
- JA-194Y or JA-194Y-LITE GSM communicator

NOTE: Modules are supplied separately or in pre-configure d sets. For more information about the current offer, please contact your distributor.



1 – holes for mounting the enclosure on the wall
2 – control panel power supply
3 – mains supply terminals
4 – fuse holder with replaceable mains fuse
5 – backup battery
6 – USB connector for connection to a PC
7 – control panel mainboard
8 – tamper switch of the housing
9 – holder for JA-11xR radio module

Figure 4 – JA-103K (component layout)



1 – connector for GSM communicator
2 – I-BUS connector for additional modules
3 – Bus terminal
4 – LED indicators and "RESET" jumper
5 – micro SD card holder (factory-fitted)
6 – connectors for control panel cover tamper switches
7 – Serial number label
8 – mini USB connector
9 – LAN connector

Figure 5 – JA–103K (PCB detail)

The control panel package includes:

1 USB cable (180 cm)
1 connecting cable for JA-11xR radio module

1 USB extension cable (20 cm) installed in the control panel
1 pcs Replacement fuse 5x20 mm (see 2.1)
4 pcs Short-circuit jumpers
6 pcs Warning stickers

4 x 8 mm dowels
4 x 40 mm cross-head screws
3 x 100 mm cable ties
1 x Abbreviated installation manual CZ
1 x Abbreviated installation manual EN

2.3 JA-103K-7Ah

The JA-103K-7Ah control panel is designed for medium-sized Bus systems (limited by the power and capacity of the backup power supply) and can be used for medium-sized systems communicating wirelessly (requires installation of the JA-11xR radio module).

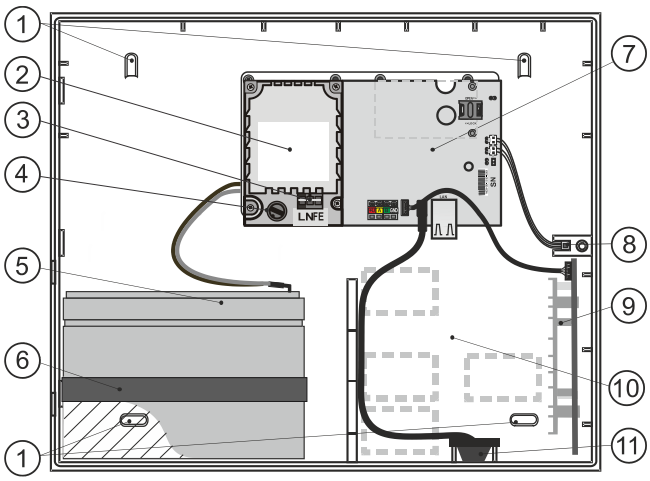
NOTE: Power and backup limits can be found in the chapter Technical specifications.

The control panel is equipped with a LAN communicator for connecting to the internet. It allows connection to the JABLOTRON cloud, establishing a connection to the ARC or remote management of the control panel using F-Link or JA-100-Link software. In addition to the LAN communicator, the control panel provides a slot for connecting an expansion GSM communicator from the JA-19xY series, which, depending on the type, can also provide voice and SMS services and extend the ARC connection with a backup channel.

Control panel expansion options (built-in):

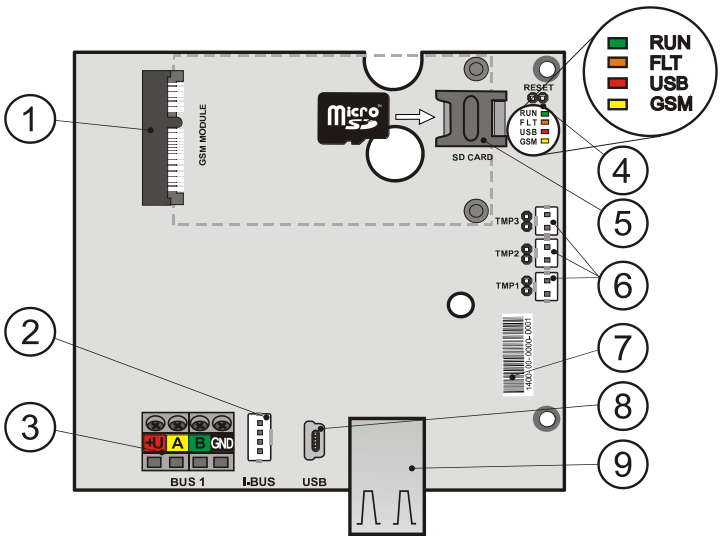
- 1x JA-11xR radio module
- JA-194Y or JA-194Y-LITE GSM communicator

NOTE: Modules are supplied separately or in pre-configure d sets. For more information about the current offer, please contact your distributor.



1 – holes for mounting the enclosure on the wall
2 – control panel power supply
3 – mains supply terminals
4 – fuse holder with replaceable mains fuse
5 – backup battery
6 – strap for attaching the backup battery
7 – control panel mainboard
8 – tamper switch of the housing
9 – holder for JA-11xR radio module
10 – space for cabling
11 – USB connector for connection to a PC

Figure 6 – JA–103K–7Ah (component layout)



1 – connector for GSM communicator
2 – I-BUS connector for additional modules
3 – Bus terminal
4 – LED indicators and „RESET" jumper
5 – micro SD card holder (factory-fitted)
6 – connectors for control panel cover tamper switches
7 – Serial number label
8 – mini USB connector
9 – LAN connector

Figure 7 – JA–103K–7Ah (PCB detail)

The control panel package includes:

1 USB cable (180 cm)
1 connecting cable for JA-11xR radio module
1 USB extension cable (20 cm) installed in the control panel
1 pcs Replacement fuse 5x20 mm (see 2.1)
4 pcs Shorting jumpers
6 pcs Warning stickers
4 x 8 mm dowels
4 x 40 mm cross-head screws
3 x 100 mm cable ties
1 x Abbreviated installation manual CZ
1 x Abbreviated installation manual EN

2.4 JA-107K

The JA-107K control panel is designed for medium to large Bus systems (limited by the power and capacity of the backup power supply) and can be used for medium to large systems communicating wirelessly (requires installation of the JA-11xR radio module).

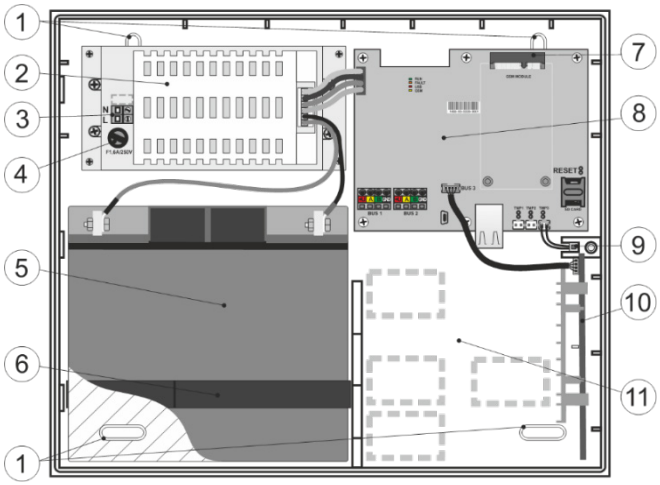
NOTE: Power and backup limits can be found in the chapter Technical specifications.

The control panel is equipped with a LAN communicator for connecting to the internet. It allows connection to the JABLOTRON Cloud, establishing a connection to an ARC or remote management of the control panel using F-Link or JA-100-Link software. In addition to the LAN communicator, the control panel provides a slot for connecting an expansion GSM communicator from the JA-19xY series, which, depending on the type, can also provide voice and SMS services and extend the ARC connection with a backup channel.

Control panel expansion options (built-in):

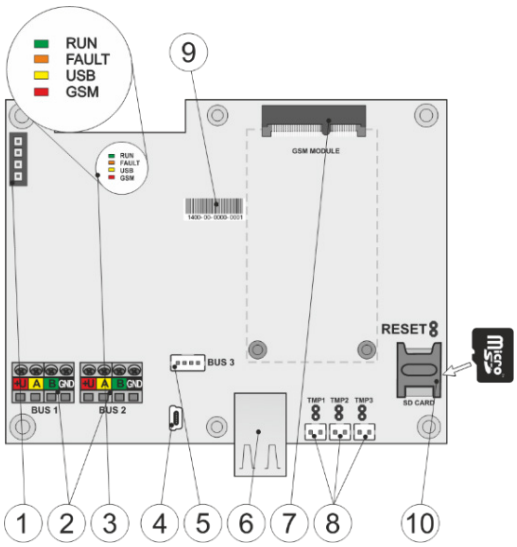
- 1x JA-11xR radio module
- JA-194Y or JA-194Y-LITE GSM communicator

NOTE: Modules are supplied separately or in pre-configure d sets. For more information about the current offer, please contact your distributor.



1 – holes for mounting the enclosure on the wall
2 – control panel power supply
3 – mains supply terminals
4 – fuse holder with replaceable mains fuse
5 – backup battery
6 – strap for attaching the backup battery
7 – GSM communicator connector
8 – control panel mainboard
9 – tamper switch of the housing
10 – JA-11xR radio module holder
11 – space for cabling

Figure 8 – JA–107K (component layout)



1 – power supply connector from the source
2 – two independent Bus terminals
3 – LED indicator
4 – mini USB connector
5 – connector for connecting a radio module or 3rd Bus
6 – LAN connector (Internet)
7 – connector for GSM communicator
8 – connectors for control panel cover tamper switches
9 – serial number label
10 – micro SD card holder (factory-installed)

Figure 9 – JA–107K (PCB detail)

The control panel package includes:

1 USB cable (180 cm)
1 connecting cable for JA-11xR radio module
1 USB extension cable (20 cm) installed in the control panel
1 pcs Replacement fuse 5x20 mm (see 2.1 Technical specifications)

4 pcs Shorting jumpers
6 pcs Warning stickers
4 pcs 8 mm dowels

4 x 40 mm cross-head screws
3 x 100 mm cable ties
2 x 3x8 mm screws
2 pcs Adapter for connecting faston connectors to the battery
1 x Abbreviated installation manual CZ
1 x Abbreviated installation manual EN

The JA-107K control panel can be powered from an external power supply that meets the requirements of EN 50131-6 in the supply voltage range of 10 to 15 V (DC) for use, for example, in stand-alone systems or in buildings without a permanent 230 V (AC) power supply. We recommend using VOD-JA-107K power cable to connect an external power supply. It consists of a conductor, a fuse holder with a fuse (F 6.3 A) and a connector.

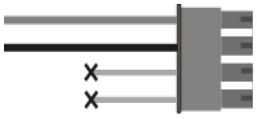


Figure 10 – VOD–JA107K (power cable)

2.5 JA-108K

The JA-108K control panel is designed for:

- Security grade 3 installations: small to medium-sized Bus systems (limited by the power and capacity of the backup power supply).
- Security grade 2 installations: medium to large Bus systems (limited by the power and capacity of the backup power supply) and can be used for medium to large systems communicating wirelessly (installation of the JA-11xR radio module required).

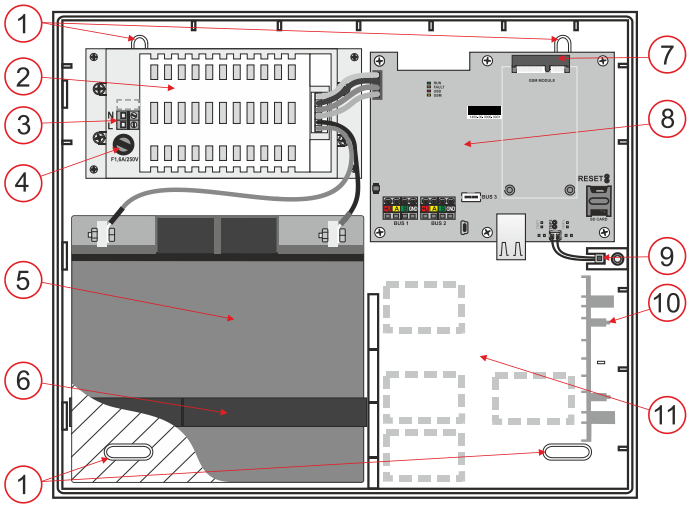
NOTE: Power and backup limits can be found in the chapter Technical specifications .

The control panel is equipped with a LAN communicator for connecting to the internet. It allows connection to the JABLOTRON cloud, establishing a connection to the ARC or remote management of the control panel using F-Link or JA-100-Link software. In addition to the LAN communicator, the control panel provides a slot for connecting an expansion GSM communicator from the JA-19xY series, which, depending on the type, can also provide voice and SMS services and extend the ARC connection with a backup channel.

Control panel expansion options (built-in):

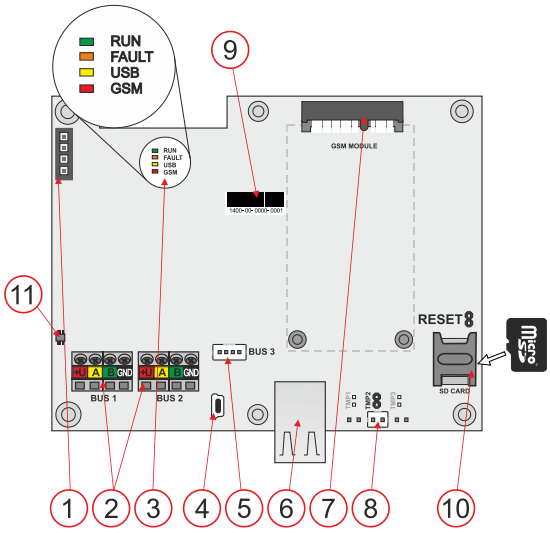
- JA-194Y or JA-194Y-LITE GSM communicator,
- 1x JA-11xR radio module (not supported in security grade 3 profile – does not meet security grade 3 requirements).

NOTE: Modules are supplied separately or in pre-configure d sets. For more information about the current offer, please contact your distributor.



1 – holes for mounting the enclosure on the wall
2 – control panel power supply
3 – mains supply terminals
4 – fuse holder with replaceable mains fuse
5 – backup battery
6 – strap for attaching the backup battery
7 – GSM communicator connector
8 – control panel mainboard
9 – tamper switch of the housing
10 – JA-11xR radio module holder
11 – space for cabling

Figure 11 – JA–108K (component layout)



1 – power supply connector
2 – two independent Bus terminals
3 – LED indicator
4 – mini USB connector
5 – connector for connecting a radio module or 3rd bus
6 – LAN connector (Internet)
7 – connector for GSM communicator
8 – tamper switch connector
9 – serial number label
10 – micro SD card holder (factory-installed)
11 – Hall probe for rear tamper protection

Figure 12 – JA–108K (PCB detail)

The control panel package includes:

1 USB cable (180 cm)
1 connecting cable for JA-11xR radio module
1 USB extension cable (20 cm) installed in the control panel
1 pcs Replacement fuse 5x20 mm (see2.1 Technical specifications)
4 pcs Shorting jumpers
6 pcs Warning stickers
4 pcs 8 mm dowels
4 x 40 mm cross-head screws
3 x 100 mm cable ties
2 x 3x8 mm screws
2 pcs Adapter for connecting faston connectors to the battery
1 x Abbreviated installation manual CZ
1 x Abbreviated installation manual EN

The JA-108K control panel allows power supply from an external power source that meets the requirements of EN 50131-6 with a supply voltage range of 10 to 15 V (DC) for use, for example, in stand-alone systems or in buildings without a permanent 230 V (AC) power supply. We recommend using the VOD-JA-107K power cable to connect an external power supply. It consists of a conductor, a fuse holder with a fuse (F 6.3 A) and a connector.

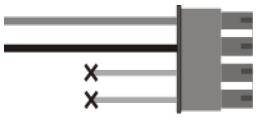


Figure 13 – VOD–JA107K (power cable)

2.6 Extension accessories for control panels

NOTE: Modules are supplied separately or in pre-configure d sets. For more information about the current offer, please contact your distributor.

2.6.1 JA-11xR radio module

The JA-11xR radio module is used to expand the control panel with the ability to communicate with JABLOTRON wireless devices. A connecting cable from the control panel package is required to install the module in the control panel.

To install the module outside the control panel, you will need the PLV-JA111R set, which is sold separately. The module enables:

- Operation of wireless detectors, keypads, sirens and other devices.
- Wireless firmware updates (only for selected devices, see the manual for details).
  - Use of up to three radio modules connected:
    - 1x internally in the control panel + 2x externally on the Bus, or
    - 3x externally on the Bus.
- The system automatically monitors RF communication quality and interference levels.

NOTE: The module is an optional accessory — it is not included in most control panels (it is only included in control panels marked "KR").

2.6.2 JA-19xY GSM communicators

JA-19xY series GSM/LTE communicators extend the control panel with mobile communication.

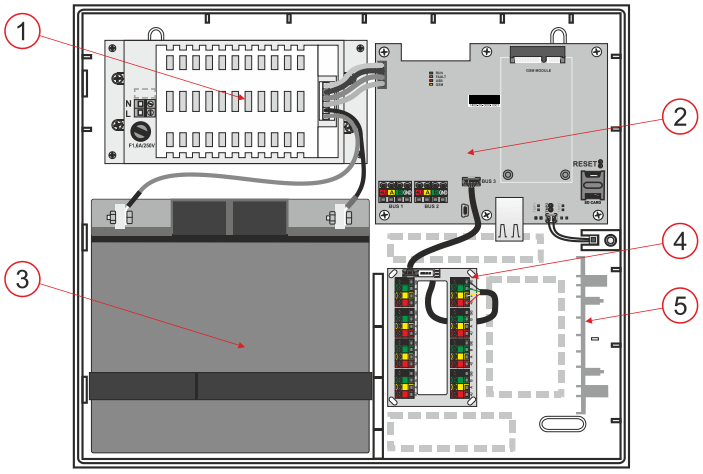
GSM Modules	GSM Technology	GSM Services	Notes
JA-192Y	2G	DATA, SMS, Voice calls	
JA-194Y	2G/3G/4G	DATA, SMS, Voice calls	
JA-194Y-LITE	2G/4G	Data services only with SDC	

Table 3 – GSM communicators

NOTE: The module is an optional accessory — it is not included in the control panel package.

For more information on the features and installation of the module, see the manual for each product, and for the configuration procedure, see the chapter 4.2.10 Communication.

2.6.3 JA-110Z-D Multi-position Bus splitter



1 – control panel power supply,
2 – control panel mainboard (PCB),
3 – backup battery,
4 – JA-110Z-D (multi-position Bus splitter),
5 – holder for JA-11xR radio module

Figure 14 – Control panel with Bus splitter

The JA-110Z-D is a Bus module designed for use with the JA-107K / JA-108K control panel, which allows the internal Bus connector to be extended to a third full-fledged Bus in the control panel while maintaining the connection of the JA-11xR radio module built into the control panel.

2.7 Common parts of control panels

The following description lists the common elements of the control panels. It includes indicator elements, connection terminals, connectors for modules and other components. The location of these parts can be found in the illustrations in the chapter 2.2 JA-103K, 2.3 JA-103K-7Ah, 2.4 JA-107K a 2.5 JA-108K.

The bag with the package insert, containing, for example, connecting jumpers, battery connectors, spare fuse, radio connection cable, etc., should not be discarded by the installer, but anything that is not used should be left inside the control panel or "in the bag". These components cannot be purchased separately and may be needed in the future.

The description of these elements serves as a quick reference for the installer during installation, diagnostics and system configuration. Detailed knowledge of the location and function of individual components is key to the correct connection of devices, evaluation of device status and safe servicing.

2.7.1 Control elements on the control panel

Reset jumper "RESET" – A two-pin connector on the board that allows you to reset the control panel to factory settings if the function is enabled. For detailed instructions, see Resetting the control panel Resetting the control panel.

4-pin "BUS" terminal – Depending on the type of control panel, one or two screw terminals are provided on the board for connecting the Bus line with devices. The terminal is colour-coded:

red *terminal +V / black terminal GND, green terminal DATA+ and yellow terminal DATB-*.

4-pin "I-BUS" connector for Bus connection (see Figure 14):

- for JA-103K and JA-103K-7Ah, this is an internal Bus designed EXCLUSIVELY for JA-11xR installed internally in the control panel (current limitation, see Technical specifications);
- JA-107K / JA-108K is a full-fledged third Bus, which can be equipped with a cable splitter using the JA-110Z-D expansion module while maintaining the internally connected JA-11xR module.JA-110Z-DJA-11xR.

Connectors "TMP1", "TMP2" and "TMP3", a – There are 3 connectors (inputs) on the control panel mainboard for connecting tamper switches (cover opening switch and wall tear-off switch). A jumper is included in the control panel package for each input, which allows the switch function to be bypassed.

NOTE: To meet the requirements of security grades 2 and 3 according to EN 50131 or T031, all tamper switches must be connected and the function activated by disconnecting the jumper.

Mains power terminals – Used to connect the mains power supply in the range of 110÷230 VAC. The terminal provides 3 terminals, one of which is blinded with a break-off cover. Two terminals are marked L (for phase conductor) and N (for working, neutral conductor). The third, blind terminal E is auxiliary and has no function of its own. It is intended for terminating the protective conductor if the cable is three-wire.÷

NOTE: The control panel is a Class II electrical device with double insulation, and a two-wire supply (phase and neutral wires) is required to connect the power supply.

WARNING: Always connect the mains power cable when the power is off, as there is a risk of injury and damage to the control panel.

Mini USB connector on the control panel mainboard – Used to configure the control panel and alarm system using PC and F-LINK software.

External USB connector – Connector accessible outside the control panel cover; the connector must be connected to the mini USB connector on the control panel mainboard using an internal cable.

WARNING: To meet the requirements of Security grade 2 and 3 according to EN 50131 or T031, the external USB connector must not be connected during operation, as this may compromise the security of the alarm system.

2.7.2 LED indicators on the control panel board

Each control panel has four LED status indicators:

LED indicator	Colour	Meaning
RUN	Green	Fast flashing indicates communication Bus operation (data flow)
FAULT	Yellow	Indicates a general fault in the system (more information will be provided by F-Link or the keypad with display)
USB	Yellow	Indicates a USB connection to a computer
GSM	Red	If the JA-19xY GSM communicator is installed: ■ It lights up after connecting the power supply when searching for a GSM network. ■ It does not light up if the GSM is working properly and no communication is currently taking place. ■ It flashes at a frequency of 0.5 s / 0.5 s if the GSM network is not available. ■ It flashes at a frequency of 0.5 s / 0.5 s when connecting to GSM communication. ■ A short flash indicates that the GSM communicator parameter is set to off.

Table 4 – LED indicators on the control panel

2.7.3 Micro SD card

Each control panel is factory-equipped with a microSD card, which serves as internal storage for files:

- FLEXI_CFG, contains the system configuration (not intended for manipulation);
- FLEXI_LOG, stores events and photos from camera detectors;
- system sounds and text files;
- also used to upload new control panel firmware for update purposes.

NOTICE: The SD card must be inserted in the control panel for proper operation.

WARNING: When replacing the card, it is necessary to perform a factory reset and subsequent firmware update in order to upload the necessary system files to the card.

NOTICE for JA-103K, JA-107K: Resetting the control panel does not delete the data stored on the card (PHOTO folder, FLEXILOG.TXT) – see 6.2.1 Resetting the Control Panel for instructions.

2.7.4 Control panel Bus

The JABLOTRON system Bus is a four-wire Bus, colour-coded and used exclusively for JABLOTRON devices. The Bus is a proprietary RS-485 standard solution.

WARNING: The Bus must not be used to power other devices without a Bus separator, or led outside the protected premises.

The galvanically isolated JA-121T converter is used to connect the Bus to other systems (for example smart home automations).

There is also the JA-110T module and its only functions as a separator, preventing short-circuiting of the Bus in front of it. It is only used if the Bus leaves the protected area or if non-alarm JABLOTRON elements without TMP (thermostats, multifunction relays, etc.) are connected to it. Furthermore, the JA-110T does not allow the connection of, for example, a smart home. It is also not possible to connect two JA-110T products in series (an addressable device must always be connected between them).

Terminal	Colour	Note
+U	red	positive power supply pole – can only be used to power JABLOTRON 100 series devices (Jx-1xxX)
A	yellow	data A
B	green	data B
GND	GND	znegative power supply terminal

Table 5 – Bus terminal description

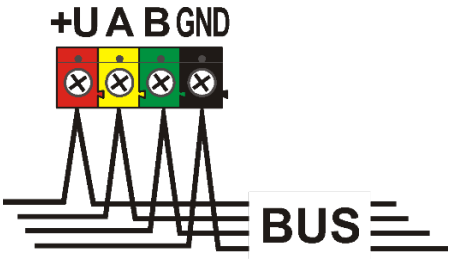


Figure 15 – Bus

2.7.4.1 Bus length and number of connected devices

The maximum length of a single Bus output without additional amplification (separation) is 500 m and is determined by the sum of the lengths of all cables between the connected devices.

NOTE: The JA-107K control panel has up to 3 separate Bus branches and can therefore have 3x500 m of Bus.

There can be a maximum of 60 addressable devices on one Bus *(within these 60 devices, it is not recommended that the total number of keypads/readers and Photo-PIR detectors exceed 10. Transferring images or active authorisation to more than 10 of these devices at once will cause Bus instability).*

If more than 60 devices need to be used on one Bus, it is necessary to use the JA-120Z Bus booster.

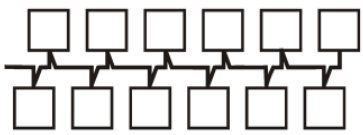
The number of connected Bus devices is limited by the capacity of the control panel's backup battery. In order for the system to meet the standard for security grade 2, it must operate reliably from the backup power supply for at least 12 hours in the event of a 230 V mains failure. The total consumption of all Bus devices must therefore not exceed the maximum continuous current consumption of the control panel, see Technical specifications.

Another limit determining the maximum Bus length may be the voltage drop on the line (clearly displayed by System Diagnostics in the F-Link software).

2.7.4.2 Bus arrangement, branching

When connecting individual system devices – detectors, keypads, sirens, output modules, etc. – it is possible to route the Bus cable as short as possible, regardless of which sections of the system the devices belong to. The Bus can be branched as needed. A linear, radial or tree structure is possible. In actual installations, the most optimal option is usually a combination of these three possibilities.

E**xamples of possible Bus connection arrangements:**



Fugure16 – Linear Bus

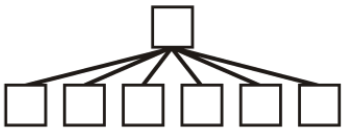


Figure 17 – Star Bus structure

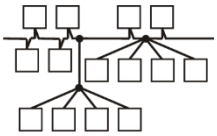


Figure 18 – Combined Bus structure.

WARNING: The Bus cable must not be connected in such a way that a closed loop is created on any conductor (the ends of individual branches must never be connected to each other; the common GND conductor must not be connected either). Furthermore, it is not recommended to connect too many devices in line, as damage to the cabling could cause a large part of the system to malfunction. It is ideal to divide the installation into several smaller branches leading to the control panel.

The JA-110Z bus splitter can be used for branching and branching the Bus. It is manufactured in four versions: JA-110Z, JA-110Z-B, JA-110Z-C, and JA-110Z-D. The JA-110Z is supplied in a surface-mounted installation box and is equipped with front and rear tamper contacts to prevent unauthorised manipulation. It occupies one position in the system. Terminals of the same colour are always connected on the hubs. Variants A and B are dimensioned for installation in the JA-190PL multi-purpose mounting box. Variant C is dimensioned for installation in the KU-68 standard electrical installation box.

2.8 Functional characteristics of the system

This chapter describes the logical and functional behaviour of the JABLOTRON security system at the control panel level. It focuses on the principles according to which the system operates, how the individual parts of the monitored object are controlled and how the control panel evaluates user actions, alarm states and operating situations.

This section also provides the installation technician with a comprehensive overview of how the system interprets inputsfrom devices, what output responses it generates, and what options it offers for adapting the control panel's behaviour to a specific installation.

2.8.1 System profiles

Selecting a system profile allows you to set parameters in bulk so that the entire system behaves according to the selected scheme, such as the selected standard, and thus meets the requirements for the relevant classification.

The JA-103K, JA-103K-7Ah and JA-107K control panels of the JABLOTRON system allow you to set the profile:

- **Default** (allows you to completely configure the system to its full extent, preset by default at the factory).
  - **EN 50131, Security Grade 2** (intended for installations requiring EN 50131 certification of components in security grade 2).
- **Grade 2 INCERT** (intended for installations requiring INCERT component certification – Belgium).
- **Larmklass II/R SSF 1014** (intended for installations requiring SSF 1014 certification of components with Larmklass II or R classification – Sweden).

The JA-108K control panel of the JABLOTRON system allows you to set the profile:

- **EN 50131, Security Grade 3** (designed for installations requiring EN 50131 component certification in security grade 3).
- EN 50131, Security Grade 2 (intended for installations requiring EN 50131 certification of components in security grade 2).
- Default (allows you to completely configure the system to its full extent, preset by default at the factory).

A description of the presets can be found in the table (see Table 6), values with change restrictions are highlighted in grey.

WARNING: Selecting a "certified" profile in the system does not guarantee that the entire security system installation complies with it. This level of security must also be ensured by the correct design of the system, its proper installation and configuration of operating modes in accordance with the guidelines of EN 50131-1, CLC/TS 50131-7 and connection to the Alarm Receiving Centre (ARC) service.

WARNING: Selecting the "Default" profile will restore the settings of the specified parameters to factory defaults and unlock options for unrestricted changes. The system will no longer meet the declared properties of the certified profile, which may result in a breach of insurance company or local regulations. In the event of a loss event, the insurance company may not pay the insurance due to a breach of requirements caused by incorrect settings of the security system by the installation company.

Devices	Parameter name	Default (factory default)	Grade 2 EN 50131	Grade 3 EN 50131	Grade 2 INCERT	(LARMKLASS II/R) SSF 1014	Compulsory
Control panel	Codes with prefix	no	yes	yes	yes	yes	Yes
Control panel	Enable EM UNIQUE 125kHz standard cards	Yes	Yes	Yes	Yes	Yes	Yes
Control panel	Code length	4 (4, 6, 8)	4	6	4	4	4 (4, 6, 8)
Control panel	Automatically check time in the connected PC	Yes	Yes	Yes	Yes	Yes	Yes
Control panel	Sirens when partially set	No	No	No	no	no	no
Control panel	Sirens enabled	Yes	yes	Yes	Yes	yes	Yes
Control panel	Warning about default codes	Yes	Yes	Yes	Yes	yes	Yes
Control panel	Administrator restricted service and ARC rights	No	Yes	Yes	yes	yes	No
Control panel	Service and ARC controls the system	Yes	No	No	No	No	yes
Control panel	Trial operation	no	No	No	No	no	no
Control panel	Service requirement	No	No	No	No	no	no

Devices	Parameter name	Default (factory default)	Grade 2 EN 50131	Grade 3 EN 50131	Grade 2 INCERT	(LARMKLASS II/R) SSF 1014	Compulsory
Control panel	Maintenance mode allowed	Yes	no	No	No	No	no
Control panel	Duress access control	yes	yes	Yes	Yes	yes	Yes
Control panel	Alarm confirmation within one section	No	No	No	no	no	no
Control panel	Siren(IW output) when tamper is triggered	no	yes	Yes	yes	yes	Yes
Control panel	Tamper alarm indication reset by Service	No	Yes	Yes	yes	yes	No
Control panel	Reset enabled	Yes	no	No	No	No	no
Control panel	Daily reset of device autobypass	yes	no	No	No	No	no
Control panel	Blocking when setting	no	yes	Yes	yes	yes	Yes
Control panel	Unsetting cancels the alarm	No	Yes	Yes	yes	yes	Yes
Control panel	Unsuccessful setting	No	Yes	yes	yes	yes	not applicable
Control panel	Fault autobypass	Yes	Yes	Yes	Yes	Yes	Yes
Control panel	System profiles	Default	EN50131-1, Grade 2	Compliant with EN50131-1, Grade 3	Incert, Grade 2	SSF 1014	Zwangsläufigkeit
Control panel	On F-Link start , automatically open the connected control panel	No	No	No	No	no	no
Control panel	Entering Service mode automatically	No	No	No	No	no	no
Control panel	Detector with Dlay C reaction extended exit	no	no	No	no	no	not applicable
Control panel	Delayed reporting to the ARC	no	yes	yes	yes	not applicable	no
Control panel	Ways of setting	Set with warning	According to system profile	According to system profile	According to system profile	According to system profile	Vds 2252
Control panel	Authorisation type	Standard	Standard	Standard	Standard	Standard	Standard
Control panel	System blocking by alarm	No	No	No	No	No	No
Control panel	Loss of a Bus device	Fault	Tamper always	Tamper always	Tamper always	Tamper always	Tamper after confirmation
Control panel	Device auto-bypass	3rd activation	3rd activation	3rd activation	3rd activation	3rd activation	3rd activation
Control panel	Alarm length	900 s (5÷1200 s)	900 s (5÷900 s)	900 s (90÷900 s)	900 s (90÷900 s)	900 s (5÷900 s)	900 s (5÷1200 s)
Control panel	Entry delay A	5 s (5÷120 s)	5 s (5÷30 s)	5 s (5÷30 s)	5 s (5÷30 s)	5 s (5÷30 s)	Not applicable
Control panel	Entry delay B	5 s (5÷120 s)	5 s (5÷60 s)	5 s (5÷30 s)	5 s (5÷60 s)	5 s (5÷30 s)	Not applicable
Control panel	Entry delay C	30 s (5÷360 s)	30 s	30 s	30 s	30 s	Not applicable
Control panel	Exit delay A	5 s (5÷120 s)	5 s (5÷60 s)	5 s (5÷60 s)	5 s (5÷60 s)	5 s (5÷60 s)	Not applicable
Control panel	Exit delay B	5 s (5÷120 s)	5 s (5÷60 s)	5 s (5÷60 s)	5 s (5÷60 s)	5 s (5÷60 s)	Not applicable
Control panel	Exit delay C	60 s (5÷360 s)	60 s	60 s	60 s	60 s	Not applicable
Control panel	Period of waiting for alarm confirmation	10 min (1÷60 min)	10 min	10 min	10 min	10 min	10 min

Devices	Parameter name	Default (factory default)	Grade 2 EN 50131	Grade 3 EN 50131	Grade 2 INCERT	(LARMKLASS II/R) SSF 1014	Compulsory
Control panel	Waiting for fire confirmation	10 min (1÷60 min)	10 min	10 min	10 min	10 min	10 min
Control panel	Period of waiting for repeated activation	30 s (11÷120 s)	30 s	30 s	30 s	30 s	30 s
Control panel	Triggered- detector blanking time	10 s (5÷60 s)	10	10 s	10 s	10 s	10 s
Control panel	Report unset section	5 min (5÷2880 min)	5 min (5÷2880 min)	5 min (5÷2880 min)	5 min (5÷2880 min)	5 min (5÷2880 min)	1 min
Control panel	Automatic setting	60 min (5÷2880 min)	0 min	0 min	0 min	0 min	Not applicable
Control panel	Maximum exit time extension	3 min	3 min	3 min	3 min	3 min	Not applicable
Control panel	Blocking authorisation when invalid authorisation is entered	No	No	10 attempts and then every single attempt Duration 90 s	No	No	No
Control panel	Tamper alarm when invalid authorisation	Off / After 10 attempts	After 10 attempts	On the 21st attempt (10 ÷ 21) / Off	After 10 attempts	After the 10th attempt	After the 10th attempt
Radio	Communication indicated by LED	Yes	Yes	Not permitted	Yes	Yes	yes
Radio	Interference detection	Low	Low	Not permitted	Low	Low	Low
Keypad	Optical indication settings	2. By changing the section status (Bus) or 4. By changing the segment status (RF)	2. By changing the status of the section (Bus) or 4. Changing the segment status (RF)	2. By changing the section status (Bus)	2. Changing the section status (Bus) or 4. Changing the status of the segment (RF)	2. Change in section status (Bus) or 4. Changing the status of the segment (RF)	1. Permanently (Bus) or 4. Changing the segment status (RF)
Keypad	Indicates Unset status	no	no	No	no	no	yes
Keyboard	Indicates Set status	no	No	No	no	no	yes
Keypad	Alarm acoustic indication	yes	Yes	Yes	Yes	Yes	Yes
Keyboard	Entry delay acoustic indication	Yes	Yes	Always at full volume	Yes	Yes	Yes
Keypad	Exit delay acoustic indication	Yes	Yes	Always	Yes	Yes	Yes
Remote controls	Control function restrictions	no	no	not applicable	no	no	no
Control panelcalendar	Control function restrictions	No	No	No	No	No	no

Table 6 – Description of system presets by profile

2.8.1.1 Overview of surmountable and insurmountable causes preventing security

When selecting a system configuration profile in the control panel (Default, EN 50131 Security Grade 2, Incert Grade 2, LARMKLASS II/R SSF 1014, Zwangsläufigkeit, EN 50131 Security Grade 3), conditions are pre-set that may prevent the system from being set. These conditions can be user-surmonutable (system is set) or insurmountable (system remains unset), or they can be automatically surmountable (user participation is not required). The Table 7 shows whether it is possible to overcome an active event for system profiles or whether it prevents the user from setting the system.

Event	Default	Grade 2 EN 50131	Grade 3 EN 50131	(Grade 2) INCERT	(LARMKLASS II/R) SSF 1014
Active tamper	YES	YES	YES	NO	NO
Active input (any input)	YES	YES	YES	YES	YES
Active instant input	YES	YES	YES	YES	YES
Active alarm memory indication	NO	YES	YES	NO	NO
RF 20 minutes no response	YES	YES	YES	YES	YES
Siren fault	YES	NO	NO	NO	NO
Fault	YES	YES	YES	NO	NO
Loss of device	YES	YES	YES	NO	NO
Blocked detectors	YES	YES	YES	NO	YES
Low battery in device	YES	YES	YES	NO	NO
Control panel battery discharged	YES	YES	YES	NO	NO
Faulty control panel battery	YES	NO	NO	NO	NO
Control panel mains power failure – AC fault	YES	YES	YES	YES	YES
AC fault for 30 minutes	YES	YES	YES	NO	NO
System in configuration	NO	NO	NO	NO	NO
GSM fault	YES	YES	YES	NO	NO
LAN failure	YES	YES	YES	NO	NO
PSTN fault	YES	YES	YES	NO	NO
Failure of all ARCs	NO	NO	NO	NO	NO

Table 7 – Causes preventing security

2.8.2 Control panel operating modes

The JABLOTRON security system has several operating modes. The authorisation to switch between individual modes is determined by the user authorisation settings, see 2.8.3 User authorisation.

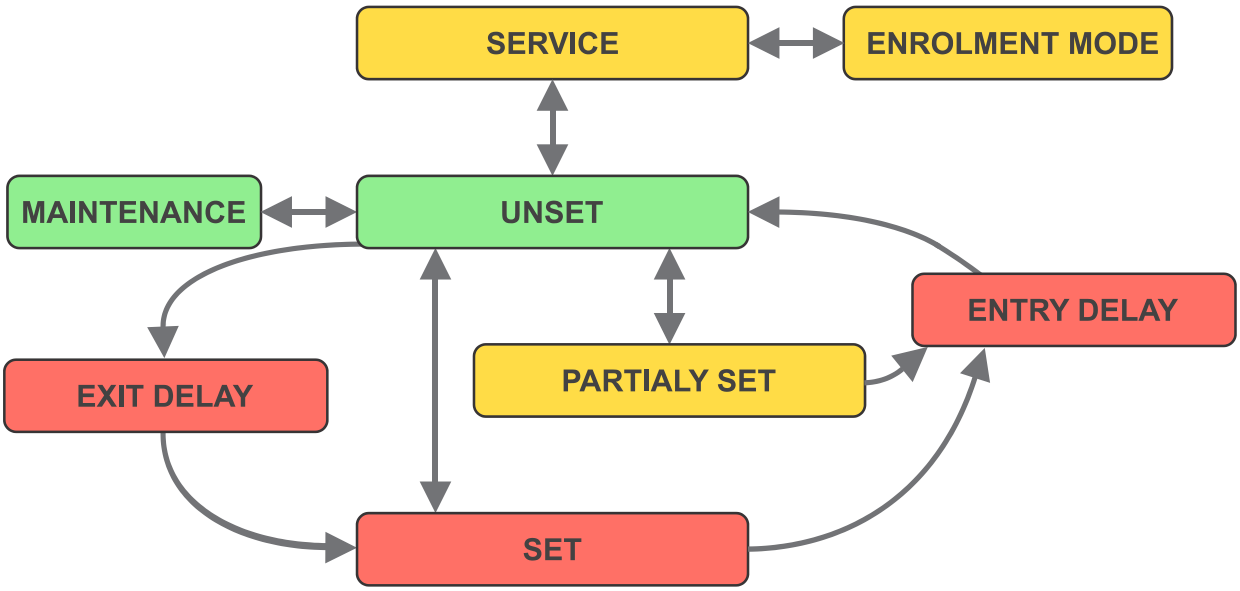


Figure 19 – Control panel operating modes

Operating mode	Description	Control and PG	Activation button	Segment
Service	Mode intended exclusively for service or ARC technicians. Used to add (teach) new devices and configure and diagnose the system. You can enter or exit Service mode from the LCD keypad or from the F-Link software on your computer. NOTE: If a computer is connected, you cannot open or exit SERVICE mode from the keypad.	It can be controlled manually from F-Link using the TEST button.	FLASH YELLOW 2x / 2 s	OFF ALL
Enrollment mode	Mode for assigning new devices to the system. Access is only possible from Service Mode and via F-Link software.	NOT PERMITTED (Locally and remotely)	FLASH YELLOW 2x / 2 s (= SERVICE status)	OFF ALL
Maintenance	Mode intended only for the Administrator. Allows maintenance to be performed in the section(s) for which the Administrator has authorisation (e.g. replacing batteries in detectors). Maintenance can be entered or exited from the LCD keypad or from the JA-100-Link (F-Link) computer software. Maintenance in a given section does not affect the status and functionality of other sections or the status of PG outputs.	ACTIVE except for the section under maintenance.	FLASHING GREEN 2x / 2 s	OFF ACCORDING TO SECTION
Unset	Operating mode in which burglar detectors are not set and it is possible to move freely in the unset object (section), open doors, windows, etc. Smoke and temperature detectors, gas leak detectors, flood detectors or emergency buttons can trigger an alarm (depending on the system configuration). Tamper protection of the control panel and each device is active, and a tamper alarm is triggered if they are tampered with.	ACTIVE	ON *) GREEN	ON *) GREEN
Exit delay	Time-limited operating mode after starting the process leading to system setting. The user must leave the building within the specified time. The system status Set, , is completed at the end of the time delay if: ■ no detector with an instant reaction has been activated in the building during this time; or ■ no detector is active at the end of the exit delay; then an alarm is triggered.	ACTIVE	PERMANENT LIGHT RED	PERMANENTLY ON RED
Set	All detectors in the building are active and monitoring. In the event of a intrusion, 2.8.6) or activate a mode according to the programmed reaction (e.g. entry delay).	ACTIVE **)	ON *) RED	ON *) RED
Entry delay	A mode in which the system, after activating a delayed reaction detector, provides time for unsetting, according to the pre-set entry delay length. If it is not disarmed in time or an instant detector is activated, an alarm is triggered.	ACTIVE	FLASHING RED FAST	FLASHING *) RED FAST
Partially set	Detectors programmed to protect the perimeter are active and monitoring (i.e. except for internal detectors). In the event of a intrusion, they trigger an alarm in the system (see 2.8.6).			

NOTE:

*) Depending on the settings, this indication may be time-limited. User authorisation may be required for further display.

**) Depending on the system settings, system control may be restricted by the "Blocking after alarm" function. The system requires a special code to be used for unblocking, after which the system can be unset. The blocking after alarm function is mainly used to secure forensic evidence after an intrusion of the premises.

Table 8 – control panel operating modes

2.8.3 User authorisation

Each system user must be assigned authorisation to operate or configure the system or its sections.

The types of authorisation and their basic description are listed in the table below (see Table 9).

Two users are pre-set at the factory:

- User in position 0 with Service authorisation, also referred to as the main service user.
- User in position 1 with Administrator authorisation, also referred to as the Main Administrator.

To create, edit, and delete additional users and to set their permissions, you must use F-Link or JA-100-Link software.

Permissions	Description
Guard code	Permission designated for security services. The number of users with Guard Codes permission is not limited in the system. Users with this permission cannot change the code. ■ Users with this authorisation: ■ can set the entire system; ■ can unset the system if there is an alarm in the system (alarm memory is signalled); ■ cannot delete the alarm memory.
Panic	Permission only for triggereing a "Panic" event. The number of users with Panici permission is not limited. Users with this permission cannot change the code or clear the alarm memory.
PG only	Permission only to control programmable (PG) outputs requiring authorisation. The number of users with Only PG permission is not limited. Users with this permission cannot change the code. Users with this permission can switch PG outputs to which they have been granted access on and off.
Set	Permission to set a section. The number of users with Set permission is not limited. Users with this permission cannot change the code. ■ Users with this permission: ■ can only set the section to which they have been granted access; ■ can switch PG outputs on and off to which they have been granted access; ■ cannot delete the alarm memory.
User	Permissions designated for controlling the system and PG outputs within the scope assigned by the Administrator. The number of users with User permissions is not limited. ■ A user with this authorisation: ■ can add and delete assigned chips/cards and change their own telephone number; can change their code when setting up the system with a prefix; can delete the alarm memory in the assigned sections. The administrator can restrict the user's access to sections for a limited time.
Administrator (main, position 1)	Permissions for controlling the system and PG outputs and performing maintenance activities throughout the entire system. The number of users with main Administrator permissions (position 1) is limited. There can only be one main Administrator in the system; they cannot be deleted and are factory set to the code 1234, which must be changed before the system is put into operation. ■ A user with this authorisation: ■ can control all sections; ■ can turn all PG outputs on and off; ■ can create, delete, turn off and turn on other Administrators (from position 2 onwards) and edit their permissions for system administration and add codes and chips/cards to them; ■ can create, delete, switch off and switch on other users with lower permissions (from position 2 onwards) and edit their permissions for controlling the system and PG outputs and add them codes and chips/cards; ■ can delete the alarm memory; ■ can perform maintenance in Maintenance mode; ■ when the "Administrator restricts Service and ARC" function is enabled, the Administrator must confirm each attempt to authorise a user with Service or ARC permissions with their own authorisation, otherwise access is not permitted.

Permissions	Description
Administrator (other)	Permissions for controlling sections and PG outputs and performing activities in maintenance mode within the scope of the system to which they have been granted access by the main Administrator. The number of users with additional Administrator permissions (from position 2 onwards) is not limited. ■ Users with this authorisation: ■ can control sections to which they have been granted access by the main Administrator; ■ can switch PG outputs on and off to which they have been granted access by the main Administrator; ■ can create, delete, disable, and enable users with the same or lower permissions and edit ■ their permissions to control those sections for which they have been granted permissions by the main Administrator and addthem codes and chips/cards; ■ can delete the alarm memory in sections to which they have been granted access by the main Administrator; ■ can perform maintenance in Maintenance mode in sections to which the main administrator has granted them access.
Service	Authorisation designated for performing service activities, allows access to Service mode and full system configuration, except for ARC settings, which may be restricted by a user with ARC authorisation. The number of users with Service authorisation is not limited, and Service user in position 0 cannot be removed. The factory default code is 1010, which must be changed before the system is put into operation. ■ A user with this authorisation: ■ can control all sections; ■ can switch PG outputs on and off; ■ can create, delete, and switch on and off users with Service and ARC authorisation and other users with lower authorisation, edit their authorisation for sections and PG outputs, and add them a code ■ and chips/cards; ■ can delete the alarm memory, including tamper alarms; ■ when the "Administrator restricts Service and ARC" function is enabled, the Administrator must confirm each attempt to authorise a user with Service authorisation with their own authorisation, otherwise access is not granted to users with Service authorisation.
Unblocking	Authorisation intended exclusively for unblocking the control of a system that has been blocked by an alarm (optional function). The number of users with this authorisation is not limited. Users with this authorisation have no other authorisations.
ARC	Permission intended for Alarm Receiving Centre operators and emergency services. The number of users with ARC permission is not limited. ■ Users with this authorisation: ■ has the highest authorisation for all system configuration changes in Service mode (more than Service); can restrict users with Service authorisation from changing the ARC configuration settings; ■ can unblock system control that has been blocked by an alarm (optional function). ■ can delete the alarm memory, including tamper alarms; ■ can create, delete, enable and disable users with Service, ARC and other lower permissions, edit their permissions for sections and PG outputs, and add them codes and chips/cards; ■ When the "Administrator restricts Service and ARC" function is enabled, the Administrator must confirm each attempt to authorise a user with ARC rights with their own authorisation, otherwise access is not permitted to users with ARC rights. ■ When the "Administrator restricts Service and ARC" function is enabled, this user cannot control sections and PG outputs.

Table 9 –User authorisationss

2.8.4 JABLOTRON system authorisation means

The JABLOTRON system allows users to authorise themselves using:

- access codes;
- chips and cards;
- remote controllers;
- MyJABLOTRON or MyCOMPANY cloud applications;
- F-Link and JA-100-Link software.

The availability of these authorisation methods depends on the choice of operating profile, control devices (keypads, readers, etc.) and the availability of JABLOTRON cloud services.

2.8.4.1 Access codes

An access code is a basic authorisation means that allows the user, within the scope of their authorisation, to access the functions and information of the alarm system via the keypad, MyJABLOTRON and MyCOMPANY smart applications, F-Link and JA-100-Link software, or via SMS and voice services over GSM communication.

The system supports multi-digit codes (4-, 6- and 8-digit codes) in two modes:

- **Code with prefix** (higher security, larger code/user range);
- **Code without prefix** (security is determined only by the length of the code, smaller range of available codes/user).

Code size	Code format without prefix:	Code format with prefix:
4-digit code:	**kkkk**	**ppp * kkkk**
6-digit code:	**kkkkkk**	**ppp * kkkkkk**
8-digit code:	**Kkkkkkkk**	**ppp * kkkkkkkk**

Legend:
- **- kkkk...** numerical code;
- **- ppp** is the prefix, identical to the user number (0 to 600), according to the position in F-Link / JA-100-Link on the Users tab;
- **-** is an asterisk character, used as a separator between the prefix and the code.

Table 10 – Access codes

Code format for duress access control:

A special code for users in danger, which allows them to control (set or unset) the system and trigger a silent panic alarm without any visual or audible signalling.

The code consists of the normal user code with the number "1" added to the last digit of the code. The function is supported for codes with and without a prefix. If the user code ends with the number 9, then for duress access control,

-0 is used for the last digit of the code.

The code setting for control under duress is optional and is enabled by default.

EXAMPLE:

Authorisation type	Code case	Code	Code under duress
No prefix	Regular code	4444	4445
	Code ending in 9	6789	6780
With prefix	Standard code	5*4444	5*4445
	Code ending in 9	6*6789	6*6780

Table 11 – Duress access control (codes)

WARNING: When the Code with Prefix function is turned off, the codes are always reset to their factory settings, and all access codes are deleted (cards and chips remain with users). When the Prefix is turned on, all codes and chips remain set and only prefixes are added. Furthermore, for codes without a prefix, only the administrator or service technician can change user codes.

The calculation of code combinations according to the parameter settings for 1 user is shown in the following Table 12:

Control panel configuration	4-digit	6-digit	8-digit
"Codes with prefix"	= 104 = (10,000)	= 106 = (1,000,000)	= 108 = (100,000,000)
"Codes without prefix"	= 104 – (Number of users in the system – 1)	= 106 – (Number of users in the system – 1)	= 108 – (Number of users used in the system – 1)
"Codes without prefix" and the "Duress access control" parameter enabled	≤ 104 – ((Number of users used in the system – 1) * 3)	≤ 106 – ((Number of users used in the system – 1) * 3)	≤ 108 – ((Number of users in the system – 1) * 3)
NOTE: When using the "Prefixed codes" parameter setting, the control panel allows the use of any numerical code combination for each user (the prefix distinguishes users with codes of the same value) EXAMPLE: Using a standard four-digit access code with the "Codes with prefix" function enabled, a value of 104 (10,000) code combinations is achieved for each user.			

Table 12 – Access code combinations

NOTE: Disabling the prefix function reduces the number of usable code combinations as the number of users increases, and is also significantly reduced by using the "Duress acces control" function, which adds a second code to each user (i.e. if one user has the code 1111, the system will not allow the second user to enter the code 1112, as this is the code for duress access control).

2.8.4.1.1 Use of invalid codes

The system responds to the entry of invalid codes. The control panel counts the entry of invalid codes from any keypad.

NOTE: The counter for incorrectly entered codes is preset and cannot be changed.

If the user (or intruder) enters the code incorrectly 10 times:

- a tampering event "Code entry attempts exceeded" is generated;";
- a tampering alarm is triggered;
- a message is sent to the ARC "Code entry attempts exceeded";
- A report is sent to the set telephone numbers in the form of an SMS or to the MyJABLOTRON and MyCOMPANY application;

Furthermore, for control panels programmed to security grade 3:

- all input devices are blocked after the tenth attempt (keypads, card readers and SW F-Link/JA-100-Link) for 90 seconds;
- after the blocking period has expired, each subsequent attempt with an invalid code triggers all messages and block the input devices for another 90 seconds.

When a valid code is entered, the recorded incorrect code attempts are deleted and the current alarm is immediately terminated.

2.8.4.1.2 Factory default codes

The table (see Table 13) lists the factory codes for users with Service and Administrator authorisation. The codes are filled in automatically by the F-Link software, so they are not required from the first start-up until the codes are changed.

WARNING: These codes must be changed when a user with Service authorisation logs in for the first time, otherwise it will not be possible to exit Service mode.

Code type	Administrator		Service	
	No prefix	With prefix	Without prefix	With prefix
4-digit codes	1234	1*1234	1010	0*1010
6-digit codes	123456	1*123456	1010	0*101010
8-digit codes	12345678	1*12345678	101010	0*10101010

Table 13 – Factory default codes

2.8.4.2 Changing access codes

When the Codes with prefix parameter is enabled, each user with User authorisation for whom the administrator has pre-set the Allow code change parameter has the option to change their own code (only the "Default" system profile; for security levels 2 and 3, the system sets this automatically).

When the Codes with prefix parameter is disabled, users cannot have the same codes, even not codes for duress access control. The control panel does not allow another user to enter a code that has already been used or a duress access code , so in these cases, entering new codes or changing existing codes for any user is the sole responsibility of the system administrator(s).

Access codes can be changed using:

- LCD keypad (the computer must be disconnected, both locally and remotely);
- JA-100-Link software (user/administrator), which is available on the control panel's disk drive (displayed after connecting the USB cable);
- SW F-Link (service technician), which can be downloaded from MyCOMPANY;
- MyJABLOTRON mobile application (from version 3.5).

2.8.4.3 RFID cards and chips

NOTE: The EN 50131 Security Grade 3 profile does not support RFID technology.

JABLOTRON systems support two types of RFID technology:

- EM UNIQUE 125 kHz;
- MIFARE Classic.

The availability of these technologies depends on the selection of control devices (keypads, card readers).

Control panel parameters	EM UNIQUE 125 kHz	MIFARE Classic
Range of JA card and the JA-19xJ chip ID codes	= 108 = (100,000,000)	= 108 = (100,000,000)
Range of ID codes for commercially standardised cards and chips	= 8 bytes = 64 bits = 264	= 7 bytes = 56 bits = 256

Table 14 – RFID cards and chips

JABLOTRON supplies its own cards and chips for both technologies (JA-190J, JA-191J, JA-192J, JA-193J, JA-194J, JA-195J, JA-196J, JA-197J and JA-198J) or commercially available ID cards with these technologies can be used (the EM UNIQUE 125 kHz cards parameter must be set).

2.8.4.4 Authorisation using a combination of codes and RFID devices

NOTICE: The EN 50131 Security Grade 3 profile does not support combined authorisation using codes and RFID technology.

The JABLOTRON system allows you to increase authorisation security by selecting:

- Card confirmation with a code – user authorisation requires the use of both, an RFID element and a card; the system only requires this for users who have both a code and an RFID element set up.
- Double authorisation – user authorisation requires the use of both an RFID element and a card; the system requires all users to have a code and RFID element set up.

NOTE: Remote access via mobile phone using the voice menu does not allow the use of an RFID element. In this case, the RFID element is replaced by the user's telephone number, which must be set up in the control panel, and the user must call from this telephone number.

2.8.5 Object and division into sections and subsections

JABLOTRON control panels allow the property to be divided into separate sections. The guarded property can thus be divided into separately guarded sub-properties (e.g. individual flats and offices in a building) or hierarchically divide the property into separate sections, which may have different levels of security, assign access rights to users and groups according to their organisational affiliation, or perform purposeful maintenance in a selected section so that it does not disrupt the operation and security of the rest of the guarded property (typically small and medium-sized companies).

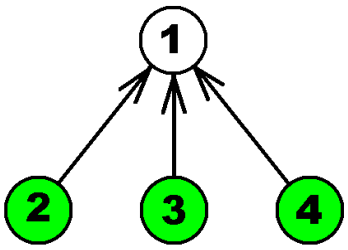
Dividing the building into sections where alarm detectors are located makes it easier to locate the source of the alarm and, depending on the scope of the installation, track the intruder's path through the building.

2.8.5.1 Common section

Larger systems may have multiple sections and also a common section where there are a large number of users who have access to their own section (e.g. offices), but in order to get there, they must pass through or use common areas (corridors, entrance halls, toilets, etc.).

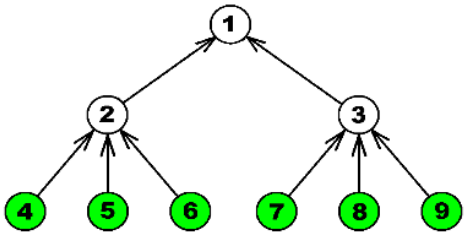
JABLOTRON control panels allow you to create common sections and associate subsections with them (e.g. offices). The common section is level 1 and the subsection is level 2, see Figure 20.

Additional (sub) common sections can be associated with the common section on level 1. A typical solution is a multi-storey company building with a reception area, staircase and separately lockable common areas on each floor. see Figure 21.



(1-common, 2,3,4-separately controlled sections)

Figure 20 – Division of sections into two levels



(1-main common, 2,3-secondary common sections, 4,5,6,7,8,9-separately controlled sections)

Figure 21 – Division of sections into three levels

The common section is automatically set when all associated sections at the lower level are set, and automatically unset when at least one section at this lower level is unset.

NOTE: It is essential for the control of such systems to assign permissions to users to control only the lowest level of their sections. The control of common sections is thus completely automatic.

RECOMMENDATION: For higher levels of common areas (Levels 2 and 3), it is recommended to use keypads with the appropriate number of segments according to the sections used, so that it is clear upon arrival which part is or is not guarded. For the keypad for the lowest level, it is sufficient to use only the segment(s) controlling the relevant sections.

2.8.6 System reactions, statuses and reports

JABLOTRON systems operate on the basis of logical functions that respond to inputs from devices and the control panel according to the current operating mode and set the status of sections, generate local indications, local and remote messages and other types of reports.

The properties of logical functions are entirely dependent on the system configuration (see 4 System configuration) and can be preset using the system profile (see 2.8.1). The basic system states are described in the following table (see Table 15). These states can occur in the operating modes Unset and Set.

System state	Description
Alarm	Based on the configuration, current operating mode and alarm inputs from devices, the control panel triggerss an Alarm state, which: ■ is indicated on the keypad by the red flashing of the activation button and segment in the section where the alarm originated. We call this indication the alarm memory, and it remains active until manually cancelled by an authorised user, see 2.8.3 User authorisation ; ■ can be reported locally for a set alarm duration by activating the IW and EW alarm outputs, which activate internal sirens (Internal Warning) and external sirens (External Warning), see 2.8.6.2 Alarm types and their processing; ■ is reported remotely to the ARC, to the MyJABLOTRON mobile application, or as an SMS or voice message to users' telephone numbers. JABLOTRON systems recognise several types of alarms, see 2.8.6.2 Types of alarms and their processing.
Fault	Based on the configuration, current operating mode and operating inputs from devices and the control panel, the control panel triggers a Fault status, which: ■ is indicated on the keypad by the yellow light of the activation button. This indication remains active until the status that caused the fault is manually adjusted. The indication can be temporarily suppressed by an alarm; ■ can be reported remotely to the ARC, to the MyJABLOTRON and MyCOMPANY mobile applications, or as an SMS message to users' telephone numbers. JABLOTRON systems recognise several types of faults, see 2.8.6.3 Fault states .
Normal	Basic operating state of the system, the system is in operation, no alarms or faults are reported.

Table 15 – System states

2.8.6.1 Overview of configurable device reactions

Devices, generally as input/output devices of the control panel, can be programmed to respond to an external physical stimulus from the environment, from an intruder, from an authorised user, or from interaction with other technology. The Table 16 provides an overview of all types of reactions that the control panel processes.

NOTE: Some devices can be assigned only a specific reactions or no reaction (e.g. external siren). For more information, see the manuals for individual devices.

Reactions	Description	Alarm status (Table 17)
Instant	Instant alarm, if the system is set. Triggers IW and EW.If it occurs during the entry delay, the IW alarm is triggered first, and after the entry delay has expired, the EW alarm is also triggered. (for more information about EW and IW, see 2.8.6.2 Alarm types and their processing).	Intrusion alarm
Delayed A	Intrusion alarm with entry/exit delay, timer A.	Intrusion alarm
Delayed B	Intrusion alarm with entry/exit delay, timer B.	Intrusion alarm
Delayed C	Intrusion alarm with entry/exit delay, timer C. In the Parameters tab, you can preset this reaction so that the exit delay is extended by an active detector that has delay C (e.g. for the duration of the garage door opening).	Intrusion alarm
Next delayed	Intrusion alarm. The detector provides the same exit delay as delayed detectors in the same section. This detector will only provide an entry delay if it is activated after a detector that has a delayed reaction preset. If it is activated first, it will trigger the alarm immediately. Its use only makes sense if a delayed detector is set in the same section.	Intrusion alarm
Final door A	Intrusion alarm with entry and exit delay, timer A. The exit delay is shortened to 5 seconds after the detector has been closed/deactivated.	Intrusion alarm
Final door B	Intrusion alarm with entry and exit delay, timer B. The exit delay is shortened to 5 seconds after the detector has been closed/deactivated.	Intrusion alarm
Final door C	Intrusion alarm with entry and exit delay, timer C. The exit delay is shortened to 5 seconds after the detector has been closed/deactivated.	Intrusion alarm

Reactions	Description	Alarm status (Table 17)
Instant always	Instant alarm if set. EW and IW alarms are triggered together and immediately, even during the entry delay.	Intrusion alarm
Instant/delayed A	The system reacts to detector activation (alarm, entry delay) with an instant response when partially set, and with a delayed response when fully set Delayed A.	Intrusion alarm
Confirmed instant	Instant alarm – Confirmed intrusion reaction.	Intrusion alarm
Confirmed delayed A	Intrusion alarm with entry and exit delay, timer A – Confirmed burglary response.	Intrusion alarm
Repeated instant	Instant alarm – see Repeated reaction below.	Intrusion alarm
Repeated delayed A	Intrusion alarm with entry and exit delay, timer A – see Repeated reaction below.	Intrusion alarm
Tamper	Sabotage alarm at any time (section does not need to be set).	Tamper alarm
24 hours	Instant intrusion alarm at any time (section does not need to be set).	24 hours
Silent panic	Silent panic alarm: 1) EW and IW are not activated, 2) the keypad does not beep, even if this is otherwise set, 3) if the system distinguishes who triggered the alarm (e.g. a key fob with a stolen user identity or by entering a panic code), it does not send an alarm SMS to that user.	This is not a classic alarm, only a report to the ARC and other communication channels.
Audible panic	Audible panic alarm (behaviour is similar to Silent Panic, except that the alarm is acoustically signalled by sirens).	Panic alarm
Fire	Fire alarm at any time (the section does not have to be set).	Fire alarm
Fire confirmed	Fire alarm at any time (section does not need to be set) - see Confirmed fire reaction below.	Fire alarm
Fire instant	Fire alarm only if the relevant section is set.	Fire alarm
Gas	Gas leak alarm at any time (section does not need to be set).	Fire alarm
Medical trouble	Sends a medical trouble report.	Not a classic alarm, only a report to the security control centre and other communication channels.
Flooding	Sends a flood alarm.	Flooding alarm
Setting / Partial setting	Setting (partial setting) of a section. If the section is Common to other sections, all sections belonging to it are set at the same time. This response also has an Unset function.	NA
Siren mute	Mute the internal siren followed by a report of a person's presence in the building.	This is not a classic alarm, only a report to the ARC and other communication channels.
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 the recording of special reports to the event memory is enabled, reports are also sent to the ARC.	Special report
Key box	Special response for a security box, where a special report is sent to the ARC in the event of an intrusion (opening). The box is used, for example, for a sealed "Emergency key". The reaction does not trigger a siren alarm.	Special report
None	Activation has no effect on the guarding of the object. Tamper detection,device monitoring and fault monitoring are maintained. This device setting is intended for controlling PG outputs.	NA
None without tamper	The system reacts to detector activation only by controlling the PG output. It does not trigger any type of alarm (including tampering), and fault monitoring is maintained.	NA

Table 16 – Overview of all types of reactions

2.8.6.2 Types of alarms and their processing

The main task of an alarm system is to alert its owner, users and professional response agency to danger. This can occur not only in the form of a break-in by an intruder, but also in the form of natural disasters or substance leaks such as smoke, gas or flooding in the guarded building.

The reporting of each type of alarm may differ depending on its cause (reactions, see 2.8.6.1 Overview of adjustable peripheral responses). The main types of alarm reporting are local, internal (IW) and external (EW) sirens and remotely to the ARC or to the user via mobile applications, SMS messages or voice calls.

The following table (see Table 17) shows the activation of both outputs (EW, IW) according to alarm types and section status:

	Alarm type					System settings – Parameters		Activates	
Section status	**Intrusion**	**Tamper**	**Audible panic**	**Fire**	**24h./ Flood**	**IW siren for partial setting**	**IW siren during tampering**	**EW**	**IW**
Unset		X				Setting has no effect	Off	NO	NO
		X				Setting has no effect	On	NO	YES
			X			Setting has no effect	Setting has no effect	YES	YES
				X	X	Setting has no effect	Setting has no effect	NO	YES
Partially set		X				Setting has no effect	Off	NO	NO
		X				Setting has no effect	On	NO	YES
	X					On	Setting has no effect	NO	YES
	X					Off	Setting has no effect	NO	NO
			X			Setting has no effect	Setting has no effect	YES	YES
				X	X	Setting has no effect	Setting has no effect	NO	YES
Set	X	X	X	X	X	Setting has no effect	Setting has no effect	YES	YES

Table 17 – Activation of EW and IW siren outputs

All types of system sirens sound a fluctuating tone (optionally intermittent or continuous) when activated. Outdoor sirens flash red or blue (depending on the type of siren and the light guide of the selected siren cover).

The duration of the alarm indication is determined by the alarm time setting in the control panel, but each siren also has its own adjustable siren duration limit, which can be used, for example, to shorten the duration of the outdoor siren compared to the indoor siren.

Each acoustic alarm notification (except for silent panic) has a start and end (by timing or cancellation by the user). The end of the acoustic alarm is recorded in the event history along with the cause, time and date.

The acoustic alarm can be **silenced** by user authorisation.

Cancelling the alarm status

On system keypads, all alarms (except for silent panic alarm) are signalled by the activation button flashing red and a continuous acoustic warning signal.

Alarm type	Activated by reaction	Description	Behaviour according to Table 17
Intrusion alarm	Instant; Delayed A, B and C; Next delayed, Final door A, B and C; Instant always; Instant/delayed A; Confirmed instant; Confirmed delayed A; Repeated instant; Repeated delayed A		Intrusion
Tamper alarm	Tamper (typically opening the cover, tearing off the mounting, masking, loss of Bus devices, short circuit on the Bus, 10× incorrect code entry)	The control panel continuously monitors all devices and their connections 24/7, as well as attempts to crack the code.	Tamper
Fire (basic reaction	Fire	Basic 24/7, typically from fire response detectors (smoke, temperature, gas, CO)	Fire
Fire instant	Fire if set	Use in areas with normal smoke occurrence (restaurants, welding shops)	Fire + Set
Fire confirmed by another detector	Fire confirmed	Confirmed 24/7, installation of at least two detectors with the same reaction required, where one confirms (verifies) the other	Fire
Gas	Gas (typically detection of toxic, flammable or explosive gas)	Special reaction for different reporting to the control centre	Fire
Silent panic	Silent panic (panic buttons, controllers, keypads, modules, codes or duress access control)	Does not fall under the standard alarm status, cannot be used for status control of outputs	---
Audible panic	Audible panic (panic buttons, controllers, keypads, modules, codes)	PG outputs can be controlled (e.g. door locking)	Loud distress
24-hour alarm / Flood	Activation of detectors with constant monitoring (24-hour or flood)	Ranked among intrusion alarms, reporting identical to other alarms	24-hour alarm / Flood

Table 18 – Alarm Types

2.8.6.2.1 Delayed A

This is an alarm condition of the control panel, which can be triggered exclusively by detectors in a delayed or instant loop (and their variations), and only in a partially or fully set system state. It is signalled by external and internal sirens according to the settings (see Table 18). The alarm signalling time is timed according to the alarm duration setting in the control panel settings. When it times out, the sirens stop sounding and the keypad stops signalling the alarm. User authorisation mutes the acoustic signalling of all sirens and keypads, but does not automatically cancel the system alarm status or unset it. This must be done subsequently using the segment or keypad menu.

2.8.6.2.2 Tamper alarm

The alarm control panel monitors each individual device enrolled to the system, both in set and unset system status. Most devices have a cover opening sensor and a sensor for removal from the base. Activation of these sensors triggers a tamper alarm, which in unset mode can only be reported acoustically by an internal siren (according to the Siren IW parameter in case of tampering), but in the set system, an acoustic alarm is always triggered by both internal and external sirens (see Table 18). A tamper alarm can also be triggered by the loss of Bus devices (e.g. a short circuit on the Bus) or by exceeding the number of incorrectly entered codes (10 times), both on the control keypad and remotely via DTMF dialling, SMS message or MyJABLOTRON control applications (WEB + Smartphone).

2.8.6.2.3 Fire alarm

A fire alarm is triggered by the activation of detectors with a preset fire reaction Fire detectors include: smoke detectors, high temperature detectors, combustible and explosive gas detectors, and toxic carbon monoxide detectors. In the unset or partially set system, a fire alarm is triggered only by internal sirensand, when the section is set, also by external sirens.

Fire detectors can react in the following ways:

1. Fi**re –** basic reaction for fire detectors,
2. Fi**re confirmed by another detector –** option for maximum reliability. For this response, at least two detectors with the same settings must be installed in each room.
3. Fi**re instant –** used only to detect smoke in a set section (e.g. smoking restaurants, welding shops, etc.),
4. Ga**s –** special fire detector reaction with identification of the presence of toxic, flammable or explosive gas for specific reporting of the event to the Alarm Receiving Centre (ARC).

2.8.6.2.4 Panic

Panic is the name of an alarm event in the system, which is split into Silent Panic and Audible Panic. Each of them behaves slightly differently.

- Silent panic is a special event that is unique in that it does not fall under the standard alarm condition, which would be signalled acoustically by both a siren and a keypad. This event is not timed and therefore has no termination event such as End of Silent Panic. It cannot therefore be used for status control of a programmable output. Silent panic can be used if the user finds themselves in a situation they need to discreetly call for help without alerting the attacker. Silent panic can be triggered from a designated (e.g. hidden or portable) panic button, either by a preset button or a combination of buttons on the remote control, or from a dedicated segment on the keypad (allows the option of postponement with an adjustable time), by pressing the internal siren button, by the input of Bus modules for wired detectors, or by entering a numerical code that triggers a silent panic alarm. A silent panic is also triggered by the control panel during so-called duress access control (see 5.8 Duress control), which is activated by entering a special code based on the code normally used.
- Audible panic alarm is a standard timed alarm event that is signalled acoustically by a siren and the keypad and has a start and end to the alarm. It can therefore also be used for status control of a programmable output. It is used, for example, to trigger a panic alarm requiring optical signalling or the locking of electrically controlled doors, etc. An audible panic alarm can be triggered from a designated (e.g. hidden or portable) panic button, a preset button on the remote control or a dedicated segment on the keypad (allows delayed announcement to be used), by pressing the internal siren button, or by the input of Bus modules for wired detectors.

NOTE: Both types of panic alarms are unique in that they can be triggered repeatedly without any restrictions or automatic blocking.

2.8.6.2.5 24-hour alarm

Detectors that provide constant monitoring in the system regardless of the system status (set or unset) can be programmed to react 24 hours a day or in case of flooding. This type of alarm is classified as an intrusion alarm, although it can also occur when the system is unset. It is signalled by an external and internal siren depending on the system status (see Table 17). Alarm events are reported in the same way as other types of alarms.

2.8.6.2.6 Ending an alarm

If an alarm with acoustic siren signalling occurs in the system, its duration is measured by setting the alarm duration timer in the F-Link software, under the Parameters tab. However, if an authorised user is present in the building, they can terminate the alarm earlier. Ending the alarm causes all acoustic signals to be switched off immediately and also terminates the voice transmission of alarm information to the preset telephone numbers. The method of ending the alarm depends on the parameter setting available in the System Parameters tab:

Unsetting cancels the alarm

- Enabling this option will terminate the ongoing alarm only by unsetting the section in alarm or after authorisation by selecting "Cancel warning indication" from the LCD keypad menu.
- By disabling this option, the current alarm will be terminated simply by authorisation of a user authorised to control the section, without the need to disarm it.

2.8.6.2.7 False alarm reduction

In installations where there is an increased risk of false alarms, special types of responses can be used:

Confirmed intrusion reaction – if a detector with a preset confirmed reaction is activated in a set section, the system reports an unconfirmed alarm only to the ARC and waits for confirmation from another detector. The alarm can be confirmed by any intrusion detector in the set section. In the Parameters tab, you can specify whether the confirmation can come from any set section or must be from the same section. The time during which the system waits for confirmation from another detector can be up to 60 minutes and is programed in the Parameters tab. If the alarm is not confirmed within the specified time, the alarm will not be triggered. If a confirmed delayed reaction is used, the activation of the detector sends an unconfirmed alarm only after the entry delay has elapsed. When using confirmed reactions, a higher number of intrusion detectors must be installed in the building so that confirmation can take place. This type of reactionis only available when the "Default" system profile is selected.

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 specify whether the confirmation can come from any section or whether it must be from the same section. The waiting time for confirmation of a fire alarm is programed in the Parameters tab. If the fire is not confirmed within the specified time, the fire alarm will not be triggered. When using confirmed reactions, a higher number of fire detectors must be installed in the building so that confirmation can take place.

WARNING: The use of this function must be considered carefully and only in accordance with local regulations.

Repeated reaction – if a detector with this type of reaction is activated, the system waits to see if the same detector will be activated again. In the Parameters tab, specify the time for which the system waits for repeated activation and also the time during which the detector is not evaluated. If the detector is not triggered again within the preset time (6 to 120 seconds can be defined), the system cancels the first activation. Repeated reaction is used in environments with an increased risk of occasional false alarms, e.g. from rodents, small insects, draughts, etc.

Three-strikes function – all detectors with programmed alarm reaction type of intrusion, tamper or fire are limited to three possible activations during one monitoring period. After three activations (on the fourth intrusion), a bypass is activated for the given alarm input and the relevant detector is disabled from further operation. If these three activations occur during a single alarm, a total of three alarm SMS messages are sent and the detector is then disabled. If these three activations occur at intervals longer than the duration of the alarm, a total of three alarm SMS messages are sent, three alarms are triggered, and only then is the detector disabled. This function can be further extended by the "Device auto-bypass" parameter on the Parameters tab and the "3rd alarm" option, which allows for an auto-bypass after three activations from each device during each of a maximum of three alarms. This allows up to nine (3x3) alarm SMS messages to be sent. By unsetting and setting the section, the bypass is deleted and the detector resumes monitoring. The bypass for fire and flood response is automatically reset the following day at 12:00 (according to the "Reset device auto-bypass daily" parameter in the Parameters tab). The Three-strikes function does not apply on devices that have defined the Panic reaction. Similarly, the number of detector fault triggering is also limited (can be disabled by the "Disable Fault autobypass" parameter on the Parameters tab).

Delayed reporting to the ARC – function according to EN 50131-1 to reduce the number of false alarms caused by incorrect operation by the system user and to limit the number of security service call-outs. Activating this function causes that after the entry delay has elapsed, a pre-alarm is triggered (sirens sounding, keypad indication), but the system waits another 30 seconds before sending the alarm to the ARC. This gives the user more time to cancel the reporting of the alarm event to the ARC even after it has been triggered. If they manage to do so in time, no alarm message is reported to the ARC. This delay only applies to alarms triggered by a delayed loop. Other types of alarms (instant, fire, tamper, etc.) are always reported immediately without delay, regardless of this function.

2.8.6.3 Fault states

A fault is a warning signal from the system that indicates a non-standard state of the control panel, communication or devices. These may include problems with radio, GSM or LAN communication, detector coverage (with anti-masking function), power supply problems (mains or battery) or backup power supply. A serious fault in the system is indicated visually by a yellow light on the indicator button.

Fault reports from each source are counted, and when the fourth fault occurs, the cause of the fault is bypassed, which means that the fourth fault is no longer reported. This automatic fault blocking is optional with the "Disable Fault autobypass " parameter, available in the F-Link software on the Parameters tab. When this parameter is activated, no faults are counted or blocked for reporting. This option is not available in the default "Default" system profile.

The most common causes of faults from basic types of devices:

Fault source	Cause
Control panel	Mains power failure lasting longer than 30 minutes.
	Faulty or low battery in the control panel.
Communicators	Loss of LAN connection or GSM signal lasting at least 15 minutes.
	Failure to transmit events to the ARC within the specified time.
Radio modules	Interference on the 868.1 MHz radio band.
	Loss of Bus communication.
Keyboard	Loss of radio or Bus communication.
Sirens	
Modules	
Detectors	Masking of motion detectors (so-called anti-masking). Internal detector fault (gas leak detector). Fault caused by reduction in beam intensity (infrared barrier).

Table 19 – Fault conditions

2.8.6.3.1 Fault due to loss of device

Each device (Bus and wireless) in the system is regularly monitored and checked by the control panel when the Supervision function is enabled (Devices tab, Supervision column). If communication with the control panel fails (the device does not respond or report within the defined time), a fault event "Loss of communication with device" is triggered, or, depending on the setting of the "Loss of a Bus device" parameter, a tamper alarm is also triggered. This is optionally triggered in the event of radio band interference lasting at least 30 seconds according to the programmed detection level in the radio module, or by a short circuit on the Bus disrupting communication with the Bus devices. The time until the fault is triggered from its occurrence is fixed and cannot be changed. For Bus devices, the fault is triggered within 8 seconds, and for wireless devices, the fault is triggered within 120 minutes after the last communication.

The "Supervision" function is optional for most wireless devices of the system designed for monitoring (detectors, sirens, keypads), for some it is completely disabled (remote controls and automation devices), and for Bus devices it is always enabled without the possibility of disabling.

The parameter which changes the behaviour of how the control panel processes when in the event of loss of communication with a Bus device, called "Loss of a Bus device" and is available in the F-Link software on the Parameters tab. It allows you to set the following options:

- Fault – the loss of a device on the Bus or it's shorting the control panel always indicates as a fault.
- Tamper always – the loss of a device on the Bus or it´s shorting the control panel always indicates as a tamper alarm whenever it occurs. If the radio module used has interference detection enabled, then an intrusion alarm will also be triggered in the event of interference. The intrusion alarm is always triggered also with a fault indication. When the fault is restored, the active intrusion alarm is also deactivated.
- Tamper after confirmation – the loss of a first device on the Bus the control panel always indicates as a fault, and if another device is lost within the time preset by parameter ”Period of waiting for alarm confirmation”, the next loss of a device is created and a tamper alarm is triggered. Restoring all lost Bus devices, both the fault and the tampering are terminated.

3 System installation and commissioning

This chapter describes the general process of installing the JABLOTRON alarm system – from preparation and design of the solution, through installation of Bus and wireless devices, to final commissioning of the control panel.

NOTICE: The entire process should comply with European technical specifications CLC/TS 50131-7 and CLC/TS 50136-7, unless local regulations or the requirements of the installer and third parties stipulate otherwise.

It contains technical requirements, manufacturer recommendations and procedures that the installation technician must follow to ensure proper system function, the required level of security and long-term reliability of the installation.

The final part of the chapter deals with the actual commissioning of the system, verification of the correct operation of individual devices, performance of tests in accordance with standards, and handover of the system to the user.

3.1 Before installing the system

The control panel provides the option of connecting a mains power supply in the range of 110 ÷ 230 VAC / 50 ÷ 60 Hz.

Before starting the design and installation, it is necessary to discuss the following with the customer:

- Clarify the requirements placed on the alarm system by third parties (e.g. insurance companies, police, local requirements), which may require installation with a specified level of security, ARC service or whether the installation must or must not be equipped with an external siren (noise emissions, urban planning requirements, historically protected buildings).
- Identify risks related to property, operating procedures in the building, crime in the immediate and surrounding areas, quality, potential threats to the surrounding area (e.g. theft of weapons from a safe, flammable materials from warehouses, etc.) and the extent of mechanical security, and determine the level of security for the building.
- Identify the building's operating mode, agree on the division of the building into sections and the methods of controlling the alarm system.
- Agree on the methods of reporting alarms (local, remote to the ARC, other).
- Agree on the methods of responding to alarms (emergency services, police, fire brigade, medical assistance) and determine response times.
- Agree on the type of installation (Bus, wireless or combined).
- Agree on other requirements.

Select a location for the control panel that:

- is **hidden inside the protected area** (for large installations, a separate, lockable room and the assignment of a separate section are recommended);
- has a mains power supply (a separate supply with a separate circuit breaker is recommended),
- has sufficient GSM signal (at least 30%; you can check the GSM signal strength at the installation location with a mobile phone) or has a LAN distribution with an internet connection.



Please note that if the trespasser knows the location of the control panel, they could damage it before sending the alarm report. We recommend protecting the control panel area with at least an instant reaction detector.

The control panel's power supply may only be installed by a person with the appropriate electrical engineering qualifications.



The control panel power supply has double circuit safety separation. During the installation and connection of the system's Bus components, all power to the control panel must be completely turned off, or the Bus power must be turned off using the F-Link software.

- When placing the components, follow their manuals, general principles of an alarm system design and instructions provided by the manufacturer during certification training. If you have any questions, please call JABLOTRON for advice. **The manufacturer is not liable for damage if the system is improperly installed or configured**.
- Prepare the control panel's power supply – use a suitable double-insulated cable with a conductor cross-section of 0.75 to 1.5 mm^2. It is recommended to install surge protection elements on the mains supply to the control panel. It is also recommended to use a separate fixed cable supply with its own circuit breaker (preferably 2 A – 6 A), which also acts as a main supply switch.

NOTE: A supply protected in this way must not be used for any other power supply or control of other circuits.

- Place the control panel on a flat wall or other non-combustible surface that is part of the protected building. Ensure that there are no metal structures (e.g. lift shaft, metal switchboard) immediately adjacent to the control panel that could interfere with the transmission or reception of radio signals (radio module and GSM communication). Prepare the holes for the dowels according to the drilling template. Screw the screws into the top two holes so that they are about 1 cm above the level of the wall, on which you then hang the control panel. Secure the control panel with the bottom screws and then tighten the top screws.

3.1.1 System design

The system design is carried out according to:

- the building documentation (project documentation);
- identified penetration routes (e.g. building openings, entrance doors, windows, balconies, skylights, fire ladders, etc.) and the quality of mechanical security;
- the specified/agreed level of security;
- agreed form of response to an alarm;
- the manner of use of the facility and the number of users;
- documentation of alarm components.

3.1.1.1 System control

JABLOTRON system control panels allow you to choose between two basic methods of alarm system control:

- Setting/unsetting inside the protected building or section with an exit/entry route and entry/exit delay (the control keypad is behind the door);
- Setting/unsetting outside the protected premises or section (the control keypad is in front of the door).

These two methods can be combined in the building according to the way the building is divided into sections, the number of entrance doors, garage doors and, if applicable, entrance gates and gates to the building's grounds.

EXAMPLE: A small family house with a garage, one main entrance, an entrance from the terrace to the living room, a rear entrance and a garden with an access road (see Figure 22 – Entrance system design).

The control method with an entry/exit route has been chosen, as the customer only wants one system keypad inside the building.

The floor plan of the building shows the entrances to the building and the routes leading to a single control point (system keypad), including the estimated times required for users to reach the control point, perform authorisation and unset the building after opening the relevant door (or gate). We call these times entry delays, and they are an adjustable parameter that is closely related to the type of building and the ability of users to "enter – walk – unset".

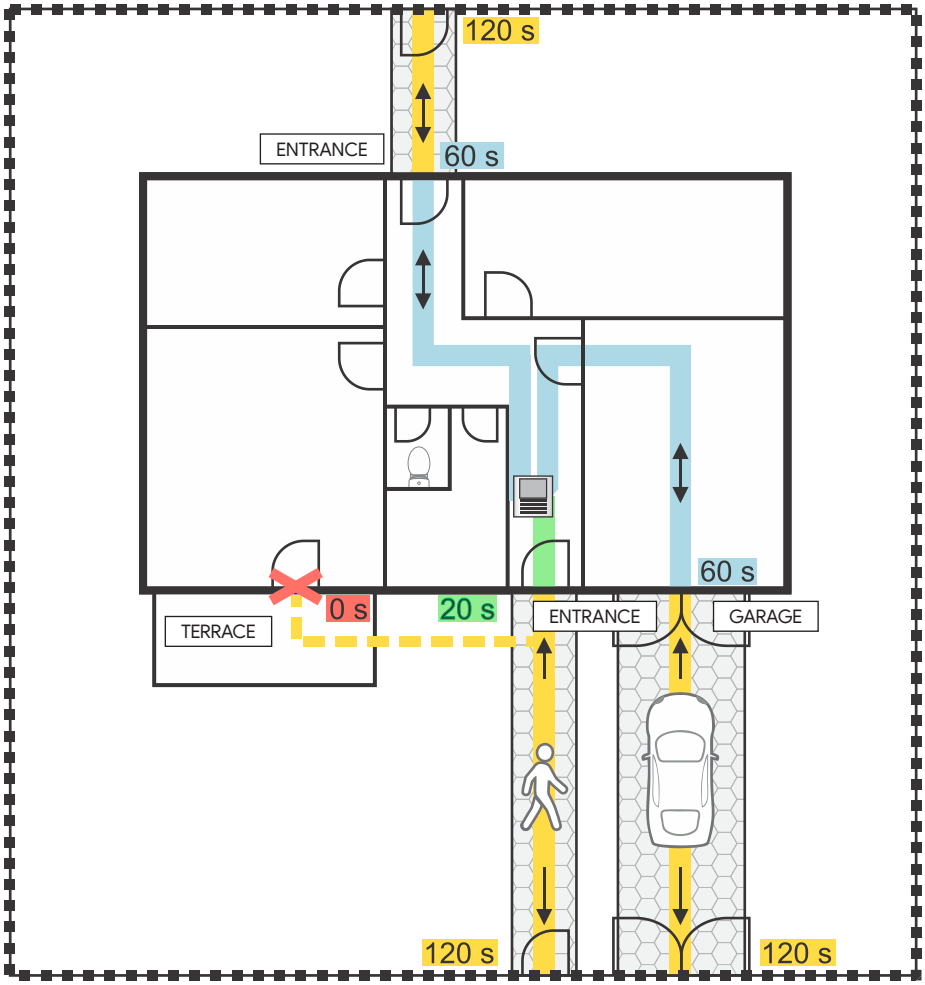


Figure 22 – Entrance system design

Entry and exit routes:

Delayed A – 20 seconds | Delayed B – 60 seconds | Delayed C – 120 seconds | Immediate – 0 seconds

NOTICE: Entry delays should be set to the minimum time necessary for the user to safely unset the system, but not enough time for a potential intruder to disable the system and its control panel.

The image also shows the entrance (door from the living room to the ground floor terrace), where no access route is considered. This part of the building therefore has no access delay, and any entry into the secured building through this door triggers an instant alarm.

The building is surrounded by a garden with an entrance gate (for pedestrians) and an access road with an entrance gate. The consideration of including the entrance gate to the secured building in the access route may have a significant impact if an intruder wants to drive a car up to the house in order to quickly and undisturbedly load stolen items and leave from the premises before the security service or police arrive. A detector placed on the entrance gate significantly reduces the response time to the alarm, subsequent intervention, and the possibility of deactivating (tampering) the alarm system.

Based on the proposed access routes and entrance doors and gates, the location of the first alarm detectors is proposed, which are designed to detect their opening (magnetic detectors) or, if necessary, their overcoming by an intruder passing through, so-called "opens - enters - is caught" (motion detectors), or overcoming them by brute force (glass break detectors, shock or tilt detectors).

In the case of medium-sized gardens, it is also recommended to guard the perimeter of the garden (infrared or laser optical gates) and to supplement large areas with spatial surveillance (outdoor motion detectors, cameras).

WARNING: The choice of these detectors will significantly affect the functionality of the alarm system, user error rates, and the security grade of the property and its users. Choose them based on a good knowledge of their functions according to the manufacturer's instructions for use and local environmental influences.

In areas outside the access routes, an additional level of security is selected according to the risk that an intruder may enter the building through these areas. These are usually windows, balcony doors, skylights and other technological openings. An intruder's passage through these entry points may be accidental or planned (open windows), by brute force (breaking glass or removing the entire window from its frame), or purposefully planned (e.g., through a ventilation shaft). Detection of intrusion into these areas is then proposed using opening detection, motion detection, glass break detection or shake /tilt detection.

Based on the conceptual design of entry routes and security for other parts of the building, a design for alarm detectors is created, a suitable response is selected, and the necessary delays for individual routes are programed.

JABLOTRON control panels provide a powerful tool that allows you to define three different entry delays and their mutual interaction. When designing the system, in addition to the entry/exit route, it is necessary to divide it into sections and select appropriate reactions for instant and delayed zones (delayed A, delayed B and delayed C) and program entry and exit times (to be described later).

Detector location	Sections, naming	Detector type	Device response selection	Entry time	Exit time
Outdoor gate	Garden	1. Magnetic detector	Delayed C	120 s	360 s
Movement outside in the garden	Garden	2. Motion detector	Delayed C	120 s	360 s
Garage door	House / Garage	3. Magnetic detector	Delayed B	60 s	120 s
Rear entrance	House/Hall/Corridor	4. Magnetic detector	Delayed B	60 s	120 s
Garage (inside)	House / Garage	5. Motion detector	Next delayed (Delayed B)	60 s	120 s
Main entrance	House / Hall / Corridor	6. Magnetic detector	Delayed A	20 s	60 s
Hall/Corridor	House / Hallway/ Corridor	7. Motion detector	Next delayed (Delayed A)	20 s	60 s
Balcony door	House / Living room	9. Magnetic detector	Instant	0 s	0 s
Living room	House / Living room	9. Motion detector	Instant	0 s	0 s

Table 20 – Detector placement

It is recommended to have multiple keypads located near the entrance doors to the building, positioned so that it is not possible potential perpetrators observe the authorisation code being entered or the status of the system from outside the building.

Entry route A** (20 seconds)**:

- *Entering a guarded premises (system set) through the main entrance triggers activation of Delay A (20 seconds), which starts timing the entry delay period.*
- *Entering a valid code on the keypad and pressing the green button on the segment puts the system into Unset mode.*
- If nobody is authorised and the system not unset within the arrival times, an alarm will be triggered from the delayed loop (Delayed A).

Entry routeEntry route B** (60 seconds)**:

- *Entering a guarded premises (system set) through the rear entrance or garage triggers activation of Delay B (60 seconds), which starts timing the entry delay.*

- *Further movement in the building in front of detectors with a Delayed A reaction shortens the entry delayto Delay A (20 seconds) if it is shorter than the timing of Delay B.*
- *Entering a valid code on the keypad and pressing the green button on the segment puts the system into Unset mode.*
- If authorisation and unsetting of the system do not occur within the entry times, an alarm will be triggered from the delayed loop that times out first (Delayed A, Delayed B).

Entry route C and then via route A or B (120 seconds):

- *Enteringa guarded premises (system set) by activating one of the outdoor detectors (by opening the gate, wicket or activating the outdoor PIR detector) triggers activation of Delayed C (120 seconds), which starts timing the entry delay. By opening:*
  - *the garage door detector triggers the Delay B entry time (60 seconds), which shortens the timing of the already activated Delay C (if the C time is not already shorter), or*
  - *the main entrance triggers the entry Delay A (20 seconds), which also shortens the entry time if it is shorter than the timing of Delay C or Delay B.*
- *Entering a valid code on the keypad and pressing the green button on the segment puts the system into Unset mode.*
- *if authorisation and unsetting of the system do not occur within the entry times, an alarm will be triggered from the delayed loop when timer expires first (Delay A, Delay B, Delay C).*

3.1.1.2 Selection of control components

In addition to selecting detectors, it is necessary to select control components. The main element should always be the system keypad, which, in addition to the basic control buttons, also provides an LCD display. The system keypad provides authorised users with important information about the system status, access to the event history and other functions (menu for changing the password, bypassing devices, entering/exiting maintenance and service mode, etc.).

NOTE: *The system keypad with LCD display can be partially replaced by the MyJABLOTRON mobile application.*

Other control components can be selected without an LCD display and are used only for controlling sections.

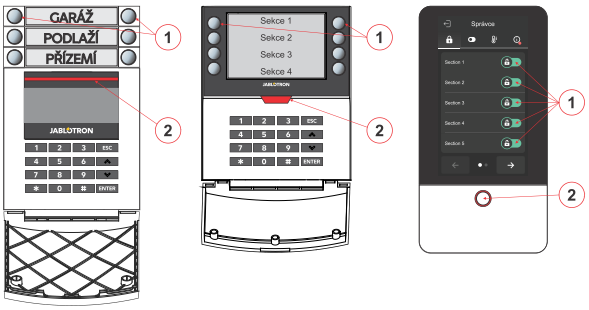
Depending on the size of the system, we select keypads and access modules with a range of control elements and segments.

JABLOTRON systems allow you to choose:

NATUS touchscreen keypad – section and PG control widgets are displayed and scrolled on the display;

- four-segment keypad with LCD display – control segments are provided as mechanical, backlit buttons;
- segment keypad with LCD display and segment access modules – control segments are modular components that can be added according to the number of sections and system requirements; they are particularly suitable for larger installations, common areas and where there is an emphasis on quick information overview of the status of the building and individual sections.

NOTE: JA-1x6E touch keypads do not have traditional control segments; these are replaced by graphic widgets for sections and PG outputs. They cannot be configure d in the same way as classic segment keypads.



1 – section and PG control (segments and widgets), 2 – LED status indication

Figure 23 – Section/PG control and optical indication

Control segments – contains two buttons (off – left and on – right). The segment is used to set or unset the setion, control appliances or call for help. The segment can also be used to indicate the status of the section or PG output (it can signal the active status with both a standard red and green indicator light – "inverse indication" segment function). For example, the segment can be used to indicate whether doors are open or closed by evaluating the activation/deactivation of a magnetic detector on the doors. The segment can have a "Common segment" function for simultaneous control of multiple sections at once.

The access module verifies user authorisation. The selection of the module determines the method of authorisation (chip reader, keypad + reader, keypad with LCD display + reader). The module also allows the door lock to be opened by simply placing a chip on it (entering a code). The modules are available in wireless and Bus versions. They are functionally equivalent.

The configuration of the control keypad is also described at 4.2.3.2 Keypad configuration.

3.1.1.3 Alarm output selection

To ensure the proper functioning of the alarm system, it is necessary to set the alarm outputs. JABLOTRON control panels allow for various configurations of local warning messages and remote alarm messages:

- External sirens (with their own power supply or backup);
- Internal sirens;
- Reporting to the ARC (LAN or GSM);
- Reporting to a dual/backup ARC (LAN + GSM);
- Reporting to the user (MyJABLOTRON app, SMS, voice call).

The choice of alarm reporting method depends on local regulations (police, municipal ordinances, other standards), third-party requirements (insurance companies, operators) and customer preferences (operators).

If a certified profile is selected, the minimum requirements are as follows:

a) at least one backup outdoor siren (e.g. JA-113A or JA-163A) and one line to the ARC in ATS configuration min SP3 (LAN or GSM); or
b) two alarm lines to the ARC in ATS configuration min. DP2 (LAN main line + GSM backup line).

WARNING: Ensure that all LAN devices providing Internet connection have a backup power supply!

3.1.1.4 Choice of control panel, profile and system size

The choice of control panel fundamentally influences the entire system design. Based on the required devices (detectors, keypads, etc.), it is necessary to choose the infrastructure concept, whether it will be Bus, wireless or hybrid. Furthermore, according to the previous steps, determine the number of sections, the number of users in the system and the profile in which the system will be operated.

The basic parameters for selecting a control panel are:

1) Number of users;
2) Number of sections (in the case of a divided system);
3) Profile for the required operation (Default, EN 50131 Security Grade 2, Incert Grade 2, LARMKLASS II/R SSF 1014, Zwangsläufigkeit, EN 50131 Security Grade 3);
4) Alarm outputs (local warning devices internal/external, single or dual transmission to ARC, ATS category);
5) Types and number of devices, including power consumption calculations for Bus-powered devices;
6) System backup in case of power failure (12h / 24h / 30h / 60h);
7) Other non-alarm requirements (PG outputs, remote control and management, etc.).

These basic parameters will allow you to select a control panel and a suitable backup battery according to the control panel specifications and, if necessary, select additional accessories necessary or suitable for operation, such as backed-up Bus boosters, Bus isolators, ARC communicators, wireless repeaters and cloud services.

WARNING: When selecting a control panel, always allow for a performance and functional reserve; the system design must allow for operation for 10 years or more.

3.2 Control panel installation

3.2.1 Preparation and installation of the control panel

The system design has selected a suitable location in the building where the control panel can be installed. Ensure that this location has a power supply and, if required, a LAN network connection.

The security control panel requires a permanent, fused AC power supply in the range of 110 ÷ 230 V AC, see Technical specifications. The control panel is an electrical device with double insulation. The power supply is provided by a two-core cable with a conductor cross-section of at least 0.75 mm² to 1.5 mm².

RECOMMENDATION: The supply cable should have a separate circuit breaker. This will ensure that a short circuit on another device does not cause the alarm system to be disconnected from the power supply. It is advisable to mark the circuit breaker with a warning against accidental shutdown.

Before installation, perforate the necessary cable passages for the power supply and output Bus cables.

RECOMMENDATION: According to good practice in security industry, all cables should be routed through the rear of the control panel to prevent access through an inappropriate opening on the side. This will prevent possible tampering of the control panel.

The control panel covers are ready for mounting using 4 screws on the wall, located in the corners of the control panel cover. **Always use all screws to ensure safety and proper tamper protection!** Keep in mind that the control panel is also loaded with the weight of the lead battery, and the dimensions of the mounting screws, wall plugs and preparation of holes in the wall must take into account the total weight.

To prepare the holes, use the drilling template included with the control panels or use the dimensions specified in the Technical specifications at 2.1.1.

Mount the control panel on the wall, connect the power cable to the power supply terminals (see 2.2 JA-103K, 2.3 JA-103K-7Ah, 2.4 JA-107K a 2.5 JA-108K).

WARNING: The power cable MUST BE DISCONNECTED FROM THE POWER SUPPLY DURING INSTALLATION, otherwise there is a risk of electric shock.

If you have it in your configuration, connect the LAN cable to the RJ45 socket on the control panel mainboard. Then, depending on the configuration, install the expansion accessories (radio module, GSM communicator, Bus splitters, etc.).

3.2.2 System

The alarm system has backup power supply. Management of powering is realised by a backup battery. The type of control panel and thus the maximum battery capacity were selected in the alarm system design. The Table 2 and the required configuration determine the maximum consumption from the control panel, i.e. the sum of the current consumption of all (I) Bus outputs.

EXAMPLE: JA-107K control panel in GSM communicator configuration is installed, LAN communicator is active and the required backup is at least 12 hours, then when using the largest usable battery, the control panel can be loaded with a maximum of 1080 mA.

Battery status/voltage	Voltage/ loss
13.2 V/13.2 V	13.6 V/0 mA ; 13.6 V/0 mA ; 13.6 V/24 mA

Figure 24 – Control panel voltage/drops

The consumption from each Bus is checked using the F-Link software, in the diagnostics tab on the zero line (for the control panel). All displayed values are added up for the total consumption of the control panel. If this consumption exceeds the required maximum current for backup, it is necessary to use the JA-120Z Bus booster.

Insert the backup battery into the designated slot in the control panel cover and secure it with a strap! This will prevent possible injury and damage to the control panel if the battery falls out.

3.2.3 Example of determining consumption for system backup

The required current consumption from the control panel can be calculated based on the system design and selected devices. The calculation is performed by compiling the consumption during backup for individual devices. Consumption during backup is a specific current that the device draws from the Bus when the system is in backup power mode. This information can be found in the documentation for each component. If consumption during backup is not specified, the normal consumption is used. The Table 21 shows an example of a small assembly.

Peripheral	Description	Pcs	Power consumption during backup
JA-112R	Bus module for wireless connection of JA-100 components	1	30 mA
JA-115E	Bus four-segment keypad with display and RFID reader	1	18 mA
JA-113M	Bus magnetic detector with foreign magnetic field detection	1	2.5 mA
JA-112P	Bus PIR motion detector	2	10 mA
JA-111ST-A	Bus combined smoke and temperature detector	2	10 mA
JA-110A II	Bus indoor siren with battery backup	1	5 mA
JA-113A-BASE-RB	Bus external siren	1	2.5 mA
		TOTAL	**78 mA**

Table 21 – Standby consumption (example)

The total consumption during backup is 78 mA. For 12-hour backup, you can use the JA-103K control panel with a GSM communicator and the LAN communicator switched off, which allows a maximum continuous load of 93 mA (see Table 2).

N*OTE: The JA-103K is more suitable for wireless systems in which the devices are powered by batteries. When configuring a wireless control panel, be sure to include the JA-11xR radio module(s) in the power consumption calculation. For larger Bus systems, use the JA-107K and, if necessary, the JA-120Z control panel.*

3.2.4 Installation of Bus devices

Only connect JABLOTRON JA-1xx series Bus devices to the system. Follow these steps when connecting:

1. Prepare the Bus cable distribution. The cables must be installed inside the protected areas protected by the system. If the cable is outside the protected area, this section must be separated by a Bus isolator JA-110T. It is recommended to follow CLC/TS 50131-7 to ensure installations comply with the required security grade.
2. Install the devices in the designated positions and follow the manufacturer's installation instructions in the manuals for these devices.
3. When connecting the Bus to devices and the control panel, the control panel power supply must be completely turned off and the backup battery disconnected, otherwise damage may occur.
4. To split the Bus, we recommend using the JA-110Z, JA-110Z-B, JA-110Z-C or JA-110Z-D Bus splitters.
5. When connecting Bus devices, ensure that terminals and cables of the same colour are connected (red, yellow, green, black).

3.2.4.1 CC-xx Bus cables

For cable distribution, we recommend using CC-xx cables, which offer the advantage of colour coding that matches the terminals.

Type	Number of conductors	Diameter	Conductor cross-sections		Application	Packaging	Resistance of power cable pair		
			Power	Data			1 m	10 m	100 m
CC-01	4	4.5 mm	0.5 mm²	0.2 mm²	Suitable for main Bus distribution	300 m	0.0754 Ω	0.754 Ω	7.54 Ω
CC-02	4	4.1 mm	0.2 mm²	0.2 mm²	Suitable for branches from the main Bus distribution or shorter cable sections.	300 m	0.1932 Ω	1.932 Ω	19.32 Ω
CC-03	8	6.4 mm	0.7 mm²	0.3 mm²	Suitable for main Bus distribution, provides 2 auxiliary pairs of conductors, e.g. for magnetic contacts or tamper loops.	250 m	0.0705 Ω	0.705 Ω	7.05 Ω
CC-11	4	6.9 mm	0.5 mm²	0.2 mm²	Suitable for main Bus distribution. Cable with increased fire resistance (flammability class B2CA)	200 m	0.0754 Ω	0.754 Ω	7.54 Ω
NOTE: The resistance of a pair of conductors refers to the resistance of the entire loop (there and back).									

Table 22 – CC–xx Bus cables

3.2.4.2 Bus arrangement, branching

When connecting individual system devices – detectors, keypads, sirens, output modules, etc. – the Bus cable can be routed as short as possible, regardless of which sections of the system the devices belong to. The Bus can be branched as needed. A linear, radial or combined structure is possible.

The Bus cable must not be connected in such a way that a closed loop is created on any of the wires (the ends of the individual branches must never be connected to each other; the common GND wire must not be connected either).

The JA-110Z Bus splitter can be used for Bus branching. It is manufactured in four versions: JA-110Z, JA110Z-B, JA110Z-C and JA-110Z-D. The JA-110Z is supplied in a surface-mounted installation box and is equipped with front and rear tamper contacts to prevent unauthorised manipulation. It occupies one position in the system. Terminals of the same colour are always connected on the splitters. Variants A and B are dimensioned for installation in the JA-190PL multi-purpose mounting box. Variant C is dimensioned for installation in the KU-68 standard electrical installation box.

Connection terminal block variants:

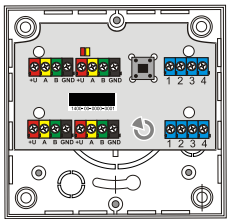


Figure 25 – JA–110Z

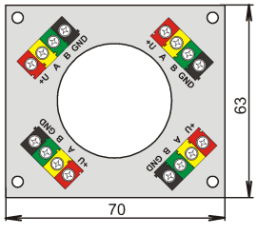


Figure 26 – JA–110Z–B

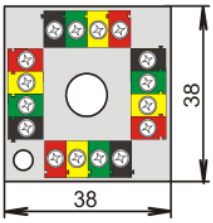


Figure 27 – JA–110Z –C

3.2.4.3 Calculation of voltage drops and consumption

Voltage drops on the line are based on the resistance of the line, which is determined by the conductor (cable) used and the current consumed. The current consumption of the components can be found in the individual instructions. From these values, it is possible to calculate the voltage drop on the line and determine whether there will be sufficient voltage at the last installed device. The calculation is performed using Ohm's law **U = I * R**.

CC-01 cable (power pair)		CC-02 cable		CC-03 cable (power pair)		CC-11 cable (power 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
NOTE: The data in the table assumes the worst-case scenario, i.e. that the total consumption is at the end of the cable.							

Table 23 – Voltage drops and consumptions

When normal operating conditions, the voltage at the +U and GND terminals is almost 14 V. For the calculation, consider a situation where the control panel is powered only by the battery and the voltage is close to 12 V. The voltage at all appliances must be greater than the minimum permissible voltage of 10 V. For the connected devices to function properly, the maximum permissible drop is 2.0 V.

The cause of unexpected voltage drops may be terminal connections with poor contact (transition resistances).

Voltage drops on individual addressable devices can be verified using the F-Link software on the Diagnostics tab. Non-addressable devices (e.g. PG output modules) do not have this option; the check must be performed using a measuring device.

We recommend always verifying the correct calculation and connection in a real installation by measuring at the terminals. For components with high power consumption (siren, keypad, relay output), perform this measurement at a time of increased consumption (active siren, backlit keypad, switched relay).

In simple terms, the limitations listed in the table apply (see Table 23).

To calculate the total load on the cables, add up the consumption for the cable selection (found in the manuals for the individual devices).

3.2.4.3.1 Example of calculating voltage drop in a simple installation

1. Determine the current consumption of individual devices (from the technical parameters of the product – Current consumption for cable selection).
2. Determine the cable lengths. It is necessary to know the exact length of the cable from node to node.
3. Draw a diagram with the cable lengths and consumption on each branch.
4. Calculate the current flowing through each branch.
5. Compare the estimated cable length and current estimate for the branches according to the table (see Table 18) to determine the suitability of the cable selection.

Subtract the individual voltage drops from the power supply to determine the voltage at the end of the line. Always assume a voltage of 12 V from the control panel for operation during a power failure.

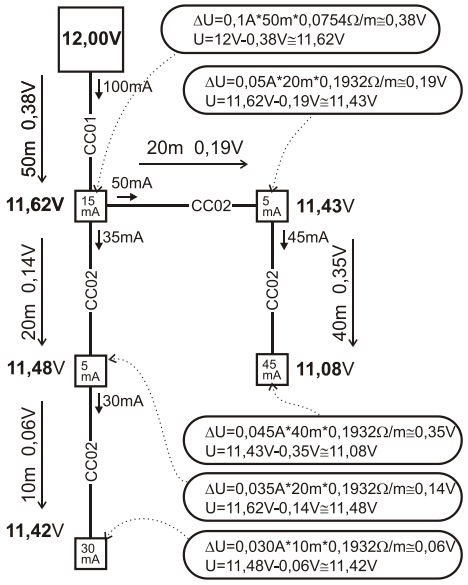


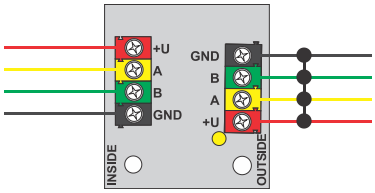
Figure 28 – Calculation of voltage drop (example)

3.2.4.4 Bus separation

Bus sections routed through unguarded areas must be protected against possible short circuits or other attempts to disable the system by separating the Bus using a JA-110T isolator. This module can be placed in a JA-190PL multipurpose mounting box. The isolator also works as a data repeater on the Bus. It is powered from the Bus, does not occupy any position, and allows the Bus branch length to be extended by another 500 m. Separators must never be placed in series in the device communication route in such a way that any device communicates with the control panel via two separators.

An example of use is the Bus connection for relay modules controlling, for example, roller blinds or sirens, to which the Bus is connected in such a way that it is accessible from the outside for possible attack. For more information, see the JA-110T manual.

Bus routing from the control panel



Any possible damage to the Bus behind the module (e.g. due to a short circuit) will not cause disruption to the Bus in front of the module!

3.2.4.5 Use of existing cabling during renovations

- For laying new wiring, it is advisable to use CC-01, CC-02, CC-03 and CC 11 cables.
- When installing on SYKFY 3x2x0.5 cables, it is necessary to connect the Bus data wires (A, B) to one selected twisted pair. For power supply (+U12, GND), it is possible to connect the corresponding wires of the remaining two pairs (double within the pair).
- When installing on UTP cables, it is necessary to connect the Bus data wires (A, B) to one selected twisted pair. For power supply (+U, GND), it is advisable to connect (double) the corresponding wires of the other pairs of wires.

WARNING: If a shielded cable is used, do not connect the shielding to the Bus terminals! We recommend connecting all shielding to an auxiliary terminal in the control panel and not connecting it anywhere else. The other end of the shielding on the device side should also be left unconnected.

3.2.5 Installation of wireless devices

The JABLOTRON system can use wireless devices from the JA-15x, JA-16x and JA-18x series. The installation of these wireless devices places higher demands on their assembly, especially in terms of understanding and experience with radio signal traffic.

WARNING: The operator of the alarm system is responsible for the operation of wireless devices. The system must comply with ERC-REC 70-03 rules and local regulations. Jablotron wireless devices comply with European requirements and their use may be restricted in some countries.

Wireless devices must be positioned in accordance with the installation manual for the specific product. When designing the layout, it is necessary to take into account in particular:

- distance from the control panel or the nearest radio module,
- obstacles and structural elements of the building that may attenuate the RF signal,
- restrictions imposed by the type of equipment installed (mounting height, orientation, IP protection),
- recommendations for testing signal quality after installation.

The JA-11xR radio module must be used as the basic for communication with wireless devices. The system can have a maximum of 3 radio modules, and the first one is usually installed in a holder located in the control panel cover.

If the wireless devices do not have a sufficient signal to communicate with the main radio module, up to two additional radio modules can be added to the building. These are connected to the control panel via a Bus.

Another option for extending the radio range is to use the JA-151R wireless repeater, but its use has limitations; please refer to the user manual for this component.

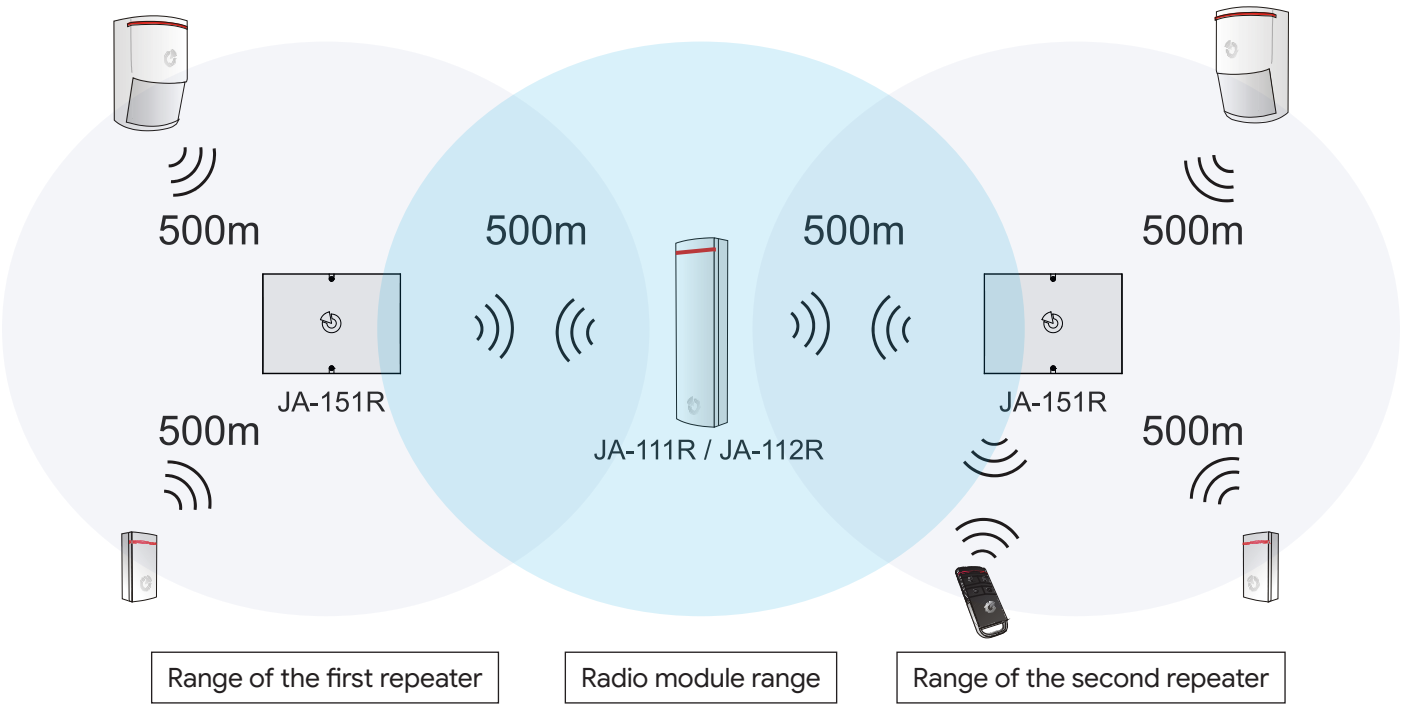


Figure 30 – Installing wireless devices

When installing individual devices, always follow the instructions in the user manual.

Wireless devices must be "enroled" to the system by inseting the batteries or assigned by entering their serial number. This process is performed in the enrolment mode exclusively using a computer and F-Link software (see 4.2.3.1).

NOTE: A maximum of 120 wireless devices can be taught to the JA-107K control panel, and they can only be enrolled to positions 1 to 120. Positions 121 to 230 are only for Bus devices. The JA-11xR radio module programmed be programmed in the range of positions 1 to 120.

Some wireless devices can operate without occupying a position (e.g. selected PG modules). The enrollment procedure is always specified in the installation manual for these wireless devices.

3.2.5.1 Installation of the JA-11xR radio module:

NOTE: The JA-11xR radio module is not part of the control panel, but may already be installed in some commercial kits. For more information, contact your distributor.

- The JA-11xR radio module is placed in the holder in the lower right corner of the control panel or can be installed outside the control panel in a separate PLV-JA111R housing.
- If the control panel is installed in a location with a weak GSM signal, the GSM module increases its transmission power, which can negatively affect the range of radio communication in the system. In such a case, it is recommended to place the radio module outside the control panel, at least 2 m away from it, where radio communication will not be negatively affected and the communicator will operate in optimal mode.

The connector for connecting the radio module on the JA-103K and JA-103K-7AH control panel board is designed exclusively for connecting one radio module located inside the control panel box.

- A larger area can be covered by the radio signal by installing up to 3 radio modules (hereinafter referred to as radios) in different locations (e.g. each on a different floor). The signal from the wireless device (hereinafter referred to as device) can be picked up by several radios at the same time. The control panel communicates with individual radios cyclically, so it receives the information sent from

the device from the radio that was the first to pick up an intact signal and responds to it. It does not receive the same information from other radios, even if it was received with a stronger signal.
- In the case of two-way devices, the control centre reserves the channel once it has been used (communication by the first radio)reserves the channel and continues to communicate with the given device only through this radio module (shown in Diagnostics, Channel column) until the device stops responding. It then searches for a signal for connection on other radio modules. To check the connection quality from individual devices to individual radios, you can use the RF signal function in the F-Link software (button on the top bar of the software). Here, select the radio on which you want to verify communication and activate the devices to be verified. The communication graph shows you the signal strength measured by a specific radio. You can have measurements open on multiple radios at the same time, making it easy to verify the radio signal coverage of the building.
- Mount the radio module vertically on the wall. It must not be near objects that shield or interfere with communication (metals, electronics, cables, pipes, etc.).
- When installing the system, you must first enroll the radio modules. Only then can you assign wireless devices.

RECOMMENDATION: Wireless devices should only be enrolled into the system after they have been placed in their final position. Although this procedure is less convenient for installation, it ensures greater reliability of the connection with the radio module after the alarm system is put into operation. The radio module has a mechanism for measuring the minimum signal from the device during service mode. This provides a reserve in case of the radio conditions are getting worse during live operation (e.g. minor changes in building layout, increase in industrial interference in the vicinity, etc.). For more information, see EN 50131-5-3.

3.2.5.2 Registration and placement of wireless devices

Wireless devices can be enrolled in the system in two ways:

- using the "Enroll" function in the F-Link software,
- by manually entering the serial number of the device indicated on the manufacturer's label.

After enrolling the device, the control panel will automatically attempt to establish radio communication and evaluate the quality of the RF signal quality. Proper enrollment procedures and appropriate placement of devices are key to ensuring stable communication and minimising faults caused by RF signal loss.

3.3 Commissioning

The alarm system is put into operation in accordance with general safety principles, local regulations and technical specification EN 50131-1.

Procedure:

1. Check the Bus cable connections.
2. Verify that the microSD card is inserted in the holder on the control panel board.
3. Check that the power supply is correctly connected to the control panel and that the power cable is securely fastened.
4. Insert the battery into the control panel and secure it in the cabinet with tape.



Caution – the backup battery is supplied in a charged state and must not be short-circuited! Only use batteries designed for backing up the JABLOTRON security system control panel. Installation and replacement may only be carried out by a certified installation technician.

5. Connect the battery leads. Ensure correct polarity! (red lead to + pole, black to – pole)
   - switch on the mains power, the green LED flashes to indicate Bus function and monitor the LED in the control panel:
   - the green LED flashes (Bus function).

Only when using a GSM communicator:

- the red LED flashes – logging into the GSM network is in progress.
- the red GSM LED goes out – the control panel has established a connection to the GSM network.
- the red LED is lit continuously – the control panel has not logged into the GSM network.

Once the connected Bus devices start flashing yellow, enroll them to the system (see 4.2.3.1 Assigning or removing devices).

6. ConFigure the keypads, see 4.2.3.2 Keyboard configuration.
7. Set the required functions (see 4.2.7 Parameters).
8. Perform a functional test of the entire system, including external communication with the ARC, and record the results (functional test report) after the test. Follow the recommendations of CLC/TS 50131-7.
9. **To comply with EN50131-1 or INCERT, Grade 2, disconnect the USB cable from the control panel PCB.**
10. Prepare technical documentation for the installed alarm system.
11. Proceed with the handover of the alarm system to the operator/user; this step is part of the commissioning process.

3.3.1 Handover of the system to the operator/user

After completing the installation and testing of the alarm system, it is recommended to prepare documentation (handover protocol, alarm system operating manual, etc.) containing information on the number and location of the components used, such as detectors, sirens, individual keypads, their segments and their assigned functions. The system user must also be properly trained and instructed on the following points:

- Control from the system keypad. Setting and unsetting individual sections (from segments or from the menu).
- Verifying sufficient exit and entry delay times. Exit via the garage, gate, etc.

1. Explanation of the importance of secure authorisation. Authorisation options (codes with or without a prefix, cards, chips).
   - Partial setting for home surveillance. Difference in signalling between partial and total setting.
   - Use of segments to control automation functions or to trigger a panic, fire, medical assistance in companies, etc.
   - From the set state of the section, alarm triggering including sirens, testing of alarm call reception.
   - Explanation of the difference between cancelling an alarm by authorisation and unsetting a section.
   - Remote control of sections by calling the voice menu with voice navigation.
2. Control of sections and automation PG outputs used by defined commands via SMS message.
3. Control using the MyJABLOTRON application on the web or on a smartphone, demonstration.
4. User code changes via keypad or JA-100-Link software.
   - Presentation of JABLOTRON Security services together with a security SIM card.

Do not forget to agree with the customer on regular annual paid service inspections, during which the functionality of the entire system, including all devices, is regularly checked and a document of the work performed for the insurance company. The system can automatically notify the customer of this regular inspection using the customer's LCD keypad.

4 System configuration

The alarm system can be divided into several independent sections as a single unit (building). Each section can be guarded either as a whole or only part of it (partial setting). If the system is partially set, detectors with the "Internal" flag do not guard.

The basic protection is the so-called perimeter protection of the object, which monitors, for example, the opening of entrance doors, garage doors, windows, balcony doors, rear or roof entrances. Perimeter protection includes not only magnetic opening detectors, but also glass break detectors, shock detectors, infrared barriers, etc. Except for entrance doors and garage doors, which are usually connected with a delayed reaction, other detectors are mainly connected with an instant reaction.

Another type is so-called space protection, which detects movement in the building using motion detectors (PIR) or a combination of these with other detectors. In addition to motion detectors in entrance zones, which are assigned an optional entry delay (delayed or next delay reaction), other detectors in the building are usually programmed to instant reaction. The option to choose from up to three delay times allows you to create access routes (e.g. longer delay when entering through the garage).

Object protection is used not only to guard valuables or safes, but also to detect break-ins by brute force, e.g. sectional garage doors with the possibility of damage without opening. Object protection includes tilt and shock detectors, but common magnetic opening detectors are also used, typically as a distance sensor.

The protection of individual security devices of the system is provided by tamper detectors, which indicates unauthorised manipulation of the devices.

Environmental protection mainly includes fire detectors, combustible and toxic gas detectors, but also flood detectors. All these detectors usually have an adjustable reaction, either continuous or 24-hour (fire, gas, flooding).

4.1 System activation

The JABLOTRON system is set up exclusively by computer using the F-Link software. The current version of the F-Link software is obtained by updating from the JABLOTRON server or can be downloaded after logging in from the MyCOMPANY web interface at www.myjablotron.com.

Immediately after launching the initial window for selecting the connection, the F-Link software can be switched to the appropriate language environment by clicking on the language change icon (flag). This change can be made at any time later. The initial window offers the following options:

1. **Local connection** – a USB cable (with A-B connectors) is required to connect the computer to the control panel.
2. **Remote connection** – offers a selection of databases from stored files and allows you to establish a remote connection.
   To establish remote communication with the control panel the computer must have access to the internet and a GSM communicator must be installed in the control panel. The SIM card used in the communicator must have GPRS data transmission activated. For a trouble-free connection, other requirements must be met, such as remote configuration enabled in the control panel, the correct registration code, knowledge of the service code, but also sufficient GSM signal at the control panel location or connection to a LAN network.
3. **Offline settings** – allows access to information about the control panel settings. This allows you to access, for example, a list of devices or notes about the last battery replacement, etc.

SW F-Link also allows you to change the control panel language for communication with users. The language refers not only to the texts displayed on the LCD keypad or messages sent to users' mobile phones in the form of SMS messages, but also the voice menu of communicators that communicate with the user. Changing the language in the control panel deletes all texts in the system, so it is necessary to perform this option as the first step, before installing and naming devices, sections or users.

The JABLOTRON system is delivered from the factory preset to the communication language "English" with the option to select to "Czech". However, it is not possible to freely select other languages in the control panel; the selection is limited to languages specific to the region where the system is exported. A trained installation company with an account on the MyCOMPANY web interface www.myjablotron.com can request a code to unlock another language. To generate the language code, you need to know the registration code of the control panel.

4.1.1 Connecting the control panel to the system

1. Connect the computer to the control panel using a USB cable – the computer will initialise the new USB device (this may take longer when connecting the control panel for the first time).
2. After connecting, Disk Management displays two newly found disks: FLEXI_CFG and FLEXI_LOG. Close Disk Management if they are displayed.
3. Launch the F-Link software. If the control panel has its original factory settings, the Initial setup tab will open and the system will automatically switch to Service mode. If the control panel has already been set up (its service code has been changed), the software will ask you to enter the code – it is entered in the format nnnn. If the prefix is enabled (on the Range tab in F-Link), it is 0*nnnn (0*1010). The Remember option saves the entered code until the database is closed. The Show code option is used to check the code entered, e.g. when using an alphanumeric keypad, where errors may occur.

NOTE: Once a connection has been established via the USB cable, it is not possible to program changes to the settings from the LCD keypad because the Settings item is blocked in its menu. After disconnecting the cable, the item reappears in the menu within a few seconds.

4. After successful authorisation, the following message may appear:

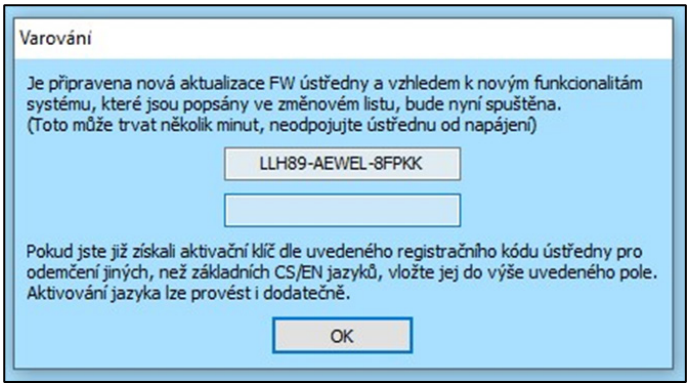


Figure 31 – System message (F-Link)

5. In this case, we recommend performing the update. After confirming the button, a new firmware package will be downloaded, which may take several minutes. After the update is complete, the first page of the Wizard with the Initial setup tab will appear.

4.1.2 Starting the Wizard

1. Set the desired parameters in each tab and click the "Next" button. If you accidentally skip a setting, you can move backwards in the wizard and between the tabs you have programmed already.
2. After setting the last tab, press “Save” and exit the wizard by clicking “Close”.
3. After exiting, you will be asked if you want to run the installation wizard the next time you start the F-Link software.
4. You can exit the wizard at any time during setup by pressing the "Close" button.
5. The wizard can be restarted independently at any time in the Control panel / Installation Wizard menu.

4.2 F-Link tabs

This chapter describes the individual tabs of the F-Link software, which are used for comprehensive configuration of the JABLOTRON system. Each tab represents a specific area of settings – from basic system design, to user editing and device enrollment, to advanced communication parameters and diagnostic tools.

4.2.1 Initial setup

This tab is used to set the basic size of the system. The programmed data can be changed at any time. The range values affect the size of the database and thus the time required for loading and saving data (mainly via remote access). It is not necessary to be in Service mode to make changes in this tab. When you start the F-Link software for the first time, the wizard will guide you through the setup of all system parameters.

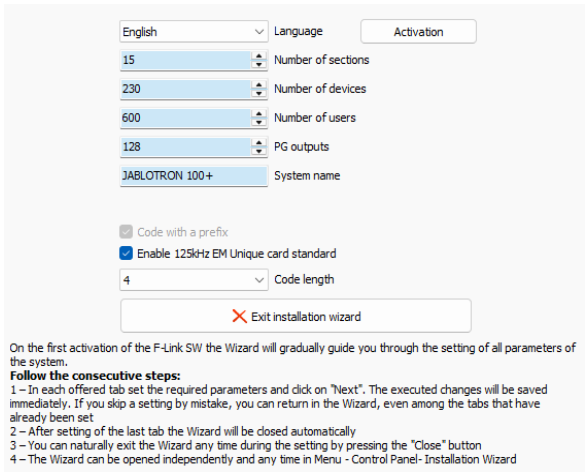


Figure 32 – JA–107K Initial setup with guide (F–Link)

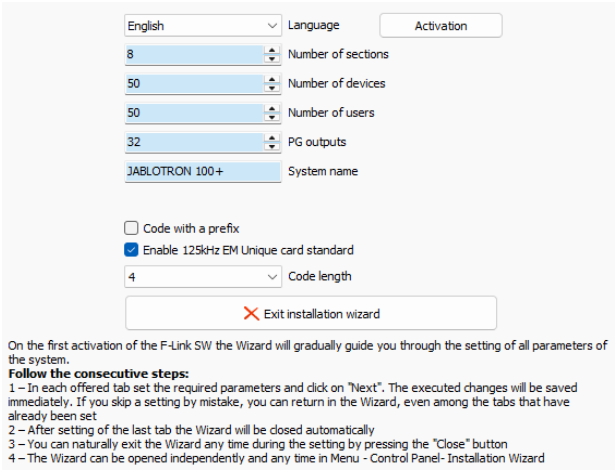


Figure 33 – JA–103K initial setup (F–Link)

Description of the Initial setup tab:

Codes with prefix – This function determines how all access codes are entered during user authorisation. When this function is enabled, the system requires a one- to three-digit code number (prefix) ending with an asterisk (e.g. 12*3456) to be entered before the access code. In this case, users are allowed to change their codes freely from the LCD keypad. When this function is disabled, only the access code is entered during user authorisation. In this case, all codes can only be assigned and changed by the System Administrator, who must prevent two users from having the same code.

WARNING: Disabling this parameter will irreversibly delete all user codes and reset the Service code and Administrator code to their factory defaults. User permissions and chips/cards of registered users will be retained.

Enable EM UNIQUE 125kHz standard cards – if this function is not enabled, only the types of chips and cards recommended by the manufacturer (JA-190J, JA-191J, JA-192J, JA-194J) can be used for user authorisation. When this function is enabled, cards from other manufacturers operating at the specified frequency are also enabled.

Code length – To increase the security of the system control, codes can be 4, 6 or 8 digits long, with or without a prefix. When changing the code length setting, all used codes are deleted and only the factory codes are set.

4.2.2 Sections

Define the properties of independently controlled guarded sections. It is not necessary to be in Service mode.

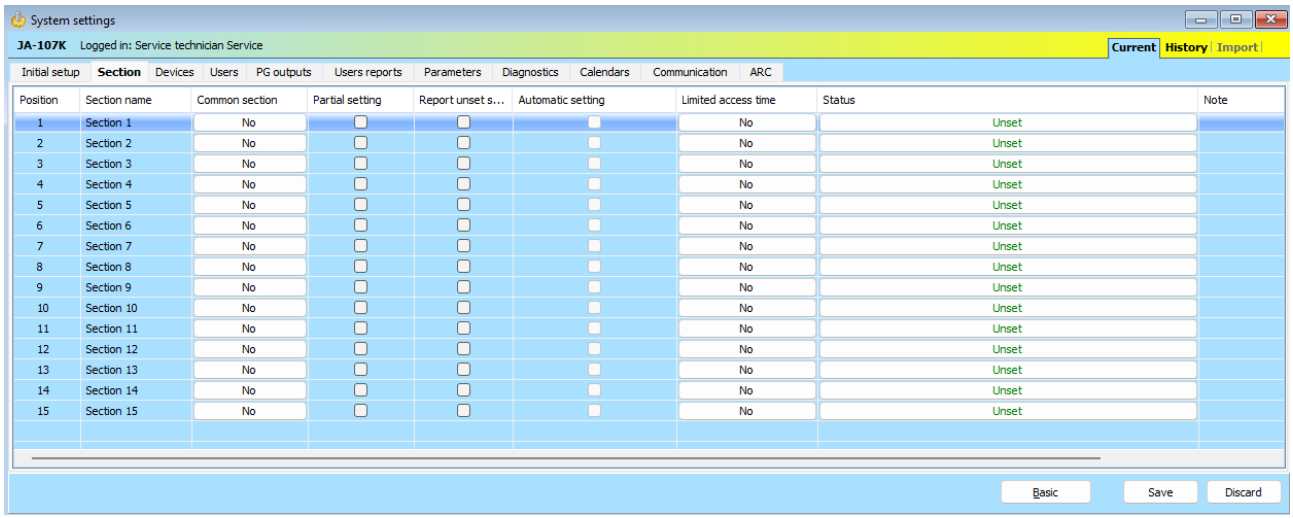


Figure 34 – Sections (F–Link)

** Items marked in this way are only displayed if Advanced Settings is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire F-LINK to basic/advanced settings).*

Section name – Section names are used for clarity in text event reports (SMS messages), in the event memory log, and in the LCD keypad display (e.g. Ground floor, Shop, etc.).

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

Partial setting* – Allows you to partially set a section if someone remains inside (detectors will not be set that are programmed to respond to the Internal type – see 4 System configuration). Without enabling this parameter, partial setting can be used in the section.

Report unset section* – If the section is unset and no detector is activated in it during the set time, a report "Unset section" will be sent. The time is defined in the Parameters tab – Report unset section tab (60 to 2,880 minutes); for details, see 4.2.7 Parameters.

Automatic setting – Used to automatically set the section in which the "report unset section" report occurred. In the Control Panel Parameters tab, you can program the time interval in minutes after which automatic arming will occur. The time interval begins when the "Report unset section" report is sent. This function is an addition to "Report unset section" and can only be used if the "Report unarmed" function is enabled.

Time-limited access* – Allows you to program a weekly calendar allowing selected users to unset the section. For details, see 5.11.1 Time-limited access of users.

Status – The button indicates the current status of the section (Unset, Set, Exit delay, Entry delay, Partially set, Alarm, Alarm memory, Disabled, Service mode). Pressing the button allows you to control the section according to the permissions set for the login (changes the status to fully set or unset).

Note – Allows you to describe the details of the section for easier orientation during annual inspections, etc.

4.2.3 Devices

Used to assign installed devices to the system and set their properties. The tab displays as many positions as you select in the Initial setup tab. The control panel is automatically assigned to Position 0 in Section 1 and cannot be moved or deleted. To make changes in this tab, you must be in Service mode.

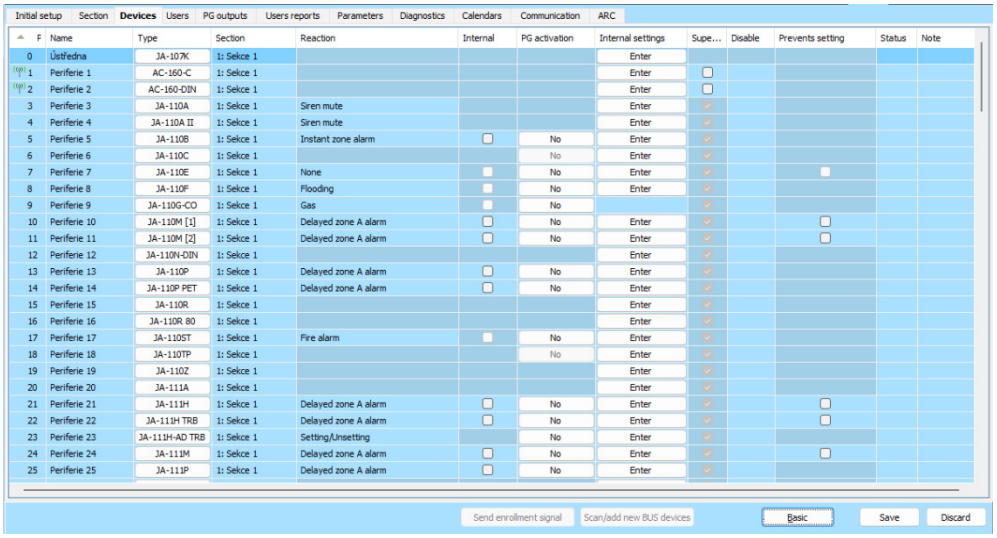


Figure 35 – Devices (F–Link)

** Items marked in this way are displayed when Advanced Settings is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire F-LINK to basic/advanced settings).*

Name – used in text event reports and memory listings (e.g. Main door).

Type – displays the type of enrolled device: Unoccupied position allows you to enrol a new device. For enrolling devices, see 4.2.3.1 Assigning or removing devices.

Section – determines to which section the device will report events (alarm, tampering, malfunction, etc.).

NOTE: For dividing an object into sections, see 4.2.2 Section.

Reaction – determines what reaction is triggered when the device is activated. If the device does not have an alarm input (e.g. Bus access module), no reaction can be assigned to it. A complete list of reactions for devices is displayed if Advanced Settings is enabled. A description of all reactions can also be found at 2.8.6.1 Overview of configurable peripheral reactions.

Internal* – this parameter is only available for intrusion detectors. Signals from devices marked in this way are not taken as alarms if the section is partially sect. Configuration of the section to be set partially see4.2.2 Section . If partial setting is not enabled for the section, this parameter has no effect.

Activates PG* – activating the device can also activate the preset reaction of the programmable PG outputs. This option is linked to the PG outputs / Activation / Devices item.

Internal settings – access to the internal parameter settings of devices that are connected to the Bus or have bidirectional wireless communication. Individual devices have different internal parameters (some have none). The internal keypad settings are also described at 4.2.3.2 Keyboard configuration . For other devices, see their manuals.

Supervision* – allows you to disable regular communication checks with wireless devices (cannot be disabled for Bus devices). This function is always enabled by default for wireless devices, except for remote controls and panic buttons.

Disable – Devices can be deactivated at three levels, depending on authorisation:

- **Input blocking** (yellow dot) is used to permanently switch off the detector input (shortcut BLK). The system ignores device activations = it does not trigger an alarm or PG activation, but tampering and faults are still monitored.
- **Device disabling** (red dot), used to permanently switch off the detector (shortcut Disabled). The system ignores all devices functions = it does not report an alarm, fault, PG activation, tampering, report, etc.
- **Tamper detection blocking** (blue dot) is used to swicth off the evaluation of tamper contacts (shortcut TMP). The system ignores the opening of the detector and its detachment from the rear cover = does not report tampering

The control panel and devices with the Panic reaction cannot be switched off or blocked.

Status – indicates the current status of the device. OK = everything is OK, TMP = tampering, ACT = alarm input activated, BLK = blocked, Disabled = switched off, ERROR = malfunction, ?? = device does not communicate, NO AC = AC power failure, Battery = battery in device or control panel discharged or disconnected, BUPFLT (Charging) – backup battery in the device or control panel is charging, BOOT = status when the device is being upgraded or if the upgrade did not complete successfully (repeat the upgrade). Move the mouse over the device STATUS to display detailed information.

Note – Allows you to describe the details of the device, e.g. location, last battery replacement date, average strength of the of the RF signal during the last test, etc.

4.2.3.1 Enrolling or removing devices

In order for the installed device (detector, keypad, siren, key fob, etc.) to function, it must be assigned a position (address) in the system. Some devices occupy multiple positions after enrollment (multiple input modules, expanders, etc). There are also devices (PG output modules, status indicators, separators and Bus splitters) that do not occupy any position. For details, refer to the manual for the relevant device.

- Devices are enrolled using the F-Link software, Devices tab, **Enroll** button. Enrolling is only possible in Service mode..
- Devices can be enrolled in several ways:
  - **by pressing the tamper switch of the Bus device = closing the cover** (some devices can be enrolled by pressing a button – see the manual of a specific device), =

- **by insertion of the batteries to the wireless device** – however, at least one radio module must first be enrolled; for JA-18xJx remote controls, connecting the battery can be replaced by pressing and holding down two buttons (forming a pair); JA-15xJ and JA-16xJ remote controllers are enrolled by pressing any button; wireless access modules (keypads) can be enrolled by pressing the illuminated activation button
- **by entering the serial number in the SN** – Production code field (located under the barcode on the PCB inside the device, e.g. 1400-00-0000-0123); the number can also be scanned with an optical barcode reader; it is then advisable to activate the detector to verify its correct enrollment,
- **selectively by scanning the Bus for not enrolled devices** – if one or more not enrolled devices are connected to the Bus, then after pressing Enroll button, then Scan/add new Bus devices button is displayed in the Device information window, which offers to assign the Bus devices; Enrolling is performed by double-clicking on the selected item,

- **Bulk scanning of not enrolled Bus devices** – if one or more not enrolled devices are connected to the Bus, pressing the Scan/add new Bus devices button on the bottom bar of the window will perform a bulk enrollment of Bus devices. During this procedure, it is not possible to specify the position of individual devices.
- Devices can be removed by deleting the serial number (only the device itself will be deleted) or by selecting the relevant row in the Devices tab and choosing Delete from the right-click menu or simply pressing the Delete key, which will delete the entire device row (including its section settings, response, PG output control, notes and other options). In this way, after selecting multiple devices (click+Shift or click+Ctrl), you can perform a total deletion or just change a common parameter.

NOTES:

- Not enrolled Bus devices flash yellow. If an not enrolled device does not start flashing a yellow LED within approximately 180 seconds after turning on the control panel power (initialisation is in progress), check that the device is connected correctly.
- Wireless devices with one-way communication do not have any means of signalling the enrollment request.When you enroll a device to the system using the above procedure, the next position is automatically offered. You do not need to step through the process, just assign the devices in the selected order. Automatic shifting can be cancelled in the device enrollment window.
- If you re-enroll an already enrolled device to another position, it will automatically move to the newly enrolled position.
- If a device occupies more than one position, it will automatically occupy the corresponding number of consecutive positions with a single enrolment (e.g. the JA-112M module, which has two alarm inputs, will occupy two positions). Please note that unwanted overwriting of devices in other positions!
- If you enroll the device to the highest possible position, the gradual enrollment process will end.
- Free positions are factory assigned to section 1. The section selection can be changed later.
- Free positions are factory assigned to section 1. The section selection can be changed later.

For multi-position devices such as JA-116H, JA-118M, JA-150M, etc., after enrolling them, when they occupy the appropriate number of positions, you can limit the number of occupied positions by deleting position rows. You can then use these to assign other devices. To delete, click on the relevant position row (NOT on the button in the Type column) and press Delete on your PC keyboard.

4.2.3.2 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 connected.
- Enroll the keypad to the selected position in the system (see 3.2.4 Installation of bus devices).
- Entering the internal settings of the keypad (Devices tab) opens the following card (the example is for the JA-114E keypad; for other keypads, the range of settings may be smaller).

Internal keypad settings:

4.2.3.2.1 Segments tab

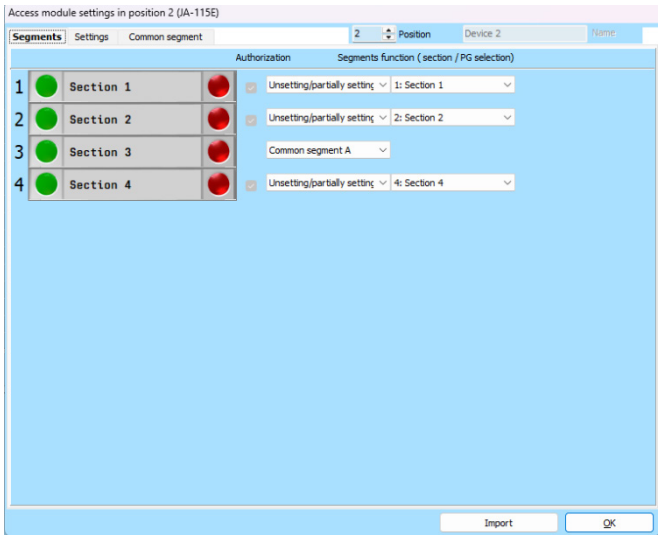


Figure 36 – Keypad segments (F–Link)

Background colour selection – allows you to change the background colour of the segment labels

Set/unset padlocks – enables the display of padlock symbols for segment buttons controlling section monitoring and wheel symbols (empty/full) for controlling PG outputs. The symbols are taken into account when printing labels.

Control segment label texts – displays the Section name (from the Section tab) or PG output name (from the PG outputs tab). You can edit your own label for printing by clicking on the relevant text. To print labels in segments, use the Print labels button (at the bottom of the tab bar).

Print labels – allows you to print labels with preset texts directly on an installed printer. Texts can be edited by clicking on the segment, which saves the changed texts to the database and simultaneously writes them to the cloud in the MyJABLOTRON application. The PT-P700 label printer from the JABLOTRON range offers advantageous use, allowing automatic cutting according to the required label size.

Import – the import button allows you to copy the keypad settings according to another identical keypad in the system, for example if the property has multiple entrances and all keypads need to have the same functions. Copying is only possible from keypads of the same type. You can also use this function when replacing a faulty keypad with a new one. The Import button will show you the history of the last keypad settings for the given device position.

Authorisation – user authorisation is required to set and unset section (system). After disabling the parameter, segments can be controlled without authorisation, with the exception of the Unsetting section function, for which authorisation is always required. For controlling PG outputs, the authorization parameter applies to both states (ON and OFF with or without authorization).

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

Function	Description
None	Segment switched off, reserved for future use
Unsetting / Setting	Section control. Segment indication: section unset = green, set = red.
Unsetting / Partial setting	If enabled (in the Section tab), it allows partial setting of the section. Segment indication: section unset = green, partially set = yellow,
Unsetting / Partial setting / Setting	Allows you to select the level of setting. Pressing the right button (Set) once offers partial setting, pressing it again offers full setting. For this option, the section must have partial setting enabled in the Section tab. Segment indication: section unset = green, partially set = yellow, fully set = red.
Section indication	The segment only displays the status of the section; it does not allow its control (suitable , for example, for signalling the status of common sections, staircases, etc.). In the event of an alarm, it can be cancelled by pressing the green segment button and subsequent valid user authorisation.
Panic	**The segment allows you to trigger a silent panic alarm. After pressing the right button, a panic report is sent without an acoustic signal from the section to which the function is assigned. The panic can also be delayed with an adjustable time and the option to cancel before the time expires. A set section will not be unset.**
Fire	The segment allows you to trigger a fire alarm. When the right button is pressed, the segment flashes red for three seconds (during this time, the action can be cancelled by pressing the Unset button). A fire alarm is then triggered from the section to which the segment is assigned.
Audible panic	**The segment allows you to trigger an audible alarm. When pressed, an audible panic alarm is triggered from the section to which the segment is assigned. The audible panic alarm can also be delayed with an adjustable time and the option to cancel before the delay expires (Delayed Panic Alarm). A set section will not be unset.**
Medical troubles	The segment allows you to send a medical problem report (without siren alarm). After pressing the button, the segment flashes red for three seconds (during this time, the action can be cancelled by pressing the Unset button). The segment then returns to its idle state and the system sends a Medical problem report from the section to which the segment is assigned.
PG OFF/ON	This segment allows you to control the PG output. Indication: PG inactive/off = green, PG active/on = red.
PG ON	The segment can only be used to switch on the PG output (e.g. switching on lights for a preset period of time).
PG OFF	This segment can only be used to switch off the PG output (e.g. emergency STOP button function).
PG indication	The segment only indicates the status of the PG output, without the possibility of control (red indicates active status)
PG indicates inversely	The segment only indicates the status of the PG output using inverted logic (green indicates active status), without the possibility of control
Common segment A / B	Allows simultaneous control of multiple sections with separate segments on the keypad using a single segment. Pressing the button on the common segment performs a collective Unset/Set for the selected section segments. If some sections controlled from the Common segment are set and others are unset, using the Common segment will unset/set the remaining segments. If any of the selected segments has Partial setting enabled, then the Common Segment will perform the following: 1st press of Set = partial set, 2nd press of Set = full setting. It is not advisable to combine the Common Segment function with the Section/Common Section function. Common segment indication: all sections unset = green, all fully set = red, any set(partially set) = yellow. There can be a maximum of 2 common segments on one keypad. The assignment of sections to a Common Segment is selected in the upper tab Common Segment. *NOTE: The "Common segment x" item is only offered if more than two segments are used to control sections on the module.*
PG indicates/ controls	The segment allows you to control a different PG output than the one it visually signals. With this option, the first parameter selects the PG output for signalling and the second (additional) parameter controls the PG output. This function is used, for example, to control garage doors with a PG output pulse, while the control segment displays the current status of the door read from the door detector.

Table 24 – Segment Functions

4.2.3.2.2 Settings tab

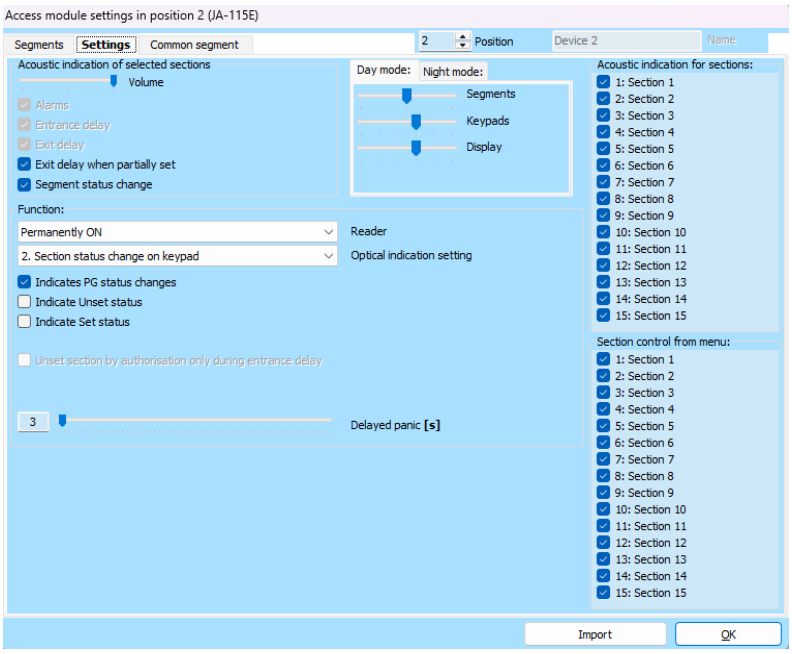


Figure 37 – Keypad settings (F–Link)

Acoustic indication for sections:

Parameter	Description
Higher volume	Adjust the volume of other acoustic indication than alarms
Alarm	Signalling during an alarm (siren sound)
Entry delay	Continuous beeping during entry delay
Exit delay	Slow beeping (1/sec)
Exit delay when partial setting	Slow beeping (disabled by default)
Segment status change	One beep when segment change takes a place

Table 25 – Acoustic signalling of sections

Function:

Adjustable functions	Description / Behaviour of adjustable functions	
Reader	In order to save energy, the reader can be limited to operating for only 3 seconds after its cover is pressed. The reader can also be switched off completely. For wireless keypads and access modules, this setting applies if they are permanently powered from an external power supply; otherwise, their reader always switches off automatically.	
	Permanently on	Permanent reader activation. For Bus keypads, the wake-up setting is ignored.
	Activated by pressing	**Wakes up the reader for 3 seconds after the keypad is activated.**
	Disabled	Reader permanently disabled
	Activated by pressing or authorisation request	Wake up after keypad activation or authorisation request for authorisation

Adjustable functions	Description / Behaviour of adjustable functions	
Optical indication settings	1. Permanently	Bus indicates continuously. Wireless keypad indicates continuously only with an external power supply. Without external power supply, it behaves according to option 2.
	2. Section status change on keypad	**Changes in section/PG status** are indicated only on the given segment. **Entry delay and alarm** are indicated by the entire keypad.
	3. By changing the status of the section – segment	Changes in section status, PG, entry delay and alarm are indicated only on the given segment.
	4. By changing the segment status	**Entry delay and alarm** are indicated only acoustically. **The change in section status and PG** is indicated only on the given segment. This option is preset at the factory.
	5. Entry delay/Alarm on segment	**Entry delay and alarm** are indicated on the given segment. **Changes in the status of the section and PG** are not indicated at all.
	6. Only after pressing	The keypad indicates visually and acoustically only after opening the front cover, pressing a key, segment or front cover.
Indicates PG status changes	Optical indication of PG status changes on the segment. Refers to the programmed optical indication options 2 to 4. If disabled, PG status changes on the segment are not optically indicated.	
Indicates unset status	Keypad segments indicate the unset status without entering a valid authorisation. When this option is disabled, they only indicate this status for the duration of the valid authorisation.	
Indicates set state	The keypad segments indicate the set status without a valid authorisation. When the option is disabled, they indicate this state only for the duration of the valid authorisation.	
Authorisation unsets the section when entry delay	Simply entering the code or attaching the chip unsets the section when entry delay (if the user has permission to do so). With wireless keypads, authorisation can be performed in this way only after an entry delay has been triggered on them. *WARNING: This option should not be applied to the Common section. In such a case, it may lead to the unwanted unsetting of all sections assigned to the common section, or even the entire system (if the unset button is pressed first and then authorisation is performed).*	
LCDbacklight goes off in 5s	When this option is enabled, the display backlight will turn off 5 seconds after the last selection (pressing a key, segment or front cover). If this option is disabled, the display backlight will turn off at the same time as the rest of the keypad. Enabling this option extends the battery life of the wireless keypad.	
Delayed panic	Function for triggering a panic alarm (silent or audible) with an adjustable delay during which the alarm can be cancelled. Activation and deactivation is performed by a segment set to the silent panic or audible panic function. The right button of the segment starts the timing and the left button cancels the timing. If Authorisation is required, it is required for both actions (activation and deactivation). The delay is adjustable from 1 to 255 seconds.	

Table 26 – Keypad Functions

Display on the LCD:

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

Table 27 – Keypad display

Light intensity:

Element	Function description
Segments	LED brightness settings on segments
Keypads	Keypad backlight settings
Display	LCD display backlight settings

Table 28 Keypad LCD display light intensity

NOTE: The brightness can be set differently for day and night mode, and the keypad's acoustic signal can also be muted.

Acoustic indication for sections – allows you to select sections for which the keypad will acoustically indicate alarms, exit and entry delays, PG output control, etc. within the range specified by the previous settings.

Sections control from menu – the LCD keypad can be used to specify which sections can be set and unset from the menu. For example, you can create a keypad that normally controls two sections using segments, but can also control other sections of the house using the menu if necessary.

4.2.3.2.3 Common segment

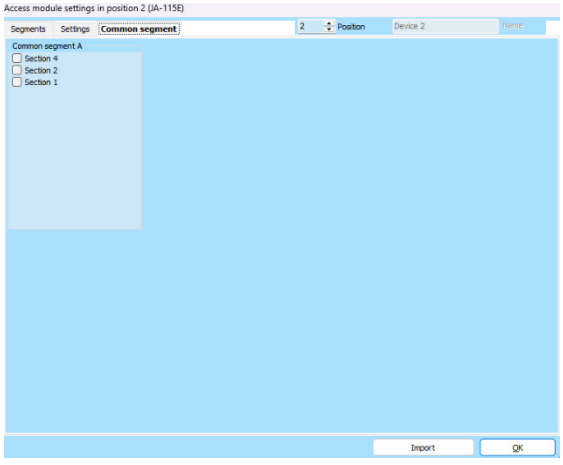


Figure 38 – Common segment (F–Link)

Enables simultaneous control of multiple sections with a single segment. Sections must have separate segments on the keypad. Pressing the button on the common segment will perform a common Unset/Set for the selected section segments. If some sections controlled from the Common Segment are set and others are unset, the remaining sections will be unset/lset after using the Common segment. If any of the selected segments

have Partial setting enabled, the Common segment will perform the following: 1st press of Set = partial setting, 2nd press of Set = full setting. The Common Segment allows you to bypass the active detector in a section with a second press if the way of setting is preset to "Set with warning" or "Set after confirmation" without affecting other segments set to "partial setting with one press and full setting with two presses".

Common segment indication: All sections unset = green, all sections fully set = red, other system status (partially set section, soem sections fully set, some sections unset) = yellow. To determine the sections for the Common segment, select the Common segment tab at the top.

There can be two segments with the Common Segment function on one keypad. A section can be selected for both common segments.

NOTE:

- *The "Common segment x" item is only offered if more than two segments are used on the module to control sections are used on the module.*
- *It is not advisable to assign a section set as a Common Section to a Common Segment.*

4.2.3.3 Internal siren configuration

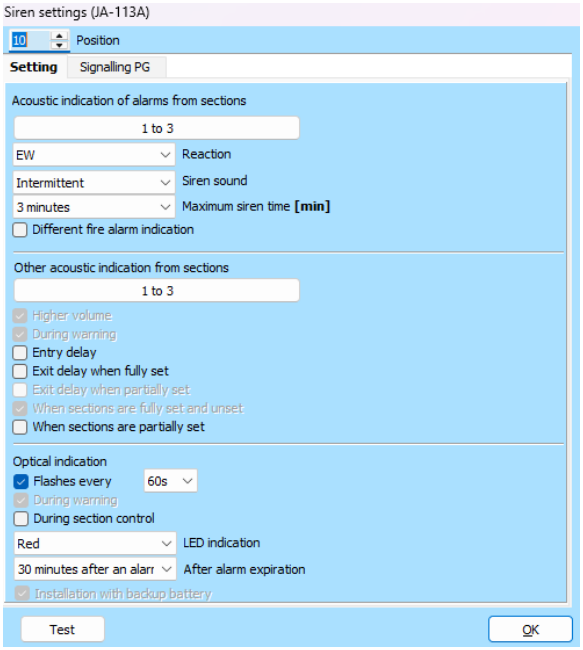


Figure 39 – Internal siren settings (F–Link)

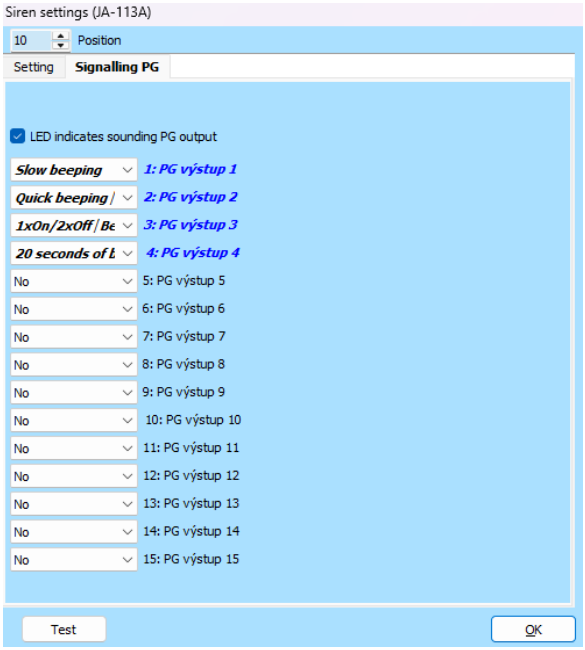


Figure 40 – Sirens – PG indication (F–Link)

Settings tab

Acoustic indication of alarms from sections – selects the sections for which the siren will sound the alarm.

Reaction – selects EW (external warning) or IW (internal warning).

Siren sound – select the type of sound: Intermittent (50/50) / Continuous (continuous).

Maximum siren time – limits the maximum siren time to 1 to 5 minutes (provided that the control panel alarm is longer, otherwise it ends with the control panel).

Different fire alarm indication – when activated, the siren will indicate a fire alarm with a rapid loud beeping sound, not the standard wailing sound used for other alarms, such as instrusion, tampering, or an audible panic. The rapid beeping of the fire alarm is thus unified with the signalling from the fire detectors and the acoustic output.

Other acoustic indication from sections – selection of sections for which other acoustic signals and signalling will be indicated – selection below: when controlling sections, when warning, entry delay, exit delay when fully set.

Higher volume – this parameter only affects other acoustic signalling and PG output sound. It does not affect the volume of the alarm indication.

During warnings – when this option is enabled, the siren beeps 3x if setting is not possible (there is a condition in the system that prevents setting, e.g. a fault or an active detector) or if setting is unsuccessful (during the exit delay, an event occurs that prevents the exit from being completed – e.g. activation of a detector). The last warning option is unsetting with alarm memory (an alarm has occurred in the system).

Entry delay – if this option is enabled, the siren will sound throughout the entire entry delay period.

Exit delay when fully set – if this option is enabled, the siren will sound continuously for the entire duration of the exit delay with fully set – intermittent beeping.

Exit delay when partially set – if enabled, the siren will sound continuously for the entire duration of the exit delay with partial setting – intermittent beeping.

When sections are fully set and unset – when sections are fully set and unset.

When sections are partially set – when sections are partially set.

Optical indication – generally, the duration of the alarm signal on all sirens in the system is determined by the settings in the control panel parameters – alarm duration (length). However, there may be cases where it is necessary to continue optical indication even after the alarm has ended. The settings allow signalling for several minutes after the alarm, up to 1 hour.

Flashes every – this parameter sets a short flash of the optical signalling at a selectable time interval of 1x per 10 to 120 seconds (adjustable in 10-second steps). It can be used as a warning that the object is equipped with an alarm system.

During warning – when this option is enabled, the siren will flash three times if setting is not possible (there is a condition in the system that prevents setting, e.g. a fault or an active detector) or if setting is unsuccessful (during the exit delay, an event occurs that prevents the exit from being completed – e.g. activation of a detector). The last warning option is unsetting with alarm memory (an alarm has occurred in the system).

During section control – 1x setting, 2x unsetting, 3x if there is a fault in the system or after an alarm.

LED indication – sirens are equipped with two-colour LEDs. Depending on the colour of the flasher on the purchased upper part of the siren, it is necessary to select the same colour of LED electronics.

After alarm expiration – in general, the duration of the alarm signal on all sirens in the system is determined by the settings in the control panel parameters – alarm duration. However, there may be cases where it is necessary to signal visually even after the alarm has ended (quick orientation for the ARC agency).

Installation with a backup battery – installation with a backup battery.

PG signalling tab

Acoustic confirmation of a change in the status of PG outputs. Allows you to select from a range of sounds for acoustic signal differentiation, e.g. a different signal for pressing the bell button and a different signal for activating the magnet when the door is opened.

Sound selection options: no, slow beep, fast beep, 1xON/2xOFF, 20 s of beeping, Melody 1, 2, 3, 4.

It is also possible to switch on LED indication.

4.2.4 Users

Creates new system users and defines their permissions. The tab displays as many positions as you select in the **Initial setup** tab. It is not necessary to be in Service mode to make changes in this tab.

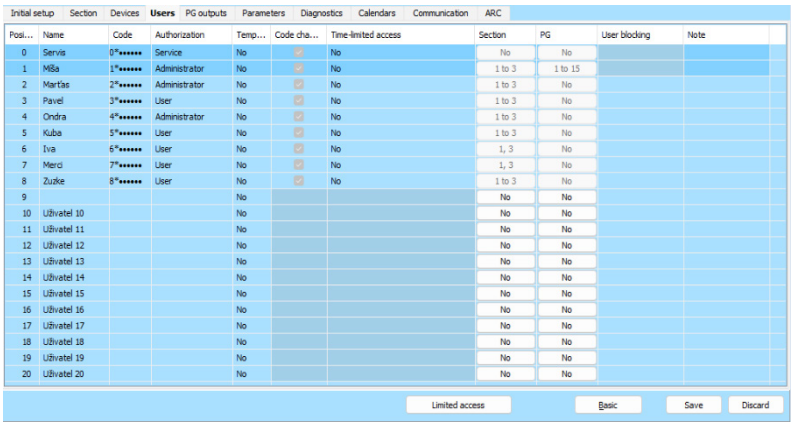


Figure 41 – Users (F–Link)

** Items marked in this way are displayed when **Advanced Settings** is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire F-LINK to basic/advanced settings).*

Name – user names are used in text event reports, event memory listings, report tabs, permission settings, and authorisation on keypads with LCD displays.

Telephone number – used for event reporting, user identification when controlling the system by telephone using the voice menu, or for activating PG outputs by ringing and SMS. The telephone number must always be entered in international format (e.g. +420710123456).

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

Card – used for assigning access cards (chips). Each user can be assigned 2 cards. Cards can be assigned:

- by entering the serial number (can be scanned from the chip using a barcode reader)
- using the JA-190T USB reader by placing the chip on it
- using any keypad by placing the chip on it

Template – allows you to copy all settings according to a template user. Any subsequent changes to the template user settings will affect all users set up according to this template.

Code change allowed* – Allows the user to change their code (not their position number). This function is only available when the Codes with prefix parameter is enabled (Administrator, Service and ARC can change their code at any time).

Time-limited access* – This parameter enables access restrictions for a given user according to the weekly calendar in the Section / Time-restricted access tab, see 5.11.1 Time restrictions on user access can only be applied to users with User authorisation.

Section – Determines which sections the user (administrator) can control. The administrator can also set user codes and cards in the assigned sections. The section cannot be assigned to a user who is only authorised to control PG outputs.

PG – determines which PG outputs the user is authorised to control (if authorisation is set for output control).

System control – This option enables the sending of informational SMS messages about setting and unsetting from the keypad by this user.

Dialling in activate PG – Information window about assigned PG control by dialling in.

User blocking – Option to block a user. Users with positions 0 (service technician) and 1 (main administrator) cannot be deactivated. Deactivation of a user is indicated by a red dot. The Administrator (via LCD keypad or JA-100-Link) and the Service Technician (via F-Link).

Note – Allows you to describe user details, e.g. access permission after working hours, etc.

Limited access – Button on the bottom bar of the window for programming the restricted access function, see 5.11.1 Time restrictions on user access.

4.2.5 PG outputs and activation maps

The PG outputs tab defines the functions of programmable outputs. The tab displays as many positions as as you select in the Initial setup tab. It is not necessary to be in Service mode to make changes in this tab.

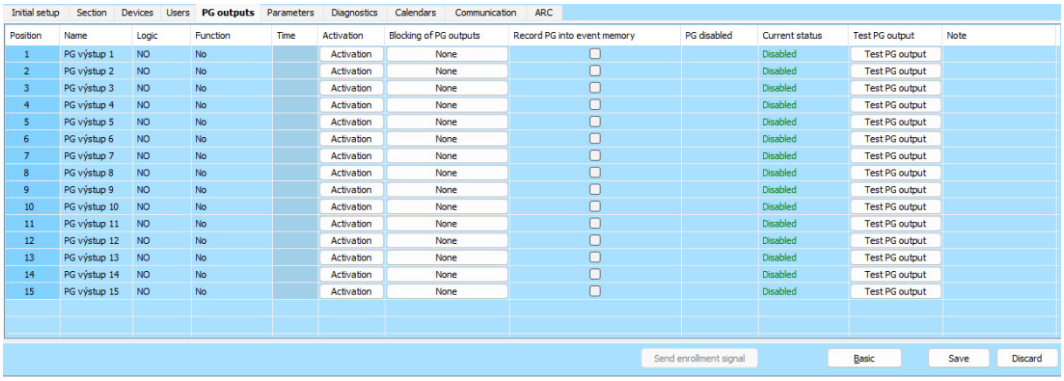


Figure 42 – PG outputs (F–Link)

Name – Output name (e.g. Air conditioning, Storage door, etc.)

Logic – Option to preset the switching or opening logic of the output.

Function – Determines how the output will behave after activation.

PG function	Function description
Impulse	Switching on will occur with a time limit (the time is defined in the Time column).
ON/OFF	The switch-on command switches it on, the switch-off command switches it off, the status of the source or duration is not checked, the last command always executes its request
Copy	Copies the activation of the detector or internal status; when requested by two devices, OR logic is used.
Delayed copy	Switches on only when the activation condition lasts longer than defined in the Time column (suitable , for example, for indicating forgotten open garage doors).
Extended copy	Copies the activation of the device (or internal state) and extends it by the time defined in the Time column column (suitable , for example, for lighting a hallway after opening a door).
Change	Activation inverts the current PG state to the opposite state (suitable only for pulse control, e.g. with a remote control button).

Table 29 – PG output functions

Time – Defines the time for the Impulse, Delayed copy and Extended copy functions. The time is entered in the format hh:mm:ss in the range 00:00:01 to 08:59:59 (in seconds) and from 09:00:00 to 23:59:00 (in minutes).

Activation – Access to the PG output activation stimulus map.

Blocking of PG outputs – Defines PG output blocking by section status, detector or other PG. Blocking prevents the given PG from being switched on and, if it is already switched on, switches it off. Suitable , for

example, for blocking a door lock if the relevant section is set. For section blocking, you can choose whether the blocking is performed when the section is set or unset, and for device or other PG blocking, whether by its activation or deactivation. All blocking options can be used simultaneously.

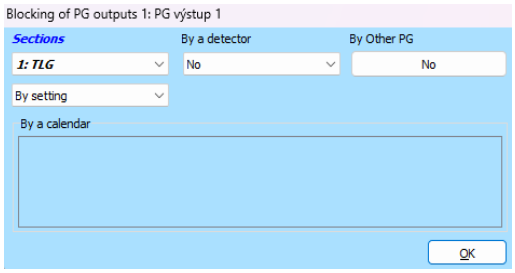


Figure 43 – Blocking of PG outputs

Reports – Presetting the text of the SMS report when the PG output is switched on or off. The option of who the report is sent to is defined in the Reports to users tab. Report texts are written to the log when changes are made, so they cannot be completely deleted.

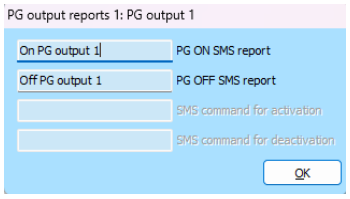


Figure 44 – PG Reports (F–Link)

Record PG into event memory* – Enables recording of PG activation to the event memory and thus SMS reporting to users and communication to the ARC (e.g. for monitoring user access to monitored doors, logging into the MyJABLOTRON web self-service, etc.)

PG Disabled – Option to block the PG output. Disabling (blocking) of the output is indicated by a red dot. Only a service technician (via F-Link) has the authorisation to deactivate.

Current status – Colour-coded information about the current status of the PG output. A green description corresponds to a green segment light, a red description to a red segment light.

Test PG output – Option to control the output manually from a computer using F-Link or JA-100-Link. Depending on the selected function, it will switch on (or off) the given PG, unless it is currently blocked.

Note – Allows you to describe the details of the PG output, the reason for use, special behaviour, warnings about switching on simultaneously with other outputs, etc.

Selecting Activation in the PG Outputs tab opens the Map of PG Activation links. The map determines which actions the output reacts to.

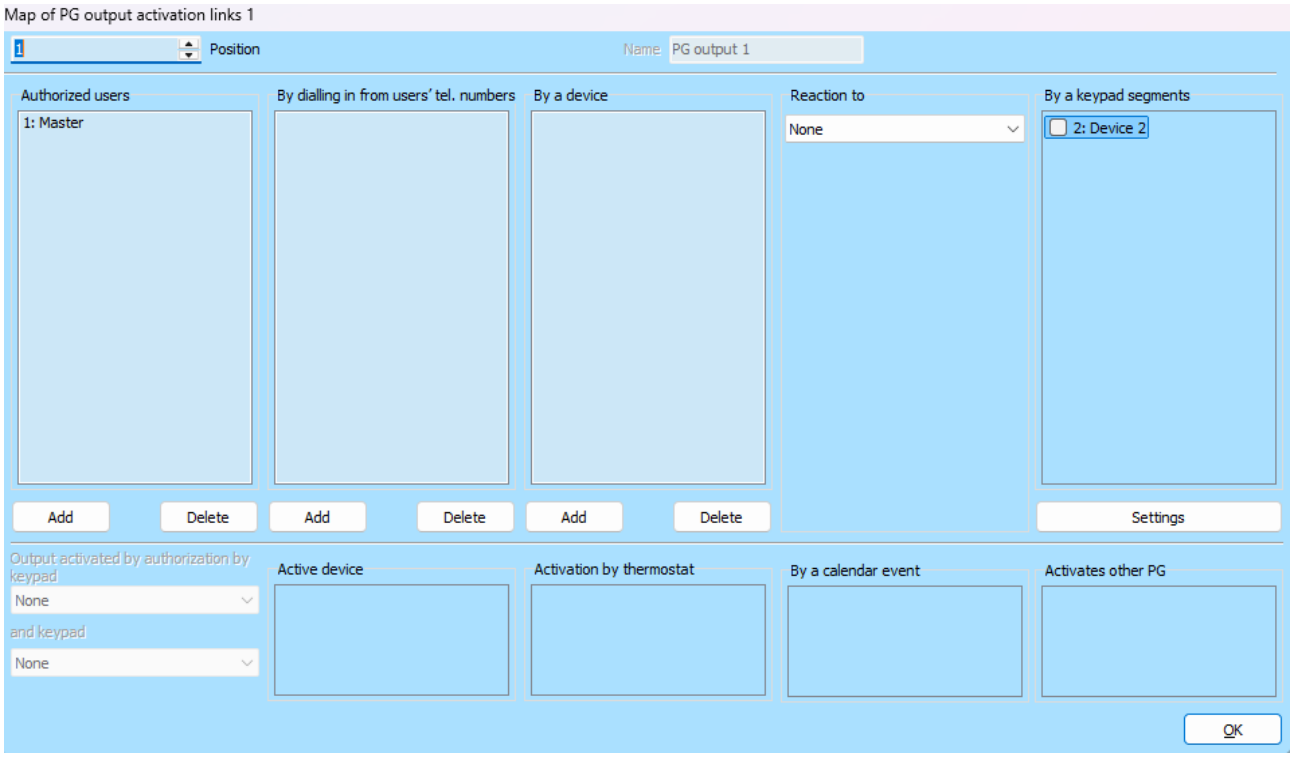


Figure 45 – Map of PG activation links

Authorised users – Says which users are authorised to control the PG output, which has an authorisation requirement set, from the keypad (segment buttons), or from MyJABLOTRON or by SMS command. The setting is linked to the Users tab.

Output activated by authorisation by keypad – Allows you to program 2 keypads that activate the PG output by simple authorisation (by placing a chip or entering a code). The function is intended for opening door locks, i.e. no manipulation of the segment buttons is required. This function is only available if the output function is programmed to Impulse.

By dialling in from user´s tel. numbers – Defines which users are authorised to activate the PG output by calling from their telephone (telephone numbers are entered in the Users tab). The telephone numbers from which the call is made must not be hidden (the CLIP service must not be deactivated). The term "ringing" means that after dialling the system's telephone number, the caller waits for at least one ring tone (but no more than the number of rings set for call pickup by the control panel, see Number of rings for incoming calls in the communicator settings) and then ends the call. The PG responds to the call being hung up. If the call is picked up by the control panel, the output will not be activated.

By a devices – Allows you to activate the PG output via devices (by activating a detector, pressing a key fob, etc.). The settings are displayed in the Devices Activation tab.

Reaction to – Allows you to activate the output with a selected internal system status (e.g. settings, alarm, mains power failure, fault, etc.). For the internal status (a total of 37 internal statuses, see Table 30), you can preset a mask of sections from which the signal will be accepted (OR logic). The relevant PG output can be programmed to copy the status of another PG output or several other outputs, where the mutual logic (OR or AND). The last item in the "Event in the system" menu allows you to set the output to switch on and its disconnection to a completely different event (e.g. connection during an alarm, but disconnection only after unsetting).

By a keypad segments – Displays an overview of keypads and remote controls in the system. Use the Settings button (below the list) to enter the internal menu of the selected device and adjust its settings see 4.2.3.2 Keyboard configuration.

Active devices – Overview of devices that are activated by switching on the PG output, e.g. requesting a photo from a photo PIR detector (information window only, the function is defined in the devices).

Activation by thermostat – Overview of thermostats that activate/deactivate or block the PG output (information window).

By a calendar event – Overview of calendar events that activate/deactivate or block the PG output (information window).

Activates other PG – Overview of PG outputs that activate/deactivate or block another PG output (information window).

CAUTION 1: The JA-107K control panel provides 128 PG outputs. Wireless transmission of PG outputs can only be addressed to outputs 1 to 32. All 128 PG outputs can be used for Bus modules.

CAUTION 2: PG outputs are not functional when the system is in Service mode. In Service mode, they can be tested using the test button in F-Link, PG outputs window. All PG outputs are switched off when entering Service mode. After exiting Service mode from F-Link, their reactivation is offered, except for Note 3.

CAUTION 3: If Parameters / Entering Service service mode automatically parameteris enabled and if the Unset option is selected in the Warning alert window when connecting the control panel to F-Link, then during this direct entry to the service, any PG outputs activated by pulses (e.g. by a keypad segment and the Turn On/Off function or by setting in the Calendar). When exiting Service, the question of whether to reactivate this PG.

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

Table 30 – Internal states for controlling PG outputs

4.2.6 User reports

NOTE: The "User reports" tab is only displayed in the F-Link software when using a full-featured communicator (e.g. when using the JA-194Y communicator, "User reports" can be edited and the tab is visible in the F-Link software; on the other hand, when using the JA-194Y-LITE communicator, the "Reports to users" tab is not displayed at all, as this communicator does not support voice or SMS reports).

The tab is used to define which users the system will report selected groups of events to by SMS or voice call. It is not necessary to be in Service mode to make changes in this tab.

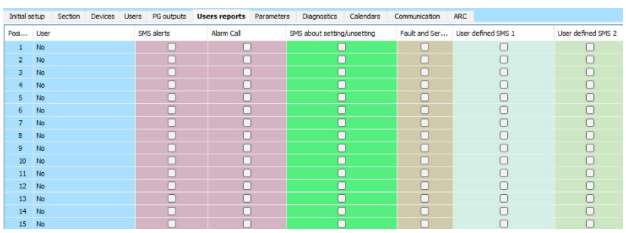


Figure 46 – Reports to Users 1

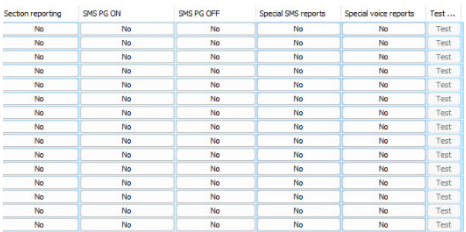


Figure 47 – Reports to users 2

* Items marked in this way are displayed when **Advanced Settings** is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire F-LINK to basic/advanced settings).

User – Allows you to select a user from the list of users.

Alarm SMS – A group of optional alarm reports for which a text message is sent about an alarm event in selected sections, as well as about a power failure or restoration lasting longer than 30 minutes, setting with an open zone, or a report about an unset section without movement (see 4.2.2).

Alarm call – A group of reports in which (after sending SMS reports) a voice alarm message is called to the user, which rings for approximately 30 seconds. If the call is not answered, the next user in the sequence is called. If the call is answered, the voice message is sent repeatedly. The message structure is: Your alarm reports – Alarm type – Section number. After the user hangs up the accepted call, but no later than after approximately 50 seconds, the call is terminated and transferred to the next user. The user can confirm receipt of the call by pressing **the # key** on the telephone and entering a valid code after the voice prompt. After entering a valid code, **the alarm** is **terminated and the next user is not called**. For voice reports, universal voice messages are preset in the system. Voice messages can be re-recorded as required by playing them back in the voice menu. For the voice menu diagram, see 5.5 Control from the communicator voice menu (GSM).

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

Fault SMS – Sends text reports of faults (low batteries, entering the service mode, etc.).

Custom group 1* – Special group 1, to which the installation technician can transfer the required events for reporting from the preset groups (typically reports of power failure and restoration, or setting with active devices) to selected users.

Custom group 2* – Special group 2, to which the installation technician can transfer the required events for reporting (typically low batteries in devices or low backup battery status) from preset groups to selected users.

Reports from sections – Specifies from which sections the selected event groups will be reported to the user. If Fault and service SMS is selected and no section is selected, only system faults and service (which are always assigned to Section 1) are reported. The selection is not linked to the user's permission to control the section.

SMS PG ON* – Setting up reports to the user about activation of PG outputs. Message sending has a fixed delay of 60 seconds. SMS texts are defined in the PG outputs tab, see 4.2.5 PG outputs and activation maps.

SMS PG OFF* – Setting up reports to the user about deactivation of PG outputs. Messages are sent with a fixed delay of 60 seconds. SMS texts are defined in the PG outputs tab, see 4.2.5 PG outputs and activation maps.

Special SMS reports* – Option to report detector activations that have a special report reaction preset (A, B, C or D) to the user via SMS. The texts of special reports are set using the **Special Reports** button at the bottom right of the User reports tab.

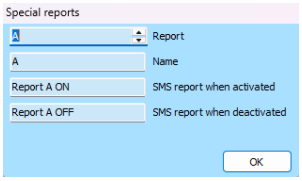


Figure 48 – Special reports to users (F–Link)

Special voice reports – Option to report detector activation to the user via voice message if the detectors are preset to react with a special report (A, B, C or D). User voice messages can be played by calling thecontrol panel telephone number, where, after picking up the call and authorising with the administrator code, the user presses 9 to enter voice message recording, see 5.5 Control from the communicator voice menu (GSM).

Test – Pressing the button sends a test SMS message to the user: "Test report, Control panel, Section 1".

Table of events and preset groups:

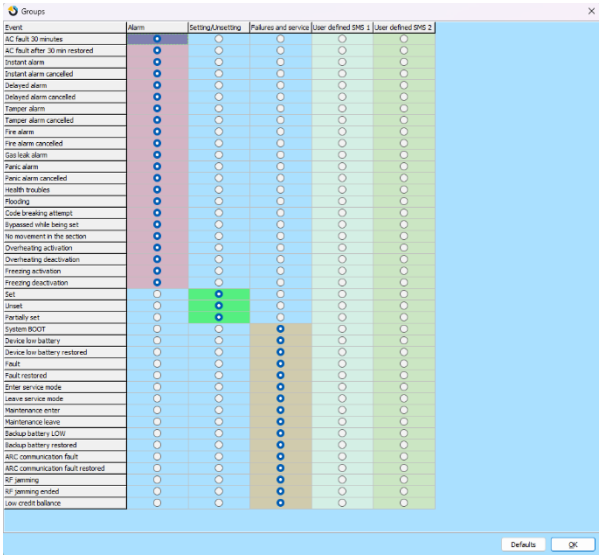


Figure 49 – Table of events and preset groups (F–Link)

Special reports – The button on the bottom bar opens a window for editting the name, SMS for activation and deactivation and writing to the event memory for reports A to D, which can be programmed as detector reactions, see 2.8.6.1 Overview of configurable peripheral responses.

4.2.7 Parameters

Sets the parameters and optional functions of the control panel. The tab is identical to Devices / Control Panel / Internal Settings. It is not necessary to be in Service mode to make most changes in this tab.

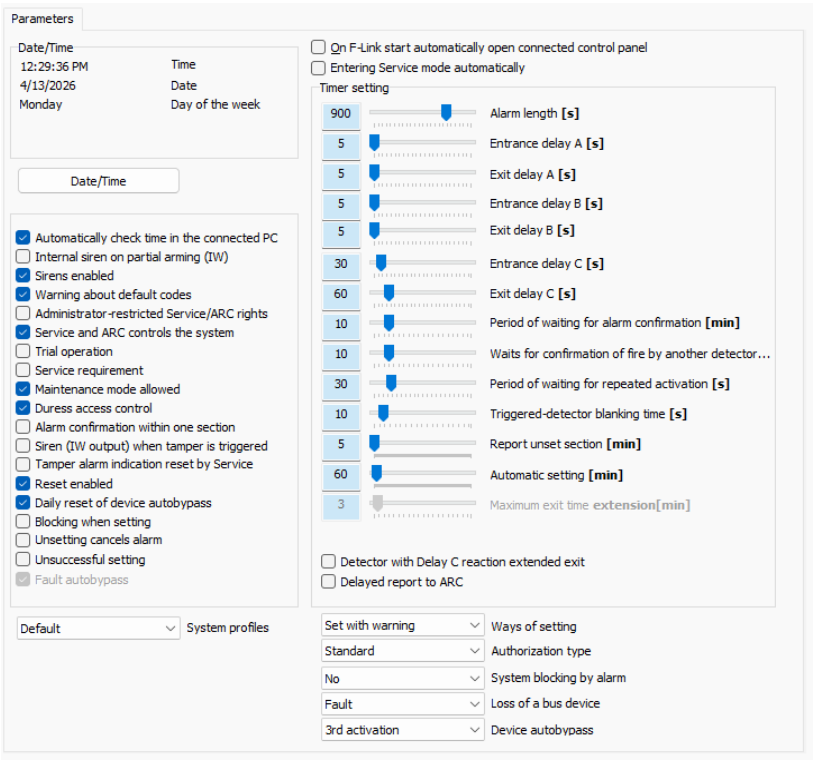


Figure 50 – Parameters (F–Link)

Menu displayed when selecting the desired "system profile" (GRADE).

NOTE: This setting option is only displayed when a specific "system profile" is selected (e.g. "comply with EN50131-1, grade 3").

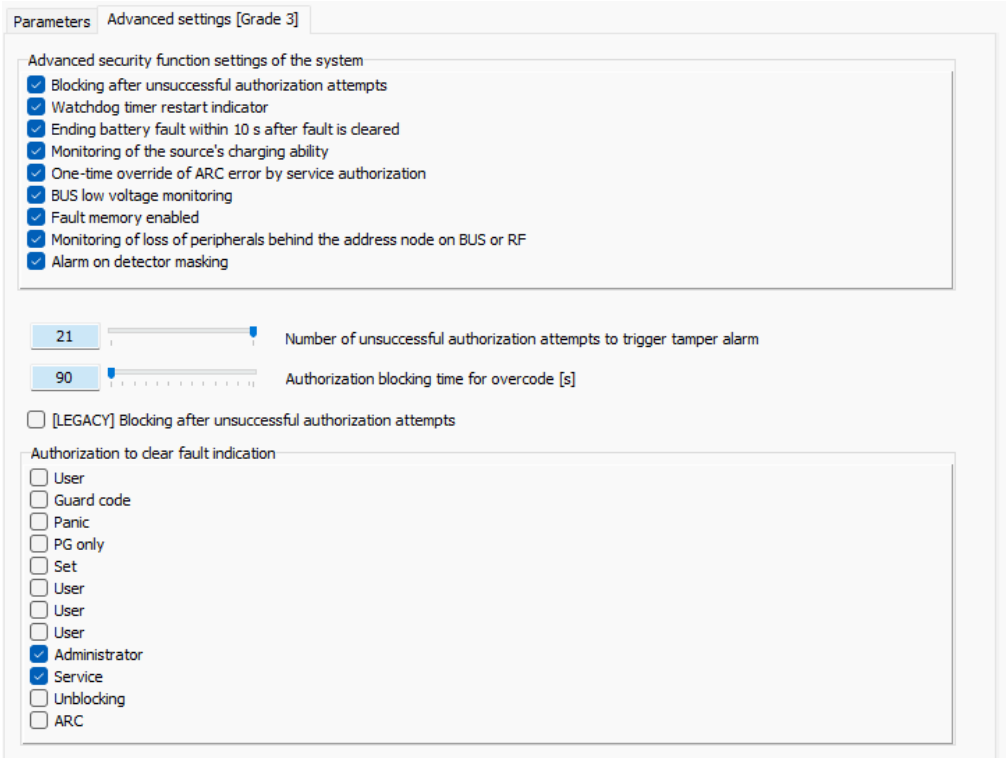


Figure 51 – Parameters – Security grade (F–Link)

Menu displayed after pressing the Date/Time button.

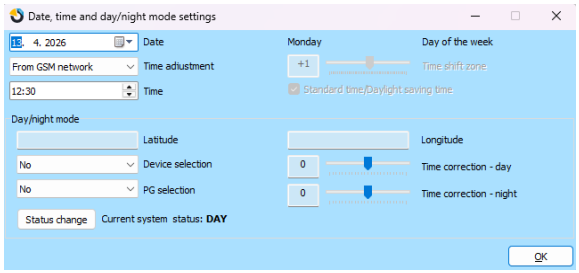


Figure 52 – Parameters – Date and time (F–Link)

* Items marked in this way are displayed when Advanced Settings is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire F-LINK to basic/advanced settings).

Parameter	Parameter description	
Date/Time	Internal calendar settings	
Date	Setting a specific date.	
Day of the week	Displaying the day of the week	
Time adjustment*	Method of adjusting the internal clock and date	
	Manually	For manual time and date setting (F-Link, JA-100-Link)
	From GSM network	The time and date are automatically adjusted from the GSM network each time you log in
	From the JABLOTRON server	The time and date are automatically adjusted according to the communication server (GMT 0). The setting does not work if the Communication type is set to "No remote configuration" (factory setting)
Time offset	Setting the time offset from GMT 0	
Time	Setting the internal clock.	
Standard time/Daylight saving time*	Automatic switching between winter and summer time can only be selected for manual time adjustment. The changeover takes place on the last Sunday in March and October at 1:00 UTC (i.e. 2:00 CET or 3:00 CEST).	
Mode Day/night	Latitude	Enter in the format xx.xxxxxxN (e.g. 50.729058N)
	Longitude	Enter in the format xx.xxxxxxE (e.g. 15.176636E)
	Device selection	Activating the selecteddevice switches thecontrol panel to "Night Mode"
	Time correction day	Option for time correction when switching to day mode
	Time correction night	Option to correct the time for switching on night mode
Automatically check time in the connected PC	If the computer andcontrol panel clocks differ by more than 1 minute, F-Link will notify you of this at start-up	
Internal siren on partial arming (IW)	Function that allows internal sirens to be activated in the event of a delayed burglar alarm during partial setting (this setting does not apply to fire and 24-hour alarms).	
Sirens enabled	Activates all wired and wireless sirens in the system (designed to turn off the acoustic alarm during system testing)	
Warning about default codes	When the service is left, it sends an SMS message to the service technician at position 0 with a notification that the factory default codes remain set in the system.	
Administrator - restricted Service/ARC rights	Blocks independent access to the system by service technicians and ARC. To access the system by the service **or ARC technician requires confirmation of authorisation by the Administrator . When a technician accesses the system remotely via F-Link, the administrator can authorise them on the keypad in the building. When a technician connects locally to the control panel using a USB cable, the administrator can authorise them remotely using the voice menu.**	
Service and ARC controls the system	Allows the service and ARC technician to control (set/unset) all sections and all PG outputs (turn on/off) that require authorisation. By disabling this parameter, the technician does not have the authorisation to control the section and will only be able to enter Service mode after all sections have been unset by the Administrator or user.	
Trial operation	All alarms are limited to 60 seconds and are reported via SMS to the set users and the service technician (position 0) even if they do not have alarm transmissions enabled. Trial operation ends automatically 7 days after leaving Service mode. A special mode used after system installation, in which, regardless of the actual alarm duration setting, the alarm is shortened to a maximum of 60 seconds and all alarm events are sent to the service technician stored in position 0 in users. This mode is automatically turned off 7 days after activation.	
Service requirement*	If this function is enabled 12 months after the last time the Service mode was left, it will trigger a "System requires service inspection" event in the system, which will be displayed together with the Information icon on keypads with an LCD display and recorded in the event history. Pressing the "i" key will display the text "call a service technician" with their telephone number. The message on the display will be automatically turned off when the service technician accesses the system locally. This will automatically reset the annual counter. The service request can also be preset as a calendar event for the exact date required in the Calendar tab (the calendar function can be combined with an automatic service request after 1 year).	

Parameter	Parameter description	
Maintenance mode allowed	Allow administrators (administrators) to switch the system to Maintenance mode	
Duress access control *	Used to trigger a silent panic alarm by simply authorising or controlling the system (setting, unsetting, PG control, etc.) if the user is in danger. The panic alarm is triggered when 1 is added to the last digit of the standard code. The function is supported for codes with and without a prefix. *EXAMPLE: User code with prefix = 4*4444, for duress control the code is =* **4*4445**. *User code without prefix = 4444, for duress control the code is =* **4445**. *NOTE: If the user code ends with the number 9, then for forced control, use 0 for the last digit of the code.*	
Alarm confirmation within one section*	If the detector is configure d to confirm the reaction with another detector, this option can be used to limit confirmation **to** the **same** section only (otherwise, the detector from any section will confirm). This applies to for both intrusion detectors and fire detectors.	
Siren (IW output) when tamper is triggered*	Sirens with IW response acoustically signal a tamper alarm if they are unset or partially set. When fully set, they always signal an alarm.	
Resetting the tamper alarm by the service*	Only a service or ARC technician can cancel the tamper alarm memory indication. If not specified, the Administrator (but not the User) can also cancel the indication.	
Reset enabled*	Option to block the control panel reset function with a jumper on the mainboard. If the reset is disabled and the service code is lost, the control panel can only be unblocked by the manufacturer. Description of the reset is also described at 6.2.1 Control panel reset .	
Daily reset of device autobypass devices	This option applies only to activation inputs (not tampering and faults). When this option is enabled, the system will automatically unblock auto-bypassed devices every day at 12:00 noon. When this option is disabled , the auto-bypass on the device will be unlocked only when the section status changes. This option is suitable , for example, when using detectors with a 24-hour reaction or flood detectors, which may be located in a section that does not need to be set and unset.	
Blocking wehn setting*	Enabling this option will block active detectors during section setting, i.e. they can no longer trigger an alarm in this set state. If the option is disabled, active detectors will will only be bypassed during setting, and the detector will resume monitoring after the alarm has been silenced (risk of false alarms, e.g. a window opened by a draught).	
Unsetting cancels the alarm*	This function allows you to configure whether the alarm will be terminated by simply authorising a valid user code or only by unsetting the section in alarm. By enabling this option, the current alarm will only be terminated by unsetting the section in alarm or by selecting "Cancel warning indication" from the LCD keypad menu.	
Unsuccessful setting*	This function is evaluated each time a section is set. If an instant zone is activated during the exit delay or remains open even after its timeout, the system will not set and an "Unsuccessful setting" event will be triggered. This is recorded in the event history, reported to the relevant user according to the "SMS about unsuccessful setting" parameter setting and is indicated on the keypads and by the outdoor siren. To cancel the unsuccessful setting indication, press "Cancel warning indication" in the LCD keypad menu.	
Fault autobypass*	This option is available when setting one of the "EN50131-1" or "INCERT" system profiles. It can be used to disable the limitation on the number of faults reported, which will then be unlimited.	
System profiles	Selection from preset system behaviour profiles.	
	Default	Factory default settings with the option to make changes according to your own requirements
	EN 50131-1, Grade 2	Fixed preset parameters complying with EN50131-1 for Grade 2 (low to medium risk) without the option to make adjustments
	EN 50131-1, Grade 3	Fixed preset parameters complying with EN50131-1 for Grade 3 (medium risks) without the possibility of making adjustments
	INCERT, Grade 2	Fixed preset parameters complying with INCERT standard for Grade 2 without the possibility of adjustments
	SSF 1014, alarm class 2	Fixed preset parameters complying with the SSF 1014 standard for alarm class 2 (R) without the possibility of making adjustments

Parameter	Parameter description	
Ways of setting	**Selection of the level at which the system approaches the setting process with active devices or system faults in the system. The selection ranges from the lowest level, where setting is always ensured regardless of active devices and faults, to the highest level, where setting cannot be ensured with an active element (in the instant zone). It is linked to the set system profile.**	
	Set always	Set regardless of system status (faults, active elements, etc.)
	Set with a warning	Visually indicates (segment, display) the system status (faults, active elements, etc.) for 8 seconds. After this time, it automatically sets. It can also be set by repeatedly pressing the segment or the ENTER key
	Set after confirmation	Visually indicates (segment, display) the system status (faults, active elements, etc.) for 8 seconds. It can ONLY be set by repeatedly pressing the segment or the ENTER key
	Do not set with an active element	Visually indicates (segment, display) the system status (faults, active elements, etc.) for 8 seconds. It can be set by pressing repeatedly (segment, ENTER), only if the detector with a DELAY or NEXT DELAY reaction is active. If the active element has a different alarm reaction, it CANNOT BE SET. CAUTION!!! This also applies to remote control (Voice Menu, SMS, MyJABLOTRON, calendar events with the exception of "Set always").
Authorisation type	Selection of user authorisation method. Also applies to PG outputs requiring authorisation. From simple authorisation with just a code or chip/card, through card confirmation with a code (if the user has both assigned), to double authorisation, where both a code and a card are always required. Confirming the user code with a card reduces the risk of unauthorised control or bypassing of the system by an unauthorised person.	
	Standard	Valid authorisation is performed by entering the user code or attaching the chip. Only one of these options is required to control the system.
	Card confirmation with a code	If the user has both a code and a card, they must authorise themselves with both (the order does not matter). If the user only has a code or card, they are authorised as in the simple option. Remote access by telephone is only possible for authorised telephone numbers.
	Double authorisation	Valid authorisation can only be achieved by entering the user code and attaching the user's chip (the order does not matter). F-Link checks that both the reader and the user code are entered on the user's card. If this is not the case, it will not allow the configuration to be saved. Remote access by telephone is only possible for authorised telephone numbers.
System blocking by alarm*	Option to block the system after an alarm is triggered, either by the first alarm (intrusion) or the first tampering, to prevent further alarms from being triggered. Unblocking is only possible by a user with an unblocking code or access from the ARC (intended for the United Kingdom). Tampering can also be unblocked using a service code (intended for Benelux).	
	NO	**No blocking**
	By tamper alarm	The system is blocked by triggering a tamper alarm (opening a device, entering incorrect codes during authorisation, jamming the radio module, etc.).
	Any alarm	The system will be blocked by any intrusion, fire, flood, 24-hour or panic alarm.

Parameter	Parameter description	
Loss of a Bus device*	The control panel evaluates the loss of devices or a short circuit on the system Bus. The parameter selects the system's response to the situation.	
	Fault	The control panel evaluates the loss of devices or a short circuit on the Bus as a fault
	Tamper always	The control panel evaluates the loss of devices and a short circuit on the Bus as a fault and a tamper alarm whenever it occurs. If the radio module used has interference detection enabled, a tamper alarm will also be triggered in the event of interference. Once the fault caused by the loss of devices has been resolved on the Bus, the tamper alarm will also be restored.
	Tamper after confirmation	The control panel evaluates the first loss of devices as a fault, and if another loss of devices occurs within the set time of the "Period of waiting for alarm confirmation by another detector" parameter, a tamper alarm is also triggered. Once the fault is resolved by the loss of devices on the Bus, the tamper alarm is also resolved.
Device auto-bypass	This option now allows you to select the autobypass method. The selection only applies to activation inputs, not tampering and faults.	
	Disabled	**A device will never be bypassed. The control panel processes every activation received from the device.**
	3rd activation	The device input is bypassed after 3 activations in a single setting period, regardless of the duration of the alarm. Until the section is unset, further activations from the device are ignored.
	3rd alarm	The control panel allows three activations of the device in one alarm period and three alarms to be triggered by the given device. The bypass is performed only after three alarm periods, during which up to 9 activations may occur.
On F-Link start, automatically open the connected control panel	When the control panel is connected to the computer via a USB cable, the connection is established automatically.	
Entering Service mode automatically	When connected to the control panel, the software automatically switches the system to Service mode. If any sections are set, it will request permission to unset them. If the factory codes are still in the system, initial authorisation is not required. This option only works when the control panel is connected via USB.	
Timer setting	In each section, entry and exit delays A, B and C are measured separately. If different exit delays are defined for detectors in one section, the longest delay is measured. If there are different entry delays, the delay corresponding to the activated detector is measured. If multiple detectors are activated, the shortest preset entry delay is measured. Detectors with delay C can extend the length of the exit delay (see option: Detector with delayed response C extends exit in the Parameters tab)	
Alarm length	Alarm duration – applies to all sections. Range 5 s ÷ 20 minutes	
Entry delay A	Timer A. Range 5 s ÷ 2 minutes	
Exit delay A	Timer A. Range 5 s ÷ 2 minutes	
Entry delay B*	Timer B. Range 5 s ÷ 2 minutes	
Exit delay B*	Timer B. Range 5 s ÷ 2 minutes	
Entry delay C*	Timer C. Range 5 s ÷ 6 minutes	
Exit delay C*	Timer C. Range 5 s ÷ 6 minutes	
Period of waiting for alarm confirmation*	Waiting time for alarm confirmation by another detector in the set section. Applies to all detectors with Instant confirmed / Delayed A confirmed (1 to 60 min.) reaction.	
Waiting for confirmation of fire by another detector*	Waiting time for fire alarm confirmation by another detector. Applies to all detectors with Fire confirmed reaction. (1 to 60 min.)	
Period of waiting for repeated activation*	Waiting time for repeating the activation of the same detector. The defined time must be longer than the minimum detector settling time before repetition. Applies to all detectors with Repeated Instantant / Repeated Delayed A reaction (6 ÷ 120 s).	
Triggered-detector blanking time*	The minimum time during which the detector is not evaluated before it can repeat activation. Applies to all detectors with Repeated Instantaneous / Repeated Delayed A response (5 ÷ 60 s).	

Parameter	Parameter description
Report unset section	The time after which an unset section reports unset status if no detector has been activated in it (reporting is enabled in the Section – Report unset tab; 5 ÷ 2880 min.).
Automatic setting	Time (0 ÷ 120 min.) after which the section in which the "Report unset section" event was triggered is automatically set.
Maximum exit time - extension*	The maximum time by which an active delayed detector in the section extends the exit delay. Only functional in conjunction with the option: Detector with Delayed C reaction extends the exit delay. If the detector is activated for longer, the section is set and the detector is bypassed (1 ÷ 60 min.).
Detector with Delayed C reaction extended exit*	The so-called garage door function – an active detector with Delayed C reaction (open door) extends the exit delay in the relevant section. Such an extension can only be triggered by sensors with a status reaction (typically magnetic detectors). The maximum possible extension time is defined by the previous selection.
Delayed report to the ARC*	Enabling this function causes the internal pre-alarm to be triggered, including the sounding of internal sirens, when the entry delay is timed, but the report to the ARC is delayed by 30 seconds to give the user time to unset the system.

Table 31 – Description of adjustable parameters

4.2.8 Diagnostics

Used to check and determine the status of devices and their properties.

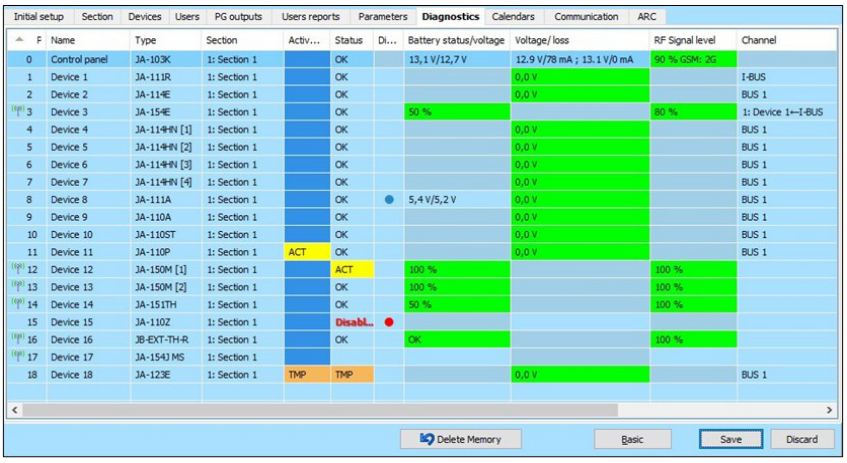


Figure 53 – Diagnostics (F–Link)

** Items marked in this way are displayed when **Advanced Settings** is enabled (the button is located on the bottom bar next to the "Save" button and switches the entire FLINK to basic/advanced settings).*

Activation memory – records what device activation has occurred since this column was last erased. The memory of all devices can be erased with the Delete Memory button (bottom bar). The memory of the selected device can be erased with the right mouse button. Tamper sensor (TMP) activation has the highest priority when writing to memory.

Status – Indicates the current status of the device. OK = everything OK, TMP = tamper, ACT = alarm input activated, ERROR = fault, ?? = device does not communicate, NO AC = mains power failure (or completely discharged battery), BUPFLT = backup battery in device or control panel is charging. Battery = discharged or disconnected battery in the device or control panel, BOOT – status when the device FW update is in progress or if the update did not proceed correctly, repeat it, INIT – reading the device configuration, Disabled = device completely disabled. Move the mouse over the STATUS of the relevant device to display details.

Battery status/voltage* – If the device contains a battery, its status is displayed. For the control panel (position 0), the backup battery voltage is displayed. If the voltage information is missing for a wireless device, communication with the device has not yet occurred. Trigger it (e.g. with a tamper sensor or by clicking the Load button in F-Link)or wait for automatic transmission. If the wireless keypads are powered by an external source, "Powered

from external power supply" is displayed. For wireless devices (except for the JA-18x series with lithium batteries) the battery life status is displayed. Colour coding for battery status: 10% red, 20% yellow, 30% and above green.

Voltage/loss* – The position of the control panel (0) displays the voltage at the control panel terminals and the current consumption by the Bus devices from the control panel (displayed for individual Buses). For Bus devices, the voltage drop on the line relative to the control panel is displayed. The drop must not exceed 2V – this must be resolved!

RF Signal level* – The control panel position displays information about the GSM signal quality. We recommend at least 50% for reliable data communication. For wireless devices, the RF signal strength is displayed. The value should be at least 30%. If the data is missing, the device has not yet communicated. Trigger it (e.g. with a tamper sensor) or wait for automatic transmission.

For interference affecting the radio and GSM module, see 2.6.1 Radio module JA-11xR.
GSM signal colour indication: 0–30% red, 40–50% yellow, and above 50% green.
RF signal colour indication: 10% red, 20% yellow, 30% and higher green.

For two-way devices (which support this), you can find out the signal strength in both directions, i.e. from the control panel to the device, by moving the cursor over the signal level.

Channel* – Provides information about the Bus on which the device communicates. There are three directions: Bus 1, Bus 2, Bus 3 (JA-107K / JA-108K only) and I-BUS designed for the JA-11xR radio module (JA-103K). For two-way wireless devices (sirens, keypads, etc.), the "channel" column displays the radio module through which the device is currently communicating.

4.2.9 Calendar

Here you can configure the time schedule for actions that the system will perform automatically and regularly. It is not necessary to be in Service mode to make changes in this tab.

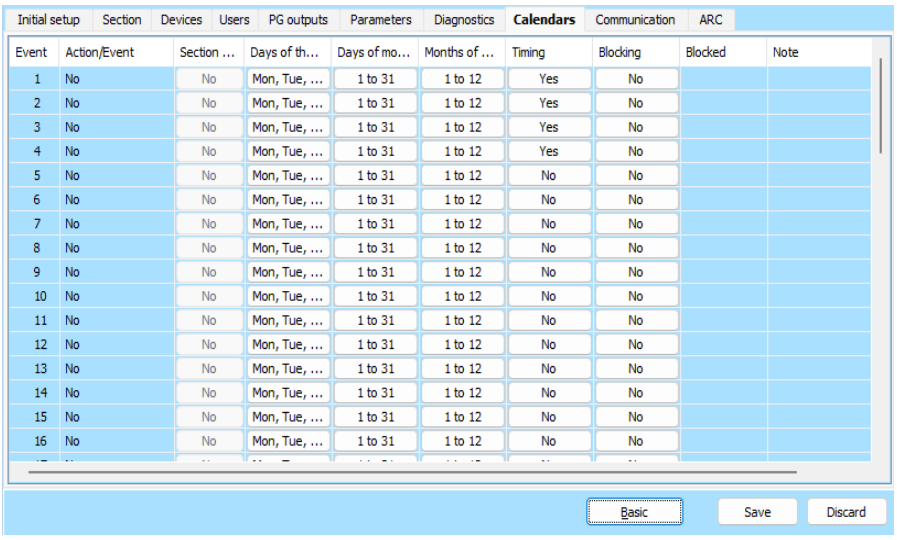


Figure 54 – Calendar (F–Link)

Actions – Configurests what action is to be performed on sections or PG outputs (Unset, Set, Partially set, PG control, Technical inspection request, etc.). Setting can be configure d to "Set immediately" (no exit delay) or "Always" (ignores the currently defined way of setting). A Technical inspection request triggers the same status in the system as a "service requirement" programmed in the system parameters.

Section/PG – Specifies in which section(s) the guarding action will be performed or which PG will be controlled.

Days of the week – Specifies on which days of the week the action is performed. (e.g. every Monday).

Days of the month – Specifies on which days of the month the action is performed.

Months of the year – Specifies in which months the action is performed.

Timing – The system allows you to set up to 4 times during the day or a time interval in which the programmed action will be repeated regularly. The repetition can be defined by the FROM – TO time window.

Blocking – In this column, you can select PG, whose activation can block the execution of a calendar event.

Blocked – Option to block the relevant event. Deactivation is indicated by a red dot. The Administrator (JA-100-Link) and Service Technician (F-Link) have the authorisation to deactivate the calendar.

Note – Allows the user to describe the calendar event.

NOTE:

There are two ways to switch an appliance on and off for a specific period of time. Either configure an action to switch the PG output on and off, or programm only an action to switch the PG output on and preset the desired pulse length.

When selecting the Set (Partially Set) option for a specific section, the exit delay with a fixed time of 3 minutes is first activated at the specified time. All detectors in the specified sections with an Instant reaction are switched to a Delayed reaction for this 3-minute period. When selecting the Set immediately option, setting is performed without an exit delay and all zones are set immediately (including delayed detectors).

4.2.10 Communication

Used to set up the behaviour of communicators and the method of communication. It is not necessary to be in Service mode to make changes in this tab.

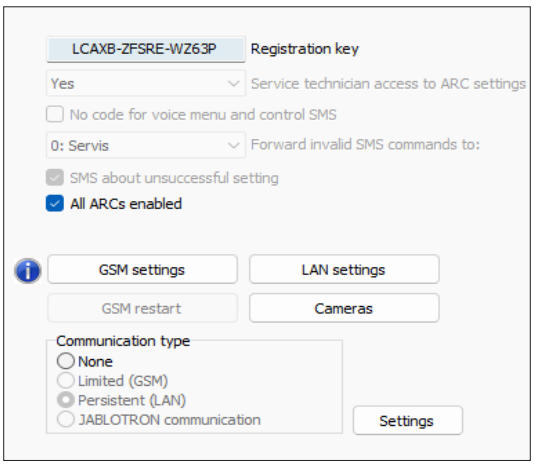


Figure 55 – Communication (F–Link)

Voice report calling priority – Selection of the channel through which the control panelreports voice events (GSM options).

Registration key – Unique registration number of the control panel.

Service technician access to ARC settings – Allows the ARC technician to restrict the service technician's access to the ARC tab (completely or only to view).

No code for voice menu and control SMS – When controlling from an authorised telephone by calling, the user does not need to enter their code (they are authorised by calling from their telephone number). Caller ID (CLIP) must be activated for this option.

Forward invalid commands to – User selection of where SMS messages that are incomprehensible to the control panel (information from the operator about billing, etc.) will be forwarded.

SMS about unsuccessful setting – In case of unsuccessful setting, an informational SMS is sent. If set with authorisation, the message is sent to the given user; if set without authorisation, the SMS is sent to the Administrator in position 1.

All ARCs enabled – Option to completely disable communication on ARCs – unavailable if the ARC technician has restricted access.

Communication type – The system offers several ways of remote communication/configuration.

- **None** – Behaves as an autonomous device with its own SIM card. The device communicates outwards (sends SMS and voice messages) and receives command SMS messages and has a functional voice menu. It does not communicate data. Remote configuration of F-Link software is not possible.
- **Limited (GSM)** – Communicates as the previous type and also allows remote system configuration. Remote configuration is possible from a computer with F-Link software (JA-100-Link) with an internet connection. To establish a connection with the control panel, F-Link connects to the manufacturer's server and transmits the registration code and telephone number of the SIM card inserted in the control panel communicator. Data communication (LAN or GSM/GPRS) must be functional in the control panel.
- **Permanent (LAN)** – The control panel maintains permanent data communication (LAN) with the server. It is possible to connect
  and management of the control panel using F-Link software.
- **JABLOTRON communication** – The device communicates with the manufacturer's server (MyJABLOTRON application) and continuously sends the current status of the device to it. When a remote connection is requested via F-Link
  (JA-100-Link), the server is ready to establish a connection immediately. This communication also allows the user to use server services. Applications enabling the user to operate the system can be installed on mobile devices with Android or iOS (Apple) , applications can be installed that allow the user to operate the system. With this option, it is necessary to use a JABLOTRON security SIM card.

Please contact your distributor for information on the types of communication available in individual countries. In the Czech Republic, for example, **Limited** remote communication can be used with all operators whose SIM cards support GPRS (Internet) data transmission.

Settings – Clicking on the button starts the process of registering the system with MyJABLOTRON cloud services. By filling in the details and confirming the registration, the request to connect the system to MyJABLOTRON will be sent. The system will immediately confirm the successful transmission of the completed form.

4.2.10.1 GSM settings

Used to set the parameters and behaviour of the GSM communicator, if used in the control panel.

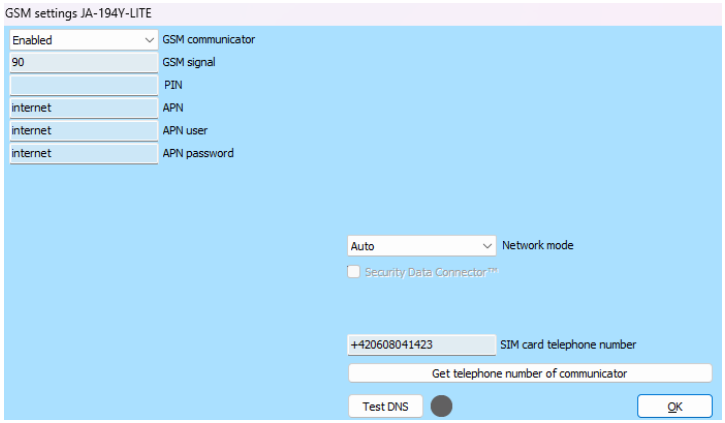


Figure 56 – GSM settings (F–Link)

** An item marked in this way is configure d automatically after switching on the control panel, provided that a GSM communicator with a functional SIM card (JABLOTRON server service) was installed in it before switching on.*

GSM communicator – Option to switch off the communicator.

GSM signal – Signal strength in percent (measured every minute). For proper operation, the signal should be at least 50%. If you experience problems with GSM signal quality, we recommend trying a SIM card from another operator. It is not recommended to use a directional or gain GSM antenna with the communicator (it reduces the module's connection to only 1 GSM cell = unstable communication). Information about signal quality can also be obtained using the STATUS SMS command (see5.6).

P**IN** – We recommend using a SIM card with the PIN code disabled.

APN * – GPRS data communication settings. Data communication provides JABLOTRON server services, remote access for service technicians, communication with the ARC, etc. In addition to the APN settings, the SIM card used must allow data transfers. To determine the usability of this communication and the settings parameters abroad, contact your JABLOTRON distributor.

APN for operators in the Czech Republic (in case of problems, verify the validity of the data with your network operator)	
Operator /	SIM APN
O2 / tariff	internet
O2 / GO	internet
T-Mobile / tariff and Twist	internet.t-mobile.cz (internet)
Vodafone / tariff	internet
Vodafone / card	Internet

Table 32 – APN network

APN user* – Name (if not used by the network, do not enter).

APN password* – Password (if not used by the network, do not enter).

Call limit min/day – Limits the range of real calls to 5 to 250 minutes per day.

SMS Limiter – Limits the number of SMS messages sent from the control panel per day. Applies to alarm and non-alarm events (alarm events – alarm, tamper, fault, report, etc.; non-alarm events – section control, PG, service, etc.). The adjustable limit is between 5–250 SMS messages. The system can send a maximum of 250 SMS messages per day. This maximum is divided between the SMS sender limiter and the alarm SMS limiter. F-Link automatically monitors that the sum of both limits does not exceed 250.

Alarm SMS Limiter – Limits the number of alarm SMS messages sent from the control panel per day if the limit for sent SMS messages (Sent SMS Limiter) has already been reached. Applies only to alarm events (alarm, tampering, fault, report, etc.). The setting range is 0–245 SMS messages.

EXAMPLE: The SMS limiter is defined to 30, the alarm SMS limiter is preset to 20. The system will behave as follows: If 30 SMS messages (alarm and non-alarm) are sent during the day, the system will not send any non--alarm SMS messages on that day. However, it can continue to send alarm SMS messages, up to a maximum of 20. This ensures that in the event of an alarm, the system always has a reserve for informing the user via SMS.

Diacritics allowed – If diacritics are enabled, messages from the system may be sent in multiple SMS messages. Diacritics must be enabled if you use Cyrillic or similar characters in your texts.

Remote control via telephone – Sets up the option to control the system remotely using the voice menu. If set to Users, the menu can only be accessed from the phones of configure d users (in the Communication tab, users can even be allowed to access the voice menu without entering their access code – the "No code for voice menu and control SMS" option). If set to Anybody, the voice menu can be accessed from any telephone. When accessing from an unknown telephone, the user's access code is always required. This function is directly dependent on the Authorisation type setting in the Parameters tab. When selecting an authorisation type other than Standard, it is not possible to use the GSM settings for control by Anybody. The system requires a user with a completed phone number as a second authorisation (code + phone number).

Remote control by sending an SMS – Sets up the option to control the system remotely using SMS commands. If set to "Users", the system only accepts SMS commands from the phones of configure d users (in the Communication tab, users can even be allowed to send SMS commands without entering an access code – the "No code for voice menu and control SMS" option). If set to "Anybody", SMS commands can be sent from any phone, but always require an access code to be entered. This function is directly dependent on the Authorisation type in the Parameters tab. When selecting an authorisation type other than Standard, it is not possible to use the GSM settings for control by Anybody. The system requires a user with a completed phone number as a second authorisation (code + phone number).

Credit query – Press this button to immediately obtain information about the credit amount from the operator's response (if this function is supported).

Credit – limit – Option to configure a lower limit for automatic credit checking on a prepaid SIM card. If the credit is below this limit, the system will send an informational SMS to the person who has set up Fault SMS reports. Warning! We do not recommend using prepaid SIM cards in the system. This increases the risk of communication failure not only when the credit is exhausted, but also when its limited validity expires.

SIM credit sequence – Command for automatic detection of the credit balance of a prepaid SIM card. Depending on the SIM card operator, enter:

Operator	Sequence
O2 / GO	*104*#
T-Mobile / Twist	*101#
Vodafone / Card	*22#

Table 33 – SIM sequence

Credit – position in text – Position (sequence number of the character) in the message from the operator where the credit balance number begins. The communicator searches only for numbers in the message and ignores other characters.

Credit – checking period – Defines how often the system will check the credit balance (can be set from 0 to 99 days, where 0 is off).

SIMLock – A function that links the SIM card phone number to the ARC settings. After changing the SIM card for another one, the entire ARC tab settings will be deleted after logging the new SIM card into the GSM operator's network without the need for intervention by a ARC technician. The deletion is irreversible and further settings must be made again by a ARC technician.

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

Level of generated DTMF to the ARC – Setting the intensity of the tone dialling signal transmitted in DTMF generated by the control panel/communicator. The intensity is adjustable in 10 steps, the factory default value is 4.

Number of incoming call rings – Number of rings before automatic pickup by the communicator. You can set 1 to 10 rings (corresponding to 5 to 50 seconds). The factory setting is 3 (15 seconds).

SIM card telephone number – The window displays the phone number of the SIM card inserted in the communicator.

Get card telephone number – Pressing the button sends an SMS query. After successfully receiving a reply, the number is displayed in the SIM card telephone number window.

Network mode – Select the network that the control panel will use for communication (Auto; 2G; 3G; 4G). When changing the parameter, the change will take effect 5 minutes after disconnecting the F-Link from the control panel. If you encounter problems with Auto mode, we recommend selecting 2G, which will limit switching between other networks and reduce the time when the control panelis out of signal range.

4.2.10.1.1 GSM restart

Button for logging out and logging back in the GSM communicator to the network. Logging back into the network may take up to several tens of seconds, depending on the status of the system. GSM can also be restarted using a GSM SMS command (see 5.6).

4.2.10.2 LAN settings

Used to configure the LAN communicator (if the control panel has one).

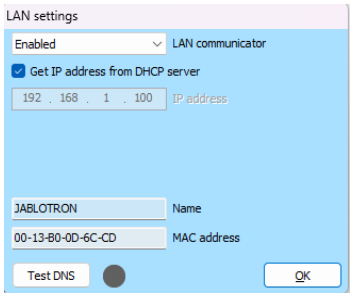


Figure 57 – LAN settings (F–Link)

LAN communicator – Option to disable LAN communication.

Get IP address from DHCP server – Option for automatic IP address acquisition from the DHCP server. If this function is not supported by the network, the corresponding parameters must be entered manually. Manual entry is only possible after disabling this option.

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

Subnet mask – Settings for manual assignment of the IP subnet mask are only available if automatic assignment from the DHCP server is not enabled. The factory setting is 255.255.255.0.

Gateway – Settings for manual assignment of the default gateway IP address, available only if automatic assignment from the DHCP server is not enabled. The factory default setting is 192.168.1.1.

DNS server – Settings for manual assignment of the DNS server IP address, available only if automatic assignment from the DHCP server is not enabled. The factory default setting is 192.168.1.1.

Name – Name of the device for easier identification on the local network.

MAC address – Unique address of each LAN device for identifying the source of information

Test DNS button – When connecting the LAN communicator to the internet, you can test the correctness of the settings. If a green circle appears after pressing the button, the connection to the server is established, but if a red circle appears after a few seconds, the time for establishing the connection has expired, which corresponds to an incorrect setting or an error in the LAN communicator connection.

4.2.10.3 Camera settings

The Cameras button allows you to test connectivity (required ports) and connection speed. After the test is complete, a graph is displayed along with information about how many cameras and at what resolution the available Internet connection is capable of supporting. If an active camera is already connected to the network, F-Link can be used to configure its basic parameters.

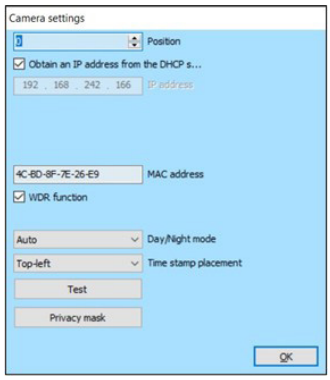


Figure 58 – Camera settings (F–Link)

Position – Order in the system

Obtain an IP address from the DHCP server – Automatic network parameter settings. If your network does not support this feature, you will need to enter the appropriate parameters manually. Manual entry is only possible after disabling this option.

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

Net mask – Settings for manual assignment of the IP subnet mask are only available if automatic assignment from the DHCP server is not enabled. The factory setting is 255.255.255.0

Gateway – Settings for manual assignment of the default gateway IP address, available only if automatic assignment from the DHCP server is not enabled. The factory default setting is 192.168.1.1

DNS server – Settings for manual assignment of the DNS server IP address, available only if automatic assignment from the DHCP server is not enabled. The factory setting is 192.168.1.1

MAC address – A unique address for each LAN device to identify the source of information.

WDR function – Allows you to disable the WDR (backlight compensation) function, e.g. in environments with high contrast between light and dark areas.

IR illumination – Option to permanently disable IR illumination. E.g. in environments with permanent lighting.

Day/night mode – Allows you to permanently select the camera mode between day, night or automatic.

Time stamp placement – Option to place the current time, date and camera name directly in the camera recording image; the selection determines in which corner of the image the information is displayed.

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

Privacy mask – Allows you to cover part of the image with a black pattern, e.g. for filming public spaces, which is illegal in the Czech Republic.

4.2.11 ARC and transmissions

Sets up communication with alarm receiving centres. If access for service technicians is restricted in the Communication tab, the settings can only be made at the ARC Technician access level. The settings are also unavailable if JABLOTRON Communication is selected, which significantly simplifies the configuration of the communication part of the system. It is not necessary to be in Service mode to make changes in this tab.

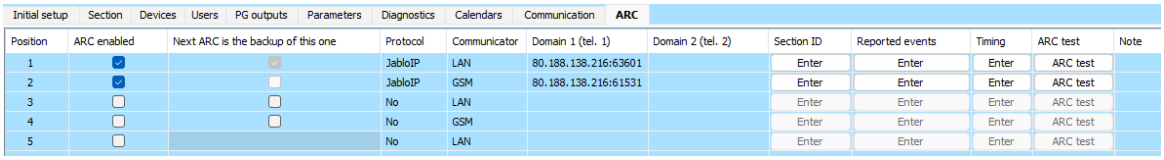


Figure 59 – ARC and transmissions (F–Link)

ARC enabled – Setting of permitted transmission directions.

Next ARC is the backup of this one – if enabled, the following position will only be used when data cannot be transferred to the main contact.

Protocol – Select the communication protocol..

Communicator – This option allows you to select the method of data communication to the ARC. The options are: GSM, LAN and Automatic, but only those that are currently available are offered. The Automatic option sets a combination of two LAN/GSM communicators, which primarily uses LAN and only switches to the backup GSM communicator if LAN is unavailable to the backup GSM communicator. If both communicators fail, a fault is reported by not transmitting messages to the ARC.

Domain 1 (tel. 1) – Setting the main domain (URL or IP address) or the main telephone number according to the protocol used. When using IP communication, it is necessary to enter the communication port after the IP address, separated by a colon. The communication port and IP address will be provided by the ARC to which the communication is routed. If the communication port is not filled in, events will not be sent.

Domain 2 (tel. 2) – Setting the backup domain (URL or IP address) or backup telephone number according to the protocol used.

Section ID – Sets the identification of the object (together for the entire object or individually for sections).

WARNING: The factory default setting is zero, which means that the communicator will not transmit any reports!

Selection of transmitted events – Selection of types of reported events and the option to set codes for additional reports (PG outputs, special reports A to D).

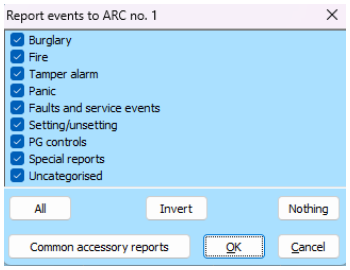


Figure 60 – Reported events

Timing – Setting time limits for transfers and connection check periods.

ARC test – Press to transfer a manual connection check test using the relevant protocol.

Note – For recording details about ARC settings, service start date, etc.

4.2.11.1 Transfer of photos to external storage

If the MyJABLOTRON service is activated in the region/country and the device user will be using it, the relevant service operator will make the necessary settings during activation.

4.3 Additional settings

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

The top menu provides instant access to virtual keypads, system events, settings, RF signal of radio modules, object map, mode changes, local or remote access to the control panel. The following chapters describe the individual settings tabs.

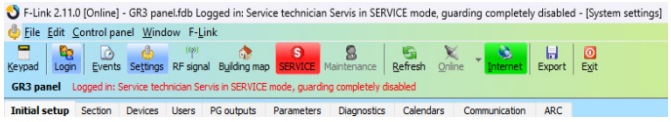


Figure 61 – Settings – top bar (F-Link)

4.3.1 Keypad (virtual)

The virtual keypad in F-Link and JA-100-Link allows control (of sections, PG outputs) using segments (rather than number keys) with authorisation from the F-Link login. No access codes are entered.

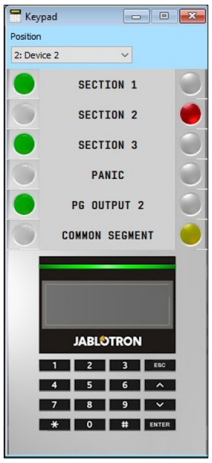


Figure 62 – Virtual keyboard 1 (F–Link)



Figure 63 – Virtual keypad 2 (F–Link)

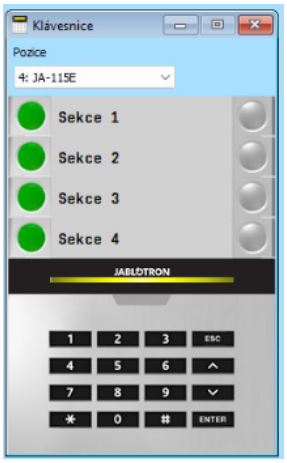


Figure 64 – Virtual Keyboard 3 (F–Link)

The system can also be controlled locally and remotely (set and unset) by clicking on the section status icons in the bottom bar, as well as by using the section status buttons in the Sections tab.

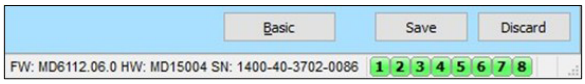


Figure 65 – Settings – bottom bar (F–Link)

4.3.2 Events

Access to the event memory can be found in F-Link under the Events button in the top menu, then select "Event memory". The control panel memory (micro SD card) can store up to several million records with a serial number, exact time with date 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

Figure 66 – Events (F–Link)

Event memory (also available by pressing F8) – Loads approximately 100 kB of events (from the micro SD card). If the load range is insufficient, you can repeatedly select Load / Next 100 (500) kB, range from – to, or all.

RefreshLoad – Allows you to load further events in the history in increments of 100 kB, 500 kB, or all (100 kB corresponds to approximately 1200 events).

Highlight – Colour highlighting allows you to distinguish between different types of events (alarm in red, control in green, fault in orange, tampers in blue, neutral in pale blue, automation or transfers in grey, etc.).

Filter settings – The filter allows you to select the information you are looking for in great detail in terms of time, event type, section, user, device or PG output. Filters can be combined to increase the efficiency of searching in the deep history.

WARNING: If Load/All is selected, loading may take several minutes for control panels with longer operating times. Events that occur during service settings are not recorded in the memory (only the entry and exit from service is recorded). Loaded events can be saved to a file in the File menu using the Export item (Shift+Ctrl+S) in several formats (FDE, PDF, TXT, CSV, XML, HTM or HTML). The FDE extension allows events to be reloaded via F-Link.

NOTE: Loading the range from – to (date) is only available for remote connections.

Online events (also available by pressing F7) – Shows all events that occur after activating this option to a temporary table , including events during service settings.

Online signals (also available by pressing F6) – Shows all signals recorded by the control panel (e.g. including detector activation and deactivation) to a temporary table .

Events from file – Events can be opened from a file saved in FDE database format (see Events from control panel memory).

4.3.3 Settings

A window with tabs for setting the behaviour of the system, all devices, sections, users, PG outputs, communicators and transfers to the ARC, located under the "Settings" button in the top menu.

1. System settings are opened and closed using the **Settings** button in the top toolbar.
   - You can switch between tabs in the card: **Initial setup, Sections, Devices, Users, Reports**, etc.
   - The tab displays the current settings of the control panel loaded when the F-Link software (hereinafter referred to as SW) is started. The **Refresh** button in the top menu can be used to reload the current contents of the control panel at any time.
   - To view previous control panel settings, use the History tab in the upper right corner. The history cannot be changed, but it can be saved to the control panel (if you need to return to previous settings). A maximum of 10 previous settings are recorded in the history (sorted by date and time), as well as all system configuration change histories.
2. You can import settings from another installation into the system, e.g. after replacing the control panel with a new one. If the control panel is replaced with another one, a completely new database is created after connecting to the computer. To import settings from another database, select File / Import in the main menu in the top bar and select the file (database) from which you want to import. After this selection, the **Import** button button in the **Settings** tab becomes active.



Figure 67 – Settings – top toolbar (F–Link)

3. For simpler applications, only **the basic functions** of the system can be configure d. If you need to configure **all** system **functions**, use the Advanced button in the lower right corner. Repeated pressing this button hides the advanced settings options (their settings remain valid even when hidden). The Advanced/Basic button is also available in other work tabs.

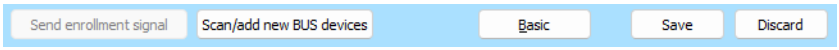


Figure 68 – Settings – bottom toolbar (F–Link)

4. **When you enter a change to the settings, it will be highlighted in blue text** (the tab name will also turn blue). The blue highlighting will disappear once you save the changes.

5. You can **save the settings by clicking the Save button** (bottom right). If you are saving the settings to the control panel for the first time, the software will ask you **to enter a file name**. A file with the extension *.FDB will be created on your computer under this name, in which the settings history will be gradually archived (each time you save the settings to the control panel). If you do not want to save the changes, select the **Cancel** button and then select **Ignore** in the confirmation prompt. The parameters can be changed in multiple tabs and the changes can then be saved together.
6. The **Scan/add new Bus devices button** on the bottom bar of the Devices tab opens a dialogue box for bulk assignment (without the option to select positions) of those devices that are connected to the Bus and have not yet been enrolled to the system in any other way. For enrolling devices individually, see 4.2.3.1 Assigning or removing devices.
7. The **Send enrolment signal** button on the bottom bar of the Devices and PG outputs tabs sends the control panel's enrolment code to wireless devices, e.g. wireless output modules.
8. **All properties can be set in Service mode** (the system is not guarding). Service is turned on and off using the Service button in the top toolbar.
9. **Some properties can be changed during operation.** The Settings tab can therefore be opened without switching to Service mode. However, only available options can be set.
10. **The software includes tooltips** – when you place the mouse cursor over an item, a text description is displayed. Tooltips can be disabled in the F-Link drop-down menu.

Possible problems when using the System Settings tab:

Problem	Possible cause
Unable to change any or some of the displayed parameters	■ The system is not in Service mode and this is a function that can only be changed in Service mode. ■ No Service Code was entered when the software was launched and you do not have authorisation. ■ This is a setting that cannot be changed (service technician authorisation, control panel position, devices not supported, etc.). ■ The ARC card settings have been blocked by a ARC technician. ■ You are offline. ■ You have the EN 50131 compliance parameter enabled.
The required parameter cannot be found.	■ Only the basic menu is displayed; use the Advanced button. ■ You cannot see the entire settings card on the monitor – use the scroll bar or enlarge the window. ■ You are authorised by a code with a different access level.
The positions are sorted differently	■ By clicking on the column heading, you can select the column by which the positions are sorted; by clicking repeatedly, you can change the sorting to ascending or descending.
A certain tab is missing	■ If the PG outputs tab is not available, check that the number of PG outputs set to zero in the Range tab. ■ The ARC tab is not available if you do not have sufficient permissions for it (it may be locked by a ARC technician). ■ It is also unavailable after registering the system in the MyJABLOTRON web application. ■ You have an older version of the F-Link software (JA-100-Link).
Internal settings cannot be configure d in the Devices tab	■ Check that the devices are correctly connected, assigned and functional. ■ Service mode is not enabled. ■ Some devices do not have internal settings. ■ Older versions of F-Link may not support new types of devices. ■ If it is a wireless device, check that you have a connected and functional radio module.
Devices cannot be enrolled in the Devices tab	■ For wireless devices – you do not yet have a JA-11xR radio module assigned. ■ The yellow LED on the Bus device should flash regularly. If it does not flash, the device is not connected correctly or has not yet stabilised after being powered up (this may take up to 180 seconds). ■ Service mode is not enabled. ■ Older versions of F-Link may not support new types of devices.
PG output does not respond to device activation	■ Check that the system is not switched to Service mode. ■ In the Diagnostics tab, check whether the device is transmitting information to the control panel. In the PG Outputs tab, check whether the output is blocked by the status of the section, device or calendar; check that the Function column settings are correct. ■ On the Jx-11xN and JA-15xN modules, check that the binary address and module function are preset correctly on the DIP switches.

Table 34 – Possible system configuration problems

4.3.4 RF signal

Window for graphical display of radio band interference intensity with a selection of used radio modules. The presence of unknown signals in the band is displayed in red. The communication signals of the system itself (learned devices) are displayed in green, and the selected device from the Highlighted Devices list is displayed in blue (see Figure 69 – RF signal (F-Link)). The background (interference) is shown in grey. The Disable Unknown Devices item can be used to filter out unknown devices and display only the devices in the system.

The monitored interference logging (while the RF Signal window is open) can be exported from the main menu to a file with the FDR extension and imported back for viewing using the button.



Figure 69 – RF signal (F–Link)

4.3.5 Buidling map

You can insert a floor plan in bitmap format (jpg, gif, bmp, tif, png, etc.) for each floor of the object separately into the object map, or you can create your own by drawing simple lines. You can insert icons of only the devices used from the menu bar into each floor by simply dragging and dropping. Saving the object map with icons for archiving can be printed or saved as a BMP image using the Print or Export option in the main menu.

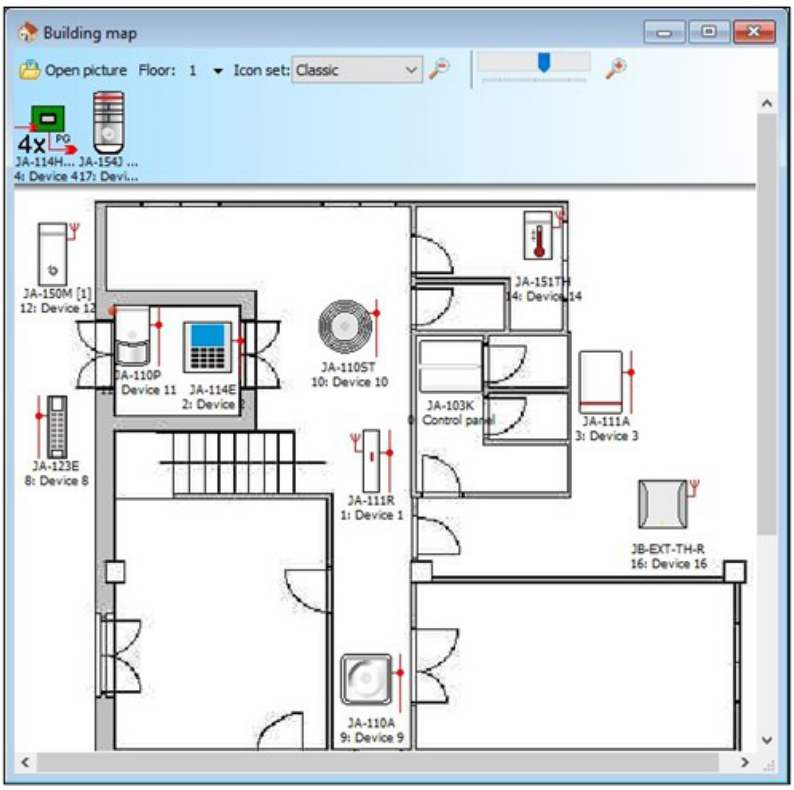


Figure 70 – Building map (F–Link)

4.3.6 Service

Switching the control panel mode between Unset state (where you can make changes to the settings in all tabs except the Settings tab) and Service mode (you can make changes in the Devices tab, including learning, changing internal settings and deleting devices).

4.3.7 Maintenance

Switching the control panel mode between Unset state and Maintenance mode. In Maintenance mode, the system cannot be controlled and ignores all alarms, including tamper alarms. Suitable , for example, for replacing batteries in wireless detectors without the need for a service technician.

4.3.8 Refresh

Updating the internal settings of devices during hardware changes, e.g. adding segments to access modules or keypads.

4.3.9 Online

Connecting or disconnecting F-Link from the control panel via a USB cable. When connected, the software automatically searches for the port on which the control panel communicates.

4.3.10 Internet

Remote connection or disconnection of F-Link from the control panel via the Internet. The prerequisite for establishing a connection is a correctly entered registration code (automatically pre-filled from the database used to program the control panel), the telephone number of the SIM card in the control panel (also pre-filled from the Installation Information) and a computer connected to the Internet. Remote access can be disabled on the Communication / Communication Type tab by selecting None. When using a SDC SIM, the PCO tab and button in Communication tab isv hidden.

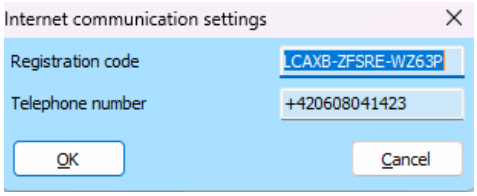


Figure 71 – Internet communication settings (F–Link)

After clicking on the Internet button, a dialogue box with pre-filled data will appear. If you are connecting from a new "empty" database, you will need to enter the registration code and telephone number. When using a security SIM card and a LAN communicator, it is not necessary to enter a telephone number. Establishing a connection takes only a few seconds, but downloading the configuration depends on the size of the system and may take up to several minutes. However, downloading the configuration usually takes about 1 to 2 minutes.

NOTE: Information about the GPRS/LAN connection and the amount of data sent and received is displayed in the lower right corner.

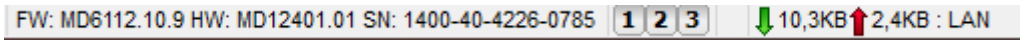


Figure 72 – Establishing a GPRS/LAN connection (F–Link)

4.3.11 Installation wizzard

A wizard for step-by-step navigation through the Settings tabs, which facilitates the system programming process. The wizard is activated in the main menu of the Control Panel and deactivated by clicking the Close button in the lower right corner of the Wizard window.

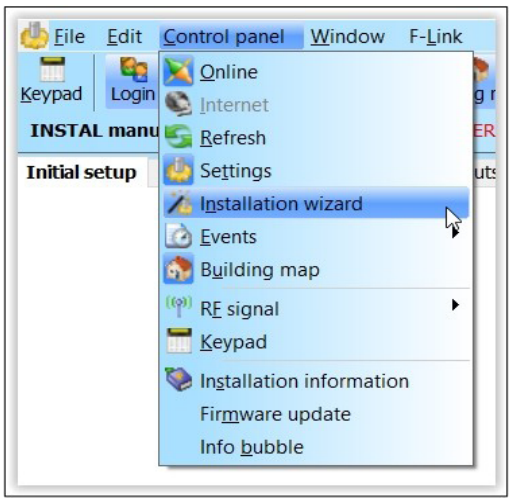


Figure 73 – Installation wizzard (F–Link)

4.3.12 Installation information

The window contains items for recording contact information about the system owner, the system itself, or an external document associated with the object (offer, handover protocol, invoice, etc.). In the text field , the installation technician can enter notes and information obtained during installation, which may be helpful with expanding the system, for example.

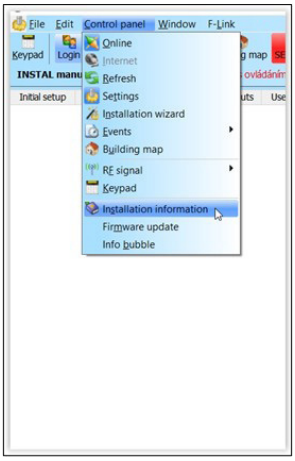


Figure 74 – Installation Information 1 (F–Link)

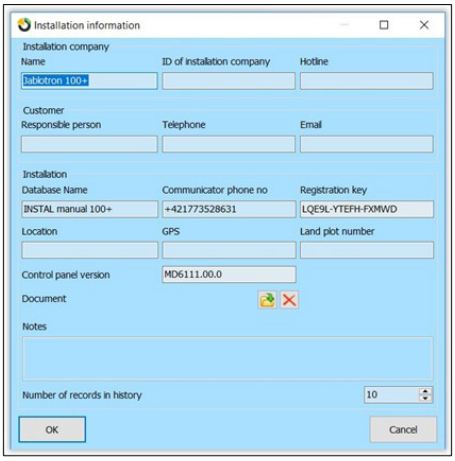


Figure 75 – Installation information 2 (F–Link)

4.3.13 Firmware update

Firmware updates allow you to change the behaviour of devices that can be updated (control panels, radio modules, keypads, detectors, etc.) using a package that the manufacturer officially releases on the JABLOTRON server. These firmware updates are downloaded by F-Link itself (upon request) from the JABLOTRON server if the Automatic update item is enabled in the F-Link menu (enabled by default). If the item is not enabled, F-Link will allow you to manually search for the path to the .fwf files on your computer before updating the system.

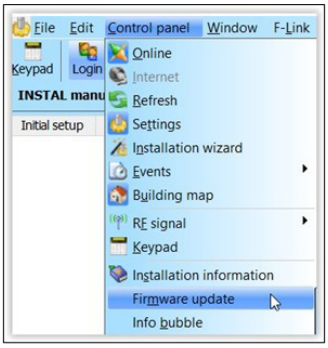


Figure 76 – FW Update (F–Link)

4.3.14 Label printing

To print the labels of the access module segments, use the Print Labels function in the Internal Settings window of each access module used, see Segments tab Segments tab.

You can enter your own text when printing labels. The software does not save the entered text after printing. When printing labels, you can align the text to the left or centre it.

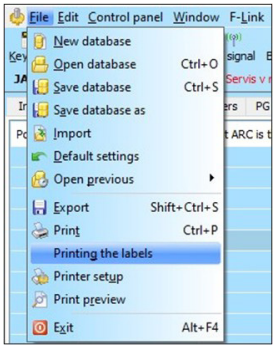


Figure 77 – Label printing (F–Link)

4.3.15 Settings history

Each time any element in the entire system is reconfigure d, the control panel saves its settings to an SD card. At the same time, an event called "configuration backup created" is added to the history with information about the file name containing the configuration before the change was made. This makes it possible to return to the previous settings or simply view them to find out when and what changes were made. All you need to do is search for the configuration change in F-Link in Events from memory by date and time of the event (see 4.3.2) and, to compare it with the current system settings, load it and select it in the "History" tab available in the upper right corner of the "System Settings" window. The changes made are displayed in blue italics. From the loaded configuration backup, you can save these settings by accepting the changes with the "Save" button or, after reviewing the changes, return to the current settings by clicking on the "Current" tab in the upper right corner. Configuration changes are saved to the SD card in the BACKUP directory in the CFGxxxxx.bak file with the serial number of the change.

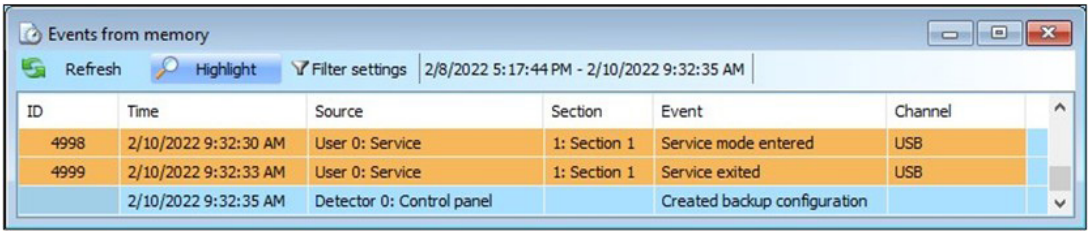


Figure 78 – Events from memory (F–Link)

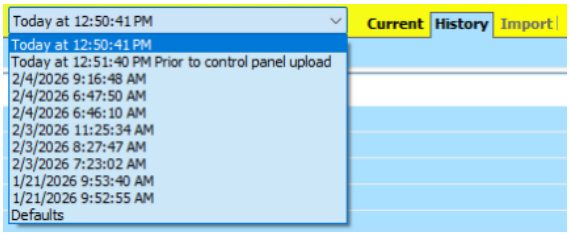


Figure 79 – History (F–Link)

The F-Link software also stores the latest system configuration changes in its own database. This history of setting changes is used, among other things, when updating the control panel firmware, when the previous settings are always lost due to the change made, and thanks to the latest history, the settings can be restored to their pre-update state. The same option applies when resetting the control panel to factory settings, replacing the SD card, switching languages, or simply when settings are changed unintentionally, resulting in the deletion of text that can be restored in this way.

5 System control

NOTICE: The range of control functions depends on the local system configuration and the choice of control devices.

The alarm system can be controlled in several ways. The basic division of control is:

Local control

Method	Device / Function	Control description
LCD touch keypad	JA-116E, JA-156E	Control is possible after user authorisation and pressing the relevant section button or PG on the touch screen.
Keypad with segment	JA-114E, JA-113E, JA-154E, JA-153E, JA-115E, JA-155E	Can be controlled after user authorisation and pressing the relevant segment button or, in the case of the LCD version, the menu item.
Keypad	JA-123E, JA-121E	Can be controlled after user authorisation and pressing the relevant control button or menu item.
Reader with segment	JA-112E, JA-152E, JA-122E, JA-120E (controls PG only)	Can be controlled after user authorisation using a chip and pressing the segment button.
Remote control	JA-15xJ, JA-16xJ	Setting and unsetting by pressing a preset button on the remote control.
Calendar	Up to 64 time-adjustable actions	Each calendar event has an option for the event and the time and day on which it is to be performed. It can control sections and PG. PG can also block.
JA-100-Link (F-Link) software	PC with Windows	After authorisation, sections and PG outputs can be controlled via a virtual keypad.
Control module	JA-111H-AD TRB, JA-121T	The system can be controlled by an external device (by activating the module's wired input or data communication).

Table 35 – Local system control

Remote control

Method *)	Device	Control description
Voice menu ***)	Telephone	After authorisation, the system can be controlled by dialling the communicator's telephone number using tone dialling (DTMF).
SMS message ***)	Mobile phone	Both sections and programmable outputs can be controlled by an authorised command to switch on or off.
By ringing/dialling in from an authorised telephone number ***)	Telephone (controls PG only)	Each authorised telephone number can control one selected PG output.
MyJABLOTRON web application **)	PC	After authorisation, you can control sections, PG outputs, and view records from photo devices, thermometers or electricity meters.
MyJABLOTRON mobile application **)	Smartphone or tablet	After authorisation, you can control sections, PG outputs, and view records from photo devices, thermometers or electricity meters.
SW JA-100-Link (F-Link)	PC with Windows	After authorisation, you can control sections and PG outputs via a virtual keypad.
*) With a GSM communicator installed in the control panel **) Mandatory registration of the system in the JABLOTRON cloud (service may be subject to a fee) ***) For voice calls, ringing and SMS, it is necessary to use JA-194Y and a SIM card that supports this.		

Table 36 – Remote system control

All of the methods described can be used to control the system for both section monitoring (full setting, partial setting and unsetting) and programmable outputs (switching on, timing, switching off). The only exceptions are outdoor readers JA-121E, JA-120E and the function of ringing from an authorised telephone number, which can only be used to control the PG output.

5.1 User authorisation

To determine whether the operator is a system user and is authorised to perform a given action, they must authorise themselves during operation. Based on the authorisation, the system then decides whether the user in question has the authorisation to control the required sections, programmable PG outputs, or whether they can only view the system status and event history in the LCD keypad menu. Each system user can be assigned the following authorisation options (see 2.8.4 Authorisation means of the JABLOTRON system):

- access code (4, 6 or 8-digit number with or without a prefix);
- chip, card or tag (up to two positions for one element);
- telephone number for authorisation during remote access by telephone, voice channel or SMS.

NOTICE: Confirming the user code with a card reduces the risk of unauthorised control or circumvention of the system by a third party!

5.2 Keypad control

Keypads are the main element for everyday control of the JABLOTRON alarm system. They allow users to intuitively perform basic tasks such as setting and unsetting the system, controlling selected sections, activating partial setting or controlling programmable outputs (PG).

5.2.1 System control from the keypad segment

The alarm system is best controlled and its status monitored using the system keypad control module, where the main coloured LED illuminated button can be used to detect exceptional situations (faults and alarms) and the segments can be used to control the system or monitor the status of sections and PG outputs and other system information (alarm memory indication, panic or medical alarm triggereing). By using a keypad with an LCD display, it is possible, after authorisation with the appropriate permission, to check more detailed information about the system, faults, event history, active or blocked detectors, or detectors preventing the system setting. Without authorisation, menu items are not available and, depending on the settings of each keypad, segments signalling section statuses may not be available either, thus ensuring that unauthorised users cannot read or operate the keypad.

The basic function of the keypad in the alarm system is to control the setting and unsetting of sections. Setting is divided into partial and full. Control can be fully performed from the LCD keypad menu or segments. Depending on the settings, segments can be set fully or only partially, or both partially and fully, either with authorisation (the event history records who set which section) or without authorisation (no code is required, so the setting user is not specified in the event history). When unsetting sections using segments, user authorisation is always required, so that the event history always records which user performed the unsetting. The segment buttons can be clearly labelled and colour-coded (traffic light logic) so that their status is clearly indicated at a glance. The segment can also be used to indicate status (e.g. open garage door) or to control various automation devices (e.g. heating or blinds). If the segments are removable, a maximum of 20 segments can be connected to one keypad.

Only 4 segments are available for the JA-115E/JA-155E keypad. The segment can also be used to call for help in an emergency (medical or panic alarm).

It is possible to secure:

1. Setting the entire section before leaving the premises

When operating the system from a keypad located in a guarded area, it is necessary to set the entrance and exit routes to the keypad with detectors with a delayed reaction. Unlike an instant reaction, a delayed and next delayed reaction is not guarded during the exit delay after setting the section. After setting the system, the user must be able to reliably leave the premises before the exit delay ends. Upon entry the set building, the entry delay is activated, during which the user must be able to safely walk along the entry route to the keypad, where the system is unset. If the user does not unset the section with entry time within the preset time, an alarm is triggered in the delayed zone. In the event of intrusion into the building by a route other than the entrance route, the system will sound an alarm in the instant zone, which will trigger the sirens without delay. Full set system is indicated by the red colour of the segment or the full framing of the section number on the LCD keypad display.

2. Partial setting when the user remains in the building:

In partial setting mode, when the user remains in the building and only perimeter protection is set, there are two control options:

a) Control from a keypad located in the guarded perimeter protection zone (e.g. guarded entrance corridor, etc.). Detectors in the entrance zone with a control keypad must be configure d to a delayed loop. When the system is set, they trigger an entry delay.

b) Control from a keypad that is not located in the guarded access zone (e.g. internal corridor, staircase, bedroom, etc.). With this option, it is not possible for another person to enter the building from outside without triggering an instant alarm. Entry into the building is only possible after prior unsetting (e.g. by remote control, remotely via voice menu, SMS or the MyJABLOTRON application). In this case, the entry zones are set to the "Instant / Delayed A" reaction.

Partial setting is indicated by a yellow segment or a faint line framing the section number on the LCD display of the keypad.

Procedure for controlling the alarm system from the keypad:

Since you can choose from multiple system profile settings that meet the different requirements of different standards, this results, among other things, in differences in keypad behaviour and differences in the control procedure. The system can be controlled in two ways:

1. Control method – option 1 (for all system profiles):

Setting the system:

F*or universal control of the system from the keypad, you must first authorise yourself, because the segments may not (depending on their settings) signal their status without authorisation!*

1. Authorisation is performed by entering a code or attaching a contactless chip or card (if both a code and a card are required, they are entered and attached in any order).
2. The unset status of the section specified in the segment name is indicated by a steady green LED on the left.
3. Press the right button of the segment to select the request for setting. You can select one or more requests depending on the number of segments used.
4. If the segment LED continues to flash red (or yellow) for 8 seconds after selection, the system reports a problem with setting (for more information, see 5.11.2 Reasons preventing system security).
5. Successful setting or partial setting is confirmed by the red or yellow LED lighting up.

Unsetting the system:

F*or universal control of the system from the keypad, you must first authorise yourself, because the segments may not (depending on their settings) signal their status without authorisation!*

1. Authorisation is performed by entering a code or attaching a contactless chip or card (if both a code and a card are required, they are entered and attached in any order).
2. When the section is set, the red or yellow LED lights up continuously. Violation of the protected area triggers an entry delay, which is indicated on the keypad by the green LED flashing rapidly.
3. The request to unset the selected section is made by pressing the left button of the section (or several sections in sequence).
4. Successful release is confirmed by the green LED on the segment lighting up.
5. If the red LED continues to flash rapidly after unsetting the section, this indicates an alarm memory report in the section. This signal can be deleted by pressing the green button on the segment again and further authorisation with the right to delete the alarm memory, or you can select the "Cancel warning indication" item in the LCD keypad menu.

2. Control method – option 2 (only when the "Default" system profile is set):

Setting the system:

This type of control is based on the procedure "first select the request on the segments and then authorise".

1. The unset status of the section specified in the segment name is indicated by a steady green LED on the left.
2. Press the right button of the segment(s) to select the request for setting. One or more requests can be selected depending on the number of segments used.
3. If authorisation is required to set the section, the red (full settting) or yellow (partial setting) LED of the segment flashes slowly to indicate that it is waiting for user authorisation (8 seconds).
4. Authorisation is performed by entering the code or attaching the chip or card (if both the code and card are required, the code and card are entered and attached in any order).
5. If the segment continues to flash red (or yellow) after authorisation, the system reports a problem with setting (for more information, see 5.11.2 Reasons preventing system security).
6. Successful setting or partial setting is confirmed by the red or yellow LED lighting up.

Unsetting the system:

1. When the section is set, the red or yellow LED lights up continuously. Intrusion into the protected area triggers an entry delay, which is indicated on the keypad by rapid flashing of the corresponding LED.
2. To unset the selected section, press the corresponding left button of the segment (or several segments in sequence), which will flash slowly to indicate that it is waiting for authorisation.
3. Authorisation is performed by entering the code or attaching the chip or card (if both the code and card are required, the code and card are entered and attached in any order).
4. Successful release is confirmed by the green LED on the segment lighting up.
5. If the red LED continues to flash rapidly after the section has been unset, this indicates an alarm memory message in the section. This signal can be deleted by pressing the green segment button again and further authorisation with the right to delete the alarm memory, or you can select the "Cancel warning indication" item in the keypad menu.

5.2.2 System control from the JA-114E, JA-115E and JA-116E keypads

The status of individual sections is indicated by status indicators for each section. The actual control (setting or unsetting the system and other automation functions) is performed using function buttons. The function buttons of the sections and status indicators are illuminated in colour so that the status of the sections is clearly indicated at a glance.

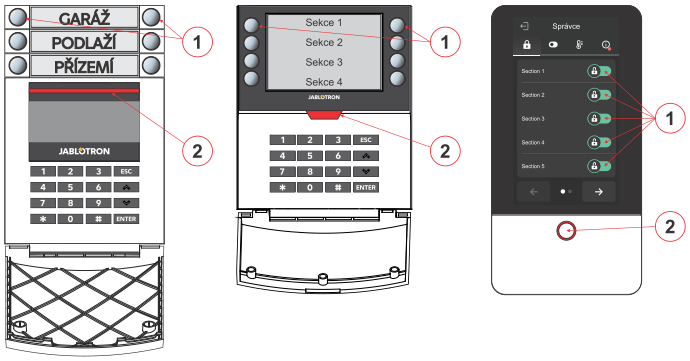


Figure 80 – Section/PG control and optical indication

1 – section and PG control (segments and widgets), 2 – LED status indication

GREEN	**– unset**
YELLOW	**– partially set**
RED	– set

Authorisation is performed by entering a code on the keypad or by placing a card (or tag) assigned to a specific user in the system. If the user wants to control multiple sections at once, after authorisation, they press the function buttons of the desired sections in sequence. This allows all sections to be controlled with a single authorisation (e.g. setting the house and unsetting the garage).

Setting:

1. Authorise yourself on the keypad. The buttons for the sections to which you have access will light up, and the system indicator on the keypad will flash green.
2. Press the function button to set the desired section. It is possible to set multiple sections in sequence. However, the delay between selecting sections must not exceed 2 seconds.
3. The command is executed, and the keypad acoustically indicates the exit time. The section is now set, and only detectors with a "Delayed" reaction during the exit delay allow you to leave the set area. The status indicator and function button of the set section light up red.

If certain status detectors are active during setting (e.g. an open window), the system will behave (based on the defined configuration) in one of the following ways:

a. The system will set, and active detectors will be automatically bypassed *).
b. The system will flash the function button red for 8 seconds to indicate that detectors are active in the system, then it will set itself (active detectors will be bypassed) *).
c. The section with active detectors can be set by repeated pressing the section function button. The user must confirm their intention to set the section with active devices (e.g. an open window). Otherwise, the section with an active detector will not be set.
d. An active detector prevents the section from being set. This status is indicated by the function button flashing red. The devices preventing setting can be read in the menu on the LCD display.

) NOTE: Options a) and b) are not supported for EN 50131 Security Grade 2/3, INCERT and SSF 1014 configurations (preset control panel profile).

If a detector with an "INSTANT" reaction is activated during the exit delay period, or if a detector with a "DELAYED" reactions remains active after the exit delay period has elapsed, the system will unset again. Unsuccessful setting is indicated by the yellow flashing of the system indicator, reported to the ARC and indicated by an external siren (applies to Security Grade 2).

If the system is configure d to be set without authorisation, it is not necessary to perform authorisation; simply press the function button for the given section. It is also possible to configuresetting by authorisation only.

WARNING: Setting without authorisation reduces the maximum possible classification of the system to Security Grade

The application of this option must be considered with regard to all risks associated with its use.

Consult your designer or service technician for the required system behaviour settings.

Unsetting:

1. After entering the building (activation of the detector with a "Delayed" reaction), the system will signal the entry delay with a continuous beeping sound and red flashing of the status indicator and function button of the section in which the entry delay is taking place.
2. Authorise yourself on the keypad – the system indicator will flash green.
3. Press the function buttons for the sections you want to unset.
4. The command will be executed, and the function buttons and status indicators will light up green to indicate that the sections have been unset.

NOTE: If the "Unset section by authorisation only during entry delay" option is enabled, simply authorising will unset the section in which the entry delay is in progress. This option must be used with caution in multi-section systems.

Consult a service technician for the required authorisation panel behaviour settings.

Partial setting:

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

The system can also be set to partial setting, which allows monitoring using only selected detectors in the section.

EXAMPLE: Overnight, only windows and doors can be set, while motion detectors inside the space do not respond..

Procedure:

- Authorise yourself on the keypad (by entering the code or placing the card/tag). The system indicator will flash green.
- Press the function button for the relevant section
- The command is executed, the function button and status indicator light up yellow continuously to indicate that the section is partially set.
- If you want to fully set a building in which partial setting is enabled, press and hold the function button (2 seconds) or press it twice. After the first press, the button lights up yellow, after the second press, it lights up red.
- To fully set the system from the partially set state (function button lit yellow), press and hold the yellow button after authorisation. After pressing, the system will be fully set and the button will change colour to red.
- Partial setting can be configure d so that it can be performed without authorisation.

To unset from the partially set state after authorisation, press the yellow button. After pressing, the system will be unset and the button will turn green.

Controlling sections by authorisation only:

The system can be configure d by a service technician to control by authorisation only. With such a configuration, the system will change the status of all assigned sections by authorisation only on the keypad (by entering a code or attaching a chip).

Controlling sections from the keypad menu:

Control procedure from the keypad menu:

1. Authorise yourself with a valid code or chip
2. Enter the menu by pressing the ENTER key
3. Section control → ENTER
4. Use the arrow keys to select the desired section
5. Press the ENTER key repeatedly to change the section status to partial setting / setting / unsetting
   - Symbol for partial setting: 1
   - Symbol for full setting: 1
6. After completing the control, exit the menu by pressing the ESC key

Structure and description of the internal menu of the JA-114E, JA-154E, JA-115E, and JA-155E keypads



Figure 81 – Internal settings of segment keypads

Structure and description of the internal menu of JA-116E and JA-156E keypads


Logout


Displays the status of individual sections


Displays the status of PG outputs


Displays the status of thermometers and thermostats


Displays information about the last action/status in the system.
Option for further display settings, service contact display, switching to Maintenance mode and event memory display

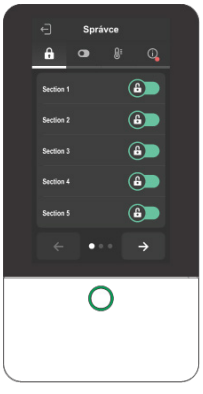


Figure 82 – Internal settings of touch keyboards

Overview of optical indication of keypad button statuses:

Optical indication	Description
Steadily lit green	Normal status. Sections controlled from the keypad are OK, no malfunction.
Solid yellow	System idle state with a fault report in one of the sections controlled by the keypad. More detailed information about the fault is available after authorisation, depending on the user's permissions, in the LCD keypad menu. If the optical signal is accompanied by a rotating JABLOTRON logo on the LCD keypad, this indicates a fault in the radio communication between the keypad and the control panel.
Steadily lit red	The keypad is in BOOT mode, which is used when updating the firmware.
Flashing green (2Hz)	Ongoing authorisation status, during which the user can select status changes on the segments or browse the LCD keypad menu. The authorisation status lasts for 8 seconds from the last keystroke or can be terminated with the ESC key.
Flashing yellow (8Hz)	Indicates unsuccessful setting.
Flashing red (8Hz)	Indicates an ongoing alarm in a section controlled from the given keypad. The type of alarm, the name of the section in which the alarm is occurring, and the source that caused the alarm are shown on the keypad LCD display.
Flashing alternately red/yellow	Ongoing alarm with active fault.
Flashing alternately green/red	Authorisation status with ongoing alarm or alarm memory.
Flashing alternately green/yellow	Authorisation status in progress with active fault.
Every 2 seconds Flashes yellow twice	Programming mode Service. In this mode, no segments are lit or available and no menus are available to users and administrators. For service technicians, the menu in Service mode is available only if no computer is connected to the control panel.
Every 2 seconds 2x flashes red	Alarm memory indication.
Every 2 seconds Flashes green twice	Maintenance mode. In this mode, the segments of sections that are switched to Maintenance do not light up.
Every 2 seconds 1x flashes yellow	Fault indication on the keypad in energy-saving sleep mode (only for EN50131-1 profile) .
Every 2 seconds 1x flashes red	Alarm memory indication on the keypad in energy-saving sleep mode (only for EN50131-1 Profile).
No indication	Keypad in energy-saving sleep mode.

Table 37 – Overview of an optical indication

Overview of an optical indication of states on keypad segments:

Optical indication of the segment	System status
Segment lights up green	Section status unset or PG status off
Segment flashes green (4Hz)	Active entry delay and waiting for unsetting
Segment lights up yellow	Section status is partially set
Segment lights up red	Section status is set or PG status is on
Segment flashes yellow (4Hz)	Waiting for authorisation during partial setting or reporting a problem during partial setting
Segment flashes yellow (8Hz)	Unsuccessful setting indication
Segment flashes red (4Hz)	Waiting for authorisation during security check or reporting a problem during security check
Segment flashes red (8Hz)	Alarm memory. It is signalled until it is deleted.
Segment not lit at all	Status: off, service, maintenance, section blocked after alarm (after blocking and deleting the alarm memory)

Table 38 – Overview of an optical segment indication

5.3 Remote control

If the user needs to control the security status before entering the secured area (when arriving by car in the garage) or if the building is secured exclusively by detectors with instant reaction that do not allow access to the keypad for unsetting, such a system can be controlled by remote control from outside before entering the building. Wireless controllers are used for this purpose. The JA-11xR radio module must be programmed into the system to receive wireless devices. It must be located in the building so as to enable reliable reception of remote-control signals at the required the required control distance.

Pairs of remote control buttons (JA-15xJ, JA-16xJ) behave identically to keypad segment buttons for controlling sections. Each button can control a selected section or sections (the right button always sets and the left one unsets). Remote controls respect the rules of system setting readiness, so it will not be possible to set a section with an obstacle preventing setting. Similar to keypad segments, two-way controllers also feature optical signalling with a three-colour indicator.

Optical status signals on two-way remote controllers (JA-15xJ) displayed after pressing a button:

Optical signalling of remote controllers	System status
LED lights up green	Section status unset or PG status off
LED lights up yellow	Section status partially set
LED lights up red	Section status set or PG status on
LED flashes red	There is an obstacle in the section preventing setting
LED flashes yellow	Command result unknown (e.g. communication error, out of radio range, etc.)

Table 39 – Overview of remote control optical indication

When using one-way remote controls (JA-16xJ, JA-18x), they control the system in the same way, but their optical signalling (red LED only) only confirms that the button has been pressed and the command has been sent. They do not provide feedback from the control panel, and the user must use other signalling to confirm a change in the status of the section (siren sound when the status of the section or PG output changes, other optical signalling, or a confirmation SMS message about setting or unsetting).

5.4 Calendar control

Automatic control of the system or its parts can be performed using the internal calendar in the control panel. The calendar allows you to configure up to 64 calendar events – automatic control of sections or programmable outputs. The calendar also allows you to preset a specific service inspection date, which is independent of the control panel's "service request" function in the Parameters tab.

Each calendar event can be defined for a day of the week, month, and month of the year. This allows you to set up an event from one specific day of the year to regular repetition on specified days (e.g., once a week or once a month). On the selected day, it is possible to preset up to 4 times at which the calendar event will take place or select the option of repeating at regular intervals. Repetitions at intervals can also be defined in terms of time from – to. A typical example of calendar control is automatic setting of a section in a shop, partial setting of a building at night, or lighting control in the evening and at night. Each automatic event is recorded in the event history with the source "Calendar".

Options for setting calendar event control for monitoring:

Action / Status	Description
Unset	Unset the set section (sections) from any set state (full or partial).
Set partially	Partially sets the set section(s), activates the exit delay timing for 180 seconds (regardless the standard exit time setting), during which all alarm zones behave as if delayed. This extended exit delay time is intended as a warning to any user in the building that the system has been partially set by the automatic timer. Unless otherwise set on the Parameters tab, partial setting is not signalled acoustically by default. With this type of setting, the control panel accepts the setting methods and checks the system readiness rules!
Set	Sets the defined section (sections), activates the acoustic exit delay beeping for 180 seconds (regardless of the standard exit time setting), during which all alarm zones behave as if delayed. This extended exit delay acoustic signal is intended as a warning to any user in the building that the system has been set by the automatic timer. During this time, the user must immediately go to the keypad and unset the set section in the usual manner or leave the building. If the user remains in the building even after the exit delay has expired, an alarm will be triggered in the set section. With this type of setting, the control panel accepts the setting methods and checks the system's readiness for setting!
Set immediately	It sets the defined section (sections) immediately without any exit delay or acoustic signal. The system is thus set immediately at the given time, preventing any movement within the building. If anyone moves within the building after this moment, an alarm will be triggered in the set section. This option is designed for silent and quick setting without notification. With this type of setting, the control panel accepts the setting methods and checks the system's readiness for setting!
Set partially now	Partially setting of defined section(s) immediately(now), without an exit delay or any acoustic indication. The system is thus set immediately at the given time. This option is designed for quiet and quick security without notification. With this type of setting, the control panel accepts the setting methods and checks the system setting readiness rules!
Set always	Sets the defined section (sections), activates the exit delay acoustic signal for 180 seconds (regardless of the standard exit delay time), during which all alarm zones behave as if delayed. With this type of setting, the control panel does not check the setting methods or the system readiness rules for setting!
Always set partially	Partially sets the defined section (sections), activates the exit delay timing for 180 seconds (regardless of the standard exit delay time), during which all alarm zones behave as if delayed. With this type of setting, the control panel does not check the setting methods or the system readiness rules for setting!
Always set immediately	Sets the defined section (sections) immediately without exit delay or any acoustic signalling. The system is thus set immediately at the given time, preventing any movement within the premises. This option is intended for silent and quick setting without notification. With this type of setting, the control panel does not check the setting methods or the rules for system readiness for setting!
Always set partially and immediately	Partially sets the defined section(s) immediately, without exit delay or any acoustic signalling. The system is thus set immediately at the given time. This option is designed for quiet and fast setting without notification. With this type of setting, the control panel does not check the setting methods or the rules for system readiness for setting!
No	No control function is defined.

Table 40 – Calendar options

PG output control options for calendar events:

PG function	Description
Activate PG	Activates the defined programmable outputs if they are not blocked (e.g. by the calendar, devices or section).
Disable PG	Disables the defined programmable outputs.
Block PG	Begins blocking the defined programmable outputs. These outputs cannot be switched on in any way until they are unblocked by the "Unblock PG" calendar action. Even opening or closing the service mode does not cancel the block.
Unblock PG	Ends the blocking status of the defined programmable outputs.
No	No blocking function is defined.
Technical inspection	At the preset time, it triggers the "System requires service inspection" event in the system, which is displayed together with the Information icon on keypads with an LCD display.

Table 41 – Calendar events

Calendar event blocking function: Each calendar event can be blocked by selected programmable outputs. Blocking means that when the programmable output is active, the corresponding calendar event will not be performed at the specified time.

5.5 Control from the communicator voice menu (GSM)

NOTE: The "User reports" tab is only displayed in the F-Link software when using a full-featured communicator (e.g. when using the JA-194Y communicator, "User reports" can be edited and the tab is visible in the F-Link software; on the other hand, when using the JA-194Y-LITE communicator, the "Reports to users" tab is not displayed at all, as this communicator does not support voice or SMS reports).

If the JA-194Y GSM communicator is installed in the control panel, the alarm system can also be controlled using its integrated voice menu and tone dialling on the telephone. By calling the telephone number of the SIM card used, after the defined number of rings (3 rings by default), the call is answered, the control panel introduces itself with a welcome voice message and, depending on the settings, requests an authorisation code. The caller must first authorise themselves with their access code to gain access to the control system. After verifying the correctness of the code, the system reports the status of the entire system and, depending on the caller's permissions, will offer them the available control options. Depending on the settings of the "No code for voice menu and control SMS" parameter in the Communication tab, the caller can be authorised based on the telephone number stored in the user list, in which case no authorisation code is required. The voice menu can be used to control sections, open and close service mode, and change/record voice messages for the names of individual sections and special reports. The voice menu cannot be used to control programmable outputs.

WARNING: Before setting the property remotely, the user should ensure that no one is inside the property.

Voice menu diagram:

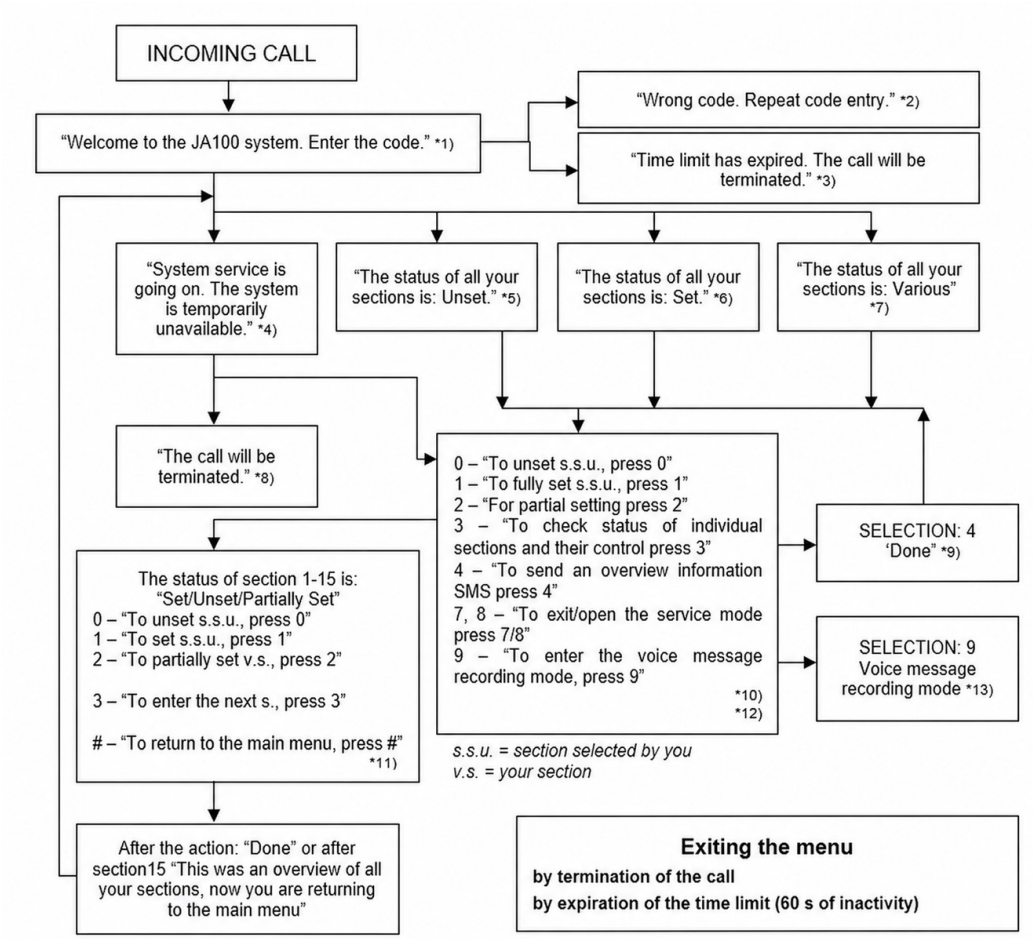


Figure 83 – Voice menu diagram

1) Answers after 3 rings. The number of rings before answering (1.10) can be set in the Communication tab tab and the relevant communicator, where you can also enable access to the voice menu without a code.

*2) Incorrect code entered. After three incorrect entries, the call will be terminated.

*3) Time limit of 60 seconds for entering the code. "Enter code" is repeated every 5 seconds.

*4) The voice menu cannot be used during servicing.

*5) All sections that can be controlled according to authorisation are unset.

*6) All sections that can be controlled according to authorisation are set.

*7) Sections that can be controlled according to authorisation are in various states.

*8) Applies to all authorisations except ARC/Service.

*9) After sending an INFO-SMS to the caller's number.

*10) Menu items that are irrelevant are omitted (e.g. if everything is set, options 1, 2, and 3 are unnecessary).

*11) The menu is adapted to the current status of the section.

*12) If authorisation has been performed using the service code, option 9 "Press 9 for voice message recording mode" is available.

*13) Voice message recording mode OPTION 9:

0 – "To record the installation name, press 0." and then "Press star."

1 – "To record the section name, press 1." Then "Enter the number of the section you want to record." and then "Press the star key."

2 (3,4,5) – "To record report A (B, C, D) messages, press 2 (3, 4, 5)" and then "Press star."

9 – "To delete all recorded messages, press 9."

– "To return to the main menu, press hash."

NOTES:

- 1 – "You do not have permission for this option" – always if you do not have permission to manipulate sections or check status
- 2 – "Important message report required, call will end in 30 seconds" – reports/important messages to the ARC take precedence over the ongoing voice menu
- The start of recording is signalled by a beep. The recorded message is played back immediately after recording.
- If you are not satisfied with the recording, you can immediately choose to re-record.
- It is advisable to start recording immediately after the beep and press the end character * immediately after the recording is finished.
- The name of the installation can be up to 40 seconds long. Any other message can be up to 20 seconds long.

5.6 SMS command control

NOTE: The "User reports" tab is only displayed in the F-Link software when using a full-featured communicator (e.g. when using the JA-194Y communicator, "User reports" can be edited and the tab is visible in the F-Link software; on the other hand, when using the JA-194Y-LITE communicator, the "Reports to users" tab is not displayed at all, as this communicator does not support voice or SMS reports).

If the JA-19xY GSM communicator is installed in the control panel, the security system can be controlled remotely using SMS commands. SMS messages can be used to arm or disarm the entire system as a whole or only selected sections, or you can simply query their status. Programmable outputs can also be switched on and off. The texts of the control commands for controlling the programmable outputs are not preset at the factory and must be selected for remote control. Other texts are already preset.

Command format:

ppp*kkkk_command

where: **ppp** is the serial number of the user code (only when selecting a code with a prefix)

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

kkkk is the user code

_ is a separator space, an empty character

command is an execution command (see commands below)

Query commands:

The system status can also be obtained using the following commands:

DINFO, STATUS, COM and GSM

Control commands:

You can control the entire system or just individual sections using the following commands:

SET, UNSET, or SET_x_x_x, UNSET_x_x_x, where x are section numbers separated by a space

Control commands for controlling PG outputs are preset from factory
in the form of ON PG output x (x = 1 ÷ 128)

NOTICE: If the control commands (preset or custom for PG control) contain diacritical marks (e.g. ěščřžýáíé), the "Enable diacritics" parameter must be activated in the "Communication" tab under the "GSM settings" button for reliable control. Furthermore, it is necessary to distinguish between the capital and small letters for these characters with diacritical marks; for standard characters, case is not distinguished.

Command table :

Control command	Authorisation	Response (example)	Note
DINFO (basic information about installation)	Service, Administrator	JABLOTRON: TYPE: JA-103K, SN: 14004026532523, SW: LJ60416, HW: LJ16107, RK: C5U6G-215CP-D2A6, GSM: 90%, GPRS: OK, LAN: off Time 17:01 22.7.	Installation name according to the Scope tab Type of control panel Serial number Firmware version Hardware version GSM communicator registration code GSM signal quality, GPRS data availability LAN connection status (OK or off) Time and date of SMS delivery to GSM network
STATUS (section status)	Service, Administrator, User. (if the user only has access to certain sections, the status will only be returned from the sections to which they have access)	JABLOTRON: Status: Section 1: Set; Section 2: Set; Section 3: Unset; Section 4: Set, Fault; Section 5: Set, Section 6: Set; Section 7: Unset, Section 8: Unset; GSM: 90%; Time 17:01 22.7.	Installation name according to the Scope 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 SMS delivery to GSM network
COM (communication info)	Service	JABLOTRON: GSM: 90%, GPRS: 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 according to the Range tab GSM signal quality, GPRS data availability Cell and operator number to which the GSM connection is connected LAN connection status and MAC address Status of transmission activation for individual possible ARCs Time and date of SMS delivery to the GSM network

Control command	Authorisation	Response (example)	Note
GSM (GSM restart)	Service, Administrator, User	JABLOTRON: SMS processed OK: GSM; Time 17:01 22.7.	Installation name according to the Initial setup tab SMS delivery confirmation (before restart) Time and date of SMS delivery to GSM network
SET (control of the entire system)	(according to the code used)	JABLOTRON: Status: Section 1: Set; Section 2: Set; Section 3: Set; Section 4: Set, Fault; Section 5: Set, Section 6: Set; Section 7: Bypasses during setting, Section 8: Bypassed during setting; GSM: 90%; Time 17:01 22.7.	Installation name according to the Scope 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 SMS delivery to the GSM network

Table 42 – SMS command table

5.7 Control of F-Link or JA-100-Link software

The F-Link and JA-100-Link software are primarily intended for local and remote programming of the entire system or user editing, but they also allow you to monitor the status of individual sections and control them. To control sections and programmable outputs, you can use virtual keypad segments according to the settings of the physical keypads used in the system or you can control sections from the Status column in the Sections tab or from the bottom status bar. System control is recorded in the event history according to the authorisation when the user logs into the SW.

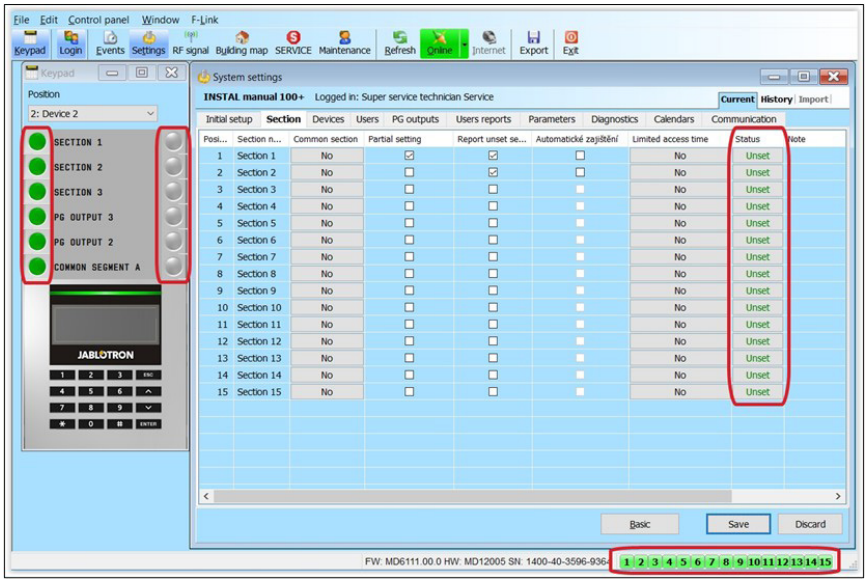


Figure 84 – F–Link or JA–100–Link (F–Link) software control

5.8 Duress access control

This function allows the user, in the event of being threatened by another person, to control (set or unset) the system using a different code than during normal control, thereby alerting others to the situation by triggering a silent panic alarm without any visual or audible signalling. Duress access control is performed by entering your user code with the number "1" added to the last digit of the code. The function is supported for codes with and without a prefix.

*EXAMPLE: user code with prefix = 4*4444, for duress access control the code is =* ***4*4445*** *user code without prefix = 4444, for duress access control the code is =* ***4445.***

NOTE: If the user code ends with the number 9, then for forced control, use 0 for the last digit of the code.

5.9 Reporting events to users

NOTE: The "User reports" tab is only displayed in the F-Link software when using a full-featured communicator (e.g. when using the JA-194Y communicator, "User reports" can be edited and the tab is visible in the F-Link software; on the other hand, when using the JA-194Y-LITE communicator, the "Reports to users" tab is not displayed at all, as this communicator does not support voice or SMS reports).

All events sent to users are divided into four basic groups. Individual groups can be freely assigned to users. Users who are assigned to a group will receive reports that are assigned to that group. If the division into four groups is not sufficient, two additional so-called custom groups (Custom 1, Custom 2) can be used to move events and assign them to selected users.

Overview table of reported events preset into groups:

Order	Event	Group
1	Set	SMS about setting/unsetting (3)
2	Unset	SMS about setting/unsetting (3)
3	Partially setting	SMS about setting/unsetting (3)
4	AC fault 30 minutes	Alarm SMS (1) / Alarm call (2)
5	AC fault after 30 minutes restored	Alarm SMS (1) / Alarm call (2)
6	Instant alarm	Alarm SMS (1) / Alarm call (2)
7	Instant alarm cancelled	Alarm SMS (1) / Alarm call (2)
8	Delayed alarm	Alarm SMS (1) / Alarm call (2)
9	Delayed alarm cancelled	Alarm SMS (1) / Alarm call (2)
10	Tamper alarm	Alarm SMS (1) / Alarm call (2)
11	Tamper alarm cancelled	Alarm SMS (1) / Alarm call (2)
12	Fire alarm	Alarm SMS (1) / Alarm call (2)
13	Fire alarm cancelled	Alarm SMS (1) / Alarm call (2)
14	Gas leak alarm	Alarm SMS (1) / Alarm call (2)
15	Panic alarm	Alarm SMS (1) / Alarm call (2)
16	Panic alarm cancelled	Alarm SMS (1) / Alarm call (2)
17	Health troubles	SMS alerts (1) / Call alerts (2)
18	Flooding	SMS alerts (1) / Call alerts (2)
19	Code breaking attempt	Alarm SMS (1) / Alarm call (2)
20	Bypassed while being set	Alarm SMS (1) / Alarm call (2)
21	No movement in the section	Alarm SMS (1) / Alarm call (2)

Order	Event	Group
22	Overheating activation	Alarm SMS (1) / Alarm call (2)
23	Overheating deactivation	Alarm SMS (1) / Alarm call (2)
24	Freezing activation	Alarm SMS (1) / Alarm call (2)
25	Freezing deactivation	Alarm SMS (1) / Alarm call (2)
26	System BOOT	Fault SMS (4)
27	Device low battery	Fault SMS (4)
28	Device low battery restored	Faulty SMS (4)
29	Fault (general)	Fault SMS (4)
30	Fault restored	Fault SMS (4)
31	Enter service mode	Fault SMS (4)
32	Leave service mode	Fault SMS (4)
33	Maintenance enter	Fault SMS (4)
34	Maintenance leave	Fault SMS (4)
35	Backup battery LOW	Fault SMS (4)
36	Backup battery restored	Fault SMS (4)
37	ARC communication fault	Fault SMS (4)
38	ARC communication fault restored	Fault SMS (4)
39	RF jamming	Fault SMS (4)
40	RF jamming ended	Fault SMS (4)
41	Low credit ballance	Fault SMS (4)

Table 43 – Event reporting to users

The table shows the preset assignment of events distinguished by the system into groups. When an event occurs , the system generates an SMS in the following format: Installation name, Time, Event, Event source, Section, Time

EXAMPLE of an SMS sent by the control panel:

JABLOTRON *(installation name)*
17:01:10, Delayed alarm *(time of event, event)*
Magnet on door, Ground floor *(detector name, section name)*
17:01:25, Instant alarm *(event time, event)*
Staircase movement, Upper floor *(detector name, section name)*
Time 17:01 22.7. *(time of dispatch)*

5.10 Acoustic signals

Acoustic signals in the system can not only report an alarm condition, but also alert to other conditions or changes in status, see Table 44 . **Keypad/reader acoustic signals:**

Sound	Description of activity
One short beep	Confirmation of key press
One long beep	Activation of a segment, setting a section or switching on PG
Two long beeps	Deactivation of segment, unsetting of section or switching off of PG
Two long beeps repeated	Unsuccessful setting
Three long beeps	Section unset with alarm memory indication

Sound	Description of activity
Continuous beeping	Exit delay
Continuous uninterrupted beeping	Entry delay
	Alarm

Table 44 – Keypad acoustic signals

Acoustic indication of indoor/outdoor sirens:

Sound	Activity description
One short beep	Section set
	PG output switched on
Two short beeps	Section unlset
	PG output switched off
Three short beeps	Section unsetting with an alarm memory indication
	Unsuccessful setting
	Setting with an active devices (only up to FW13 version)
Continuous rapid beeping	PG status indication – fast beeping
Continuous slow beeping	Exit delay
	PG status signal – slow beeping
Continuous uninterrupted whistling	Entry delay
	PG status signal – continuous whistling
Hooting	Alarm in section
Melody (1-4) *	PG status signalling

Table 45 – Acoustic siren signals

**only for sirens that support this function*

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

Sound	Activity description
Continuous rapid beeping	Fire alarm
Continuous wailing	

Table 46 – Acoustic signalling of fire detectors

5.11 System restrictions and blockages

This chapter describes the conditions and states that may affect the ability to set, control or generally operate the JABLOTRON system. Restrictions and blockages are an important part of the system's security logic – they ensure that the alarm is only triggered under safe and correctly evaluated conditions, while also allowing technicians and users to selectively deactivate parts of the system for service purposes or specific operational situations.

5.11.1 Time-limited access of users

The access restriction function is intended for selected users divided into up to four groups. Each group can be assigned different time permissions for entering the assigned sections according to a specified weekly calendar. This allows each user group to unset selected sections in two defined time periods (Interval 1 and

Interval 2) for each day of the week separately. Example of group use: in a company, these could be cleaning crews, workers, supervisors and managers, or in a nursery school, they could be cleaners, cooks, teachers and parents.

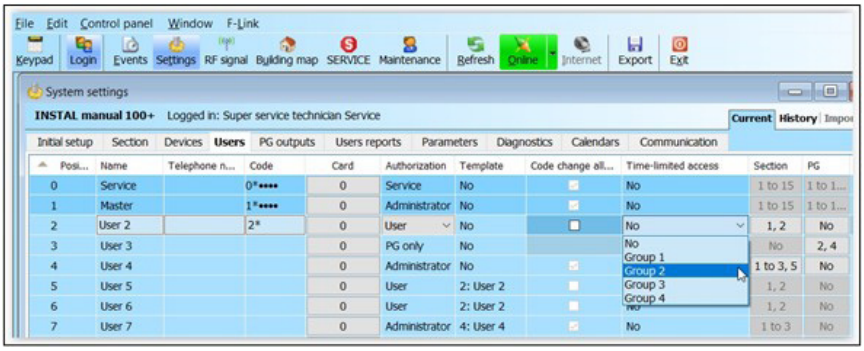


Figure 85 – Time restrictions on user access (F–Link)

Each system user whose access is to be restricted according to the preset calendars must have the option "Group 1" to "Group 4" in their "Time-limited access" settings, which represents individual user groups.

Access restrictions can only be applied to system users with "User" authorisation. If a user with restrictions enabled attempts to unset their section during a blocked time, the system will not allow it, and if the user is already in the set section, a standard intrusion alarm will be triggered after the entry delay expires. The user will have the permission to cancel it, but will not be able to unset during the blocked time.

The following figures show examples of settings for granting access to selected users to "Group 1", in which access to "Section 1" is restricted. On Monday and Tuesday, access is allowed from 5:00 a.m. to 8:59 p.m. On Wednesday to Friday, access is permitted from 5:00 a.m. to 11:59 a.m. and then from 2:00 p.m. to 8:00 p.m. On Saturday and Sunday, access is not permitted at all.

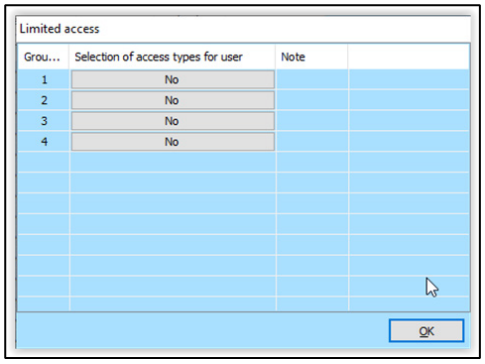


Figure 86 – Restricted access (F–Link)



Figure 87 – Access to sections (F–Link)

To define access restrictions, there is a button with the same name in the Users tab in F-Link, which allows you to access the access group settings for each section separately.

5.11.2 Reasons preventing system security

When setting each section of the system, the control panel can check the active or fault states of individual devices or the entire system according to the **Way of setting** option (on the Parameters tab). For some states, the system only alerts you (**surmountable obstacles**), and for some states, it even prevents setting (**insurmountable obstacles**).

Surmountable obstacles include any fault in the system (signalled by the yellow light on the keypad indicator button), loss of connection with a wireless detector or active status detector (typically a magnetic detector) programmed in a delayed loop (which includes entrance door or garage door detectors), as well as a low battery in the system or a main power failure.

A cause that may prevent the system from setting the premises is, for example, an active status detector (typically a magnetic detector) set to an instant zone, which includes detectors for opening windows, balcony or rear entrance doors, but it can also be serious system faults such as a fault of the control panel's backup power supply or a malfunction of the communication direction with transmission to the ARC. The causes preventing setting may vary depending on the preset system profile. An exception to this rule of blocking when setting a section that does not check any active detectors or system faults is automatic setting by the calendar using the "Set always" option. With this option, the calendar can set the selected section whenever there is a request for setting defined in it (available only in the default profile).

Pulse detectors (e.g. motion, glass breakage, tilt, shock detectors, etc.) cannot prevent setting when activated.

The system informs about setting with active devices or faults by sending an SMS (to a group of users with set SMS alarm reports) with details of the situation.

Table of setting options:

Security method options	From the system keypad	Voice menu / SMS / calendar	MyJABLOTRON application	F-Link JA-100-Link
Set always	Always sets regardless of the status of faults or active elements.	Always sets regardless of the status of faults or active elements.	Always sets regardless the status of faults or active elements.	It will always set regardless of the status of faults or active elements.
Set with a warning	When attempting to set with a fault or active element, it will flash for 8 seconds. After this time, it will automatically set. It can be set by repeatedly pressing the segment or the Enter key	It will always set regardless of the status of faults or active elements.	It sets according to the "Ways of setting" setting (with/without check) in the Service settings tab.	Always sets regardless of the status of faults or active elements.
Set after confirmation	When attempting to set with a fault or active element, it will flash for 8 seconds to alert you. Setting is ONLY possible by repeatedly pressing the segment or the Enter key	Always sets regardless of the status of faults or active elements.	Sets according to the "Ways of setting" setting (with/without check) in the Service Settings tab.	Always sets regardless of the status of faults or active elements.
Do not set with an active element	When attempting to set with a fault or active element, it flashes for 8 seconds. Repeatedly pressing the segment or the Enter key will set ONLY if there is no active detector with an INSTANT reaction.	It will not set when there is an active element with an INSTANT reaction. Calendar when preset to "Set always" Sets regardless the status of faults or active elements	Does not set when the active element has an INSTANT reaction.	Always sets regardless of the status of faults or active elements.

Table 47 – Ways of setting

5.11.3 Unsuccessful setting

This is a security function whereby the control panel evaluates during each exit delay whether the system can be set and the security of the building is not compromised by the following cases. If this function is enabled, unsuccessful setting may occur:

1. activation of an instant detector at any time during the exit delay (someone has entered an already set part of the building)
2. permanent activation of the delayed detector even after the exit delay has been timed (the user did not close the main door, garage, gate, etc. when leaving) did not close the main door, garage, gate, etc. behind them)

If setting cannot take place, the system will trigger an "Arming Failed" event, which is indicated on the keypads by rapid flashing of the yellow indicator button, an acoustic signal beeping, an acoustic signal from the outdoor siren, and is also reported according to the "SMS about unsuccessful setting" parameter setting (in F-Link on the Communication tab) to the relevant user who attempted to arm the system or to the system administrator.

To cancel the unsuccessful setting indication, press "Cancel warning indication" in the LCD keypad menu or, in the "Default" system profile, rearm the section.

5.11.4 Non-alarm system functions

The alarm system allows authorised users to control not only the guarding status of sections, but also to control (switch on, switch off) programmable outputs, which can switch devices (signallers, traffic lights, status of sections or access permission indicators) or appliances related to the alarm system using relay or semiconductor modules (lighting when movement is detected, air conditioning when entering a room, controlling or blocking heating when a window is open or a section is set) or completely independent devices, known as home automation (e.g. opening electric gates, garage doors, heating, watering).

PG functions	Description	Example of use
On/Off	Bistable output state that can be changed by any command and any device	Manual switching on of appliances from a segment, SMS command or device from the system with the option of manual switch-off without restriction. Typically control of heating, air conditioning, lighting
impulse	Monostable output state with precisely defined time	Pulse switching of most other control circuits, such as commands for controlling barriers, electric gates, garage doors, electric blinds and shutters, irrigation, opening release locks, etc.
Copy	Output state with logical sum. The output will be switched on if at least one device is active, but it will only switch off when all control devices are inactive.	Suitable for signalling uniform or collective states (e.g. open windows, doors, garage doors, etc.) on the keypad segment. In a similar way, PG outputs can also be used to signal the status of sections, alarms, alarm memories, faults and other events where the start and end are clearly defined.
Extended copy	Monostable output state with defined switch-on time with the possibility of further extension	A typical output setting is for controlling lighting during activity e.g. a motion detector, which triggers and thus extends the lighting time.
Delayed copy	Time-delayed output status	The most common use of this output is to signal garage doors that have been open for too long, e.g. because someone forgot to close them. The signal can be visual on a segment of the keypad, but also acoustic from the keypad or an indoor or outdoor siren.
Change status	Bistable output state	Output designed for cyclic control (switching on and off), e.g. from a pulsing device, authorisation or simply by calling from an authorised telephone number.

Table 48 – Non–alarm system functions

The system also offers the user temperature measurement functions using temperature detectors or thermostats, which are displayed on LCD keypads and in the MyJABLOTRON application, as well as measurement, counting and monitoring of consumption, e.g. of electricity, gas or water flow or other media. The JA-150EM-DIN pulse counter is designed for this purpose in combination with a measuring device (electricity meter, gas meter, water meter, etc.). For more information, see the Case studies in MyCOMPANY in the MySTORAGE section.

5.11.5 Bypassing and blocking options

5.11.5.1 Disabling a device

Before setting the system, a situation may arise in which it is necessary to deliberately exclude a device from monitoring (e.g. a garage due to construction work or leaving a dog in a room that is otherwise normally monitored). This option is called Bypass and is available in the LCD keypad menu or using the JA-100-Link software and can be performed at two levels depending on user authorisation:

- **Input blocking (shortcut BLK)** - this function is used to switch off the detector input (blocks activation). The system ignores device activations = it does not trigger alarms, reports or PG activation. However, tampering, faults and low battery reports are still monitored. This is indicated by a yellow dot in JA-100-Link. The Administrator and Service Technician have permission to block.
- **Disabled (shortcut Disabled)** - this function is used to shut down the entire detector. The system ignores all device functions = it does not report any alarms, faults, reports, PG activations or sabotages. Indicated by a red dot in JA-100-Link. Only the Service Technician has permission to shut down the devices.

Not only devices can be **disabled**, but also users outside positions 0 (service) and 1 (administrator), PG output or calendar events. The disabling remains in effect until it is cancelled using the same procedure.

WARNING: It is not possible to switch off or block a control panel or device that has a Panic reaction!

5.11.5.2 Blocking when setting

During section setting, a situation may arise where some devices remain active (e.g. an open window or balcony, flooded detector in the basement, etc.). The system can alert you to the situation that has arisen during section setting, and after confirmation, there are two possible system behaviours depending on the programming parameter settings

Blocking when setting:

- **Blocking enabled** – Enabling this option will block active detectors during section setting, i.e. they cannot trigger an alarm for the entire duration of section arming.
- **Blocking off** – When this option is turned off, active detectors will only be bypassed during section setting. Once the detector has restored, it will start monitoring again and will be able to trigger an alarm. However, this creates the risk of a false alarm, e.g. a window opened by a draught.

6 Maintenance and service

This chapter describes activities related to the long-term reliability, inspection and restoration of the JABLOTRON system's operability. Maintenance and service are an integral part of the proper operation of the security system and include both regular tasks performed by the administrator or end user and professional interventions by a service technician.

6.1 Maintenance

The alarm system as a whole requires not only regular testing of the correct functioning of all components used, but also cleaning and inspection both from the outside (dust and dirt, which is cleaned by the system user) and internally (cobwebs, insects, battery condition, etc., which are checked by a service technician).

Some components in the system are able to test their own parts using a self-test and report any faults to the control panel, which then informs the user of the fault according to the settings. However, the vast majority of component maintenance steps must be performed by a service technician during the recommended annual inspection of the entire system.

The control panel regularly tests the backup battery with a load test. For wireless devices (detectors, keypads, sirens, remote controls), the batteries are automatically tested each time a regular test is transmitted. The system reports a low battery in each device from the moment the report is generated until the battery is replaced with a new one on the LCD keypad or via a configure d SMS report. Battery replacement is performed by a service technician in Service mode mode or by the administrator in Maintenance mode. After removing the discharged battery from the device, it is necessary to wait for the internal capacitors to discharge completely (at least 20 seconds) before inserting a new battery.

Overview of recommended maintenance/function checks:

Component	Description	Who performs	Period
Fire detectors	Function test, report to the ARC before testing!	System administrator	Once a month
	Cleaning of dust and dirt	System administrator	Once a year
	Battery condition check (both wireless and Bus)	Service technician	Once a year
Panic buttons	Function test, report to the ARC before testing!	System administrator	Once a month
	Check battery status, voltage, physical condition	Service technician	Once a year
Detectors	Cleaning of dust and dirt	System administrator	Once a year
	Function test, range test for wireless detectors. For photo detectors, image test.	Service technician	Once a year
	Check battery condition, physical condition of batteries, voltage of each battery, etc.	Service technician	Once a year
Keypad	Cleaning of dust and dirt	System administrator	Once a year
	Testing the functionality of buttons, segments and chip/card readers, including wireless range.	Service technician	Once a year
	Check the condition of the batteries, their physical condition, voltage of each battery, etc.	Service technician	Once a year
Sirens	Cleaning of dirt, insects, checking for water ingress into electronic parts, etc.	Service technician	Once a year
	Function test, including range for wireless devices.	Service technician	Once a year
	Check the condition of batteries or accumulators, their physical condition, voltage of each battery, etc.	Service technician	Once a year
Remote controls	Function test, range, battery indicator check. Cleaning or replacement of plastic parts.	System administrator or service technician	Once a year

Component	Description	Who performs	Period
System alarm status	Test communication with the ARC, voice message call, SMS delivery	System administrator or service technician	Once a year
Battery in the control panel	Testing during power failure, voltage measurement after 5 minutes of operation without power supply	Service technician	Once a year
Programmable outputs	Function test, wireless module range	Service technician	Once a year

Table 49 – System maintenance

All tasks are recommended by the manufacturer, but do not take precedence over local regulations or ordinances.

6.2 Service

This chapter focuses on service interventions that require a higher level of authorisation and can significantly affect the configuration or operation of the system. Service activities are performed exclusively by an authorised technician who has access to the full system settings and is trained in diagnostics and troubleshooting.

This chapter describes procedures that enable the restoration of system operability or its update — from restoring the control panel to its factory settings to safely updating the firmware of all devices. It also includes guidelines for checking after service intervention, recommendations for verifying functions and information about service tools available in the F-Link software.

6.2.1 Resetting the control panel

You can reset the control panel to factory settings using the following procedure only if Reset enabled is selected in the Parameters tab in the F Link software. If reset is not enabled and you do not know the service code, it will not be possible to perform a reset and the control panel mainboard must be sent to the manufacturer. The reset is performed as follows:

NOTICE for JA-103K, JA-107K: Resetting the control panel to factory settings does not delete data stored on the microSD card. Before performing the reset, the service technician connects the control panel to a PC using a USB cable, logs into the F-Link software with a “Service” authorization code, manually deletes the contents of the PHOTO folder (images from camera devices) on the displayed FLEXI_LOG drive, and only then performs the factory reset according to Section 6.2.1, “Resetting the Control Panel.

1. Put the control panel into service mode (not a requirement)
2. Open the control panelcover: the tamper contact must be active to perform the reset. If condition ad/1 is not met, an alarm will be triggered.
3. Disconnect the USB cable from the control panel.
4. Turn off the mains power supply (easiest by removing the fuse from the power supply) and disconnect the battery.
5. Connect the pins on the control panel marked RESET (using the supplied jumper).
6. First connect the battery and then the mains power supply to the control panel and wait. The green, yellow and red LEDs on the jumper will light up (if only the red LED remains lit, it is not enabled in the Parameters / Reset settings).
7. Wait approx. 15 seconds and then disconnect the jumper.
8. All LEDs will then flash to confirm that the control panel reset is complete. The control panel and Bus devices will then perform a power restart, causing all segments on the keypads will also flash.
9. The control panel has now been reset to its factory settings, including the language selection. However, resetting the control panel does not delete the event history and PHOTO folder stored on the SD memory card, see NOTICE above. If the reset was not performed correctly, the control panel will remain in its original settings without any changes.

6.2.2 Firmware updates

The control panels and a number of other JABLOTRON system devices allow firmware (FW) updates. Performing a FW update usually extends the useful parameters of the device or changes or corrects unsatisfactory behaviour.

6.2.2.1 General rules

1. Changes can only be made using a computer with F-Link software installed, either locally via a USB cable or remotely, where it is only possible to make limited FW changes to devices.
2. The FW can be changed by a user with Service authorisation.
3. Please check that you are using the latest version of F-Link. The latest version can be downloaded from www.myjablotron.com in MyCOMPANY / MySTORAGE / Software. F-Link is only available to authorised technicians after logging in. If it is already installed on your computer, F-Link performs updates of the software itself and the FW package for updating devices, fully automatically.
4. Connect your computer and the control panel with a USB cable. The cable is included with the control panel
5. Start the F-Link software with the control panel connected. **F-Link**
6. Switch the control panel to Service mode.
7. Open the Control panel / Firmware Update menu.

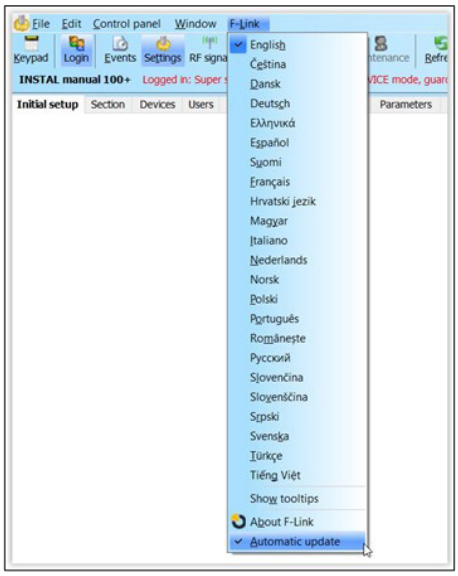


Figure 88 – Automatic FW update (F–Link)

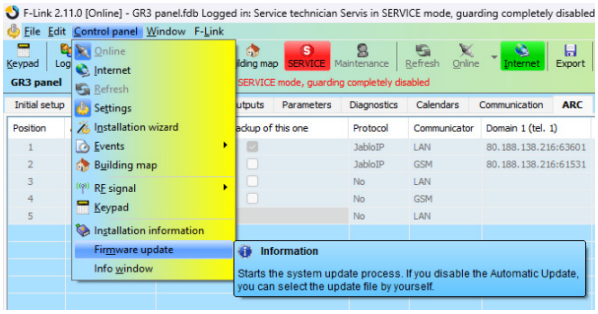


Figure 89 – FW Update 1 (F–Link)

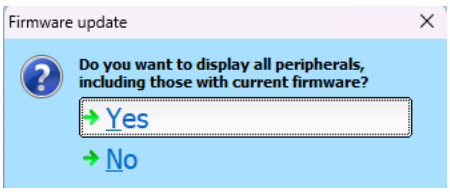


Figure 90 – FW Update 2 (F–Link)

If Automatic Update is enabled in the F-Link menu (enabled by default), a list of devices that can be updated will be displayed. The FW file is part of F-Link and is automatically stored in the F-Link x.x.x / Firmware directory. Its validity is only guaranteed at the time of downloading F-Link.

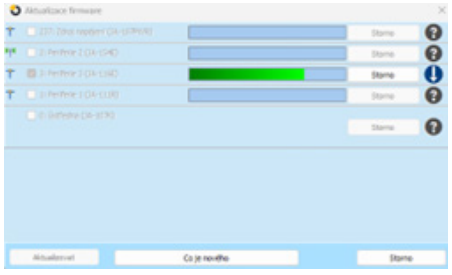


Figure 91 – Devices during update

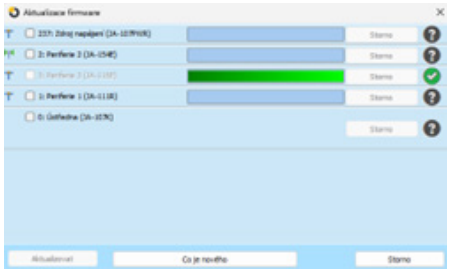


Figure 92 – Devices with completed update

6.2.2.2 Updating the FW of the control panel and devices connected to the Bus

1. The FW Update selection window only displays Bus devices and the control panel that can be updated. F-Link marks those in the list of devices that need to be updated (they have older FW than in the current package).
2. F-Link will also notify you of wireless system components for which an update is possible. Their update is described at Devices FW update of wireless devices .
3. Detailed information about the current and new versions of individual devices is displayed in a tooltip when you hover your mouse over each of the offered devices.
4. Items selected for update are marked with a cross in the selection boxes. We recommend that you respect the selection. Some items may be mandatory and therefore unavailable (greyed out) for cancellation of the update.
5. When the option to update the control panel is enabled, the option to retain the modified user voice menu is displayed. If you cancel the option to retain, the voice menu will be restored to factory settings.
6. Confirm with OK to start updating the firmware of all selected devices. All changes will be made within a few minutes (depending on the number of devices). Finally, the control panel will restart the system.
7. After the FW change, part of the registration code will change. This change will not affect remote access
(via F-Link) or the control panel's communication with the MyJABLOTRON service.
8. If F-Link detects damaged files on the SD card during the control panel update, it will format the card and, after completing the update, offer the option to re-import the original settings.
9. Although the update does not change the behaviour of the system, perform a check as described Check after FW update Check after FW update .

6.2.2.3 FW update for wireless devices

1. The FW update for wireless devices is performed in the same way as for Bus devices.
If the firmware cannot be updated wirelessly, proceed as follows:
2. Open the updatable wireless device (e.g. JA-152E, JA-153E, JA-154E, JA-160PC, AC-160DIN, etc.) by pressing the latch.
3. If it contains batteries, remove them and disconnect the external power supply.
4. Start F-Link, open the database and connect the USB cable (mini USB or micro USB depending on the device used) to your computer.

NOTE: USB cables are not included with individual devices. We recommend using a direct USB connection to the PC, as connecting via a USB hub may reduce reliability.

5. The FW update of wireless devices must be performed sequentially; it cannot be performed simultaneously on multiple USB cables.
6. For updated wireless devices, open the mode for uploading new firmware. Always follow the instructions in the manual for the relevant device.
7. Then proceed as when upgrading the F-Link SW system: Control panel → Firmware Update
8. In the device menu Table , select USB (usually in the first position).
9. Detailed information about the current and new versions of individual devices is displayed in a tooltip when you hover your mouse over each of the available devices.
10. Press the OK button to upgrade the selected device.
11. After the update is complete, disconnect the USB cable, reinsert the batteries or connect the power supply, and reassemble the module.
12. Perform a check as described at Check after FW update Check after FW update .
13. Continue updating other wireless devices.

6.2.2.4 Check after FW update

1. Check the settings of all changed devices and the control panel in F-Link, Devices / Internal Settings. Depending on the extent of the changes made during the update, the previous settings may be retained or reset to the factory defaults. If a reset has been performed, you can use the Import button in the internal settings of each device to select from the previous settings.
2. If new functions were added during the update, they will have factory settings. Check them and adjust the settings as needed for the installation.
3. Check the settings and test the operation of the updated devices.

6.2.2.5 Info window

It opens from the main menu Control panel / Info window. While generating the Info window, the control panel addresses all connected devices and wireless devices and requests their current information.

The Info window provides a comprehensive overview of the technical data of the system, including the control panel (serial number, registration code, FW and HW versions, Bus voltage and current, initial setup size: devices, sections, PG outputs), all communicators used (GSM: telephone number, signal, CELL ID, LAN, status, MAC, IP) and all Bus and wireless devices (unidirectional and bidirectional): device type, identification of FW/HW versions of individual devices and their status. The info window is available in all system states (set/unset/service).

This data is needed, for example, for communication with JABLOTRON technical support, for which the Save to send button in the lower right corner is used. The file is compressed in ZIP format and contains numerical data about the installation, including part of the event history (100 kB). The file does not contain any sensitive data, such as the control panel settings database, users' telephone numbers or their access codes, or other confidential data. The saved file is several hundred kB in size and can therefore be distributed by normal means, e.g. by e-mail.

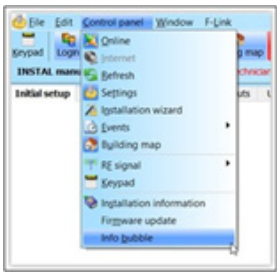


Figure 93 – Info window 1 (F–Link)

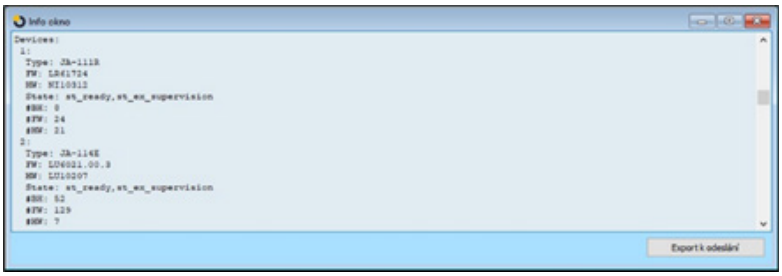


Figure 94 – Info window 2 (F–Link)

7 Legislative information and declaration of conformity

EMC	EN 50130-4, EN 55032, EN IEC 63000
Electrical safety	EN 62368-1

Table 50 – Legislative Information and Declaration of Conformity

JABLOTRON a.s. hereby declares that the JA-103K, JA-103K-7Ah JA-107K and JA-108K products are designed and manufactured in accordance with the harmonised legislation of the European Union: Directive No.: 2014/35/EU, 2014/30/EU, 2011/65/EU, when used as intended. The original declaration of conformity is available at www.jablotron.com in the Downloads section.

Note: Although the products do not contain any harmful materials, do not dispose of them in the rubbish, but take them to an electronic waste collection point. For more detailed information, visit www.jablotron.com in the Downloads section.

8 Overview of related documents

CID/SIA Codes | Jablotron

Product Compatibility

Seznam obrázků:

Figure 1 – Event memory . . . 9
Figure 2 – JA–103K (dimensions) . . . 14
Figure 3 – JA–103K–7Ah, JA–107K and JA–108K (dimensions) . . . 14
Figure 4 – JA–103K (component layout) . . . 14
Figure 5 – JA–103K (PCB detail) . . . 15
Figure 6 – JA–103K–7Ah (component layout) . . . 15
Figure 7 – JA–103K–7Ah (PCB detail) . . . 16
Figure 8 – JA–107K (component layout) . . . 16
Figure 9 – JA–107K (PCB detail) . . . 17
Figure 10 – VOD–JA107K (power cable) . . . 17
Figure 11 – JA–108K (component layout) . . . 18
Figure 12 – JA–108K (PCB detail) . . . 18
Figure 13 – VOD–JA107K (power cable) . . . 18
Figure 14 – Control panel with Bus splitter . . . 19
Figure 15 – Bus . . . 21
Fugure16 – Linear Bus . . . 22
Figure 17 – Star Bus structure . . . 22
Figure 18 – Combined Bus structure. . . . 22
Figure 19 – Control panel operating modes . . . 26
Figure 20 – Division of sections into two levels . . . 33
Figure 21 – Division of sections into three levels . . . 33
Figure 22 – Entrance system design . . . 43
Figure 23 – Section/PG control and optical indication . . . 46
Figure 25 – JA–110Z . . . 49
Figure 26 – JA–110Z–B . . . 49
Figure 27 – JA–110Z –C . . . 49
Figure 28 – Calculation of voltage drop (example) . . . 50
Figure 30 – Installing wireless devices . . . 52
Figure 32 – JA–107K Initial setup with guide (F–Link) . . . 57
Figure 33 – JA–103K initial setup (F–Link) . . . 57
Figure 34 – Sections (F–Link) . . . 57
Figure 35 – Devices (F–Link) . . . 58

Figure 36 – Keypad segments (F–Link) . . . 61
Figure 37 – Keypad settings (F–Link) . . . 63
Figure 38 – Common segment (F–Link) . . . 65
Figure 39 – Internal siren settings (F–Link) . . . 66
Figure 40 – Sirens – PG indication (F–Link) . . . 66
Figure 41 – Users (F–Link) . . . 68
Figure 42 – PG outputs (F–Link) . . . 69
Figure 43 – Blocking of PG outputs . . . 70
Figure 44 – PG Reports (F–Link) . . . 70
Figure 45 – Map of PG activation links . . . 71
Figure 46 – Reports to Users 1 . . . 72
Figure 47 – Reports to users 2 . . . 72
Figure 48 – Special reports to users (F–Link) . . . 73
Figure 49 – Table of events and preset groups (F–Link) . . . 74
Figure 50 – Parameters (F–Link) . . . 74
Figure 51 – Parameters – Security grade (F–Link) . . . 75
Figure 52 – Parameters – Date and time (F–Link) . . . 75
Figure 53 – Diagnostics (F–Link) . . . 80
Figure 54 – Calendar (F–Link) . . . 81
Figure 55 – Communication (F–Link) . . . 82
Figure 56 – GSM settings (F–Link) . . . 83
Figure 57 – LAN settings (F–Link) . . . 86
Figure 58 – Camera settings (F–Link) . . . 86
Figure 59 – ARC and transmissions (F–Link) . . . 87
Figure 60 – Reported events . . . 88
Figure 61 – Settings – top bar (F–Link) . . . 88
Figure 62 – Virtual keyboard 1 (F–Link) . . . 89
Figure 63 – Virtual keypad 2 (F–Link) . . . 89
Figure 64 – Virtual Keyboard 3 (F–Link) . . . 89
Figure 65 – Settings – bottom bar (F–Link) . . . 89
Figure 66 – Events (F–Link) . . . 89
Figure 67 – Settings – top toolbar (F–Link) . . . 90
Figure 68 – Settings – bottom toolbar (F–Link) . . . 90
Figure 69 – RF signal (F–Link) . . . 92
Figure 70 – Building map (F–Link) . . . 92
Figure 71 – Internet communication settings (F–Link) . . . 93
Figure 72 – Establishing a GPRS/LAN connection (F–Link) . . . 93
Figure 73 – Installation wizzard (F–Link) . . . 94
Figure 74 – Installation Information 1 (F–Link) . . . 94
Figure 75 – Installation information 2 (F–Link) . . . 94
Figure 76 – FW Update (F–Link) . . . 95
Figure 77 – Label printing (F–Link) . . . 95
Figure 78 – Events from memory (F–Link) . . . 96
Figure 79 – History (F–Link) . . . 96
Figure 80 – Section/PG control and optical indication . . . 101
Figure 81 – Internal settings of segment keypads . . . 103
Figure 82 – Internal settings of touch keyboards . . . 103
Figure 83 – Voice menu diagram . . . 107

Figure 84 – F–Link or JA–100–Link (F–Link) software control . . . 110
Figure 85 – Time restrictions on user access (F–Link) . . . 114
Figure 86 – Restricted access (F–Link) . . . 114
Figure 87 – Access to sections (F–Link) . . . 114
Figure 88 – Automatic FW update (F–Link) . . . 120
Figure 89 – FW Update 1 (F–Link) . . . 120
Figure 90 – FW Update 2 (F–Link) . . . 120
Figure 91 – Devices during update . . . 120
Figure 92 – Devices with completed update . . . 120
Figure 93 – Info window 1 (F–Link) . . . 122
Figure 94 – Info window 2 (F–Link) . . . 122

Seznam tabulek:

Table 1 – Technical Specifications table . . . 13
Table 2 – Current consumption (backup) table . . . 13
Table 3 – GSM communicators . . . 19
Table 4 – LED indicators on the control panel . . . 21
Table 5 – Bus terminal description . . . 21
Table 6 – Description of system presets by profile . . . 25
Table 7 – Causes preventing security . . . 26
Table 8 – control panel operating modes . . . 27
Table 9 – User authorisations . . . 29
Table 10 – Access codes . . . 30
Table 11 – Duress access control (codes) . . . 30
Table 12 – Access code combinations . . . 31
Table 13 – Factory default codes . . . 31
Table 14 – RFID cards and chips . . . 32
Table 15 – System states . . . 34
Table 16 – Overview of all types of reactions . . . 35
Table 17 – Activation of EW and IW siren outputs . . . 36
Table 18 – Alarm Types . . . 37
Table 19 – Fault conditions . . . 40
Table 20 – Detector placement . . . 44
Table 21 – Standby consumption (example) . . . 48
Table 22 – CC–xx Bus cables . . . 49
Table 23 – Voltage drops and consumptions . . . 50
Table 24 – Segment Functions . . . 62
Table 25 – Acoustic signalling of sections . . . 63
Table 26 – Keypad Functions . . . 64
Table 27 – Keypad display . . . 65
Table 28 Keypad LCD display light intensity . . . 65
Table 29 – PG output functions . . . 69
Table 30 – Internal states for controlling PG outputs . . . 72
Table 31 – Description of adjustable parameters . . . 80
Table 32 – APN network . . . 84
Table 33 – SIM sequence . . . 85

Table 34 – Possible system configuration problems 91
Table 35 – Local system control. 97
Table 36 – Remote system control 97
Table 37 – Overview of an optical indication 104
Table 38 – Overview of an optical segment indication 104
Table 39 – Overview of remote control optical indication 105
Table 40 – Calendar options 106
Table 41 – Calendar events 106
Table 42 – SMS command table 110
Table 43 – Event reporting to users 112
Table 44 – Keypad acoustic signals 113
Table 45 – Acoustic siren signals 113
Table 46 – Acoustic signalling of fire detectors 113
Table 47 – Ways of setting 115
Table 48 – Non–alarm system functions 116
Table 49 – System maintenance 119
Table 50 – Legislative Information and Declaration of Conformity 123