JA-101K and JA-106K alarm system control panel

Warning:

The JABLOTRON 100 series alarm system should be installed exclusively by a trained technician with a valid certificate issued by an authorized Jablotron distributor. It is recommended to use only Jablotron's JA-100 series devices in the system. The correct functioning of the system cannot be guaranteed when other devices are used.

Manual is valid for firmware LJ60205 in the control panel or higher.

Contents:

1 Basic description and definitions

Modular architecture: enables users to create a system whose scope of installation and functions perfectly meet their needs and suit the size of the building.

Control segment: a structural element of a control keypad. The segment has two buttons (green = off, red = on). It is possible to create a keypad which exactly meets the functional requirements by adding the required number of segments to an access module The segments clearly indicate the state of the system thus enabling its intuitive control. The installed segments allow the user to see clearly which functions their system provides (they are not hidden somewhere in a menu).

Access module: a structural element of a keypad which serves for user identification. The simplest version contains a radio frequency identification chip scanner. A version with a keypad and an LCD display is also available. Jablotron manufactures bus-powered and wireless access modules.

Voice communication segment: allows supplementing the keypad with a voice communication function. By pressing a button on the segment the user can dial a telephone number saved in the system or receive an incoming telephone call from the ARC ? The voice communication segment can be used in a bus-powered version of the keypad. The connecting cable contains 6 conductors (4 for the bus and 2 for audio terminals) in such a case.

Alarm detection: the system is able to react to a break-in, fire, gas leak or flooding. It is also possible to report other dangers (movement in the garden, manipulation of a guarded item, etc.) using suitable detectors. There are accessories for the reduction of false alarms available. It is possible to set in the system that the activation of critical detectors must be confirmed by another detector (or an identical detector must be activated repeatedly).

Visual alarm verification: detectors equipped with a surveillance camera can automatically take and transmit photographs of what is happening in the guarded area.

Personal protection: users can call for help when they are in distress, when they have some health problems or when there is a fire (by pressing a keypad button or wireless button).

Panic alarm: If a user is forced to disarm the system under threat, they can call for help inconspicuously by means of a small change of their code during entering (1*1234 = code, swapping the first two digits for the second two digits of the code - 1*3412 = panic alarm). This function is only active if the codes have a prefix

Event reporting: reporting of all events to the ARC may ensure the timely reaction of professional response teams. The information can also be sent directly to users in an SMS message. Direct reporting is suitable for monitoring electricity outages, the comings and goings of children or employees, etc.

Special reports: SMS reports whose wording and importance can be set independently of other functions. Report sending can be linked to detector activation. It can thus be used to monitor guard service activity, etc.

Remote control: authorized users can dial into the system and control or inspect its guarding performance using a voice menu. SMS instructions or dialling in can be used to switch programmable outputs on/off. After registration the system can also be controlled via web access at www.jablotron.com, (button WEB SELF SERVICE). For a system registration contact your regional distributor.

Users' access rights: It is possible to set for an ordinary user which guarded part in the house they are allowed to control. It is also possible to set authorizations for opening electric locks, doors or for switching on various appliances (by programmable PG outputs). Users prove their identity by applying a radio frequency identification chip or keying in their code on the keypad. Users can change their code if they are authorized to do so. It is possible to use a weekly calendar to forbid users' access outside the set time (e.g. shop assistant's access outside opening hours).

Administrator: It is possible to set a required number of administrators in the system who can then set access rights to ordinary users. Different sections in a building can have different administrators. The default setting is that there is one main administrator in the system always authorized to set access rights to all users (default code 1*1234).

Service technician: uses a special service code (the default code is 0*1010). The technician is authorized to set all system properties using this code. It is also possible to authorize multiple service technicians (if the maintenance system requires it). Service technician's access can be set to require the administrator's consent. An ARC technician is a special case of service authorization. ARC technicians can use their codes to lock access to the parameter settings concerning communication with an ARC.

System settings: all properties are set by a computer using the F-Link software. The computer can be connected locally via a USB cable or remotely via the Internet.

Service mode: a mode in which complete system configuration can be changed. When in SERVICE mode the system is not operational (it does not guard and it provides no user functions). The majority of properties can be changed by a service technician while the system remains in operation (without the need to switch to SERVICE mode).

Appliance control: The system is equipped with programmable PG outputs which can serve for switching various electric appliances on/off. PG outputs can be controlled by keypad buttons, detector activation, events in the system (e.g. by setting a section), SMS instructions, dialling in by an authorized user or access from the web. Switching the PG output on can be signalled both optically and acoustically (by a siren). Switching the output on/off can be reported by an SMS message to users or by data transmission to an ARC.

Door lock control: An electric door lock (connected to a PG output) can be opened by scanning a chip or keying in a code on a keypad. It can be set for individual users which doors they are authorized to open. The output can be blocked by a set section, so that there is no danger of accidentally entering guarded premises. Door opening can be recorded in the system memory (to provide an overview of who went where and when).

Automatic event calendar: It is possible to program the automatic setting (unsetting) of sections and switching on/off programmable outputs using a weekly calendar.

Bus-powered devices: These are connected to the system by a bus cable (4 conductors). The bus ensures both a power supply and communication. Bus-powered devices (detectors, keypads, sirens, etc.) require enrollment to a position (address) in the system in order to work. However, there are also devices which are only connected and which function without having been enrolled to any positions (output relay modules, status indicators, bus separators, etc.).

Wireless devices: A control panel must be equipped with a radio module in order to work with wireless devices. It is possible to install up to 3 radio modules in order to cover a larger space in the building (they are connected by a bus cable). Enrolled wireless devices perform regular activity checks. Monitoring the battery status is also a part of these checks.

GSM communicator: provides connection to a mobile telephone network and to the Internet. The system can thus transmit data to an ARC, report events to users and provide remote access via F-Link SW. The communicator also allows the user to control the system remotely by telephone (voice menu, SMS instructions and dialling-in). When the system has been registered, it is possible to use web services at www.jablotron.com , button WEB SELF SERVICE (remote control, transmission of alarm photographs, etc.). For a system registration contact your regional distributor.

LAN communicator: When it is a component of a control panel, a LAN communicator provides an Internet connection. It enables data transmission to an ARC. When the system has been registered, it is possible to use web services at www.jablotron.com button WEB SELF SERVICE (remote control, transfer of alarm photographs, etc.). For a system registration contact your regional distributor. If the control panel includes both a GSM and a LAN communicator at the same time, it is possible to select which form of communication should be the primary one and which one should be used as a backup.

Telephone communicator: A telephone communicator can be installed into the control panel as a supplementary module. It can transmit data in classic telephone formats to an ARC (CID and SIA). It can also report events to users by calling their numbers and enables remote control of the system by a telephone (using a voice menu). The telephone module is usually used as a backup to GSM or LAN communication.

Sections: The system can be divided into different parts (sections) in which guarding is switched on and off independently. It is thus possible to guard the ground floor and the garage at night, while the bedrooms remain unguarded and accessible. However, a section can also represent a terraced house or a shop in a shopping centre. The users can thus have the feeling that they are controlling their own alarm, but they actually share one system together.

Common section: The guarding section can check automatically whether the slave sections have been set. Example: There are 4 different offices in a building and each of them constitutes an independently controlled section (1 to 4). The fifth section is a corridor which has been set as a common section for all offices (sections 1 to 4). This means the corridor is set automatically if all independently controlled offices are set.

Partial setting of a section: If partial guarding of a section is activated, the system does not react to intrusion detectors for which a so-called internal reaction has been set. It is therefore possible to remain in the guarded area thanks to this. The system does not react to the activation of the corresponding detectors. For example, movement in the residential part of the house is allowed but entry through the door or movement in the garage are reported by the system. If the section is set completely, it reacts to the activation of all detectors which have been enrolled in it.

Detector isolation: A system administrator can deactivate detectors which belong to their section(s) if the need arises. Detector deactivation (bypass) can be performed using a computer or a keypad with an LCD display. It is not possible to deactivate detectors (buttons) which serve for triggering a panic alarm.

Bypass (override): Intervention, by a user, to permit setting when a active detector, tamper and fault condition exists, In such a case the system is not set after entering a setting request on the keypad and the segment of the particular section signals the setting request by flashing. If you insist on setting with an active detector, tamper or fault, it is necessary to repeat the setting request in such a case.

Automatic detector bypass: If some of the detectors are permanently active (e.g. the door is open) during the setting of a certain section, the section is set and the currently active detector is automatically excluded from

guarding. If the detector is deactivated (e.g. the previously open door is closed) the detector begins guarding again. The automatic bypass function can be deactivated.

1.1 Access codes and their default settings

If you control the system with a keypad or using the F-Link software, you have to prove your authorization by entering a numerical code. **The code should be entered in the following format:**

0*nnnn to **300*nnnn**

where: **0 to 300** is a user's serial number (position) (prefix)
***** is a separator
nnnn is a 4-digit code

There are two codes as the control panel default setting:

Service: 0*1010
Administrator: 1*1234

Default codes are filled in automatically by the F-Link software and are therefore not required by the software from the first launch until the change of code. Code setting details are available in chapter 8.5.

For a small system with only a few users the prefix can be disabled, after which the system only accepts 4-digit codes. For disabling the prefix , open the Initial setup tab in the F-Link software. Master and Service codes are set to:

Service: 1010
Master: 1234

Warning: When you disable using the prefix , all codes will be erased. Master and Service codes are set to the default (1234 and 1010). You can enabled the prefix anytime in future. All codes stay the same but a prefix will be added to each code.

2 System size

The scope of the system can be set according to the size of the building and the users' needs.

2.1 External size

The keypad set can be used to determine the external look of the system as seen by its users.

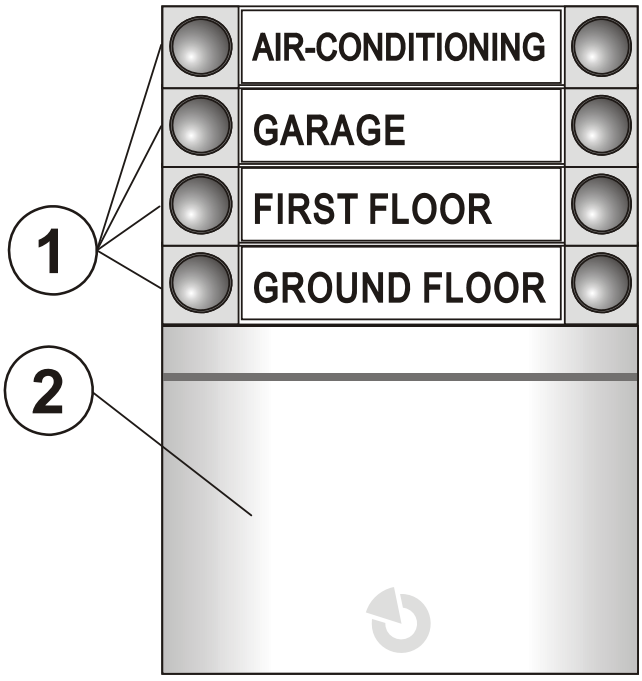


Fig. 1: 1 – control segments; 2 – access module

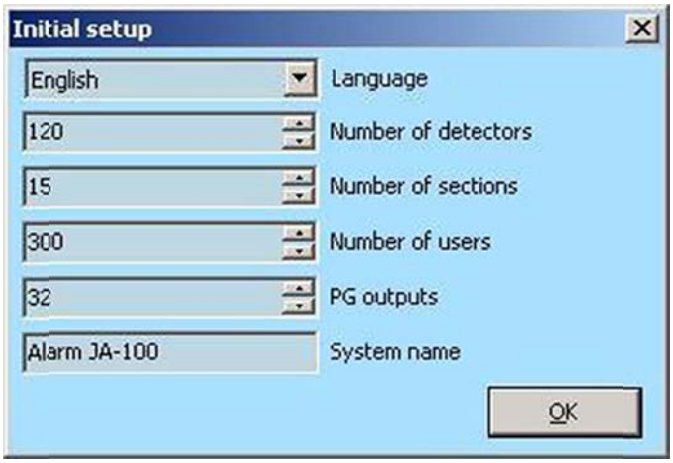
The keypad can have up to 20 control segments. Each segment has two buttons (ON – on the right and OFF – on the left). The segment is used for the activation of section guarding, electrical appliance control or to call help. It can also be used to signal the status of a section or a PG output only.

The access module verifies users' authorizations. The selection of the module defines the means of authorization (RFID chip scanner, keypad + RFID scanner, keypad with a display + RFID scanner, etc.). The module also enables door lock opening by scanning a chip (entering a code). The modules are available in wireless and bus-powered versions.

Keypad configuration is described in chapter 8.3.2.

2.2 Internal area size (scope of the system)

The number of detectors, sections, users and PG outputs can be set in the F-Link software (see chapter 8.1). You can thus create a system for a small flat or for a large building with independently controlled sections. The scope setting automatically enlarges or reduces the internal area setting tables in the F-link software.



3 Control panel type

There are two control panel types available in the JA-100 system. The basic differences between them are shown in the following table.

Property / Type	JA-101K	JA-106K	note
Max. number of detectors	50	120	
Max. number of users	50	300	
Max. number of independently guarded sections	6	15	
Max. number of programmable outputs	8	32	
GSM/GPRS communicator	yes	yes	
IP LAN (Ethernet) communicator	no	yes	
Maximum radio modules in system	3	3	
Maximum internal sirens in system	3	15	
SMS reports	up to 8 users	up to 30 users	
Recommended 12V backup battery	2.6 Ah	18 Ah	
Control panel power supply max. continuous current output	125 mA	1000 mA	Takes control panel consumption into consideration in the calculation of a 12 hour backup time by the recommended battery
Max. possible intermittent current output	1 A	2 A	Max for a period of 5min
Bus terminals	1	2	The JA-106K terminals are mutually isolated, i.e. a short circuit in one bus branch does not affect the other one
Maximum bus cable length	500m	2 x 500m	The JA-106K allows the connection of 2 separate bus branches

More technical data is available in chapter 11

3.1 JA-101K description

This control panel has been designed **for small bus systems** (limited by the battery output) and for **medium-sized systems using wireless communication**.

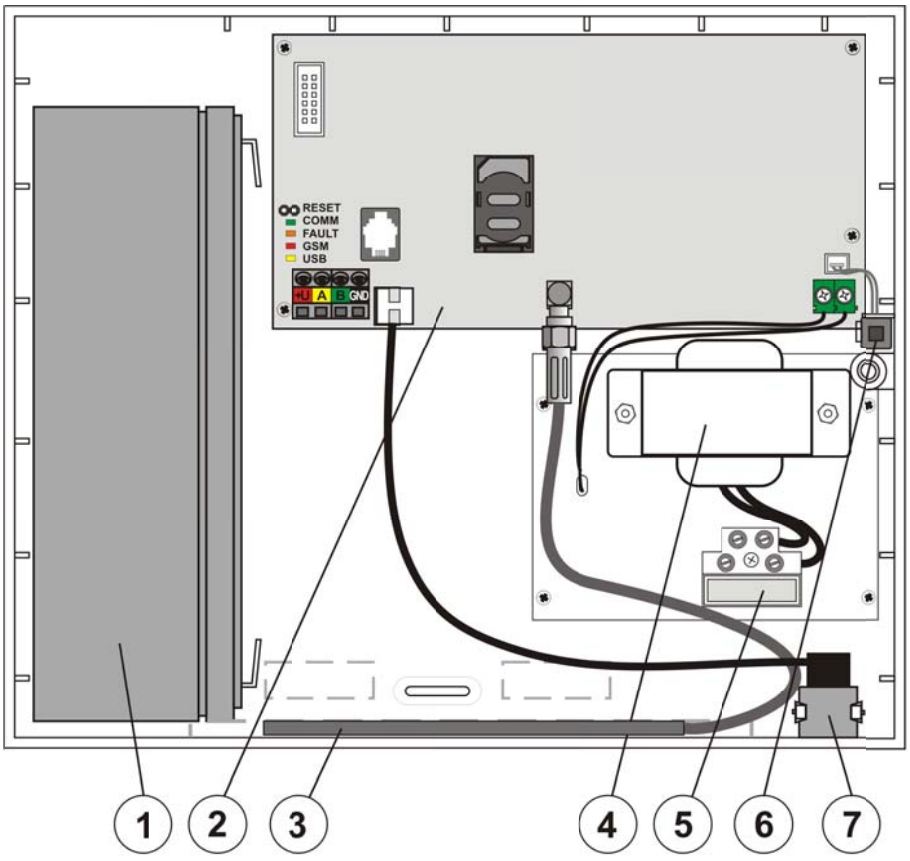


Fig. 2 (control panel internal layout): 1 – backup battery; 2 – control panel main board; 3 – GSM antenna; 4 – power supply transformer; 5 – power supply terminal with a fuse; 6 – control panel box tamper contact; 7 - USB connector for connection to a PC

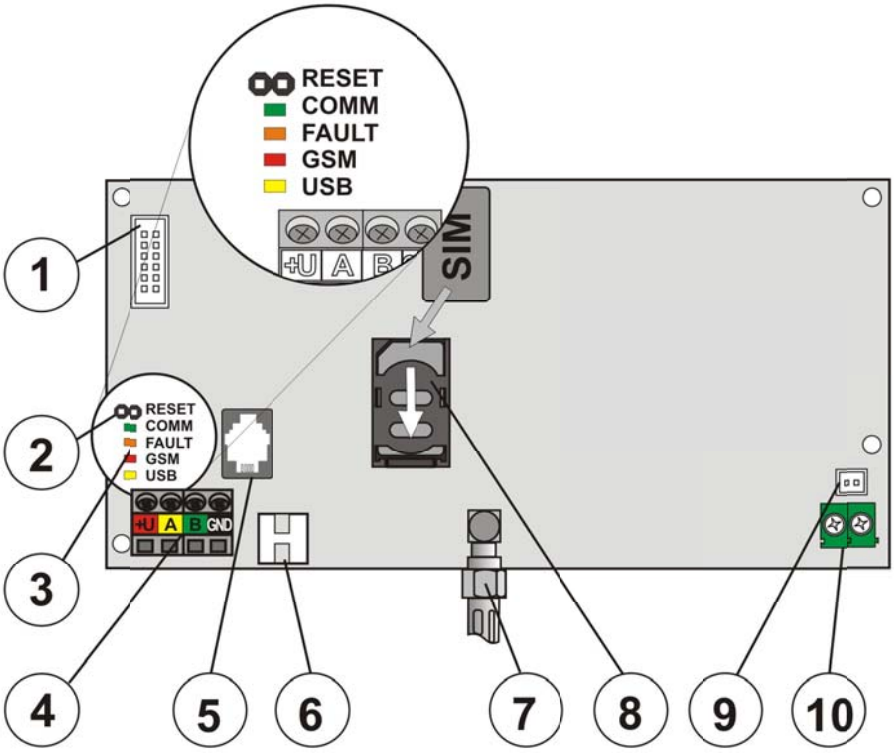


Fig. 3 (control panel main board): 1 – PSTN telephone communicator connector; 2 – RESET jumper; 3 – LED indicators; 4 – bus terminals; 5 – bus connector; 6 – USB cable connector; 7 – GSM antenna connector; 8 – SIM card holder; 9 – tamper contact; 10 – Low voltage AC supply input

3.2 JA-106K description

This control panel is suitable for **medium-sized and large bus and wireless systems**.

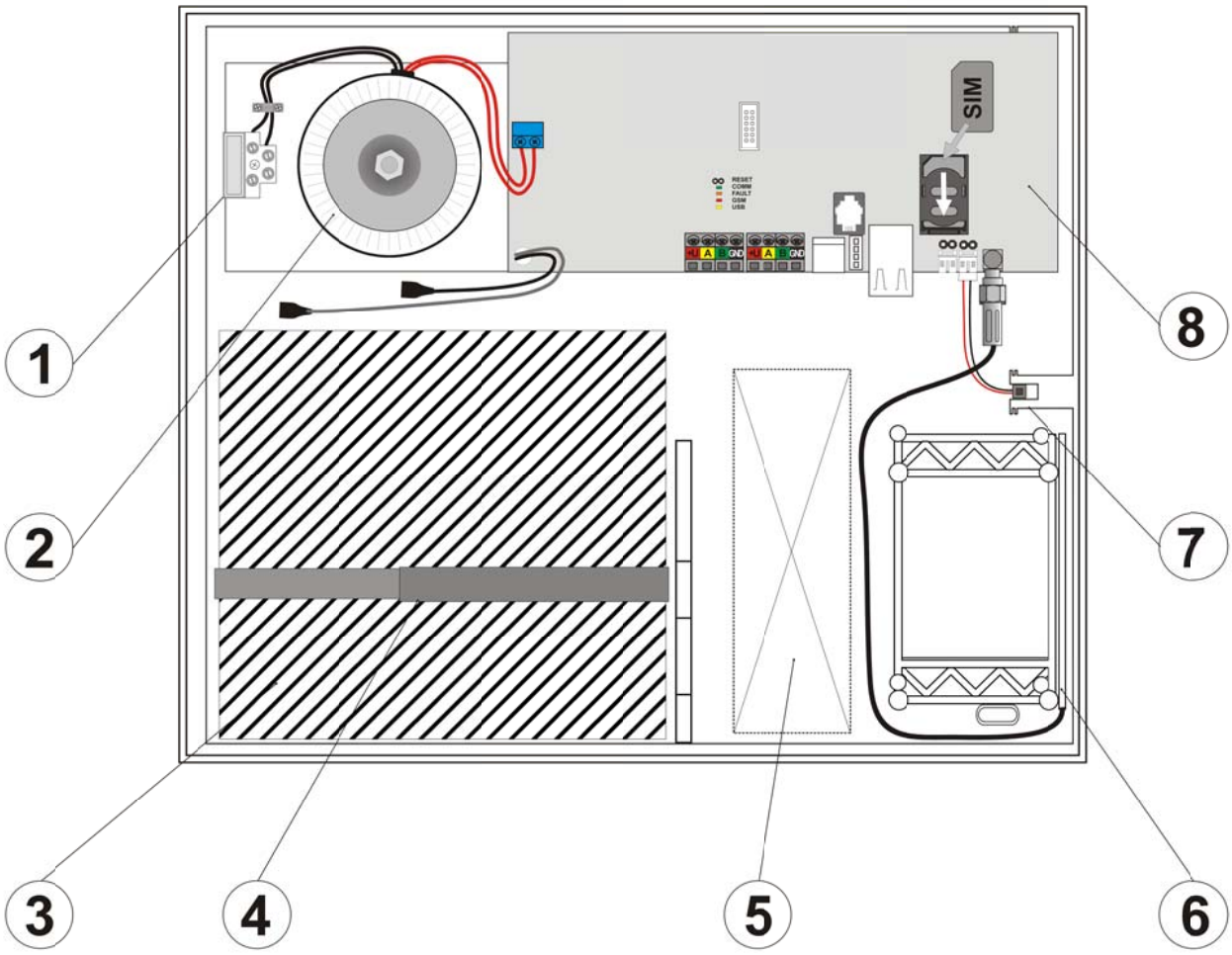


Fig. 4 (control panel internal layout): 1 – power supply terminals with a fuse; 2 – power supply transformer; 3 – backup battery; 4 – backup battery holding strap; 5 – space for cables; 6 – GSM antenna; 7 – control panel box tamper contact; 8 – control panel main board

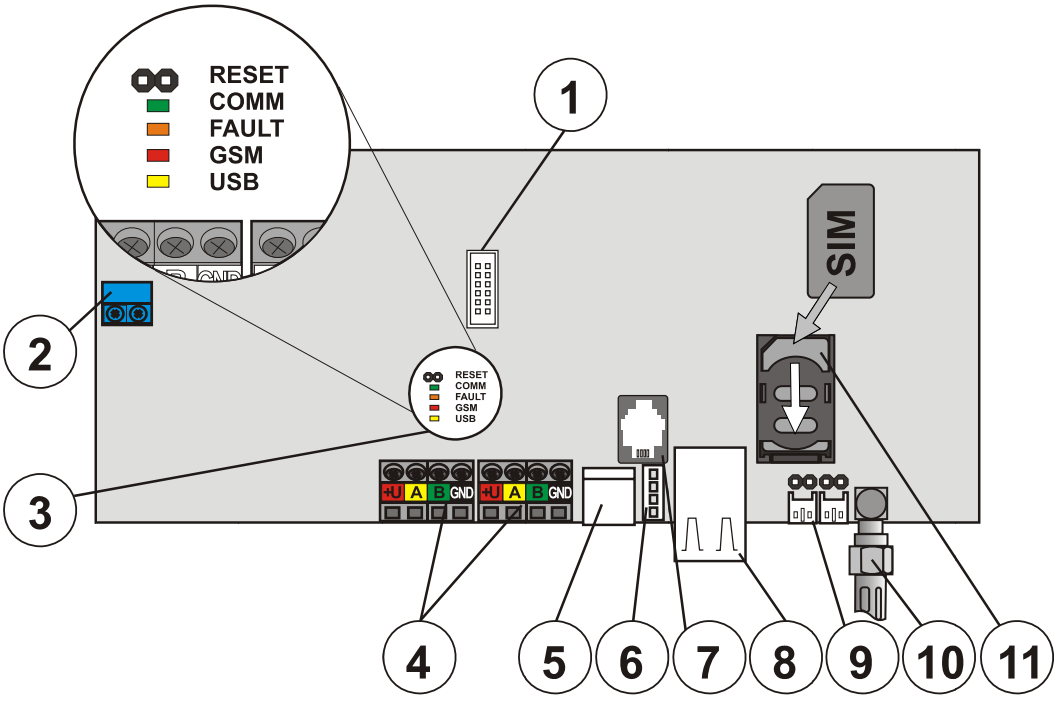


Fig. 5 (control panel main board): 1 –PSTN telephone communicator connector; 2 – transformer power supply terminal; 3 – LED indicators; 4 – two independent bus terminal sets; 5 – USB cable connector; 7 – bus connector; 8 – LAN (Internet) connector; 9 – tamper contact connectors; 10 – GSM antenna connector; 11 – SIM card;

3.3 LED indicators on the control panel main board

All control panel versions are equipped with the following LED indicators on the main board:

COMM	green	flashes during bus communication
FAULT	yellow	indicates system faults (see details in F-Link, keypad with display)
GSM	red	flashes repeatedly in 1s intervals if the GSM network is not available. short repeated flashes indicate a "GSM communicator deactivated" parameter setting
USB	Yellow	indicates USB connection to a computer

4 Before installing the system

- **Find a concealed place (inside the guarded area) with a mains supply for the control panel. There must be good GSM signal reception in such a place (check with your mobile phone). Warning: if a possible intruder knows where the control panel is located, there is a risk that they may damage the system before it manages to send alarm information.**
- **The control panel power supply can only be installed by a person with an adequate electrotechnical qualification. The control panel power supply has double-insulated circuits. The protective earth conductor is not connected.**
- **All control panel power supplies must be switched off completely during installation and connection of system components.**

1. First, think of the layout and the target system settings. Clarify the required means of control with your customer. In the case of more complex systems it is recommended to prepare project documentation.
2. When positioning individual devices, follow their manuals, and the general security system design principles and instructions handed over by the manufacturer at certification training. Should any questions arise, call Jablotron technical support? **The manufacturer shall not be held responsible if the system has been installed or set incorrectly**.
3. Prepare the control panel mains supply – use a solid dual-core double-insulated cable 0.75 to 1.5 mm^2 in diameter. Connect the L terminal to an independent circuit breaker (max. 10 A which concurrently functions as a switch - not secure safe disconnection). **Do not connect the mains yet.**

5 Bus-powered detector installation

Connect JA-1xx Jablotron series bus-powered devices to the system. The connection of devices from other types of Jablotron alarms or from non-Jablotron alarms is only possible by using a suitable connection module (e.g. JA-111H, JA-110M, etc.). The manufacturer cannot guarantee correct functioning when other than the recommended devices are used.

5.1 How many bus-powered devices can be connected to the control panel?

The number is limited by the capacity of the control panel backup battery. Legal regulations require the system to remain functional for at least 12 hours after a power outage. The overall consumption of all bus-powered devices must therefore not exceed the maximum continuous-current output capability of the control panel (see chapter 3). When calculating the total continuous current requirement of the connected devices, add up their standby currents (it is stated in their manuals or you can possibly use the current overview table (see 10.).

5.1.1 Example calculation of the current consumption of a real system

The table shows an example of a small system with 14 devices. The total standby current consumption equals 78 mA. It is therefore possible to use the JA-101K control panel (it allows a max. continuous current of 125 mA). For bigger bus systems use the JA-106K control panel.

The JA-101K is more suitable for wireless systems with battery-powered detectors. Do not forget to add the radio module(s) to the current consumption calculation when configuring a wireless control panel. The continuous current output capability of a control panel can be increased by using an external battery. Details are available in the application sheet (chapter 10.2.).

Device	*Description*	*pcs*	*Standby consumption*
JA-114E	control panel + 3 segments	1	18 mA
JA-110M	magnetic sensor module	2	10 mA
JA-110P	PIR motion detector	6	30 mA
JA-110ST	fire detector	2	10 mA
JA-110A	internal siren	1	5 mA
JA-111A	backed-up external siren	1	5 mA
TOTAL			**78 mA**

5.2 Bus cable

colour	*signal*	*note*
red	+U	Positive power supply line – can only be used as a power supply for JA-100 series detectors
yellow	A	data line
green	B	data line
GND	GND	common line

Bus-powered detectors should be connected by **Jablotron's CC-01 or CC-02 cable.** The cable consists of 4 wires (the colours correspond to the bus terminals). The **CC-02** cable has a smaller wire diameter and is therefore more suitable **for smaller networks with a small amount of detectors.**

When using a shielded cable do not connect the shield wires to any bus terminals! In such a case it is recommended to connect all shield wires to a common floating auxiliary terminal in the control panel and to leave the regular terminals only for the data/supply wires.

5.3 Maximum cable length

CC-01 cable		*CC-02 cable*	
total current	max. length	total current	max. length
50 mA	400 m	25 mA	200 m
100 mA	300 m	50 mA	150 m
200 mA	150 m	100 mA	100 m
300 mA	100 m	200 mA	50 m
500 mA	50 m	300 mA	30 m
The data in the table presumes the worst possible case, i.e. that all the current is drawn at the end of the cable.			

The total **length of all bus cables must not exceed 500 meters**. With the **JA-106K it is 2 x 500m** (it has two separate bus outputs).

The length of individual cables leading from the control panel is limited by the current consumption of the detectors connected to the cable (due to the voltage loss in the wires). Simply speaking, the limitations stated in the table apply. If the current consumption of all detectors connected to one branch of the wire exceeds the total current consumption stated in the table, the current distribution must be divided into multiple separate branches leading from the control panel (see Fig. 6).

When calculating the total current of the cables use the **current consumption for cable selection** (you will find this in the detector manuals or you can use the overview table – see chapter 10.). The methodology for the precise laying of cables for complex bus networks is available in the application sheet (chapter 10.2.).

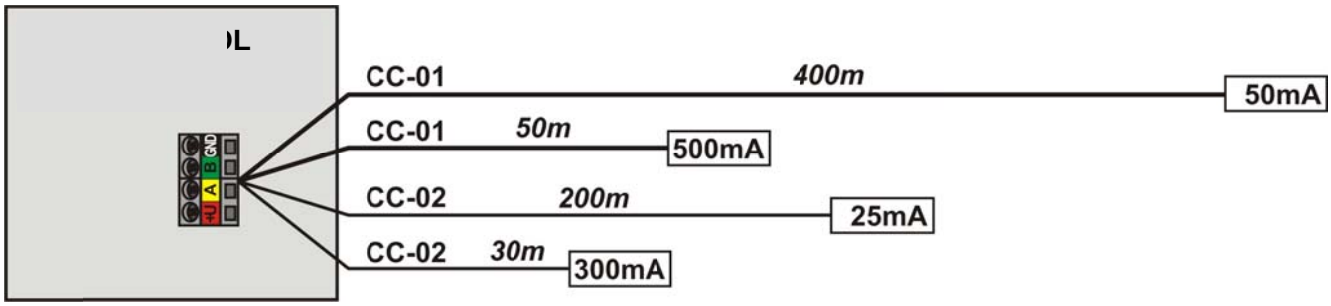


Fig. 6: Maximum cable lengths with regard to current consumption

Greater current consumption has to be divided into multiple separate branches. The CC-02 cable has a smaller wire diameter (can only be used with smaller bus networks with lower currents). However, it should always be kept in mind that the sum of the lengths of all the bus cables connected to one control panel terminal block must not exceed 500m.

5.4 Bus cable connection

1. The control panel mains supply must be switched off completely during the connecting.
2. Follow the installation manuals of individual detectors and devices
3. A bus cable **must not** be connected in a way which creates a **closed loop** on any wire. The cables leading from the control panel can be split but the ends of the individual branches must never be connected together. (**Note:** it is not even possible to connect them to a common GND wire).
4. The bus cable must be installed inside the premises which are guarded by the system. If the cable leads outside the guarded area, such a part must be separated using a JA-110T bus insulator.
5. Use a JA-110Z bus splitter in order to split the wiring.

6 Use of wireless detectors

It is possible to use JA-15x, JA-16x and JA-18x series wireless detectors in the JA-100 system. However, the control panel must be equipped with a JA-110R radio module.

When installing individual detectors, follow their installation manual.

6.1 JA-110R radio module installation

1. The module can be installed in a control panel housing or elsewhere in the building and connected with a bus cable. If the module is installed in the control panel housing, plug it into the internal bus connector using a flat cable with RJ connectors.

The bus connector on the control panel main board has been designed exclusively for the connection of modules located directly inside the control panel box.

2. **More extensive premises can be covered with a radio signal by installing up to 3 radio modules** at various places (e.g. each on a different floor). The system selects automatically which of the modules has the best connection to a specific detector.
3. The radio module should be installed vertically on a wall. It must not be shielded by objects which can disturb its communication (metals, electronics, cables, piping, etc.).
4. When the system has been switched on, **it is necessary to enroll the radio modules first**. Only then it is possible to enroll wireless detectors (see chapter 8.3.1).

7 Powering up the system for the first time

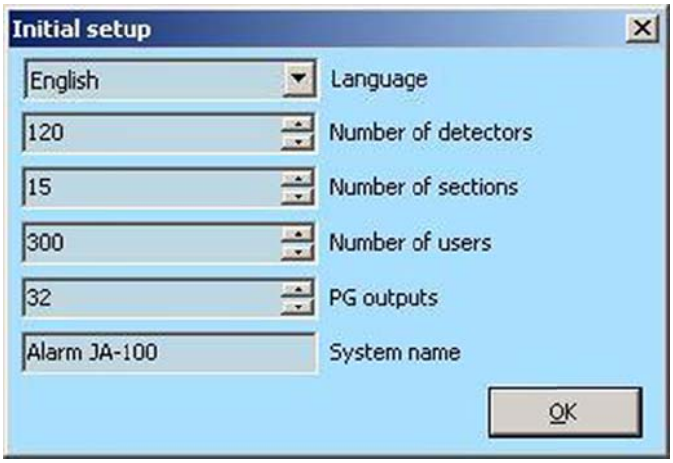
1. Check the bus cable connection.
2. Make sure that a SIM card has been inserted in the control panel SIM holder.
3. Check that the mains cable is correctly connected to the control panel and that the cable has been secured properly.
4. Insert a battery into the control panel and fix it in the box (using self-adhesive blocks or tape). **Warning – the backup battery is charged, it must not be short-circuited!**
5. Connect the battery power supply cables.
6. Switch the power on and watch the LEDs in the control panel:
   a. the green LED starts flashing (bus function).
   b. red LED flashing – connection to GSM network in progress.
   c. the red GSM LED indicator stops flashing – the control panel has managed to establish a connection to a mobile network.
7. When the connected bus detectors start flashing yellow, enroll them to the system (see chapter 8.3.1).
8. Carry out keypad configuration (see chapter 8.3.2.)
9. Set the required functions and test the system.

8 System settings

JA-100 system setting is performed with a computer using the F-Link software. The software is supplied with the control panel or it can also be downloaded from www.jablotron.com (button WEB SELF SERVICE).

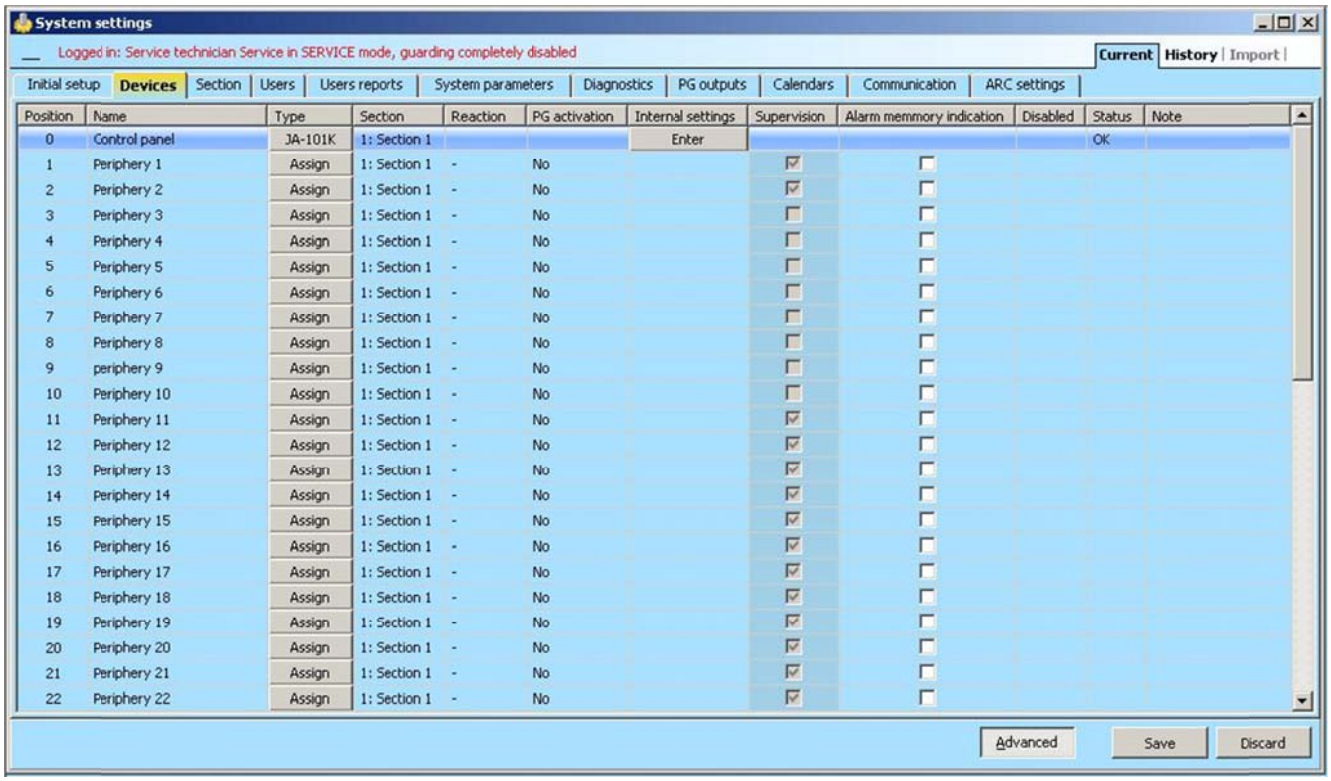
8.1 Launching the F-link software and setting the system size

1. Connect the computer to the control panel using a USB cable – the computer performs initialization of a new USB device (this can take longer when the control panel is connected for the first time).
2. Launch the F-Link software. If the control panel still uses the default settings, a **Initial setup** window opens and the system automatically switches to Service mode. If the control panel has already been set (i.e. its service code has been changed), the software requests a code –



it should be entered in the following format: **0*nnnn** (default code 0*1010). When the prefix is disabled (Initial setup tab) insert only nnnn (default 1010).

3. Choose the required language, set the scope and press OK. **Installation name** is used in SMS event reports (e.g. Grocery store alarm……).
4. The **System settings** window is displayed.



8.2 System settings window

1. The System settings window can be opened and closed by the **Settings** button in the top toolbar.
2. It is possible to switch between the following **tabs** in the card: **Initial setup, Devices, Sections, Users,….**
3. The tab displays the **current control panel settings** uploaded during SW launch. Press the **Import** button on the top toolbar to reupload the current control panel contents.
4. If you want to view the **previous control panel settings, use the History tab** at the top right corner. The history cannot be modified but it is possible to save it in into the control panel (if you want to return to the previous settings). There can be max. 10 previous settings recorded in the history (they are sorted by date and time).
5. Only the **basic functions** of the system can be set for simpler applications. If you need to set **all system functions**, use the **Advanced** button at the bottom right corner. You can hide the advanced settings by pressing the button repeatedly (those settings remain valid even though they are hidden).
6. **If you change the settings, the changes are marked in blue** (the name of the tab also turns blue). The blue markings disappear once you save the changes.
7. You can **save the settings** using the **Save** button (bottom right). When saving the settings into the control panel for the first time, the SW asks you to **enter a filename**. There is a file created in the computer under this name and the settings history is archived into this file (each time new settings are saved into the control panel).
8. **Setting all properties is possible in Service mode** (the system is unset). Service mode can be switched on and off by the **Service** button in the top toolbar.
9. **Some properties can be changed during operation**. The Settings tab can therefore be opened without having to switch to Service mode. However, it is only possible to set the limited options.
10. **The SW contains help bubbles–** if you move the mouse cursor to an option, a description appears. The help bubble can be switched off in the F-link rolldown menu.

Problems that might occur when using the System settings tab

Problem	Possible cause
The displayed settings cannot be changed	– The system is not in Service mode and the given function can only be changed in Service mode – You did not enter a Service code when you launched the SW and you are therefore not authorized to carry out any changes – These settings cannot be changed (Service technician's authorization, control panel position, the device does not support this, etc.), – The ARC settings have been locked by an ARC technician
I cannot find the required parameter	– Only the basic selection is shown, use the Advanced button – You cannot see the whole settings tab – use a scroll bar or enlarge the window
The positions are sorted differently	– When you click on a column header, you can select the column according to which the position should be sorted. Repeated clicking changes to an ascending or descending order
A certain tab is missing	– If the PG output tab is not available, make sure there is not a zero amount of PG outputs set in the Initial setup tab – The ARC tab is not available if you do not have sufficient authorization to access it (it can be locked by an ARC technician)
It is not possible to define the internal settings in the Devices tab	– Check whether the device is correctly connected, enrolled and functional – Service mode is not activated – Some devices have no internal settings
A device cannot be enrolled in the Devices tab	– For wireless devices – you do not have the JA-110R radio module enrolled – The yellow LED indicator must flash regularly in a bus device. If it is not flashing, the device is not connected correctly or it has not yet been activated after powering up the system (this can last up to 90 sec.) – You are trying to enroll a device which requires 2 positions – to the last remaining position – Service mode is not activated
PG output does not react to detector activation	– Check whether the detector transfers information to the control panel in the Diagnostics window – Check the PG output tab and make sure that the output is not blocked by the section status or by a different detector; check whether the PG function column is set correctly

8.3 Devices tab

Here the installed devices are enrolled to the system and their properties are set. The tab displays as many positions as you select in the Initial setup tab. The control panel is enrolled to position 0 automatically and it cannot be moved to a different position or erased.

* Thus marked items are displayed when the Advanced settings are activated.

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

Type – Shows the type of the enrolled device and enables enrolling a new one. **For device enrollment see chapter 8.3.1.**

Section – Defines to which section the device reports possible events (alarm input activation, tamper alarm, failure…).

Reaction – Defines which alarm reaction is triggered by an activation of the device's alarm input. If a device has no alarm input (for example an access module), no reaction can be assigned to it. A complete list of reactions for individual devices is displayed when Advanced settings are activated. The description of all reactions is shown in chapter 8.3.3.

Activates PG* – A device's alarm input can activate a programmable PG output.

Internal settings – Access to internal parameter setting of a device. Individual devices have different internal parameters (some have no parameters). Keypad internal settings are described in chapter 8.3.2. The settings of other devices are stated in their installation manuals.

Supervision* – Allows the user to disable the checking of regular communication with a wireless device (it cannot be deactivated for bus devices).

Alarm memory indication* – Option for alarm memory indication with an LED indicator in a triggered detector. Can be set for detectors which support this function. The indication can also be deactivated centrally for all devices in the Parameters tab – see chapter 8.7.

STOP – An option to completely deactivate a device = bypass (no alarm, tamper alarm, PG activation…). It is not possible to deactivate a control panel or a device which has a Panic reaction set.

Status – Indicates the current status of a device. OK = everything is all right, TMP = tamper alarm, ACT = alarm input activated, ERR = error, ?? = the device is not responding, NO AC = mains failure (or a completely depleted battery), Battery = battery fault or battery is not connected (control panel or device), Charging = charging the backup battery in device or in control panel, Disabled = device is bypassed. More detailed information is displayed by moving the mouse cursor to the device STATUS.

8.3.1 Device enrollment

If an installed device (detector, keypad, siren, key fob, etc.) is to function properly, it must be enrolled to a certain position (address) in a control panel. Some bus-powered devices (output relay modules, status indicators, bus isolators and bus splitters) are not enrolled (the details can be found in the user manual of the corresponding device).

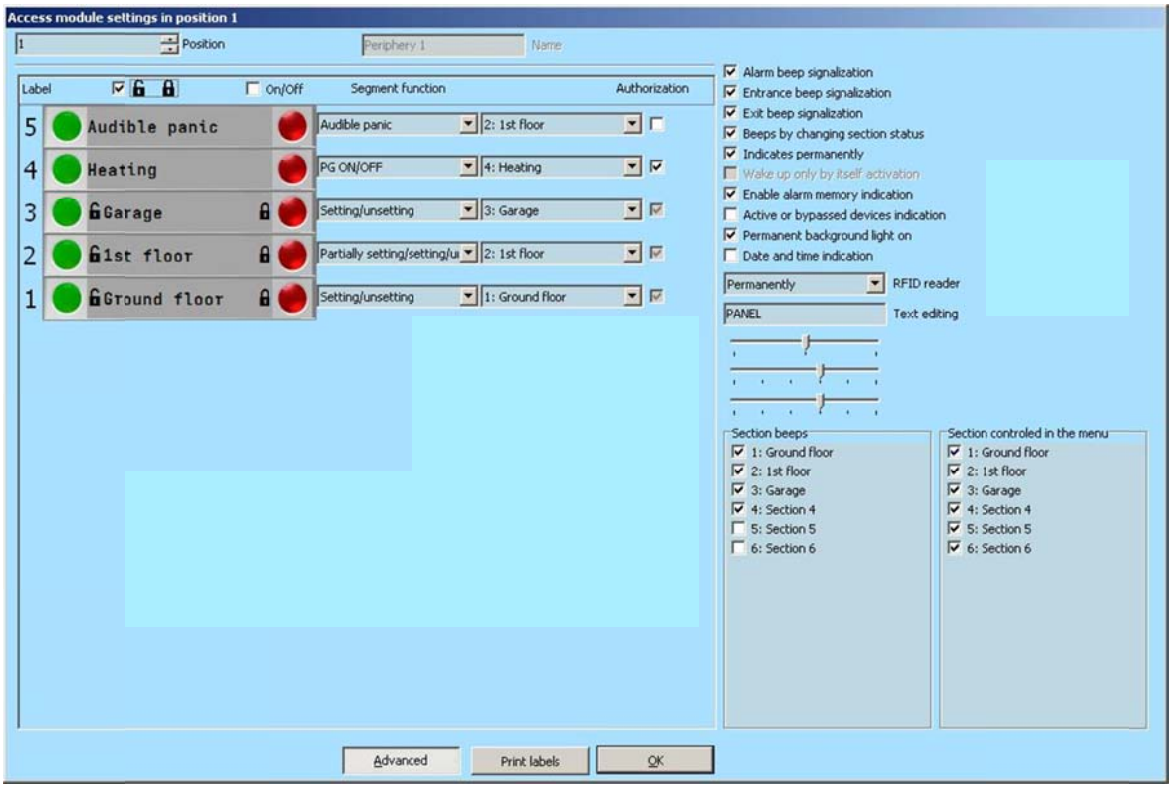
1. A device can be enrolled by pressing the **Enroll** button in the Devices tab in the F-Link software. Enrollment is **possible only in Service mode**.
2. Enrollment can be carried out in several ways:
   a. **by pressing a tamper contact of a bus-powered device** (some devices can be enrolled by pressing a button – see the installation manual of the particular device).
   b. **by inserting a battery into a wireless device** – however, the radio module(s) must be connected and enrolled first. With JA-186Jx or JA-15xJ type remote controls it is just required to press and hold two buttons (paired ones) instead of inserting a battery.
   c. **by entering a production code** (it is stated under a bar code on the main board inside the device). The number can also be scanned with a bar code scanner.
3. **A device can be deleted** by selecting a line in the Devices tab and pressing the Delete key.

Notes:

- Unenrolled bus devices are indicated by a flashing yellow LED. If the yellow LED indicator does not start flashing to indicate an unenrolled device within about 180s after powering up the control panel (initialization takes place), check whether the device is connected correctly.
- Wireless devices with one-way communication do not have enrollment request signalling.
- If you enroll a device to the system by the above-mentioned means, the following available position is offered automatically. You just have to enroll the devices one-by-one in the desired order.
- If you enroll a device to a position which has already been enrolled to, the originally enrolled device is replaced by the new one.
- If you enroll an already enrolled device to a different position, it is moved there.
- If a device occupies multiple positions, it automatically occupies the corresponding number of successive positions during one enrollment (e.g. the JA-110M module which has two alarm inputs occupies two positions). **Note**: beware of any unwanted deletion of the original device enrolled to the second position!
- If you enroll a device to the last possible position, the process of one-by-one enrollment is terminated.
- Free positions are set to section 1 by default. Section selection can be subsequently changed.

8.3.2 Keypad configuration

- Assemble the control keypad first - i.e. attach the required number of control segments to the selected access module (max. 20). Their internal cables must be interconnected.
- Enroll the keypad to the desired position in the system (see chapter 8.3.1.)
- The following window opens when you access the internal keypad settings (Devices tab)



Example of keypad settings:

Note: The window only shows what features are available in the version of keypad connected.

Segment label options – activates the inclusion of padlock symbols by the section control segment buttons or the On/Off symbols on PG output control segments.

Control segment description wording – displays the Section name (from the Section tab) or PG output name (from the PG output tab). The Print labels button (at the bottom) serves for segment label printing to stick on the actual segments.

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

None	The segment is deactivated
Setting / Unsetting	Section control
Partial setting / Unsetting	Allows the activation of partial setting of the section (if it is allowed in the Section tab).
Partial setting / Setting/ Unsetting	Enables the user to select the scope of setting. First pressing the Set button offers partial setting (yellow LED indication), repeated pressing offers complete setting (red indication). The section must have partial setting enabled in the Sections tab in order to use this option.
Section indicator	The segment only displays section status and it does not allow itself to be controlled (suitable e.g. for signalling the status of common sections, stairs, etc.)
Panic	The segment allows the user to trigger a silent panic alarm. When the button is pressed, a panic report is sent from the section to which the function has been assigned.
Loud panic	The segment allows triggering a loud panic alarm. When the button is pressed, the segment flashes red for a period of three seconds (the action can be cancelled by pressing the Unset button at this time). Then a loud panic alarm is triggered in the section to which the segment has been enrolled.
Fire	The segment enables triggering a fire alarm. When the button is pressed, the segment flashes red for a period of three seconds (the action can be cancelled by pressing the Unset button during this time). Then a fire alarm is triggered in the section to which the segment has been enrolled.
Call for medical aid	The segment allows sending a health problem report. When the button is pressed, the segment flashes red for a period of three seconds (the action can be cancelled by pressing the Unset button at this time). Then the segment returns to an idle state and the system sends a Health problem report from the section to which the segment has been enrolled.
Enable PG / Disable PG	The segment allows PG output control
Enable PG	The segment can only be used to activate a PG output (e.g. switch on the lights for a set time)
Disable PG	The segment can only be used to deactivate a PG output (e.g. an emergency STOP button function)
Indicates PG	The segment only indicates PG output status without the possibility to control such a segment

Authorization – user authorization is always required for setting and unsetting the system. For other functions (PG and panic section control) it can be selected whether they can be carried out by anyone or just by an authorized user.

Beeps during… - setting of acoustic indications during control.

Permanent status indication on segments – if disabled, the system status signalling on a keypad goes off 3 minutes after the last human touch.

Wake up only by own controls – If the permanent display of a segment's status is disabled, this option can be used to set that the display can only be restored by pressing the associated keypad. This means that it neither starts signalling if someone presses a different keypad nor if an event occurs (alarm, PG output activation, etc.).

Indicate alarm memory on segments – if enabled, the section segments indicate an alarm memory even when the section has been unset. Alarm memory signalling can be disabled by repeatedly unsetting the section (or setting it again). If a keypad with a display is included in the system, it is possible to cancel alarm indication using the internal keypad menu.

Display active or disabled devices – an option to display information about permanently active detectors (open doors or windows) or disabled detectors (bypassing) on a display. The details can be shown on the display by pressing # (***i***).

Show date and time – an option to show the time on a keypad's LCD display.

RFID scanner – it is possible to reduce scanner activity to 3 seconds after pressing its cover in order to save electricity. The RFID scanner can also be switched off completely.

Keypad text – allows the user to enter text which should appear on the keypad LCD display when no other important information is displayed.

Beeps for sections – it can be specified for which sections the set acoustic signalling should apply.

Sections controlled from the menu – a keypad equipped with an LCD display allows users to set which guarding sections can be activated and deactivated from the menu. It is thus possible to create a keypad which normally controls 2 sections via segments, but if the need arises, it can use the menu to control other parts of a building for which it has no segments installed.

8.3.3 Alarm reaction overview

The system alarm reaction to the activation of an enrolled device input can be set in the Devices tab. Only the types of reactions which are applicable to the particular product are offered for individual devices. Some devices cannot have any reaction assigned (they have no alarm input – e.g. a siren).

Instant	Instant intruder alarm if the detector is set.
Delayed A	Intruder alarm with entrance and exit delay, A timer.
Delayed B	Intruder alarm with entrance and exit delay, B timer.
Delayed C	Intruder alarm with entrance and exit delay, C timer. It is possible to set for this reaction in the Parameters tab that the exit delay can be extended by an active detector which has a C delay set (e.g. for a period of time needed to open the garage door).
Next delayed	Intruder alarm. A detector which provides an exit delay just like delayed detectors in the same section. The entrance delay is provided by the detector only if it has been activated subsequently after an activation of a detector with a delayed reaction. The use of this function makes sense only if a delayed detector is set in the same section.
Internal instant	Instant intruder alarm. The detector fails to react if the given section is only partially armed.
Internal delayed A	Intruder alarm with entrance and exit delay, A timer. The detector does not react if the section is only partially set.
Instant confirmed	Instant intruder alarm – **see Confirmed intruder reaction**.
Delayed A confirmed	Intruder alarm with entrance and exit delay, A timer – **see Confirmed intruder reaction**.
Repeated instant	Instant intruder alarm – **see Repeated reaction**.
Repeated delayed A	Intruder alarm with entrance and exit delay, A timer – **see Repeated reaction**.
Tamper alarm	Tamper alarm at any time (the section does not have to be set).

24 hours	Instant intruder alarm at any time (the section does not have to be set).
Silent panic	Silent panic report (detectors with this reaction cannot be blocked with a STOP button in the Detectors tab).
Loud panic	Loud panic alarm (detectors with this reaction cannot be blocked with a STOP button in the Detectors tab).
Fire	Fire alarm at any time (the section does not have to be set).
Confirmed fire alarm	Fire alarm at any time (the section does not have to be set) – **see Confirmed fire reaction.**
Fire if set	Fire alarm only if the particular section is set.
Health problems	Sends a health problem report.
Setting	Section setting. If the section is common, then all sections belonging to it are concurrently set.
Partial setting	Partial section setting. If the section is common, then all sections belonging to it are concurrently set.
Unsetting	Section unsetting. If the section is common, then all sections belonging to it are concurrently unset.
Siren silencing	Switches off an internal siren with subsequent reporting of the presence of a person in the building.
Report A	Sends a special report (Special reports A, B, C and D can be set in the Reports to users tab). If special report recording in the event memory is enabled, reports are also sent to an ARC
Report B	
Report C	
Report D	
None	With no effect on the building guarding, but the device can serve for PG output activation.

Reduction of false alarms

- special reaction types can be used in installations with increased false alarm risks:

Confirmed intruder reaction – if a detector with a confirmed reaction is activated while panel is set, the system only reports an unconfirmed alarm to an ARC and waits for confirmation by a different detector. An alarm can be confirmed by any intrusion detector in the set section. It is possible to define in the Parameters tab whether the confirmation can come from any set section or whether the alarm must be confirmed by a detector in the same section. It is also possible to set a period of time for which the system waits for a confirmation by another detector (in the Parameters tab). If an alarm is not confirmed during the set time period, the alarm is not triggered. If a confirmed reaction with an entrance and exit delay is set, detector activation sends only unconfirmed alarms. The entrance delay in the section only starts running when some other detector with a delayed reaction is activated. If a confirmed reaction is set, there must be multiple detectors installed in the building (in order to confirm the alarm).

Confirmed fire reaction – if a fire detector with such a reaction is activated, it reports only an unconfirmed fire alarm to the ARC and the system then waits for the confirmation of fire by some other fire detector. It is possible to define in the Parameters tab whether the confirmation can come from any section or whether the fire alarm must be confirmed by a detector in the same section. The period of waiting for a fire alarm confirmation can be set in the Parameters tab. If a fire alarm is not confirmed during the set time period, the fire alarm is not triggered. If a confirmed reaction is set, there must be multiple detectors installed in the building (in order to confirm the alarm).

Repeated reaction – if a detector with this type of reaction is activated, the system waits for a repeated activation of the same detector. The period of time for which the system waits for the repeated activation as well as the period of time for which the detector must be deactivated before a repeated activation can be set in the Parameters tab. If a detector is not activated repeatedly, the system ignores the first activation.

No more than 3 times – all detectors with a set intrusion type alarm reaction have a limited total amount of possible alarms during a single period of guarding. If a detector triggers more than 3 alarms in a row, it is disabled and it does not trigger any more alarms (the same limitations apply to the number of triggered tamper alarms, fire alarms and detector failures). The detector is activated again by unsetting or setting the section. The “No more than 3 times” mechanism does not apply to devices with a set Panic reaction. On the fourth triggering

of the detector, a bypass is activated for that input. The bypass is automatically cancelled the next day at 12:00. This is valid for fire alarms and for flooding.

8.4 Sections tab

Sets the properties of independently controlled guarding sections.

* Thus marked items are displayed when the Advanced settings are activated.

Name – it is used in event text reports and memory listings (e.g. Ground floor, Shop,…)

Common area sections – Allows the user to set that a section is a common area and that it starts guarding automatically if all sections assigned to the common area section are set (suitable for corridors, staircases and other common premises). On the other hand, setting (unsetting) a common-area section can be used to set (unset) all the sections assigned to it. However, there is a condition that the user should be authorized to control all these sections.

Partial guarding* – Enables partial section setting if someone stays inside (the detectors with an Internal reaction type set will not guard – see chapter 8.3.3). It is not possible to use partial guarding in a section without enabling this parameter.

Siren-reported alarm* – An option to disable acoustic alarm signalling in a given section. A siren can also be disabled centrally for all sections in the Parameters tab.

Report when unset* – If a section is unset and no detector is activated in it during a defined period of time, a report saying “Unset section“ is sent. The period of time is set in Parameters – Report when a section is unset for (h).

Limited access time* – It enables the user to set a weekly calendar enabling section unsetting. Two sections with allowed access can be defined for each day. It is possible to set for individual users whether the time restrictions should apply to them – see the Users tab.

STOP – Option to block section guarding (section blocking means that all enrolled devices in this section are disabled collectively). It is not possible to block a section to which a control panel is enrolled.

Status – Indicates the current section status (Unset, Set, Partially set, Alarm, Alarm memory, Blocked).

8.5 Users tab

Sets user authorization.

* Thus marked items are displayed when the Advanced settings are activated.

Name – it is used in event text reports and event memory list (e.g. John Smith).

Telephone number – It is used for event reporting or system control by telephone via voice menu and PG output activation by dialling in. The telephone number must always be entered in the international format (e.g. +420123456789).

Code – A user’s access code is entered in the following format: **p*nnnn (p = position number, * = separator, nnnn = 4 digits)**. When the prefix is disabled (Initial setup tab) only nnnn is used. It is not possible to delete the code in positions 0 and 1 (Service and main Administrator).

Card – Serves for the enrollment of access cards (chips). It is possible to enroll 2 cards for each user. A card can be enrolled by entering a production code (it can be scanned with a barcode scanner). A card can also be enrolled to a position **using the JA-190T reader** (it is connected to a computer USB port).

Authorization – Defines users’ rights. It is not possible to change authorizations for positions 0 and 1. See chapter 8.5.1. for details.

Code changes* – Allows a user to change their four-digit code (not a position number). The option can be enabled only when a code and its authorization have been set. This option is available only for “User” authorization (Administrator, Service and ARC can change their code at any time).

Time restriction* - Enables restriction of users’ access according to a weekly calendar in the Section tab. The option can be enabled only when a code and its authorization have been set. It is available only for “User” authorization (the Administrator always has access rights).

Section – Defines which guarding sections can be controlled by a user (administrator). Administrators can also set codes and user cards in the assigned sections. A section cannot be assigned to a user who is authorized to control PG outputs only. If a user is to be authorized to control a common section directly, they concurrently have to be authorized for all slave sections.

PG – Defines which PG outputs a user is authorized to control.

STOP – Option to block a user. It is not possible to block positions 0 (service technician) and 1 (main administrator).

8.5.1 User authorization level

The system allows setting of the following authorization levels:

User – can activate and deactivate guarding of selected sections and control assigned PG outputs.

Panic – serves only for triggering a panic alarm.

PG only – authorizes the user to control programmable outputs only.

Set – allows activation of guarding, cannot deactivate it.

Administrator – can control guarding and set user authorization in sections for which they are authorized. An administrator in position 1 is always authorized for all sections (main administrator). There can be an arbitrary number of administrators with various section access authorizations set in the system.

Service – Full configuration access for installers. However, switching to service mode can be conditioned by the administrator's consent (in the Parameters tab, see chapter 8.7). There can be multiple service technicians set in the system.

ARC – can set the whole system and can also block service technician's access to ARC communication setting (in the Communication tab, see chapter 8.11). ARC technician's access can be conditioned by the administrator's consent (in the Parameters tab, see chapter 8.7). It is possible to set multiple ARC technicians.

8.6 Reports to users tab

Sets which users should receive event reports which the system sends to their telephone number.

* Thus marked items are displayed when the Advanced settings are activated.

To a user – Enables user selection from a list of users.

SMS alarm – Sends SMS reports if there is any alarm in the selected sections.

Alarm by dialling in – Dials a user's telephone number and sends them a voice alarm message (after sending SMS reports). A voice message can only be set for up to 15 users (calling is time-consuming). Alarm calls can be terminated by alarm cancellation. A user can confirm acceptance of a call by pressing the # button on a telephone (the system does not call any other users then).

SMS setting/unsetting – Sends SMS reports confirming setting and unsetting, or reports about an unset section without any movement (if this function has been enabled in the tab). A setting report is sent 60 sec after setting. Setting and unsetting is not reported to the user who set/unset the system. The only exception is setting a common section (source of setting is the control panel, not a user).

Alarm photo – Sends alarm photographs to a user if surveillance camera detectors are installed.

Failures and service SMS messages – Sends failure SMS reports (Mains failure exceeding 30 minutes, low battery, switching to service mode, etc.).

Report from sections – Defines from which sections the selected events should be reported. This has no meaning for failure and service reporting (these are always reported for the whole system).

PG reports* – An option to report activation and deactivation of PG outputs to a user. SMS texts can be set in the PG outputs tab, see chapter 8.9.

Special SMS reports* – An option to report the activation of detectors with special report reactions (A, B, C, D) to a user. Special report texts can be set by pressing the **Special reports** button at the bottom right corner in the Reports to users tab.

Test – When this button is pressed, a test SMS report is sent to them.

Control transmissions – by pressing this button (bottom right) it is possible to set **Test dialling in** or **Test SMS reports** which are sent to a selected user at a set time every day.

8.7 Parameters tab

Sets parameters and optional system functions.

* Thus marked items are displayed when the Advanced settings are activated.

Date	**Internal calendar setting.**
Time	Internal clock setting.
Standard time/Daylight saving	Automatic switching between standard time and daylight saving time (it can only be

time*	selected for manual time adjustment).
Time adjustment	Means of adjusting the internal clock (Manually, From a GSM network, From Jablotron server).
Notify about different PC clock setting	If the computer time and control panel time differ from each other by more than 1 min, the SW will notify the user about this during the F-Link software (hereinafter referred to as software) launch.
Confirm bypass	When setting with a bypass (deactivated device) or with an active device, the user must confirm this status (repeat the setting request on a keypad). Options: No, instant with delay – active detectors with an instant reaction (system is set automatically after 5 sec.), repeated pressing – active detectors with instant and delay reactions (sets the system after repeated confirming presses), active delayed zone not set – active detectors with instant and delayed reactions (if delayed detectors are active, the system cannot be set)
Card confirmation with a code	If enabled system can be only operated by code and card, assigned to the same user position (regardless of their order).
Siren when partially set	Loud alarm when partially set. Valid only for IW, not EW.
Sirens enabled	Option to disable all system sirens.
Warning by default codes	Sends an SMS warning to a service technician (position 0) saying that default codes remained in the system when servicing is finished.
An administrator restricts Service and ARC	Blocks independent access to the system by service technicians.
Trial operation	All alarms are restricted to 60 sec. and they are reported to a service technician (position 0) by an SMS message, even if the technician has no alarm transmissions enabled. The trial operation is terminated automatically 7 days after the termination of the servicing. A keypad with a display shows “Trial operation“
Service inspection	The system informs about a service inspection request a year after the termination of service mode. It sends an SMS message to an administrator (position 1) and a service technician (position 0). A keypad with a display shows a service request.
Radio interference report	An option to disable interference detection for all radio modules installed.
Panic alarm by entering a different code*	Silent alarm activation by swapping the pairs of digits in the code (example: 1*1234 = code, 1*3412 = panic) – suitable for control under duress.
Alarm confirmation from a section*	If an activation confirmation by another detector is set for a detector, this option can be used to limit the confirmation to the same section only (otherwise it can be confirmed by a detector from any section). This applies both to intrusion detectors and to fire detectors
Siren (IW output) on / off when tamper is triggered	Siren (IW output) on / off when tamper is triggered in unset or partially set system.
Tamper alarm reset by Service*	Alarm memory indication can only be cancelled by a service technician.
Reset enabled*	An option to block control panel resets with a jumper on the main board.
Access the connected control panel automatically upon software launch	Establishes a connection to a control panel automatically if it is connected to a computer with an USB cable.
Switch to service mode automatically upon software launch	When a connection with the control panel is established the software switches the system to Service mode automatically. If any sections are set, it requests their unsetting with a corresponding authorization request. This only applies to cases when the software is being used by a service technician.
Timer setting	A, B and C entrance and exit delays are measured separately in each section. If different exit delays are set for detectors in one section, the longest of the delays is used. When there are different entrance delays, the one which belongs to the activated detector is used. If multiple detectors are activated, the shortest set entrance delay is used. Detectors with a C delay can extend the length of the exit delay (see the option: A detector with a delayed C reaction can extend the exit delay in the Parameters tab)
Alarm length	Alarm length – applies to all sections.
Entrance delay A	A timer.
Exit delay A	A timer.
Entrance delay B*	B timer.
Exit delay B*	B timer.
Entrance delay C*	C timer.
Exit delay C*	C timer.

Waits for intrusion confirmation by another detector*	A period of waiting for the confirmation of an alarm by another detector of the set section. Applies to all detectors with a Confirmed instant / Confirmed delayed A reaction.
Waits for fire confirmation by another detector*	Period of waiting for fire alarm confirmation by another detector. Applies to all detectors with Confirmed fire alarm reactions.
Waits for repeated detector activation*	A period of waiting for the repeated activation of the same detector. The set time must exceed the minimum detector deactivation time before repeating. Applies to all detectors with Repeated instant / Repeated delayed A reaction.
Minimum detector deactivation before repeating*	A minimum period of time for which a detector must be deactivated before it can repeat its activation. Applies to all detectors with Repeated instant / Repeated delayed A reaction.
Report when unset after*	A period of time after which an unset section reports that it is unset if none of its detectors has been activated during this time (the reporting can be enabled in the Section tab – Report when unset)
Maximum C exit time extension*	The maximum time by which the exit delay can be extended by an active delayed detector in the section – if the option is set. A detector with a Delayed C reaction extends the exit delay. If the detector is activated for a longer time, the section is set and the detector is bypassed.
Detector with Delayed C reaction extends exit delay	The so-called garage door function – an active detector with a Delayed C reaction (open door) extends the exit delay in the corresponding section. The maximum possible extension time can be set by the previous option.
Comply with EN50131	This button allows the setting of the system parameters so that they are in conformity with the EN50131 standard (a confirmation is required before the changes apply).
Blocking by alarm/tamper alarm*	An alarm or tamper alarm blocks the system. Unblocking is possible only by access from the ARC or in the case of a tamper alarm by a service technician.

8.8 Diagnostics tab

Serves for the inspection of devices.

* Thus marked items are displayed when the Advanced settings are activated.

Activation memory – shows which devices have been activated since the last deletion of this column. The memory of all devices can be deleted by the Erase memory button (bottom right). The memory of a selected device can be deleted with a right mouse button. Tamper sensor (TMP) activation enjoys the highest priority for recording into the memory.

Status – Indicates the current status of a device. OK = everything is all right, TMP = tamper alarm, ACT = alarm input activated, ERR = error, ?? = the device is not responding, NO AC = mains failure(or a completely depleted battery), Battery = battery fault or battery is not connected (control panel or device), Charging = charging the backup battery in device or in control panel, Disabled = device is bypassed. When you move the mouse cursor over the STATUS of the corresponding device detailed information is displayed.

Battery* – If a device contains a battery, its status is displayed. The backup battery voltage is displayed for a control panel (position 0). If there is no voltage information shown for a wireless device, the device has not started communicating yet – activate its signal transmission (e.g. by a tamper sensor).

Voltage* – If a device is powered by the control panel, a drop in the DC voltage on its terminals is displayed in the SW (applies to the control panel DC voltage line). If it drops by more than 2V, the cable voltage is too low – it has to be solved! The voltage at the control panel output terminals / total current drawn by bus-powered devices are shown at the control panel enrollment position (0).

Radio* – Defines the quality of the signal which a wireless device communicates with. If there is no information, the device has not started communicating yet – so activate its signal transmission (e.g. by a tamper sensor). The value in the control panel row indicates the GSM signal strength.

8.9 PG outputs tab

Sets programmable output functions.

* Thus marked items are displayed when the Advanced settings are activated.

Name – Output description (e.g. Air-conditioning, Warehouse door,…)

Logic – option to set an inverse output logic.

Function – Defines how an output should behave after its activation.

On/off – permanently switches the output on/off.

Impulse – time restricted activation of the output (the period of time can be set in the Time column).

Copy – copies activation of a detector or internal status.

Copy after delay – triggers only when the condition required for activation lasts longer than it has been set in the Time column (suitable e.g. for indication that someone has forgotten to close the garage door).

Copy with an overlap – copies detector (or internal status) activation and extends it by a period of time set in the Time column (suitable e.g. for corridor lighting after opening the door).

Time – Time setting for Impulse, Copy after delay and Copy with an overlap functions. Time should be set in the following format: hh:mm:ss.

Activation – Access to a PG output activation map – see chapter 8.9.1.

Block PG – Allows blocking the output with a section status or with a detector. Blocking prevents the output from activating and if it has already been activated, it deactivates it permanently. Suitable e.g. for blocking a door lock if a particular section is set.

Reports* – Sets the wording of SMS reports which are sent when a PG output is activated or deactivated. It is then possible to set to whom the reports should be sent in the Reports to users tab.

Record PG into the memory* – Allows recording of output activations into an event memory and thus also their reporting to an ARC (e.g. for monitoring users' access to a monitored door).

STOP – An option to block an output.

Current status – Information about the current status of an output.

Test – An option to control an output manually using a computer. It activates (or deactivates) a particular PG output with regards to the selected function.

8.9.1 PG output activation map

An activation map which can be accessed by the Activation option in the PG outputs tab. The map defines which control mechanisms each output should react to.

Authorized users – Defines which users are authorized to control the keypad output (using segment buttons). The settings are interlinked with the Users tab.

Output activation by an authorized user by mere authorization. This allows the setting of up to 5 keypads – which can activate a PG output by mere authorization (scanning a chip or entering a code). The function is intended for door lock opening. (i.e. no pressing segment buttons is required).

By dialling in from users – Sets which users are authorized to activate the output by dialling in from their telephone number (the telephone numbers are set in the Users tab). The caller's phone has to have caller ID enabled otherwise the system cannot indentify the caller and does nothing.

By a device – Enables PG output activation by a system device (detector activation, keyfob button pressing, etc.). This setting is interlinked with the Devices tab.

By internal status – Allows output activation by an event in the system (e.g. setting, alarm, etc.). It is possible to set a mask of sections from which the signal should be accepted as the internal status (OR logic).

By a keypad segment – Shows an overview of keypads in the system. Using the Settings button (under the list of keypads) it is possible to access the internal menu of the selected keypad and modify its settings – see chapter 8.3.2.

SMS instructions – Enables setting of text instructions for PG output activation and deactivation by telephone. The reception of the corresponding SMS has a similar effect to pressing an ON or OFF button on a keypad segment. For PG output control use the SMS sequence : code _ command , for example 2*2345 lights on.

Warning: PG outputs are not functional if the system is in Service mode (all PG outputs are deactivated when the system switches to Service mode).

8.10 Calendar tab

Here you can set a schedule of actions which the system should perform automatically and regularly.

* Thus marked items are displayed when the Advanced settings are activated.

Days in a week – Defines on which day(s) the given action should be carried out.

Time – Defines what time the given action should be carried out on the selected day.

Guarding – Allows the user to set an action associated with building guarding.

Sections – Defines in which section(s) a guarding type action should be carried out.

Controls PG* – Allows the setting of PG output activation or deactivation.

PG number* – Defines which output(s) should be activated or deactivated.

STOP – An option to block particular actions.

Notes:

- An action can control guarding and PG outputs concurrently.
- Switching an electric appliance on/off for a certain period of time is possible in two ways. You can either set an action for PG output activation and an action for PG output deactivation or set an action for activation only and then set an impulse of the required length for the PG output.

8.11 Communication tab

Primary connection to WPP – Selection of a channel which the control panel uses for communication with the Jablotron server.

Voice report calling priority – Selection of a channel which the control panel uses for the voice reporting of events.

Registration key – A unique control panel registration number.

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

Voice menu without a code – When controlling the system from an authorized telephone the user does not have to enter their code (they are already authorized by calling from their telephone).

Forwarding received SMSes– Select a user to whom messages are to be forwarded, e.g. SMSes with no valid system commands.

All ARCs enabled – An option to disable communication with an ARC completely – not available if an ARC technician restricts access to the ARC settings.

GSM restart – A button for logging the GSM communicator out of the network and logging it in again. The logging in to a GSM network can take tens of seconds (depending on the operator, signal strength, etc.).

8.11.1 GSM settings button

Serves for GSM communicator setting.

***** thus marked item is set automatically when the control panel is switched on if a functional SIM card has been inserted in it before (Jablotron server service)

GSM communicator – an option to disable a communicator.

GSM signal – information about signal strength in percent (the measurement takes place every minute). The signal strength should be at least 30% to ensure correct functioning. If you have trouble with GSM signal quality, it is recommended to test a SIM card from a different operator. It is not recommended to use a directional GSM antenna or a high gain antenna with the communicator (the module would thus communicate with a single cellular base station only = unstable communication).

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

Network APN* – GPRS data communication setting. Data communication ensures Jablotron server services, service technicians' remote access, communication with an ARC, etc. Besides the APN setting, the SIM used must allow data transmissions.

APN*user – Name (do not enter if not required by the network)

APN*password – Password (do not enter if not required by the network)

Call limit in min/day – Restricts the scope of calls to 5 - 500 minutes per day.

Daily SMS limit – Restricts the number of sent SMS messages to 5 - 500 SMS per day.

Remote control by telephone – sets the option to control the system remotely via a voice menu. If set for individual users, the menu can only be accessed from the set users' telephones (it is even possible to allow users to access the voice menu without having to enter their access code. This is done in the Communication tab – Control without a code option). If the "Anyone" option is set, the voice menu can be accessed from any telephone. However, the user's access code is always required upon access.

Remote control by sending SMS – sets the option to control the PG outputs remotely by SMS instructions. If set for individual users, the system only accepts instructions from the set users' telephones (it is even possible to allow users to send SMS instructions without having to enter their access code. This is done in the

Communication tab – Control without a code option). If the “Anyone” option is set, SMS instructions can be sent from any telephone, but it is always necessary to enter the access code.

Credit – limit – an option to set a bottom limit for an automatic credit inquiry on a pre-paid SIM card. If the remaining credit is below this limit, the system sends an SMS to the person for whom the **Failures and service SMS option has been set**. Warning: **It is not advisable to use a pre-paid card in the system** – there is an increased communication failure risk.

SIM credit sequence – An instruction for an automatic inquiry about the remaining credit. Enter the correct sequences obtainable from the GSM network operator used.

Credit – position in the SMS text – Position in an SMS message from the GSM operator in which the numerical data representing the remaining credit is located (an integer counting how many positions along the message the value starts).

Credit – inquiry period – sets how often the system should inquire about the remaining credit (can be set from 0 to 99 days, where 0 means the function is disabled).

Number for outgoing calls to maintain SIM card validity – if a pre-paid SIM card requires outgoing calls to maintain its validity, it is possible to set a telephone number which the system dials in automatically if there has been no outgoing call from the system for a period of time exceeding 90 days (the system terminates the call after 10s)

8.11.2 LAN setting button

Serves for LAN communicator setting (if the control panel contains it).

LAN transmission – option to disable LAN communication.

Get an IP from DHCP server – automatic network parameter setting. If the network does not support this function, the corresponding parameters have to be entered manually. Manual setting is possible only when this option has been disabled.

8.11.3 Keypad voice module button

If a segment allowing voice communication is used in the system keypad, the telephone numbers can be set here. The numbers should be entered in international format (e.g.: +420123456789).

Tel. no. for calling from a keypad – the system dials this number when a button is pressed on a keypad voice segment.

Tel. no. for calling a keypad – if an incoming call comes from this number, the systems puts it through to a keypad voice segment.

Backup telephone number for calling to keypad – if an incoming call comes from this number, the system puts it through to a keypad voice segment (i.e. 2 different numbers can be set for calling the system).

8.12 ARC tab

Sets communication with up to 4 ARCs. If service technicians’ access is restricted in the Communication tab, the setting can only be carried out with ARC technician’s access authorization.

Transmissions enabled – option to disable set communication

The following ARC should serve as a backup – If enabled, the following ARC channel should be used only if it is not possible to transmit the data to this channel.

Protocol – transmission protocol settings

Communicator – if the set protocol can be transmitted by multiple means, this option sets the communicator type

Domain 1 (tel.1) – Setting of the main domain (URL or IP address) or the main telephone number depending on the protocol used

Domain 2 (tel.1) – Setting of a backup domain (URL or IP address) or a backup telephone number depending on the protocol used

Section ID – defines the building identification (either for the whole building or for individual sections)

Reported events – selection of reported event types and the option to set supplementary reports (PG outputs, special reports A to D)

Timing – setting of time limits for transmissions and connection check period setting.

Transmission test – When pressed, the periodical connection check is transmitted via the corresponding protocol.

9 Control panel reset

You can return the control panel to its default settings by the following means. Disconnect the USB cable and the battery and switch off the mains. Then connect the RESET pins on the control panel main board (use the jumper supplied with the control panel). Switch the control panel mains on and wait until the red and yellow LED indicators at the jumper go off (about 5 s). Then disconnect the jumper (the control panel returns to its default settings). Note: If resets are disabled in the Parameters tab, it cannot be carried out using the above-mentioned method.

10 Additional information

10.1 An overview table showing the current consumption of bus-powered devices

If the current consumption stated in the manual supplied together with the device differs from the data stated in this table, the data in the manual should be used.

Device	Standby current (mA)	Cable selection current (mA)	Note
JA-114E Access module with an LCD display, a keypad and an RFID	15	50	
JA-113E Access module with a keypad and an RFID	10	20	
JA-112E RFID access module	10	15	
JA-192E Control segment	0.5	0.5	
JA-110P PIR motion detector	5	5	
JA-110B Glass break detector	5	5	
JA-110M Magnetic detector connection module	5	5	
JA-110ST Fire detector	5	10	
JA-111H Detector connection module	5 + current consumption of the connected ext. detector	5 + current consumption of the connected ext. detector	
JA-110N PG power output module	5/45	5/45	Relay off / on
JA-111N PG signal output module	5/25	5/25	Relay off / on
JA-110A Internal siren	5	30	30 mA during alarm
JA-111A External siren	5	50	During AC failure without BATT recharge, then 5-50 mA depending on BATT recharge
JA-110I Section / PG indicator	5	5	
JA-110T Bus isolator module	5	5	
JA-110R Wireless communication module	25	25	

10.2 Application sheet

An application sheet is available to certified technicians at www.jablotron.com (button WEB SELF SERVICE).

11 Technical specifications

Parameter	JA-101K	JA-106K
Control panel mains	230 V / 50 Hz, max. 0.1 A, protection class II	230 V / 50 Hz, max. 0.2 A, protection class II
Power supply	type A (EN 50131-6)	
Backup battery	12V; 2.9Ah (2.2 to 7Ah)	12V; 18Ah (7 to 35Ah)
Maximum time needed for battery recharge	72 h	72 h
Max. continuous control panel current output	400 mA	1.2A
Max. continuous current output for 12 hour backup	125 mA with a 2.6Ah battery	1.2 A with an 18Ah battery
Max. number of enrolled devices	50	120
LAN communicator	no	Ethernet interface
QUAD-BAND GSM communicator	850/900/1800/1900MHz	
Operating frequency (with the JA-110R module)	868.1 MHz ISM band	
Invalid code-entries exceeded	After 10 incorrect code entries	
Event memory	approx. 1 million of the latest events including date and time	
Security rating	grade 2 according to EN 50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3	
Operating environment	class II indoor general (-10 to +40°C), according to EN 50131-1	
Radio transmission conformity	ETSI EN 300220 (R module), ETSI EN 301 419-1, EN 301 511 (GSM)	
EMC conformity	EN 50130-4, EN 55022, ETSI EN 301 489-7	
Health and safety conformity	EN 60950-1	
Can be operated according to	ERC REC 70-03, ERC DEC (98) 20	
CLIP protocol (caller ID + SMS)	ETSI EN 300 089	

JABLOTRON ALARMS a.s. hereby declares that the JA-101K and JA-106K control panels are in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The original of the conformity assessment can be found at www.jablotron.com.

Note: Although this product does not contain any harmful materials we suggest you return the product to the dealer or directly to the producer after use. More detailed information can be found at www.jablotron.com - Technical Support section