SAFETY WARNINGS

Short programming manual is recommended for professional installers who are experienced in the installation of intruder alarm systems and have already read the SECOLINK wiring manual. The wiring manual must be read before the installation to avoid accidents with high voltage and temperature.

The device must be connected to AC power supply with Protective Earthing. Cable color and purpose: Phase or Live line (L) - black or brown cable, Neutral line (N) - blue cable, Protective Earth line (PE) - green cable with a vertical yellow stripe. Only double isolated cables with cross-sectional area of no less than 0,75 mm^2 shall be used for 230V power supply.

Additional automatic two-pole circuit breaker should be installed in AC electric power circuit in order to prevent over-current and short circuits. The circuit breaker should be placed close to the system's housing and should be easily reached. Full shutdown could be done by turning off the 230V AC main power supply with automatic two-pole circuit breaker and by disconnecting the battery. Before performing any installation work or maintenance ALWAYS disconnect the device from the power supply.

DEFAULT TEMPLATE

The system is shipped from the factory with specific default values (further default template) suitable for a typical installation. If the default template is suitable for your installation, then programming can be simplified. If template is not suitable for your installation, then you can easily customize this default template with the software MASCAD. Download MASCAD at www.secolink.eu prior to installation:

1.Connect the keypad to your computer using a USB cable (keypad should not be connected to system data bus).
2. Download default template from the keypad to software MASCAD (use the tab *Project data sending/receiving*).

Note: the default template can be different for different countries. Check a sticker on the keypad for a country prefix or pre-installed template code. Example: KM24G_EN.

3.Once you customize the predefined template, you can use it to program an individual system or thousands of systems.
4. DO NOT FORGET to upload the customized template (further project) back to the keypad (use the tab *Project data sending/receiving*).

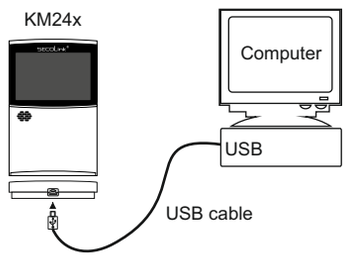


Fig. 1 USB connection

STARTING THE SYSTEM WITH A SINGLE KEYPAD

Upon power-up of the system, the keypad will display a phrase *First Start Press [ENT].* It means that the keypad is ready to run an automatic module registration procedure and later send the default template (or customized project) to the control panel and all successfully registered system modules.

On keypad's LCD screen:

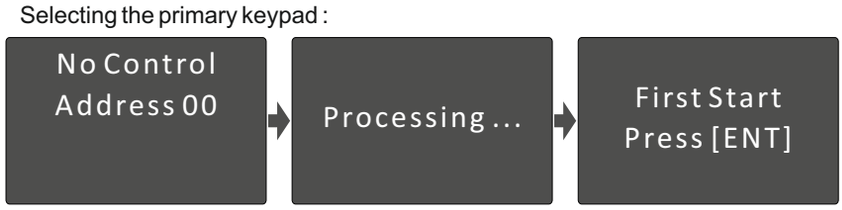
Press the [ENT] key. | Entering Service. | Registration of modules is in progress. | Template is being sent to the system. | Leaving Service.

STARTING THE SYSTEM WITH MULTIPLE KEYPADS

No Control Address 00 phrase will display upon power-up of the system with multiple keypads. It means that the keypad has the same address in the system as the other keypads or modules. Press the [∗] key on a keypad which will become the primary keypad. The primary keypad should become the one which has a customized project OR it could be any keypad if the default template is not customized. When the [∗] key is pressed the keypad will emit a short audible signal and a phrase *First Start Press [ENT]* will appear on the screen.
Simply press [ENT] if the primary keypad contains a customized project with precise module addressing. If the primary keypad contains just a default template, then use keys [1], [2], [3], [4], [5] to manually assign the address to each keypad. When all addresses of the keypads are assigned, return to the primary keypad and press the [ENT] key. All keypads will be registered according to their addresses, which were given manually. **Note:** the keypad will remain unregistered if you will forget to assign the address.

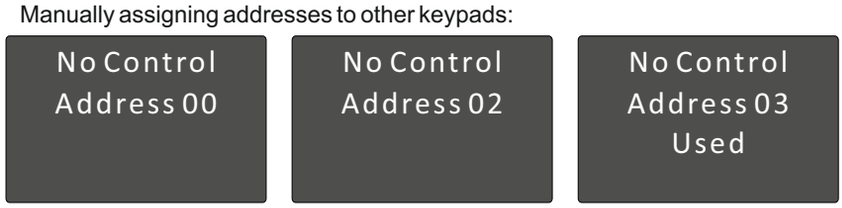
For a small system with a few keypads, it is recommended to choose addresses of keypads in 01 - 04 range, and for a large system in 01 - 04 and 10 - 15 ranges. This is done in order to not disturb the default addresses of other modules with the addresses of the keypads.

Selecting the primary keypad :



Press the [∗] key. | Processing ... | Primary keypad

Manually assigning addresses to other keypads:



Enter the address | Assigned address 02. | Used. Choose another.

DEFAULT ADDRESSES OF THE MODULES

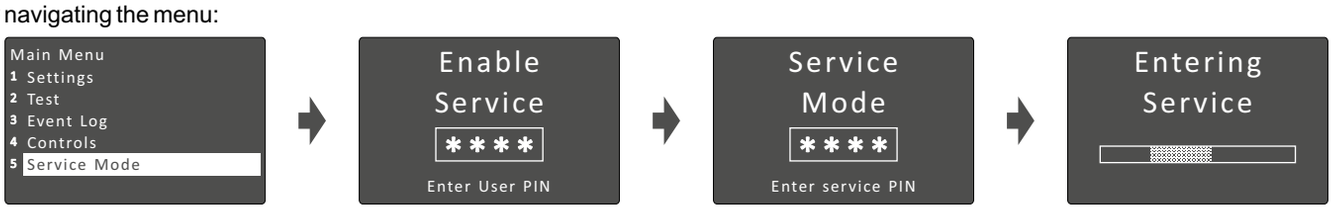
System manufacturer has provided the modules with default addresses assigned to them. This is done in order to simplify the process of registration for most frequently used combinations of the system modules (such as PAS808M, KM20B, GSV6U or PAS816, KM24A, EXM800, EXT116S, GSV6U). While registering modules of a different type, you will not need to enter serial numbers of each module, as the system will automatically assign default addresses for the modules that are listed below:

- For all control panels - address **00**;
- For the keypad **KM20B, KM24, KM25** - address **01** or **03**;
- For the keypad with a temperature sensor **KM24A, KM24G** - address **02** or **04**;
- For extra power supply module **PWR20** - address **04** or none;
- For the zone/PGM expansion module **EXM800** - address **05**;
- For the remote control module **EXT016**, **EXT116S**, **EXT216** - address **06**;
- For the proximity reader **PROX8** - address **06**;
- For the GSM/GPRS, LAN communicator **GSV6U**, **GSVU, LAN800** - address **07 or 11** (for GSVU);

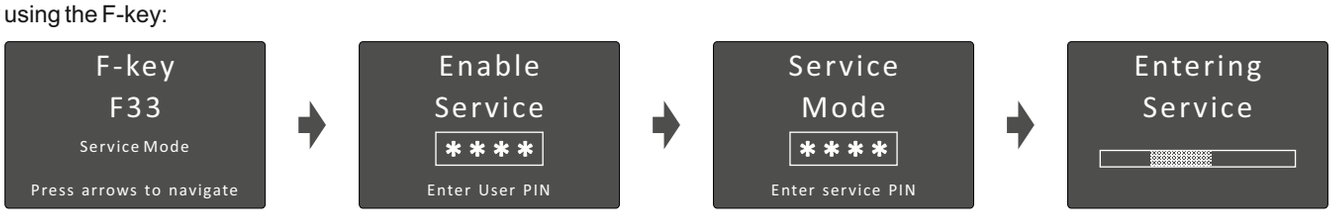
ENTERING SERVICE MODE

It is recommended to use the computer and software MASCAD for the installations with few partitions and more than 10 zones. For simple installations it is more efficient to change the template manually by using the LCD keypad. Changes should be made in service mode when the system is disarmed.
For security reasons permission to access the service mode has to be enabled by entering user's PIN (default PIN codes: first user - **0001**,service - **0000**). There are 2 ways to enter the service mode:

- by navigating the menu:



- by using the F-key:



There is an option to set the system without entering the required user's PIN that is needed to access the service mode. To do this, you will need to modify the template by using software MASCAD:

1. Connect the keypad to your computer using a USB cable.
2. Establish a connection with the computer. Using the keys with arrows go to the menu: *Service Mode* ▸ *Project Loading* ▸ *Start connection with PC*.
3. Download data from the keypad to software MASCAD (use the tab *Project data sending/receiving*).
4. Go to *F-key* tab.
5. Click on row *F33 SERVICE Mode* and uncheck the box *User PIN required* from the settings (see Fig. 2).
6. Upload the customized project back to the keypad (use the tab *Project data sending/receiving*).

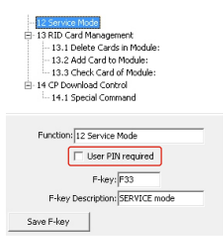


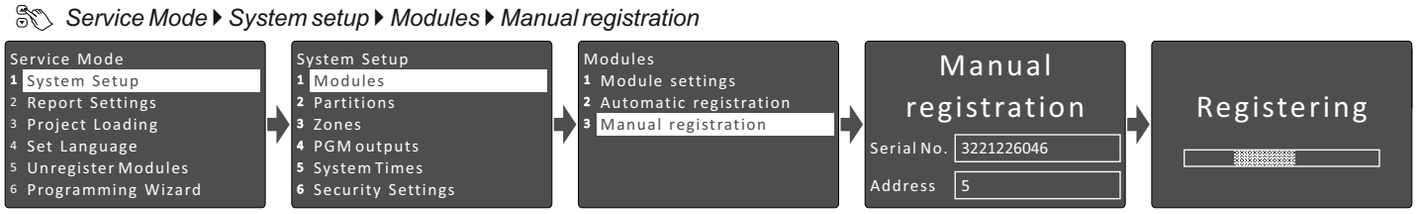
Fig. 2 Tab *F - keys*

MANUAL REGISTRATION OF MODULES

Control panel PAS808M supports up to 7 modules and control panels PAS816, PAS832, P16, P32, P64 supports up to 15 modules (incl. enabled virtual modules EXT116VM on P series control panels). If there are a few modules with the same default addresses in the system (for example: several EXM800 or GSV6U and LAN800 modules), only the module with a greater serial number will be registered during the module registration procedure. All remaining modules (not registered) must be registered manually.
To register the module, an installer must enter the service mode, type in a 10 digit serial number, which is on the module's label (see Fig. 3), then press the [ENT] key to jump to second row, enter module address of the system, and press [ENT] again to start registration.

Fig. 3 EXM800 label

Service Mode ▸ *System setup* ▸ *Modules* ▸ *Manual registration*



The module will start to flash its address with the green LED after a correct serial number and address is entered. If a mistake was made while entering serial number, the module will stay unregistered. If a mistake was made while entering the address which is used by another module, then the new module will overtake this address and the other module will stay unregistered.

Note: a registered module will slowly flash its address on a green LED, which is located on the module's PCB (excluding keypads and a control panel).

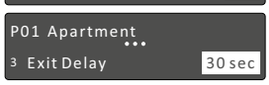
PARTITIONS

Partitions allow you to break up a large area into smaller sections. This feature is useful to disarm certain areas while leaving other areas armed, or to limit access of certain areas to other users.

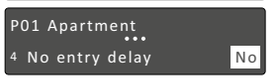
Service Mode ▸ System Setup ▸ Partitions

It is recommended to give an appropriate name to a partition. The system will use it when sending SMS or when showing status of the partition on keypad's LCD. For next character possition press [▲] or [▼] key. Move the cursor on the wrong character to delete it and press [0].

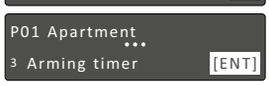
The alarm system can be divided into 4 partitions for operating flexibility. Confirm the activation of a new partition by selecting *Yes*. Press [*] or [7] for the next partition.



Exit Delay time can be different for each partition in control panels PAS816v3, PAS832v3, P16, P32, and P64.



This setting changes entry delay time in partition to 0 seconds (excluding PAS808M). User should remotely disarm the system before entering partition.



In this menu it is possible to assign the timer(s) to partition. Auto-arming starts at a specific time of day and arms the partition in *Stay* mode. Auto-arming will be aborted if any of the zones in partition will be violated or trouble will appear during exit delay. Use the [ENT] key to access the menu, then press [#] to assign a timer to the partition. Save changes by pressing the [ENT] key. **Note:** if you see dashes (---) instead of [ENT], it means that no timers are programmed in the system (program system timers in the menu: *Main menu ▸ Settings ▸ Timers*).

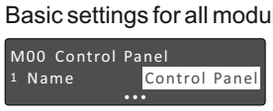
In this menu it is possible to assign the timer(s) to partition. Auto-arming starts at a specific time of day and arms the partition in *Pre-Alarm* mode. Use [ENT] key to access menu, then press [#] key to assign a timer to the partition. Save changes by pressing the [ENT] key. **Note:** if you see dashes (---) instead of [ENT], it means that no timers are programmed in the system (program system timers in menu: *Main menu ▸ Settings ▸ Timers*).

MODULES

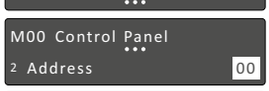
Control panel PAS808M supports up to 7 modules and control panels PAS816, PAS832, P16, P32, P64 supports up to 15 modules.

Service Mode ▸ System Setup ▸ Modules ▸ Module settings

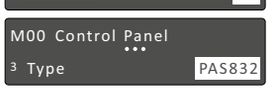
Basic settings for all modules:



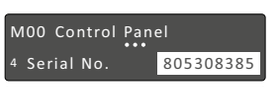
It is recommended to give an appropriate name to the module. The module name will appear on keypad's LCD if there will be any trouble with the module.



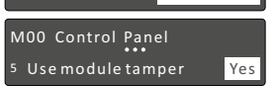
Registered module address is shown in a second row and on the upper-left corner of LCD (eg. M00 = 00 address). Please remember the module address and use it to program zones and PGM outputs.



Registered module type is shown on LCD. Available module types: PAS816, PAS832, P16, P32, P64, PWR20, KM24, KM24A, KM24G, EXT116S, GSV6U, GSVU, EXM800, PROX8, and LAN800.



Registered module serial number is shown on LCD. If you don't see modules serial number, it means that the module is not registered in the system. See page 2 for more information about manual module registration.

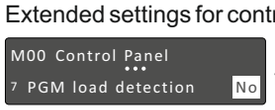


For additional security it's recommended to use tamper to protect modules. Tamper can be activated by using:

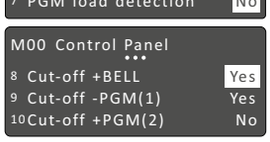
- Z6 - on control panels;
- Z1 - on EXM800;
- TMP - on PWR20;
- back switch - on keypads.

If *Use module tamper* is selected as *No*, then zones Z6 on control panel and Z1 on EXM800 can be used as regular zone terminals.

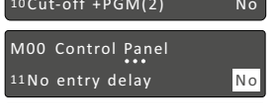
Extended settings for control panel:



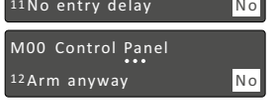
Keypad's screen will show PGM trouble when the load on a preprogrammed PGM output will not be detected by the control panel. By default PGM load detection is disabled.



Control panel can be programmed to cut-off the PGM output when it detects battery's voltage is approaching a critical level of discharge. The threshold is 11,5V.



This setting changes entry delay time in all partitions to 0 seconds (for PAS808M only). User should remotely disarm the system before the entering partition.

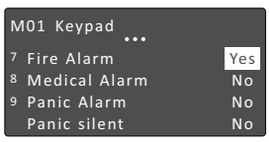


Usually the system stops counting exit delay if system's zone is violated during the exit delay. If this setting is set to *Yes,* then the system will continue counting the exit delay and will sound an alarm if any of the zones will be violated during exit delay.

All virtual wireless modules EXT116VM are usually enabled by default. DO NOT FORGET to run an automatic module registration if this setting was changed.

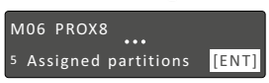
Extended settings for keypads:

All partitions are usually assigned to the keypad by default. All events related to all partitions are shown on keypad's LCD. If there is a need to monitor only one of all enabled partitions, then assign this particular partition to the keypad. Use [ENT] to enter the menu, then press [#] to assign partition to the keypad. Save changes by pressing the [ENT] key.



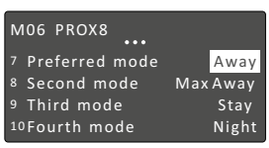
The keypads have additional keys dedicated for emergency conditions. These can be activated by pressing both keys at the same time. However, in some places like a corridor it is recommended to disable emergency keys to prevent false alarms.

Extended settings for PROX8 module:



All partitions by default are usually assigned to the proximity reader PROX8. All events related to all partitions are shown on proximity reader's LED. If there is a need to monitor only one of all enabled partitions, then assign this particular partition to the proximity reader. Use [ENT] to enter the menu, then press the [#] key to assign a partition to the proximity reader. Save changes by pressing the [ENT] key.

This setting is related to entry/exit counting when the module is installed indoors and outdoors. If proximity reader is installed outdoors, then the Entry/Exit delay is excluded.

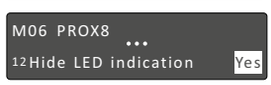


The preferred arming mode will appear as a first option. With preferred arming mode selected correctly the user will spend less time on arming. Arming mode is indicated by a color of PROX8 LED:

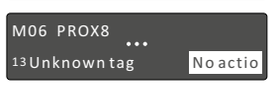
- *Away* - red color;
- *Night* - blue color;
- *Stay* - green color;
- *Max Away* - white color.

Note: if there is a need for only 1 arming mode, program all options with the same arming mode.

The proximity reader has a buzzer for audible notifications which can be enabled or disabled.

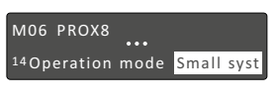


The proximity reader can be programmed to indicate present status of the system on LED for a short period of time when the tag is near a sensitive area of the module or it can indicate the status continuously.



The proximity reader has 3 options on what it must do when the unknown proximity tag is detected:

- *No action*
- *Indication* - module starts blinking red and starts emitting an annoying noise.
- *Indication and alarm* -module starts blinking red and starts emitting an annoying noise. The alarm siren will be triggered after 3 attempts to control the system with an unknown tag.

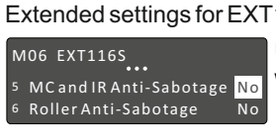


The meaning of LED indication depends on module operation mode:

- *Small System* (up to 3 partitions) - this operation mode is useful when the system has 1 or 2 partitions enabled.
  - 1st and 2nd module LED indicates the arming mode in 1st and 2nd partitions respectively;
  - 3rd LED indicates system troubles;
  - 4th LED indicates an alarm, an alarm memory, not ready status (open zones), and zone bypass.

  If the system has 3 partitions enabled, then the 3rd LED will indicate the arming mode of the 3rd partition. Troubles will be indicated on the 4th LED. Color meaning:
  - Red color - Alarm;
  - Red slow blinking - Alarm memory;
  - Green color - Not Ready;
  - Yellow color - Trouble;
  - Blue color - Bypassed Zone.
- *Large System* (4 partitions) - each partition is assigned to different module's LED. Module LED indicates all information (arming mode, alarm, alarm memory, troubles, and zone bypass).

Extended settings for EXT116S or EXT116VM modules:



Used to secure communication between the detector and a receiver. When this feature is turned on, the detector will consume more battery power and battery life will decrease.

ZONE PROGRAMMING

Zones, in the context of an alarm system, are individual detectors. If the alarm gets triggered, the system records the zones that were tripped, allowing the user to know the exact point of action. Zones also help the monitoring station to know whether they should call the police or fire department upon an alarm. Each zone must be assigned to a partition.

Service Mode ▸ System Setup ▸ Zones

It is recommended to give an appropriate name to the zone. This name will be used by the system for SMS sending or for display on keypad's LCD screen and etc.

Z01 Door
2 Address 00_1

Z01 Door
2 Address 00_1A

Z01 Door
2 Address 00_1B

Zone address is a 3-digit number represented in MA_Z format, where MA specifies a module address in the system and *Z* specifies a zone terminal in the module board. Example: *00_1* - where 00 means the control panel and 1 means zone terminal Z1. To program a doubled zone - detectors A and B must be specified. Use keypad keys [A] or [B] to specify these detectors in the zone address field (example: 00_1 A, 00_1 B, ...).
Note: use loop types *NO/DEOL* or *NC/DEOL* for the doubled zones.
For a keypad firmware version to v.5.xxx, wireless zone loop type depends on zone address. For wireless zones MA_1 – MA_8 the system will automatically assign *NO/DEOL* loop type and for wireless zones MA_9 – MA_16 the *Vibration* loop type. Do not change the loop type of the zone!
For a keypad firmware version v.5.xxx or higher the loop type is *Wireless* for all wireless zones MA_1 – MA_16.
Wireless module address:
- EXT116S - address **06** (default) or one that is given during the registration process.

Virtual wireless module EXT116VM address:
- P16 - address **12**;
- P32 - address **12** and **13**;
- P64 - address **12**, **13**, **14** and **15**.

Z01 Door
3 Loop Type NC

The *Loop type* menu enables you to program the connection type used for each of the system's zones. The actual (physical) loop type for each zone must comply with that selected in the *Loop type* menu. Available loop types:
- *Not used*
- *NC* - uses normally closed contacts and no end of line resistor;
- *NO* - uses normally open contacts and no end of line resistor;
- *NC/EOL* - uses normally closed (NC) contacts in a zone terminated by a 1k end of line resistor;
- *NO/EOL* - uses normally open (NO) contacts in a zone terminated by a 1k end of line resistor;
- *NC/DEOL* - uses normally closed (NC) contacts in a zone using at least two 1k end of line resistors to distinguish between alarms and tamper conditions;
- *NO/DEOL* - uses normally open (NO) contacts in a zone using at least two 1k end of line resistors to distinguish between alarms and tamper conditions;
- *Vibration* - special purpose zone loop type;
- *Roller* - special purpose zone loop type (exluding PAS808M);
- *Wireless*

Z01 Door
4 Serial No. N/A

Z01 Door
4 Serial No. 8388608
Model BK4
Loop (zone) Magnetas
Detect tamper Taip
Battery ER14250
5 Operation code 201

Wireless detectors can be enrolled using serial number in a system with following firmware version or higher:
- control panel P16, P32, P64 – v.5.00;
- wireless zone expansion module EXT116S – v.5.000;
- keypads KM24, KM24A arba KM24G – v.5.000;
- keypads KM25 – v.5.000;
- software MASCAD – v.1.9403;
- GSM/GPRS communicator GSVU or GSV6U – v.5.000;
- LAN communicator LAN800 – v.5.00.

Enrolment using serial number is a two step process:
- **1 step.** Enter detector serial number. The keypad will identify the detector's type and will show all other related settings that are required for enrolment.
- **2 step.** SERVICE MODE DOES NOT HAVE TO BE ENTERED AT THIS STEP! To complete enrolment, the detector must be activated to send a signal to the receiver. It could be done by triggering the detector's loop (zone) OR by pressing the tamper switch. All wireless detector zones that are still not activated, therefore not enrolled, are marked with a phrase *Not activ.* in menu *Wireless communication.*

? ▸ *Technical information* ▸ *Wireless communication*

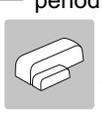
Wireless communication
Detector status
1 Entry doors Not activ.
2 Window LR
3 Living room No SN.
4 Kitchen only LR

When the detector is successfully enrolled, the mode *LR* or *ES* will be displayed in the row. Phrase *No SN.* will be displayed when wireless zone is enabled, but serial number of the detector is not entered. Phrase *only LR* will be displayed when the detector supports only the *LR* mode (firmware version < 2.000).

Z01 Door
4 Operation code N/A

Wireless detector can also be enrolled using *Operation code*. Enter wireless detector's *Operation code* and press the [ENT] key. When enrolment has started, immediately press the detector's tamper switch for a short period of time (~1 sec).


200
Temperature (BT1)


201
Magnet (BK1, BK4)

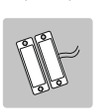

010
Water leakage detector (BF1)

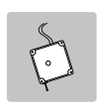

181
Motion (BP2)

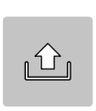

180
Temperature (BP2)


255
Delete single detector

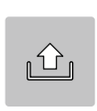

254
Delete all detectors from module


2 1 0 — input terminal 1, 2 or 3. Zone response (speed) time of 0,4 sec.
NC type detector (BK2, BK3, BK4)


2 1 1 — Input terminal (1, 2, 3).
Last digit defines the number of Roller pulses (1, 2, 3, 4, 5, 7, 9).


102


103


104

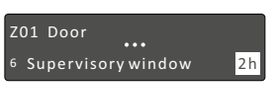

105

Wireless output BS100. **Important!** the LAST digit of the *Operation code* which was used for enrolling BS100 indicates the wireless PGM output number in the module.

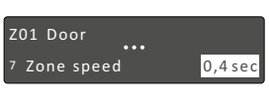
Each zone must be assigned to a partition. All zones are assigned to the 1st partition by default.

Setting the zone definition is partly determined by the arming mode:

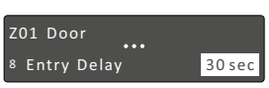
- *Entry/Exit* - used for Entry/Exit doors. A zone must be closed during arming and when the delay expires. Entry delay will be available when the system is armed in *Away* or *Stay* mode.
- *Interior* - usually assigned to motion detectors and to interior doors. Violation of this zone will not trigger an alarm when the system is armed in *Night* or *Stay* mode.
- *Perimeter* or *Instant* - usually intended for non-exit/entry doors, window protection, shock detection, and motion detectors. A zone goes immediately into an alarm state when violated while armed.
- *24h Burglary* - a violation of such a zone causes an instant intrusion alarm, regardless of the system's state.
- *24h Panic Silent* - used for external panic buttons. If violated, an immediate panic alarm is triggered, with the exception that there is no audible indication of the violation.
- *24h Panic Audible* - same as *Panic Silent*, except that the alarm will be audible.
- *24h Tamper* - the tamper function is continuously operational. When a *24h tamper* zone is activated, a tamper alarm is generated.
- *24h Fire* or *24h Smoke* - for smoke or other types of fire detectors. To avoid false alarms, zone attribute *Fire Verification* is recommended to use.
- *24h Fire button* - for external auxiliary emergency alert buttons. If violated, an immediate fire alarm will sound, regardless of the system's state.
- *24h Medical button* - for external auxiliary emergency alert buttons. If violated, an immediate medical alarm will sound, regardless of the system's state.
- *24h Fire supervisory*, *24h Low Water Level*, *24h RF Jam*, *24h Gas Detected*, *24h Water leakage*, *24h High Temperature, 24h Low Temperature* - this group of definitions is used for the 24h technical zones to report about abnormalities in the environment.
- *Control* - zone is mostly used to arm/disarm the system (*Key-switch* zone). Momentary and maintained key-switch arming are available. This definition can also be used to turn On / Off the PGM output. Violation of this zone will not trigger an alarm, regardless of the system's state.
- *Follower* - usually assigned to motion detectors and to interior doors protecting the area between entry door and the keypad. This zone(s) causes an immediate intrusion alarm when violated unless an *Entry/Exit* zone was violated first. Violation of this zone will not trigger an alarm when the system is armed in *Night* or *Stay* mode.
- *Follower Night Armed* - this zone is the same as the *Follower* zone, but violation of this zone will not trigger an alarm when the system is armed in *Stay* mode.
- *Interior Night Armed* - this zone is the same as the *Interior* zone, but violation of this zone will not trigger an alarm when the system is armed in *Stay* mode.
- *Entry/Exit Forced* - same as *Entry/Exit* zone but unlike a regular entry/exit zone this zone can be violated before the arming.



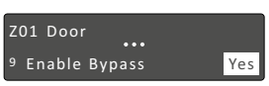
Specifies how often the system checks for supervision signals, identifying each of the system's wireless detectors. The system generates a local trouble signal identifying the zone of any wireless detectors from which a signal is not received during the specified interval. Control panel then sends the supervision report code to the CMS. **Note:** 0 hours disables the supervision. If there are many detectors in the system, due to increased collision effect, it is recommended to set the supervision time to a minimum of 2 hours.



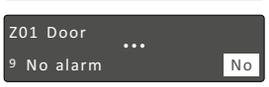
The loop speed menu enables you to set different times for which zone violation must exist before the zone will trigger an alarm condition. Normally zone speed is within 0,1 - 2,5 seconds range. With *Vibration* zone loop type selected, the zone speed must be within 0,01 - 0,25 seconds range (fast zone). This zone loop speed time can be defined only for zones located on the control panel.



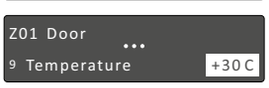
Used for *Entry/Exit* or *Entry/Exit Forced* zones. Entry delay time is programmable within 1 - 255 seconds range.



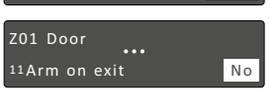
This attribute permits zone bypassing by authorized system users. If *No* is displayed as an option, then the zone cannot be manually bypassed.



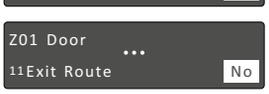
Used for *24h High temperature* or *24h Low temperature*. A zone with this attribute will not trigger an alarm, but can start PGM action.



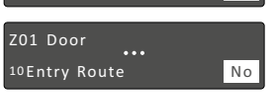
Used for *24h High temperature* or *24h Low temperature.* Enter the temperature. Use [▲] or [▼] to change temperature sign (+ or -). **Note:** temperature field will be visible if wireless detector is in use.



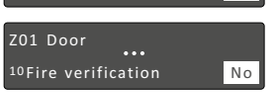
This attribute is only used for *Entry/Exit* or *Entry/Exit Forced*. With this attribute being set - the system will finish an exit delay countdown and will arm the system immediately after the entrance door will close.



With this attribute being set - a zone with *Interior* definition can be violated during an exit delay.



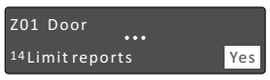
With this attribute being set - a zone with *Interior* definition can be violated during an entry delay.



This attribute is used in fire (smoke) verification procedure. Power to the smoke detector(s) in the affected zone will cut off and then restore. If a subsequent detection occurs in the same zone within a predefined time of the first detection, the system will emit a fire alarm. It's recommended to use +PGM as fire detector power supply.

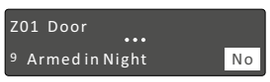
Repeated violation of the same zone, often resulting in a false alarm and usually arising due to a malfunction, an environmental problem, or incorrect installation of a detector or sensor. By default, the system is set to make a

zone shutdown when 3 or 7 (use MASCAD to change this number) violations of the zone are detected. When this parameter is enabled it specifies the number of violations of the same zone (triggered the siren, keypad buzzer, and etc.), during a single armed period before the zone is automatically shutdown.



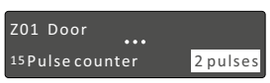
By default, the system is set to make a zone shutdown when 3 or 7 (use MASCAD to change this number) violations of the zone are detected. When this parameter is enabled it specifies number of violations of the same zone reported to central monitoring station during a single armed period, before the zone is automatically shutdown.

Used for perimeter protection. When special arming mode *Pre-alarm* is turned on and the pre-alarm zone is violated, *the* system will make an alarm without reporting to central monitoring station or to the user.

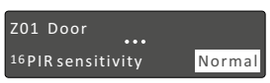


With this attribute being set - a zone with *Interior* definition can't be violated when the system is armed in Night mode - the violation of this zone will trigger an alarm (except systems with PAS808M).

Upon an alarm event occurrence the keypad KM24G informs the user of a security situation by playing voice files assigned to the zone (for example: Entry doors). The system user will hear the same voice announcement in case of an alarm if the system will call him using a PSTN dialer or a GSM module. This menu allows to assign up to 8 voice files from a suggested dictionary to each of the system zones. Press [ENT] to enter the menu.



Pulse counter determines the amount of beams that need to be crossed before the sensor will produce the alarm. Use [▲] or [▼] to change wireless detector BP2 pulse counter value: *2 pulses* (the most sensitive mode), *3 pulses*, *4 pulses* or *SPEC* (the less sensitive mode).



Use [▲] or [▼] to change wireless detector BP2 sensitivity: *Normal* or *High*.

PGM PROGRAMMING

The control panel has three built-in programmable trigger outputs (+BELL, -PGM, +PGM). System allows up to 16 programmable outputs.

Service Mode ▸ System Setup ▸ PGM outputs

It is recommended to give an appropriate name to the PGM. This name will be used by the system for SMS sending or for display on keypad's LCD screen and etc.

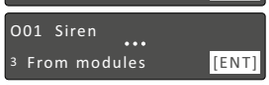
PGM output address is a 3-digit number represented in *MA_P* format, where *MA* specifies a module address in the system and *P* specifies a PGM output terminal in the module board. Example: *00_1* - where 00 means control panel and *1* is the +BELL output. PGM output addresses on modules:

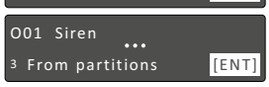
- *Control panel:*
  - *+BELL - 00_1;*
  - *-PGM - 00_2;*
  - *+PGM - 00_3.*
- *KM24/24A/24G:*
  - *Z2/PGM - MA_1.*
- *EXM800:*
  - *Z8/K1 - MA_1;*
  - *...*
  - *Z2/K7 - MA_7.*
- *EXT116S:*
  - *Relay - MA_1.*
- *PWR20:*
  - *+BELL - MA_1;*
  - *PGM1 - MA_2;*
  - *PGM2 - MA_3.*

PGM output Definition describes what kind of system activity will activate the output. DON'T FORGET to assign zones, partitions and etc. to PGM'S output triggering source, otherwise the PGM will not work correctly.

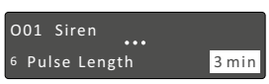
- *Not used* - unused PGM output should be programmed as *Not Used*.
- *Fire Alarm* - output activates if an alarm occurs on the selected zone or module (emergency keys).
- *Fire/Burglary Alarm* - output activates if fire or burglary alarm occurs on the selected zone or module (emergency keys). **Note:** output also activates when zone or module tamper conditions are present (when the system is armed).
- *Burglary Alarm* - output activates if burglary alarm occurs on the selected zone or module (emergency keys). **Note:** output also activates when zone or module tamper conditions are present (when the system is armed).
- *Tamper Alarm* - output activates if tamper alarm occurs on the selected zone or module.
- *Technical Alarm* - output activates if technical alarm occurs on the selected technical zone.
- *Selected Alarms* - output activates if a selected type of alarm occurs on the selected partition.
- *Chime* - output activates if the selected zone is violated (when the system is disarmed).
- *Zone Violation* - output activates if the selected zone is violated. If *Pulse length* is 0 seconds, then the output is activated until any of the selected zones remain violated.
- *Bypass Status* - output activates when a zone is bypassed and deactivates when the zone is reinstated.
- *System Trouble* - output activates if any selected trouble is present.
- *Exit /Entry Delay Warning* - output activates if an entry/exit delay is in progress in the selected partition.
- *Exit Delay/Arm Status* - output activates during an exit delay and if selected partition is armed it will remain active after the exit delay expires.
- *Full Arm Status* - output activates if all of the selected partitions are armed.
- *Notifications* - output activates if the selected partition is being armed (1 pulse) or it is being disarmed (2 pulses). In case of an unsuccessful arming - the output activates for 5 pulses. After alarm clearing this output can also be activated for a specific period of time.
- *Power Supply* - output can be used as a power supply for external devices.
- *Resettable Power Supply* - output can be used as a power supply for external devices. It can be switched off for a specific period of time from the keypad.
- *Fire Power Supply* - output can be used as power supply for fire or smoke detectors. When the system requires a reset for these detectors the output will be switched off for a specific amount of time. This output will be switched off each time after system arming and alarm clearing. This output can also be switched off from the menu.
- *Timer* - output activates when a selected timer activates and it deactivates when a selected timer deactivates (program the system timers in the menu: *Main menu ▸ Settings ▸ Timers).*

◆ *Mono/Bi Switch* - output activates if the selected zone is violated or manually triggered from the keypad. If the *Pulse length* time is set to 0 seconds, then the output is active until the next signal from the zone or from the keypad appears.

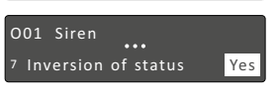




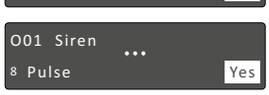
Different PGM output definition requires different triggering sources. Press [ENT] to enter the menu, then press the [#] key to assign a system element (zone, partition and etc.) to the PGM output. Save changes by pressing [ENT].



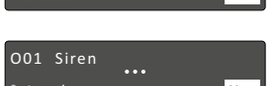
Pulse length determines for how long PGM will be activated. TThe range is between 1 second and 255 minutes.



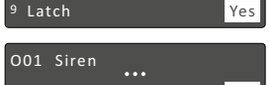
If selected, the output signal is inverted. This is useful when using self-activating alarm sirens.



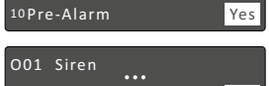
With this attribute being set the output will generate a pulsing DC voltage (1 Hz frequency). If PGM definition is *Fire alarm, Fire/Burglary alarm,* or *Selected alarms* (*Fire alarm*), then the fire alarms will only generate pulsed output signals.



When triggered, output activates and remains activated (latched) until a valid user code is entered or is cleared from the menu (depends on the definition).

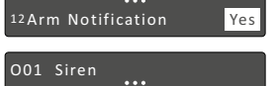


If selected, the output activates when the zone with an attribute *Pre-alarm* is violated (special arming mode *Pre-alarm* must be turned on).



If selected, the alarm siren will ding five times when the arming has failed (for example: perimeter zone was violated or trouble appeared during exit delay).

If selected, the alarm siren will ding once upon arming.

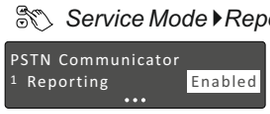


If selected, the alarm siren will ding twice upon disarming.

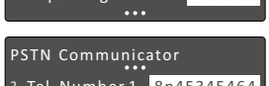
PSTN DIALER SETTINGS

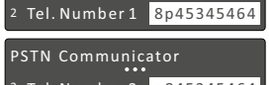
The *PSTN communicator* menu contains parameters that enable the routing of specified events of up to four Central Monitoring Station (CMS) receivers or users. The system automatically generates all reporting codes using the *Contact ID* format.

Service Mode ▸ Report settings ▸ PSTN communicator

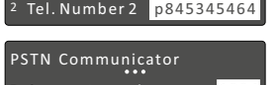


This menu allows to enable/ disable reporting to CMS or to the user via the PSTN line.

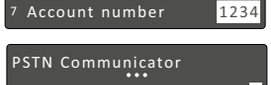




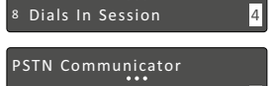
Program the phone numbers as required. Use the [#] key to enter additional symbols: *p* - 3 sec. pause, *P* - 10 sec. pause, *w* - wait dial tone. User must acknowledge the call by pressing the [*] key on the phone, otherwise the control panel will call again.



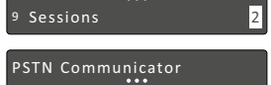
Program the *Account number*. This account number will be used for all reporting events. Use the [#] key to enter additional hex symbols: *B*, *C*, *D*, *E*, *F* .



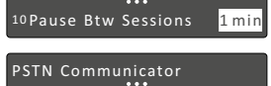
Value programmed in this parameter determines how many times the control panel will re-dial all numbers before proceeding to the next session.



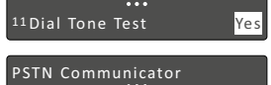
Value programmed in this parameter determines how many dialing sessions the system will run in case of an unsuccessful attempt to deliver the report to CMS.



This parameter determines the pause between the dialing sessions.

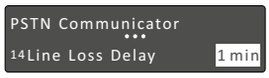


The system dials only if a dial tone is detected.



Use *Tone* for the touchtone (DTMF) dialing or *Pulse* for the rotary (pulse) dialing.

If selected, then the control panel continuously checks the presence of the telephone line voltage.



The control panel indicates telephone line tampering if the telephone line voltage is absent for a longer time than it is set in this parameter.

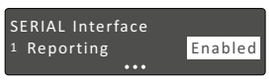
Program the number of consecutive rings that the panel must detect to answer for controlling.

Program the maximum time, in minutes, between calls when connecting to the panel using a double call feature.

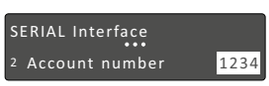
SERIAL INTERFACE SETTINGS

The *SERIAL interface* menu is used to enable reporting to the device which is connected to the SERIAL port.

Service Mode ▸ Report settings ▸ SERIAL Interface



This menu allows to enable /disable reporting to the device which is connected to the SERIAL port. Control panel uses protocol *7 byte slow* by default. Use software MASCAD to change the protocol to *9600 Baud Serial*.

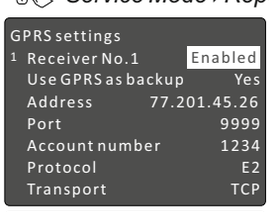


Program the *Account number*. This account number will be used for all reporting events. Use the [#] key to enter additional hex symbols: *B*, *C*, *D*, *E*, *F* .

GPRS SETTINGS

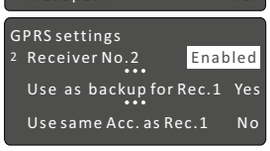
The *GPRS settings* menu contains parameters that enable the routing of specified events for up to two CMS receivers via GPRS.

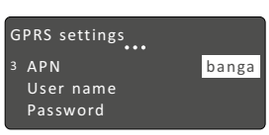
Service Mode ▸ Report settings ▸ GPRS settings



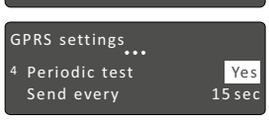
All settings below are visible when reporting to CMS Receiver No.1 or Receiver No.2 via GPRS is enabled.

- *Use GPRS as backup* - if communication with a receiver is not established via PSTN or LAN, the system sends a report via GPRS.
- *Address* - program the address of the CMS receiver (for example: 77.201.45.26 or receiver.secolink.eu). Use the [1] key to enter the DOT character for the address.
- *Port* - program the port used for communication with the CMS receiver.
- *Account number* - this account number will be used for all reporting events. Use the [#] key to enter additional hex symbols: *B*, *C*, *D*, *E*, *F* . **Note:** this account number is also used in the SERIAL interface menu.
- *Protocol* - define the protocol format used to report system events. Available protocols: *E2*, *CSV IP, Fibro*.
- *Transport* - define transport layer protocol: *TCP* or *UDP.*
- *Use as backup for Rec.1* - if communication with a receiver No.1 is not established via GPRS, the system sends the report to a receiver No.2
- *Use same Acc. as Rec.1* - use the same account set for the receiver No.1.





APN is the name of a gateway between a GPRS mobile network and another computer network, frequently the public Internet. A GSM/GPRS module making a data connection must be configured with an APN to present to the network provider. Contact your provider to verify the correct APN settings.

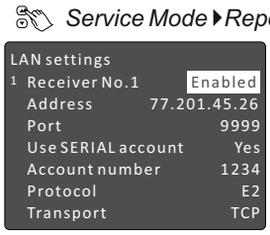


The *Periodic test* menu enables you to set the time period that the module will automatically send a test report to the CMS in order to check the GPRS network.

LAN SETTINGS

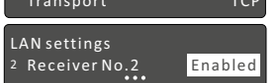
The *LAN settings* menu contains parameters that enable the routing of specified events to the CMS receivers.

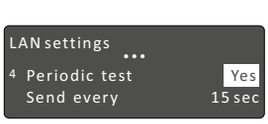
Service Mode ▸ Report settings ▸ LAN settings



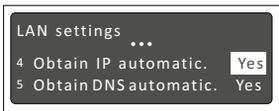
All settings below are visible when reporting to a CMS Receiver No.1 or Receiver No.2 via LAN if it's enabled.

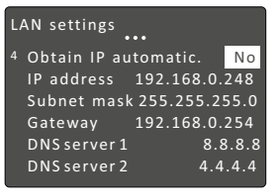
- *Address* - program the address of the CMS receiver (for example: 77.201.45.26 or receiver.secolink.eu).
- *Port* - program the port used for communication with the CMS receiver.
- *Use SERIAL account* - if selected, then the module will use the same account as it is programmed in the *SERIAL interface menu.* The programmed account number and this number will be shown in the menu *Account number.*
- *Account number* - this account number will be used for all reporting events. Use the [#] key to enter additional hex symbols: *B*, *C*, *D*, *E*, *F* .
- *Protocol* - define the protocol format used to report the system events. Available protocols: *E2*, *CSV IP, Fibro*.
- *Transport* - define the transport layer protocol: *TCP* or *UDP.*
- *Use as backup for Rec.1* - if the communication with a receiver No.1 is not established via LAN, the system sends a report to the receiver No.2.





The *Periodic test* menu enables you to set time intervals during which the module will automatically send a test report to the CMS in order to check the LAN network.





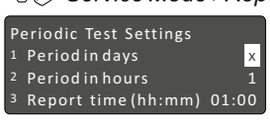
By default, the LAN module is set to obtain IP automatically, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. If you are required to use a permanent IP address to connect to the Internet, select *No*. In this case all IP settings must be manually entered.

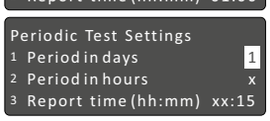
- *IP address* - enter IP address of the module in the network.
- *Subnet mask* - enter a mask of the subnet in which the module works.
- *Gateway* - the default gateway provides a default route for TCP/IP hosts to use when communicating with other hosts on remote networks.
- *DNS server 1 & 2* - DNS technology allows you to type names into receivers No.1 or No.2 address fields (www.alarmserver.net) and the LAN module will automatically find that IP address on the internet.

PERIODIC TEST SETTINGS

The *Periodic Test Settings* menu contains parameters that enable the routing of a periodic test event to CMS receivers.

Service Mode ▸ Report settings ▸ Periodic test settings





Set the test time and hourly/daily interval for periodic test reporting.

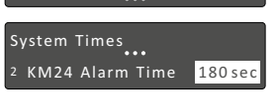
- Daily reporting - use the keypad's numeric keys [0] to [9] to type in the time of the day (in 24-hour format) for periodic test reports to be sent. Use the list below to specify the daily testing intervals:
  - *0* - daily reporting is disabled
  - *1* - Every day;
  - *2* - Every other day;
  - ...
  - *30 Every 30th day;*
  - *31 Every 31th day.*
- Hourly reporting (except systems with PAS808M) - use the keypad's numeric keys [0] to [9] to type in the hour interval and the minute at the hour for periodic test reports to be sent. Disable the periodic reporting by setting the *Period in hours* to 0.

SYSTEM TIMES SETTINGS

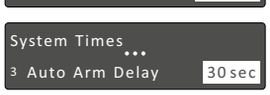
The *System times* settings menu contains parameters that specify the duration of an action.

Service Mode ▸ System Setup ▸ System times

The programmed exit delay will be applied for all enabled partitions.

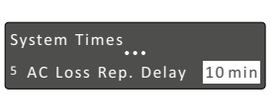


The buzzer (or loudspeaker) housed inside the keypad emits (annunciates) sounds in case of alarm. The duration of alarm sound is programmable within a 1 - 255 seconds range.

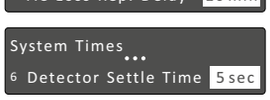


Used for all partitions. An audible *Auto Arm Delay* (warning) countdown will commence prior the automatic arming. User, that has right to stop auto arming, can enter a valid PIN code at any time during the countdown to stop auto arming.

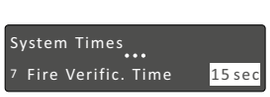
This time is related to special arming mode *Pre-alarm*. When a pre-alarm zone is violated, the system will trigger the siren and a keypad buzzer (loudspeaker). The duration of pre-alarm is programmable within a 1 - 255 seconds range.



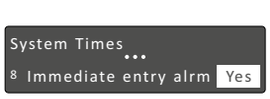
In case of AC power loss, this parameter specifies the delay period before reporting the event.



Implemented on detection of smoke or fire for verification. When smoke of fire zone is violated, the system will reset all smoke or fire detectors, then wait for detectors to settle. Detector's settling time is programmable within a 1 - 255 seconds range.



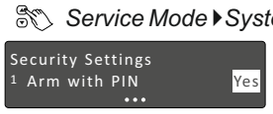
Implemented on detection of smoke or fire for verification. When smoke or fire zone is violated, the system will reset these detectors, then wait for detectors to settle. If a subsequent detection occurs in the same zone within the time that is programmed in *Fire Verification Time*, the system will emit a fire alarm.



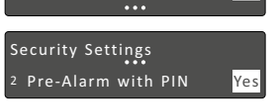
Event reports from entry zones to the CMS are delayed for 30 seconds after they are detected. Select *Yes* if the event report should be sent immediately.

SECURITY SETTINGS

Service Mode ▸ System Setup ▸ Security Settings



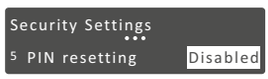
Used for the [🔒] key. If selected, then the keypad will skip the PIN entering procedure and will automatically enter the 1st user's PIN.



Used for the [🔊] key. If selected, then the keypad will skip the PIN entering procedure and will automatically enter the 1st user's PIN.

Used for the [B] key. If selected, then the keypad will skip the PIN entering procedure and will automatically enter the 1st user's PIN.

This settings allows to enable or disable access to *System summary* menu.



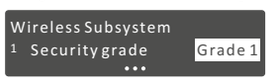
This setting allows to enable or to disable access to the special user menu, where installer with his PIN can restore 1st user's PIN to default and the 1st user with his PIN can restore all enabled user PINs to default.

This feature is intended for situations where the user is forced to disarm or arm the system under a threat. This setting enables or disables this feature. Duress code is individual for every system user. Duress code = X1, X2, X3, X4 when X4 = X4 + 1 (X1, X2, X3, X4 are digits). Example: user PIN is 123**4**, duress code will be 123**5**.

Note: if certain system *user's A* duress code matches with another system *user's B* PIN code, then the system will use *user's B* PIN instead of the duress code of *user A* to complete the control action. It is recommended to test duress code availability before using the system. The event of duress code use will be generated in the event log.

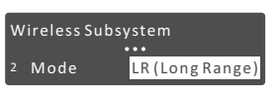
WIRELESS SETTINGS

Service Mode ▸ *System Setup* ▸ *Wireless Subsystem*



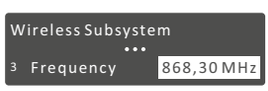
How often the detector should send a supervision signal and what supervisory window will be in the system depends upon the setting *Security grade*.

- *Grade 1* – supervision signal is sent every 1 hour, supervisory window is 1 hour.
- *Custom* – supervision signal is sent every 1 hour, supervisory window is 0 - 24 hour (0 - disables supervision).
- *Grade 2* – supervision signal is sent every 20 minutes, supervisory window is 20 minutes.

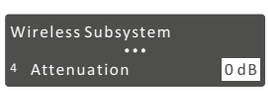


Wireless devices, starting from version 2.000 support new communication mode, that can be selected in menu *Mode:*

- *LR* – long range mode – distance is bigger, but due to the longer data packet the battery last shorter.
- *ES* – energy save mode – the distance is shorter, but due to the shorter data packet the battery last longer.



The default frequency is 868,30 MHz. Depending on country of distribution the wireless devices (detectors, PGM outputs and remote control) can be programmed at factory to operate on different frequency. Receiver can receive a signal from transmitter when operating frequency matches.



Due to the fact that there may be changes in the passive environment after installation, it is possible to *temporarily* for 3dB attenuate the radio frequency link during installation or maintenance. If the system will continue receiving signal from the detector with an attenuated radio frequency link, then it will work for sure under normal conditions. New setting will be applied in 20 min or 1 hour time (depends on supervisory signal sending frequency).
DO NOT FORGET to change the *Attenuation* setting's value to *0dB* when installation or maintenance works are finished.

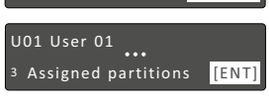
USER PROGRAMMING

Each installation typically accommodates unique user PIN codes of up to 4 digits. The *Edit Users* menu provides access to submenus and their related parameters that enable you to maintain user PIN codes in the system. The first user's PIN code is used by the system's owner or chief user. This user has access to all the menus (except *Service mode*) and it can't be disabled.

Main menu ▸ *Settings* ▸ *Users* ▸ *Edit Users*

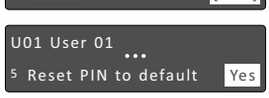
It is recommended to give an appropriate name to a user. The system will use it to send SMS or for display on keypad's LCD screen.

All users that have the status mode *Enabled* can control the system or its partitions.



The *Assigned partitions* menu enables you to assign the partition(s) in which the user (except for the 1st system user) will operate.

Used to allow users to control the system during predefined time periods. **Note:** if the timer is not assigned, the user will be able to control the system without time limitations.

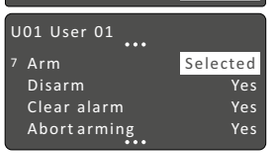


This option allows to restore current user PIN to default. Factory default user PIN depends on user's number in the system. System user number is shown next to letter *U* on top-left corner of the keypad's LCD. For example U01 means the 1st system user, U02 means the 2nd user, and so on. Default PIN code used by U01 (1st user) - 0001, U02 (2nd user) default PIN - 0002, ..., U63 (63th user) default PIN - 0063. Default PIN code is temporary and should be changed as soon as possible to a new one. It is recommended to change the old PIN code to one that will not be used as default for other users (default PIN range 0000 to 0063).

This menu entry is used to assign the remote control (RCU) or proximity tag to the system user. To assign the RCU or tag - choose the corresponding menu and press the [ENT] key to program:

- HC3S - simultaneously hold down all buttons.
- LT5 - simultaneously hold down the buttons [A] and [D].
- Proximity tag - put the tag on a sensitive area of the proximity reader.

Removing the control unit can be done in the same menu. Message *Done* should appear on keypad's LCD when *all* control units are removed from the user.



All system users have all rights assigned by default. However, it is possible to change them. The user has access to the following:

- *Arm*;
- *Disarm*;
- *Clear alarm*;
- *Abort arming*;
- *Bypass zones*;
- *Edit settings*;
- *View Event log*;
- *Test fire zones*;
- *Reporting test;*
- *Run other tests*;
- *Control PGM outputs*;
- *Edit system users*;
- *Right to enable service*;

Additional information:

Minimum number of PIN code variations could be calculated using this equation: *Number of variations = 10* $^{PIN\ code\ length}$ *- Installer PIN - Max total available number of users limited by panel.* For example: for P64 control panel when PIN code length is 4 digits, the number of variations will be 10^4 - 1 - 63 = 9936. Remaining number of PIN code variations for each user can be calculated using this equation: *Number of variations for a new user = Number of variations* - (*Number of enabled users - 1)*. For example: 1 user is enabled, then number of PIN code variations is 10^4 - (1 - 1) = 9936.

Note: the system doesn't allow to use same PIN codes for different users. User will be informed if the PIN is already taken. When user's PIN code is recognized, notification message on LCD screen will ask to change it.

The keypad will block access to the system if invalid PIN code is entered 3 times. The system will be blocked for 90 seconds and this event will be recorded in the event log.

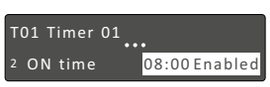
User should press the [CLR] key multiple times to return to the main screen (date and time should be visible). This keeps the information inaccessible for other non-system users. Installer should exit the service mode and block access to it when he finishes installation or maintenance work. This keeps the information inaccessible for system users.

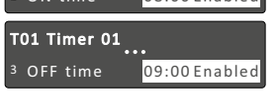
SYSTEM TIMERS PROGRAMMING

System timers consist of an ON time and an OFF time, and selected days of the week in which they are active. There are up to 16 timers (depends on control panel type) that can be used to make auto arming schedule or to control various devices, such as lights or appliances.

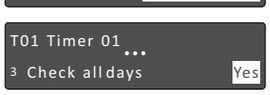
Main menu ▸ Settings ▸ Timers

It is recommended to give an appropriate name to a timer.





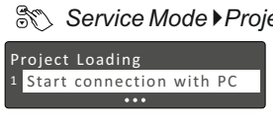
Timer is in use when it is enabled. Use the 24-hour clock to program the timer On/Off time .



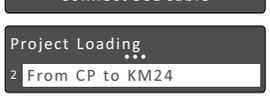
Select the days when the system timer will activate.

PROJECT LOADING

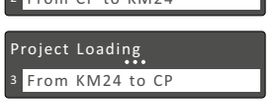
Service Mode ▸ Project Loading



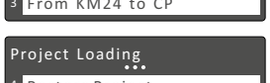
If entered the keypad initiates a communications session with the PC. Software MASCAD is used to program SECOLINK intruder alarm system. **Note:** it is necessary to register modules to the system, if a new module was added to the project by using MASCAD software. After module registration the data from the keypad should be sent to the system.



If entered the control panel will start uploading the project to all registered system modules.



If entered the keypad will start uploading the project to control panel and all registered system modules.



Two sub-menus are available:

- *Restore Main settings* - restores all settings, excluding entered names and reporting settings.
- *Restore Default project* - restores all settings to factory default values.

LANGUAGE

Service Mode ▸ Set Language

Usually the keypad is supplied with only one language. Contact your local distributor for an additional language.

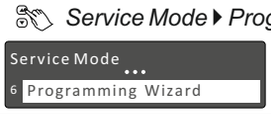
UNREGISTER MODULES

Service Mode ▸ Unregister Modules

Used to unregister system modules. The message *First Start Press [ENT]* will appear on keypad's LCD screen when this procedure will end.

PROGRAMMING WIZARD (KM24G)

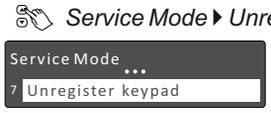
Service Mode ▸ Programming Wizard



Step by step programming wizzard with explanations and wiring schemes.

UNREGISTER KEYPAD (KM24G)

Service Mode ▸ Unregister keypad



Used to unregister the keypad from the system.

SERVICE MODE MENU TREE