STEMAX

STEMAX ZE10

ZONE
EXPANDERS

USER
MANUAL

TABLE OF CONTENTS

1 EXPANDER DESCRIPTION AND OPERATION

1.1 INTENDED PURPOSE OF THE STEMAX ZE10 ZONE EXPANDERS

STEMAX ZE10 zone expanders (hereinafter *the expanders*) are designed for monitoring guard and technological alarm loops and sending notifications to the main controller they are connected to.

The STEMAX MX840 controllers can be used as the **main controller** for the expander.

The expander allows to increase the number of monitored alarm loops (ALs) and partitions when organizing security of large sites and groups of sites. In this case only one main controller is installed at one of the sites, and other sites are equipped with the expanders which communicate with the main controller via RS-485 network. It is possible to connect up to 15 expanders to one main controller.

The expanders have outputs for connecting 10 ALs, 3 open collector (OC) control outputs, and 1 Touch Memory input.

The use of the expanders does not disrupt communication with endpoint equipment and its control. For the sake of convenience, the expander can be mounted on a DIN rail. The modular design allows connecting wires to an adapter terminal board and to greatly simplify maintenance and repair.

1.2 SPECIFICATIONS

Specifications of the expander are provided in table 1.1.

Table 1.1. Specifications

Parameter	**Value**
Number of controlled alarm loops	10
Type of monitored alarm loops	Guard, technological
Alarm loop voltage	4.6 V
Nominal resistance of an alarm loop termination resistor	5.6 kΩ
Resistance of alarm loop wires	up to 150 Ω
Insulation resistance of alarm loop wiring	at least 50 kΩ
Number of open collector control outputs	3
Maximum total load current of the +12 V output	400 mA
Communication interface	RS-485
Nominal supply voltage of the expander	12 V
Current consumption in the standby mode without external load	50 mA
Maximum current consumption	0.5 A
Operating temperature range	from -40 °C to +55 °C
Dimensions	210 × 118 × 44 mm
Enclosure material	ABS plastic
Enclosure protection rating	IP30

1.3 SUPPLY SET

The supply set of the expander is provided in table 1.2.

Table 1.2. Supply set

Name	Document ID	Quantity
STEMAX ZE10 Zone Expander	AGNS.425511.010 TU	1
Passport	AGNS.425511.010 PS	1
5.6 Ω 0.25 W CF resistor		10
Unit container		1

1.4 FUNCTIONAL DIAGRAM

The expander consists of the following units:

- microcontroller;
- input circuits;
- control circuits of endpoint devices;
- Touch Memory port;
- indication panel;
- RS-485 interface;
- tamper detection sensor;
- voltage converter.

The microcontroller serves as a connection and control link.

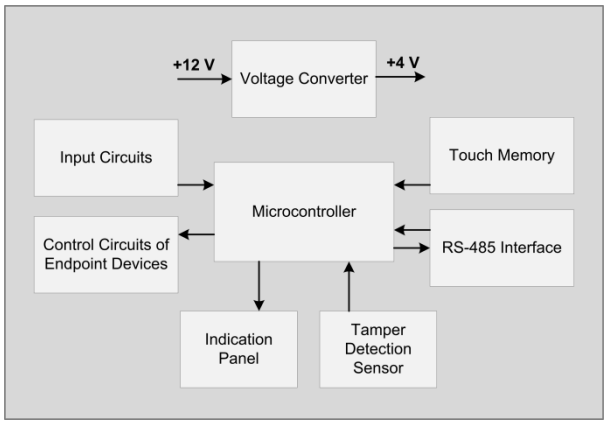

Figure 1.1 Functional diagram

Functions performed by the control module of the expander:

- monitoring voltage of guard and technological ALs;
- data exchange with devices over RS-485 interface;
- monitoring and control of peripheral devices (tamper detection sensor, Touch Memory port, indication panel);
- control of endpoint device circuits;
- storage of information about the operation of the main controller in the event log.

1.5 LABELLING

Labelling on the expander:

- model;
- serial number;
- manufacturing month and day;
- standard compliance mark;
- labels of indicators, control elements, and other functionally significant elements.

Labelling on the expander packaging:

- model;

- serial number;
- manufacturing month and day;
- standard compliance mark;
- specification requirements.

1.6 PACKAGING

The supply set (see table 1.2) is put into an individual cardboard container for protection from damage during transportation. Additionally, the supply set is packaged in a plastic bag to protect it from high humidity exposure during transportation and storage.

2 OPERATING RESTRICTIONS

Warning

To prevent electric shock or fire, do not use the expander under the following conditions:

- outdoors;
- in places with high humidity or where it is possible for liquid to get inside the enclosure;
- in aggressive environments that can cause corrosion;
- in the presence of conductive dust.

The operating conditions of the expanders and the supplied voltage must correspond to the values provided in the Specifications table (see 1.2).

Mount/dismount and maintain only de-energized expanders.

Attention

Install the expanders in areas with limited access for unauthorized persons.

After transportation at sub-zero temperatures, the expanders must be kept unpacked under normal conditions for at least two hours before being turned on.

When designing a system, consider specification of the power source of the expander. If the total current consumed by external devices (signaling and endpoint devices) exceeds 400 mA, an additional power source must be used. In this case, we recommend connecting the -12 V common line of the expander with the common line of the additional power source to equalize the potentials.

3 PREPARING THE EXPANDER FOR CONFIGURATION AND OPERATION

3.1 RS-485 NETWORK TOPOLOGY

RS-485 is a half-duplex multipoint serial data interface. Data is transmitted over a single twisted pair using differential signals. Devices in the network connected over RS-485 interface are divided into two types: Master and Slave. A Master device is the main device in the network that can request data from Slave devices and send broadband messages. A Slave device is a device in the network that cannot initiate transmission of its data, but transmits or accepts them only when requested by the Master device. In case of the STEMAX MX 840 controller with the STEMAX ZE10 expanders connected to it, the status of Master device is assigned to the main controller, and it is not possible to change it.

An example of an RS-485 network topology of the STEMAX equipment that allows to organize guarding of several sites with one controller is provided in figure 3.1.

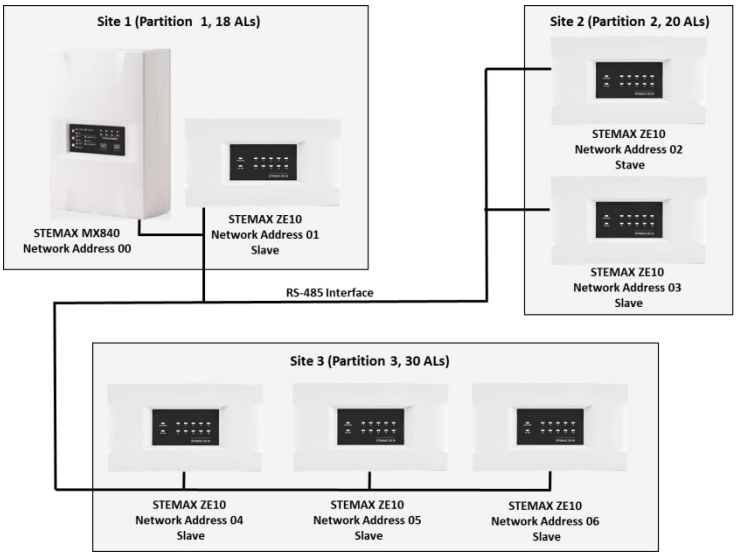

Figure 3.1 An example of an RS-485 network topology of the STEMAX equipment

The Master device controls the guard mode of all sites and monitors their alarm loops. The Master device also stores a database of electronic keys. The Slave devices monitor their alarm loops and subdue to their Master device when the guard mode of the site changes.

When designing a system, refer to the distribution of network device addresses provided in table 3.1.

Table 3.1. Distribution of devices in a RS-485 network

Network address	**Device type**
0	Main controller
1..31	Zone expanders

Main capabilities of device integration over RS-485 interface:

- up to 158 ALs monitored by one controller without information loss;
- guarding of a group of up to 15 sites by one controller;
- RS-485 interface signals are transmitted using differential voltage levels ranging from 0.2 to 8 V, which provides high noise immunity.

3.2 CONNECTION OF THE EXPANDER TO THE MAIN CONTROLLER

The expander is connected to the main controller over RS-485 interface. RS-485 interface terminals are labeled A and B on the controller and on the expander. To link the devices, connect the matching terminals of the expander and the controller. The device is connected to the interface in a *shared bus* topology.

It is recommended to use a UTP-4 *twisted pair* cable for wiring the RS-485 interface. If your cable is longer than 300 m, use a STP-4 shielded *twisted pair*. When using an interface cable, ensure that the interference from power cables, industrial and retail equipment, powerful radio transmitters is at minimal level.

Supply the power via +12 V and ⊥ (-12 V) terminals of the expander. There are two ways to do that:

1) From the +12 V and -12 V of the controller (in this case take into account that the total current consumed by the devices connected to the controller must not exceed the maximum load current provided in the specification).
2) From another 12 V DC source that meets the requirements for security and fire alarm systems. When an external power source is used, connect its -12 V output with the -12 V output of the expander.

See the expander appearance with its lid open and the general external connection diagram in *Appendix A* on page 27 and *Appendix B* on page 28.

3.3 ASSIGNING NETWORK ADDRESS TO THE EXPANDER

After connecting the expander to a controller, you need to assign an unoccupied RS-485 network address to it (see 3.1). If several devices have the same network address, the system is not able to operate as intended. You can select network addresses for the expander in a range from 01 to 16. By default, the expander has the network address 01. To change the network address, follow the steps below.

1) Open the lid and energize the expander.
2) Switch the expander into the network address programming mode by switching the ADR microswitch into the ON state (see *Appendix A* on page 27). The current network address is displayed by the alarm loop indicators and the RS-485 indicator as described in table 5.1**Ошибка! Источник ссылки не найден.**.
3) Select network address of the expander by pressing the tamper detection sensor button (see *Appendix A* on page 27). The address number increases by one with each press of the button, when the number 16 is reached, the next press returns the count to 01. The indicators on the expander light up and down sequentially as described in table 3.2.
4) Move the ADR microswitch lever into the position 1 to switch the expander into standby mode with the new network address.

Table 3.2. Indication of the expander network address

Address	AL indicator	RS-485 indicator	Address	AL indicator	RS-485 indicator
01	1	Off	09	9	Off
02	2	Off	10	10	Off
03	3	Off	11	1	On
04	4	Off	12	2	On
05	5	Off	13	3	On
06	6	Off	14	4	On
07	7	Off	15	5	On
08	8	Off	16	6	On

3.4 USE OF THE 120 OM MICROSWITCH

The 120 Om microswitch (see *Appendix A* on page 27) is used for impedance matching in long lines (when several expanders are included into a circuit and the cable is longer than 200 m). Moving the microswitch lever into the ON position includes an additional resistor into the circuit.

Only the microswitch of one expander located at the farthest distance from the controller in the circuit shall be switched ON.

3.5 CONNECTING ALARM LOOPS

The expander has ten inputs for connecting alarm loops, which ensure the reception of notifications from analogue signaling devices and output relays of control units listed below.

- *Guard input*: any passive or active dry contact signaling devices.
- *Panic button*: a hard-wired panic button.

- *Technological, Flood sensor, Gas leak sensor*: any passive or active dry contact signaling devices appropriate for their purposes and output relays of control units.

When connecting alarm loops with normally **open** signaling devices, include a 5.6 kΩ resistor **in parallel** with the circuit. When connecting alarm loops with normally **closed** signaling devices, include a 5.6 kΩ resistor **in series** with the circuit.

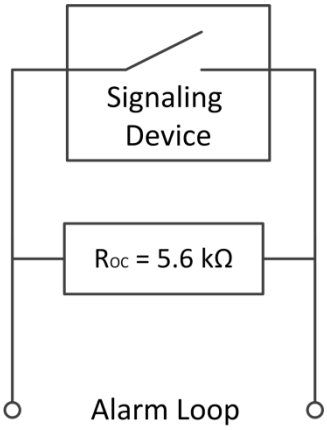

Figure 3.2. Connection of alarm loops with normally open signaling devices

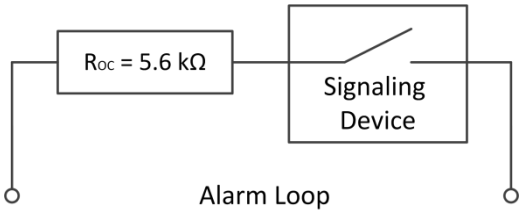

Figure 3.3. Connection of alarm loops with normally closed signaling devices

In case of **digital alarm loops** (of *Technological* type), a resistor is not required. They are monitored by their closed/open state. You can select their normal and triggered state using the *Inversion* attribute. By default, the inputs are normally closed, and if the inversion attribute is selected, they are normally open.

In high noise environment, we recommend using shielded cable for an alarm loop and connecting its shield to ground screw of an external power supply.

Note — If an alarm loop is not used, assign the *Disabled* type to it.

3.6 CONNECTING SOUND AND LIGHT SIGNALING DEVICES

It is recommended to use a combined outdoor sound and light alarm as a sound and light signaling device. When connecting hard-wired sound and light signaling devices, connect their minus contact to an *open collector* output (with an appropriate tactics assigned) and the plus contact to the +12 V output of the expander.

We recommend using a 2 V 5 mm LED as an external indicator (*Guard mode* lamp) connected to REG and –12 V terminals. A current limiting resistor is installed in the expander.

3.7 CONNECTION OF GUARD MODE CONTROL DEVICES

You can purchase and connect the following arming/disarming devices to the expander:

- STEMAX-KD-04 keypad;

  electronic key reader, such as the STEMAX TM reader (for arming/disarming using Touch Memory electronic keys).

The length of a communication line between the keypad or an electronic key readers and the expander may reach up to 50 m, in case an installation cable, such as an indoor signal cable, is used and no electromagnetic interference is present. In case the distance is longer than 50 m, use a shielded twisted pair.

3.8 INSTALLING THE STEMAX CONFIGURATOR SOFTWARE

To configure the expander and to monitor its status, the *STEMAX Configurator* software designed for personal computers running Windows OS is used.

When installing the software on your PC for the first time, also install the following components:

- the USB driver (required for the correct connection of the devices manufactured by NPP «Stels» to your PC via USB interface);
- .NET Framework 4.5.2 library packages (required for the correct operation of the *STEMAX Configurator* software).

Note — Expander operation is supported by the *STEMAX Configurator* 4.27 and above. Before starting the work with the expander, make sure that the latest version of the software is installed.

Installation of all components can be carried out using the STEMAX Configurator installation file by following the instructions below:

1. Download the *STEMAX Configurator* installer from https://stemax.nppstels.ru/manuals_en*:* the installer is provided as a Configurator_pro_setup_(X).exe (X is the version number).
2. Run the installer. We recommend running the installer as administrator to ensure correct installation of the software. To do this, right-click on the file and select *Run as Administrator* in the menu.
3. In the window that opens, leave all the checkboxes selected and click the Next > button (see figure 3.4).

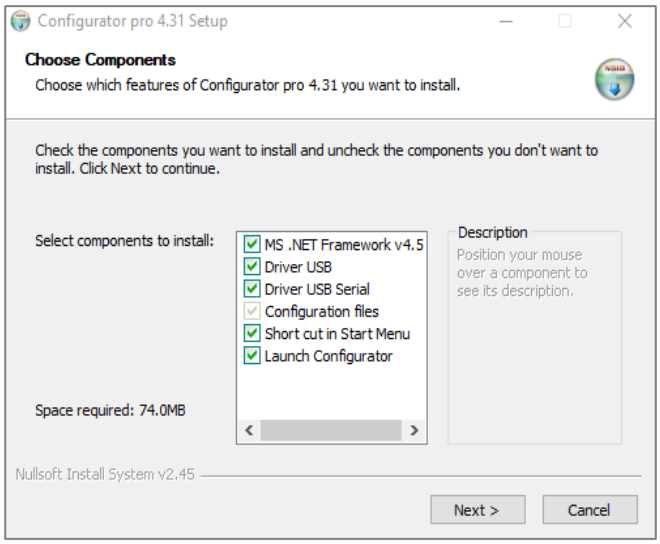

Figure 3.4.The window *Choose components*

4. In the next window, specify the installation folder and click the Install button (see figure 3.5).

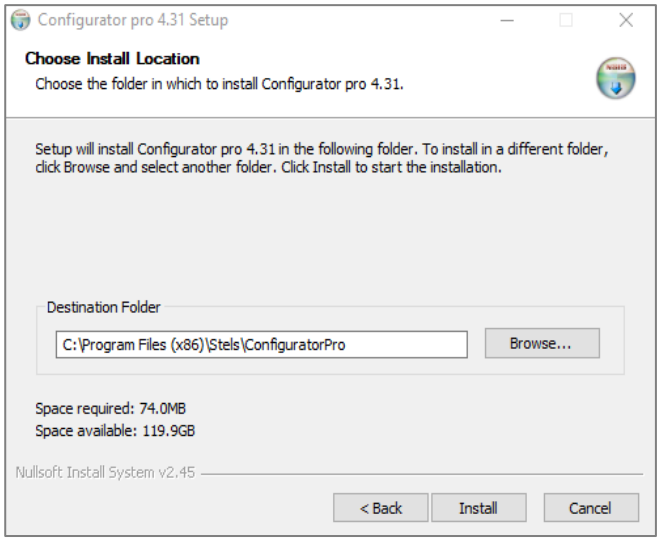

Figure 3.5. Window *Choose Install location*

When the installation is complete, the software can be launched by:

- using a shortcut created on the Windows desktop;
- from the Windows Start menu (Start → Programs → Stels → Configurator Pro);
- from the installation folder by running the MirajConfigurator.exe file.

During its operation, the software creates other files and subfolders required for its operation, data saving, and settings in the folder where its executable file is located.

3.9 STEMAX CONFIGURATOR INTERFACE

The interface of the main window of the software is provided in figure 3.6[1].

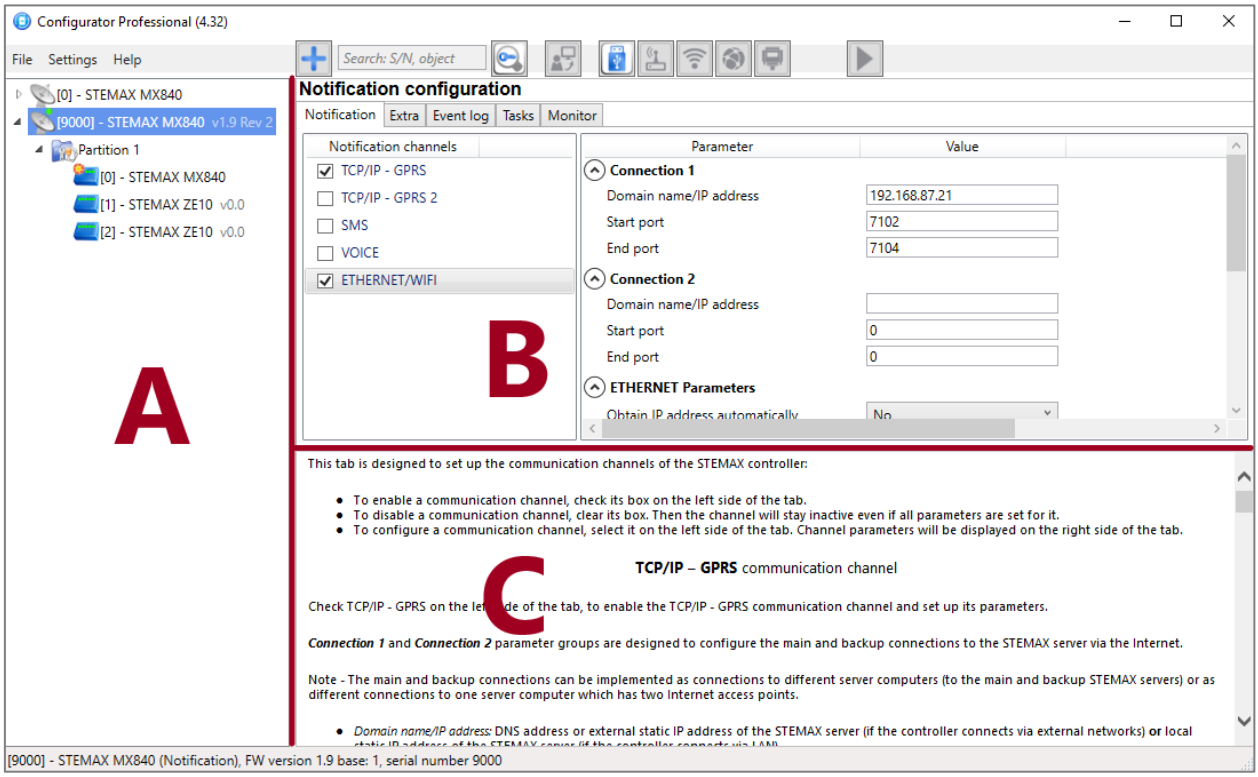

Figure 3.6. Structure of the main window
(A — device tree, B — parameter area, C — help area)

The **device tree** (area A) displays devices added, their parameter groups, the version of the firmware installed on them, and their connection statuses.

The device tree has a **multi-level structure**:

 — parameter group of the controller's notification module (notification configuration that includes parameters of data transmission channels, etc.);

 — parameter group of the controller's partitions (parameters related to controller arming and disarming);

 — parameter group of the controller's and the expanders' control modules (parameters of alarm loops, radio devices, integration etc.);

 — relay control parameters (remote control tools for *open collector* outputs). The relay control parameter group is displayed in case at least one *open collector* control output is assigned the *Remote control* tactic.

When a parameter group is selected in the device tree, tabs with the corresponding parameters are displayed in the **parameter area** (area B) (to select a parameter group, left-click on the corresponding line in the device tree and make sure that the line got highlighted in blue, see figure 3.7).

[1] Screenshots from the STEMAX Configurator version 4.32 running under Windows 10 are provided as illustrations. The software is linked to the STEMAX MX840 controller. The interface of the program installed on your PC may slightly differ depending on the version of the software and operating system in use.

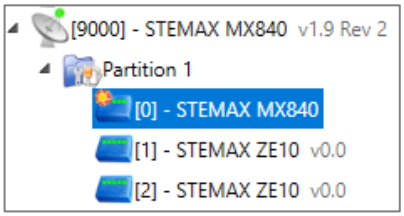

Figure 3.7. The controller's control module parameter group is selected

If a large number of devices is displayed in the tree, then it is possible to collapse parameter groups for convenience by left-clicking on the ◢ icon. To expand the groups, left-click on the ▷ icon.

The **help area** (area C) displays help information about the parameters displayed.

Note — It is possible to hide the help area. To do this, select *Yes* for the *Hide comments area* option in the *Settings* menu.

At the top of the main program window, there are **menus**, buttons (**toolbar**), and a **search field** for searching by serial number or device name (see figure 3.8).

Figure 3.8. Menu, search field, and toolbar

3.10 PREPARING THE EXPANDER FOR CONFIGURING

Registration and configuration of the expander is performed in the *STEMAX Configurator* software. To link the expander with the software, follow the steps below:

1. Connect the expander to the main controller (see 3.2).
2. Connect the controller to a PC with the software running using one of the methods described in the main controller user manual available on the NPP «Stels» website.

4 CONFIGURING THE EXPANDER

The STEMAX ZE10 expander operates as an AL number expander of the STEMAX MX840. The use of the expanders increases the number of guard and technological alarm loops monitored by the main controller to up to 158 and the number of OC control outputs to up to 48 (maximum 15 expanders, each having 10 ALs and 3 OC outputs, can be connected to the main controller). You can divide ALs of the expander between the controller's partitions, and the OC outputs are going to be controlled by the main controller.

The Touch Memory port of the expander operates using passthrough logic: electronic key data base is stored in the memory of the main controller, and the number of the partition controlled by each key can be selected in the expander parameters (see 4.2.1).

4.1 ADDING AN EXPANDER

To register the STEMAX ZE10 zone expander in the controller configuration, right-click on the line of the main controller partition in the device tree and select *Add peripheral* in the menu (see figure 4.1).

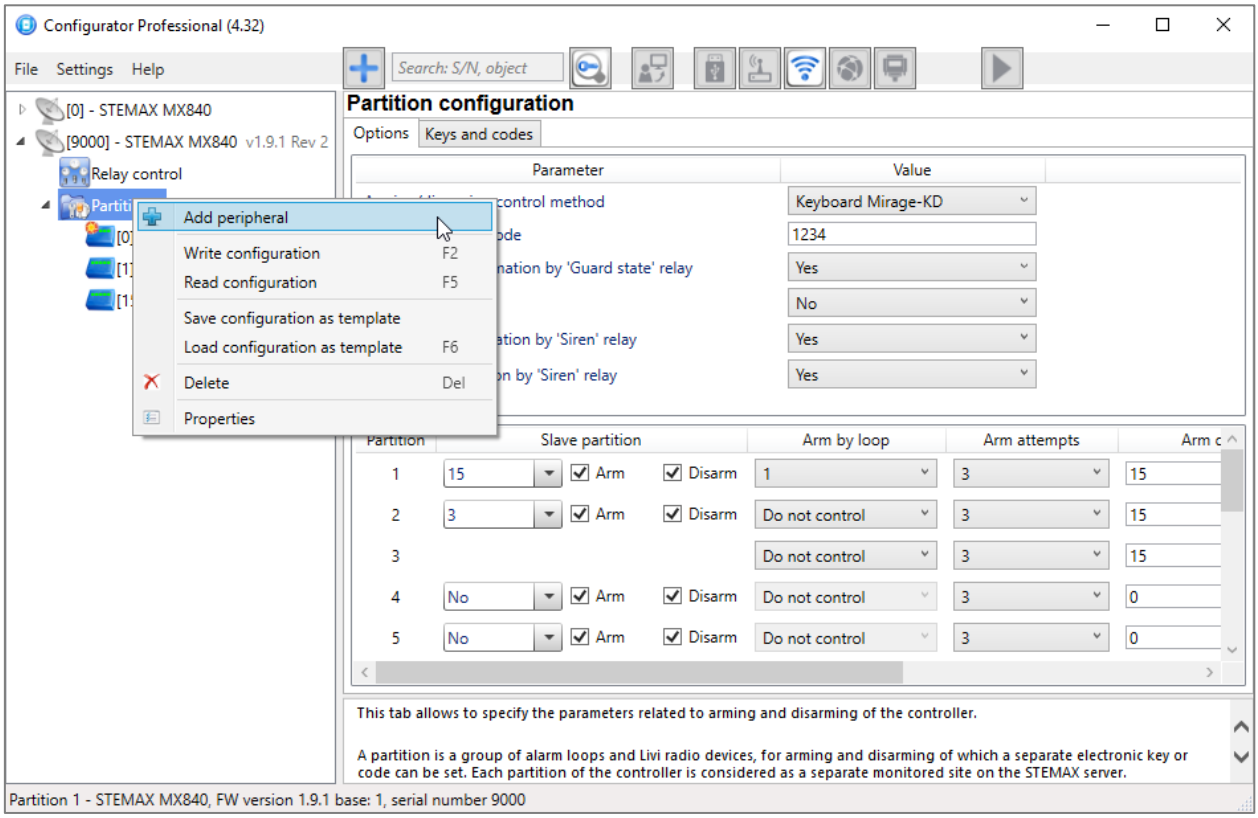

Figure 4.1. Adding a zone expander

In the *New device* window that opens, select *STEMAX ZE10* in the device type drop-down menu, enter the network address of the device, the number of devices to add into the configuration, and click *OK* (see figure 4.2). If you want to connect several expanders to the controller, enter the network address of the first expander.

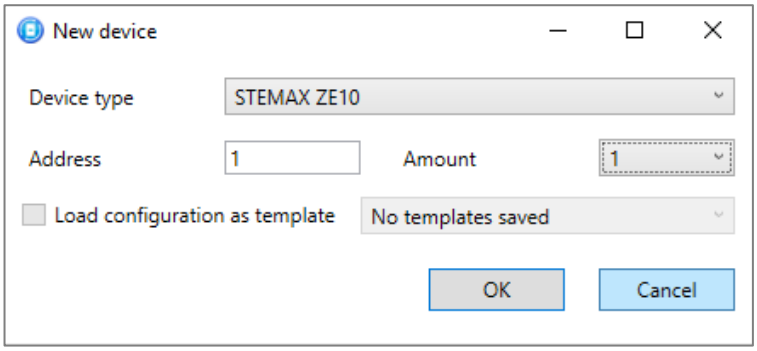

Figure 4.2. *New device* window

4.2 PERIPHERAL CONFIGURATION OF THE EXPANDER

To proceed to the expander configuration, select its line in the device tree by left-clicking on it. *Options, Loops*, *Relays*, *Extra*, *Monitor* tabs open in the parameter area of the *STEMAX Configurator* (see figure 4.3).

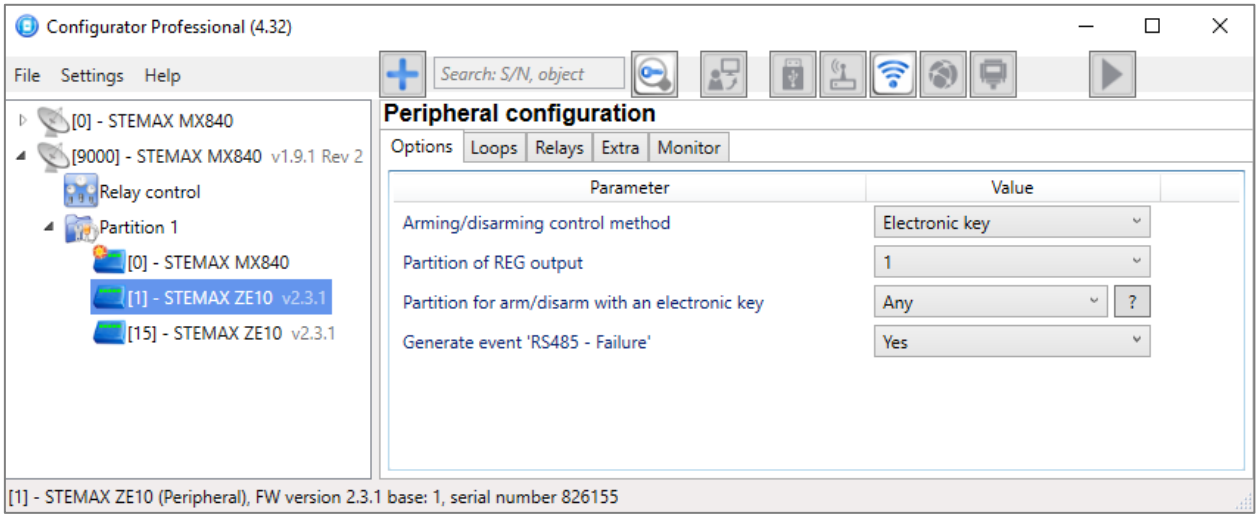

Figure 4.3. Expander configuration, *Options* tab

After selecting the options in the software, you need to write the configuration into the expander. To do this, right-click on the expander name in the device tree and select *Write configuration* in the context menu **or** press F2 button on you PC's keyboard.

4.2.1 Options tab

Options tab (see figure 4.3) is used for setting the following parameters:

- *Arming/disarming control method:* select the model of the control device connected to the Touch Memory port of this zone expander. If your model is not in the list, select *Electronic key*.
  - *Electronic key*: if a control device (including TM readers) manufactured by other manufacturers is connected to the expander (see figure 4.3).
  - *Keyboard Mirage-KD:* if a STEMAX-KD series keypad by NPP «Stels» is connected to the expander (see figure 4.4).
  - *STEMAX TM:* if the STEMAX TM reader with indication module by NPP «Stels» is connected to the expander (see figure 4.5).
  - *STEMAX RFID*: if the STEMAX RFID proximity reader by NPP «Stels» (no longer in production) is connected to the expander (see figure 4.6).
- *Partition of REG output:* defines the partition the guard mode of which is going to be displayed by the device connected to the REG output of this zone expander.
- *Partition for arm/disarm with an electronic key:*
  - *Only 1 — Only 15*: select one partition if the control device connected to this zone expander should be able to arm/disarm only a specific partition.

Note — If you selected a specific partition in *the Partition for arm/disarm with an electronic key* parameter, it becomes possible to select several partitions for one electronic key/code in the *Keys and codes* tab of the main controller. After it you can arm/disarm different partitions with one electronic key. In this case, the controlled partition is defined by the reader the key is applied to. For example, if *Only partition 3* is selected for the zone expander's reader, and partitions 3, 5, and 7 are selected for the electronic key, then when you touch the reader with this key, the main controller changes the guard mode of partition 3 only. If next you apply the same key to the reader of another zone expander for which *Only partition 5* is selected, the security mode changes only for partition 5.

  - *Any:* select this value if the number of the controlled partition should be determined by the settings of the electronic key/code. If several partitions are selected for the key on the *Keys and codes* tab of the base controller, the security mode changes for the partition with the smallest number of those allowed for the key. For example, partitions 3, 5, 7 are selected for

the key. When the owner touches the reader of this zone expander with this key, the security mode of the partition 3 changes.

- *Generate event 'RS-485 — Failure:* if *Yes* is selected, then the controller generates an *RS-485 Alarm* event in case of a malfunction of the RS-485.

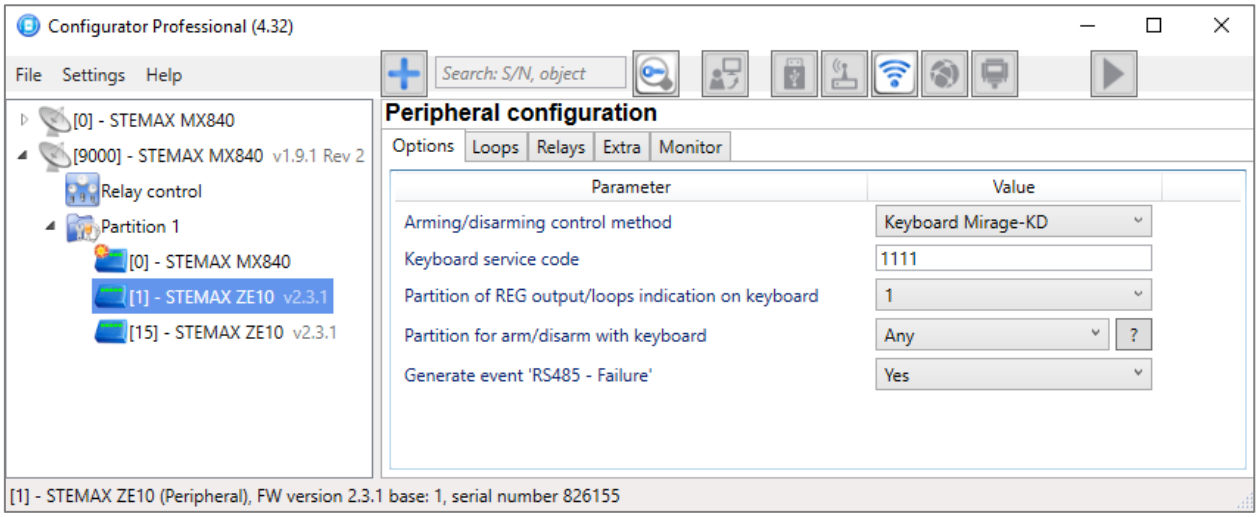

Figure 4.4. Expander configuration, *Options* tab

If you select *Keyboard Mirage-KD* as an arming/disarming method, additional parameters are displayed:

- *Keyboard service code:* a field for entering a 4-digit combination that you need to enter on a STEMAX-KD keypad before entering service codes.
- *Partition of REG output/loops indication on keyboard:*
  - a partition, the guard mode of which is displayed by a device connected to the REG output of this zone expander,
  - a partition, the state of ALs of which is displayed by indicators on the keypad connected to this zone expander. If more than 8 ALs are added to the selected partition, enter 2* on the keypad to display the state of ALs 9—16, 3* to display the state of ALs 17—24 and so on up to 20* (ALs 152—158). To get back to ALs 1—8, enter 1*.
- *Partition for arm/disarm with keyboard:* select a partition in the same way as for the parameter *Partition for arm/disarm with an electronic key* described above.

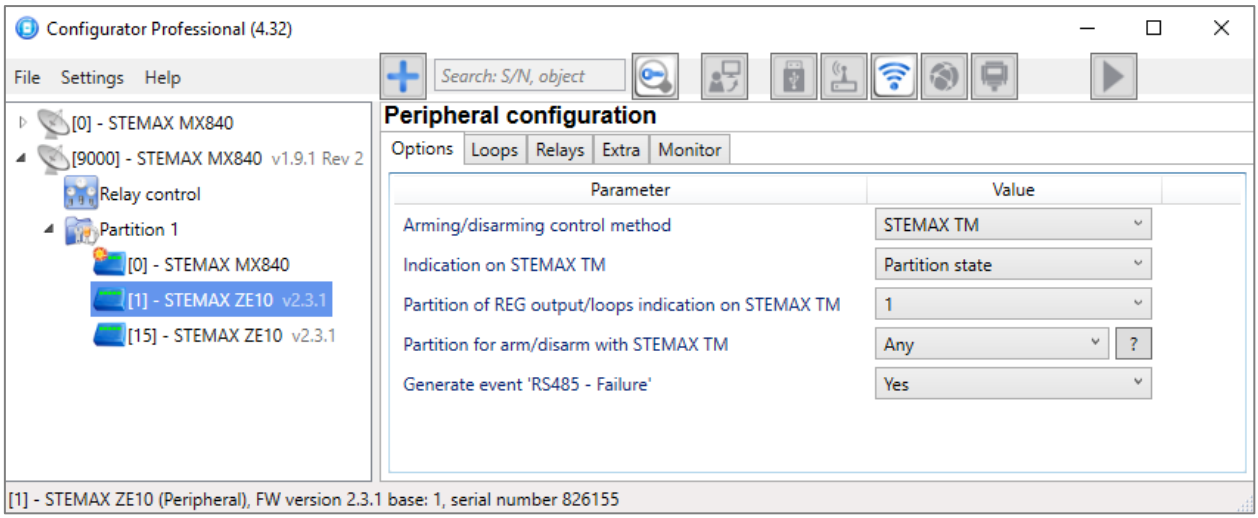

Figure 4.5. Expander configuration, *Options* tab

If you select *STEMAX-TM* as an arming/disarming method, additional parameters are displayed:

- *Indication on STEMAX TM:* information to be displayed by the STEMAX TM reader indicators. It is possible to display AL state or partition state.
- *Partition of REG output/loops indication on STEMAX TM:*
  - a partition, the guard mode of which is displayed by a device connected to the REG output of this zone expander,

- a partition, the guard mode of first 8 partitions of which is displayed by indicators on the reader connected to this zone expander, in case *Loops state* is selected for the *Indication on STEMAX TM* parameter.

Note — If *Partition state* is selected for the *Indication on STEMAX TM* parameter, the indicators on the reader display the state of the first 8 partitions (regardless of the partition selected for the *Partition of REG output/loops indication on STEMAX TM*).

- *Partition for arm/disarm with STEMAX TM:* select a partition in the same way as for the parameter *Partition for arm/disarm with an electronic key* described above.

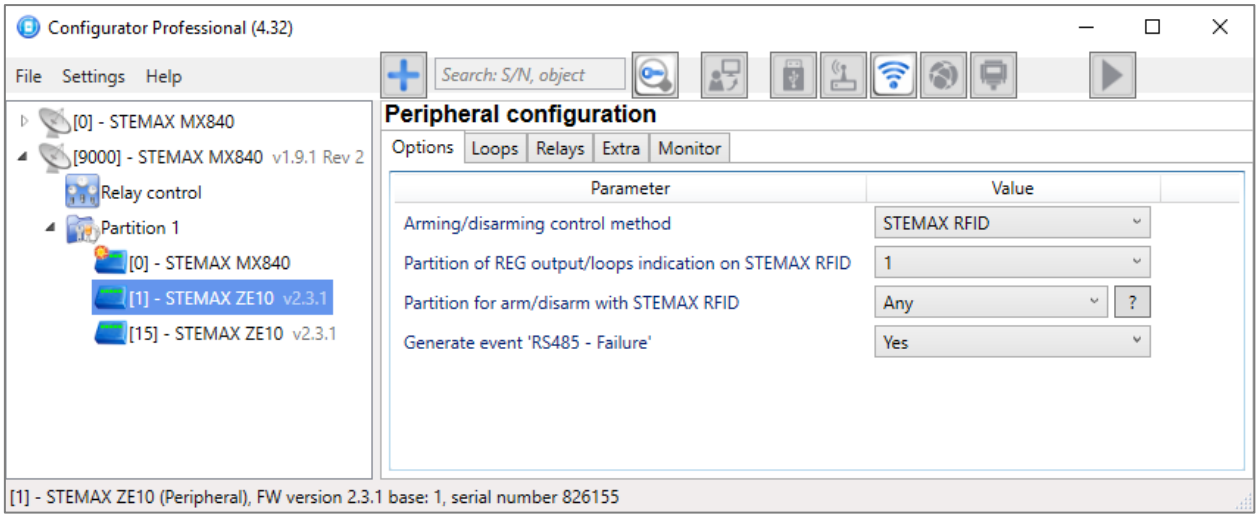

Figure 4.6. Expander configuration, *Options* tab

If you select *STEMAX RFID* as an arming/disarming method, additional parameters are displayed:

- *Partition of REG output/loops indication on STEMAX RFID:*
  - a partition, the guard mode of which is displayed by the device connected to the REG output of this zone expander,
  - a partition the state of the first 8 ALs of which are displayed by the *Zone* indicator of the reader connected to this zone expander.

Note — *Partition* indicators of the reader display the state of the first 8 partitions (regardless of the partition selected for the *Partition of REG output/loops indication on STEMAX RFID* parameter).

- *Partition for arm/disarm with STEMAX RFID:* select a partition in the same way as for the parameter *Partition for arm/disarm with an electronic key* described above.

4.2.2 Loops tab

This tab is used for setting the parameters of wired alarm loops connected to the zone expander and for distributing them between partitions.

The main part of the tab is designed as a table with the columns described below.

- *#:* the number of the loop. You can change the number of the AL to any other number unused by other ALs or Livi radio devices at the site. To change the number, left-click on it and select a new number from the drop-down list.
- *Loop type:* alarm loop type (see more on the loop types in the Appendix C on page 30).
- *Attributes:* parameters of the alarm loop operation (see more on attributes in the Appendix C on page 30). The set of available attributes depends on the type selected for the loop. Left-click on an attribute icon to activate a corresponding function (to set an attribute). Left-click on it again to deactivate the function. If it is required to set or deactivate an attribute for all guard loops at once, press and hold the Ctrl or Shift key on the keyboard and click on the attribute icon in any line.

Note — It is impossible to assign the attributes *Armed schedule* and *Auto arm* or *Round-the-clock* to the same loop.

- *Partition:* a partition of the main controller to which a loop of the zone expander should be assigned.

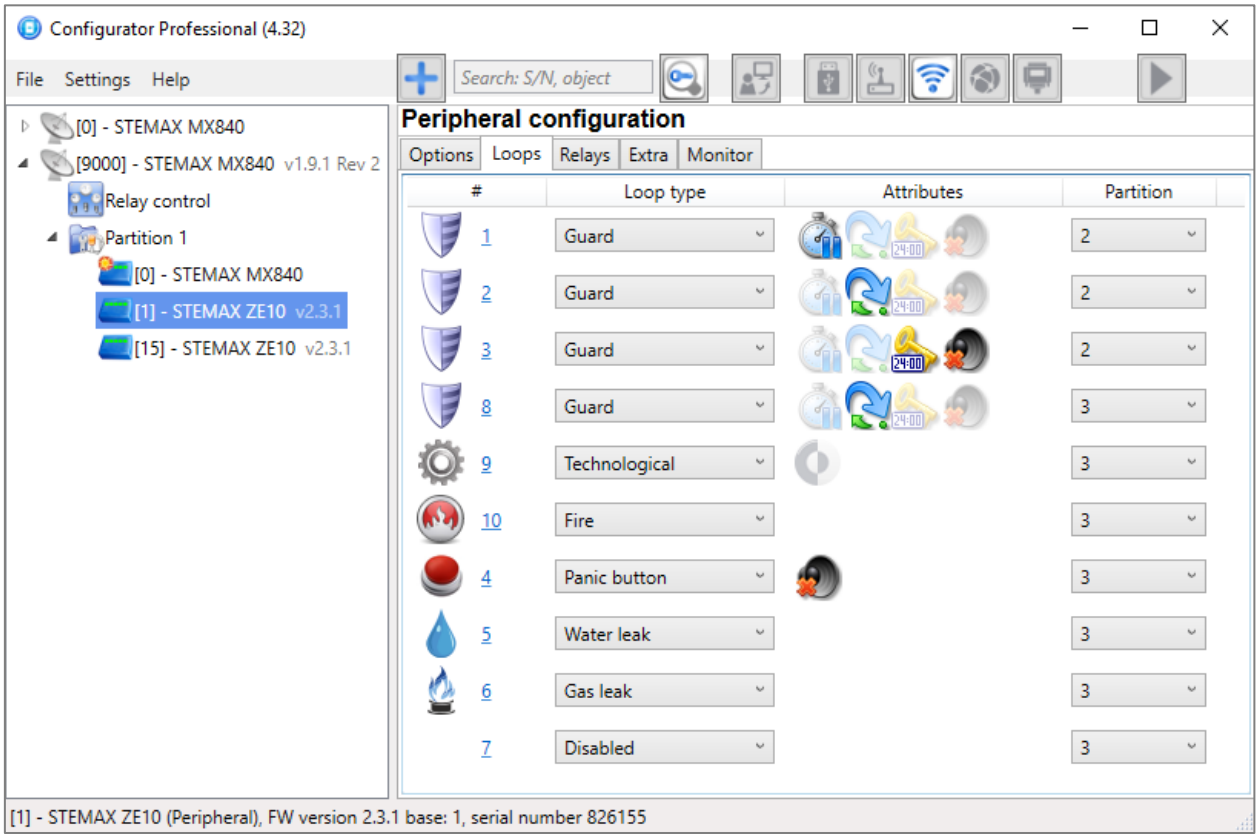

Figure 4.7. Expander configuration, *Loops* tab

4.2.3 Relays tab

The *Relays* tab is used for configuring activation settings of *open collector* control outputs. The outputs are used for connecting external devices with various electrical specifications and for controlling them.

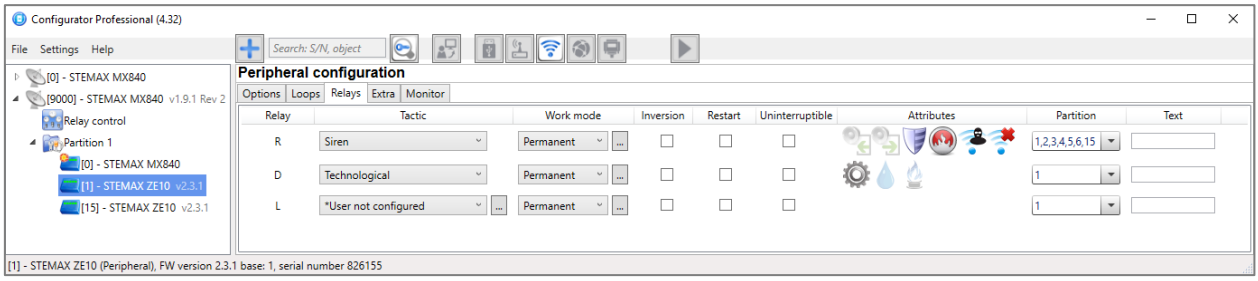

Figure 4.8. *Relays* tab of the zones expander configuration

The tab is designed as a table with the columns described below.

- *Relay:* the output name on the connection board of the controller.
- *Tactic:* selection of a general tactic for the output operation. A set of additional settings for the output operation and activation conditions depends on the tactic selected (see Appendix D on page 32).
- *Work mode:* setting of the output activation pattern and duration.
  - *Permanent:* constant voltage supply to the activated output.
  - *Impulse:* pulse voltage supply to the activated output.
- *Inversion:* if this box is not checked, then the output is deactivated when the value of the "alarm counter" = 0 and activates when the value of the "alarm counter" ≥ 1. If this box is checked, then the output is activated when the value of the "alarm counter" = 0 and it deactivates when the value of the "alarm counter" ≥ 1. See more on the "alarm counter" in Appendix D on page 32.
- *Restart:* if this box is checked, then the application of the output tactics restarts on every activation event.
- *Uninterruptible*: if this box is checked, then the application of the output tactics is not interrupted by any deactivation event. Only deactivation at once events interrupt the tactic application.

For example, if a fire detector was triggered and generated an *Alarm* event, then the output with the *Siren* tactic is activated. A *Recovery* event generated by the same detector is not going to deactivate the output if the *Uninterruptible* parameter is activated for the output. In this case, to stop the alarm you can disarm the partition (*Mode: Disarmed* is an event for deactivation at once for the *Siren* tactic).

- *Attributes:* selecting activation conditions for the *Siren* and *Technological* tactics (see Appendix D on page 32). You can select all attributes or any combination of them.
- *Partition:* selection of partitions events from which trigger the output.
- *Text:* information about the control output, for example, an endpoint device controlled by the output.

Note — The information from the *Text* field is not transmitted to the STEMAX server as a part of a notification and is not written into the controller memory. It is saved only in the configuration file on your PC.

If at least one *open collector* output is assigned the tactic *Relay control* (capability of remote manual control) in the *Relays* tab, then to set activation and remote control parameters of these outputs you need to move to the *Relay control* tab in the controller configuration (see user manual for the main controller available on the NPP «Stels» website).

When the *Siren*, *Malfunction*, *Technological*, or *User defined* tactics are selected, you can fine-set the output work mode. To do this, click the ... button, which appears on the right side of the *Work mode* column. The window *Work mode settings for relay X* where X is the name of the output opens (see figure 4.9). In this window, the following parameters can be set.

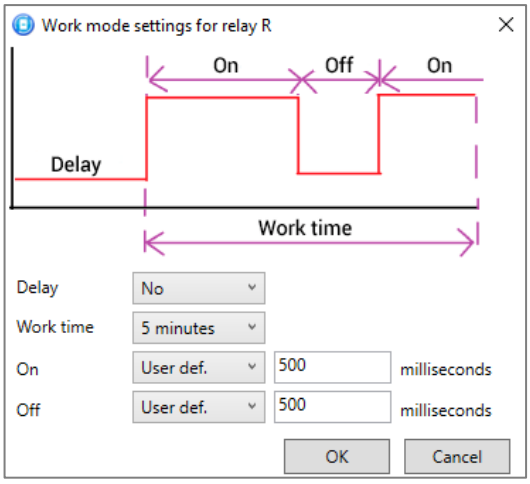

Figure 4.9. Work mode settings for relay R *window*

- *Delay:* a delay between an event generation and output activation.
- *Work time:* the time an output stays active after its activation.
- *On:* the time of voltage supply to the output. You can select the time from the list or manually set it in the field on the left in milliseconds if *User def.* option is selected.
- *Off:* the time without voltage supply to the output. You can select the time from the list or manually set it in the field on the left in milliseconds if *User def.* option is selected.

The upper part of the window displays a graph that illustrates the activation pattern of an output in the selected work mode and explains the settings.

4.2.4 Extra tab

The *Extra* tab (see figure 4.10) is used for setting the parameters described below.

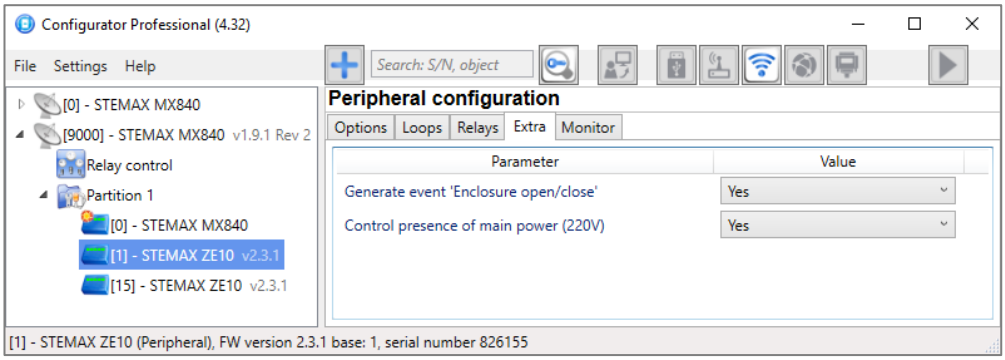

Figure 4.10. *Extra* tab

- *Generate event 'Enclosure open/closed'* (*Yes/No):* if *Yes* is selected, then an *Enclosure closed* or an *Enclosure open* event is generated whenever the state of the tamper detection sensor of the controller changes.
- *Control presence of main power (220V) (Yes/No*): if Yes is selected, then the *Power 220V Failure* event is generated whenever the main power supply fails for 3 minutes or longer. When the main power is restored for at least 3 minutes, then a *Power 220 V OK* event is generated.

4.2.5 Monitor tab

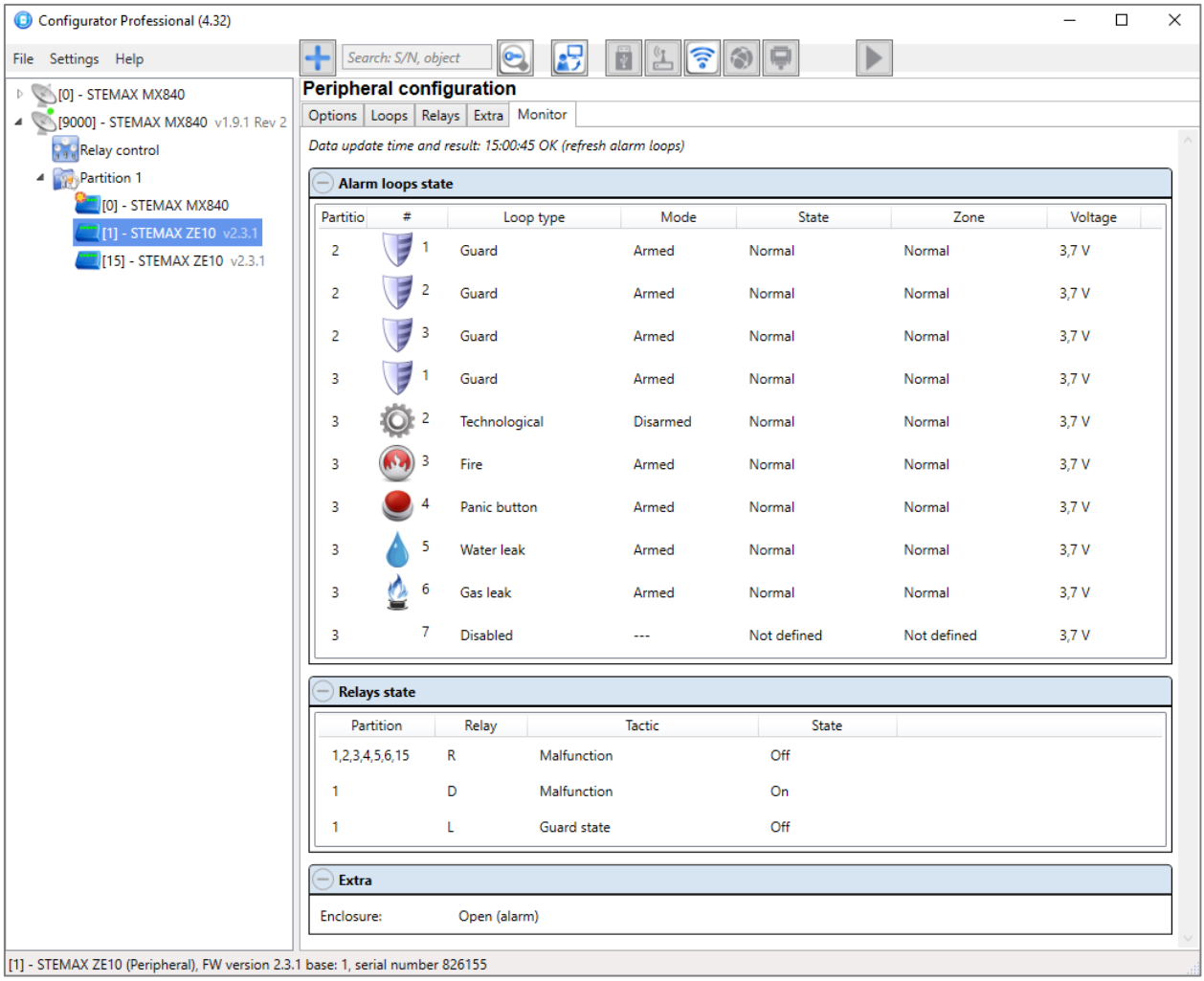

Figure 4.11. *Monitor* tab

The *Monitor* tab displays the current status of the zone expander. The information is automatically updated in real time if there is an online connection between the *STEMAX Configurator* program and the main controller.

In the *Alarm loops state*, the *Zone* column displays the value of the parameter at the moment (regardless of the hold timer), and the *State* column displays the value recorded as per the hold timer settings. You can set the control time in the *Loops* tab of the main controller peripheral configuration.

For example, in case of an open circuit, if the control time has not elapsed yet, the *Zone* column of the AL displays *No* and the *State* column displays *Yes* during the hold timer countdown.

4.3 DELETING THE ZONE EXPANDER FROM THE CONTROLLER CONFIGURATION

If you need to delete the zone expander from the controller configuration, right-click on its line in the device tree and select *Delete* in the menu that opens. Then right-click on the main controller name in the device tree and select *Write configuration* in the context menu **or** press F2 button on you PC's keyboard.

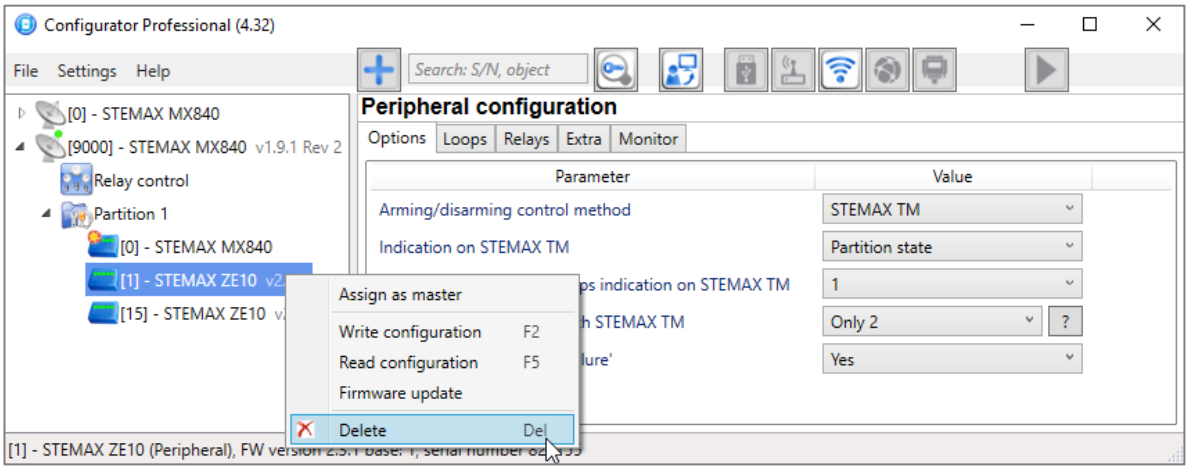

Figure 4.12. Removing the zone expander

4.4 PARTITION CONFIGURATION OF THE EXPANDER

As the expander operates only as an AL number expander of its main controller, its ALs belong to the partition of the main controller. To select arming/disarming method, subdue logical partitions to each other, save electronic keys and codes etc., left-click on the line of the partition of the main controller in the device tree and configure it. See more on configuring the partition of the main controller in its used manual available on [the NPP «Stels» website](#).

4.5 CONTEXT MENU OF THE ZONE EXPANDER

To display the expander context menu (see figure 4.13), right-click on it in the device tree. The following functions are available in the menu:

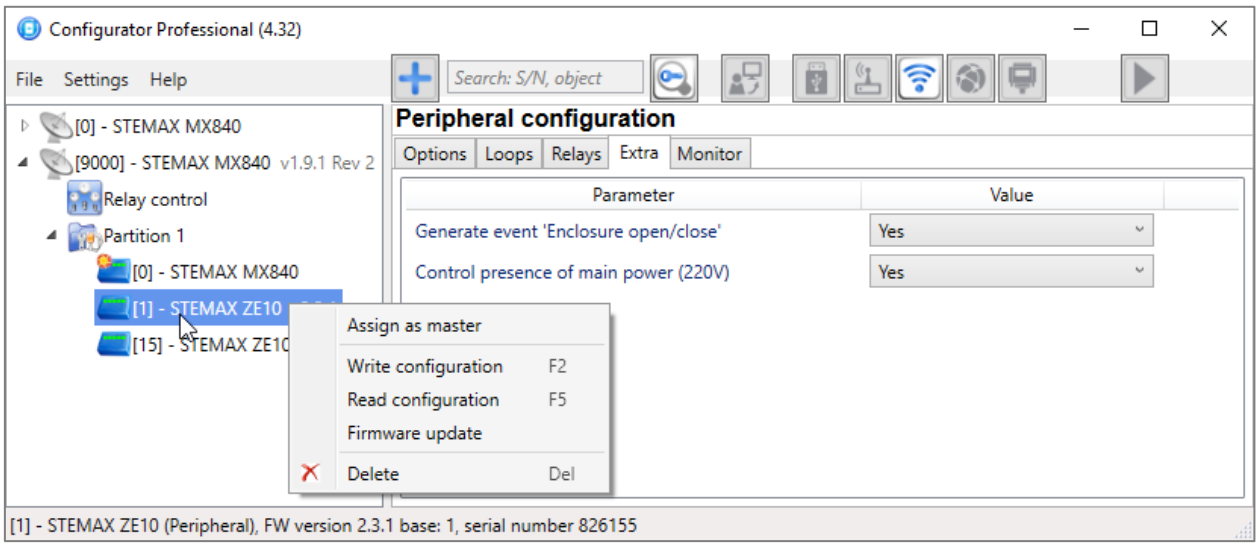

Figure 4.13. Zone expander context menu

- *Assign as Master:* not applicable. The main controller is the Master one.
- *Write configuration:* writing the parameters set in the *STEMAX Configurator* into the expander.

- *Read configuration:* loading the parameters set in the expander into the *STEMAX Configurator* software.
- *Load configuration as template:* clicking on this option opens the *Download template notification*
- *Firmware update:* updating the firmware of the zone expander (see 6.2).
- *Delete:* deleting the zone expander from the *STEMAX Configurator* software (see 4.3).

5 INTENDED USE OF THE ZONE EXPANDER

5.1 RECOMMENDATIONS FOR THE EXPANDER INSTALLATION

When choosing a location for installing the expander, we recommend that the following criteria are met:

- limited access for unauthorized persons;
- maximum distance from entrance doors and windows.

5.2 INITIALISING THE ZONE EXPANDER

When you start or restart the expander, it goes into functional control mode: it checks its main functional blocks. Upon completion of the functional control, the expander starts normal operation in the same guard mode (armed or disarmed) in which it was when the power was turned off or when it was restarted.

5.3 ZONE EXPANDER APPEARANCE

The expander consists of two parts: panel board and external connection board (see Appendix A on page 27). Connection board and panel board are connected with two connectors, so you can dismantle the expander to change or repair it without disconnecting external connections.

The expander enclosure is made of ABS plastic and consists of a base and a lid. To disconnect the lid from the base, press on the latches on the top of the expander. The boards are located on the base of the enclosure. The lid has indicator labels on it. The enclosure design allows for two-way wiring. The zone expander enclosure appearance is provided in figure 5.1. The expander can be mounted on a DIN rail.

Figure 5.1. Appearance of the STEMAX ZE10 with the lid (front view)

5.4 INDICATION

The face of the device (see figure 5.2) has LED indicators described in table 5.1. See indication pattern for guard alarm loops in table 5.2.

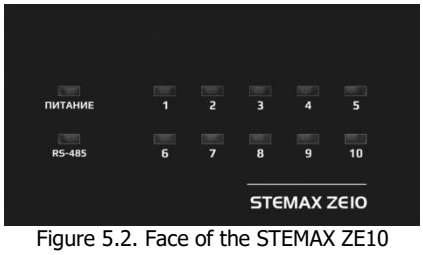

Figure 5.2. Face of the STEMAX ZE10

Table 5.1. LED indication pattern of the STEMAX ZE10

Indicator name	Description	Indication	State description
POWER	Indication of power supply from the external 12 V source	green constant	Power supply from the external 12 V source
		yellow constant	Power below 10 V
		not lit	No power supply

Table 5.1. LED indication pattern of the STEMAX ZE10

Indicator name	Description	Indication	State description
RS-485	RS-485 interface status	green constant	Communication over RS-485 interface OK
		green flashing	Expander firmware update
		yellow constant	Interrupted communication over RS-485 interface
"1" **"2"** **"3"** **"4"** **"5"** **"6"** **"7"** **"8"** **"9"** **"10"**	Alarm loop state	green constant	The loop is OK / in the *Armed* state
		red constant	The loop is in the *Alarm* state
		yellow flashing	The loop is in the *Malfunction* state
		not lit	The loop is the *Disarmed* state

AL and RS-485 indicators are also used for displaying the network address of the zone expander (see 3.3).

Table 5.2. Indication and local signaling for guard ALs

Operation mode	Guard alarm loop status	Alarm loop indicator	L output, sec	R output	D output
Disarmed	OK	Off	Off	Off	Off
Arming	—	Off	0.5 sec / 0.5 sec during a set delay time	Off	Off
Armed	OK	Off	On	Off	Off
Armed with a malfunctioned AL	Malfunctions of separate ALs	Flashes twice (0.5 sec / 0.5 sec), then lit for 2 sec	Flashes twice (0.5 sec / 0.5 sec), then lit for 2 sec	Off	On
Armed	Alarm	On	Flashes twice (0.5 sec / 0.5 sec), then lit for 2 sec	On	Off

Table 5.2 describes operation of the outputs L, R and D for the default tactics setting. You can assign any tactics to any output (see 5.4.2). In case you change the operation tactics of the outputs, then read the table in the following way: L output = *Guard mode lamp* tactics, R output = *Siren* tactics, D output = *Malfunction lamp* tactics.

5.5 ALARM LOOP MONITORING

Operation of the zone expander is based on AL resistance monitoring. An event is generated in case of any change in resistance that exceeds the limits set. The change may be caused by triggering of signaling devices or mechanical damage to an alarm loop. When notification is generated, an AL triggering indicator on the face of the expander lights up and in case relevant equipment is available and configured, a beeper (siren) activates and a strobe light (lamp) starts flashing. The events are transmitted to the main controller over RS-485 network and are stored in its event log.

The expander registers the resistance of the alarm loops beyond the threshold values if it lasts for over 300 ms and does not register it if it lasts less than 250 ms.

If an alarm loop with the *Round-the-clock* attribute is triggered, an *Alarm* event is generated regardless of the guard mode of the partition it belongs to.

See resistance threshold values for alarm loops in table 5.3.

Table 5.3. Alarm loop resistance threshold values

Notification	**Alarm loop resistance, Ω**
OK	4700—6400
Alarm (short circuit)	< 3600
Alarm (open circuit)	> 8200

6 MAINTENANCE AND ROUTINE REPAIRS

6.1 MAINTENANCE

It is necessary to regularly inspect and maintain the zone expander during its operation. An interval between inspections depends on the operating conditions. Maintain the expander at least once a year. Failure to comply with the operating conditions may result in failure of the expander.

Regular inspection of the expander is performed to:

- check its operating conditions;
- check the absence of external damage to the expander;
- check the absence of cable rupture or insulation breakdown;

Maintain the expander when there are false alarms, the signal strength is low, notifications take a long time to arrive, etc.

WARNING

Maintain the expander only when it is completely de-energized.

The maintenance includes:

- checking connections;
- removing dust from the surface of the board;
- checking contacts for rust and oxidation.

6.2 UPDATING FIRMWARE OF THE STEMAX ZE10 ZONE EXPANDER

Attention

Firmware update is possible only when the STEMAX ZE10 zone expanders are connected to the STEMAX MX840 controller.

New versions of the firmware are available on the NPP «Stels» website on the relevant pages of the devices.

To update the firmware of the expander, follow the steps below.

1. Connect the STEMAX ZE10 zone expander to the STEMAX MX840 controller and add it into the controller's configuration (see 3.2).
2. Right-click on the controller name in the device tree and select *Firmware update* in the context menu (see figure 6.1).
3. In the window *Firmware update* (see figure 6.2), specify the path to the new firmware file for the zone expander on your PC (an **.sbin** or an **.sbinx** file) and click *Start*.

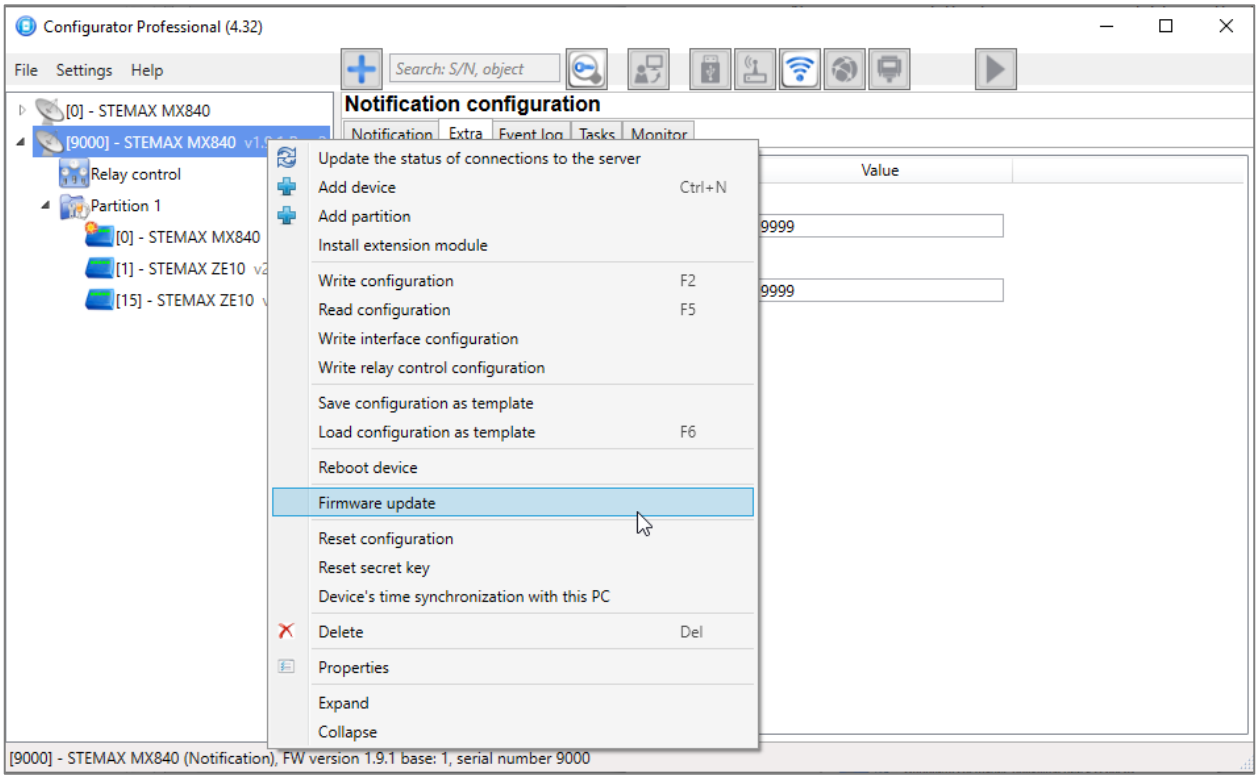

Figure 6.1. The STEMAX MX840 controller context menu

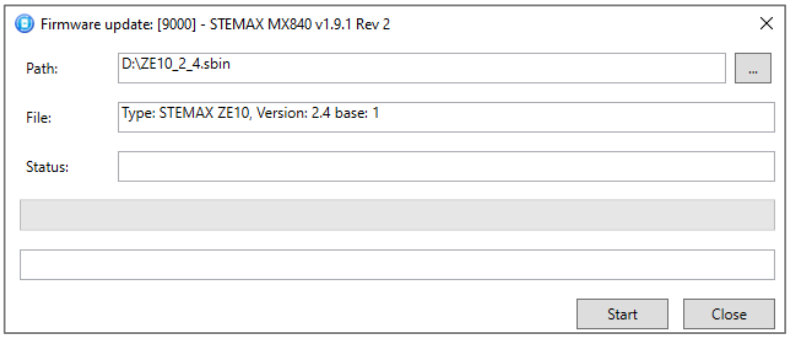

Figure 6.2. Firmware update window

In the *File* field, properties of the selected file (firmware version and the model of the device it is built for) are displayed automatically.

The progress of firmware updating is graphically displayed by a progress bar in the lower part of the window. The *Status* field displays the number of the packet that is being transferred. The window closes automatically at update completion.

In case several zone expanders are connected to the controller, the main controller sequentially checks the firmware version of each zone expander connected to it and updates the firmware only if its version is older than the one used for updating.

6.3 ROUTINE REPAIRS

Warranty service and repairs of the zone expander must be carried out by specialists of the Manufacturer.

7 TRANSPORTATION AND STORAGE

7.1 TRANSPORTATION

Zone expanders packaged according to 1.6 can be transported by all modes of transport in covered vehicles, except for non-pressurized aircraft compartments. They should be handled in accordance with the transportation rules applicable to the mode of transport used.

During transportation, the shipping container must be protected from atmospheric precipitation. Arrangement and fastening of cargo in vehicles must ensure a stable position of the container during transportation. It is allowed to transport the zone expanders without packaging within a city, if they are protected against atmospheric precipitation and shock during transportation.

7.2 STORAGE

Packaged zone expanders should be stored in warehouses at a temperature from minus 25 °C to plus 70 °C and a relative humidity of no more than 85%.

It is prohibited to store the expanders in places where acids, alkalis, and other aggressive impurities are present in the air.

8 DISPOSAL

Disposal of all parts of the expanders must be carried out in accordance with the local legislation.

At disposing, take into account that the device belongs to the hazard class 4 (low hazard waste as per the laws of the Russian Federation).

The content of precious metals: accounting during storage and disposal is not required.

APPENDIX A — APPEARANCE OF THE ZONE EXPANDER WITH ITS LID OPEN

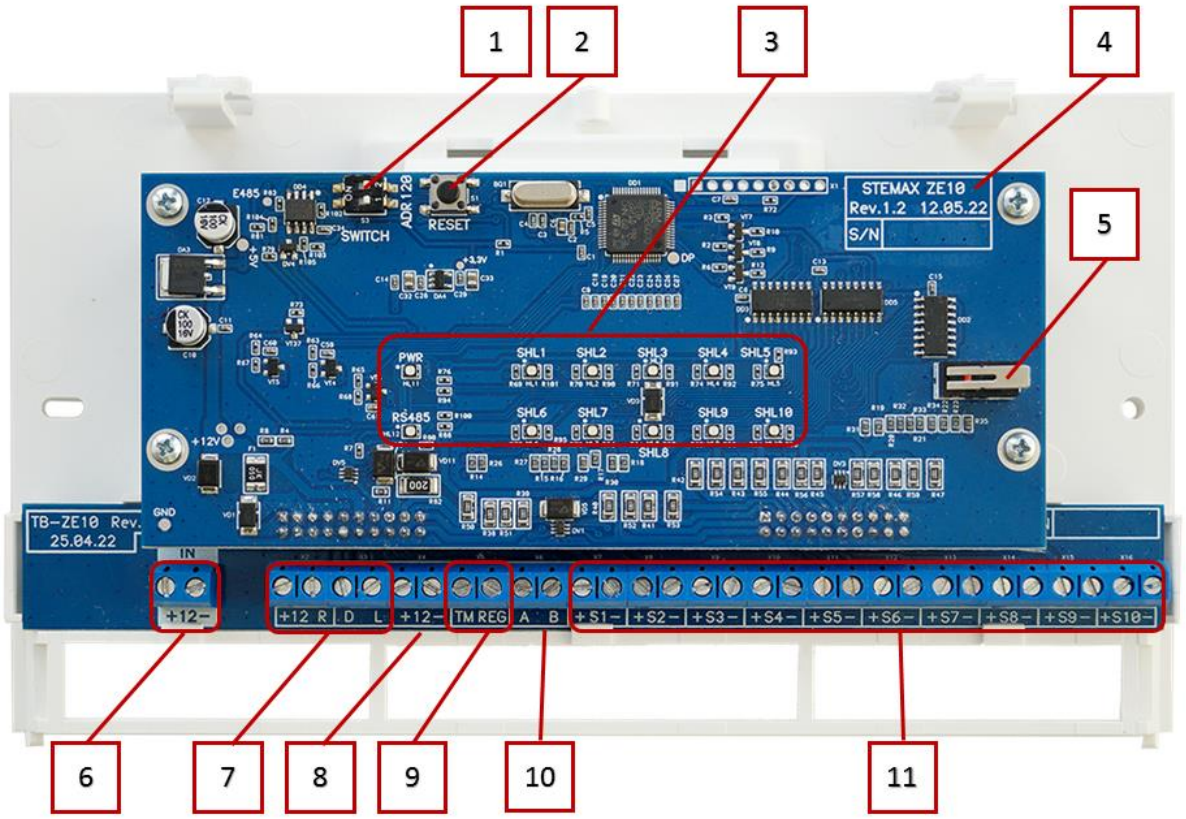

Figure A.1. Zone expander appearance with its lid open

1) ADR microswitch (for changing the network address) and 120 Om microswitch (for impedance matching for RS-485 interface)
2) RESET button
3) Indicators
4) Labelling: device type, board revision, manufacturing date, serial number
5) Tamper detection sensor button
6) Power input terminals (12 V) of the expander
7) *Open collector* output terminals(R, D, L) and a +12 V output terminal
8) 12 V power supply output terminals of external devices
9) Touch Memory reader and REG indicator connection terminals
10) RS-485 interface terminals
11) Alarm loop terminals

APPENDIX B — EXTERNAL CONNECTION DIAGRAM

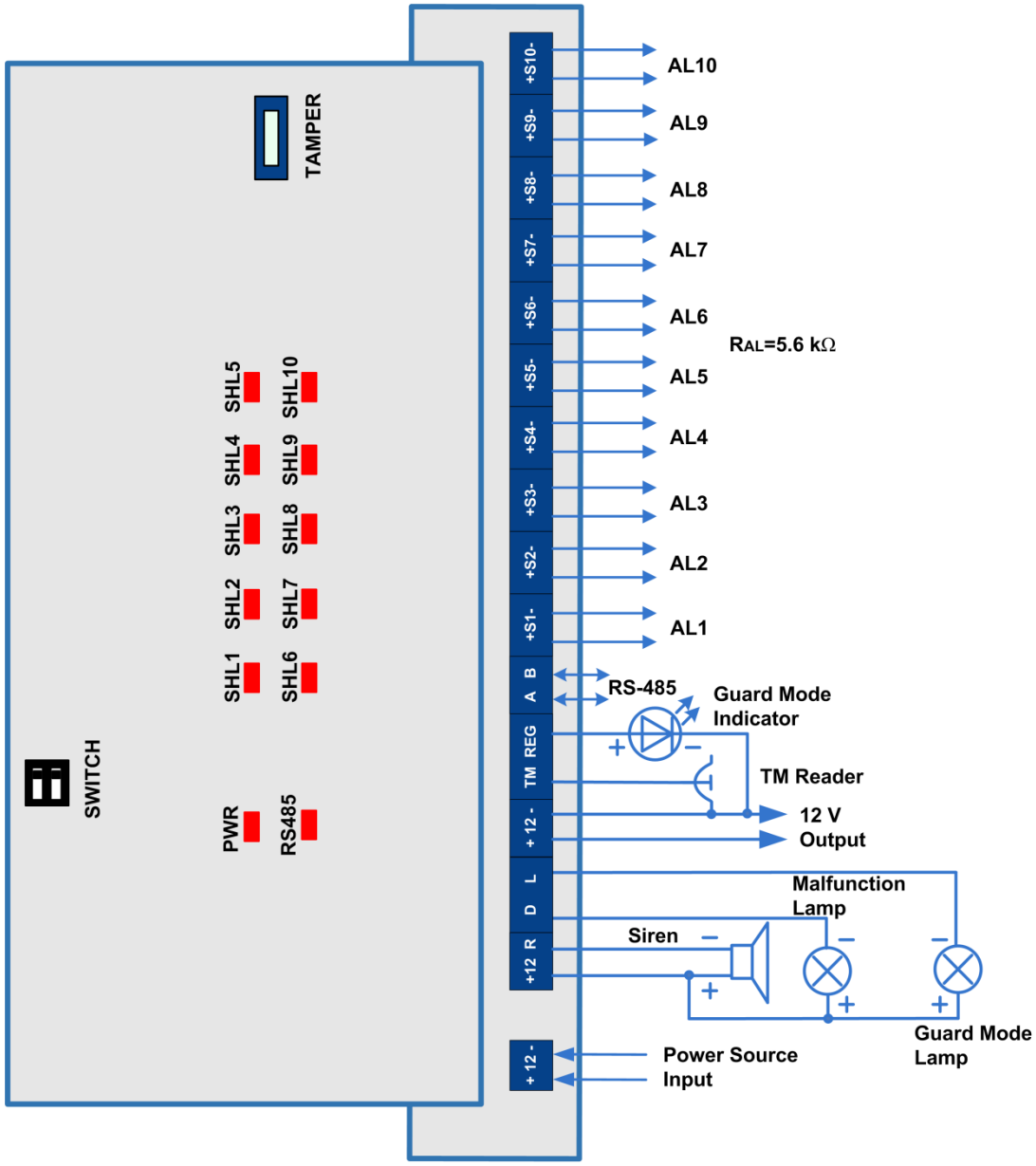

Figure B.1. STEMAX ZE10 external connection diagram

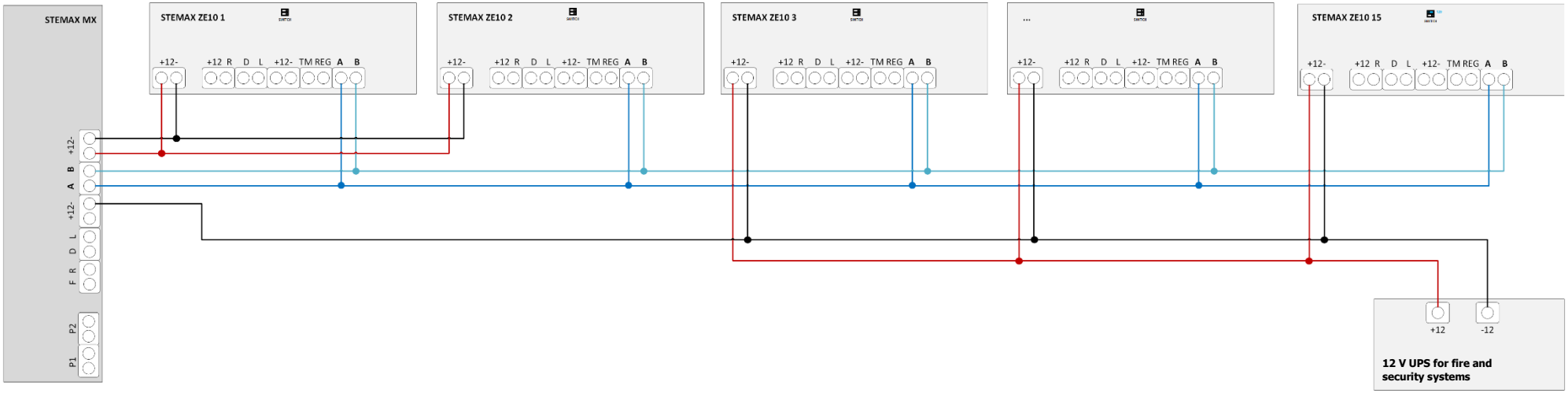

Figure B.2. A typical wiring diagram for connecting 15 STEMAX ZE10 expanders to a controller of the STEMAX MX series

APPENDIX C — ALARM LOOP TYPES AND ATTRIBUTES

Table C.1. Types of alarm loops

Alarm loop type	Description
Guard	A loop triggering of which induces generation of an *Alarm* event. Any security sensors with *dry contact* output can be connected to the loop. A 5.6 kΩ resistor is included in the alarm loop in parallel or in series depending on triggering patter of its sensors (on sensor opening or closing at triggering). The loop is monitored by the resistance: 5.6 kΩ is a *Normal* state, short or open circuit is an *Alarm* state. Guard loop power supply voltage is (4.6 ± 0.3) V.
Technological	A loop for connecting technological signaling sensors. The loop is monitored by its state: closed — normal state, open — alarm state (digital AL). The loop is monitored continuously (regardless of the controller guard mode). An *Alarm — Technological* event is generated at its triggering. This event is NOT treated as an alarm event. You can change the loop triggering conditions using the *Inversion* attribute (see table C.3).
Panic button	A loop for connecting a panic button. The loop is monitored in the same way as guard alarm loops, but its monitoring is continuous regardless of the controller guard mode. Its triggering induces generation of a *Panic button alarm* event.
Water leak sensor	A loop for connecting water leak sensors. The loop is monitored continuously regardless of the controller guard mode. Its triggering induces generation of a *Water leak alarm* event.
Gas leak sensor	A loop for connecting gas leak sensors. The loop is monitored continuously regardless of the controller guard mode. Its triggering induces generation of a *Gas leak alarm* event.
Disabled	If an alarm loop is not used, assign the *Disabled* type to it. The alarm loops with this tactic are not monitored.

Table C.2. Attributes of guard alarm loops

Attribute	Pictogram	Description
Delay		Delay for entry function. The function is used when a site is **disarmed** using a device inside the site (after a user enters the site). When a loop or a radio device without this attribute is triggered, an *Alarm* event is generated immediately. When a loop or a radio device with the *Delay for entry* attribute is triggered, an *Alarm* is generated only after the delay time elapses (if the site is not disarmed within the delay time period). The duration of the *Delay* is set separately for each partition in the *Disarm delay, sec* column in the *Options* tab (Partition configuration block).
Auto arm		Automatic alarm reset and arming of a loop / radio device after its state has been *Normal* for the period of time set in the partition parameters. The attribute can be used for technological sensors.
Round-the-clock		A loop / radio device stays armed round-the-clock regardless of the controller guard mode. This attribute can be used for panic buttons and technological sensors.

Table C.2. Attributes of guard alarm loops

Attribute	Pictogram	Description
Quiet alarm		Alarm events are generated without any sound or light indication of the alarm triggered by the alarm loop. This attribute can be used for panic buttons and technological sensors.

Table C.3. Attributes of technological alarm loops

Attribute	Pictogram	Description
Inversion		By default, a loop input is normally closed (NC): closed — *normal* state, open — *alarm* state. If the *Inversion* attribute is assigned, a loop input becomes normally open (NO): open — *normal* state, closed — *alarm* state.

Table C.4. Attributes of *Panic button* alarm loops

Attribute	Pictogram	Description
Quiet alarm		Alarm events are generated without any sound or light indication of the alarm triggered by the alarm loop. This attribute can be used for panic buttons and technological sensors.

APPENDIX D — USE TACTICS AND ATTRIBUTES OF OPEN COLLECTOR OUTPUTS AND CONTROL OUTPUTS

Table D.1. Use tactics of *open collector* outputs and control outputs

Name	Description
Fire	A tactic for devices that need to be activated at a *Fire* event. Specify output activation pattern in the *Work mode* column.
Siren	A tactic for light and sound signaling devices. Specify activation conditions of an output with this tactic in the *Attributes* column (see table D.2) and activation pattern in the *Work mode* column.
Guard state	A tactic for guard mode indication devices.
Malfunction	A tactic for devices that indicate malfunctioning of alarm loops. Specify output activation pattern in the *Work mode* column.
Technological	A tactic for devices that need to be activated when technological loops of various types are triggered. Specify activation conditions of the output with this tactic in the *Attributes* column (see table D.3) and activation pattern in the *Work mode* column.
Arm block	A tactic for indication devices that notify about the suspension of the security service by your security company due to non-payment: the output is activated when the controller arming is blocked by the STEMAX server.
Communication line failure	A tactic for devices notifying about loss of communication with the STEMAX server via online channel. The output is activated if communication is lost for 1 minute or more.
User defined	A tactic that allows user to specify the conditions and logic of the output activation. Select the events to which the output reacts (activates or deactivates) and the way the "alarm counter" changes in case of each event (in the *User defined tactic settings for relay* window). The output activation details can also be specified in the *Work mode* column. See more on configuring the *User defined* tactic below.
CMS fault	A tactic for transmitting information on malfunctions (short or open circuit, AL arming failure) to a central monitoring station connected directly to the output. It is activated when a malfunction occurs. Specify output activation pattern in the *Work mode* column.
Thermoregulation	A tactic for automating the control of a heating or cooling system at the site. When this tactic is selected, the relay switches on and off automatically to maintain the temperature set in the T °C column. It is controlled based on the readings of the selected measurement channel specified in the *Measurements* tab of the main controller. The permissible deviation of the temperature from the desired one (hysteresis) is set in the ΔT °C column The smaller the hysteresis set, the more often the output is switched on/off.
Relay control	A tactic that allows to remotely manually control an output using the buttons in the *Relay control* tab of the STEMAX Configurator, from the site cards on the STEMAX server (from the STEMAX Administrator), and from the STEMAX mobile app. See more on relay control in user manual of your main controller (available on the NPP «Stels» website).
Disabled	The output is always deactivated.

Table D.2. Attributes of the control outputs with the *Siren* tactic

Attribute	Pictogram	Description
Sound notification of arm delay		The output is activated to make repeated beeps during arm delay (Delay for exit).

Table D.2. Attributes of the control outputs with the *Siren* tactic

Attribute	Pictogram	Description
Sound notification of disarm delay		The output is activated to make repeated beeps during disarm delay (Delay for entry).
Alarms		The output is activated if an *Alarm* event is generated.
Fire		The output is activated if a *Fire* event is generated (by alarm loops of the *Fire* type).
Jamming		The output is activated if cellular signal jamming is detected.
Sensor loss		The output is activated if communication loss with any armed radio device is detected. If a radio device is disarmed, the output does not react at loss of communication with it.

Table D.3. Attributes of outputs with the *Technological* tactic

Attribute	Pictogram	Description
Technological reaction		The output reacts to the state of *Technological* loops / radio devices.
Water leak		The output reacts to the state of *Water leak* loops / radio devices.
Gas leak		The output reacts to the state of *Gas leak* loops / radio devices.

To configure the ***User defined*** **tactic**, follow the steps below:

1) Select the *User defined* tactic and click the ... button to the right of the *Tactic* cell.
2) In the *User defined tactic settings for relay: x* (where x is the output name) window, select the events that you want the output to react to and the way the "alarm counter" should change.

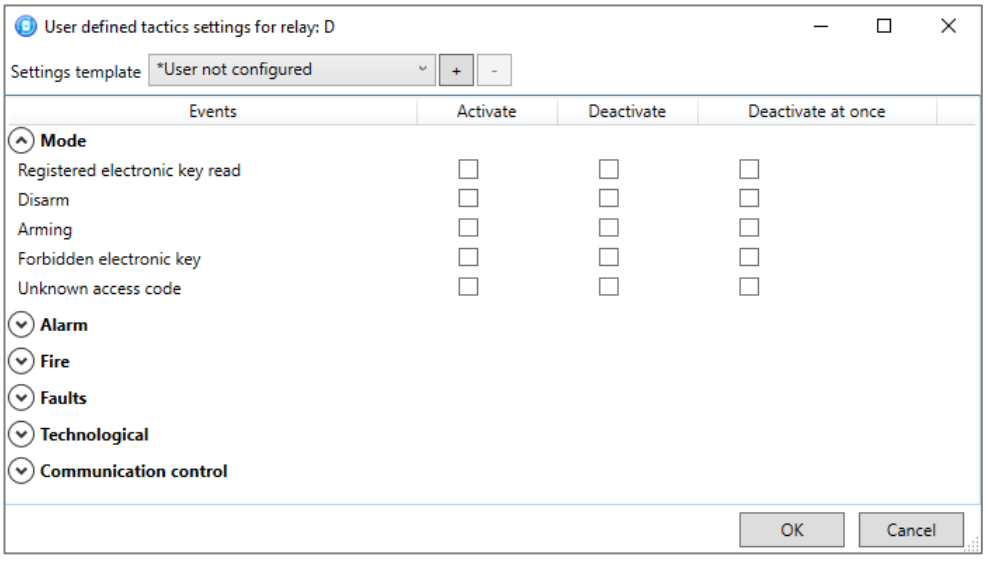

Figure D.1. Configuring a user defined tactic for a relay

The window *User defined tactic settings for relay* is designed as a table with the following columns:

- *Events:* evens that can induce output activation/deactivation.
- *Activate:* if a box is checked, a corresponding event adds 1 to the "alarm counter" (and the output activates).
- *Deactivate:* if a box is checked, a corresponding event subtracts 1 from the "alarm counter" (the output deactivates when the "alarm counter reaches 0).

- *Deactivate at once:* if a box is checked, a corresponding event sets the "alarm counter" for the output to 0 regardless of its previous value (and the output deactivates).

Note — Outputs with the Inversion box checked are active when their "alarm counter" = 0 and not active when their "alarm counter" ≥ 1 (see above).

Example: An *Alarm* event is selected as an event for output activation, an *Alarm Recovery* event as an event for its deactivation, and an *Arming* event as an event for deactivation at once. Three *Guard* loops in one of the partitions assigned to the output triggered and caused generation of three *Alarm* events. The "alarm counter" of the output now equals 3, therefore the output activates (in case the *Inversion* box is not checked). For deactivation of the output, thee *Alarm Recovery* events (causing the "alarm counter" value to sequentially decrease to 0) or one *Arming* event (causing the "alarm counter" value to be reset to 0 at once) must be generated.

You can select one of the predefined manufacturer's templates or a saved user defined template in the *Settings template* drop-down list on the top of the *User defined tactic settings for relay* window.

The following predefined manufacturer's templates are available:

- User not configured: no events are selected. User can select any events.
- Technological: enabling/disabling Technological loop are selected as activation and deactivation events.
- Siren:
  - all alarms except for silent alarm and fire 1 are selected as activation events,
  - alarm recovery events are selected as deactivation events,
  - arming, disarmed, and registered electronic key read events are selected as the events are selected as the events for deactivation at once.
- Malfunction:
  - malfunctions and loop failure are selected as activation events,
  - recoveries after malfunctions are selected as deactivation events,
  - arming and disarming are selected as the events for deactivation at once.
- Fire CMS:
  - a Fire 2 event is selected as an activation event,
  - Norm after Fire 2 is selected as a deactivation event,
  - arming, disarmed, and registered electronic key read events are selected as the events are selected as the events for deactivation at once.
- Fault CMS:
  - loop fault, control line faults, and loop failure events are selected as activation events,
  - recoveries after malfunctions are selected as deactivation events,
  - disarm event is selected as the event for deactivation at once.
- Alarm:
  - sensor — communication loss event and all alarm events except for silent alarm are selected as activation events,
  - recovery events are selected as deactivation events,
  - arming, disarmed, and registered electronic key read events are selected as the events are selected as the events for deactivation at once.

To save a user defined configuration as a template, click the  button, enter a name in the *Enter name of template* window and click *OK*.

To delete a template, select it in the drop-down list and click  (only user defined templates can be deleted).

APPENDIX E — TERMS AND ABBREVIATIONS

The terms used in this manual:

Acknowledgement	confirmation of information delivery
Alarm loop	an electrical circuit connecting the output circuits of signaling devices with the control module, designed to transmit notifications to the control module and to supply power to signaling devices
Firmware	software written to the non-volatile memory of the controller (microprogram)
Flush mount switch, hidden switch	an actual switch used for controller arming and disarming
Partition	a group of alarm loops and/or radio devices connected to the controller that are armed and disarmed with their own electronic key or code
RFID (Radio Frequency IDentification)	an authentication system that utilizes wireless scanners
Tamper detection sensor	a sensor that detects opening of the controller enclosure
Touch Memory	a system of electronic keys and readers used for authorization in security equipment
Transit area	the part of the room where signaling devices can be triggered upon entering and exiting the room (before the controller is disarmed and after it is armed when the functions of delay for entry and exit respectively are activated)
RS-485	a half-duplex multipoint serial data interface

The following abbreviations are used in this user manual:

AL	alarm loop
CMS	Central Monitoring Station
OC	open collector
PC	personal computer
UPS	uninterrupted power supply

APPENDIX F — TECHNICAL SUPPORT CONTACTS

If you cannot find the answer to your question in this Manual, contact our Technical support team:

e-mail:

support@nppstels.ru

APPENDIX G — DOCUMENT CHANGE LOG

Table G.1 — Document change log

Date	Version	Description
27.12.2024	1.0	The English version of the manual is created