

# JA-100K Security System Control Panel

A control panel is an elementary part of the security system JABLOTRON 100. As the smallest control panel from the JA-10xK series it is designed to protect small and medium premises. The security system offers a lot of configuration options including the system profiles for easy complying with requirements of security grade 2.

The control panel has BUS and/or wireless device (when the control panel is equipped with a radio module) compatibility. It is recommended that only JABLOTRON 100 devices are used with the system. Proper functionality cannot be guaranteed when using third party devices.

**Caution:** The JABLOTRON 100 security system can only be installed by a trained technician with a valid certificate issued by an authorized distributor.

**The manual is intended for trained technicians and is valid for control panel firmware LJ60421 and F-Link configuration software 1.6.0 or higher.**

## Contents

1	Basic description and definitions.....	3
1.1	Basic system configuration requirements .....	6
1.2	Access codes and their default settings.....	7
1.2.1	Change of access codes .....	7
1.2.2	Security access codes and RFID devices .....	7
1.3	Regular system check (maintenance).....	8
2	System size .....	9
2.1	Configuration and splitting .....	9
2.2	System control .....	10
3	The JA-100K control panel utility parameters .....	11
3.1	Description of JA-100K control panel.....	11
3.2	Indication LEDs on the control panel board.....	13
3.3	Additional Connectors on the control panel PCB.....	13
3.4	Connection terminals on the control panel PCB .....	13
4	Before system installation.....	14
5	Installation of BUS devices .....	14
5.1	JA-100 BUS .....	15
5.2	BUS cables .....	15
5.3	BUS length and numbers of connected devices.....	15
5.4	Example of calculation of BUS consumption to back-up the system .....	16
5.5	Power supply requirements .....	16
6	Use of wireless devices .....	17
6.1	Installation of a JA-111R radio module .....	17
6.2	Installation of wireless devices – enrollment mode.....	17
7	Switching the system ON .....	18
8	System configuration.....	18
8.1	The system profiles.....	18
8.2	Control panel operation modes.....	21
8.3	Authorisation of users .....	22
8.4	System optional parameters (F-Link – Parameters tab) .....	23
8.4.1	Enrolling and erasing devices.....	23
8.4.2	List of applicable reactions .....	25
8.4.3	Limitation of false alarms.....	26
8.5	Types of alarms .....	27
8.5.1	Intrusion alarm.....	27
8.5.2	Tamper alarm .....	27
8.5.3	Fire alarm .....	28
8.5.4	Panic alarm.....	28
8.5.5	24hr alarm .....	28
8.6	System faults .....	28
8.7	Fault caused by loss of a device.....	29
9	System control options .....	30
9.1	Way of authorization .....	30
9.2	System control by keypad.....	31
9.3	System control by remote controller .....	33
9.4	System control by a calendar.....	33
9.5	System control via supplementary communicator voice menu (GSM / PSTN).....	34

9.6	SMS commands.....	36
9.7	Controlling the system via F-Link.....	38
9.8	Control from the MyJABLOTRON web app.....	38
9.9	Control via the MyJABLOTRON mobile app.....	39
9.10	Control by Duress access control.....	39
9.11	Obstacles preventing setting the system.....	39
9.12	Unsuccessful setting.....	40
9.13	Overview table of Groups of Events reported to users.....	40
9.14	System acoustic indication.....	42
9.15	Disabling and blocking options.....	42
9.15.1	Disabling.....	42
9.16	Non-alarm functions – Functions of PG outputs.....	43
10	Setting the system through F-Link SW.....	43
10.1	Starting the F-Link software and setting the system size.....	43
10.2	Sections tab.....	44
10.3	Devices tab.....	44
10.3.1	Keypad configuration.....	45
	Settings tab:.....	47
10.3.2	Internal siren settings:.....	49
10.4	Users tab.....	50
10.5	PG outputs tab.....	51
10.5.1	Activation Map of a PG outputs.....	52
10.6	Reports to users tab.....	53
10.7	Parameters tab.....	55
10.8	Calendars tab.....	58
10.9	Communication tab.....	59
10.9.1	JA-190Y Settings.....	60
10.9.2	GSM restart.....	61
10.9.3	LAN Settings.....	61
10.9.4	PSTN Settings.....	62
10.10	ARC tab.....	62
10.10.1	Requirements for the setup of transmission paths to an ARC.....	64
10.10.2	Transmission paths.....	64
10.10.3	JABLOTRON 100 CID and SIA codes.....	65
10.11	Diagnostics tab.....	67
11	Other F-Link options.....	68
11.1	System control by F-Link.....	68
11.2	Event history:.....	68
11.3	System settings.....	69
11.4	RF Signal.....	70
11.5	Service.....	71
11.6	Refresh.....	71
11.7	Online.....	71
11.8	Internet.....	71
11.9	Installation Information.....	71
11.10	Firmware update.....	72
11.11	History of Settings.....	72
12	Reset of the control panel.....	73
13	Firmware updates.....	73
13.1	General firmware update rules (FW).....	73
13.2	FW updates for the control panel and devices connected to the BUS.....	73
13.3	FW updates for wireless devices.....	74
13.4	Check after a FW check.....	74
13.5	Info Window.....	75
14	Supplementary information.....	76
14.1	Overview table of current consumption of BUS devices.....	76
14.2	Control panels dimensions.....	76
15	System takeover by the user.....	77
16	Technical specifications.....	78

# 1 Basic description and definitions

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

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

**Control keypad** – a module meant for user authorisation, for system control and for indication of its status. It consists of an RFID tag/card reader, a keypad to enter digit access codes, four functional buttons and an LCD display. The keypad is supplied as a BUS and wireless version.

**System indicator** – a square LED in the keypad's left upper corner, indication is performed by 3 colours: green = everything OK, control panel with no faults; red = alarm and alarm memory; yellow = system fault, etc.

**Section indicator** – LEDs marked with letters representing sections A, B, C, D and the colour (red, yellow and green) indicates the status of all system sections.

**Functional button** – A universal programmable/control/indication button on the indoor keypad and. There are 4 functional buttons available marked A, B, C, D. Every individual functional button has intuitive indication provided by backlight with different colour and also it offers control of the system (selected sections).

**Alarm types** – the system is able to react to intrusion, panic, tamper, fire, gas leak and water flooding. The use of suitable detectors makes it possible to report other dangers as well (somebody moving in the garden, handling of a guarded object etc.). Means to reducing the occurrence of false alarms are available. Detectors located in a difficult environment from the structural or operational point of view can be set in such a way that their activation must be confirmed by another detector.

**Visual verification of an alarm** – Photo verification devices (camera detectors, photo verification cameras) are able to automatically take and send photos of what is happening in the monitored area.

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

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

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

**Event reporting** – reporting of all events to an alarm receiving centre (ARC) may ensure the timely intervention of professionals. Information can also be directly sent to users by a built-in LAN communicator or by a GSM or PSTN communicator by means of SMS messages (valid for GSM only) or voice calls. Direct reports are especially suitable for monitoring power supply failures, the departures and arrivals of children or employees etc.

**Remote control** – using supplementary diallers the authorized users may call the system and use a voice menu to control or check the setting status. Statuses of individual sections can be remotely controlled by means of defined SMS commands (GSM only). SMS commands can also be used to switch programmable (PG) outputs on and off. They can also be activated by simply ringing (without establishing a call) from authorized phone numbers. There is F-link SW meant for service technicians to perform remote control. The system can also be remotely controlled via the MyJABLOTRON or MyCOMPANY web or smart applications.

**Users' access rights** – defines the user authorization access level. You can modify user access rights to which part of the protected premises they can control and also control by means of programmable (PG) outputs. The users prove their identity by applying a contactless tag or entering a code using a keypad.

**Administrator** – (Master) a required number of administrators can be defined in the system, they can assign access rights to standard users. Different sections in the building may have different administrators. In the default setting there is one main administrator of the system (position 1), who is always authorized to set access rights for all users; default code 1234 or 123456, according to the Code length option (Initial setup tab) or pre-set system profile.

**Service technician** – A special service code (default setting 1010 or 101010 according to the selected profile). With this code the technician is authorized to adjust all features of the system. There may be more than one authorized service technician (if required). The access of a service technician may be conditional on the administrator's approval. A special case of service authorization is a technician of the Alarm Receiving Centre (also referred to as 'ARC' in the texts. This technician can use his code (F-Link menu: Settings / Users / User authorization = ARC) to lock access to settings of the parameters of communication with the Alarm Receiving Centre.

**F-Link (J-Link)** – To program the system, a computer with a 'Windows' operating system (WIN XP SP3 or higher) is necessary. The control panel can be connected to the computer locally using a USB cable or remotely from a computer connected to the Internet. All features are set using the computer and the F-Link software. This software is exclusively designed for trained technicians. Access to it cannot be granted to an administrator or end user of the system. For this purpose a simplified version of this software (J-Link) is designed, which gives system administrators access to some settings (user management, diagnostics, setting of scheduled events, reading the event history).

**Service mode** – is the mode in which complete configuration of the system can be modified. Only a service technician (or an ARC technician) can enter the system into service mode. This can be done by using a keypad with an LCD display, local connection of the control panel and PC (with a USB cable) or remote access via the Internet. In the SERVICE mode the system is completely out of operation (it does not do any monitoring and does not provide any user functions, e.g. control of programmable PG outputs). The service technician may adjust a significant part of the system features during operation (ie. without having to switch the system over to the SERVICE mode).

**Control of appliances** – the system has programmable PG outputs that can be used to switch various devices on and off. It represents the system logic and it controls the required number of output modules (devices assigned to the system). An output can be controlled using the keypad functional button, by activation of detectors, remote controllers, by an event in the system (e.g. setting a section, alarm triggering,...), by a calendar action, using an SMS command, by ringing of an authorized user. Activation of a PG output can also be blocked by a status of a section or detector or by any other PG output. Activation of a PG output can also be, besides optical indication, indicated acoustically (by a siren).

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

**Schedule of automatic events (Calendar)** – using the weekly schedule automatic guarding (setting / partial setting / unsetting) of sections and control of PG (activation / deactivation, blocking / unblocking) programmable outputs can be programmed. The yearly schedule can be used to set deviations from the weekly schedule (e.g. state holidays, personal holidays). The yearly schedule can be set for the current and following year.

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

**Wireless devices** – to ensure communication, the control panel must be equipped with a radio module and the wireless devices (detectors, keypads, sirens etc.) must be enrolled to a position (address) in the system. However, there may also be devices in the system that do not occupy system positions (they are used for reception only and do not report to the control panel), e.g. modules of PG outputs. To cover the area of a larger site up to 3 radio modules can be installed in the system (connected with a BUS cable). The control panel regularly checks the activity of selected wireless devices (the Supervision parameter) and also checks current state of batteries. If communication with a wireless device is lost, the control panel indicates communication fault. Radio modules check RF jamming/interference on the JABLOTRON 100 system communication band. If the band is jammed, the system triggers a Fault.

**Intrusion detectors** – a group of detectors designed to identify the intruder. It includes detectors of motion, opening, glass breaking, tilt or shock detectors. If they have set reactions for releasing a delayed or immediate alarm and its variations (e.g. repeated or confirmed) it determines how the detector is going to react to its activation. Fire, gas, flood or panic reaction detectors do not belong to the group of intrusion detectors.

**GSM communicator** – provides connection to a mobile phone network and the Internet. Thus, the system may transmit data to the alarm receiving centre (ARC) as a main or backup channel. The communicator provides remote access to the control panel with the use of the F-Link software, reporting events to users, remote control of the system (via voice menu and SMS commands).

**LAN communicator** – if included in the control panel, it provides fast remote access by F-Link (J-Link) SW and it can also transmit data to an alarm receiving centre (ARC) service that is equipped with reception technology for the Jablotron IP protocol. In the control panel settings you can select which communication type will be primary and which will be used as a backup.

**PSTN - Telephone communicator** – it can be installed in the control panel as a supplementary module for analogue PSTN phone lines. It is able to transmit data to the alarm receiving centre in the standard phone formats (CID, SIA DC-05 and SIA DC-03). It can also report events to users (by calling) and supports the system remote control using the voice menu. The phone module is usually used as backup for the LAN communication. The module can also communicate to a phone line simulated by radio transmitter.

**Section** – a system can be split into parts 'Sections' which can be set and unset independently. A section may also be a separate apartment in an apartment building, a store in a shopping mall or department in some

company or office building. Section interdependency can be set on the way it reminds you it is protected by your own control panel (access rights, reports, displaying things on the keypad, acoustic indication,...).

**Common section** – is a separate section designed to be a subsection for a selected group of other sections. When the master section is set as a last one, the common section is then set automatically. When a first master section is unset then the common section is unset as well. The purpose is to secure areas such as halls, toilets, kitchens in companies, etc.

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

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

**Blocking** - it blocks an active device input to activate a PG output or to perform any reaction activation. Perform blocking manually by keypad, F-Link, J-Link or the MyJABLOTRON application. So this way it is possible to block a device input anytime not during the setting procedure. The function depends on the option given by the parameter Ways of setting.

**Autobypass** – automatic bypass of the system reaction to a device according to options. Input activation after 3x activations or 3x alarms (optionally by F-Link SW , Parameters tab), faults after 3x activations as well.

**Disabling** – this option serves for temporarily manual disabling selected sections, devices, users, programmable outputs (PG) or calendar actions. The section to which the control panel is assigned (always section 1) cannot be disabled and this is true for the Service code at position 0, Administrator's code at position 1. For devices we distinguish Blocking (it is only about input activation) and Disabling the device, see chapter 9.13 Disabling and blocking options.

**Ways of setting** – selection of the level of the system setting procedure. Options are from the lowest level where the system doesn't check anything (always sets) up to the highest level where the system doesn't allow you to set if any device is activated (for example an open window), see chapter 9.9 Obstacles preventing setting the system.

**Event history** – the system records occurring events in its memory. The contents of the memory can be viewed from the F-Link SW using the “Event history” key or from keypad. The beginning of an event is usually registered as Activation (status of a device, fault, tampering etc.) and the end of an event as Deactivation. Statuses of sections are registered as Set / Unset, alarm statuses as Alarm / Alarm expiration, Alarm mute or Alarm Cancellation.

ID	Time	Source	Section	Event	Channel
59	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant activation	11: Device 11
60	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant Deactivation	11: Device 11
61	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant alarm	11: Device 11
62	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant activation	4: Device 4
63	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant alarm	4: Device 4

Magnet activation and deactivation  
Alarm Beginning and End

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

**MicroSD memory card** – the control panel uses a microSD card as a memory medium. After connecting the control panel to a PC using a USB cable two drives will be displayed in the File Manager. FLEXI\_CFG and FLEXI\_LOG. The capacity of supplied card can be 4GB (SD/SD-HC), or it can be higher. Before you use brand new SD card perform the control panel reset to get default settings see chapter 12 Reset of the control panel. And then perform upgrade firmware, see chapter 13 Firmware updates This procedure save all required files (default texts, voices, etc..) to the SD card.

**FLEXI\_CFG** – with hidden directories and files that contain system settings. Do not alter the contents of the drive, there is a risk of loss of functionality of the system.

**FLEXI\_LOG** – contains the BACKUP, PHOTO directory and the FLEXILOG.TXT file, where all system events are recorded. Selected data from the file can be viewed in F-Link / Event History. The PHOTO directory is used to store IMGnnnnn.JPG files that have been sent to the control panel from camera devices (e.g. from a JA-160PC motion detector with a camera). Both file types (txt and jpg) are stored in an encrypted form and their contents cannot be normally viewed with text and picture viewers. Their contents can only be viewed if the F-Link software is also run in the PC at the same time and the authorization level Service, Administrator or ARC is confirmed by entering of the respective code. Events are recorded in the FLEXILOG.TXT file up to the size of 10 MB, then the file is renamed to FLEXILOG.OLD and a new file is created.

**SIMLock** – a function of the control panel that can be activated by the respective ARC on registration of the control panel to MyJABLOTRON. If this function is activated, then after replacement of the used SIM card with another one the system will automatically delete the ARC setting (the registration of the system JA-100K Security System Control Panel

to MyJABLOTRON will have to be renewed). This step is used to prevent undesired transmission of information to the ARC from a different card than the one that was registered for it and from which the setting was done.

## 1.1 Basic system configuration requirements

Adhere to the requirements of the valid norms when designing the system. The basic handbook for designing security systems, their commissioning and servicing is described in the technical specifications CLC/TS 50131-7. This document must be applied to systems installed and classified according to the EN 50131-1, Security grade 2.

The JA-100K control panel can be set to have behaviour according to a pre-set **System profile** along with further stated conditions comply with the following profiles:

1. **Default** Factory pre-set profile, all system parameters are optional.
2. **EN50131-1, Grade 2** Profile pre-sets some specific system parameters (valid for control panel, keypads, sirens, etc.) according to the given norm requirements valid for security grade 2.
3. **INCERT T031, Grade 2** Profile pre-sets some specific system parameters (valid for control panel, keypads, sirens, etc.) according to the given norm requirements (Belgium directive T031) valid for security grade 2. The profile is based on the EN 50131-1 profile, Grade 2 and it's highly regarded for increased premises security against tampering and intrusion.

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

Ways of reporting	System profile and adequate configuration		
	Default	EN 50131-1, Grade 2	INCERT T031, Grade 2
Local alarm reporting	<b>Recommended:</b> JA-110A or JA-163A or JA-110A pre-set as an external siren	<b>Required:</b> JA-110A or JA-163A or JA-110A pre-set as an external siren	<b>Required:</b> JA-110A or JA-163A or JA-110A pre-set as an external siren
Remote alarm reporting – main channel (main communication path to ARC)	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol
Remote alarm reporting – backup channel (backup communication path to ARC)	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol	<b>Recommended:</b> LAN or GSM/GPRS channel with IP protocol or PSTN line with Contact ID protocol

**NOTE 1:** The JABLOTRON 100 alarm system is designed to comply with the norms mentioned in the individual system profiles. There have to be at least the basic requirements for alarm reporting ways and warning indications. Ways of reporting given by this table are based on EN 50131-1 + A1+A2, requirements, paragraph 8.6.4, Table 10. Detailed requirements considering the communication path properties to the ARC are mentioned in the chapter on communicator settings.

**NOTE 2:** The term communication path is meant as a physical transmission medium, for instance metallic cables, optical fibre/cables, or radio transmission.

**NOTE 3:** A backup communication path should be realized using a different physical transmission medium than the main medium. It is not possible to combine for instance GSM technology and a LAN based on a WIFI network. Both ways are radio transmission and can be jammed (tampered) simultaneously.

### \*Caution:

- Ensure that all LAN devices providing connection to the Internet network have their power backed up!
- Access to LAN devices or other communication panels or exchanges should be restricted for unauthorized persons!

During system designing it is necessary to take into account splitting into sections and pre-set entrance delays to be able to set the definition of delay zones. There can be 2 kinds of delayed zones (Delay and Garage door), each of them has its own timer to pre-set entrance and exit times.

Entrance/exit routes should be chosen as short as possible i.e. the route from the entrance door to the control keypad. The keypad (the main control device of the security system) should be placed close to the entrance

door considering the fact the user should be able to unset the system in 30 sec from the moment when the protected premises has been accessed. This requirement pushes to use multiple keypads in the protected premises and multiple access routes.

## 1.2 Access codes and their default settings

Authorization is necessary by a valid code or by applying the RFID card or tag to the authorization module (keypad) to be able to operate the system (setting, unsetting or to check the status of some section or device). According to the authorization level of the specific user the system shows you all information and allows system control appropriate to your access rights. A service technician performing system access from F-Link (J-Link) SW, remotely from the MyJABLOTRON app or by voice menu has to also be authorized by entering a valid access code.

The access code can have 4 or 6-digits (according to the selected system profile).

Codes for JA-100K	Default profile (4-digit codes)	EN50131-1 profile, (6-digit codes)	INCERT T 0xx (6-digit codes)
Code format:	<i>nnnn</i>	<i>nnnnnn</i>	<i>nnnnnn</i>
Service (default):	1010	101010	101010
Administrator (default):	1234	123456	123456

**Warning:** When the system profile setting is changed, all user defined codes are erased and the default codes (Service, Administrator) are pre-set to default values. All RFID cards/tags remain set in the system.

The service default code is filled in automatically by the F-Link software, so from the first activation until a code change the software does not request it. However for security reasons immediately when the installation is finished, it is imperative to change all default codes.

### 1.2.1 Change of access codes

The creation or change of user codes or RFID tags/cards can be performed by the system Administrator or a service technician. A new code or RFID tag/card can be assigned to the user with pre-set authorization. Only the service technician has rights to create such a user using F-Link SW.

**Access codes can be added and changed by:**

- the administrator from an LCD keypad (condition: the PC has to be disconnected from the control panel, no remote or local connection and already pre-set user with the required authorization)
- A service technician and F-Link software (condition: the enabled parameter Service and ARC can control the system)
- A user that doesn't have authorization to change his own code

Every user code can be set to an arbitrary value considering the code length given by the selected system profile, but the control panel restricts using the same code value for another user which has already been used in the system. Only system Administrator(s) is/are fully responsible for assigning and editing the user codes.

### 1.2.2 Security access codes and RFID devices

The control panel allows to every user assign one code (according to the selected profile) and one RFID tag/card for user authorization. Authorisation is required when the system is operated with a keypad. The security level is adequate for this fact and it can be represented by numbers in following table.

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

Control panel parameters	4-digit codes	6-digit codes
Duress access control – OFF Standard authorization – OFF	$= 10^4 - (\text{Number of users stored in the system} - 1)$	$= 10^6 - (\text{Number of users stored in the system} - 1)$
Duress access control – ON Standard authorization – ON	$\leq 10^4 - ((\text{Number of users stored in the system} - 1) * 3)$	$\leq 10^6 - ((\text{Number of users stored in the system} - 1) * 3)$
Duress access control – OFF Double authorization - OFF	$= 10^8 * (10^4 - (\text{Number of users stored in the system} - 1))$	$= 10^8 * (10^6 - (\text{Number of users stored in the system} - 1))$
Duress access control – ON Double authorization - ON	$\leq 10^8 * (10^4 - ((\text{Number of users stored in the system} - 1) * 3))$	$\leq 10^8 * (10^6 - ((\text{Number of users stored in the system} - 1) * 3))$
Using RFID card only with no digit code	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$

**Example:**

Selected profile:	Default	~ 4-digit codes
Number of users stored in the system:	Max 33	
Duress access control:	Disabled	
Number of code combinations:	$10^4 - 33 = 9\,967$ combinations / users (when there are 33 users)	

**Increasing the security level of codes:**

- Select a 6-digit codes (System profile EN-50131-1, INCERT)
- Select a level of authorization to „Double authorisation“, where the standard valid access code and an RFID tag/card are required to be both applied

**Protection against a code breaking attempt:**

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

### 1.3 Regular system check (maintenance)

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

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



**Overview of recommended maintenance / function control:**

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

All the procedures recommended by the system producer don't have a higher priority than local regulations and decrees.

## 2 System size

The security system size can be set optionally according to the protected premises size and the end user's requirements.

The control panel can be split into 4 sections (independently adjustable areas). Every device has its own address (keypads, detectors, sirens) and has to be enrolled to one of the sections. The number of devices, sections, users and programmable outputs is set using the F-Link software on the Initial setup tab. It makes installation more clear for programming. Their quantity can be increased or reduced (reducing is possible only when there are not already pre-set logical links which would block it).

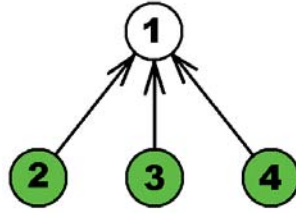
By that you can create a system either for a small apartment with one section and a few devices or for a large building which uses all the potential of the JA-100K control panel with independently controlled sections. Sections can be linked to other sections (common section) to control them and their statuses together.

### 2.1 Configuration and splitting

The JA-100K security system control panel is meant to be used for protecting small and medium premises thanks to its range, dimensions and number of sections. A section is a part of the system to which devices related to a protected area are assigned. Small premises may have one basic section (flat, garage, etc...) and in this case all devices are assigned to the same section. Medium systems can have multiple sections (for instance a family house, or an office building) and also its own 2<sup>nd</sup> level common section (common hall, cellars,

garages, toilets etc...). Very important for the operation of such systems is setting the user's authorisation to the lowest control level of the very basic sections. A common section is set automatically when every common section is set and unset automatically if at least one of the basic sections is unset.

Sections split into two levels  
(1-common, 2,3,4-controlled independently)



**2nd level**  
(controlled)

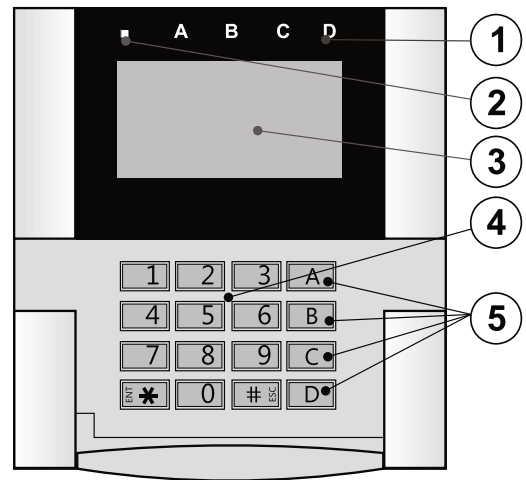
**1st level**  
(operated)

Note: The “cleaning lady” user with access only to the common section can have a virtual section assigned (1st level) and it does not have to include any detectors. Unsetting this virtual section also automatically unsets all the common premises sections (2nd level) where then she can move.

## 2.2 System control

The system keypad is meant for basic system control. There can be multiple keypads used in the system and each one of them can work differently according to its own settings. Any system section can be controlled from each keypad.

Every keypad offers 4 **functional buttons** for quick control. Each of them can be set for various functions such as setting/unsetting, appliance control or emergency calling. It can also be used for section status indication or PG output indication (it can indicate the active status by a standard red LED or a green LED – the function “PG indicates inversely”). That’s why the function button can for example serve as an indicator for a magnetic contact placed on a door to see if the door is open or closed. And one more purpose is as a “Common functional button” and by this you can control several sections simultaneously. Configuration of the keypad is described in the chapter 10.3.1 Keypad configuration.



1 – status indicator; 2 – system indicator; 3 - LCD display; 4 – keypad and RFID reader; 5 – functional buttons

## 3 The JA-100K control panel utility parameters

Primary component of the JABLOTRON 100 system is the JA-100K control panel. Its basic parameters are summarized in the table below:

Tab. 1

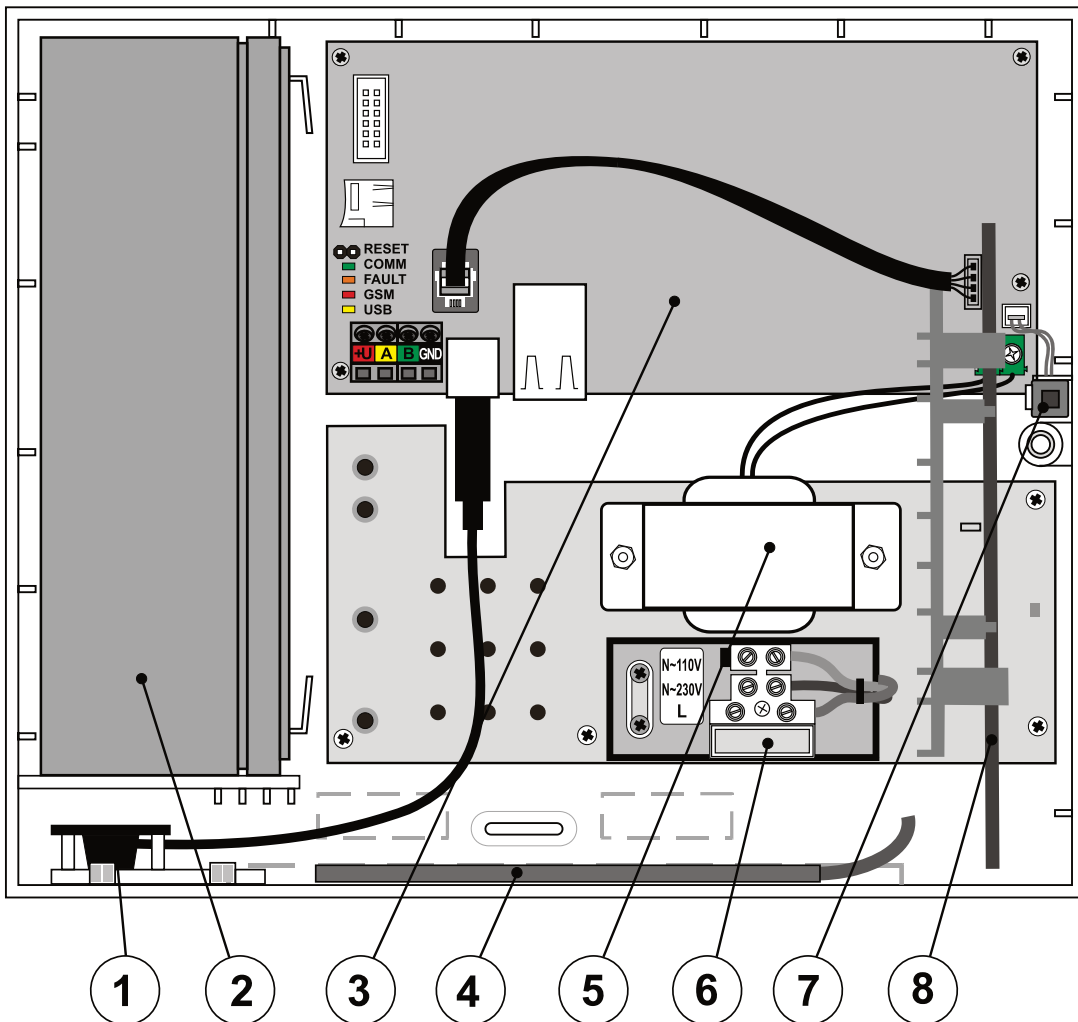
Feature / Type	JA-100K	Note
Maximum number of devices	32	The sum of wireless and BUS components
Maximum number of users	33	
Maximum number of independent sections (partitions)	4	
Maximum number of programmable outputs	4	
Maximum number of radio modules	3	
IP LAN (Ethernet) communicator	Yes	
GSM / GPRS communicator	No	Optional accessory
PSTN telephone communicator	No	Optional accessory
Recommended 12 V backup battery	Max. 2.6 Ah	Lead-acid battery
Maximum continuous current consumption available for devices from the control panel	85 mA (with LAN) 125 mA (no LAN)	For a 12 h backup supply from the recommended battery, the figure takes into account the internal consumption of the control panel
Maximum possible short-term current demand	1000 mA	Max. 5 min
BUS terminal	1+RJ connector	The RJ connector is only used to connect the radio module directly in the control panel.
Maximum BUS cable length	500 m	

### 3.1 Description of JA-100K control panel

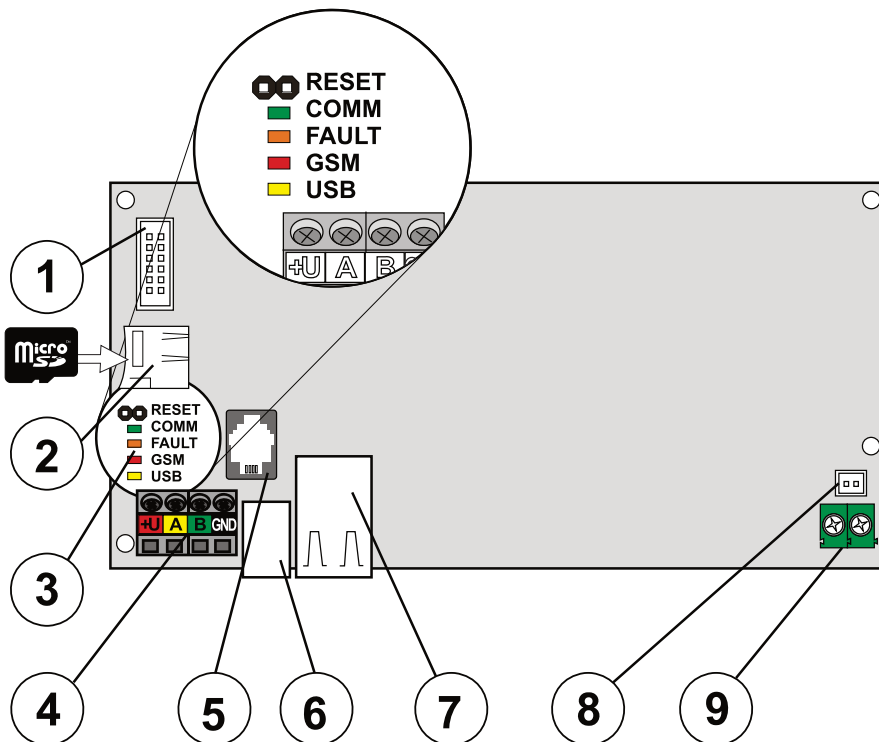
The JA-100K control panel can be also supplied with a pre-installed JA-111R radio module as a kit called the JA-100KR.

The JA-100K control panel is designed for **small BUS systems** and for **medium-sized systems** with wireless communication. The JA-100K control panel is equipped with a LAN communicator which can be connected to the Internet and with the ability to send data to secure mass storage areas, the so-called cloud (images taken by PIR detectors with a camera or photo verification cameras) or to the server of security agencies with technical equipment for this data to be received. It is also able to provide remote access using F-Link (J-Link) software thanks to an internet connection.

The control panel can also be equipped with a JA-190Y meant to be used with a GSM provider's network or the JA-190X supplementary telephone communicator (PSTN) to be connected to an analogue landline (e.g. PSTN) or to simulated telephone lines. They cannot be both used simultaneously (there is only one connector on the PCB). Those supplementary modules can be used for the system events reporting and also as a backup communicator if the previously mentioned LAN communicator indicates a fault (communication path failed).



1 – USB connector for PC connection ; 2 - Back-up battery 2.6 Ah; 3 - Control panel PCB; 4 - GSM antenna of a supplementary GSM dialler; 5 - Transformer; 6 - Mains power terminals, 200 mA fuse; 7 - Tamper contact of the housing; 8 – Radio module;



1 - Connector for supplementary modules (GSM or PSTN communicator); 2 - MicroSD card holder; 3 - LED indicators and RESET jumper; 4 - BUS terminal; 5 – Internal BUS connector for the JA-11xR module; 6 - USB cable connector; 7 - LAN connector, 8 - Panel Lid Tamper pins; 9 - Power supply input from the transformer

**Parts of the JA-100K control panel (changeable parts) are:**

- MicroSD card 4GB or higher – meant as storage to save events, pictures from PIR detectors and cameras

**To extend control panel options use:**

- The JA-111R radio module (from default pre-installed in the JA-100KR kit)
- The JA-190X PSTN communicator
- The JA-190Y GSM communicator
- The SA-214/2.6 Ah back-up battery

**Control panel accessories include:**

- 1pc Extension USB cable (20 cm) installed in the control panel
- 1pc Fuse T 0.2 A; 250 V (meant to protect a 230 V circuit)
- 1pc Fuse T 0.4 A; 250 V (meant to protect a 110 V circuit)
- 3pcs Fasteners 8 mm
- 3pcs Screws 40 mm
- 2pcs Ties 100 mm
- Installation manual

**3.2 Indication LEDs on the control panel board**

The following indication LEDs are on the main board:

Description	Colour	Meaning
<b>COMM</b>	green	Flashing during operation of the communication BUS indicates correct functioning
<b>FAULT</b>	yellow	Permanently lit indicates a general error in the system (more information provided by F-Link or a keypad with a display)
<b>GSM</b>	red	Status indication of a supplementary communicator (GSM or PSTN)
<b>USB</b>	yellow	Indicating USB connection to a PC

**3.3 Additional Connectors on the control panel PCB**

Additional Connectors on the control panel PCB:

- **RESET jumper** on its PCB, thanks to which the system can be set to factory default settings (if enabled by the parameter “Reset enabled”). The procedure is described in chapter 12 Reset of the control panel.
- **10 pin connector** to be used for connecting a supplementary communicator.
- **RJ connector (RJ-44)** for the connection of the JA-111R radio module if installed inside the control panel box. It is strictly forbidden to connect any device to this connector out of the control panel box.
- **LAN connector** for connection to the Internet
- **2-PIN connector** designed for a tamper contact to be connected. It indicates any attempt at damaging the front cover or opening the control panel. A rear tamper contact is not included with this version of the control panel.

**3.4 Connection terminals on the control panel PCB**

The control panel of a security system has the requirement to be connected to the mains (230 V / 50 Hz or 110 V / 60 Hz) power permanently. For more detailed information see the chapter 16 Technical specifications

The mains power is connected via terminals equipped with a replaceable fuse. The control panel is a protection class 2 device with double isolation. That’s why a 2-wire cable is enough (a live wire and a neutral wire). With a 3-wire cable leave the protective earth wire disconnected and isolated.

**Caution:** Don’t ever connect the earth wire to any terminal in the control panel!

For powering the control panel with a low voltage and BUS security isolation from the mains power, a small protective isolating transformer is used. The transformer is connected to the control panel by the small green terminal.

Internal communication between the control panel and connected devices is performed via the 4-wire BUS. It is realized by a single four-colour terminal (red, yellow, green and black).

A built-in USB connector type B is placed on control panel PCBs. Using a short extension it is possible to establish a connection with a PC via the USB cable without opening the control panel.

## 4 Before system installation



Select a hidden place for the control panel (inside the protected area) where mains supply is available.

The mains supply of the control panel may only be installed by a person with the required electrical qualifications.

The manufacturer doesn't allow to power the control panel up from other alternate power supply sources such as high capacity batteries charged by solar energy and so on.

The control unit JA-100K provides power supply terminals to select from 2 type of power supply voltage networks: ~230 V / 50 Hz and ~110 V / 60 Hz. According to the type of power supply voltage system, the correct connection terminal and the corresponding fuse must be used in comply with chapter no. 16 Technical specifications.

The power supply of the control panel has double safety separation of the circuits. No protective conductor is connected.

During the installation and connection of the BUS components of the control panel all the power supply of the control panel must be completely off.

**The manufacturer declines any liability for damage if the system is installed or set improperly.**

1. The arrangement and configuration of the system has to correspond to the design documentation of an alarm system according to the technical specification CLC/TS 50131-7, consultation with the customer and the valid technical norms for electrical installations.
2. Prepare the power supply of the control panel – use a suitable cable with double insulation and a cross-section of 0.75 to 1.5 mm<sup>2</sup>. Voltage surge protection on the control panel mains supply is recommended. It is also recommended to use a single cable with a circuit breaker (2 A-6 A) and it also functions as a main switch.

Caution: Don't connect any other electrical appliance to this specific circuit, not even power for external PG outputs or a heating system or any other device related to control panel functions (heat control etc.). Put a sticky label marked "Don't switch off" on the circuit breaker placed on the mains switchboard.

3. It is recommended to put some overvoltage protection in the mains circuit for the control panel.
4. Attach the control panel straight onto the wall or any other incombustible surface. Ensure there are no metal objects which could negatively influence transmitting or receiving radio signals (radio module and GSM communicator). Use the supplied template to prepare holes for fasteners. Put the screws through the upper holes in the plastic housing to keep it 1 cm from the wall, then hang the control panel housing on it. Also put an additional screw through the lower hole(s) and screw it in as well to stabilize the position of the control panel. Tighten all the screws.

## 5 Installation of BUS devices

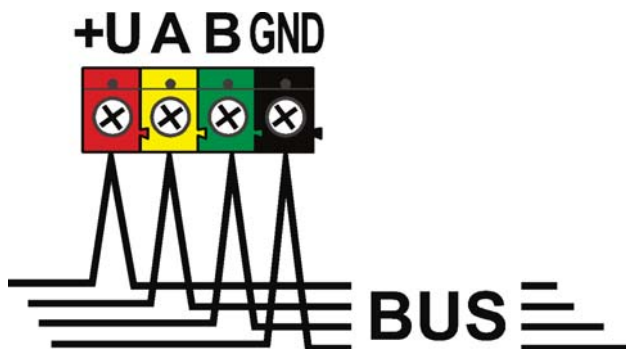
The BUS of the JABLOTRON 100 is meant to be used with BUS devices of the JA-1xx series. Proceed with the following procedure:

1. During the connection of any BUS modules the power supply of the control panel must be completely off (backup battery as well).
2. Follow the installation manuals of individual devices.
3. The BUS cable must be installed inside the area that is protected by the system. Inside the walls, metal pipes, in a lower ceiling or through places which cannot be easily accessed.
4. If the cable is outside the protected area, this part must be separated with a JA-110T BUS isolator. This isolator has to be placed in the protected premises and the cables installed out of the protected area are not meant for security applications.
5. For line branching use a JA-110Z BUS splitter (and/or the JA-110Z-B, JA-110Z-C).
6. During the connection of BUS devices pay attention to the colour of wires (red, yellow, green, black).

Connection of third party devices is possible via an appropriate module such as the JA-111H, JA-116H, JA-118M, JA-114HN, etc. The producer cannot guarantee proper functioning of the connected device nor its security grade.

## 5.1 JA-100 BUS

The BUS of the JABLOTRON 100 system consists of four wires (4-wire). The BUS cannot be shared with another system not even to power different devices.



BUS terminal board

terminal	colour	note
+U	red	positive power supply terminal; it can only be used to supply devices of the JABLOTRON 100 series
A	yellow	data A
B	green	data B
GND	GND	common terminal (negative power supply terminal)

## 5.2 BUS cables

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

Connect BUS devices using CC-01, CC-02 or CC-11 cable or equivalent.

**CC-01 cable** is designed for the main BUS line, or the connection of elements with a high consumption (siren) or remote elements. The cable has 4 wires (the colours corresponding to the BUS colour). The power supply wires (black and red) have a bigger cross-section of the core (0.5 mm<sup>2</sup>) as compared to the communication conductors (0.2 mm<sup>2</sup>). The cable is supplied in packs (1 pack - 300 m).

**CC-02 cable** is designed for branches from the main BUS line or for the connection of elements with a low consumption (detectors) or for short distances. The cable has 4 wires (the colours correspond to the BUS colour). All the wires of the CC-02 cable have the same core cross-section (0.2 mm<sup>2</sup>). The cable is supplied in packs per 300 m.

**CC-11 cable** is designed for the main BUS line, or the connection of elements with a high consumption (siren) or remote elements. The cable has 4 wires (the colours corresponding to the BUS colour). The power supply wires (black and red) have a bigger cross-section of the core (0.5 mm<sup>2</sup>) as compared to the communication conductors (0.2 mm<sup>2</sup>). The cable is supplied in packs (1 pack - 300 m) and it has fire certification.

### BUS layout:

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

## 5.3 BUS length and numbers of connected devices

The maximum length of one BUS without boosting (separation) is 500 m. The length is calculated as the sum of the length of all the cables between all the connected devices. The number of connected BUS devices is limited by the capacity of the backup battery of the control panel. To meet the standard for security grade 2, in case of a 230 V mains failure the system must reliably work for at least 12 hours being powered by the backup source. Thus, the total consumption of all the BUS devices must not exceed the maximum continuous consumption of current from the control panel, see chapter 5.4 Example of the calculation of BUS current consumption to back-up the system. To calculate the total continuous consumption of connected elements summarize their **backup consumption** (it is specified in the manual or use the summarizing table, see 14.1 Overview table of the current consumption of BUS devices).

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

## 5.4 Example of calculation of BUS consumption to back-up the system

The table presents an example of a small system with 5 BUS devices. The total idle consumption in the backup mode is 78 mA. Thus you can use the JA-100K control panel, which enables a maximum permanent loading of 125 mA and 85 mA when the LAN module is enabled.

Tab. 5

Device	Description	No. of pieces	Consumption in backup mode
JA-111R	Module for radio communication	1	25 mA
JA-110E	Control keypad	1	18 mA
JA-110A	Internal siren	1	5 mA
JA-111A RB	External backed-up siren	1	5 mA
JA-110N	PG output module	1	25 mA
<b>TOTAL</b>			<b>78 mA</b>

Parameter	JA-100K
Maximum permanent current from BUS	400 mA permanently (1000 mA for 5 min)
Maximum permanent current for 12 hrs backup	125 mA (with 2.6 Ah backup battery)

Calculation of BUS current according to the control panel HW configuration:

Backup battery 2,6Ah	175mA max. current from backup battery													
JA-100K	50	x	x	x	x	x	x	x	x	x	x	X	x	x
JA-111R	30		x	x	x	x							x	x
LAN	40			x	x	x	x	x	x					
JA-190Y	25				x			x		x			x	
JA-190X	15					x			x		X			x
Max. current taken from BUS for backup time 12h (mA)		125	95	55	30	40	85	60	70	100	110	70	80	

## 5.5 Power supply requirements

A security system which has to comply with security grade 2 has to be backed up by a backup battery for 12 hrs (according to EN 50131-1) and 24 hrs (according to INCERT T 031) during a mains power failure and it also has to be fully re-charged within 72 hrs (according to EN 50131-1) and within 48 hrs (according to INCERT T 031) after mains power recovery.

To comply with this requirement it is necessary to ensure that the backup battery capacity is adequate for the required time, see the following example. The nominal capacity of the battery should be checked by a test, see technical specifications CLC/TS 50131-7, system testing.

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

**JA-100K control panel**, for 2.6 Ah battery (calculation is valid for 80% of battery capacity)  
 $2.6 \text{ Ah} * 0.8 / 12 \text{ h} = 0.17 \text{ A}$  (according to the capacity - maximum current for 12 hrs)  
 $I_{\text{max}} = 0.17 \text{ A} - 0.05 \text{ A} = 0.12 \text{ A}$  (subtract the control panel self-current 0.05 A)

The current taken from each BUS output terminal is shown in the F-Link SW in the Diagnostics tab on line 0 where the control panel is. It is necessary to take consideration of the shown current especially when the JA-111R module is used

(wireless control panel) connected to the special RJ connector so also add the current of this module. This current is compared with a calculated current and it determines if the backup battery capacity is adequate to norm

Diagnostics	Calendars	Communication	ARC	
Battery stat...	Voltage/loss	RF Signal level	Chan...	Note
13,7 V/13,6 V	13.7 V/0 mA			
	0,0 V		BUS 1	



requirements for system backup time. If the measured current is higher than the calculated one, the backup battery should have a bigger capacity.

## 6 Use of wireless devices

In the JA-100 system you can use wireless devices of the JA-1xx series. The control panel must be equipped with at least one JA-111R radio module, a maximum of 3 radio modules can be used in the system.

When installing individual device follow the instructions in their manuals.

### 6.1 Installation of a JA-111R radio module

1. The JA-100KR kit has a built-in JA-111R radio module in the control panel box next to the transformer in a special plastic holder.
2. If the control panel is installed in a place with poor GSM signal reception, the GSM module increases its transmission power, which can have a negative impact on the radio module communication range. In such a case you are recommended to place the radio module outside the control panel, namely at least 2 m from it, where it will not be negatively influenced anymore and will have higher-quality radio reception from the devices, which will allow for longer ranges and consequently installation distances. It is necessary to put the JA-111R installed outside the control panel box inside a PLV-111R installation box (it is not supplied with a JA-100K kit, it has to be ordered individually).



**The RJ BUS connector on the control panel board is exclusively designed for the connection of a radio module installed inside the control panel housing.**

3. You can cover a larger area with radio signal by installing up to 3 JA-11xR radio modules in their own plastic housing in different places (e.g. each one on a different floor). Signals from a wireless device (here in after device) can be received by more radio modules simultaneously. The control panel communicates in a cycle with individual radio modules, so it will get information sent by a device from the radio module that was the first to receive an intact signal and reacts to it. Then, it will not get the same information from the other radio modules any more even though it was received with a stronger signal. Thus, it may happen that signals from the same unidirectional device may exhibit quite different data in F-Link / System settings / Diagnostics during repeated measurements depending on from which module the signal was taken. As regards to bidirectional devices, the control panel “reserves” the once used channel (communication with the first radio module) and after that it communicates with the particular device via this radio module only (shown in Diagnostics, the Channel column) until the device stops responding. Then, it looks for the connection signal in the other radio modules. If you need to verify the quality of connection of individual devices to individual radio modules, check it by the RF signal graph in the F-Link SW (button on the upper toolbar). There select the radio module for which communication should be checked and the activate devices you want to check. A graph of radio communication shows the RF signal strength measured by a specific radio module. It is also possible to have several RF signal windows open so you can very simply monitor the RF coverage in that premises.
4. Install a radio module vertically on a wall. It must not be situated near objects that shield or interfere with communications (metals, electronic devices, cables, pipelines etc.).
5. After switching the system on you must **enroll the radio modules first**. It is only then that you can enroll wireless devices.
6. Recommendation: It is recommended to enroll wireless devices to the system when they are placed in their final position. This installation procedure is not so comfortable but it helps you to achieve better and reliable radio reception at the radio module. The radio module has an algorithm which ensures a “minimum signal” from the device measured during service mode. That gives a reserve when radio conditions get worse in full operation mode (for instance when a building is re-configured, industrial interference, etc..). See more detailed information in the EN 50131-5-3 norm.

### 6.2 Installation of wireless devices – enrollment mode

Wireless devices have to be enrolled to the system individually. The enrollment procedure can be performed in Enrollment mode only using a PC with installed F-Link software. See chapter 8.4.1 Enrolling and erasing devices.



## 7 Switching the system ON

1. Check connection of the BUS cables.
2. Verify whether a microSD card is present in its holder on the control panel board.
3. Check whether the mains supply cable is correctly connected to the control panel and that the supply cable is firmly fixed.
4. Insert a battery in the control panel and fix it in the housing (using self-sticking blocks or a strap)  
**Caution - the backup battery is delivered in a charged condition, it must not be short-circuited!**
5. Connect the supply leads of the battery. Mind the correct polarity (red +, black -).
6. Switch on power from the mains and check the LED indicators on the control panel:
  - a. the green LED starts flashing (BUS function)
  - b. the red LED flashes – logging in to the GSM network by supplementary GSM communicator
  - c. the red GSM LED goes out – the GSM communicator is logged in to the GSM network
  - d. the red LED permanently lit – the control panel has not logged in to the GSM network
7. When the connected BUS devices start flashing yellow, assign them to the system, see chapter 8.4.1 Enrolling and erasing devices.
8. Perform configuration of the keypads, see chapter 10.3.1 Keypad configuration.
9. Set the required functions and test the system, see chapter 10.7 Parameters tab.

## 8 System configuration

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

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

The following part is about **Motion detectors**. It follows movement in protected premises using motion detectors (PIR) or their combination with other detectors. Detectors placed in a premises entrance usually have pre-set delay reaction or next delay reaction. The rest of the motion detectors are in most cases pre-set to instant reactions. You can select from up to 2 timers to make the entrance paths (for instance, a longer delay during entry through a garage).

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

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

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

### 8.1 The system profiles

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

**Caution:** *setting individual parameters by selection of a system profile doesn’t guarantee that the installed system complies with security grade 2. Only correct system design (using the right devices) and correct installation with CLC/TS 50131-7 requirements and ARC service implementation can ensure security grade 2. Classification of the JA-100K control panel and individual system devices of the JABLOTRON 100 system for security grade 2 is just the basic input, and according to that fact the security grade of the protected premises can be set.*

**System parameters overview considering the system profile is set:**

Device	Profile Parameter	DEFAULT		EN50131-1, Grade 2		INCERT	
		Option enabled	Blocking	Option enabled	Blocking	Option enabled	Blocking
Control p.	Siren when partially set (IW)	NO	NO	NO	NO	NO	NO
Control p.	Sirens enabled	YES	NO	YES	YES	YES	YES
Control p.	Administrator restricted Service/ARC rights	NO	NO	YES	YES	YES	YES
Control p.	Service and ARC controls the system	YES	NO	NO	YES	NO	YES
Control p.	Duress access control	YES	NO	YES	NO	YES	NO
Control p.	Alarm confirmation within one section	NO	NO	NO	NO	NO	NO
Control p.	Siren (IW output) when tamper is triggered	NO	NO	YES	YES	YES	YES
Control p.	Reset enabled	YES	NO	NO	YES	NO	YES
Control p.	Report unset section	NO	NO	NO	NO	NO	NO
Control p.	Unsuccessful setting	NO	NO	YES	YES	YES	YES
Control p.	Alarm memory indication	YES	NO	NO	YES	NO	YES
Control p.	Delayed report to ARC	NO	NO	YES	NO	YES	NO
Control p.	Ways of setting	According to system profile	NO	According to system profile	YES	According to system profile	YES
Control p.	Authorization type	Standard	NO	Standard	NO	Standard	NO
Control p.	Loss of a BUS device	Fault	NO	Tamper always	NO	Tamper always	NO
Control p.	Alarm length	240	90..1200	240	90...900	240	90...900
Control p.	Entrance delay	30	5...120 s	30	5...30 s	30	5...30 s
Control p.	Exit delay	30	5...120 s	30	5...60 s	30	5...60 s
Control p.	Entrance delay by garage door	60	5...360 s	30	5...30 s	30	5...30 s
Control p.	Exit delay by garage door	60	5...360 s	60	5...60 s	60	5...60 s
Radio module	RF jamming detection	Disabled	NO	Low	NO	Low	NO
Keypad	Optical indication setting	1.(BUS) or 4.(RF)	NO	2.(BUS) or 4.(RF)	YES	2.(BUS) or 4.(RF)	YES
Keypad	Indicate UNSET status	YES	NO	NO	NO	NO	NO
Keypad	Indicate SET status	YES	NO	NO	NO	NO	NO
Siren	Warning (Acoustic indication)	NO	NO	YES	YES	YES	YES
Siren	Communication loss	NO	NO	YES	YES	YES	YES
Siren	Warning (Optical indication)	NO	NO	YES	YES	YES	YES

By setting the „Default“ system profile, all the mentioned parameters are pre-set back to factory settings and all parameters can be changed. The alarm system then doesn't comply with the requirements of security grade 2 and also violate the requirements given by the insurance company or local regulations. In the case of a harmful event, the insurance company doesn't have to pay for the damage because of incorrectly programmed system caused by the installation company.

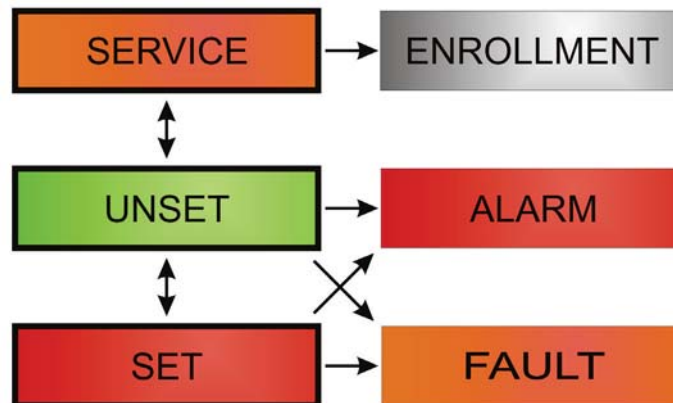
**Global overview of reasons preventing setting according to the pre-set system profile:**

Event \ Profile	Default		EN50131-1, grade 2		INCERT, grade 2	
	Passable	Impassable	Passable	Impassable	Passable	Impassable
Active tamper	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Active input (any input)					<input checked="" type="checkbox"/>	
Active instant input	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Active alarm memory indication				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
RF device 20 min no response			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Siren fault				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Fault	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Loss of a device	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Low Batt in device	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Low Batt in control panel	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Failure of battery in control panel	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
AC fault			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
AC fault for 30 minutes	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
System in configuration				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
GSM fault	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
LAN fault	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
PSTN fault	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Fault of all ARCs				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

## 8.2 Control panel operation modes

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

MODE	Description
<b>SERVICE</b> (+ Enrollment mode)	A mode in which no alarm can be triggered. It is only meant for a service or an ARC technician and it is for enrolling new devices and system configuration. No control is available in this mode (locally nor remotely). Functional buttons on keypads are switched off and the mode is indicated by yellow flashing of the system indication button (2x flashes every 2 sec) and signals from remote controls or other devices are ignored. Entering or leaving service mode can be performed from an LCD keypad or from a PC using F-Link software. When a PC is connected online, service mode cannot be entered or left from the keypad.
<b>UNSET</b>	A normal mode in which intrusion detectors don't guard. Free movement is possible through the premises, opening windows and doors is allowed. Environmental (Smoke / temperature, gas leak detectors or flood) detectors or panic buttons can trigger an alarm all the time. Also tamper contacts of all devices always protect and when they are activated the system triggers a tamper alarm. Unset mode is indicated on the keypad by a green light on the specific status indicator (letters A-D) and indication button.
<b>SET</b> (fully or partially)	All detectors are active and guard (except Internal detectors when partially set) and when they are activated then an alarm is triggered (next point). Set mode is indicated on the keypad by a red light (yellow light when partially set) on the specific status indicator (letters A-D) and indication button.
<b>ALARM</b>	Alarm is a state when for a pre-set time (alarm length) the IW and EW outputs are activated and the internal and external sirens sound. The Alarm state is indicated on the keypad by rapid flashing of the red system indicator. For a description of differences in EW and IW output behaviour read the chapter 8.5 Types of alarms.
<b>FAULT</b>	Fault is a warning signal of the system which indicates some abnormal state of the control panel, communicators or devices and their power problems (mains power or battery) or communication troubles.



## 8.3 Authorisation of users

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

Code authorization	Type Description
<b>ARC code</b>	This code has the highest level of authorization to configure the system's behaviour and is exclusively allowed to perform the system unblock after a triggered alarm. It can enter Service mode, access all tabs with options including ARC communication to which it can deny access to a Service technician (Service code). As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the ARC code can control all sections and PG outputs used in the system. This code enables to add more Administrators and other users with a lower level of authorization assign them with codes, RFID tags or cards. It also has a permission to erase alarm and tamper alarm memory. The number of ARC codes is limited only by remaining capacity of the control panel. The number of ARC codes in the system is limited only by remaining capacity of the control panel and no ARC code is pre-set by default.
<b>Service code (Service)</b>	It can enter Service mode and configure the system's behaviour. It has access to all tabs with options including ARC communication unless the access is limited by the ARC technician. As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the Service code can control all sections and PG outputs used in the system. It can create a user with ARC permission, other Service technicians, Administrators and other users with a lower level of authorization and assign them with access codes, RFID tags or cards. The number of Service codes is limited only by remaining capacity of the control panel. It is given position 0 and it cannot be changed. The default Service code is 1010 and when the EN profile is enabled then it's 101010. The code cannot be erased.
<b>Administrator (Main)</b>	This code has always full access to all sections and is authorized to control all PG outputs. The Administrator can create other Administrator and other codes with a lower level of authorization and assign them with access to sections and PG outputs, access codes, RFID chips or cards. Has permission to erase the alarm memory. There can be only one main Administrator code which can't be erased. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized as to confirm access. It is given position 1 and it cannot be changed. The default Administrator code is 1234 and when the EN profile is enabled then it's 123456. The code cannot be erased.
<b>Administrator (Other)</b>	Has access to sections selected by the main Administrator to which the other Administrator can add new users with the same or lower level of authorization to control sections and PG outputs, assign them with access codes, RFID tags or cards. Has permission to erase the alarm memory in assigned sections. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized as to confirm access. The number of Administrator codes (other) is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
<b>User</b>	This code has access to sections and PG control rights assigned by an Administrator. Users can add/delete their RFID tags and access cards and change their telephone numbers. It has permission to erase the alarm memory in assigned sections. Selected users may have their access to sections limited by a schedule. The number of User codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults. The user doesn't have permission to edit their own access code nor to erase it.
<b>Set</b>	This code is allowed only to set a designated section. Users with this level of authorization are not allowed to change their code and are not allowed to erase the alarm memory. The number of Set codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
<b>PG only</b>	Allows the user to control programmable outputs with authorization only. This applies to both switching on and off. Users with this level of authorization are not allowed to change their code and are not allowed to erase the alarm memory. The number of PG only codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
<b>Panic</b>	This code is allowed only to trigger Panic alarm. A user of this code is not allowed to change it or erase the alarm memory. The number of Panic codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
<b>Guard Code</b>	This is a code for a security agency. This level of authorization allows to set the whole system. However the guard code can unset the system only during alarm or after it as long as the alarm memory is still active. A user of this code is not allowed to change it or erase the alarm memory. The number of Guard codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.
<b>Unblocking code</b>	This code is designated to unblock the system after System blocking by alarm. A user of this code is not allowed to change it or erase the alarm memory. The number of Unblocking codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.

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



## 8.4 System optional parameters (F-Link – Parameters tab)

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

**Sirens enabled** – Enables all BUS and wireless sirens of the system. Designed for disabling the acoustic alarm during system testing.

**Administrator – restricted Service / ARC rights** - Administrator authorisation (code at position 1) is required to access the system for the ARC or service technician. In the case of remote access by a service technician to the system via F-Link the administrator may get authorised using a keypad in the building. In the case of a local connection by a service technician to the control panel using a USB cable the administrator may get authorized remotely using the voice menu when a GSM communicator is connected.

**Service and ARC controls the system** - This is for the service and ARC technicians to control (Set / unset) all sections and all PG outputs (ON / OFF) who require authorisation.

**Duress access control** – This function is to trigger a silent panic alarm by authorization only or during system control (setting, unsetting, PG) when a user is under pressure from an intruder. A panic alarm is triggered during system control by adding the number „1“ to the last digit of the code. When a user code has the number 9 as the last digit then during access control enter 0 as the last digit.

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

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

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

**Report unset section** – The system reports about an unset section when there is no movement detected within 16 hours.

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

**Alarm memory indication** – Indication of an alarm by a built-in LED in the detector by which the alarm was triggered. Available for devices which support this function.

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

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

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

### 8.4.1 Enrolling and erasing devices

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

1. Device enrollment is performed through the F-Link software, the Devices tab, **Enroll** button Enrolling is **only possible in the Service mode**.
2. You can enroll a device in several ways:
  - a. **by pressing the tamper switch of a BUS device = closing the cover** (some devices can be enrolled by the pressing of a key – see the manual of the particular device).
  - b. **by connecting the battery to a wireless device** - however, at least one radio module must be enrolled first. In the case of remote controls of the JA-186Jx type the battery connection can be replaced by pressing and holding two buttons (forming a pair). Remote controls of the JA-154Jx type are enrolled by pressing of any button.

- c. **By entering the serial number in the SN production code field** (it is found under the barcode on the board inside the device, e.g. 1400-00-0000-0123). The number can also be read with an optical barcode reader. Subsequently, you should activate the detector to verify its enrollment.
  - d. **by selectively loading not enrolled BUS devices** – if one or more devices that have not been enrolled yet are connected to the BUS, after pressing of **Enroll** in the **Device** the **Scan/add new BUS devices** button will be displayed, which will offer enrollment of the BUS device. You will enroll the device by double clicking on the selected item.
  - e. by collectively loading **not enrolled BUS devices** – if one or more devices that have not been enrolled yet are connected to the BUS, after pressing of the **Scan/add new BUS devices** button all the BUS devices will be enrolled collectively. This procedure does not allow you to determine the sequential positions for individual devices.
3. You can delete a device by deleting its production code (just the device will be deleted) or by selecting the respective line in the Devices tab and the Delete option in the menu or under the right mouse button or by merely pressing the Delete key, which will delete the whole line of the device (with its settings of the section, reaction, PG output control, notes and other options). This way, after marking more devices (click+Shift or click+Ctrl) you can delete all of them or you can just change a common parameter.

**Caution:**

*It is recommended to enroll wireless devices to the system according to point B in real conditions and at the required place in the protected premises. You can prevent troubles with insufficient RF range when you enroll devices "on the table".*

**Notes:**

- BUS devices that have not been enrolled flash with yellow light. If a not enrolled device does not start flashing with the yellow LED within approx. 180 sec. after enabling of the power supply of the control panel (in the course of initialization) check whether the device is properly connected.
- Wireless devices with unidirectional communication do not have any means of signalling the enrollment request.
- If you enroll a device in the system using the above mentioned procedure, the next position will be offered automatically. You do not need to take any steps; you just need to enroll devices in the selected order. Automatic movement to the next position can be cancelled in the device enrollment window.
- If you enroll an already enrolled device on another position, it will move automatically.
- If a device occupies more than one position, it will automatically occupy the respective number of consecutive position by one enrollment (e.g. the JA-116H module, which has sixteen alarm inputs, will occupy sixteen positions). Caution, inadvertent deletion of device enrolled on other position can occur!
- If you enroll a device on the highest possible position, the process of gradual enrollment will be completed.
- Free positions are assigned to section 1 by default. The assignment to a section can be changed later.
- For multi-position devices such as JA-116H, JA-118M, JA-114HN, JA-150M etc. you can limit the number of occupied positions by erasing specific lines when the module is enrolled. Perform erasing by clicking on the particular line on required position (Not button in column type!) and press button Delete on the PC keyboard.



## 8.4.2 List of applicable reactions

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

**Caution:** The range of reactions can be limited by the system profile.

<b>Delayed</b>	Intrusion alarm with entry / exit delay
<b>Instant</b>	Instant alarm if it is set. If an entry delay is set, an IW alarm is released. An EW alarm is only released after expiration of the entry delay time (more information about EW and IW - see chapter 8.5 Types of alarms).
<b>Garage door</b>	Intrusion alarm with entry / exit delay, timer garage door. In the Parameters tab you can set for this reaction that the exit delay will be extended by an active status detector with the Garage door reaction (e.g. for the time of opening of the garage gate).
<b>Next delayed</b>	Intrusion alarm. A detector provides the same exit delay as the delayed detectors in the same section. This detector will only provide the entry delay if it is activated after a detector for which a delayed reaction has been set. If it is the first one to be activated, it will release an alarm immediately. This setting makes sense if a delayed detector is set in the same section.
<b>Instant always</b>	Instant zone reaction. If set, then based on activation, instant including EW and IW alarm warnings is activated also during entry delay time.
<b>Instant / Delayed</b>	The system reacts to triggering a detector (alarm, entrance delay) when partially set as an Instant zone, and when fully set as a Delayed A zone.
<b>Instant confirmed</b>	Instant intrusion alarm – see the chapter <b>Confirmed intrusion reaction</b> below.
<b>Delay confirmed</b>	Intrusion alarm with an entry and exit delay, timer A - see the chapter <b>Confirmed intrusion reaction</b> .
<b>Tampering</b>	Tamper alarm any time (the section does not need to be set).
<b>24 hours</b>	Immediate intrusion alarm (the section does not need to be set).
<b>Silent Panic</b>	Silent Panic alarm: 1) EW and IW not activated (see chapter 8.5 Types of alarms); 2) the keypad does not beep although otherwise it is set like this; 3) if the system can distinguish who triggered the Panic alarm (e.g. through a tag with adopted user's identity or by entering of the code by the user, it does not send Panic SMS to this user.
<b>Audible Panic</b>	Audible panic alarm (the behaviour is the same as a Silent panic, the only difference is that an alarm is signalled by the used siren according to the table in chapter 8.5 Types of alarms).
<b>Fire alarm</b>	Fire alarm regardless section status (the section does not need to be set).
<b>Fire confirmation</b>	Fire alarm regardless section status (the section does not need to be set), see the chapter <b>Confirmed fire reaction</b> below.
<b>Fire instant</b>	Fire alarm only if the respective section is set.
<b>Gas</b>	A fire alarm triggered by a gas leakage detector can be always triggered regardless section status.
<b>Health troubles</b>	Sends a health trouble report.
<b>Flooding</b>	Sends a flood alarm
<b>Set / Partial Set</b>	Setting (partial setting) of a section. If the section is a common one, all sections that belong to it will be set at the same time. This reaction also has the Unset function.
<b>Mute</b>	Silencing of the internal siren with a subsequent report of the presence of a person in the building.
<b>None</b>	Without any impact on the intrusion alarm however, the device may be used to activate PG outputs. Tampering, supervision and fault detection is kept.
<b>None with no tamper</b>	The system reacts to detector triggering by PG output control only. None of the alarm types are triggered (even a tamper alarm), fault detection is kept.

### 8.4.3 Limitation of false alarms

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

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

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

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

**Three-strikes function (3x and STOP!)** - all detectors with an activated alarm reaction of the intrusion and fire type are limited to three possible activations of the control panel during one monitoring period at the most. After three activations (on the fourth intrusion) a bypass is activated for the respective alarm input and the corresponding sensor is excluded from further activity. If these three activations occur during an alarm, three alarm SMS messages are generated altogether and then the detector is disabled. If these three activations occur in time intervals that are longer than the duration of an alarm, three alarm SMS messages are generated, three alarms are triggered and then the detector is disabled.

A bypass can be cancelled by unsetting and subsequently setting the section, then the detector is back in guarding mode again. The bypass for the fire and flooding reaction is also cancelled automatically on the next day at 12:00. The bypass mechanism of 3x and stop is not applied to devices where the Panic reaction has been set.

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

## 8.5 Types of alarms

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

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

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

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

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

### 8.5.1 Intrusion alarm

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

### 8.5.2 Tamper alarm

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

### 8.5.3 Fire alarm

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

There are different types of alarms such as:

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

### 8.5.4 Panic alarm

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

- 1) **Silent panic** – a special event not assigned to a group of intrusion alarms, which would be indicated by a siren or keypad. A silent panic has no timer and there is no end to this event. So it cannot be used for the status control of a PG output. It is only for triggering a silent panic alarm and call help under duress without the awareness of the attacker. A silent panic can be triggered from a particular (hidden or portable button) panic button. Usually by a button pre-set to a silent panic, by a combination of keys A,B,C or D on the remote, by a keypad with a special functional button pre-set to a silent panic (in this case a panic alarm can be delayed with an optional timer), by pressing the button on the internal siren, by an input on the BUS module meant for wired devices or by entering a special code for silent panic triggering. A silent panic can also be triggered when Duress access control is performed (see chapter 9.8) where the standard user code is modified.
- 2) **Audible panic** – is a usual alarm event with a beginning and an end so it is indicated acoustically by siren and keypad. It can be used for the status control of a PG output. And mostly it is used for triggering a panic alarm with an optical indication requirement or for blocking electric door locks etc. An audible panic alarm can be triggered from a particular (hidden or portable button) panic button. Usually by a button pre-set to a silent panic, by a combination of keys on the remote, by a keypad with a special functional button pre-set to a silent panic (in this case a panic alarm can be delayed with an optional timer), by pressing the button on the internal siren, by an input on the BUS module meant for wired devices.

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

### 8.5.5 24hr alarm

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

## 8.6 System faults

A fault is a warning signal from the system which indicates some abnormal state of the control panel, communication or devices. The problem can be related to radio, the supplementary GSM module or the LAN communicator, masking the detectors (with an antimasking function), problems with power (mains power or battery) or the back-up power supply. Fault(s) is/are optically indicated on system keypads by the yellow system indicator. Fault reporting is taken from every source and with the 4<sup>th</sup> fault activation the source of the fault is bypassed which means that the 4<sup>th</sup> fault is not reported.

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

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

## 8.7 Fault caused by loss of a device

Every device (BUS or wireless) in the system is supervised by the control panel when the Supervision parameter is enabled (see Parameters tab/ Supervision column) and communication with the control panel is lost (no response within a pre-set time) then the system triggers the event “Fault activation” and according to the “Loss of a BUS device” it can be followed by a tamper alarm. It is optional and can be triggered when the radio module detects RF jamming or some kind of RF interference which takes a minimum 30 sec at 2 detection levels. And it can also trigger a tamper alarm when a short circuit occurs on the system BUS which avoids proper the communication of BUS devices. The communication time-out is a fixed time and cannot be changed. For BUS devices it is 8 sec and for wireless 120 min from the last communication.

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

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

## 9 System control options

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

Type	Way/mode	Device	Condition	Control description
Local	Keypad (authorization and functional button)	JA-110E, JA-150E	The JA-111R radio module for wireless keypad	Operation can be performed after user authorization and pressing a specific functional button or also via the keypad menu.
	RFID reader (authorization only)	JA-110E, JA-150E	The JA-111R radio module for wireless keypad	Operation can be performed after user authorization or using an RFID tag or entering a code
	Calendar	10 calendar actions		Every calendar action has options to select: event, time of its performance, day of the week. It can control sections and PG outputs. PG outputs can be blocked.
	F-Link or J-Link software	PC with Windows	USB cable	Sections and also PG outputs can be controlled after authorization.
Remote	Voice menu	Telephone	Supplementary GSM or PSTN dialler	Calling the system telephone number and control system by DTMF tones after authorization.
	Remote controller	JA-16xJ	The JA-111R radio module	Setting and unsetting by pressing a pre-set button of a remote.
	SMS message	Cell phone	Supplementary GSM dialler	Authorized command for setting or unsetting sections and also control of PG outputs.
	Dialling in from authorized telephone number	Telephone (PG control only)	Supplementary GSM or PSTN dialler	For every authorized telephone number one specific PG output can be controlled.
	F-Link or J-Link software	PC with Windows (XP SP 3 or higher)	Supplementary GSM or LAN dialler	Sections and PG outputs can be controlled by virtual keypad after authorization.

All mentioned ways can be used for system control (setting, partial setting, unsetting) for PG output control (ON, OFF, timing).

### 9.1 Way of authorization

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

- Access code (4, or 6-digit number depending on selected system profile (default, EN, INCERT))
- RFID card or tag
- Telephone number for authorization during remote access by telephone call or by SMS (when a supplementary GSM dialler is connected)

To adjust the security level the authorization level can be pre-set at the following 2 levels:

1. **Standard** – authorization is performed by applying an RFID card/tag or entering a valid access code
2. **Double authorization** - For authorization on the system keypad it is always required to enter a valid access code and RFID tag/card (regardless of the order of authorization). During remote access the telephone number is always verified and entry of a valid access code as well. F-Link monitors whether a code and a card are assigned to a user in the Users tab (otherwise F-Link won't allow you to save the configuration).

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

## 9.2 System control by keypad

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

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

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

### The setting procedure:

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

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

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

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

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

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

- a) Control from a keypad placed inside the protected premises with perimeter protection (entrance hall, etc.). All detectors in the entrance hall have to be pre-set to a Delay reaction to ensure that when the system is set their activation triggers some time for entry to unset the system.
- b) Control from a keypad placed outside protected premises with perimeter protection (internal hall, stairs, bedroom, etc.). This variant doesn't allow the entrance of any person without instant alarm triggering. The premises can be entered by previous unsetting by remote controller, when supplementary GSM module connected then by voice menu or by SMS. Detectors are pre-set to an Instant / Delay reaction in this case.

### System control by keypad - procedure:

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

#### Setting the system:

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

### Unsetting the system:

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

### **Keypad system indicator - overview of statuses:**

Lights green ON	Normal operation. Sections controlled from keypad are OK with no faults.
Lights yellow ON	Normal operation and in some of the controlled sections a fault has been detected. From the keypad menu you can get more detailed information after user authorization according to their access rights. If the fault is followed by a rotating Jablotron logo on the keypad it represents a fault of radio communication between the control panel and the keypad.
Lights red ON	Keypad in BOOT mode, during a FW upgrade.
Flashes green (2 Hz)	Authorization performed, the user can change the system status by the functional button or browse the menu of the keypad. Authorization time-out takes 8 sec from the last key pressing or cancelled by pressing ESC.
Flashes yellow (8 Hz)	Unsuccessful setting warning indication
Flashes red (8 Hz)	Indication of a currently triggered alarm in a specific section on the keypad. The type of alarm, name of the section where an alarm has been triggered and the source of the triggered alarm are visible on the keypad.
Flashes alternate red/yellow	Triggered alarm with an active fault
Flashes alternate green/red	Authorization with alarm memory
Flashes alternate green/yellow	Authorization with an active fault
Flashes yellow (2x every 2 sec)	Programming / Service mode. All functional buttons are not available for users and the Administrator keypad menu. The keypad menu is only available for a service technician until the PC is connected to the control panel.
Flashes red (2x every 2 sec.)	Alarm memory indication
Flashes yellow (1x every 2 sec)	Fault indication on keypad in sleep mode (valid for EN50131-1 profile only)
Flashes red (1x every 2 sec)	Alarm memory indication on keypad in sleep mode (valid for EN50131-1 profile only)
No indication	Keypad in sleep mode

### **Keypad functional button optical indication overview:**

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



### 9.3 System control by remote controller

If there is a requirement to control the system before access to the protected premises (arriving by car at the garage) or building to be protected just by detectors with an instant reaction, it ensures no one can unset the system from a keypad inside the protected premises (no entrance path), this can be realized by remote controller before you access the building. It requires the JA-111R radio module to be enrolled to the system for communication with wireless devices. It has to be placed at the right place to ensure reliable communication with the remote in addition to the required working distance.

Every button of a controller can control a selected section (the right one always sets and the left one always unsets). Remote controllers respect the rules on how the system should be set, so with any obstacles preventing the setting it will not be possible to set the system.

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

### 9.4 System control by a calendar

Automatic system control can be performed by the control panel's internal calendar. The calendar can be pre-set to do up to 10 actions (full setting, partial setting, unsetting of selected sections and also switching ON / OFF or blocking / unblocking of selected PG outputs).

Every action can allow days of the week (from Monday to Sunday) to be pre-set when it can be performed so only working days or the weekend can be pre-set. For every action it is necessary to select the time and the particular action to be done and also one event (action) for PG output control. So at a specific hour section(s) can be set or unset and simultaneously a PG output ON or OFF. A typical application is the automatic setting of a section in shops, partial setting of a building at night or light control in the night. Every automatic event is recorded in the history log with the name of the source being "Calendar".

#### Calendar control options related to guarding:

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

<b>Always set immediately</b>	It sets pre-set section(s) immediately without an exit delay or any acoustic indication. The system is set immediately so no movement is possible in the protected premises. The option is for fast and silent setting with no warning. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
<b>Always set partially and immediately</b>	It sets pre-set section(s) partially and immediately without an exit delay or any acoustic indication. The system is set immediately in a pre-set time. The option is for fast and silent setting with no warning. The control panel doesn't fully respect all ways of setting and checking the systems ready to be set rules.
<b>Unset</b>	Unset pre-set section from any guarding level (fully or partially set).
<b>No</b>	No control function pre-set.

**PG output control options using calendar:**

<b>Activate PG</b>	Activates programmable output(s) if they are not blocked (for instance by calendar, device or section).
<b>Deactivate PG</b>	Disable programmable PG outputs.
<b>Block PG</b>	Blocks pre-set PG outputs. Those outputs won't be possible to switch on at all until it will be unblocked by the calendar action "Unblock PG". Entering or leaving service mode don't unblock it.
<b>Unblock PG</b>	Unblocks pre-set PG output blocking.
<b>No</b>	No blocking function pre-set.

**Function blocking action by the calendar:**

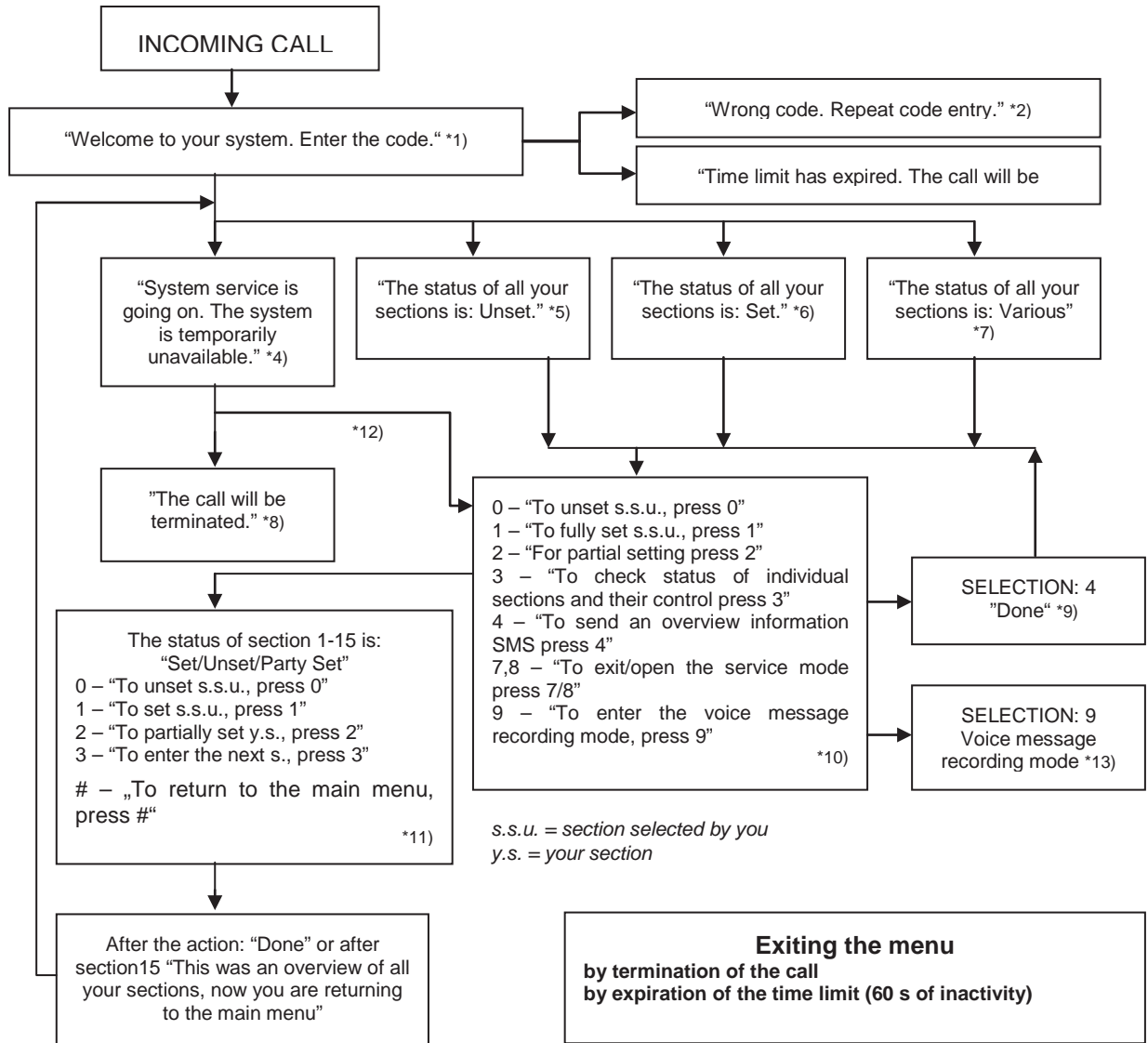
Every planned action can be blocked by one optional PG output. Blocking means: when a PG output is activated then a specific action won't be performed for a predefined time. This blocking can for example be a blocked calendar action for unsetting before you go for a holiday. Blocking can be indicated on a functional button on the keypad (pre-set to PG ON / OFF) named as "Holiday", etc.

## 9.5 System control via supplementary communicator voice menu (GSM / PSTN)

The security system can be controlled remotely via a supplementary communicator (GSM or PSTN) and DTMF tones on the caller's cell phone. By calling from a previously known SIM card telephone number or a land line telephone number the system picks up the call after a pre-set number of rings (default is 3 rings), the control panel plays an introduction voice message and according to the settings maybe require a valid code entry. The caller has to authorize himself by his access code. When the code is successfully verified then the system tells the status of the whole system and according to caller authorization offers available control options. By voice menu can be controlled sections, entering and leaving service mode and recording voice messages with the names of individual sections and special reports. Control of PG outputs is not possible via the voice menu.

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

## Voice menu overview:



- \*1) Answers after 3 ringing impulses. The number of ringing impulses until answering (1.10) is adjustable in the Communication tab and the tab of the respective communicator where entry in the voice menu without code can be allowed.
- \*2) Wrong code entry. After the third wrong entry the call will be terminated.
- \*3) 60s time limit for code entry. Every 5s the "Enter code" request is repeated.
- \*4) The voice menu cannot be used during service.
- \*5) All sections that can be controlled on the basis of the authorization are unset.
- \*6) All sections that can be controlled on the basis of the authorization are set.
- \*7) The sections that can be controlled on the basis of the authorization are in various statuses.
- \*8) Valid for all authorizations except ARC / Service.
- \*9) After sending of an INFO-SMS to the caller's number.
- \*10) Points in the menu that do not make sense are skipped (e.g. if everything is set, the selection 1,2,3 is not applicable).
- \*11) The menu is adapted to the current status of the section.
- \*12) If the user has been authorized with the service code, selection 9 is possible - "For the voice message recording mode press 9"
- \*13) Voice message recording mode **SELECTION 9:**  
 0 – "To record the installation name, press 0." and then "Press star (\*)"  
 1 – "To record section names, press 1", then enter the number of section that you want to record and then "Press star (\*)"  
 9 – "To delete all recorded messages, press 9."  
 # – „To return to the main menu, press #.“

### Notes:

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

## 9.6 SMS commands

The system can be controlled with SMS commands thanks to supplementary GSM communicator. SMS commands can be used to control the setting statuses of individual sections (setting, unsetting), or just a query about the statuses of individual sections or other statuses of the whole system. The texts of the command used to control PG outputs are editable, the other texts cannot be changed. There are no factory commands to control PG outputs, it is necessary to set them first. Other texts are already set.

### SMS Command structure:

#### **kkkk\_ command**

where: **kkkk** is a user code;

\_ is a separating space;

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

### Query commands:

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

**DINFO, STATUS, COM and GSM** (the texts of the commands cannot be changed).

### Control command:

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

**SET, UNSET, or SET x x x, UNSET x x x, where x are numbers of sections separated by a space** (the texts of the commands cannot be changed).

The control commands for the control of **PG** outputs are not pre-set by the manufacturer and if necessary, they must be set.

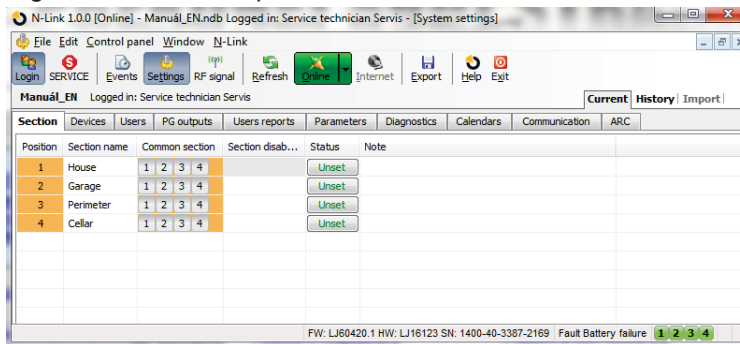
**Caution:** If control commands include accented diacritics (like with the languages GR and RU), then the Diacritics parameter on the Communication tab under the “JA-190Y” settings” button should be enabled for correct and reliable functioning. It is also necessary to mind small and capital letters when diacritics are enabled. With usual characters size doesn't matter.

Control command and authorization	Answer (specimen)	Note
<b>DINFO</b> (basic information about the installation)  <b>Authorization:</b> Service, Administrator	JABLOTRON 100: TYPE: JA-100K, SN: 14004026532523, SW: LJ60420, HW: LJ16123, RC: 79167-5FYA9-ZSQJ, GSM: 90%, GPRS:ok,  LAN: off Time 17:01 22.7.	Installation name according to the Communication tab Control panel type Serial number Firmware version Hardware version Registration code of GSM communicator GSM signal quality, GPRS data availability  LAN connection status (OK or OFF) Time and date of handing over the SMS to the GSM network
<b>STATUS</b> (status of sections)  <b>Authorization:</b> Service, Administrator, User. If the user only has access to some sections, the status of the sections that are accessible for him/her will be returned.	JABLOTRON 100: Status: Section 1: Unset; Section 2: Set; Section 3: Unset; Section 4: Set, Error;  GSM: 90%; Time 17:01 22.7.	Installation name according to the Communication 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  GSM signal quality Time and date of sending the SMS to the GSM network
<b>COM</b> (info about communication)  <b>Authorization:</b> Service	JABLOTRON 100: GSM: 90%,DATA: ok, CELLID: 44905, OPID: 23003, LAN: ok, MAC: hh:hh:hh:hh:hh:hh, PSTN: off, ARC: 1:ok, 2:ok, 3:off, 4:ok, 5:off, Time 17:01 22.7.	Installation name according to the Communication tab GSM signal quality, GPRS data availability Number of the cell and operator providing the GSM connection LAN connection status and MAC address Connection status of the phone line (possible with JA-190X) Activation status of transmissions to individual ARC's Time and date of handing over the SMS to the GSM network
<b>GSM</b> (restart GSM)  <b>Authorization:</b> Service, Administrator, User	JABLOTRON 100: SMS processed OK: GSM; Time 17:01 22.7.	Installation name according to the Communication tab Confirmation of SMS delivery (before restart) Time and date of handing over the SMS to the GSM network
<b>SET</b> (control of the whole system)  <b>Authorization:</b> All	JABLOTRON 100: Status: Section 1: Set; Section 2: Set; Section 3: Set with an active zone; Section 4: Set, Error;  GSM: 90%; Time 17:01 22.7.	Installation name according to the Communication 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  GSM signal quality Time and date of sending the SMS to the GSM network
<b>UNSET</b> (control of the whole system)	JABLOTRON 100: Status: Section 1: Unset; Section 2: Unset;	Installation name according to the Communication tab Status: Name and status of Section 1 Name and status of Section 2

<b>Authorization:</b> All	Section 3: Unset; Section 4: Unset, Error; GSM: 90%; Time 17:01 22.7.	Name and status of Section 3 Name and status of Section 4 GSM signal quality Time and date of sending the SMS to the GSM network
<b>SET 1 3</b> (control of selected system sections) <b>Authorization:</b> All	JABLOTRON 100: Status: Section 1: Set; Section 3: Set with an active zone; GSM: 90%; Time 17:01 22.7.	Installation name according to the Communication tab Status: Name and status of Section 1 Name and status of Section 3 GSM signal quality Time and date of sending the SMS to GSM
<b>UNSET 2 4</b> (control of selected system sections) <b>Authorization:</b> All	JABLOTRON 100: Status: Section 2: Unset; Section 4: Unset; GSM: 90%; Time 17:01 22.7.	Installation name according to the Communication tab Status: Name and status of Section 2 Name and status of Section 4 GSM signal quality Time and date of sending the SMS to GSM
<b>CREDIT</b> (checking the credit balance on the pre-paid SIM card) <b>Authorization:</b> All	JABLOTRON 100: ... ... ... Time 17:01 22.7.	Installation name according to the Communication tab Text from GSM provider response Text from GSM provider response Text from GSM provider response Time and date of sending the SMS to GSM

## 9.7 Controlling the system via F-Link

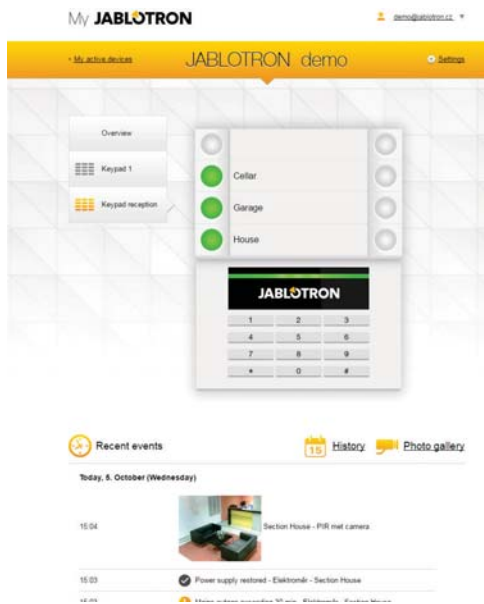
F-Link SW is used for local and remote programming of the whole system or user editing; provide an overview of section statuses and section control. Control is possible by clicking on the “Section” tab in the “status” column or also by clicking on the number of the section on the lower status bar. The system records system control to its event memory according to authorization upon user authorization in the software.



## 9.8 Control from the MyJABLOTRON web app

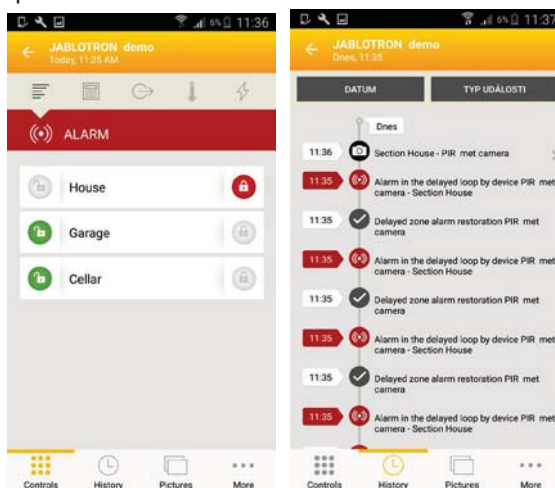
Remote control from the MyJABLOTRON web app is the most user-friendly way to control the security system from any internet browser regardless of computer platform. Once logged in, the app enables you to control the system not just from the virtual keypad of every physical keypad present in the system, but also enables you to control all sections and PG outputs from an overall list. The user can also browse through a detailed event history including taken photos. New photos can be taken immediately by a user's request. Unlike with the physical system, the user can see the current temperatures from thermometers, values from various meters and configure messages notifying you about system events or exceeded user-set values (such as temperature).

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



## 9.9 Control via the MyJABLOTRON mobile app

Users of MyJABLOTRON can download an application for smart devices. Available for iOS and Android. The mobile app is the most user-friendly way to control the security system which the user can even carry in a pocket thanks to almost unlimited internet access. After once secured logging in, the app enables you to control the system not just from the virtual keypad of every physical keypad present in the system, but also enables you to control all sections and PG outputs from an overall list.



## 9.10 Control by Duress access control

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

### **Example:**

User code = 4444. Duress access control code = 4445

**Warning:** If the user code ends with the number 9 when using Duress access control, then the last number of the code will be 0 (4449 – 4440).

## 9.11 Obstacles preventing setting the system

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

One of the most common obstacles is system fault (indicated by a yellow system indicator), a loss of connection with a wireless detector or a triggered status detector (typically a magnetic opening sensor) set with

a delayed zone reaction (front door and garage door sensors), low system battery, a long lasting power supply failure or a communication fault of one of the communicators. It is influenced by the system profile.

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

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

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

### Ways of setting - table overview

	System keypad	Via voice menu/SMS/remote controller/calendar	F-Link J-Link	Web and smart app
<b>Set always</b>	Will set always despite faults or triggered devices status	Will set always despite faults or triggered devices status	Will set always despite faults or triggered devices status	Will set always despite faults or triggered devices status
<b>Set with warning</b>	While attempting to set with a fault or a triggered device, the keypad flashes for 8 sec after which the system will automatically set. It's possible to set the system by pressing the functional button again or by pressing the Enter key.	Will set always despite faults or triggered devices status	Will set always despite faults or triggered devices status	Will set according to "Ways of setting" in the Service configuration tab
<b>Set after confirmation</b>	While attempting to set with a fault or a triggered device, the keypad flashes for 8 sec after which the system will automatically set. It's possible to set the system by pressing the functional button again or by pressing the Enter key.	Will set always despite faults or triggered devices status	Will set always despite faults or triggered devices status	Will set according to "Ways of setting" (with Set with check / set with no check) in the Service configuration tab
<b>Will not set with an active element</b>	While attempting to set with a fault or a triggered device, the keypad flashes for 8 sec after which the system will automatically set. It's possible to set the system by pressing the functional button again or by pressing the Enter key.	Will not set when a triggered detector is set to an INSTANT zone reaction	Will always set despite faults or a triggered devices status	Will not set when a triggered detector is set to an INSTANT zone reaction

## 9.12 Unsuccessful setting

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

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

In the case when setting the system is prevented, an "Unsuccessful setting" event is triggered and indicated by rapid flashing of the system indicator with a yellow colour on the keypads and also by their beeping, and acoustically by an outdoor siren as well. Simultaneously it is reported to a specific user or to the system administrator if the report "Unsuccessful setting is enabled, see F-Link SW, Communication tab.

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

## 9.13 Overview table of Groups of Events reported to users

When a supplementary GSM or PSTN communicator is connected, then system events can be sent not only to the ARC but also to up to 8 users (alarms, voice calls and SMS reports). Events which can be reported to the users are divided into 5 groups. Every group can be assigned to users arbitrary. Users to whom a group will be



assigned will be sent reports from this group. When the basic settings of the groups are not enough then there are 2 special user defined groups which can be used. Selected events can be added to those groups and based on that reported only to specific users.

**Overview table:**

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

The assignment of events distinguished by the system to groups is specified in the table. On occurrence of an event the system generates an SMS in the format:

**Installation name** (see the Communication setup tab):

**Time** (of event occurrence), **Event** (see table).

**Event source** (see the Devices/Name or User/Name tab), **Section** (where the event occurred);

**Time** (time and date of sending)

Example of a sent SMS:

<b>JABLOTRON 100</b>	(installation name)
<b>17:01:10, Delayed alarm</b>	(event time, event)
<b>Door magnet, Ground floor</b>	(detector name, section name)
<b>17:01:25, Instant alarm</b>	(event time, event)
<b>Staircase movement, Upstairs</b>	(detector name, section name)
<b>Time 17:01 22.7.</b>	(time of sending)

## 9.14 System acoustic indication

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

### Acoustic indication by keypad / reader:

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

### Acoustic indication by indoor / outdoor sirens:

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

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

Sound	Action description
Permanent rapid beeping	Fire alarm
Permanent whooping	

## 9.15 Disabling and blocking options

### 9.15.1 Disabling

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

- Blocking of input (BLK)** – the function is for blocking a detector input (it blocks its activation). The system ignores any detector activation = an alarm is not triggered, nor reports PG activation. Tamper alarms, faults or low battery reports are supervised all the time. In the F-Link software it is indicated by a yellow dot. Authorization for blocking to be performed belong to the Administrator and Service technician.

- 2. Device disabling (DIS)** – this function is for disabling a detector. The system ignores all device functions = it doesn't trigger any alarms nor tamper alarms, reports or faults. In the F-Link software it is indicated by red dot. Authorization for disabling is done by the Service technician only.

Not only a device but also a section can be **Disabled** but only one without the control panel, also applies to users except position 0 (service technician) and 1 (Administrator), PG outputs or calendar actions. Disabling is permanent until it cancelled by the same procedure as its activation.

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

## 9.16 Non-alarm functions – Functions of PG outputs

The security system allows authorized users (according to the settings) to control the system functions – not just functions related to guarding the sections but also controlling PG programmable outputs (switching ON / OFF). Using relay modules or a module with special semiconductor outputs they can switch on devices such as indicators, traffic lights, acoustic indicators, or other appliances related to the security system like lights, systems for access control, blocking the heating when a window is open or when a section is set, garden watering, etc., i.e. home automation.

Function of PG output	Description	Example
ON / OFF	Bi-stabile output status, can be changed by arbitrary command or device	Manually switching ON appliances using a functional button, SMS or also by some device with an option of manually switching off with no limitation. Typically heating control, air conditioning, lights
Impulse	Mono-stabile output status with pre-set time	Impulse switching of other additional control circuits such as gate control, rollers, jalousies, garden watering, door locks, etc.
Copy	Output status with OR logic. Output will be active if minimum one device at least will also be active, but deactivation occurs when all control devices will be inactive.	Useful for indication of some single or collective statuses (typically of open windows, garage doors, etc.) on the keypad functional button. In similar ways statuses of all sections, alarms, alarm memories, faults and many other events can also be indicated where the beginning and the end are given.

The system also offers user functions such as measuring the temperature, which can be shown on the LCD keypad and in the MyJABLOTRON application.

## 10 Setting the system through F-Link SW

The JABLOTRON 100 system is exclusively programmed using a computer, through F-Link software. F-Link current version of the software you can get from your distributor or supplier or after authorization it can be downloaded from [www.myjablotron.com](http://www.myjablotron.com).

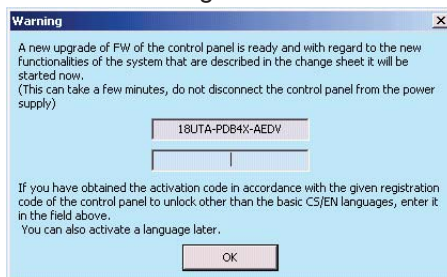
Immediately after opening the initial window for connection selection, the F-Link software can be switched over to the desired language environment by clicking on a language icon (flags). Language can be changed at any time later in F-Link menu. The initial window offers the following options:

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

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

1. Connect a computer to the control panel using a USB cable – the computer will initialize the new USB device (it may take a longer time if the control panel is being connected for the first time).
2. After the connection your computer will display two newly found drives: FLEXI\_CFG and FLEXI\_LOG. If displayed, in a new window you can simply close them.

- Start the F-Link software. If the control panel has default settings, the Settings window will open and the system will automatically get into the Service mode. If the control panel has been configured before (its service code has been changed), the software will request entry of the code – it should be entered in the format **nnnn** (the default setting of the service code is 1010). You can use the **Remember** option to make the software save the code until closing of the database. Use the **Display Code** option to check the entered code e.g. if you use an alphanumeric keyboard where a mistake can be made.
- After a valid authorization it could shows this message:



In such a case we recommend upgrade to be performed. By clicking to OK button it downloads new firmware package, it can take a few minutes. When upgrade process is finished wizard pop ups the Initial setup tab.

Note: After establishing connection using the USB cable the possibility of programming changes of settings from the LCD keypad will be disabled (menu item Settings will be disabled). After disconnection of the cable the item will re-appear in the menu in a few seconds.

## 10.2 Sections tab

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

Position	Section name	Common section	Section disabled	Status	Note
1	House	1 2 3 4		Service mode	
2	Garage	1 2 3 4		Service mode	
3	Garden	1 2 3 4		Service mode	
4	Shop	1 2 3 4		Service mode	

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

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

**Section disabled** – disabling possibility to set section, (blocking a section means that all devices assigned to the section are collectively disabled), indicated by a red dot. The section to which the control panel is assigned to cannot be blocked. A section may only be blocked by a service technician (through F-Link).

*Warning: When section where the radio module has been assigned is blocked then this radio module stops receiving signals from all sections. That's why we recommend to assign it to section 1 where the control panel is assigned as well. When section which is part of Common functional button is blocked it is indicated by yellow colour (it cannot shows if all its sections are fully set or unset).*

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

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

## 10.3 Devices tab

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

Position	Name	Type	Section	Reaction	Internal	Internal settings	Disable	Status	Note
0	Control panel	JA-100K	1: House			Enter		Error	
1	Device 1	JA-111R	1: House			Enter		OK	
2	Device 2	JA-110E	1: House	None	<input type="checkbox"/>	Enter		??	
3	Device 3	JA-110A	1: House	None	<input type="checkbox"/>	Enter		??	
4	Device 4	Enroll	1: House	-	<input type="checkbox"/>				
5	Device 5	Enroll	1: House	-	<input type="checkbox"/>				
6	Device 6	Enroll	1: House	-	<input type="checkbox"/>				
7	Device 7	Enroll	1: House	-	<input type="checkbox"/>				
8	Device 8	Enroll	1: House	-	<input type="checkbox"/>				
9	Device 9	Enroll	1: House	-	<input type="checkbox"/>				
10	Device 10	Enroll	1: House	-	<input type="checkbox"/>				
11	Device 11	Enroll	1: House	-	<input type="checkbox"/>				
12	Device 12	Enroll	1: House	-	<input type="checkbox"/>				
13	Device 13	Enroll	1: House	-	<input type="checkbox"/>				
14	Device 14	Enroll	1: House	-	<input type="checkbox"/>				
15	Device 15	Enroll	1: House	-	<input type="checkbox"/>				
16	Device 16	Enroll	1: House	-	<input type="checkbox"/>				

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

**Type** – displays the type of the assigned device. An empty position allows you to enroll a new device.

**Enrolling devices**, see chapter 8.4.1 Enrolling and erasing devices.

**Section** – determines to which monitoring section the device will report events (alarm, tampering, fault ...).  
Note: division of a building into sections - see chapter 10.2 Sections tab.

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

**Internal** – this parameter is only available for intrusion detectors. Signals from devices with this indication are not evaluated as alarm signals if a section is partially set. Partial setting of a section - see chapter 10.2 Sections tab.

**Internal settings** – access to settings of internal parameters of perimeters that are connected to the BUS or feature bidirectional wireless communication. Individual devices have different internal parameters (some have none). The internal settings of a keypad are described in chapter 10.3.1 Keypad configuration. Settings of other devices are described in their manuals.

**Disable** – can be performed at 2 levels given by your authorization:

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

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

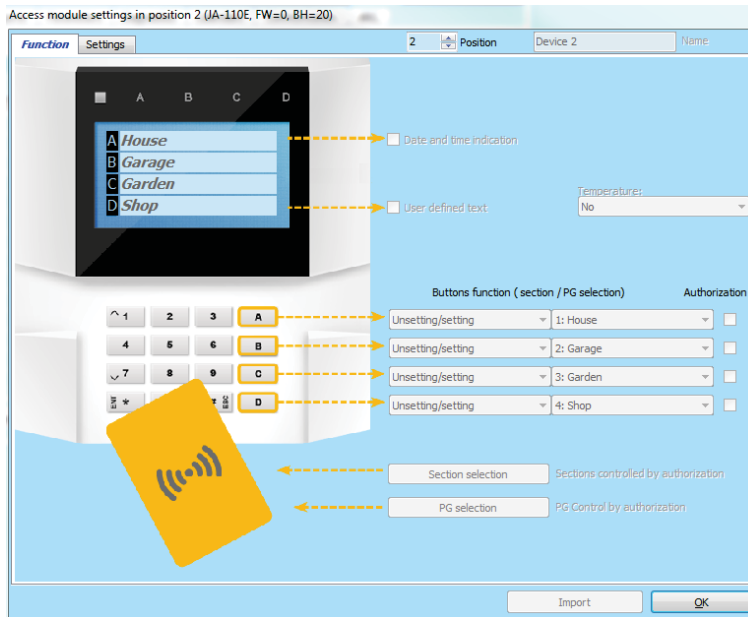
**Status** – indicates the current status of the device. OK = everything all right, TMP = tampering, ACT = alarm input activated, BLK = blocked, Disabled = Disabled, ERR = error, ?? = no communication with the device, Mains supply = supply failure, Battery = discharged or disconnected battery in the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

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

### 10.3.1 Keypad configuration

On entering the internal settings of the keypad (the Devices tab) the following window will open (the example refers to the JA-110E keypad).

**Function tab:**



**Date and time** – Allows showing the current system time in the keypad’s right upper corner

**User text** – allows showing arbitrary text on the LCD keypad (telephone no. of installer, etc ...). Activation of such an option disables the functional button “D”.

**Temperature** – Allows showing the measured temperature of a selected detector in the lower keypad corner

**Functional buttons** – on the left side select the buttons function, on the right side the section or PG output to which the function is assigned. The following can be assigned to the functional button: None, Unset/Set, Unset/Partially set, Unset/partially set/Set, Section indication, Silent panic, Fire, Audible panic, Health troubles, PG OFF/ON, PG ON, PG OFF, PG indication, PG indicates inversely, Common functional button.

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

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

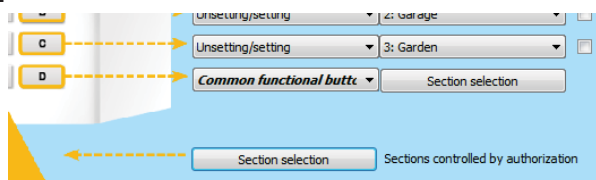
**Section selection** – pre-set sections to be controlled by authorization only (RFID card/tag or code).

**PG control** – select PG outputs for control by authorization only (RFID card/tag or code)

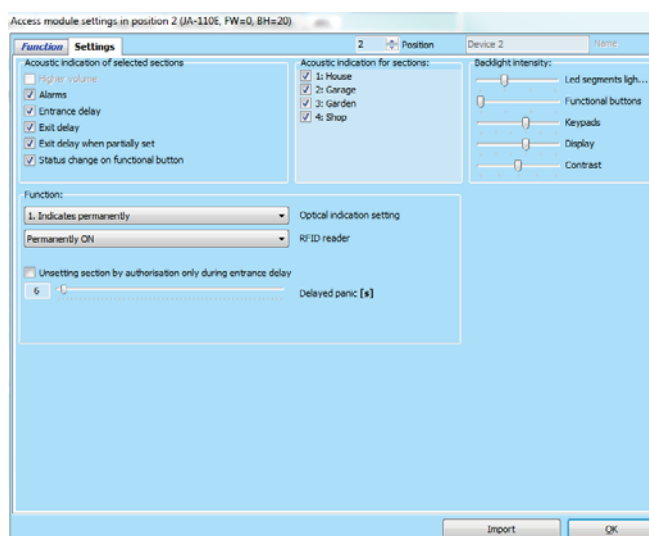
<b>None</b>	Functional button has no function; disabled
<b>Unset / Set</b>	Section control. Functional button indication: section unset = green, set = red
<b>Unset / Partially set</b>	Enables activation of partial setting mode of the section (if enabled in the Sections tab). Functional button indication: section unset = green, partially set = yellow
<b>Unset / Partially set / Set</b>	Allows you to select the setting level. After pressing the functional button (Set) partial setting is offered, after repeated pressing system is completely set. When the system is fully set by pressing the functional button is fully unset. Button indication: section unset = green, partly set = yellow, fully set = red.
<b>Indicates section</b>	The functional button only shows the status of the section, but does not enable its control (suitable e.g. for indication of the status of common sections, staircase etc.) If an alarm is released, it allows you to cancel it by pressing the green button of the functional button with subsequent valid authorization of the user.
<b>Panic (silent)</b>	The functional button activates a silent Panic alarm. After pressing the button a Panic report is sent from the section the function button is assigned to, without acoustic indication. The Panic alarm may also be Delayed with adjustable time and possibility of cancellation before expiration of the pre-set time (see Delayed Panic). If the section is set, it will not be unset.

<b>Fire</b>	The functional button triggers the fire alarm. Then, a fire alarm is activated from the section the functional button is assigned to.
<b>Audible Panic</b>	The functional button activates a loud panic alarm. After pressing, a loud Panic alarm is activated from the section the functional button is assigned to. The loud Panic alarm may be Delayed with adjustable time and possibility of cancellation before expiration of the set time (see Delayed Panic). If the section is set, it will not be unset.
<b>Medical troubles</b>	The functional button allows to send a health problem report (without activating a siren) from the section the functional button is assigned to.
<b>Disable PG / Enable PG</b>	The functional button allows to control a PG output. Indication: PG inactive = green, PG active/enabled = red
<b>Enable PG</b>	The functional button can only be used to enable the PG output (e.g. switch on the lights for a pre-set time)
<b>Disable PG</b>	The functional button can only be used to disable the PG output (e.g. function of an emergency STOP button)
<b>Indicates PG</b>	The functional button only indicates the status of the PG output without the possibility to control it (red indicates the active status)
<b>Indicates PG inversely</b>	The functional button only indicates the status of the PG output with the inversed logic (green indicates the active status) without the possibility to control it
<b>Common functional button</b>	<p>Enables simultaneous control of several sections using the functional button on the keypad. After pressing the common functional button, the Unset/Set command is executed collectively for the pre-selected section buttons. If some sections controlled by the Common button are set and the others unset, after using the Common functional button the remaining buttons will be Unset with a short press/Set completely with a long press. If Partial Setting is enabled for one of the selected functional buttons (details see 9.2 System control by keypad), the Common button will behave as follows: 1st press of Set = partial setting, 2nd press of Set = full setting. It is not suitable to combine the Common functional button with the Sections/Common section.</p> <p>Common button indication: all sections unset = green, all sections fully set = red, any section set (party set) = yellow.</p> <p>Sections are assigned to the Common functional button in the other window when the option is selected.</p>

**Common functional button:**



**Settings tab:**



**Acoustic indication of selected sections:**

Higher volume	Setting of indication volume except for an alarm
Alarms	acoustic output in case of an alarm (siren sound)
Entrance delay	continuous whistling tone during an entry delay
Exit delay	slow intermittent beeps (1/s)
Exit delay when partly set	slow intermittent beeps (off by default)
Functional button status change	acoustic indication with one beep at a change

**Functions:**

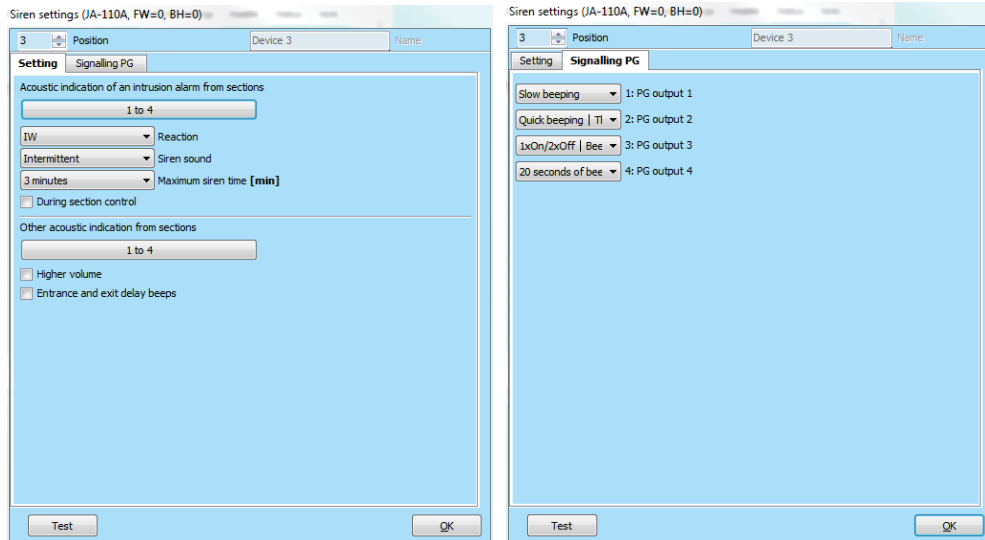
RFID reader	To save energy, the activity of the reader can only be limited to 3 s from pressing of its cover. The RFID reader can also be completely disabled. This setting applies to wireless keypads when they are permanently supplied with power from an external source, otherwise their RFID reader is always switched off automatically.	
	Permanently on	The RFID reader is permanently enabled. In the case of a BUS keypad it does not respect the wake-up setting.
	Enabled by pressing	Waking up the RFID reader for 3 s after activation on the keypad.
	Off	The RFID reader is permanently disabled.
	By pressing or authorization requirement	Wakes the RFID reader up after keypad activation or authorization requirement.
Optical indication settings	1. Indicates permanently	A BUS keypad indicates permanently. A wireless keypad will only indicate permanently with external power supply. Without external power supply it behaves like in option 2.
	2. After a section status change on the keypad	The keypad indicates a change of the status of a section / PG. A status change is only indicated on the concerned functional button. An entry delay and alarm are indicated by the whole keypad.
	3. After a section status change - indicator	A status change of a section / PG is only indicated on the concerned functional button.
	4. Status indicator change on keypad	Entrance delays and alarms are just indicated acoustically. A status change is only indicated on the concerned functional button. This option is the default setting.
	5. After an entry and alarm	The keypad indicates an entrance delay and alarm on the concerned functional button. A change of the PG output status and section status are not indicated at all.
	6. Wake-up by pressing	The keypad only provides optical and acoustic indications after opening of the front cover; pressing of a key, functional button or front cover
Unsetting section by authorization only during entrance delay	If enabled, then a section where the entrance delay has started is unset by a user valid RFID card/tag or code authorisation only. With wireless keypads authorization can be performed after the entrance delay is triggered. CAUTION: We strictly recommend you to disable this function when the entrance delay usually runs for a common section, otherwise all sections assigned to the common section will be unset for a given authorisation.	
Wake the keypad up by applying an RFID card	When an RFID card is applied, the keypad wakes up. We do not recommend enabling this function if there are a lot of obstacles such as metal objects and electric wiring surrounding the keypad. If you decide to enable it, then make sure the keypad will not be woken up coincidentally and it prevents a reduced battery lifetime	
Delayed panic	The function serves to postpone triggering of a silent or audible panic by a pre-set time. It is possible to determine the time interval when you can cancel the activation by repeated pressing of the same functional button with a pre-set to silent or audible panic. When authorization is enabled then it is required for activation and deactivation as well. The delay is adjustable from 1 sec to 255 sec.	



**Backlight intensity:**

Indicators	Adjustment of the indicators illumination
Functional buttons	Adjustment of functional buttons
Keypad	Adjustment of the keypad backlighting
Display	Setting of the LCD display backlighting
Contrast	Setting the LCD display contrast

**10.3.2 Internal siren settings:**



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

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

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

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

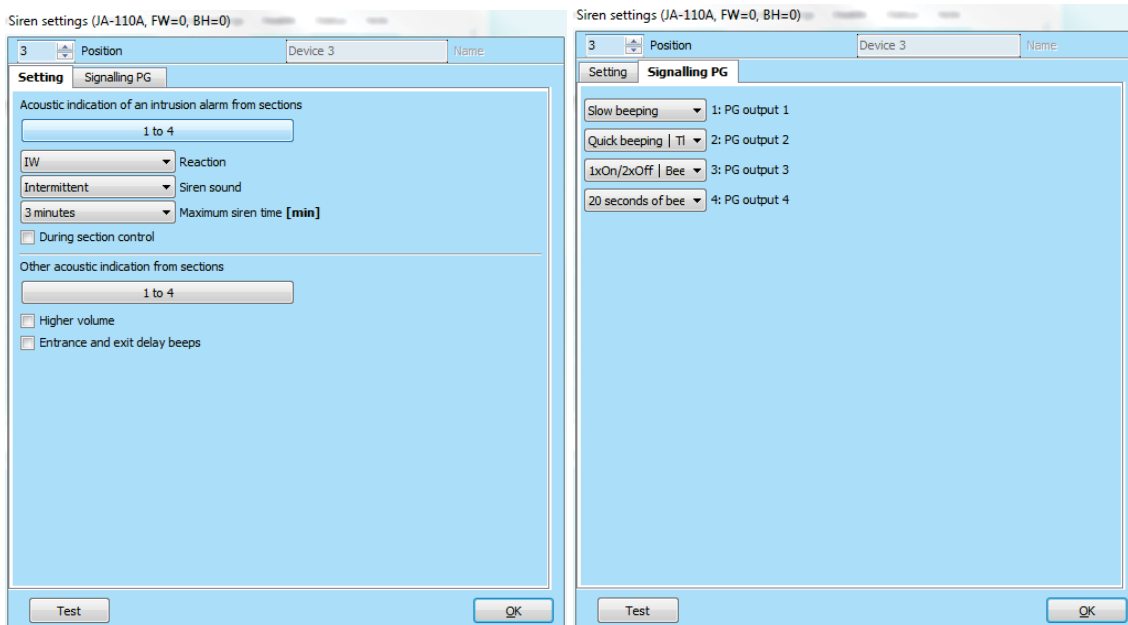
**During section control** – acoustic confirmation of section status changes (beeps 1x – set / 2x unset)

**Other acoustic indication from sections** – selection of the sections for other acoustic indications (entrance/exit delay)

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

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

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



## 10.4 Users tab

It is used to establish new system users and their rights. To make changes in this tab you do not need to be in Service mode.

Position	Name	Telephone number	Code	Card	Authorization	Section	PG	Dialling in activates PG	User blocking	Note
0	Service		****	No	Service	1 2 3 4	1 2 3 4			
1	Master		****	No	Administrator	1 2 3 4	1 2 3 4			
2	User 2			No		1 2 3 4	1 2 3 4			
3	User 3			No		1 2 3 4	1 2 3 4			
4	User 4			No		1 2 3 4	1 2 3 4			
5	User 5			No		1 2 3 4	1 2 3 4			
6	User 6			No		1 2 3 4	1 2 3 4			
7	User 7			No		1 2 3 4	1 2 3 4			
8	User 8			No		1 2 3 4	1 2 3 4			
9	User 9			No		1 2 3 4	1 2 3 4			
10	User 10			No		1 2 3 4	1 2 3 4			
11	User 11			No		1 2 3 4	1 2 3 4			
12	User 12			No		1 2 3 4	1 2 3 4			
13	User 13			No		1 2 3 4	1 2 3 4			
14	User 14			No		1 2 3 4	1 2 3 4			
15	User 15			No		1 2 3 4	1 2 3 4			
16	User 16			No		1 2 3 4	1 2 3 4			

**Name** – names of users are used in textual event reports in the readouts of the event history, in tabs for reports, authorization settings or for authorization on a keypad or in SMS reports sent by supplementary GSM communicator.

**Telephone number** – used for reporting events when supplementary communicators are connected and for identification of users when the system is controlled by phone using a voice menu or for activation of PG outputs by ringing and SMS. The phone number must always be entered in the international format (e.g. +420710123456).

**Code** – the user access code is entered in the format **nnnn** (4 or 6 digits according to the system profile). The code on positions 0 and 1 cannot be deleted (Service and Main Administrator).

**Card** – used to assign RFID access cards (tags). Each user can have one RFID card. Cards/tags can be assigned:

- by entering the serial number (it can be read with a barcode reader from the RFID card/tag)
- using the JA-190T USB reader for a PC **and applying and** RFID card/tag
- using any keypad and applying an RFID card/tag

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

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

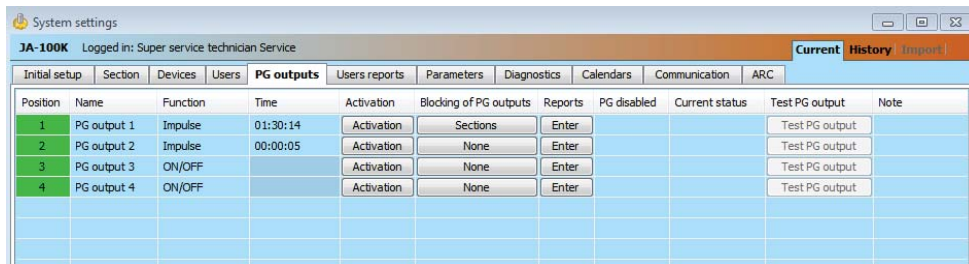
**PG** – defines which PG outputs the user is authorized to control (if authorization is required for the output control).

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

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

## 10.5 PG outputs tab

It is used to set functions and links of the programmable outputs. To make changes in this tab you do not need to be in the Service mode.



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

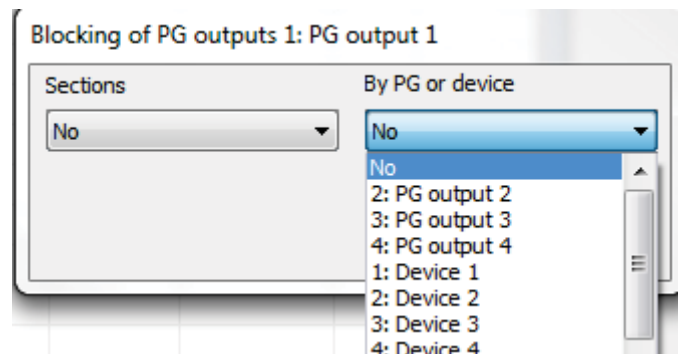
**Function** – determines behaviour of the output after activation.

<b>Impulse</b>	enables activation with a time limitation (the time is set in the Time button).
<b>ON/OFF</b>	the enabling command will cause activation, disabling command deactivation while the status of the source or duration is not checked, the last command always performs its request
<b>Copy</b>	copies activation of a detector or internal status; if there is a request from two devices, the OR logic is used

**Time** – setting of time for the Impulse function. Time is set in the format *hh:mm:ss* in the range of 00:00:01 to 23:59:59.

**Activation** – Opening the Activation Map of the PG output – see chapter 10.5.1 Activation Map of a PG outputs.

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



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

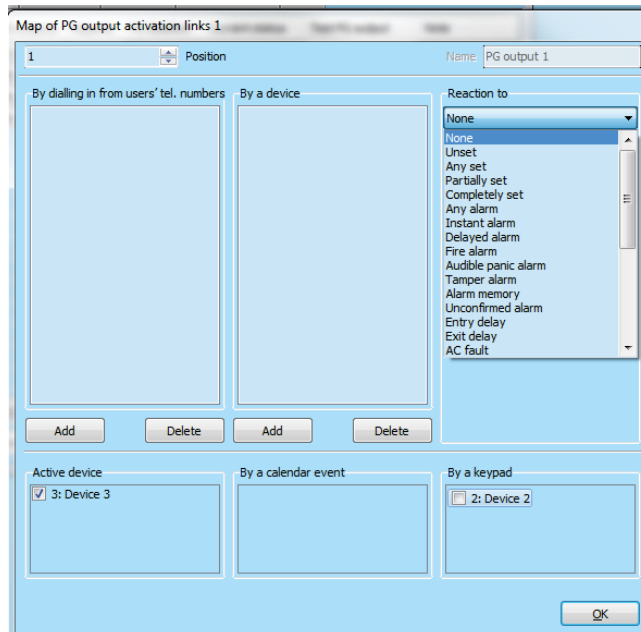
**Current status** – color-coded information about the current status of a PG output. Green description corresponds to the green light of the functional button; red description corresponds to the red light of the button.

**Test** – possibility to control an output manually from the computer using F-Link SW. Depending on the selected function it will enable (or disable) the particular PG, if it’s not currently blocked.

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

## 10.5.1 Activation Map of a PG outputs

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



**By dialling in from user's tel. numbers** – defining users that are authorized to activate a PG output by calling from their phone when a supplementary GSM or PSTN communicator is connected. Phone numbers used for the ringing activation must not be hidden (the CLIP service must not be deactivated for them). The term “ringing” means that after dialling the phone number the caller waits for at least one ringing tone and before the control panel would answer the call (see the number of ringing tones of incoming calls in the communicator settings) terminate the call. The PG output switches on when call hangs up. If the call is answered by the control panel, the output will not be activated.

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

**Reaction to** – enables activation of an output by a selected event in the system (e.g. setting, alarm, power supply failure, error etc.). For an internal status (29 internal statuses altogether, see the following table) you can set the group of sections the signal will be accepted from (the OR logic). The concerned PG output may be set to copy the status of another PG output or several other outputs where the mutual logic is selectable (OR or AND). The last item in the menu allows you to set activation of an output and its deactivation in response to a completely different event (e.g. activation in case of an alarm, but deactivation by unsetting only).

**Activated by device** – a list of devices that activate the concerned PG output with their activation, for instance a photo from a PIR with a camera (the function can be set in the device's internal settings) or acoustic indication by sirens, etc.

**By a calendar event** – list of scheduled events that activate or deactivate or block the concerned PG output (information window)

**By a keypad (functional button)** – Shows the list of keypads and remote controllers in system with ability to control specific PG output.

**By SMS commands** – when supplementary GSM communicator is connected then it allows you to set text commands to activate and deactivate a PG output by phone. To control outputs use SMS in the format **code\_command**, e.g. **2345\_enable\_light** (note: the \_ character is a blank space). The code before the command is not obligatory if in the **Communication** tab the “Voice menu and control SMS without a code” item is enabled and the phone number of a user authorized to control the corresponding PG output is identified.

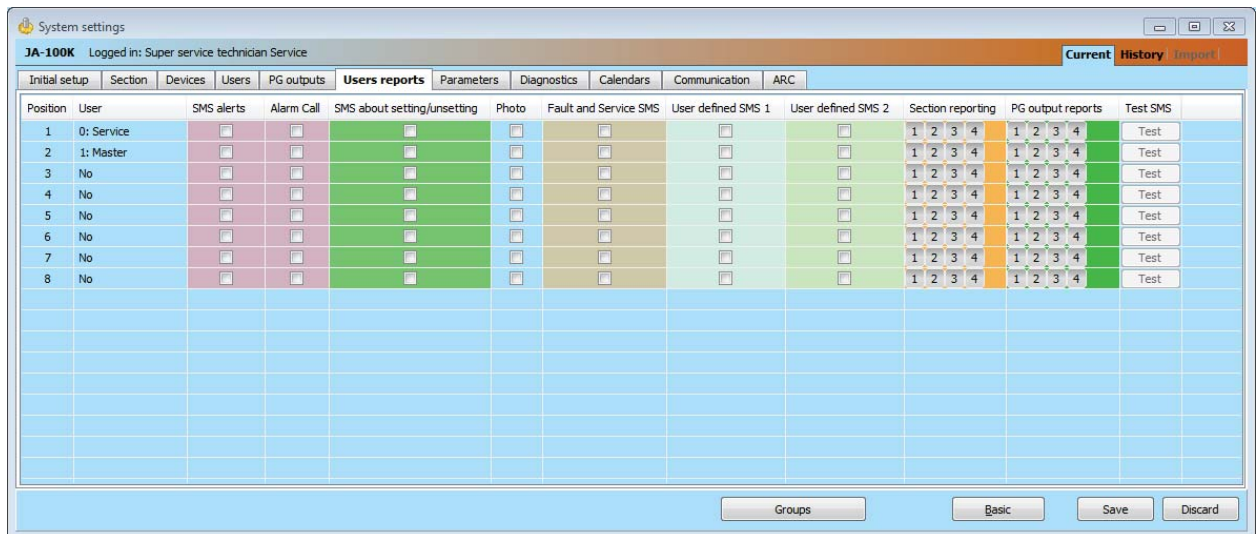
**Warning:** The PG outputs are not functional if the system is in the Service mode. By pressing the Test button all PG outputs can be tested (by F-Link SW). On activation of the Service mode all the PG outputs get disabled. After exiting of the Service mode from F-Link their re-activation is offered.

**Internal statuses for control of PG outputs:**

1. Unset	11. Alarm memory	21. Triggered detector
2. Any set	12. Unconfirmed alarm	22. Device with a low battery
3. Partially set	13. Entry delay	23. Device with tamper activated
4. Completely set	14. Exit delay	24. No movement in section
5. Any alarm	15. AC fault	25. Annual check request
6. Instant alarm	16. AC fault for 30 minutes	26. GSM fault
7. Delayed alarm	17. Backup battery fault	27. LAN fault
8. Fire alarm	18. Internal warning (IW)	28. PSTN fault
9. Audible panic alarm	19. External warning (EW)	29. Event in system
10. Tamper alarm	20. Fault	

**10.6 Reports to users tab**

This tab is available when a supplementary GSM or PSTN communicator is connected and is used to define users the system will report to about selected groups of events in the form of SMSes or voice calls to their phones. The groups and the SMS format are described in the attached table. The basic structure of the voice menu is described in the attached table 9.5. To make changes in this tab you do not need to be in the Service mode.



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

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

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

**Caution:** reporting of one voice event is limited to a maximum of 5 users.

**SMS about setting / unsetting** – group of reports for which a text message about setting and unsetting is sent. A setting report is sent with the fixed **delay of 60 seconds** after setting. Setting and unsetting

is not reported to the user who has performed it. An exception is setting of a common section (done by the control panel, not user).

**Photo** – sends the user an SMS saying that an alarm photo has been taken if photo-verification devices are installed. More details - see manuals of the respective camera detectors.

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

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

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

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

**PG output reports\*** – possibility to report switching ON / OFF of PG outputs to a user. The messages are sent with a fixed delay of 60 s. The texts of the SMS messages are set in the PG Outputs tab, see chapter 10.5 PG outputs tab.

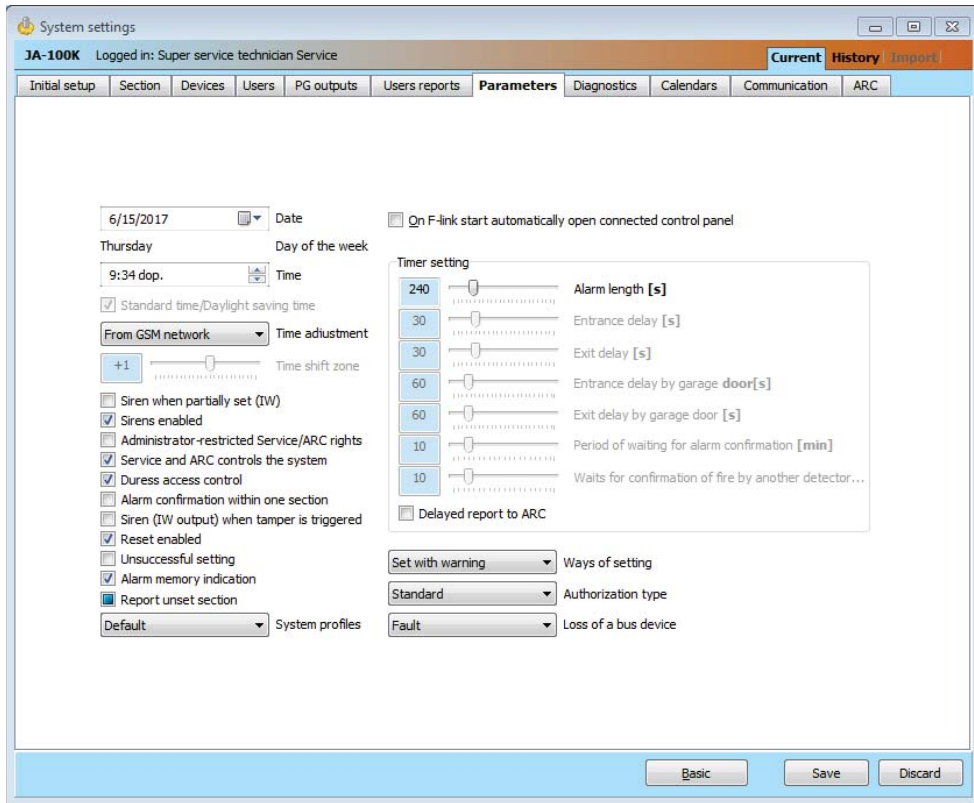
**Test** – by pressing of this button the test SMS report will be sent to the user: „Test report, Control Panel, Section 1“

**Table of events and pre-set groups:**

Event	Alarm	Setting/Unsetting	Failures and service	User defined SMS 1	User defined SMS 2
AC fault 30 minutes	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AC fault after 30 min restored	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant alarm cancelled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delayed alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delayed alarm cancelled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tamper alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tamper alarm cancelled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fire alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fire alarm cancelled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gas leak alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Panic alarm	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Panic alarm cancelled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health troubles	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Flooding	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Code breaking attempt	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Set with active device	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No movement in the section	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Overheating activation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Overheating deactivation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Freezing activation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Freezing deactivation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Set	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unset	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Partially set	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System BOOT	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device low battery	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device low battery restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fault	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fault restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enter service mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Leave service mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Backup battery LOW	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Backup battery restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ARC communication fault	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ARC communication fault restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RF jamming	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RF jamming ended	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Low credit balance	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 10.7 Parameters tab

It is used to set parameters and selectable functions of the control panel. To make changes in this tab you do not need to be in the Service mode.



<b>Date</b>	Internal calendar setting.	
<b>Day of the week</b>	Displaying the day of the week	
<b>Time</b>	Internal clock setting.	
<b>Standard time / Daylight saving time*</b>	Automatic switching of the winter and summer time can only be selected for manual time adjustment. The change occurs on the last Sunday of March or October, respectively at 1:00 UTC (i.e. e.g. 2:00 CET, or 3:00 CEST).	
<b>Time adjustment*</b>	Internal time and date adjustment method:	
	Manually	Manual setting of the time and data using F-Link
	From the GSM network	Time and date are taken from the GSM provider with every logging in to the GSM network
	From the Jablotron server (LAN / GSM)	Time and date are adjusted automatically according to communication server. Option does nothing when the type of communication is set to "Without remote programming" (factory default setting)
<b>Siren IW when partially set</b>	Allows you to set an acoustic alarm with the IW system if the section is partially set. Fire and 24 hours reactions never activate a siren in the case of an alarm, regardless of how is this parameter set.	
<b>Sirens enabled*</b>	Enables all BUS and wireless sirens of the system (designed for disabling the acoustic alarm during system testing).	
<b>Administrator restricted Service and ARC</b>	It blocks independent access of service technicians and ARC to the system. Note: In case of remote access of a technician to the system via F-Link the administrator may get authorized using a keypad in the building. In the case of a local connection of a technician to the control panel using a USB cable and a supplementary GSM / PSTN communicator being connected the administrator may get authorized remotely using the voice menu.	



<b>Service and ARC control system*</b>	This setting allows the service technician and ARC technician to control the system for all the sections. If this parameter is disabled, the technician is not authorized to control sections and will only be able to enter the Service mode after unsetting of all the sections by the Administrator or a user.	
<b>Duress access control</b>	Serves for triggering of a silent alarm by authorization only or by system control (setting, unsetting, PG control, ...) when a user is in the presence of a criminal. A Panic alarm is triggered during system control when a code is entered with 1 mathematically added to the last digit's value. Example: a user code 4444, for duress access control enter 4445. Caution: when the user code's last digit is 9 then for duress access control use 0 as a last digit. Example: A user code = 4449, for duress access control enter 4440 (only enter 0 on the end). Caution: enabling this function erase all predefined codes in the system!!!	
<b>Alarm confirmation within one section*</b>	If confirmation reaction by another detector is set for a detector, this confirmation option can be used to limit confirmation <b>to the same</b> section only (otherwise a detector from any section can confirm an alarm). This is valid equally for intrusion detectors and for fire detectors.	
<b>Siren (IW output) when tamper is triggered*</b>	A siren with the IW response acoustically indicates a tamper alarm if the zone is unset or partially set	
<b>Reset enabled*</b>	Possibility to lock reset of the control panel with a jumper on the board. If reset is prohibited and the service code is lost, the control panel can only be unlocked by the manufacturer. Reset of the control panel is described in chapter 12 Reset of the control panel.	
<b>Unsuccessful setting</b>	The function is processed during every setting procedure. If an instant zone is triggered within the exit time or a delayed zone stays open when the exit time expires, the system is not set and triggers an "Unsuccessful setting" event and records it in the history. It is recorded in the system history and also reported by a supplementary GSM or PSTN module if connected by SMS to a pre-set user if the event "SMS about unsuccessful setting" is enabled to be sent. It is indicated by keypads and also by an outdoor siren. To cancel the indication about unsuccessful setting it is necessary to press "Cancel warning indication" in the keypad menu.	
<b>Alarm memory indication</b>	The option allows alarm memory indication by an LED built into the detector which triggered the alarm. Available for supported devices only.	
<b>System profiles</b>	Selection from pre-set system profiles according to requirements.	
	Default	Parameters set by factory default with the option to modify them according to needs
	EN50131-1, Grade 2	Some parameters are pre-set automatically to comply with EN50131-1, grade 2 with no option to be modified
	INCERT, Grade 2	Some parameters are pre-set automatically to comply with INCERT, grade 2 with no option to be modified
<b>Ways of setting</b>	Selection of the way how the system manages the setting process. From the lowest level when the system can be set regardless of active devices and faults in system to the highest level when the system cannot be set at all with active devices (instant zone). This setting is also linked to the system profile.	
	Set always	Set always regardless of the system status (faults, active devices,..)
	Set with warning	Optically indicates (on the functional button and display) the system status (faults, active elements, low battery or backup battery) for 8 seconds and sets automatically once this period expires. Setting is also possible by repeatedly pressing the functional button (or by pressing the ENTER key).
	Set after confirmation	Optically indicates (functional button and display) the system status (faults, active elements, low battery or backup battery) for 8 seconds. Can be set <b>ONLY</b> by repeatedly pressing the functional button (or by pressing the ENTER key).

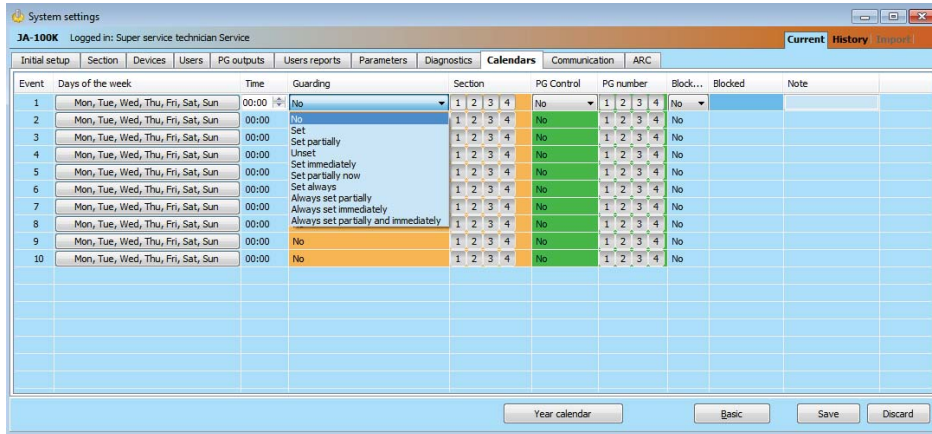


	Don't set with an active element	Optically indicates (functional button and display) the system status (faults, active device, low battery or backup battery) for 8 seconds. System can be set by repeatedly pressing the functional button (or by pressing the ENTER key) but only if the active detector is of the DELAYED or NEXT DELAYED reaction type. An active element with any other alarm reaction CANNOT be set this way. ATTENTION!!! this also applies to remote control (Voice menu, SMS, web or smart application, action through calendar).
<b>Authorization type</b>	Selection of the way the system processes user authorization. Related also to controlling a PG output with authorization.	
	Standard	Entering a user code, using an RFID card or a tag will accomplish valid authorization. Just one of these options is necessary to control the system.
	Double authorization	Entering a user code and using an RFID card will accomplish valid authorization (regardless of the order of authorization). F-Link monitors whether a code and a card are assigned to a user in the Users tab (otherwise F-Link won't allow you to save the configuration). Remote phone access is enabled for authorized numbers only.
<b>Loss of a BUS device</b>	The control panel processes the loss of a device or a short circuit on the system BUS. According to the selected option system will react to occurred situation:	
	Fault	The control panel always processes the loss of a device on the BUS or a short circuit of the BUS just as a Fault.
	Tamper always	The control panel processes the loss of a device on the BUS or a short circuit of the BUS as a tamper alarm always when it occurs. If the radio module has RF jamming detection allowed and the jamming is detected then it also triggers a tamper alarm. A tamper alarm is also followed by a fault and when the fault disappears, it cancels the tamper alarm as well.
	Tamper after confirmation	The control panel processes the loss of a first device as a fault and if within a pre-set time given by the parameter "Period of waiting for alarm confirmation" another device loss occurs, then the system confirms it and triggers a tamper alarm. When the faults of all the lost devices are restored then the system cancels the fault and tamper alarm.
<b>Timer setting</b>	In each section, the entry and exit delays are measured separately. If different exit delays are defined for detectors within one section the longest delay is provided. In case of different entry delays the one that belongs to the activated detector is measured. If more detectors are activated, the shortest one of the defined entry delays is provided.	
<b>Alarm length</b>	Alarm length – valid for all sections. Range 5 sec. – 20 min.	
<b>Entrance delay</b>	Timer. Range 5 sec. – 2 min.	
<b>Exit delay</b>	Timer. Range 5 sec. – 2 min.	
<b>Garage door entrance delay</b>	Timer. Range 5 sec. – 6 min.	
<b>Garage door exit delay</b>	Timer. Range 5 sec. – 6 min.	
<b>Waits for confirmation of intrusion by another detector</b>	Waiting time for alarm confirmation by another detector of a set section. Valid for all detectors with the reaction Confirmed immediate / Confirmed delayed (1 – 60 min.)	

<b>Waits for confirmation of fire by another detector</b>	Waiting time for fire alarm confirmation by another detector. Valid for all detectors with the reaction Fire confirmed. (1 – 60 min.)
<b>Report unset section</b>	A section which has remained unset with no movement detection for longer than 16 hours will report “unset section”.
<b>Delayed report to ARC</b>	When enabled, an Internal alarm will be triggered after the entrance delay has timed out, but the system waits for 15 sec to send an alarm report to the ARC. By that a user is provided 15 sec more to unset the system without triggering an alarm reported to the ARC.

## 10.8 Calendars tab

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



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

**Time** – Defines at what time the action is executed on the specified day.

**Guarding** – Allows to execute the actions “Set”, “Partially set” with the variant “Immediately” (no exit delay or acoustic indication) and the variant “Always” (it always ignores the ready to be set rules) and also “Unset”.

**Sections** – Specifies in which section (sections) the action of the set type is executed.

**Controls PG\*** – Allows to set PG Activation, PG Deactivation, PG Blocking or Unblocking of PG outputs. Blocked PG outputs cannot be controlled by the functional button or with an SMS.

**PG number\*** – Specifies which output/s will be enabled or disabled.

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

**Disable** – possibility to block a particular action. Disabling is indicated by a red dot. The Service Technician (using F-Link) is authorized to disable the schedule.

**Note** – Provides the possibility of customized description of scheduled events

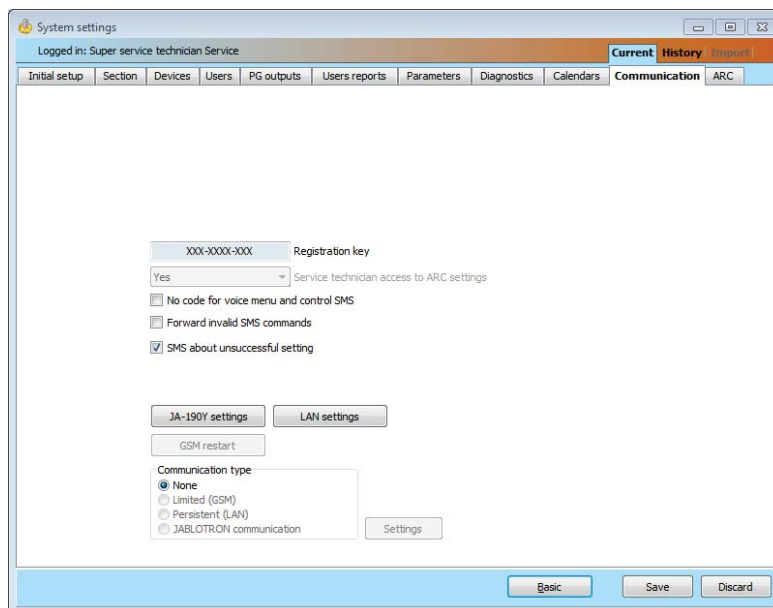
**Year schedule** – Allows you to change the attribute of the day to “Sunday” for individual days of the current and next year. You can change the attributed by (repeated) clicking of the mouse button on the corresponding day. Application example: For a public holiday (non-working day) falling on Wednesday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

### Notes:

- One schedule event can control (enable or disable) setting and PG outputs at the same time.
- Switching an application on and off for a certain time is possible in 2 ways. You can either set an action for enabling and an action for disabling the PG output or only an action for enabling and set an impulse of the required length for the PG output.
- If you select Setting (Partial setting) of a specified section, at the specified time an exit delay with the fixed time of 3 min. is first activated. All sensors in the specified sections with the Instant reaction are readjusted to have the Delayed reaction during this 3 min period. If you select Set immediately, then no exit delay is provided and all the detectors are active immediately (including delayed detectors).

## 10.9 Communication tab

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



**Registration key** – the unique registration code of the control panel.

**No code for voice menu and controls SMS** – when using an authorized phone to control a function by calling, the user does not have to enter his/her code (he/she is authorized by calling from his/her phone). For this function the caller's identification (CLIP) must be activated.

**Forward invalid SMS commands to** – selecting if the SMS messages that are incomprehensible to the control panel will be forwarded (invoicing information from the operator etc.) to the Administrator's telephone number at position 1.

**SMS about unsuccessful setting** – If enabled, the control panel sends an SMS about unsuccessful setting. When control is performed by an authorized user, then the control panel sends an SMS to the telephone assigned to this authorized user. When controlling with no authorization, then the control panel sends an SMS to the Administrator's telephone number at position 1.

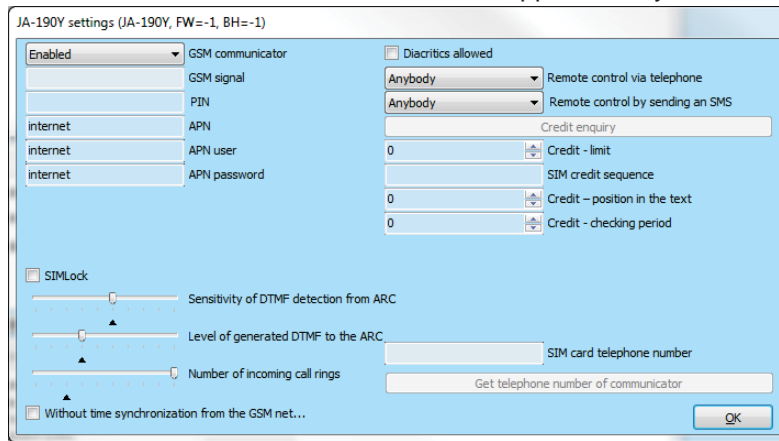
**Communication type** – the system offers several methods of remote communication/configuration

- **Without remote configuration** – no data communication is used at all. Remote configuration by F-Link is not possible.
- **Limited (GSM)** – the control panel can establish a data connection with the server and allows a remote connection via F-Link. The connection is not as data consuming as persistent (LAN) communication. When the system is equipped with a GSM communicator, the option can be enabled.
- **Persistent (LAN)** – the control panel communicates persistently with the server and it allows remote connection via F-Link. When the system doesn't include a GSM dialler, this option can be enabled.
- **Jablotron communication** – registration to the JABLOTRON Cloud allows all options offered by the system such as remote connection via F-Link and the MyJABLOTRON and MyCOMPANY applications.

**Settings** – Selection of a type of control panel with external communication with the JABLOTRON server. Allows remote connection via F-Link, registering the system to the Cloud and using the MyJABLOTRON and MyCOMPANY applications.

## 10.9.1 JA-190Y Settings

It is used to set the parameters and behaviour of the JA-190Y supplementary GSM communicator



**GSM communicator** – possibility to switch off the communicator.

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

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

**APN\*** – GPRS data communication settings. Data communication provides access to services such as the remote access of a service technician and the user, communication with the JABLOTRON CLOUD, ARC etc. Besides the APN settings the used SIM card must support data transmission.

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

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

**Sensitivity of DTMF detection from ARC** – setting the sensitivity of reception of the signals generated by the ARC. The sensitivity is adjustable in 10 steps; the optimum default value is 6.

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

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

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

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

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

**Credit enquiry** – by pressing this button you can immediately get information about the credit balance from the operator’s SMS reply (if this function is supported).

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

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

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

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

**SIM card telephone number** – The telephone number of the inserted SIM card is shown here, the system obtains it from the server.

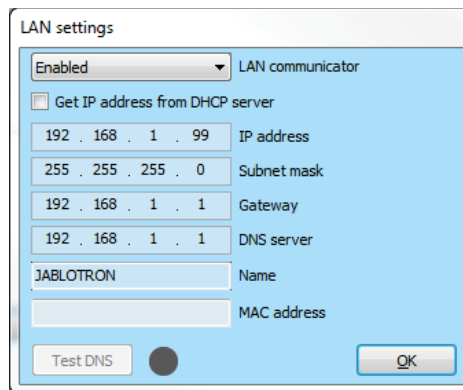
**Get telephone number of communicator** – Button serves for getting the telephone number from server manually.

### 10.9.2 GSM restart

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

### 10.9.3 LAN Settings

It is used to set the LAN communicator.



**LAN communicator** – possibility to enable or disable LAN communication.

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

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

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

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

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

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

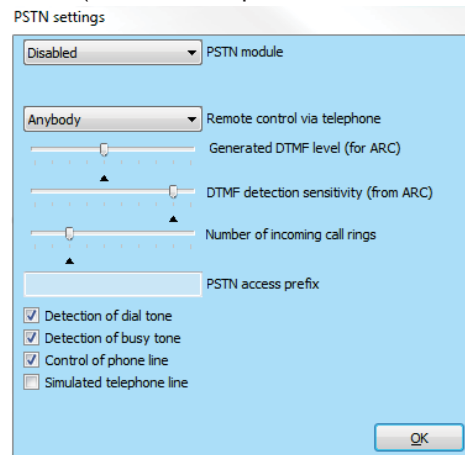
**MAC address** – unique address of every LAN device (identification of data source)

LAN device for identification of the source of information

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

## 10.9.4 PSTN Settings

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



**PSTN Module** – possibility to enable or disable communication over a phone line.

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

**Generated DTMF level (for ARC)** – setting the intensity of the transmitted tone dialling signal in DTMF generated by the control panel. The intensity is adjustable in 10 steps; the optimum default value is 4.

**DTMF detection sensitivity (from ARC)** – setting the sensitivity of reception of the signal generated by the alarm receiving centre. The sensitivity is adjustable in 10 steps; the optimum default value is 8.

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

**PSTN access prefix** – code for dialling through the internal phone exchange.

**Dial tone** – if this parameter is off, the communicator will start dialling the set phone number regardless of the type or presence of dialling tone. If it is on, the communicator will not start working until it detects the dialling tone (e.g. dialling tone assignment delay in some phone exchanges).

**Detection of busy tone** – if the communicator detects the engaged tone, e.g. in a parallel line, it will hang up and inform the system. It is not recommended to enable this parameter as the communicator then does not detect hanging up.

**Phone line check** – The communicator completely disables detection of voltage in the phone line. It means that it will not report the torn-off phone line error. If it gets torn-off, an error will be indicated after 30 min. from the detection of phone line loss. The communicator indicates the error using a yellow LED.

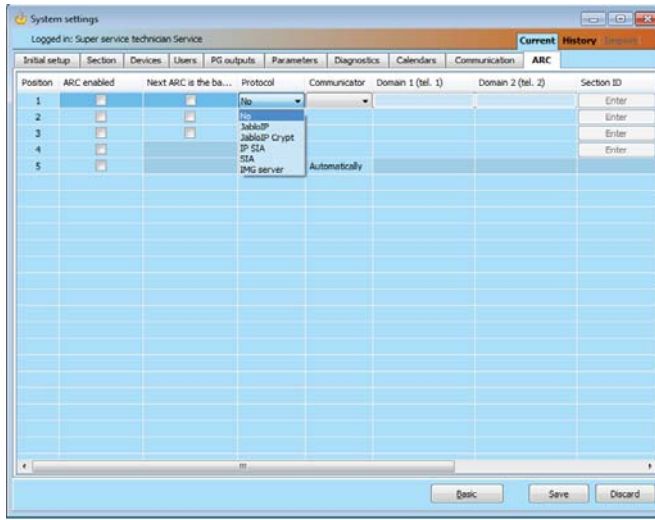
**Simulated telephone line** – If activated, the communicator does not check presence of the phone line or its tones. Thus, it will not detect a phone line error at a lower voltage than 15 V. The use is designed for radio modems.

You will find a detailed description of parameter settings in the manual of the JA190X phone communicator module.

## 10.10 ARC tab

This tab is used to set up communication by up to 4 alarm transmission paths or by 4 communication protocols. Each transmission path can be used for 4 different alarm receiving centres or generally for 4 different alarm reports receivers.

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



**ARC enabled** – possibility to disable the set outputs

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

**Protocol** – transmission protocol setting

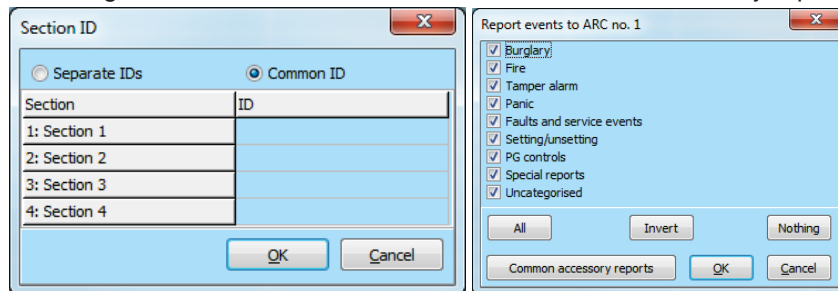
**Communicator** – if the selected protocol can be transmitted in more ways, the communicator type is selected here

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

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

**Section ID** – setting of the building identification (common for the whole building or individually for sections).

**Warning:** The default setting is zero, with which the communicator will not send any reports!



**Reported events** – selecting types of reported events and the possibility of setting codes of supplementary reports (PG outputs)

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

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

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

## 10.10.1 Requirements for the setup of transmission paths to an ARC

The JA-100K control panel can establish transmission paths to the ARCs according to European standards EN 50136-1 and EN 50136-2. The following table states the individual parameters to comply with a specific ATS class. There must be full support of the ATS classes at the ARC.

ATS Class	Useable interfaces (Alarm protocols)	Connection check at fixed time	Connection check time	Fault when event report delay over limit	Number of repeats	Period of waiting after an unsuccessful attempt	Encryption System time Event time
SP2	PSTN / GSM / LAN (JABLO IP, SIA IP, SIA CID)	Optional	1x per 24 hrs	120 s	2	30 s	Optional Required Required
SP3	GSM / LAN (JABLO IP, SIA IP, SIA CID)	Not allowed	1x 30 min	60 s	2	30 s	Optional Required Required
SP4	GSM / LAN (JABLO IP, SIA IP)	Not allowed	1x 3 min	60 s	3	20 s	Required Required Required
SP5	GSM / LAN (JABLO IP, SIA IP)	Not allowed	1x 1 min	30 s	6	5 s	Required Required Required
DP2	LAN + PSTN (JABLO IP, SIA IP)	Not allowed	1x 30 min	60 s	2	30 s	Optional Required Required
DP3	LAN + GSM (JABLO IP, SIA IP)	Not allowed	1x 3 min	60 s	3	20 s	Required Required Required

## 10.10.2 Transmission paths

For GSM (GPRS) and LAN communication using IP protocols:

1) Protocol ANSI SIA DC-09, SIA IP (DC9), methods DCS or ADM\_CID (data message)

- encryption according to the AES standard with 128, 192 or 256 bit keys
- unique message time stamps inserted
- very precise time synchronization between alarm system and ARC

2) Protocol JABLO\_IP (data message)

- Proprietary Jablotron protocol
- 256 bit encryption
- unique message time stamps inserted
- precise time synchronization between alarm system and ARC

3) JABLO\_SMS (data SMS messages)

- based on JABLO\_IP protocol with floating data encryption



### 10.10.3 JABLOTRON 100 CID and SIA codes

CID	SIA	Event EN	Report category
1101	QA	Health problem	Burglary
1110	FA	Fire alarm	Fire
1118	FG	Unconfirmed fire alarm	Fire
1120	PA	Panic alarm	Panic
1130	BA	Instant alarm	Burglary
1133	BA	24H alarm	Burglary
1134	BA	Delayed alarm	Burglary
1138	BG	Unconfirmed alarm	Burglary
1144	TA	Tamper of device	Tamper
1151	GA	Gas leak	Fire
1154	WA	Flood alarm	Tamper
1170	UA	Special Reaction A	Special reports
1171	UA	Special Reaction B	Special reports
1172	UA	Special Reaction C	Special reports
1173	UA	Special Reaction D	Special reports
1174	UA	Not used	Special reports
1175	UA	Not used	Special reports
1176	UA	Not used	Special reports
1177	UA	Keybox	Special reports
1300	ET	Fault	Faults and service events
1301	AT	AC loss	Burglary
6301	AT	AC loss longer than 30 min (from FW 10 and higher)	Burglary
1302	YT	Low Battery in control panel	Faults and service events
1305	RR	System boot	Faults and service events
1306	LB	Entering service mode	Faults and service events
1308	RE	System shutdown	Faults and service events
1313	YX	Blocked after alarm - Engineer reset	Uncategorised
1314	YG	ARC setting erased	Uncategorised
1344	XQ	RF jamming / RF interference	Faults and service events
1350	YC	Event to ARC not delivered	Uncategorised
1354	YS	Event to ARC was not delivered in pre-set time	Faults and service events
1384	XT	Low Battery in device	Faults and service events
1401	OP	Unset	Setting / Unsetting
1402	OG	Unset partially	Setting / Unsetting
1406	BC	Alarm cancelled by user	Burglary
1407	OQ	Unset remotely	Setting / Unsetting
1412	LF	Remote access	Uncategorised
1416	LS	Configuration saved	Uncategorised
1454	CI	Section with no movement	Faults and service events
1455	CI	Unsuccessful setting	Uncategorised
1461	JA	Code breaking attempt exceeded	Tamper
1521	BL	Siren mute	Uncategorised
1570	EB	Device bypass (Disabled)	Uncategorised
1572	TB	Tamper bypass	Faults and service events
1573	BB	Activation bypass	Faults and service events
1574	UB	Bypass of a section (Disabled)	Uncategorised
1578	UO	Fault bypass	Faults and service events
1601	RX	Manual test	Faults and service events
1602	RP	Periodic test / Link test	Uncategorised
1625	JT	Reset of time	Uncategorised
1661	RC	PG1 ON	PG controls
1662	RC	PG2 ON	PG controls
1663	RC	PG3 ON	PG controls
1664	RC	PG4 ON	PG controls
3101	QR	Health troubles (deactivation)	Burglary
3110	FR	Fire alarm (deactivation)	Fire
3118	FG	Unconfirmed fire alarm (deactivation)	Fire
3120	PR	Panic (deactivation)	Panic
3130	BR	Instant alarm (deactivation)	Burglary
3133	BR	24hr alarm (deactivation)	Burglary



3134	BR	Delayed alarm (deactivation)	Burglary
3138	BG	Unconfirmed alarm (deactivation)	Burglary
3144	TR	Tamper (deactivation)	Tamper
3151	GR	Gas leak (deactivation)	Fire
3154	WR	Flood alarm (deactivation)	Tamper
3170	UR	Special Reaction A (deactivation)	Special reports
3171	UR	Special Reaction B (deactivation)	Special reports
3172	UR	Special Reaction C (deactivation)	Special reports
3173	UR	Special Reaction D (deactivation)	Special reports
3174	UR	Not used	Special reports
3175	UR	Not used	Special reports
3176	UR	Not used	Special reports
3177	UR	Keybox (deactivation)	Special reports
3300	ER	Fault (deactivation)	Faults and service events
3301	AR	AC recovery	Uncategorised
3302	YR	Control panel backup battery OK	Special reports
3306	LX	Service mode exit	Special reports
3313	YZ	Unblocked after alarm	Uncategorised
3344	YH	RF interference / RF jamming (deactivation)	Faults and service events
3350	YK	Communication to ARC restored	Uncategorised
3354	YL	Event to ARC was not delivered in pre-set time (deactivation)	Faults and service events
3384	XR	Battery of device OK	Faults and service events
3401	CL	Set	Setting / Unsetting
3402	CG	Partially set	Setting / Unsetting
3407	CQ	Set remotely	Setting / Unsetting
3412	LE	Remote access closed	Uncategorised
3417	CU	Remotely partially armed	Setting / Unsetting
3570	EU	End of device bypass (deactivation)	Uncategorised
3572	TU	Tamper bypass end	Tamper
3573	BU	Activation bypass end	Uncategorised
3574	UU	End of section bypass (deactivation)	Uncategorised
3578	UP	Fault bypass (deactivation)	Faults and service events
3661	RO	PG1 OFF	PG controls
3662	RO	PG2 OFF	PG controls
3663	RO	PG3 OFF	PG controls
3664	RO	PG4 OFF	PG controls

Source code	Description
001 - 120	Devices
501 - 800	User codes
500	Service code
901	Control panel
921	ARC1
922	ARC2
923	ARC3
924	ARC4
912	LAN communicator
913	PSTN communicator
914	Supplementary GSM communicator

## 10.11 Diagnostics tab

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

P	Name	Type	Section	Activation...	Status	Battery status/voltage	Voltage/ loss	RF Signal level	Channel	Note
0	Control panel	JA-101K	1: Groud floor		OK	13.7 V/13.7 V	13.7 V/163 mA	100 % GSM		
1	Radio module	JA-110R	1: Groud floor		OK		-0,1 V		RJ	
2	LCD keypad	JA-114E	1: Groud floor		OK		-0,4 V		RJ	
3	Main door	JA-110M	1: Groud floor		ACT		0,0 V		Bus 1	
4	Kitchen window	JA-110M	1: Groud floor		OK		0,0 V		Bus 1	
5	Garage door	JA-111M	3: Garage		ACT		0,0 V		Bus 1	
6	Hall	JA-110P	1: Groud floor		OK		-0,1 V		Bus 1	
7	Garage PIR	JA-120PW	3: Garage	ACT	OK		-0,2 V		RJ	
8	Indoor siren	JA-110A	1: Groud floor		OK		0,0 V		Bus 1	
(?) 9	Balcony door	JA-150M	2: First floor		ACT	100 %		100 %		
(?) 10	Balcony window	JA-150M	2: First floor		OK	100 %		100 %		
(?) 11	Living room	JA-151P	2: First floor		ACT	100 %		80 %		
12	Interface	JA-121T	1: Groud floor		OK		-0,3 V		RJ	
(?) 13	Remote control	JA-182J	4: Fully set							

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

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

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

**Voltage/loss\*** – On the position of the control panel (0) voltage of the control panel terminals and current that is drawn by the BUS devices from the control panel are displayed. For BUS device the line voltage loss as compared to the control panel is displayed. The loss must not be higher than 2 V; otherwise the problem must be solved (e.g. by adding a BUS power booster).

**RF signal level\*** – indicates the quality of the signal with which the control panel communicates via GSM when a supplementary GSM communicator connected or wireless device RF. The value should be at least 50%. If the indication is missing, the device has not communicated yet – activated its transmission (e.g. by means of the tamper sensor) or wait until automatic transmission occurs. The value on the control panel line is the strength of the GSM network signal (about the interference between radio modules and the GSM module see also chapter 6.1 Installation of a JA-111R radio module).

Colour coding of the GSM signal: 0-30% red, 40-50% yellow and over 50% green.

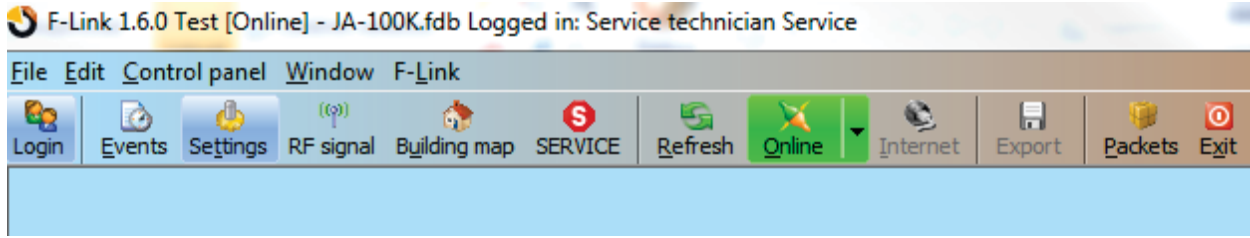
Colour coding of the RF signal: 10% red, 20% yellow, 30% and higher green.

**Channel\*** – informs about the BUS used by the device to communicate. Two paths are distinguished: BUS output and the RJ connector designed for the JA-11xR radio module. There is a special column called Channel which displays via which bidirectional devices communication currently occurs.

# 11 Other F-Link options

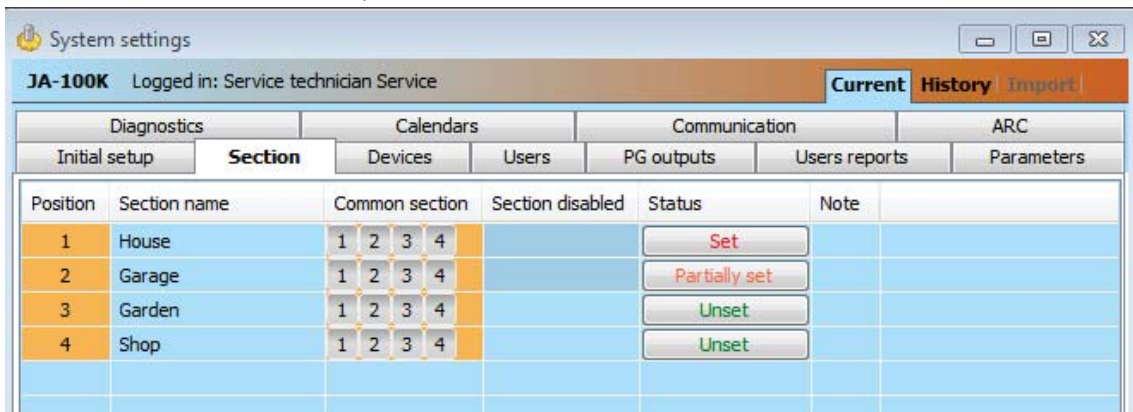
The F-Link version is always indicated in the top bar behind the name.

The toolbar provides brief access to often-used items such as the button for mode changes, system events, settings, the RF signal of radio modules, settings exporting or local and remote access to the control panel.

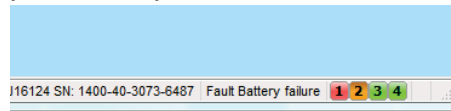


## 11.1 System control by F-Link

Individual sections in the F-Link SW can be controlled locally or remotely, there are two ways. The first way is to click on the button in the Section tab, Status column.



The second way is clicking on the icons representing the system status on the lower toolbar; user authorization is recorded in the system history based on current code used for log-in to the F-Link SW.



## 11.2 Event history:

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

**Events from the control panel memory** (available also after pressing F8) – approx. 100 kB of events (from the microSD card) are loaded. If the loading range is insufficient, you can repeatedly select Load / Next 100(500) kB or All. Warning: If you select Load/All, in a control panel with a longer time of operation the loading may take a few minutes. The history does not record events that occur during service setting (just the opening and closing of

The screenshot shows the "Events from memory" window. It has a table with columns for "ID", "Time", "Source", "Section", "Event", and "Channel". The events are listed chronologically from 1/6/2017 3:06:46 PM to 1/6/2017 3:44:53 PM.

ID	Time	Source	Section	Event	Channel
200	1/6/2017 3:06:46 PM	Detector 2: Periferie 2	1: Section 1	Sabotáž aktivace	0: Control panel
201	1/6/2017 3:06:46 PM	Externí komunikátor	1: Section 1	Periferie vypnuta	0: Control panel
202	1/6/2017 3:06:46 PM	Detector 0: Ústředna	1: Section 1	Varování, kódy z výroby	0: Control panel
	1/6/2017 3:06:46 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
203	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišení aktivace	2: Device 2
204	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišení deaktivace	2: Device 2
205	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišení	2: Device 2
206	1/6/2017 3:06:58 PM	User 1: Správce	2: Device 2	Autorizace OK	2: Device 2
207	1/6/2017 3:06:59 PM	User 1: Správce	2: Section 2	Zajistěno	2: Device 2
208	1/6/2017 3:06:59 PM	User 1: Správce	3: Section 3	Zajistěno	2: Device 2
209	1/6/2017 3:07:01 PM	User 1: Správce	2: Device 2	Autorizace OK	2: Device 2
210	1/6/2017 3:07:01 PM	User 1: Správce	2: Section 2	Odstiženo	2: Device 2
211	1/6/2017 3:07:01 PM	User 1: Správce	3: Section 3	Odstiženo	2: Device 2
	1/6/2017 3:07:47 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
	1/6/2017 3:08:48 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
212	1/6/2017 3:12:24 PM	User 0: Servis 0	1: Section 1	Vstup do servis.režimu	USB
213	1/6/2017 3:12:48 PM	User 0: Servis 0	1: Section 1	Opuštění servis.režimu	USB
214	1/6/2017 3:12:51 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potřeže aktivace	2: Device 2
	1/6/2017 3:12:52 PM	Detector 0: Control panel		Created backup configuration	
215	1/6/2017 3:12:59 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potřeže deaktivace	2: Device 2
216	1/6/2017 3:12:59 PM	Detector 0: Ústředna	1: Section 1	Sabotáž aktivace	0: Control panel
217	1/6/2017 3:12:59 PM	Detector 2: Periferie 2	1: Section 1	Sabotáž aktivace	0: Control panel
218	1/6/2017 3:12:59 PM	Externí komunikátor	1: Section 1	Periferie vypnuta	0: Control panel
219	1/6/2017 3:12:59 PM	Detector 0: Ústředna	1: Section 1	Varování, kódy z výroby	0: Control panel
	1/6/2017 3:12:59 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
220	1/6/2017 3:13:04 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potřeže aktivace	2: Device 2
221	1/6/2017 3:13:04 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potřeže deaktivace	2: Device 2
	1/6/2017 3:14:00 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
	1/6/2017 3:15:01 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
222	1/6/2017 3:19:43 PM	User 0: Servis 0	1: Section 1	Vstup do servis.režimu	USB
223	1/6/2017 3:44:53 PM	User 0: Servis 0	1: Section 1	Opuštění servis.režimu	USB
	1/6/2017 3:44:58 PM	Detector 0: Control panel		Created backup configuration	

the Service mode is registered). Loaded events can be saved in a file in the File menu using the Export item (Shft+Ctrl+S), namely in several formats (FDE, PDF, TXT, CSV, XML, HTM or HTML). The FDE suffix makes it possible for the F-Link to download the events again.

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

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

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

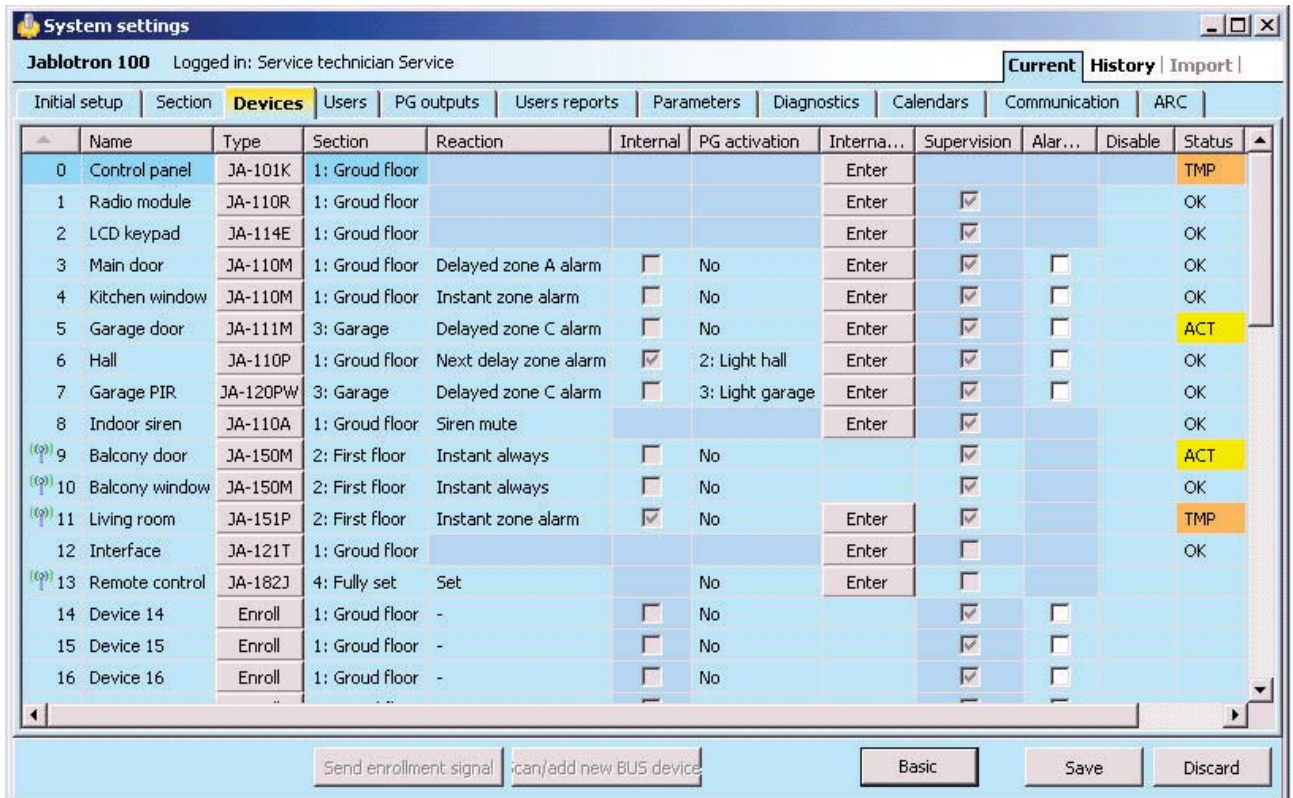
**Refresh** – makes it possible to load more events deeper from the history by 100 kB, 500 kB (100 kB corresponds to approx. 1200 events) or all.


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

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

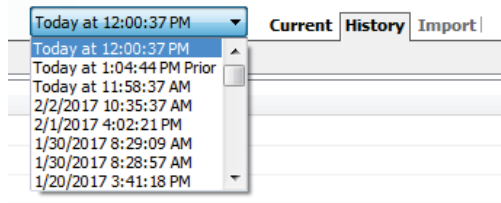
### 11.3 System settings

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



1. The System Settings Window is opened and closed by the **Settings**  button in the top toolbar.
2. In the window you can switch between the following **tabs: Sections, Devices, Users, PG outputs, Parameters, ...**
3. The window will display the **current setting of the control panel** loaded on opening of the F-Link SW (hereinafter SW only). The **Refresh** button in the top toolbar can be used to load the current content of the control panel at any time.
4. If you want to view **older settings of the control panel, use the History tab** in the top right corner. The history cannot be changed, but it can be saved in the control panel (if you need to return to earlier settings). The 100 previous settings are over-recorded in the history (arranged by date and time) and also all setting changes.
5. You can **import settings** from another installation to the system, e.g. after replacing an old control panel with a new one or using a default template. If the control panel is replaced with a new one, after the connection a completely new database will be created in the computer. To import settings from


another database, in the top bar of the main menu select **File / Import** and select the file you want to import settings from. After this selection the **Import** button in the **System Settings** tab will be.

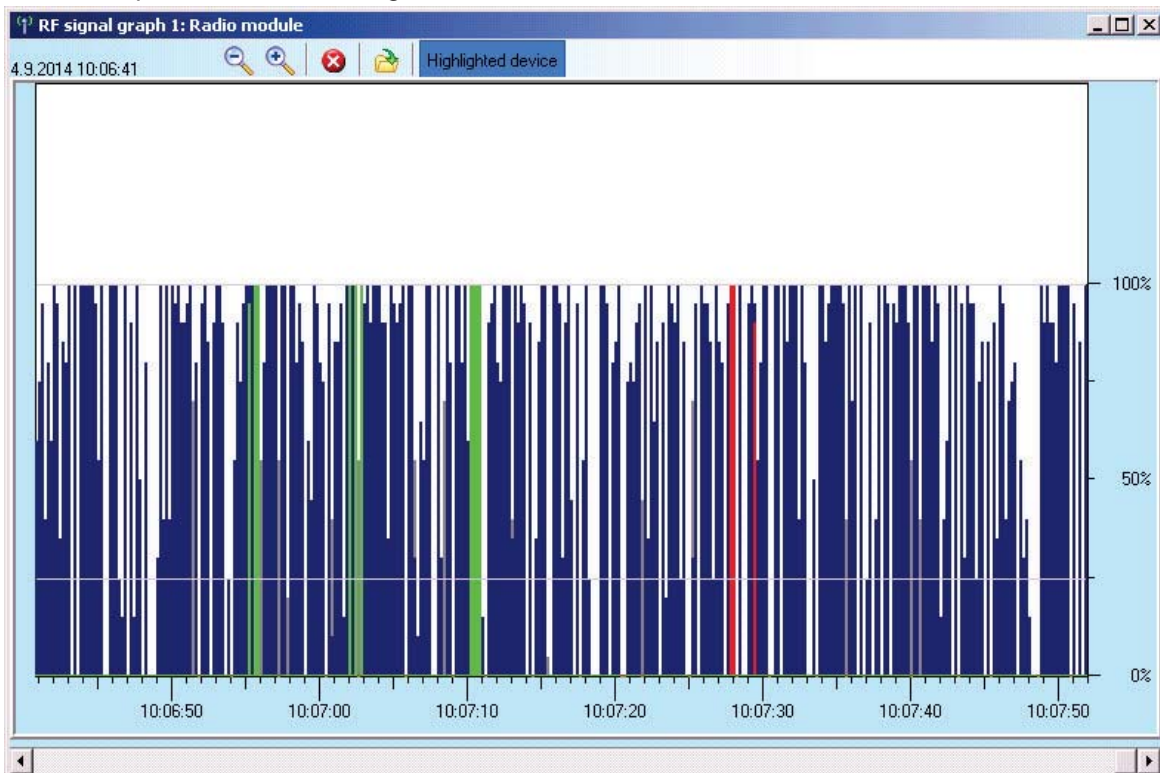


6. **If you make a change to a setting, it will be indicated with blue text** (the name of the tab will become blue, too). The blue indication will disappear as soon as you save the changes.
7. You can **Save the Settings** using the **Save** button (at the bottom on the right). If you are saving settings in the control panel for the first time, SW will ask you to **enter the file name**. In the computer, a file with the \*FDB suffix will be created where the history of settings is gradually saved (every time the settings are saved in the control panel). If you do not want to save the changes, select the **Cancel** button and in the confirmation question select **Ignore**. Parameters can be changed in more tabs and you can then Save all changes.
8. The **Enroll not enrolled** button (Lower toolbar on the Devices tab) will open a dialog for collective enrollment (without the possibility to select positions) of devices that are connected to the BUS and have not been connected to the system in another way. See chapter 8.4.1 Enrolling and erasing devices.
9. The **Send enrolling signal** button (Devices and PG outputs tab) will release sending of the enrolling code of the control panel to wireless devices, e.g. to wireless output modules.
10. **Setting of all parameters is only possible in the Service mode** (the system is not in the active setting mode. The Service mode is activated and deactivated with the **Service** button in the top toolbar.
11. **Some parameters can be changed during operation**. Therefore, the Settings tab can be opened without entering the Service mode. However, available options can only be set.
12. **The SW contains bubble help** – after placing the mouse cursor over an item the text description will be displayed. You can disable the bubble help in the F-Link roll-down menu.

## 11.4 RF Signal

Window for graphic representation of radio band interference intensity with the possibility to select from the used radio modules. Presence of signals in the band is indicated in blue. Red colour identifies communication signals of the entire system (enrolled devices) and green is used to display the selected RF device from the list of the **Highlighted device** item (see figure). Monitored interference logging (when the RF Signal

window is open) can be exported from the main menu to a file with an FDR extension and the  button can be used to import it back for viewing.



## 11.5 Service



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

## 11.6 Refresh



Updating the internal settings of devices after a hardware change.

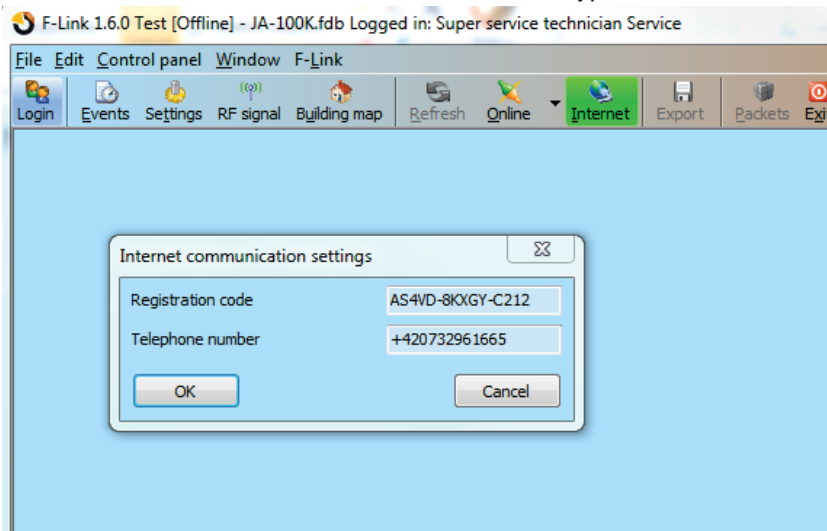
## 11.7 Online



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

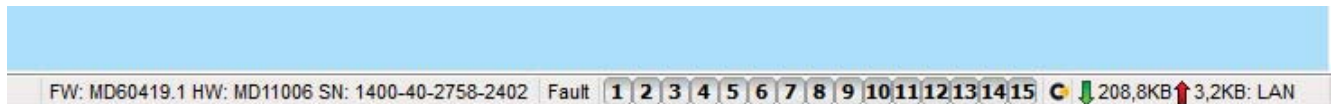
## 11.8 Internet

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



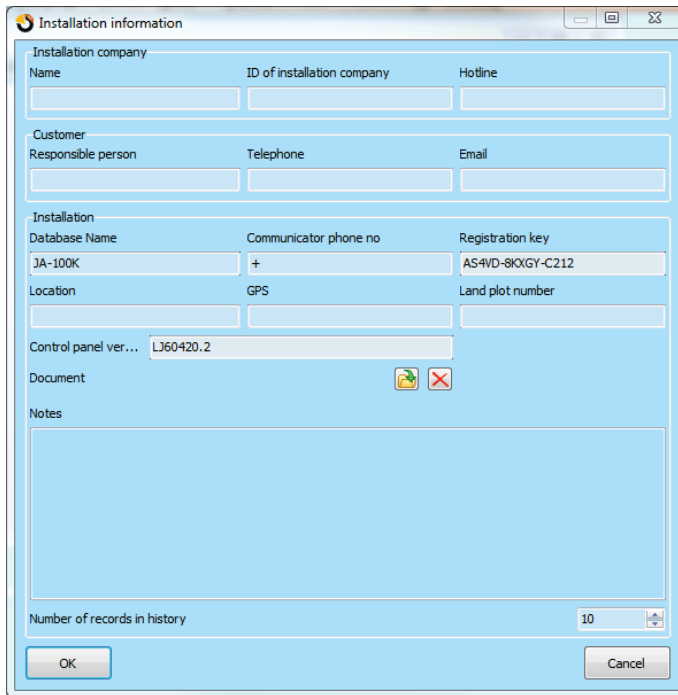
After clicking on the Internet button a dialog window with pre-entered data is displayed. If you are connecting from a new “empty” database, the registration code and the phone number will have to be added. When a LAN communicator is used and Jablotron communication enabled, then the telephone number cannot be filled in (field must remain blank). Establishing the connection only takes a few seconds, but the downloading of the configuration depends on the system size and it may usually take 1 to 2 minutes.

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



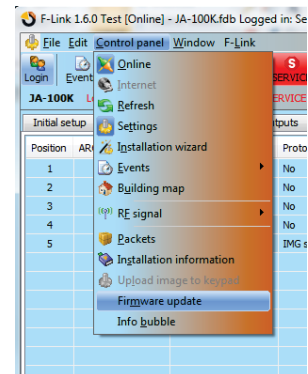
## 11.9 Installation Information

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



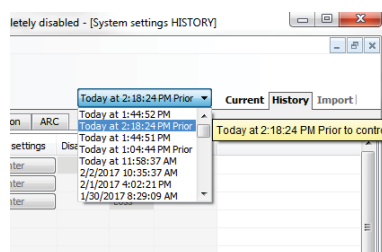
## 11.10 Firmware update

A firmware update makes it possible to change the behaviour of updatable devices (control panel, radio modules, keypads, detectors etc.) with a FW package that the manufacturer officially releases in the Jablotron sever. F-Link downloads from the Jablotron server automatically (after a query), if in the F-Link menu the Automatic Updates item is activated (default setting). If not enabled F-Link will make it possible to find the FWP files in the computer manually before the upgrade. Read more in the chapter 13 Firmware update.



## 11.11 History of Settings

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



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



## 12 Reset of the control panel

Default settings of the control panel can be restored only if in the F-Link SW in the Parameters tab the “Reset enabled” is checked. If Reset is not enabled and you do not know the service code, you cannot reset the control panel and the control panel board must be sent to the distributor.

Procedure:

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

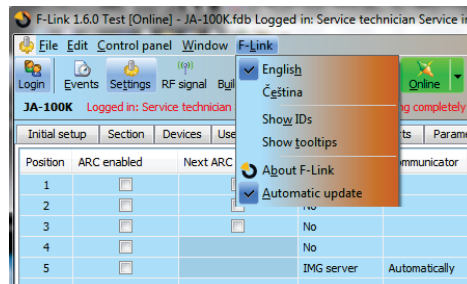
## 13 Firmware updates

The control panels and some other devices of the JABLOTRON 100 system enable a firmware change. Firmware is usually changed to extend the useful parameters of the equipment and to support newly launched products.

### 13.1 General firmware (FW) update rules

1. A FW update can only be performed with a computer with the installed **F-Link** SW either with the use of local access via a USB cable or remotely where the possibility to change firmware is limited to BUS devices and also on bidirectional wireless devices.
2. Firmware (FW) can be changed by a user with the Service authorization.
3. The latest F-Link version is accessible for authorized technicians after login to the MyCOMPANY (F-Link SW includes also the FW package). If the F-Link is already installed and the computer has Internet access, then F-Link checks automatically available updates after the start and if there is newer version, it will offer its download along with the latest FW package.
4. Connect the computer to the control panel with a USB cable.
5. Start the **F-Link** software with the control panel connected.
6. Switch the control panel to the **Service** mode.
7. Start the **Control Panel / Firmware Update**  
If **Automatic Update** is allowed in the **F-Link** menu (default setting), the list of updatable devices is displayed. This file is part of F-Link in the **F-Link x.x.x / Firmware** directory and its up-to-date status is only guaranteed at the time of the F-Link download.

Location of the Automatic Update parameter:



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

1. In the Firmware Update selection window, updatable BUS and bidirectional wireless devices of the control panel are displayed. F-Link automatically selects devices for which an update is required (they have older FW than the one in the FW pack).

2. F-Link displays also wireless devices which can be updated wirelessly (see 13.3 FW updates for wireless devices) or individually over additional USB cable connected to the computer.
3. More detailed information about the existing and new versions of individual devices is displayed in the help bubble after moving the mouse cursor over each of the offered devices.
4. In the selection boxes the devices for which never FW is available are checked, we recommend to leave it checked. Some items may be obligatory and thus unavailable (greyed) for update cancellation.
5. If the control panel update is checked, the possibility to keep the modified user voice menu is displayed (if disabled, the default voice menu recording will be restored).
6. Click on OK to start the update of FW of all selected devices. All the changes will be executed within a few minutes (depending on the number of devices). Finally, the control panel will restart the system.
7. After a change of FW a part of the registration code may be changed. Its change will not have any impact on the possibility of remote access (using F-Link) or possible communication of the control panel with the JABLOTRON Cloud service and also the img.jablotron.com server.
8. If during the control panel update F-Link finds damaged files in the SD card, it will format it and after completion of the update it will offer the possibility of re-importing the original settings.
9. Perform a check in accordance with the description in chapter 13.4 Check after a FW check.

### 13.3 FW updates for wireless devices

The most convenient way of FW update for selected wireless devices is over the system's radio network without the need of a cable connection. If a wireless upgrade of any device is impossible (e.g. because of current local radio conditions) it can be updated by USB cable.

#### Wireless update using radio module:

1. Start F-Link with the control panel connected
2. Open the menu in the **F-Link software: Control Panel → Firmware Update**
3. The SW offers a table with enrolled upgradable devices, check if all required wireless devices are selected (an update of the greyed-out devices can be mandatory and selected automatically because of compatibility reasons).
4. More detailed information about the existing and new versions of individual devices is displayed in the help bubble after moving the mouse cursor over each of the offered devices.
5. By pressing the OK button all selected devices will be updated.
6. After completion of the upgrade perform a check in accordance with the description in chapter 13.4 Check after a FW check.

#### Upgrade using a USB cable:

1. Open the updatable wireless device (not related to AC-160xx).
2. If batteries are included, remove them and if the device is powered by an external adapter, disconnect it as well (AC-160xx only).
3. Start F-Link, open the database and connect a USB cable to the computer (miniUSB or microUSB depending on the used device).  
**Warning:** *USB cables are not included with individual devices. We recommend you to use a direct USB connection to the PC, a connection with a USB HUB may reduce reliability.*
4. The updates of FW in wireless devices must be carried out one at a time, it cannot be done simultaneously with multiple USB cables.
5. In the wireless device to be updated open the mode for loading new FW. Follow the instructions of the respective manuals.
6. Then continue as during a system upgrade with **F-Link software: Control Panel → Firmware Update**.
7. In the device selection table, select a USB item (typically in the first position).
8. More detailed information about the existing and new versions of individual devices are displayed in the help bubble after moving the mouse cursor over each of the offered devices.
9. By pressing the OK button you will update all the devices.
10. After completion of the update disconnect the USB cable, reinsert the batteries or connect the power supply and re-assemble the module.
11. Perform a check in accordance with the description in chapter 13.4 Check after a FW check
12. Go on to upgrade the next wireless device

### 13.4 Check after a FW check

1. Check the settings of all the changed devices and control panel in **F-Link, Devices / Internal Settings** Depending on the range of changes implemented during the update the previous setting may be

maintained or reset to the default production values. If reset to the default values has been done, you can use the Import button in the internal settings of individual devices to select from previous settings.

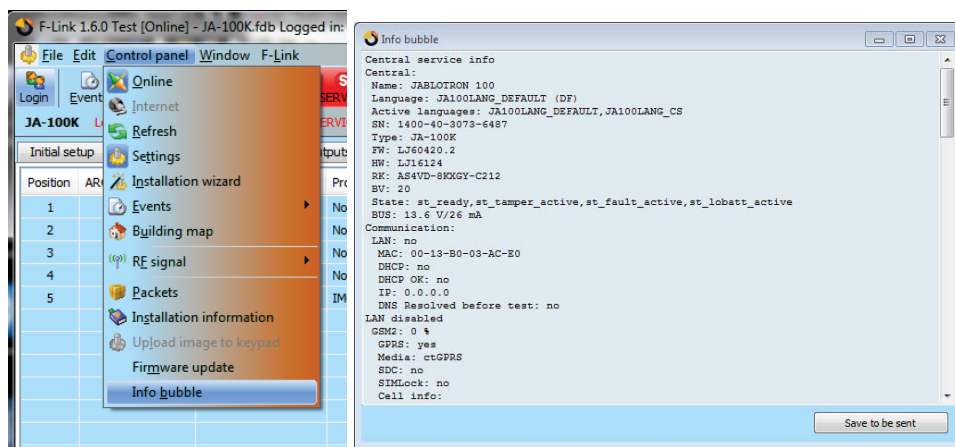
2. If new items were added within the update, they will have the default settings. Check them and adapt the settings as necessary for the installation
3. Check the settings and test function of the updated devices.

## 13.5 Info Window

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

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

This data is necessary e.g. for communication with the technical consultant for which the “Save for Sending” button in the bottom right corner is designed for. The file is a ZIP compressed file and it contains data of the installation, incl. a part of the event history (100 kB), but it does not contain any sensitive data as phone numbers of users or their access codes or other confidential data.

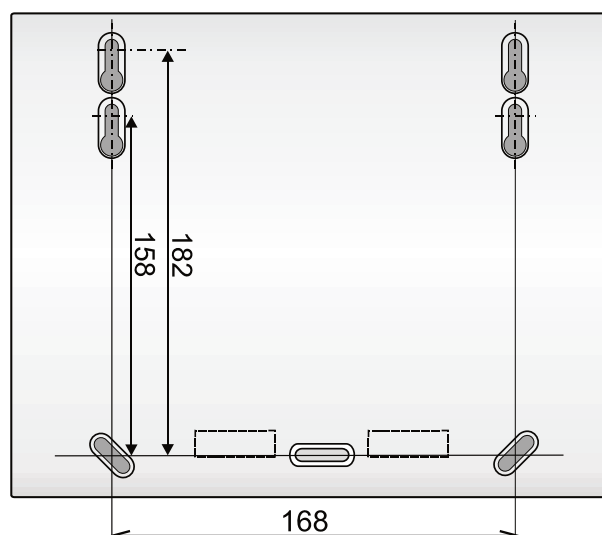
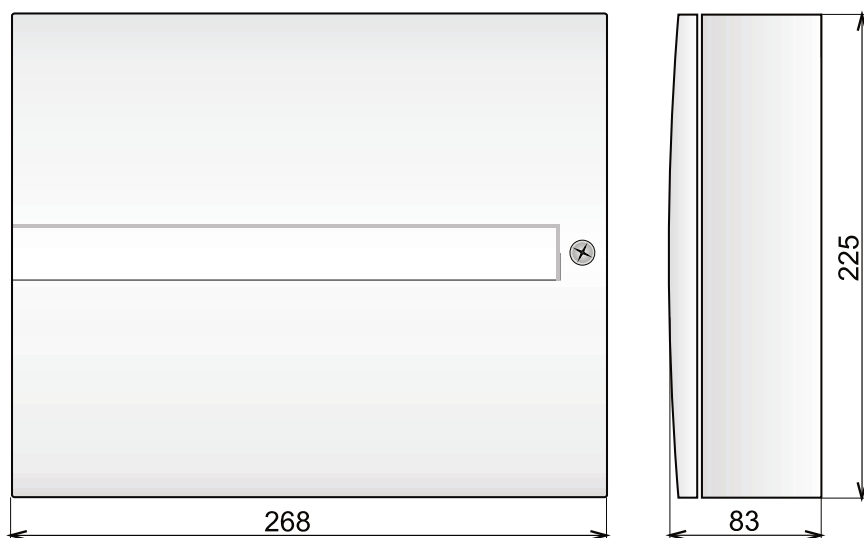


# 14 Supplementary information

## 14.1 Overview table of current consumption of BUS devices

Device	Consumption in the backup mode (mA)	Consumption for cable selection	Note
JA-110E LCD keypad with an RFID reader	15	110	
JA-11xR Radio module for wireless connection	25	25	
JA-110A Internal siren	5	30	30 mA during an alarm
JA-111A External siren	5	50	In case of an AC supply failure without battery charging, otherwise 550 mA depending on battery charge
JA-190X Phone communicator Module	15	30	
JA-190Y GSM communicator	25	220	Maximum current for communication with provider

## 14.2 Control panels dimensions



## 15 System takeover by the user

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

1. Control from system keypad. Setting and unsetting of sections (using functional buttons, or from the keypad menu).
2. Ensure that exit / entrance time is adequate and also valid for garage doors or other entrance routes.
3. Explain what authorization is, what it is for and options like codes, RFIS tags, etc...
4. Partial setting at home. Difference in indication between partial and full setting.
5. Control of home automation using functional buttons and other functions (Panic, Fire, health troubles).
6. Triggering an alarm when the system is set included sirens, test of alarm call.
7. Explaining the difference between alarm cancelling by authorization and unsetting a section.
8. Section control (remotely via voice menu using cell phone keypad).
9. Section control and home automation (PG outputs) via SMS.
10. Control using the web or smart application from tablets, smart phones or from a website.

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

# 16 Technical specifications

Parameter	JA-100K
Type of installation	Fixed installation
Nominal control panel voltage / frequency / fuse	~ 230 V / 50 Hz, T200 mA fuse 250 V 5 x 20 mm ~ 115 V / 60 Hz, T400 mA fuse 250 V 5 x 20 mm
Operational AC voltage range	~ 195 V ÷ 250 V ~ 110 V ÷ 120 V
Electric power / current	Max 23 VA / 0.1 A
Protection class	II.
Back-up battery	12 V; 2.6 Ah max. (lead-acid)
Low battery voltage (fault indication)	≤11 V
Maximum battery charging time	48 ÷ 72 hrs
BUS voltage / max. voltage ripple (red-black)	12.0 ÷ 13.8 V <sub>DC</sub> / ± 100 mV
Max. continuous consumption from the control panel BUS +RJ	400 mA permanently (1000 mA for 5 minutes)
@ 12 hours backup (2.6 Ah)	LAN OFF: 125 mA – consumption of modules JA-190X (Y) LAN ON: 85 mA – consumption of modules JA-190X (Y)
Max. number of sections	4
Max. number of devices	32
Max. number of users	33
Max. number of PG outputs	4
Alarm connection	Jablotron BUS – dedicated wiring Wireless connection (with JA-111R) – unspecified wireless connection, Jablotron wireless protocol
Alarm system classification	Security grade 2 / environmental class II
@ according to standards	EN 50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN50131-10, EN 50136-1, EN 50136-2
@ environment	indoor general
@ operational temperature / humidity	-10°C to +40°C, relative humidity 75% no condensation
@ power	Type A – primary supply with a charged backup battery
@ event history	approx. 7 million latest events, incl. date and time
@ system reaction to communication loss	Fault or tamper – according to the pre-set profile @ BUS until 10 sec @ wireless communication in 2 hrs (report) @ wireless communication in 20 min, blocks system to be set
@ reaction to invalid code entry	After 10 wrong code entries a tamper alarm is triggered and according to the selected profile it blocks all control devices for 10 min
@ ATS classification	Supported ATS classes : SP2 – SP 5, DP2 – DP3 SPT: type Z Operation type: Pass-Through Built-in LAN: SP2 – SP5 (with IP protocol) JA-190Y SP2 – SP5 (with IP protocol) JA-190X SP2 (with Contact ID protocol) LAN + JA-190Y DP2 – DP3 (with IP protocol) LAN + JA-190X DP2 (with IP / CID protocol)
@ ATS transmission protocols	JABLO IP, SIA IP, Contact ID, JABLO SMS

@ ATC protection against substitution and data protection	Jablotron protocol: Proprietary AES encryption with minimum 128 bit key ANSI SIA DC-09.2012 protocol with 128 bit AES encryption
LAN communicator	Ethernet interface CAT 5 (RJ-45)
Dimensions (mm)	268 x 225 x 83
Weight	1450 g
Basic parameters of the JA-111R module	868.1 MHz, < 25 mW, GFSK < 80 kHz
Radio emissions	ETSI EN 300 220-2 (R module)
EMC	EN 50130-4, EN 55022, ETSI EN 301 489-7, ETSI EN 301 489-3
Electric safety	EN 60950-1
Operational conditions	ERC REC 70-03, ERC DEC (98) 20
Certification body	TREZOR TEST



JABLOTRON ALARMS a.s. hereby declares that these control panels JA-100K meet the basic requirements and other relevant provisions of the Directives no. 2014/53/EU, 2014/35/EU, 2014/30/EU and 2011/65/EU. You will find the original Declaration of Conformity at [www.jablotron.com](http://www.jablotron.com).



Note: Although the product does not contain any harmful materials, do not dispose of it as municipal waste, but bring it to a collection facility of electronic waste. More detailed information at [www.jablotron.com](http://www.jablotron.com) Technical Support section.