



ELMOGWAY, ELMOGWAY2

Multi-protocol gateway between
EL.MO. control units and Home &
Building Automation systems

090021051





FOREWORD

FOR THE INSTALLER:

Comply strictly with current standards governing the installation of electrical systems and security systems, and with the manufacturer's directions given in the manuals supplied with the products.

Provide the user with full information on using the system installed and on its limitations, pointing out that there are different levels of security performance that will need to suit the user's requirements within the constraints of the specific applicable standards. See that the user looks through the warnings given herein.

FOR THE USER:

Check the system's operation thoroughly at regular intervals, making sure the equipment can be armed and disarmed properly.

Make sure the system receives proper routine maintenance, employing the services of specialist personnel who meet the requirements prescribed by current regulations.

Ask your installer to check that the system suits changing operating conditions (e.g. changes in the extent of the areas to be protected, change in access methods, etc...).

This device has been designed, built and tested with the utmost care and attention, adopting test and inspection procedures in accordance with current legislation. Full compliance of the working specifications is only achieved in the event the device is used solely for its intended purpose, namely:

Gateway between EL.MO. control units and Home & Building Automation systems.

The device is not intended for any use other than the above and hence its correct functioning in such cases cannot be assured.

Consequently, any use of the manual in your possession for any purpose other than those for which it was compiled - namely for the purpose of explaining the product's technical features and operating procedures - is strictly prohibited.

Production processes are closely monitored in order to prevent faults and malfunctions. However, the componentry adopted is subject to an extremely modest percentage of faults, which is nonetheless the case with any electronic or mechanical product.

Given the intended use of this item (protection of property and people), we invite you to adapt the level of protection offered by the system to suit the actual situation of risk (allowing for the possibility of impaired system operation due to faults or other problems), while reminding you that there are specific standards for the design and production of systems intended for this kind of application.

We hereby advise you (the system's operator) to see that the system receives regular routine maintenance, at least in accordance with the provisions of current legislation, and also check on as regular a basis as the risk involved requires that the system in question is operating properly, with particular reference to the control unit, sensors, sounders, dialler(s) and any other device connected. You must let the installer know how well the system seems to be operating, based on the results of periodic checks, without delay.

Work involved in the design, installation and maintenance of systems incorporating this product should be performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the mains and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply. If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

EU DECLARATION OF CONFORMITY

The products comply with current European EMC and LVD directives. The full text of the EU Declaration of Conformity is available at the following Internet address: elmospa.com – registration is quick and easy.

DISPOSAL INSTRUCTIONS - INFORMATION FOR THE USER



In accordance with Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), please be advised that the EEE was placed on the market after 13 August 2005 and must be disposed of separately from normal household waste.

IT08020000001624



1. GENERAL FEATURES

ELMOGWAY and ELMOGWAY2 give the possibility of interfacing EL.MO intrusion detection control units to automation systems, integrating the intrusion detection protection provided by EL.MO with the latest generation home & building systems. ELMOGWAY and ELMOGWAY2 feature **MASTER-SLAVE operation**. In Master-Slave systems, two devices talk to each other according to a precise rule: the Master is the unit that demands information, the Slave is the unit that can provide it.

The Master device performs query processes to a Slave device, that answers providing the required data, if available.

A Slave device does not provide data autonomously, but only upon specific request. This allows connecting many Slave devices to the same bus, and the Master device forwards the request to the Slave device of interest. The other Slave devices listen, but do not answer if they are not the addressee of the request.

ELMOGWAY and ELMOGWAY2 are both Master and Slave devices at the same time:

- they are Master to the EL.MO. control unit, performing queries and storing data.
- they are Slave to a Master unit, for example a PLC, a supervisor or other device. When questioned, they answer to the Master.

This is the bucket brigade criterion: the gateway queries the slave control unit and transfers data to its master upon request. **The gateways are compatible with all the EL.MO. intrusion detection control units and with TACÓRA (TA1002, TA1004, TA2000, TA4000) fire detection control units.**

ELMOGWAY and ELMOGWAY2 can communicate with the system through various **communication protocols**: MODBUS, KNX and SCS, for greater use flexibility. They support LAN or serial port connections to the EL.MO intrusion detection and TACÓRA fire detection control units.

A web interface ensures quick programming and configuration of the device. Among the many functions, there is also the possibility of defining operating rules among statuses and commands.

2. FEATURES

Model	ELMOGWAY	ELMOGWAY2
Protection class according to EN 60335-1	II	
Power source	10 - 16 V _{DC}	
Power consumption	3 W - 300 mA max	
LED di segnalazione	1 red LED: alarm/reset; 1 green LED: power ON (normally ON when the device is powered).	
Communication ports	KNX : Plug-in connector. RS-485 : Plug-in connector. RS-232 : Plug-in connector. LAN : RJ45 connector (10/100 Mbps). USB 2.0 : 2 ports.	KNX : Plug-in connector. RS-485 : Plug-in connector. - LAN : RJ45 connector (10/100 Mbps). USB 2.0 : 1 port.
Reset button	On the top of the enclosure.	Reachable by removing front cover.
Memory expansion	MicroSD (up to 32 GB, for future uses).	-
Operating temperature	0 °C — +50 °C	
Storage temperature	-10 °C — + 70°C	
Dimensions	L90 × H98 × D62 mm 5 DIN modules.	L90 × H36 × D62 mm 2 DIN modules.
Enclosure material	Self-extinguishing thermoplastic material.	

WARNING:

The gateway was designed for the integration of intrusion detection systems. The security level obtained during installation must therefore be preserved intact.

Arming and disarming of control units must always be performed using their own control devices.

The disabling and exclusion of the sensors also require the utmost attention.

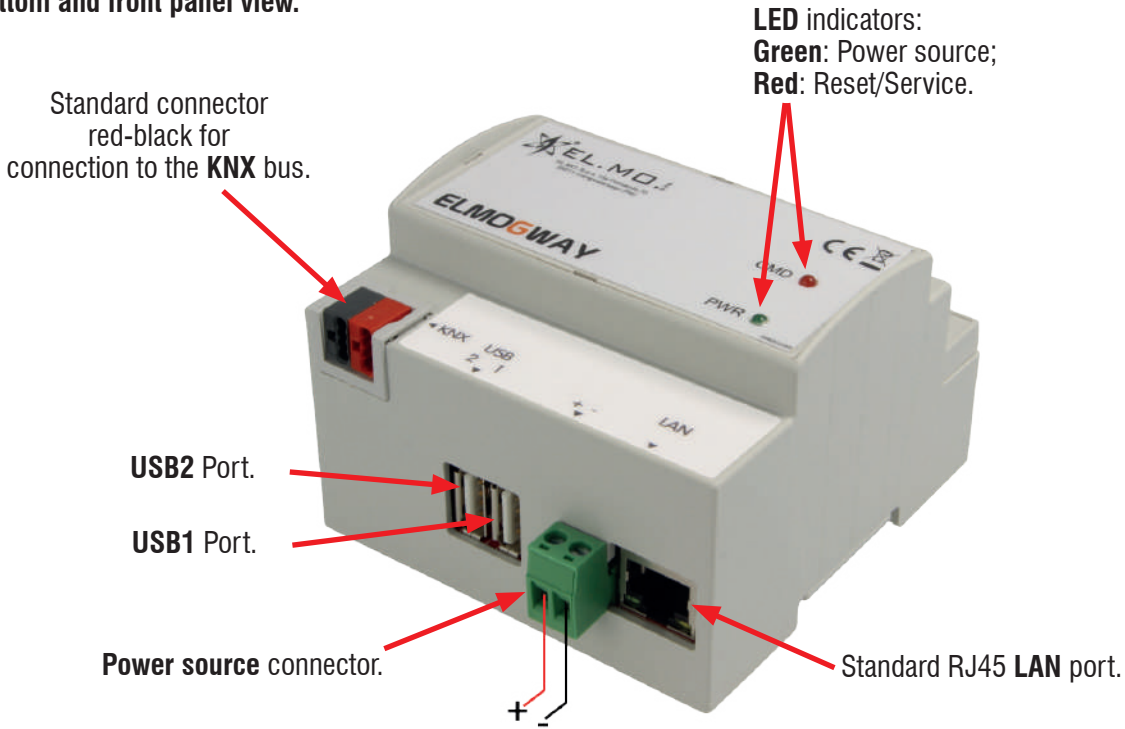
A control unit not in compliance with the standards is downgraded to a zero security level.

For any further information on the matter refer to IEC79-3:2012 and EN50131-1:2009.

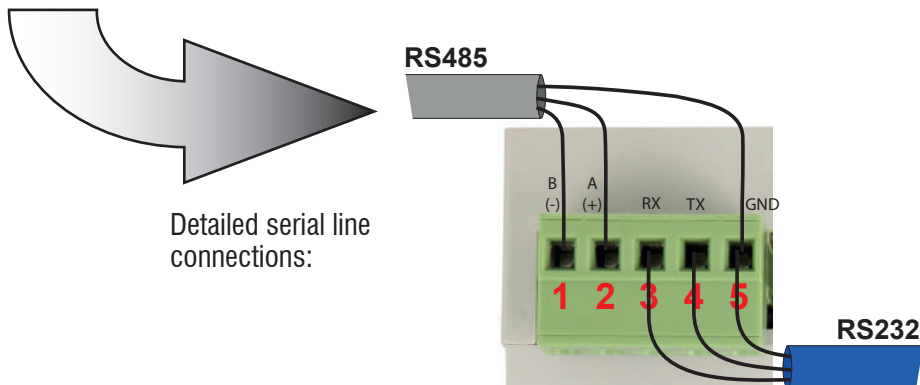
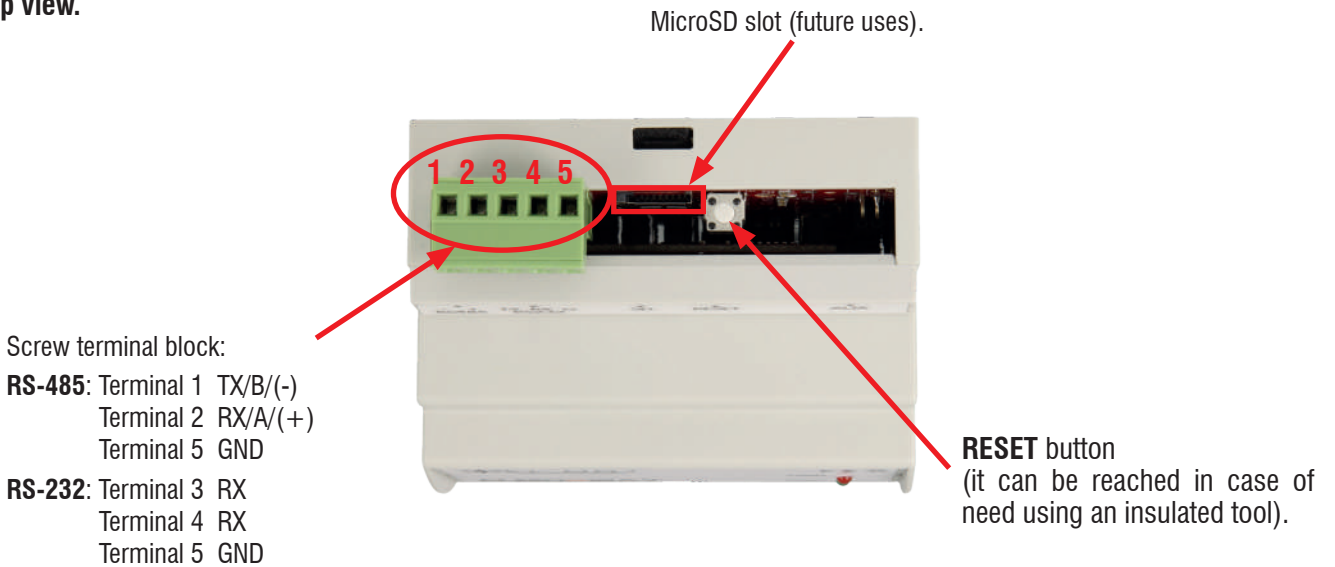


3. ELMOGWAY STRUCTURE

Bottom and front panel view.



Top view.





4. ELMOGWAY2 STRUCTURE

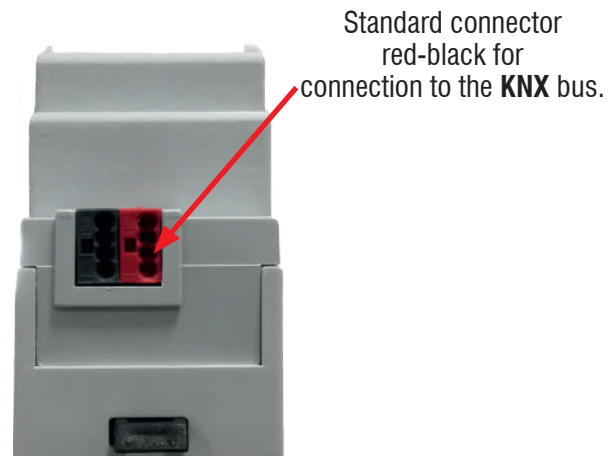
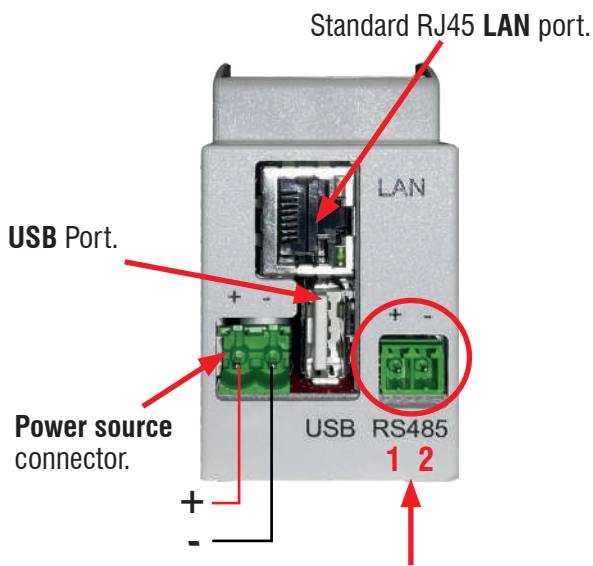
Front panel view.

LED indicators:
Green: Power source;
Red: Reset/Service.

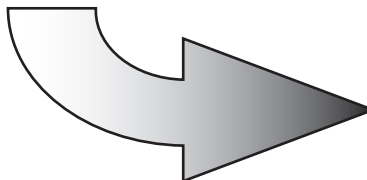


Top view.

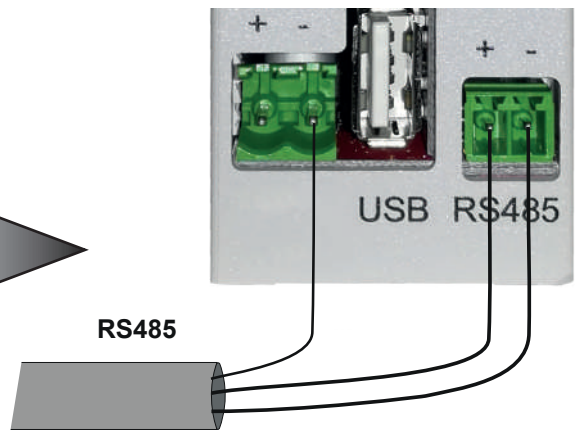
Bottom view.



Screw terminal block:
RS-485: Terminal 1 RX/A/(+)
Terminal 2 TX/B/(-)



Detailed serial line connections:



Connect RS-485 serial line GND wire to power supply negative terminal.



5. INSTALLATION AND RESET

5.1 Installation

Install the device in an area protected from opening (tamper), and not freely accessible by users. For example, the gateway housing should be secured to a standard 35 mm DIN bar.

5.2 Wiring

- Power source:** connect the gateway to the power source using the appropriate Sauro CGM green connector. The gateway may be directly powered by the control unit (in which case, continuity will be guaranteed in case of lack of mains power), or using an external power supply unit.
- Connection to the control unit:** proceed by connecting the gateway to the control unit.
For intrusion detection control units: three types of connections are possible for ELMOGWAY: RS-232, USB or LAN. Two types of connections are possible for ELMOGWAY2: USB or LAN.
For TACORA fire detection control units: for ELMOGWAY, LAN or RS-232 connection can be used. For ELMOGWAY2, LAN connection can be used.
- Connection to the home automation bus:** connect ELMOGWAY selecting the type of connector based on the protocol being used. Refer to the following table:

Protocol	Connector
MODBUS	LAN or RS-485
KNX	on-board KNX connector
SCS	LAN

After wiring, complete the first software configuration as indicated in section “6.1 Access to the configuration software” on page 17.

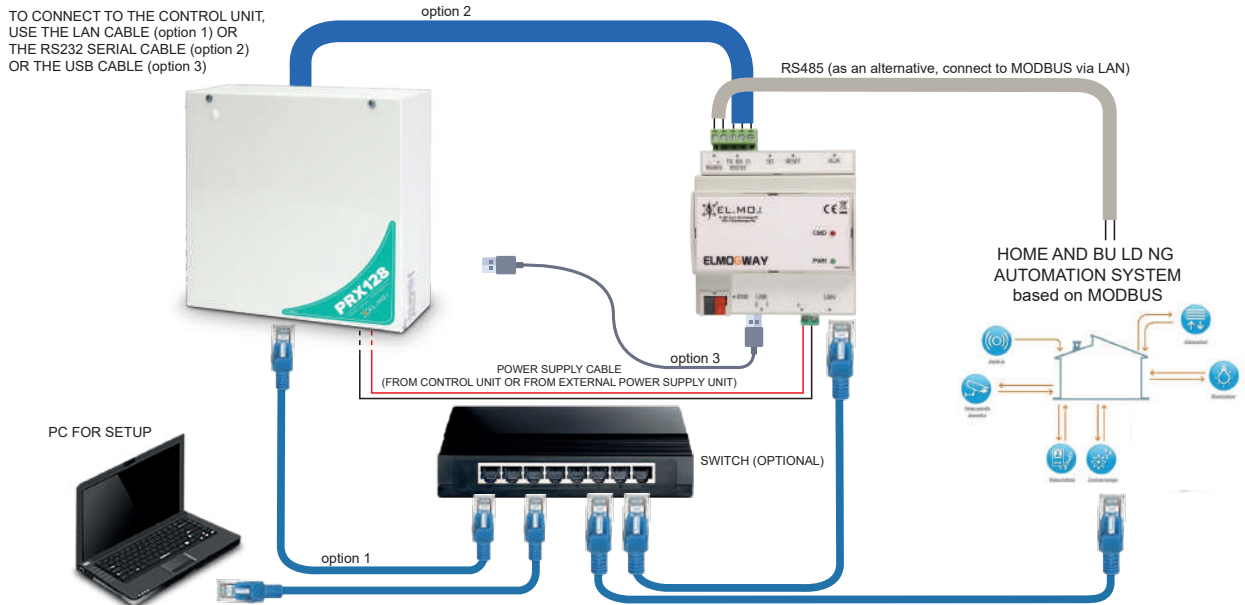
Note: in case of LAN connection, ensure that the same is protected, and that the network is not open to the Internet.

Nota: in case of RS-485 connection, the RS-485 serial line of the automation bus must not be wired to the RS-485 serial line of the control unit bus.

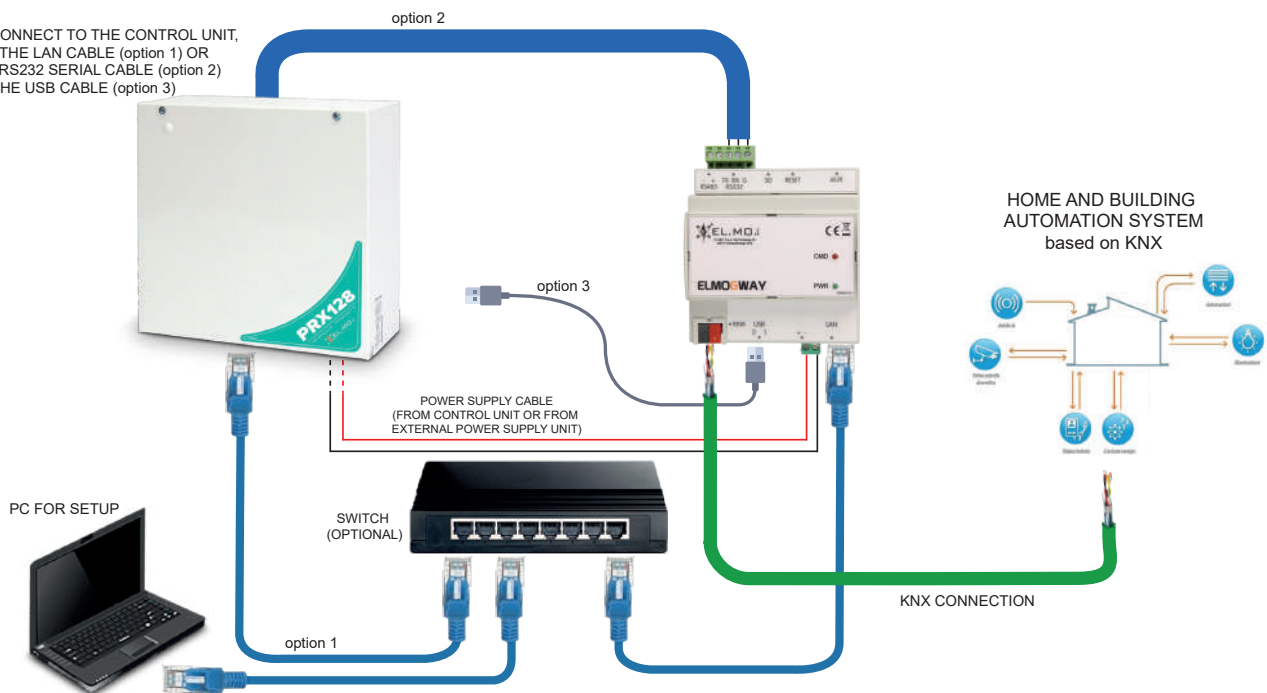


5.3 Wiring examples: ELMOGWAY

Example of connection in MODBUS mode using an intrusion detection control unit.

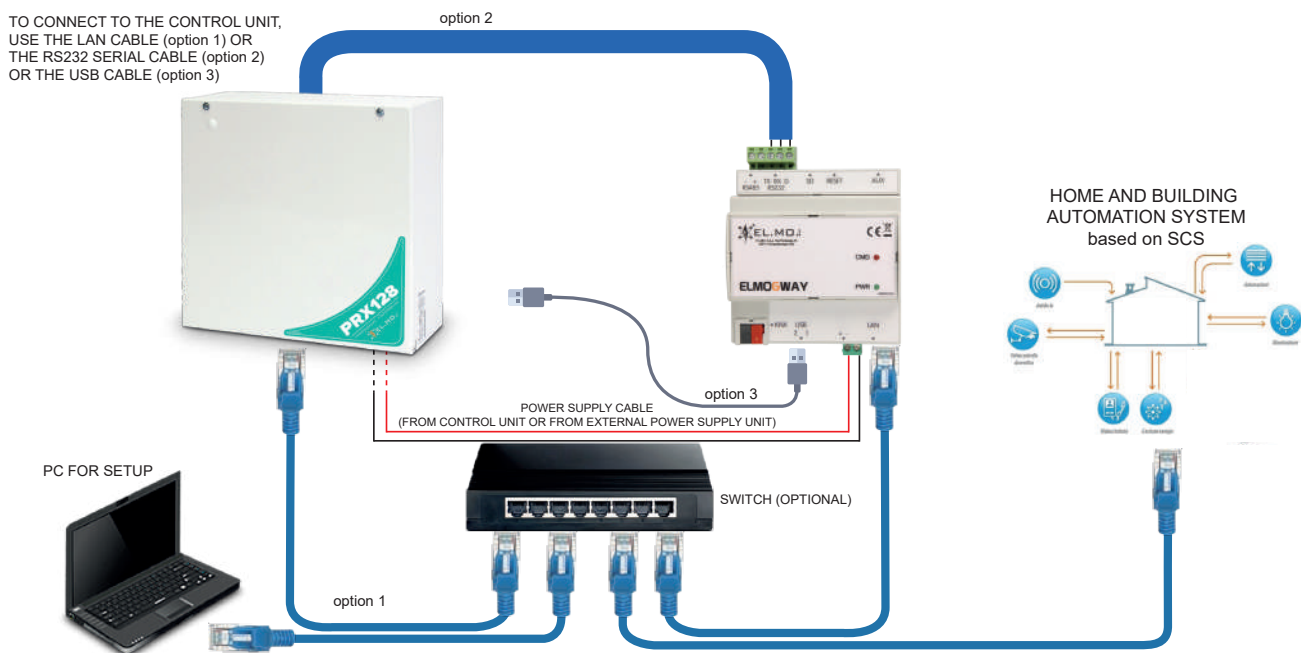


Example of connection in KNX mode using an intrusion detection control unit.

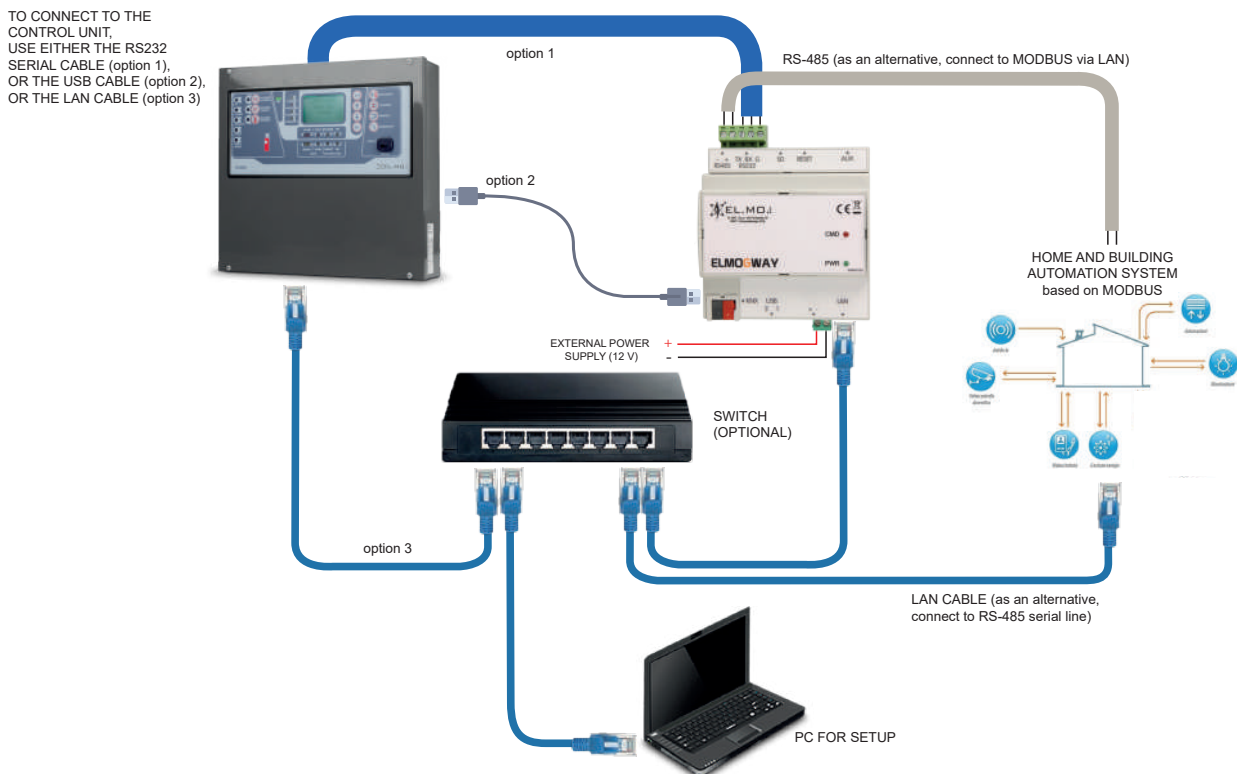




Example of connection in SCS mode using an intrusion detection control unit.



Example of connection in MODBUS mode using a TACÓRA fire detection control panel.



To connect to ELMOGWAY via LAN, the TACÓRA control unit must be equipped with one of the following modules:

- FXLAN2 board (for each firmware version of TACÓRA)
- MDLAN board (for TACÓRA with firmware version 5.2.2 or higher)

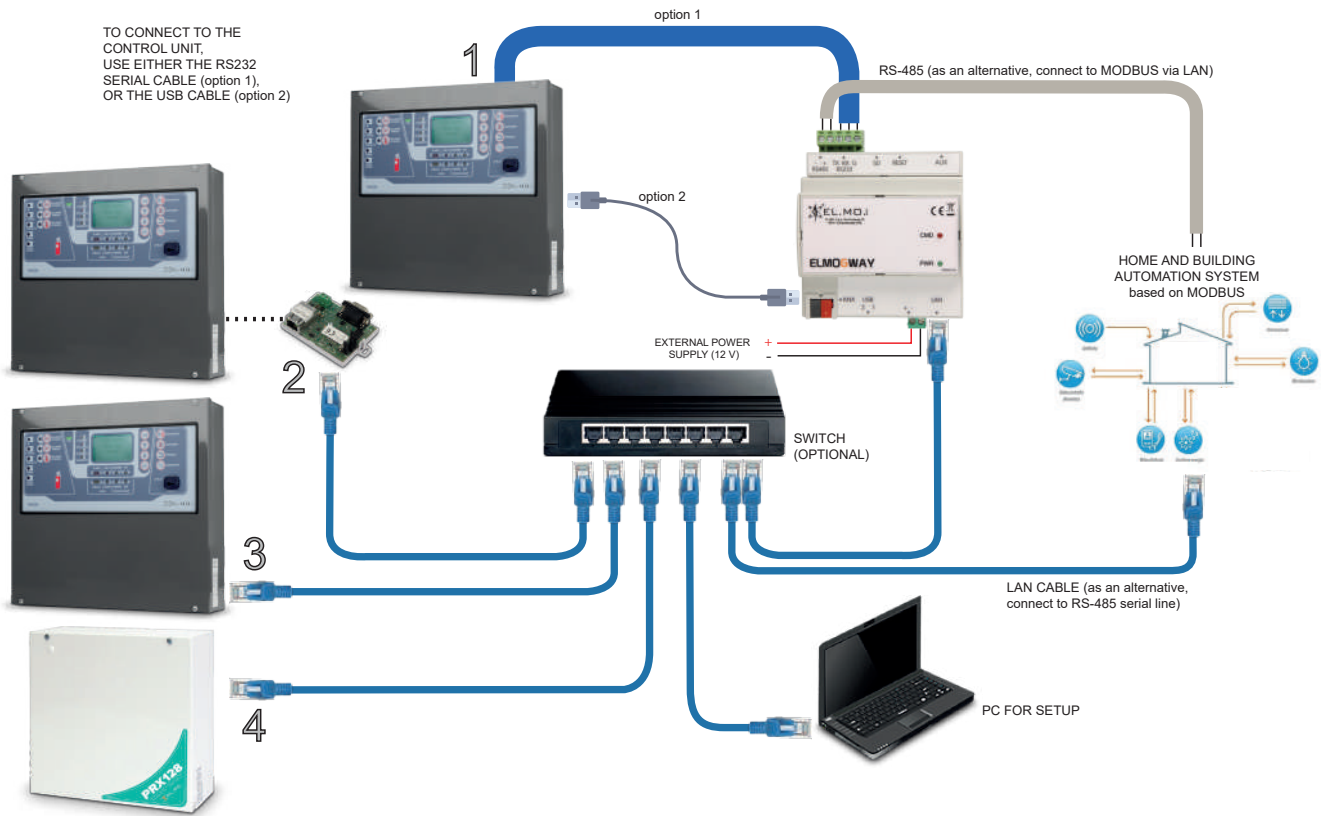


Example of connection in MODBUS mode using an intrusion control unit and several TACÓRA fire detection control units at the same time.

It is possible to connect ELMOGWAY to one or more TACÓRA control units and to one intrusion detection control unit at the same time, provided that a different IP port for each control unit is set in the **Bridge Modbus** section (see the related communication settings on pages 29 and 33).

Choose one of the following alternatives to connect the unit to the gateway:

- connect a control unit via RS-232 serial line or USB and all the remaining control units via LAN
- connect all control units via LAN



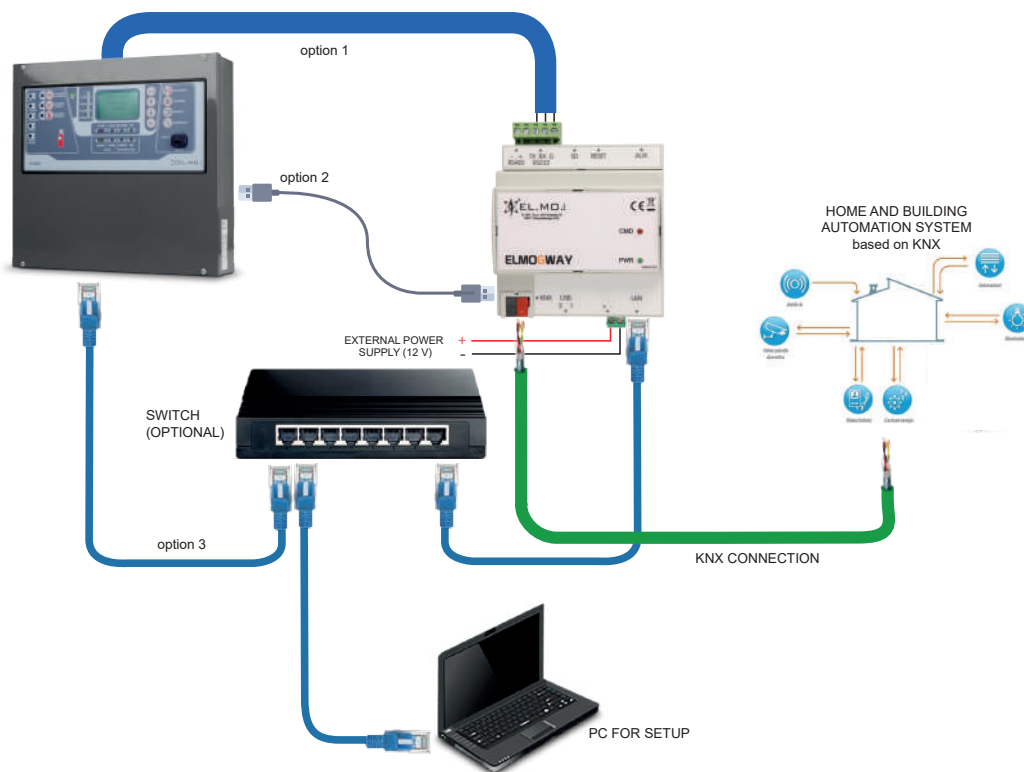
In the previous example, the following control units are wired to ELMOGWAY:

- 1) a TACÓRA unit via RS-232 or USB
- 2) a TACÓRA unit with firmware version lower than 5.2.2 via LAN through FXLAN2 module
- 3) a TACÓRA unit with firmware version 5.2.2 via LAN through MDLAN module
- 4) an intrusion detection control unit via LAN



Example of connection in KNX mode using a TACÓRA fire detection control panel.

TO CONNECT TO THE CONTROL UNIT, USE EITHER THE RS232 SERIAL CABLE (option 1), OR THE USB CABLE (option 2), OR THE LAN CABLE (option 3)



To connect to ELMOGWAY via LAN, the TACÓRA control unit must be equipped with one of the following modules:

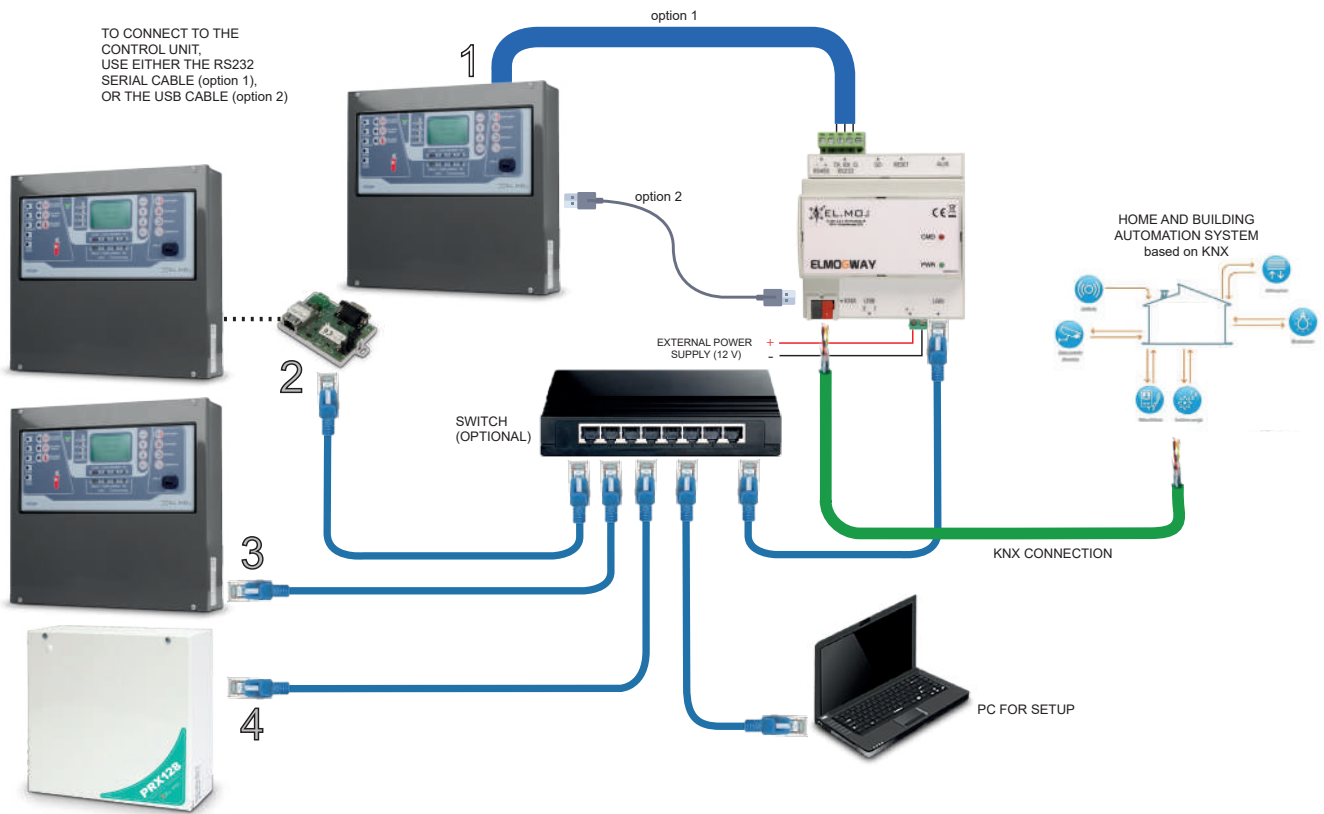
- FXLAN2 board (for each firmware version of TACÓRA)
- MDLAN board (for TACÓRA with firmware version 5.2.2 or higher)



Example of connection in KNX mode using an intrusion control unit and several TACÓRA fire detection control units at the same time.

Choose one of the following alternatives to connect the unit to the gateway:

- connect a control unit via RS-232 serial line or USB and all the remaining control units via LAN
- connect all control units via LAN



In the previous example, the following control units are wired to ELMOGWAY:

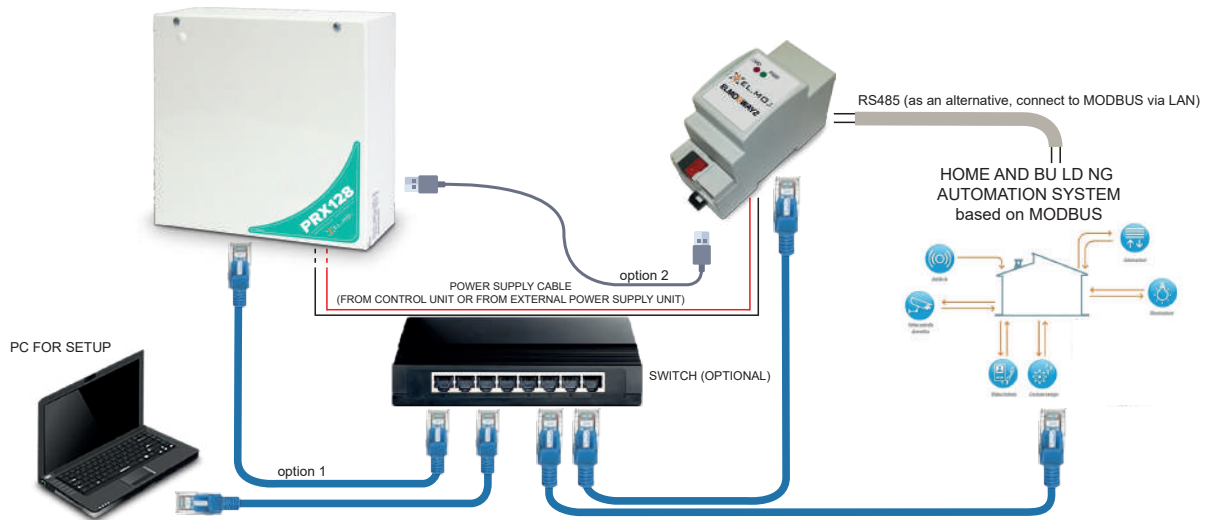
- 1) a TACÓRA unit via RS-232 or USB
- 2) a TACÓRA unit with firmware version lower than 5.2.2 via LAN through FXLAN2 module
- 3) a TACÓRA unit with firmware version 5.2.2 via LAN through MDLAN module
- 4) an intrusion detection control unit via LAN



5.4 Wiring examples: ELMOGWAY2

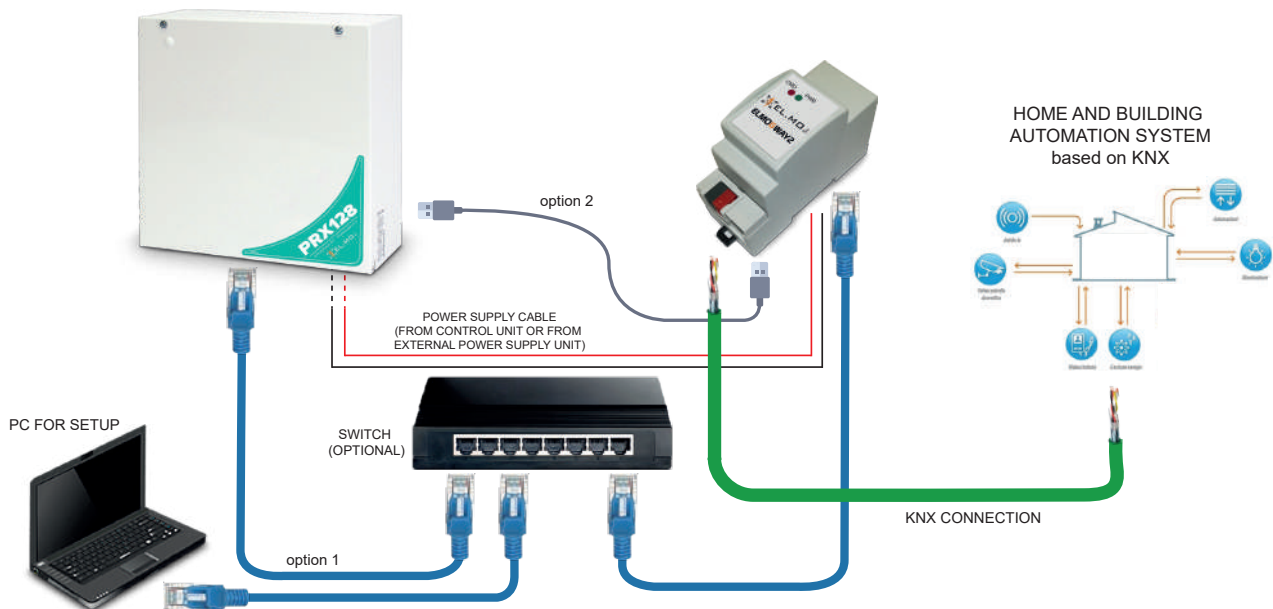
Example of connection in MODBUS mode using a PROXIMA intrusion detection control unit.

TO CONNECT TO THE CONTROL UNIT,
USE THE LAN CABLE (option 1)
OR THE USB CABLE (option 2)



Example of connection in KNX mode using a PROXIMA intrusion detection control unit.

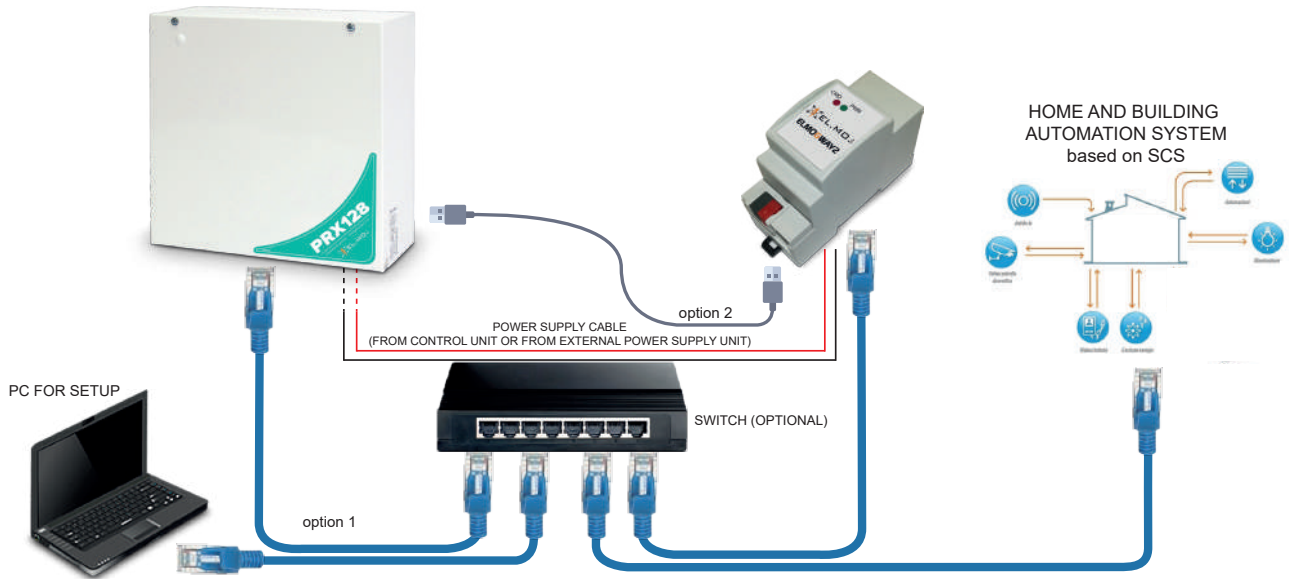
TO CONNECT TO THE CONTROL UNIT,
USE THE LAN CABLE (option 1) OR
OR THE USB CABLE (option 2)





Example of connection in SCS mode using a PROXIMA intrusion detection control unit.

TO CONNECT TO THE CONTROL UNIT,
USE THE LAN CABLE (option 1)
OR THE USB CABLE (option 2)

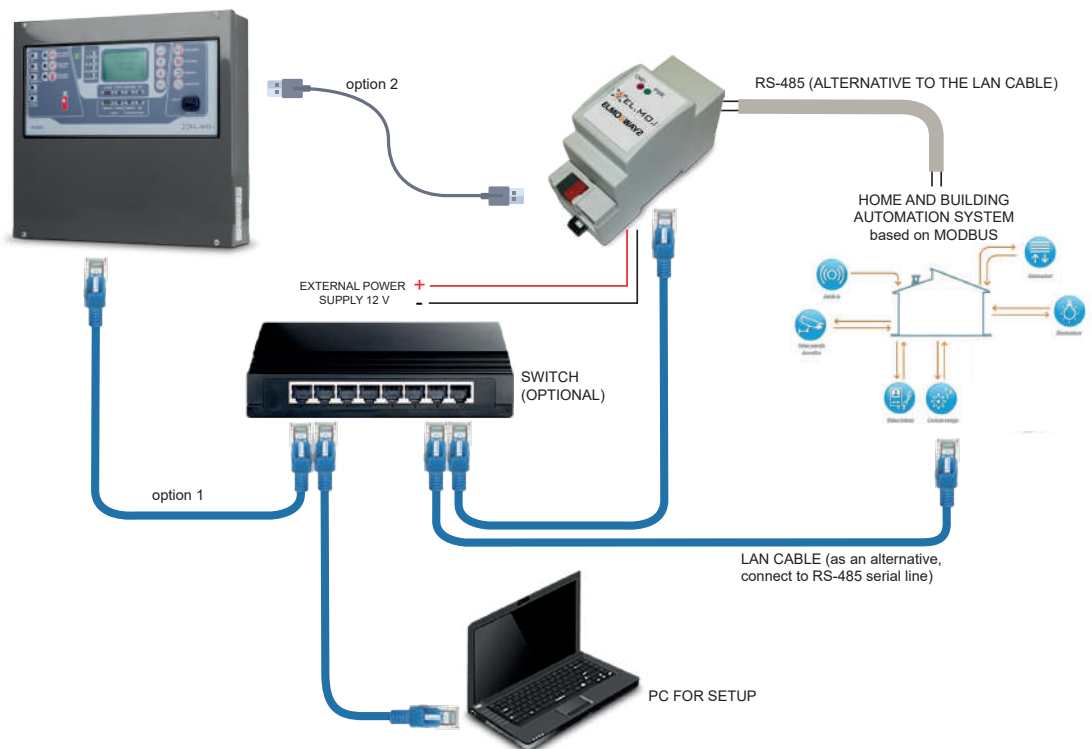


Example of connection in MODBUS mode using a TACÓRA fire detection control panel.

To perform LAN connection, the TACÓRA control unit must be equipped with one of the following modules:

- FXLAN2 board (for each firmware version of TACÓRA)
- MDLAN board (for TACÓRA with firmware version 5.2.2 or higher)

TO CONNECT TO THE CONTROL UNIT,
USE EITHER
THE LAN CABLE (option 1),
OR THE USB CABLE (option 2)



As an alternative, it is possible to connect the fire detection unit to the gateway via USB.

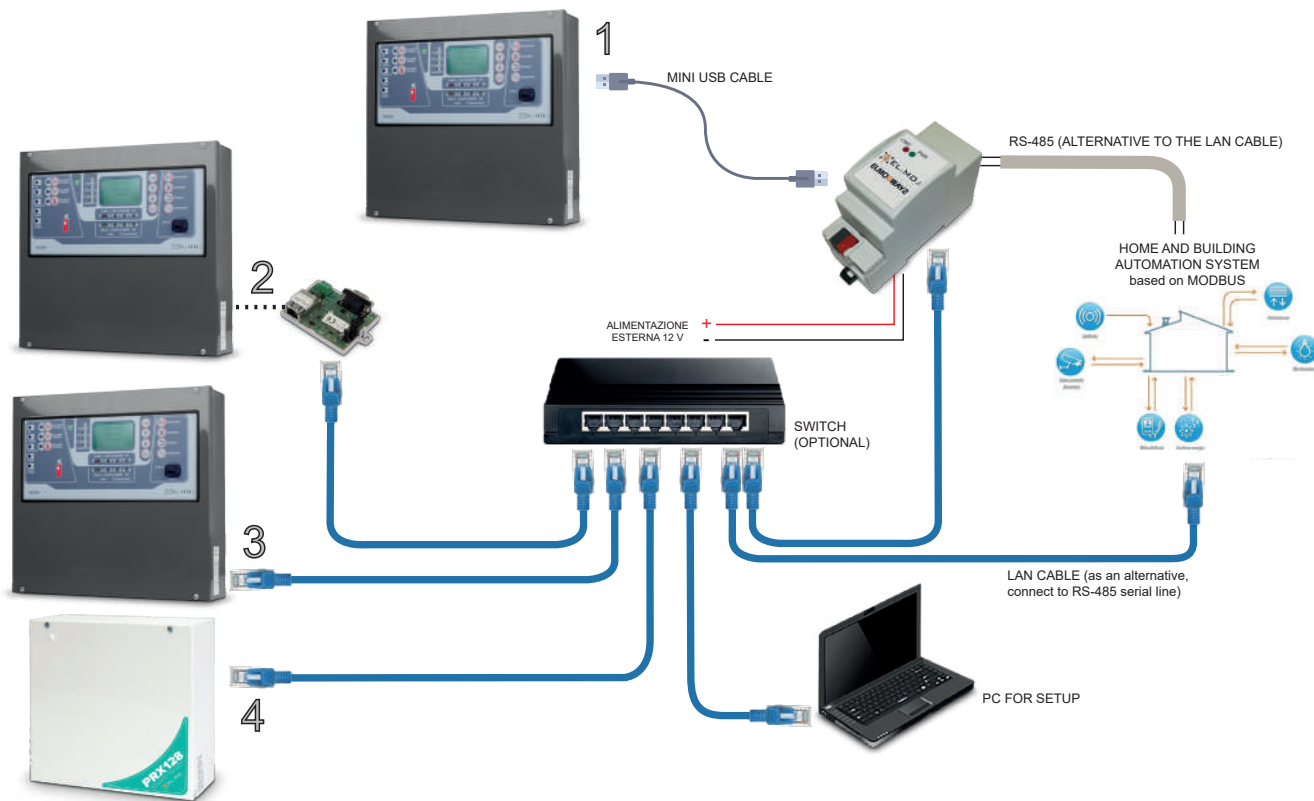


Example of connection in MODBUS mode using one intrusion control unit and several TACÓRA fire detection control units at the same time.

It is possible to connect ELMOGWAY2 to one or more TACÓRA control units and to one intrusion detection control unit at the same time, provided that a different IP port for each control unit is set in the **Bridge Modbus** section (see the related communication settings on pages 29 and 33).

Choose one of the following alternatives to connect the unit to the gateway:

- connect a control unit via USB and all the remaining control units via LAN
- connect all control units via LAN



In the previous example, the following control units are wired to ELMOGWAY:

- 1) a TACÓRA unit via USB
- 2) a TACÓRA unit with firmware version lower than 5.2.2 via LAN through FXLAN2 module
- 3) a TACÓRA unit with firmware version 5.2.2 via LAN through MDLAN module
- 4) an intrusion detection control unit via LAN

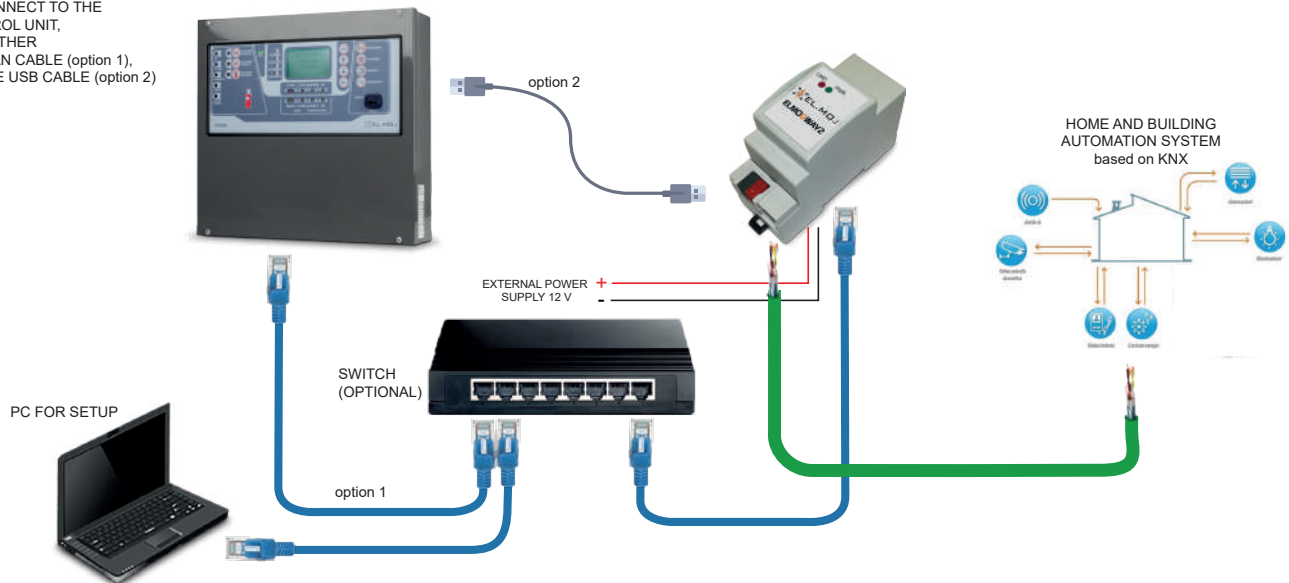


Example of connection in KNX mode using a TACÓRA fire detection control panel.

To perform LAN connection, the TACÓRA control unit must be equipped with one of the following modules:

- FXLAN2 board (for each firmware version of TACÓRA)
- MDLAN board (for TACÓRA with firmware version 5.2.2 or higher)

TO CONNECT TO THE CONTROL UNIT, USE EITHER THE LAN CABLE (option 1), OR THE USB CABLE (option 2)



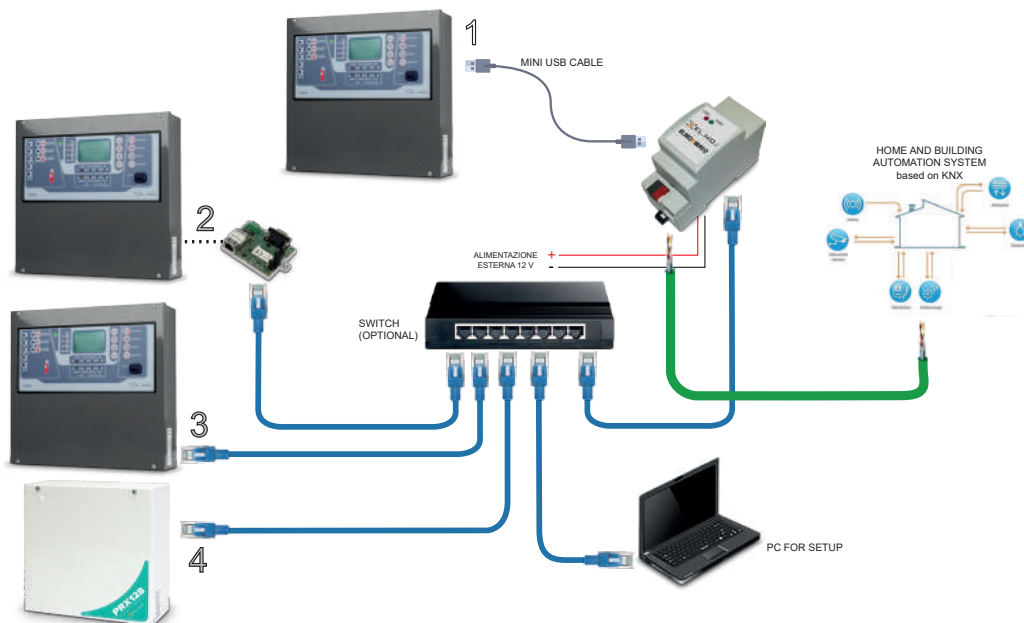
As an alternative, it is possible to connect the fire detection unit to the gateway via USB.

Example of connection in MODBUS mode using one intrusion control unit and several TACÓRA fire detection control units at the same time.

It is possible to connect ELMOGWAY2 to one or more TACÓRA control units and to one intrusion detection control unit at the same time, provided that a different IP port for each control unit is set in the **Bridge Modbus** section (see the related communication settings on pages 29 and 33).

Choose one of the following alternatives to connect the unit to the gateway:

- connect a control unit via USB and all the remaining control units via LAN
- connect all control units via LAN



In the previous example, the following control units are wired to ELMOGWAY:

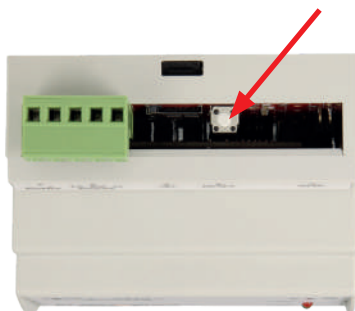
- 1) a TACÓRA unit via USB
- 2) a TACÓRA unit with firmware version lower than 5.2.2 via LAN through FXLAN2 module
- 3) a TACÓRA unit with firmware version 5.2.2 via LAN through MDLAN module
- 4) an intrusion detection control unit via LAN



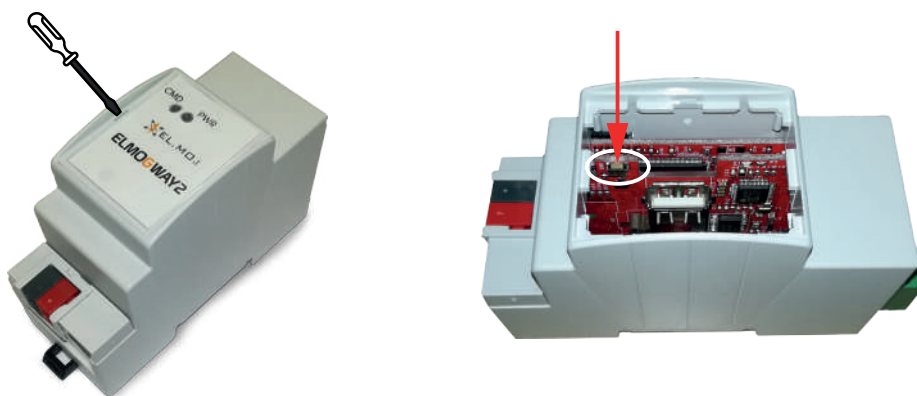
5.5 Reset procedures

The gateways offer two reset levels: factory IP address only, and total factory configuration reset (total reset), depending on how the RESET button is pressed.

On ELMOGWAY, the RESET button is at the top of the device (see picture below), freely reachable.



On ELMOGWAY2, to reach the button remove the front cover by pivoting with a screwdriver on one of the two side grooves. The button is located as shown in the right picture below.



Use an insulated tool of appropriate size for reaching the button.

5.5.1 Factory IP address reset

For the reset of the factory IP address only, proceed as follows:

1. Press and hold down the RESET button for at least 10 seconds, until the red LED on the front of the device starts flashing, and then release the button;
2. Within the next 5 seconds, press the button for 1 second and then release.
Within a couple of seconds the front LED will turn on steady for approximately 2 seconds;
3. After the LED turns off again, the gateway will be reachable at the factory IP address (192.168.0.110).

If the LED turns off after the first extended pressure (10 seconds), before the short pressure, repeat the whole procedure.

5.5.2 Total factory configuration reset

For the total reset of the configuration of ELMOGWAY to the factory settings, proceed as indicated below.

The total reset of the gateway may be required if the current configuration makes it impossible to access or to correctly use ELMOGWAY. During the reset, the device will be reconfigured using the factory settings, including the IP address.

1. Press and hold down the RESET button for at least 10 seconds, until the red LED on the front of the device starts flashing, and then release the button;
2. Within the next 5 seconds press and hold down the button for at least 10 seconds;
3. When the LED comes on steady, release the button and wait for the LED to turn off;
4. When the LED turns off, disconnect and then reconnect the power source;
5. Wait one minute, and then access ELMOGWAY using the factory IP address (192.168.0.110).



6. SOFTWARE CONFIGURATION

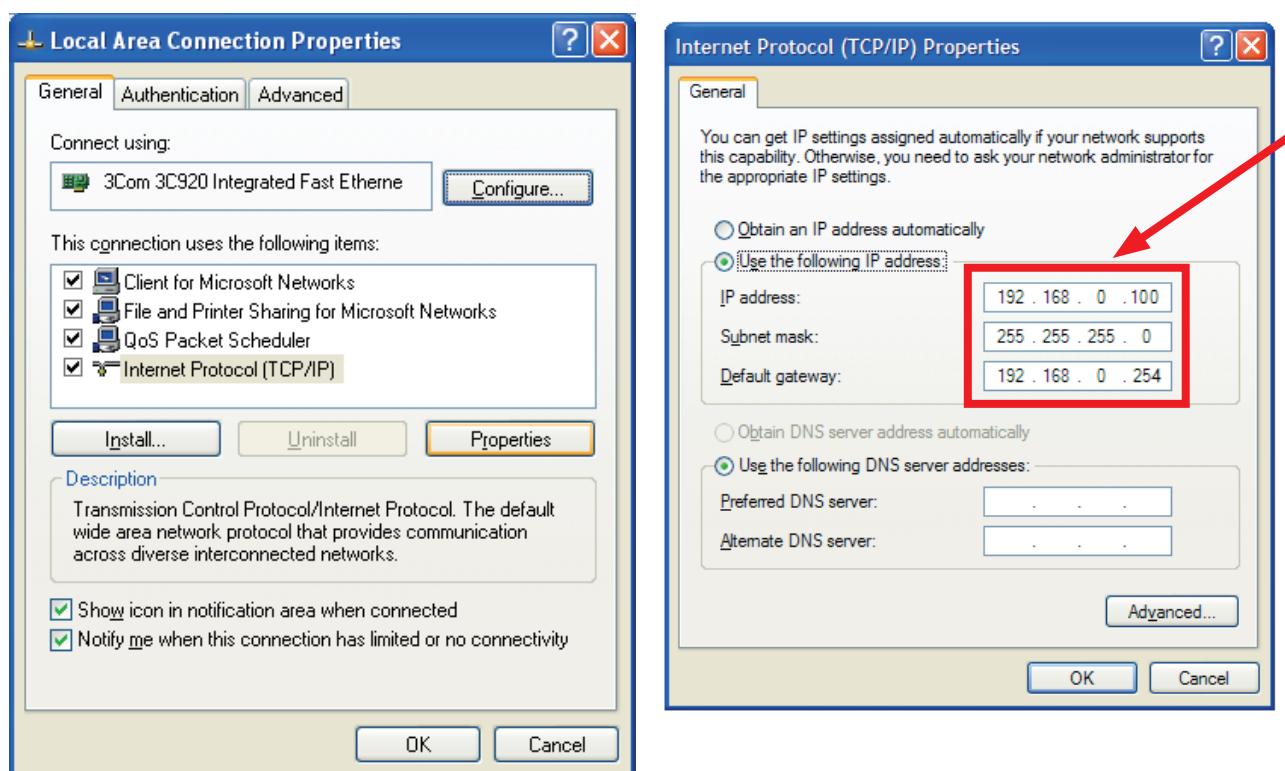
6.1 Access to the configuration software

To configure the gateway using the dedicated software proceed as indicated below. This procedure applies both in case of first installation, and at any other time in case of maintenance activities.

1. Directly connect the gateway to a PC using a network cable connected to the LAN port on the bottom.
2. In the PC, open the LAN and TCP/IP properties window and temporary set the IP address of the PC as follows:

IP Address	192.168.0.100
Net mask	255.255.255.0
Preset gateway	192.168.0.254

The gateway address can be replaced later on with the one of the network to which the device will be connected. As an example, below are the windows where to set the addresses on a PC with Windows XP operating system installed:



3. Open a browser (preferably Google Chrome), and enter the following address: **http://192.168.0.110**.
4. After connecting to the device, when asked enter the following details:

Username	admin
Password	admin

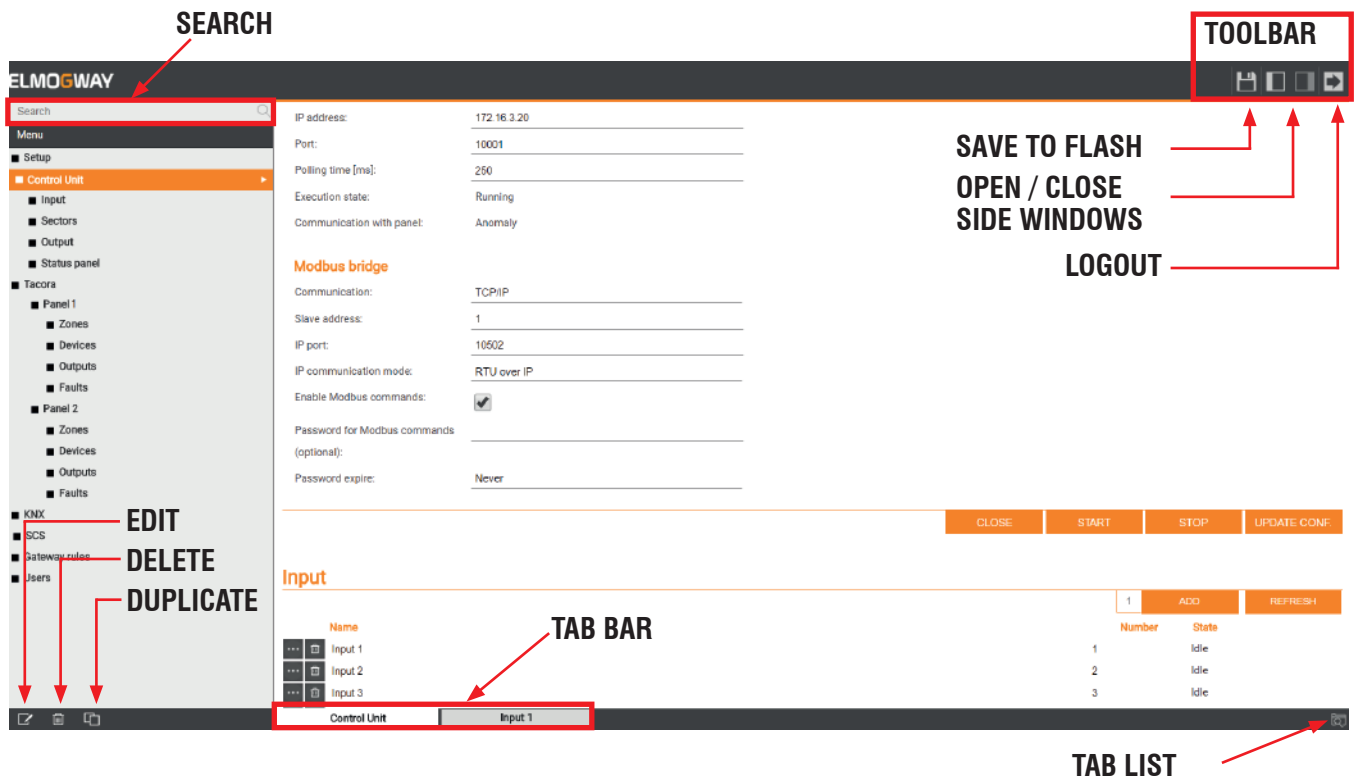
After login, it will be possible to carry out several operations.

The chapters that follow will provide specific configuration information for each section.

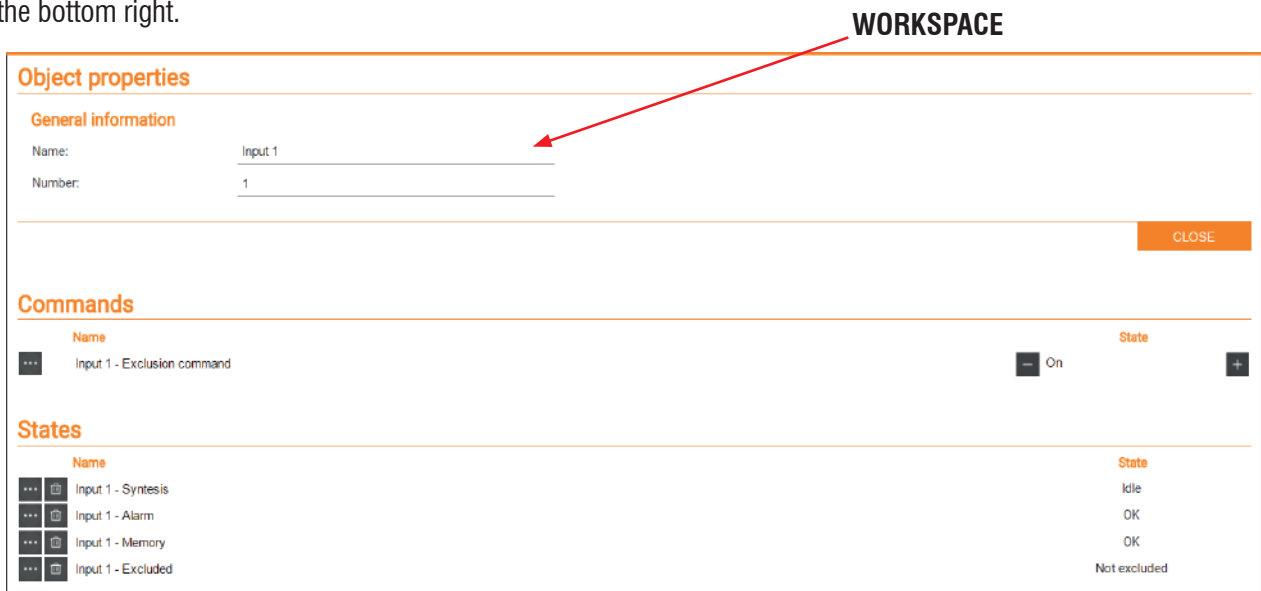


6.2 General overview of the user interface

The following figure shows an overview of the user interface.



The main working area is called **WORKSPACE**. It gives the possibility of working on several pages, switching from one to the next using the **TAB BAR** at the bottom. If the number of tabs exceeds the available space, the full list of all pages can be viewed by pressing the **TAB LIST** button on the bottom right.





MENU


The menu on the left of the page grants access to all the gateway functions.

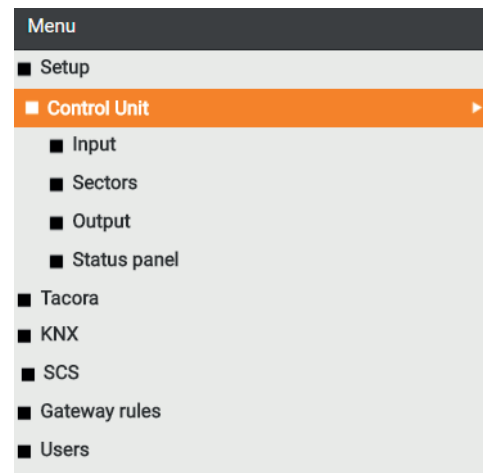
When a section is opened, this is highlighted and then possibly expanded to show any sub-items.

When highlighted, some items will make available one or more of the following buttons at the bottom of the menu:

- **NEW:** to create a new element within the section highlighted in the menu.
- **EDIT:** to change the selected element.
- **DELETE:** to permanently delete the selected element.
- **DUPLICATE:** to duplicate the selected element.

If a selected element can be changed, in addition to the EDIT button, the bottom toolbar will also include a “shortcut” at its side, consisting of a button with three dots. 

Pressing either button will open a new tab within the workspace. Open elements are highlighted in the list by an arrow. 



TOOLBAR

The toolbar (top right) contains the following buttons:

- **SAVE TO FLASH:** To force saving to a permanent memory. Saving is automatic during configuration. In case of need to disconnect the power source while this button is red, press it to force saving.
- **OPEN / CLOSE SIDE WINDOWS:** to open and close the side panels of the user interface.
- **LOGOUT:** To terminate the current session.

SEARCH

Enter one or more keywords to search for one or more previously created project elements.

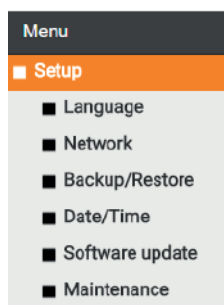
It is possible to select several elements from the search list by pressing CTRL.

It is possible to interact with the search results using the buttons of the toolbar (the buttons have the same meanings as those of the menu toolbar).



6.3 SETUP Menu

The “Setup” page can be used to configure the general parameters of the gateway, and to complete the main maintenance operations.



6.3.1 Language

Access this menu to change the language (selectable from the drop-down menu), then click on SAVE.

6.3.2 Network

This section can be used to set the following parameters for the configuration of the gateway LAN network:

IP	Gateway address within the LAN network
NETMASK	Default: 255.255.255.0
DEFAULT GATEWAY	Preset gateway Default: router IP address
PRIMARY DNS SECONDARY DNS	DNS addresses for access to the Internet

6.3.3 Backup/Restore

This section can be used to:

- make a backup copy of the project
- import a previous backup
- reset the gateway to factory settings by selecting the appropriate item (the network address is not changed)

After selecting the desired operation (and selecting the backup file in case of import), press "GO" and wait for the completion of all the operations, which will be confirmed by a pop-up message. Do not interrupt the procedure with other browser activities, or by closing the browser windows, as this may result in malfunctioning.

6.3.4 Date/Time

This section can be used to set a range of options relating to the system clock.

The required information is as follows:

Configuration of date and time	Current date and time.
Timezone configuration	Geographical area and capital of reference, to set the correct time zone.
Synchronize date/time from	Server for automatic update of the time, and synchronisation interval (in minutes) of the system clock.

Note: Unless in case of specific requirements, the preset settings should be maintained.



6.3.5 Software update

This section can be used to update the gateway software.

Only use official installation packages, or malfunctioning may be experienced.

To update the ELMOGWAY software proceed as follows:

1. Save the update package (downloaded from the site, or received by email) in the PC, without extracting the files;
2. Open the update page;
3. Select the update package using the "BROWSE" button (or similar, depending on the browser used).

Note for MAC users: if downloading the package using SAFARI or the MAIL electronic mail client, the files are extracted automatically, which will cause the update to fail. It is therefore recommended that the package is downloaded using a different browser and/or electronic mail client.

Note: the update must only be installed using Google Chrome (Windows platform) or Apple Safari (Mac OSX platform): other browsers may cause problems and make the webserver unusable.

4. Make sure that you do not already have the same software version installed (shown at the start of the page);
5. Click "UPDATE".

The update procedure is performed automatically. Wait for it to be completed without using the browser for other activities and without closing it (or malfunctioning of the web server may occur).

The procedure may require a few minutes, depending on the software version and the configuration.

After installation, the screen will show a summary of the operations carried out, with the new software version. To complete the procedure press "RESTART", which will restart the gateway operating system.

In case of accidental interruption of the update procedure (e.g.: interruption of the power source or the network connection to the PC), try the following:

1. Switch the gateway off and then on again;
2. Wait a minute and then open the browser entering the gateway IP address;
3. Wait for the automatic reset procedure to be completed and the gateway to be restarted.

Note: the automatic reset procedure can also be started by performing a full reset using the reset button.

If the automatic reset fails (wait at least 15 minutes to make sure), contact our technical support service.

6.3.6 Maintenance

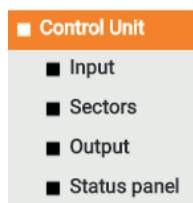
This section can be used to:

- access the device hardware parameters (**panel information:** serial code, hardware code, chipset);
- check the **system status** (time from the last startup and RAM information, with the possibility of downloading the data log file);
- restart the communication services and the system.



6.4 CONTROL UNIT Menu - intrusion detection control unit

The "Control unit" page can be used to map the communication with the security control unit, and to manage inputs, outputs, sectors and control unit statuses.



WARNING:

The gateway is integrated in intrusion detection systems. Therefore, it will be necessary to preserve the security level obtained during installation by complying with the requirements of the standards. In particular, the arming and disarming of the control units must always be performed using their own control devices. The disabling and exclusion of the sensors also requires the utmost attention.

Note: web pages are a testing tool. They give no indication on actual system response times.

6.4.1 General settings

This preliminary section of the "Control unit" menu is used to set the parameters for connection to the intrusion detection control unit:

GENERAL DETAILS	
NAME	Control Unit data plate.
USER	User code used by the gateway for communication with the control unit. It must be a numerical code, and must be valid for the control unit.
CODE	Numerical code (password) for the authentication of the user by the control unit.

COMMUNICATION	
COMMUNICATION TYPE	Selection of the gateway communication mode: RS-232 (serial communication), IP (TCP/IP protocol communication) or USB.
SERIAL PORT	Communication port to use in case of serial communication (default: RS-232). <i>(option only available for serial communication)</i>
PORT SPEED	Communication Baud rate <i>(option only available for serial and USB communication. For USB, set 9600)</i>
PORT	Control unit address and port within the LAN network (default: 10001).
POLLING TIMER	Control unit interrogation time (in ms). Adjust the time to increase or decrease the frequency at which the gateway requests the control unit to provide the status.
EXECUTION	Operating status of the driver for communication with the control unit. In normal conditions it must be "Running".
COMMUNICATION WITH PANEL	Connected: connection is present. Not connected: connection is absent. Password error: wrong password or user code.
ALLOWED SECTOR COMMANDS(*)	Select one option: All: both arming and disarming commands are allowed. Armed: only the arming command is allowed. None: no command allowed.
ALLOWED ZONE COMMANDS (*)	Select one option: All: both inclusion and exclusion commands are allowed. Armed: only the inclusion command is allowed. None: no command allowed.

(*) **Note:** the Allowed Sector/Zone Commands defined above have effect on commands from KNX, SCS, Modbus and panel.



Communication with the control unit can be started or stopped using the "START" and "STOP" buttons respectively. The "UPDATE CONF." button causes a stop, followed by a start of the communication.



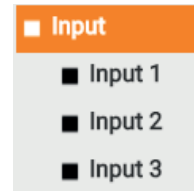
The parameters that can be configured in this section include those for MODBUS protocol connection ("**Modbus Bridge**"). For information on the configuration using this protocol, see the specific section of this manual ("7. MODBUS PROTOCOL - INTRUSION DETECTION CONTROL UNITS" on page 29).

6.4.2 Inputs

This section can be used to add and configure the control unit sensors within the gateway.

To add inputs, proceed as follows:

1. Enter the number of inputs to add in the appropriate field at the side of "ADD" (default: 1);
2. Press "ADD" and wait until the operation is completed. The created inputs will automatically be listed after any already existing ones.



Input

Number	State
1	Idle
2	Idle
3	Idle
4	Idle

After the inputs have been created, it will be possible to change their names and numbers (we recommend that the automatically assigned numbers are kept unchanged), and check their status.

The action button at the side of each input name gives access to its detail tab. It also allows to permanently remove an input from the project.

Object properties

General information

Name: Input 1
Number: 1

Commands

Name	State
Input 1 - Exclusion command	On

States

Name	State
Input 1 - Synthesis	Idle
Input 1 - Alarm	OK
Input 1 - Memory	OK
Input 1 - Excluded	Not excluded

The previous image shows a detailed view of the tab of an input.

Using the "**Commands**" section, it is possible to send the exclusion command to the input: when ON is set using the appropriate selector, the input in question will be excluded.

The "**States**" section displays the various status details updated in real time. Each input is characterised by the following statuses:

- **Synthesis:** it identifies the summary status of the input;
- **Alarm:** ON/OFF, based on the sensor alarm status;
- **Memory:** ON/OFF, based on the sensor alarm memory;



- **Excluded:** ON/OFF, based on the sensor exclusion status.

The gateway does not normally interface with all available inputs, but only with a limited number of them. To facilitate the setup procedure, it is possible to only generate the number of inputs required, and then assign to each new element the actual physical address and the label:

Name	Number	State
Input 15	15	Idle
Input 16	233	Idle

In this way, if for example the actual lines that must be interfaced are only 16, it will be possible to generate 16 of them using the previously explained procedure and then, for example, assign the last line to input 233 without the need to generate 233 inputs. The same is also possible for outputs and sectors.

Note: if a control unit input has been set as "Remote" input via BrowserOne, it is required to enable the "Basic maintenance" property for the user associated to domotics functions for proper operation with the gateway.

6.4.3 Sectors

This section can be used to configure the control unit sectors, associating the various inputs. In the same way as discussed in the previous section for inputs, it is possible to specify how many sectors to create, and confirm their creation by pressing the "ADD" button; once the elements have been created, it is possible to change some characteristics, check the status, or access the detail tab of each sector, as shown in the following image:

Sectors

- Sector 1
- Sector 2
- Sector 3
- Sector 4

Commands

Name	State
Sector 1 - Arm command	Off
Sector 1 - Prior arm command	Off

States

Name	State
Sector 1 - Synthesis	Idle
Sector 1 - Alarm	OK
Sector 1 - Armability state	Ready
Sector 1 - Prior arming state	Not armed
Sector 1 - Arming state	Not armed
Sector 1 - Memory	OK

Related inputs

Name	Number
Drop here objects from search results or tree menu	

Using the appropriate selectors, it is possible to configure the following "Commands":

- **Arm command:** It arms the sector in "normal" mode;
- **Prior arm command:** It arms the sector in "high security" or priority mode;

The "States" section displays the various status details updated in real time. Each input is characterised by the following statuses:

- **Synthesis:** Label that identifies the summary status of the sector;
- **Alarm:** sector alarm status;
- **Armability state:** it indicates whether the sector is "Ready" or "Not ready" for arming;
- **Prior arming state:** ON if the sector is armed in maximum security mode;
- **Arming state:** ON if the sector is armed;
- **Memory:** sector alarm memory status.

Note: the "Related inputs" section may be used to associate the desired inputs to each sector: simply look for the inputs (identifying them from the side menu, or searching for them using the search tool) and drag them in the grey field indicated by *****. Multiple selections are possible.

By associating inputs to a sector, modbus registers "Alarm status, sector 1 ... X" and "Memory status, sector 1 ... X" become readable,



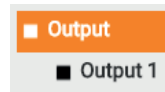
as well as the outputs of the sector element in rules. If no input is associated, these registers/outputs will not be available.

Sector numbering

Sector numbering is always sequential. For example, a control unit with 8 four-sector areas has 32 total sectors numbered from 1 to 32: therefore, sector 2 of area 2 is number 6 in the list.

6.4.4 Outputs

This section can be used to configure the control unit outputs.



In the same way as discussed in the previous sections, it is possible to specify how many outputs to create and confirm their creation by pressing the "ADD" button; once the elements have been created, it is possible to change some characteristics, check their status, or access the detail tab of each output as shown in the following image:

Object properties

General information

Name:

Number:

CLOSE

Commands

Name	State
Output 1 - Command	Off

States

Name	State
Output 1 - Synthesis	Idle
Output 1 - Status	Off

In the "Commands" section, it is possible to force the output to ON or OFF. The "States" section shows the summary status, and if the output is ON or OFF.

6.4.5 Control unit statuses

This section can be used to manage the general control unit notifications. By pressing "ADD" in the appropriate section, all the objects that it will then be possible to manage at gateway level are created.

The following statuses among the ones available may be controlled:

- **Total arming:** Arming of all sectors;
- **Total prior arming:** Arming of all sectors in maximum security mode.

Status panel

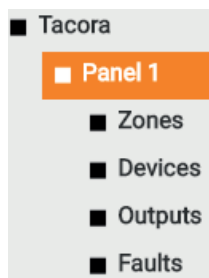
Name	ADD	REFRESH	State
Total arming			OFF
Total prior arming			OFF
Alarm			OK
Excluded inputs			OK
Prior armed sectors			OK
Armed sectors			OK
Sectors with memory			OK
All ready sectors			OK
Battery anomaly			Anomaly
AC anomaly			OK
Panel alarm			OK
Panel tamper			OK



6.5 CONTROL UNIT Menu - fire detection control unit

Starting from software version 1.0.10 (beta), the gateway supports the connection to TACÓRA fire detection control units. To add a control unit, click on the **Tacora** menu and then on : "Panel 1" sub-menu will appear.

The "Control unit" page allows mapping the communication to the TACÓRA control unit, managing its zones and consulting its output and fault states.



6.5.1 General settings

This preliminary section of the "Control unit" menu is used to set the parameters for connection to the intrusion detection control unit:

GENERAL DETAILS	
NAME	Control unit data plate.
USER	User code used by the gateway for communication with the control unit. It must be a numerical code, and must be valid for the control unit.
CODE	Numerical code (password) for the authentication of the user by the control unit.

COMMUNICATION	
COMMUNICATION TYPE	Selection of the gateway communication mode: TCP/IP or Serial/USB
PORT	Communication port to use in case of serial communication (option only available for TCP/IP communication).
IP ADDRESS	Control unit address and port within the LAN network.
PORT	
SPEED	Communication Baud rate
POLLING TIMER	Control unit interrogation time (in ms). Adjust the time to increase or decrease the frequency at which the gateway requests the control unit to provide the status.
EXECUTION STATE	Operating status of the driver for communication with the control unit. In normal conditions it must be "Running".
COMMUNICATION WITH PANEL	Connection status notification.

Communication with the control unit can be started or stopped using the "START" and "STOP" buttons respectively. The "UPDATE CONF." button causes a stop, followed by a start of the communication.



The parameters that can be configured in this section include those for MODBUS protocol connection ("Modbus Bridge"). For information on the configuration using this protocol, see the specific section of this manual ("8. MODBUS PROTOCOL - TACÓRA FIRE DETECTION CONTROL UNITS" on page 33).

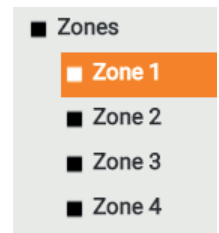


6.5.2 Zones

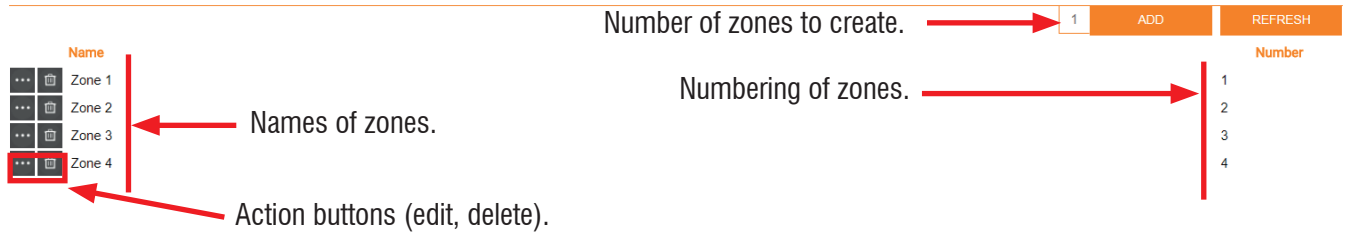
This section can be used to add and configure the control unit zones within the gateway.

To add zones, proceed as follows:

1. Enter the number of zones to add in the appropriate field at the side of “ADD” (default: 1);
2. Press “ADD” and wait until the operation is completed. The created zones will automatically be listed after any already existing ones.



Zones



After the zones have been created, it will be possible to change their names and numbers (we recommend that the automatically assigned numbers are kept unchanged), and check their status. On-board zone 0, reserved to buttons, is not created automatically. To create it, rename one zone (for example the last one) as zone 0 with number 0.

The action button at the side of each zone name gives access to its detail tab. It also allows to permanently remove a zone from the project.

Detailed view of the single zone.

Object properties

General information

Name: Zone 1
 Number: 1

CLOSE

States

Name	State
Zone 1 - Alarm	OK
Zone 1 - Fault	OK
Zone 1 - Exclusion	Alarm

The “States” section displays status information updated on a real time basis.

Each zone has the following statuses:

- **Alarm:** zone alarm status;
- **Fault:** zone fault status;
- **Exclusion:** zone exclusion status.

6.5.3 Devices

This section allows associating devices to the zones. It is not currently supported.



6.5.4 Outputs

This section shows the control unit output statuses. These can be only accessed on a “read-only” basis: they cannot be controlled, but only viewed in real time.

The status of the **Alarm** output is very important, since it notifies the control unit alarm states in real time.

Outputs

Name	State
Alarm	OK
Pre-alarm	OK
Fault	Alarm
Buzzer	OK
OpenCollector 1	OK
OpenCollector 2	OK
OpenCollector 3	OK
OpenCollector 4	OK
Sensors power	OK
Sensors power output	OK
Bell exclusion	OK
Repeater exclusion 1	OK
Repeater exclusion 2	OK
Relay status Zone 1	OK
Relay status Zone 2	OK
Relay status Zone 3	OK
Relay status Zone 4	OK
Relay esclusion Zone 1	OK
Relay esclusion Zone 2	OK
Relay esclusion Zone 3	OK
Relay esclusion Zone 4	OK
Relay status Aux 1	OK
Relay status Aux 2	OK
Relay esclusion Aux 1	OK
Relay esclusion Aux 2	OK

6.5.5 Faults

This section allows consulting any control unit fault status.

The **General fault** is the most important among all, since it summarizes all the possible faults.

Faults

Name	State
General fault	OK
Bell fault	OK
Battery fault	OK
AC fault	OK
24V fault	OK
24V restorable fault	OK
AC vs ground fault	OK
Mass vs ground fault	OK
GSM fault	OK
CPU fault	OK
EEPROM fault	OK
Card Communication fauld	OK
Card registration fault	OK
Loop fault	OK



7. MODBUS PROTOCOL - INTRUSION DETECTION CONTROL UNITS

The gateway can be configured to monitor and manage the control unit functions using the MODBUS protocol. This protocol is based on a master-slave type communication, where a master Modbus device (for example a PLC or SCADA) interrogates the various slave devices.

As slave type device, the gateway supplies information on its status through *registers* that are updated in real time.

7.1 Communication settings for intrusion detection control units

The parameters for Modbus protocol connection may be configured in the “**Modbus bridge**” section, which can be accessed by scrolling to the bottom of the “**Control unit**” page.

Modbus bridge

Communication:

Slave address:

IP port:

IP communication mode:

Enable Modbus commands:

Password for Modbus commands (optional):

Password expire:

Filter Modbus commands on change of value:

CLOSE
START
STOP
UPDATE CONF.

The following parameters must be provided:

COMMUNICATION	Type of connection. Three types of Modbus connection are possible: <ul style="list-style-type: none"> • RTU, through RS-485 serial connection (see the v.1.02 guide at the following web address: www.modbus.org); • TCP/IP, through LAN connection (see the v.1.0b guide at the following web address: www.modbus.org); • Encapsulated RTU (RTU over IP, see below). The gateway can also make available both connections at the same time (RTU + TCP/IP). In case of serial connection, the fields SERIAL PORT and TRANSMISSION SPEED will be enabled: enter their respective values.
SLAVE ADDRESS	Identification number of the Gateway as a slave device. Useful in case of serial line connection. (Default: 1. We recommend that this is not changed)
IP PORT	Number of the IP port used for Modbus communication in case of TCP/IP communication. A port number higher than 1024 must be specified. Warning: the IP port must be different from the port used by another fire detection control unit possibly connected.
IP COMMUNICATION MODE	Type of packet encapsulation in case of TCP/IP communication. Possible options: <ul style="list-style-type: none"> • Standard TCP/IP • RTU over IP
ENABLE COMMANDS	Flag the box to enable the forwarding of commands to the control unit through Modbus.
FILTER COMMANDS	Flag the box to prevent forwarding multiple identical commands. Note: check Filter Commands only if the PLC server repeatedly sends the same command.
ALLOWED SECTOR COMMANDS(*)	Select one option: All: both arming and disarming commands are allowed. Armed: only the arming command is allowed. None: no command allowed.
ALLOWED ZONE COMMANDS (*)	Select one option: All: both inclusion and exclusion commands are allowed. Armed: only the inclusion command is allowed. None: no command allowed.

(*) **Note:** the Allowed Sector/Zone Commands defined above only have effect on commands from Modbus (not SCS or KNX).



7.2 Registers for intrusion detection control units

If Modbus communication is enabled, the registers listed in the following table are available. These registers contain information updated in real time on the status of the gateway. The status-address mapping is preconfigured during the development stage. Therefore, the Modbus protocol does not contemplate the need to define gateway rules. Addresses are both in hexadecimal and decimal format. To obtain the decimal coding, use a simple HEX → DEC conversion, for example:

0x3001 → 12289

WARNING: Some pollers consider registers starting from 0, others from 1.

STATUS READING:

ADDRESS / RANGE		FUNCTION	CODING	DESCRIPTION
0x0000	0	FC3	Unsigned integer	Status of the communication with the control unit 0: error 1: ok 2: wrong password
0x0001	1	FC2	INPUT (0/1)	Status of the communication with the control unit 0: error 1: ok
0x0100	256	FC2	INPUT (0/1)	Control unit power source fault status
0x0101	257	FC2	INPUT (0/1)	Control unit battery fault status
0x0200 (*)	512	FC2	INPUT (0/1)	Control unit alarm
0x0201 (*)	513	FC2	INPUT (0/1)	Control unit tampering
0x0401 (*)	1025	FC2	INPUT (0/1)	All sectors ready
0x0402 (*)	1026	FC2	INPUT (0/1)	Sectors armed
0x0403 (*)	1027	FC2	INPUT (0/1)	Sectors armed in maximum security mode
0x0404 (*)	1028	FC2	INPUT (0/1)	Alarm
0x0405 (*)	1029	FC2	INPUT (0/1)	Sectors with memory
0x0406 (*)	1030	FC2	INPUT (0/1)	Excluded inputs
0x1001 ... 0x1400	4097 ... 5120	FC2	INPUT (0/1)	Alarm status, input 1 ... X
0x1401 ... 0x1440	5121 ... 5184	FC2	INPUT (0/1)	Alarm status, sector 1 ... X (**)
0x1501 ... 0x1900	5377 ... 6400	FC2	INPUT (0/1)	Memory status, input 1 ... X
0x1901 ... 0x1940	6401 ... 6464	FC2	INPUT (0/1)	Memory status, sector 1 ... X (**)
0x2001 ... 0x2400	8193 ... 9216	FC2	INPUT (0/1)	Inclusion status, input 1 ... X
0x3001 ... 0x3040	12289 ... 12352	FC2	INPUT (0/1)	Arming status, sector 1 ... X
0x3101 ... 0x3140	12545 ... 12608	FC2	INPUT (0/1)	Maximum security status, sector 1 ... X
0x3201 ... 0x3240	12801 ... 12864	FC2	INPUT (0/1)	Sector that can be armed, 1 ... X
0x5001 ... 0x5400	20481 ... 21504	FC2	INPUT (0/1)	Output status, 1 ... X

(*) statuses available starting from software version 1.0.5

(**) see Note on page 24



If Modbus commands are enabled, it will be possible to send commands to the control unit. Command-address mapping is completed as per the following table.

COMMANDS:

ADDRESS / RANGE		FUNCTION	CODING	DESCRIPTION
0x0100	256	FC5	COIL (0/1)	General arming command
0x0101	257	FC5	COIL (0/1)	Priority general arming command
0x2001 ... 0x2400	8193 ... 9216	FC5	COIL (0/1)	Exclusion command, input 1 ... X
0x3001 ... 0x3040	12289 ... 12352	FC5	COIL (0/1)	Arming command, sector 1 ... X
0x3101 ... 0x3140	12545 ... 12608	FC5	COIL (0/1)	Maximum security command, sector 1 ... X
0x4401 ... 0x4800	17409 ... 18432	FC6	0/1/2	Remote zone command 0 = idle; 1 = alarm; 2 = tamper (only for firmware versions Villeggio v.8.6.10, Pregio v.3.0.7, Proxima v.1.0.7 or higher)
0x5001 ... 0x5400	20481 ... 21504	FC5	COIL (0/1)	Output command, 1 ... X

NOTE: the interrogation of a register that has not been configured in the gateway will be met by an "ILLEGAL ADDRESS" type error (response hex81).

7.3 Protection of commands

The forwarding of commands through Modbus can be password protected. This password must have been previously specified in the control unit configuration interface using the following parameters (available if the "ENABLE COMMANDS" option is active):

PASSWORD FOR MODBUS COMMANDS	Password to be entered using Modbus (16 characters maximum).
MODBUS PASSWORD EXPIRE	The duration of the password indicated as valid: <ul style="list-style-type: none"> • Never (does not expire until reset) • 30 seconds to 30 minutes • At each command

To send the password using Modbus, it will be necessary to use the following registers, in write-only mode:

ADDRESS / RANGE		FUNCTION	CODING	DESCRIPTION
0xFF01 0xFF10	65281 65296	FC6 FC16	ASCII	Password characters (1 to 16)
0xFF11	65297	FC6 FC16	0/1	If set to 1, the password is checked If set to 0, the password is reset

The password characters (and final confirmation register) can be sent through Modbus one at the time (in which case processing will only occur when the 0xFF11 register is set to 1), or using a single multiple writing command. The usage status of the password may be checked through the following register:

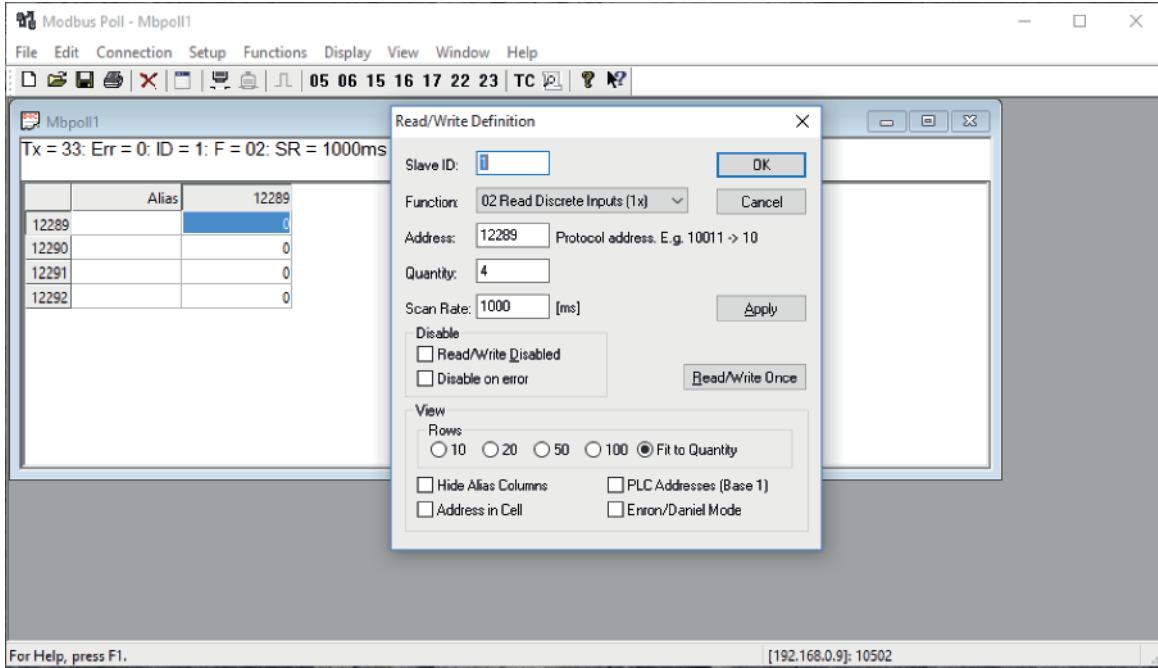
ADDRESS / RANGE		FUNCTION	CODING	DESCRIPTION
0xFF00	65280	FC3	Unsigned Integer	0 = not enabled / not used 1 = Invalid password 2 = Valid password



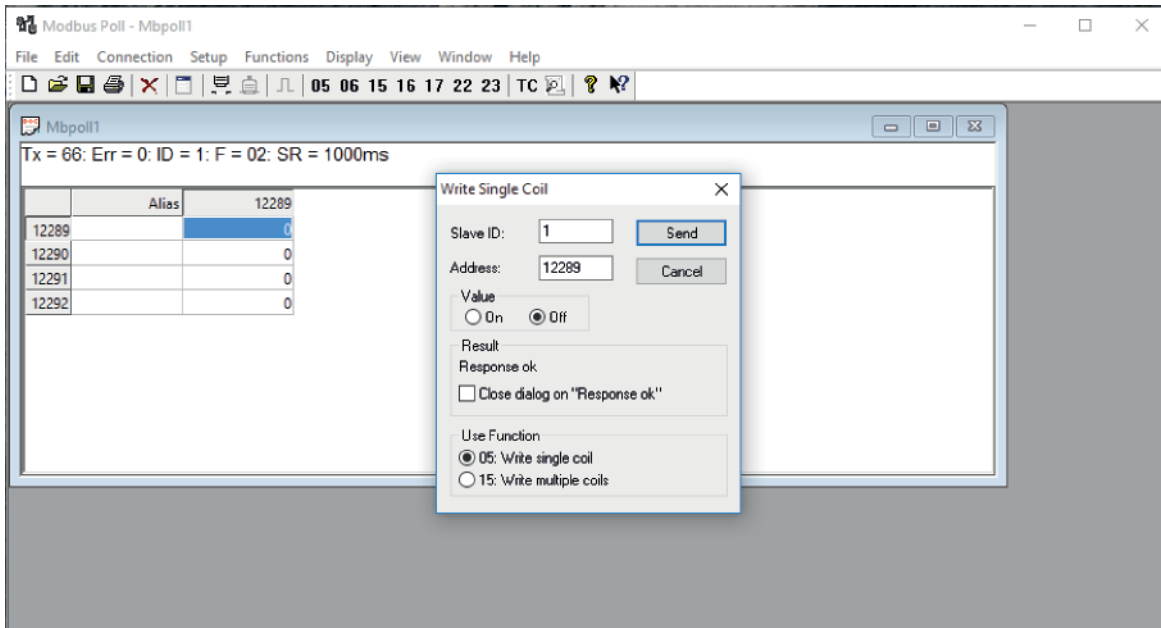
Example

The following screens show an example of gateway reading and control using the Modbus test software:

- reading of the arming status of 4 sectors:



- first sector control:





8. MODBUS PROTOCOL - TACÓRA FIRE DETECTION CONTROL UNITS

The TACÓRA fire detection control units can dialogue with the home automation system via the gateway (equipped with software version 1.0.10 or higher) through the MODBUS protocol.

This protocol is based on a master-slave type communication, where a master Modbus device (for example a PLC or SCADA) interrogates the various slave devices.

As slave type device, the gateway supplies information on its status through *registers* that are updated in real time.

8.1 Communication settings for intrusion detection control units

The parameters for Modbus protocol connection may be configured in the “**Modbus bridge**” section, which can be accessed by scrolling to the bottom of the “**Control unit**” page.

Modbus bridge

Communication:	TCP/IP
Slave address:	1
IP port:	10503
Packets encapsulation:	RTU over IP

CLOSE

START

STOP

UPDATE CONF.

Unlike for the intrusion detection control units, the fire prevention regulations require that no commands can be sent to the control unit. Therefore, the **ENABLE COMMANDS** box is not present.

The following parameters must be provided:

COMMUNICATION	Type of connection. Two types of Modbus connection are possible: <ul style="list-style-type: none"> • RTU, through RS-485 serial connection (see the v.1.02 guide at the following web address: www.modbus.org); • TCP/IP, through LAN connection (see the v.1.0b guide at the following web address: www.modbus.org). ELMOGWAY can also make available both connections at the same time (RTU + TCP/IP). In case of serial connection, the fields SERIAL PORT and TRANSMISSION SPEED will be enabled: enter their respective values.
SLAVE ADDRESS	Identification number of the Gateway as a slave device. Useful in case of serial line connection. (Default: 1. We recommend that this is not changed)
IP PORT	Number of the IP port used for Modbus communication in case of TCP/IP communication. A port number higher than 1024 must be specified. Warning: the IP port must be different from the port used by another intrusion detection control unit possibly connected.
IP COMMUNICATION MODE	Type of packet encapsulation in case of TCP/IP communication. Possible options: <ul style="list-style-type: none"> • Standard TCP/IP • RTU over IP



8.2 Registers for fire detection control units

The registers listed in the table below are available for connection of the TACÓRA control unit to the home and building automation system. These registers contain information updated in real time on the status of the gateway. The addresses are both in hexadecimal and decimal format. To obtain the decimal coding, use a simple HEX → DEC conversion, for example:

0x006C → 108

WARNING: Some pollers consider registers starting from 0, others from 1.

STATUS READING:

ADDRESS	FUNCT.	CODING	DESCRIPTION
0x0065	101	FC2	INPUT (0/1) Zone 1 output
0x0066	102	FC2	INPUT (0/1) Zone 2 output
0x0067	103	FC2	INPUT (0/1) Zone 3 output
0x0068	104	FC2	INPUT (0/1) Zone 4 output
0x0069	105	FC2	INPUT (0/1) Aux 1
0x006A	106	FC2	INPUT (0/1) Aux 2
0x006B	107	FC2	INPUT (0/1) Open-collector output 1
0x006C	108	FC2	INPUT (0/1) Open-collector output 2
0x006D	109	FC2	INPUT (0/1) Open-collector output 3
0x006E	110	FC2	INPUT (0/1) Open-collector output 4
0x006F	111	FC2	INPUT (0/1) Buzzer
0x0070	112	FC2	INPUT (0/1) Pre-alarm
0x0071	113	FC2	INPUT (0/1) Alarm
0x0072	114	FC2	INPUT (0/1) Fault
0x0073	115	FC2	INPUT (0/1) Detectors supply
0x0074	116	FC2	INPUT (0/1) Resettable power supply output
0x0075	117	FC2	INPUT (0/1) Zone 1 output exclusion
0x0076	118	FC2	INPUT (0/1) Zone 2 output exclusion
0x0077	119	FC2	INPUT (0/1) Zone 3 output exclusion
0x0078	120	FC2	INPUT (0/1) Zone 4 output exclusion
0x0079	121	FC2	INPUT (0/1) Aux 1 exclusion
0x007A	122	FC2	INPUT (0/1) Aux 2 exclusion
0x007B	123	FC2	INPUT (0/1) Bell output exclusion
0x007C	124		
0x007D	125		
0x007E	126		
0x007F	127		
0x0080	128		
0x00C9	201	FC2	INPUT (0/1) General fault
0x00CA	202	FC2	INPUT (0/1) Bell output fault
0x00CB	203	FC2	INPUT (0/1) Battery fault
0x00CC	204	FC2	INPUT (0/1) Power supply fault
0x00CD	205	FC2	INPUT (0/1) 24V out fault
0x00CE	206	FC2	INPUT (0/1) 24V RST out fault
0x00CF	207	FC2	INPUT (0/1) Earth-power shortcircuit fault

0x00D0	208	FC2	INPUT (0/1)	Earth-ground shortcircuit fault
0x00D1	209	FC2	INPUT (0/1)	GSM fault
0x00D2	210	FC2	INPUT (0/1)	CPU fault
0x00D3	211	FC2	INPUT (0/1)	EEPROM fault
0x012D	301	FC2	INPUT (0/1)	No communication
0x012E	302	FC2	INPUT (0/1)	Not registered
0x012F	303	FC2	INPUT (0/1)	Loop fault
0x0135	309	FC2	INPUT (0/1)	Repeater 1 exclusion
0x0136	310	FC2	INPUT (0/1)	Repeater 2 exclusion
0x1000 ... 0x102F	4096 ... 4143	FC2	INPUT (0/1)	Alarmed zones (*)
0x1100 ... 0x112F	4352 ... 4399	FC2	INPUT (0/1)	Faulty zones (*)
0x1200 ... 0x122F	4608 ... 4655	FC2	INPUT (0/1)	Excluded zones (*)
0x2001 ... 0x2FFF	8193 ... 12287	FC2	INPUT (0/1)	Excluded loop devices
0x3001 ... 0x3FFF	12289 ... 16383	FC2	INPUT (0/1)	Loop device outputs state
0x4001 ... 0x4FFF	16385 ... 20479	FC2	INPUT (0/1)	Loop devices requesting reset
0x5001 ... 0x5FFF	20481 ... 24575	FC2	INPUT (0/1)	- Not active -
0xF001	61441	FC2	INPUT (0/1)	Status of the communication with the control unit 0: error 1: ok

(*) The count of the zones starts from 0, thus including on-board zone 0 dedicated to buttons only.

9. KNX PROTOCOL

The KNX protocol is based on a distributed system with shared bus to which all the devices are connected. It contemplates two types of addresses:

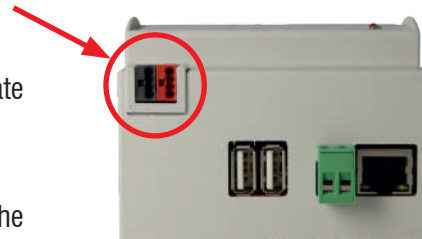
- a physical address, different for each device connected to the KNX bus, with X.Y.Z syntax;
- a logic group address, relating to the function, with X.Y.Z. syntax.

The gateway may be connected to a KNX system and interact bidirectionally with the home automation functions, sending control units status notifications and receiving commands on as many group addresses.



9.1 Connection to the KNX bus

It is possible to connect the gateway to the KNX bus using the appropriate standard red-black connector found on the device. No additional interface is required.



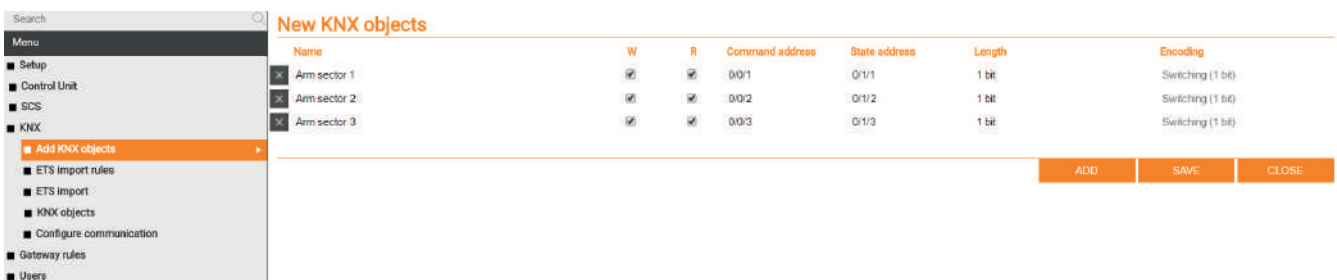
The procedure for interfacing the control unit with a KNX system requires the following steps:

1. Creation of group addresses;
2. Association between KNX group addresses and the control unit functions through one or more *gateway rules* (see “11. GATEWAY RULES” on page 42).

Note for creation of rules with KNX elements: in order to make reaction and signal propagation correct, at least power supply on KNX bus is required.

9.2 Creation of group addresses

In order to set ELMOGWAY for communication on one or more KNX group addresses, it will be necessary to first of all add them to the project through the item “**Add KNX objects**” in the “**KNX**” section of the side menu.





Press ADD to insert a new row in the list (previously empty), where it will be possible to specify the following parameters:

NAME	Text label identifying the new address in the project.
W / R	Flags enabling writing and reading mode respectively. The flags specify if the new addresses can be controlled and/or read by the gateway.
COMMAND ADDRESS	If the W flag is active, enter the group address for the command (to the KNX bus) in the 3-level format (X/Y/Z).
STATE ADDRESS	If the R flag is active, enter the group address for the reading (from the KNX bus) in the 3-level format (X/Y/Z). Note: this field is optional if the W flag is also active and a command address has been entered. In this case, the status will be read from the same command group address.
LENGTH	Select, among the ones available, the length of the <i>payload</i> of the telegrams sent/received through the KNX bus on the specified addresses. This selection must be consistent with the settings of the ETS project.
ENCODING	Based on the preselected length, select the coding most suitable for representing the data sent or received on the group addresses to create.

Once the list has been compiled with all the group addresses to add, press "SAVE" to start the creation procedure, and wait for its completion. Once the confirmation message has been received, it will be possible to add new addresses, or to continue with the subsequent steps.

9.3 List of KNX objects

The list of KNX objects created with the previous procedure is available in the "**KNX OBJECTS**" list of the side menu. By selecting one of these items, it is possible to access its detail tab in one of two possible ways:

- By pressing the "three dots" at the side of the name;
- By pressing "EDIT" on the toolbar at the bottom of the menu.

In both cases, a page similar to the one in the figure that follows will open:



Inside this tab, it is possible to change the previously assigned name.

However, the group address cannot be changed: for a new group address, it will be necessary to delete the object by pressing "DELETE" on the toolbar, and then create a new object with the desired address.

Once all the desired objects have been created, they must be associated to the control unit functions by means of appropriate gateway rules, as shown in chapter "11. GATEWAY RULES".

9.4 Communication configuration

This page can be used to set the *physical address* used by the gateway to send commands on the KNX bus.

In the appropriate field, insert a value in X.Y.Z format consistent with the line and sector addressing to which the gateway is physically connected.

In case of doubts, leave the preset value **0.0.255** unchanged, as this normally allows communication with all system devices.



9.5 Import from ETS (optional)

ETS (Engineering Tool Software) is a software developed to design and configure a KNX system.

The gateway can import a project created in ETS, making the creation of KNX objects much faster than if following the previously described manual procedure.

A project may be imported from ETS in the following supported formats:

- **ESF + PHD:** Export for OPC
- **CSV:** export of group addresses (it only contains the list of group addresses: any data type information must be entered by hand)

9.5.1 ESF + PHD format

In ETS, select "**Export for OPC server**". This will generate two files:

- ESF: it contains the group addresses, their labels and their relations with other group addresses
- PHD: it contains the physical addresses of the project devices

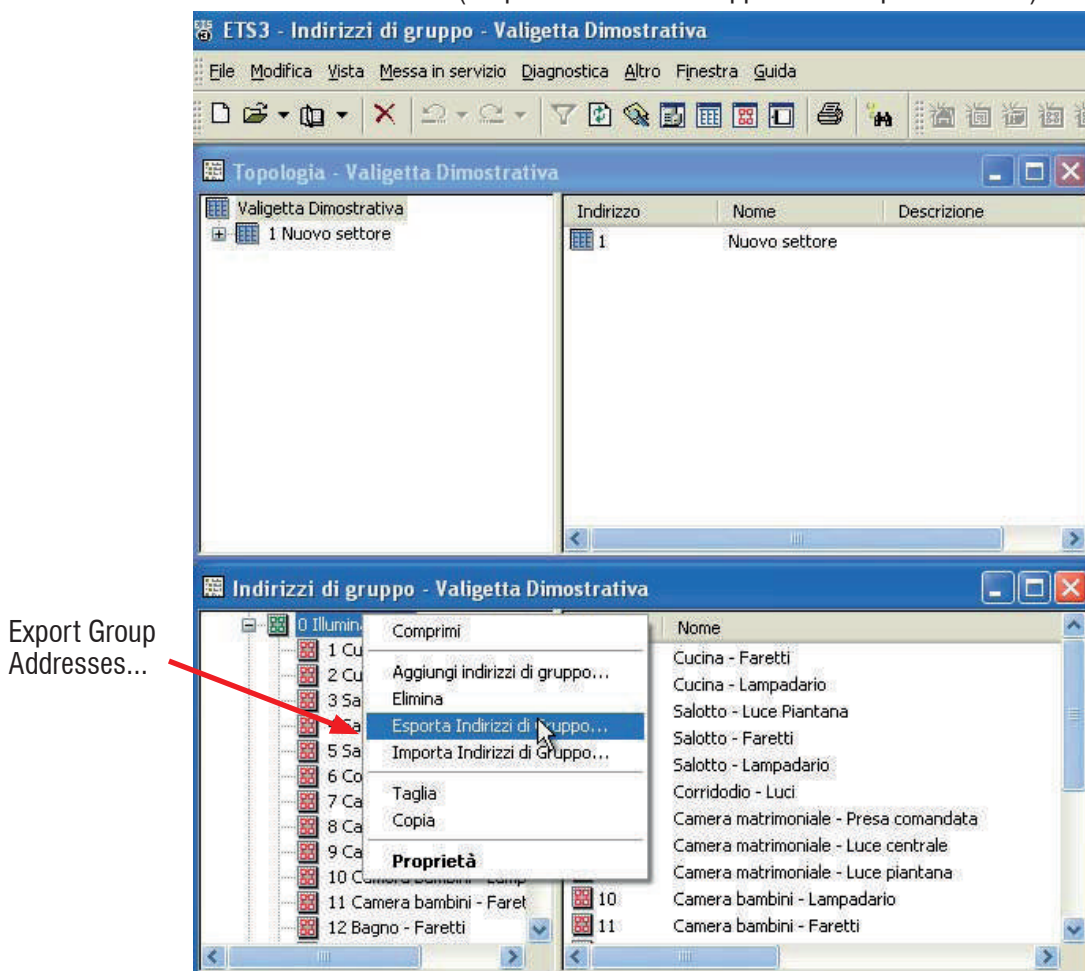
9.5.2 CSV format

The gateway can also import KNX addresses from a CSV file having the following features:

- Tabs as column separators
- Group address label in the first column
- Group address in the second column
- Bit length (optional) in the third column

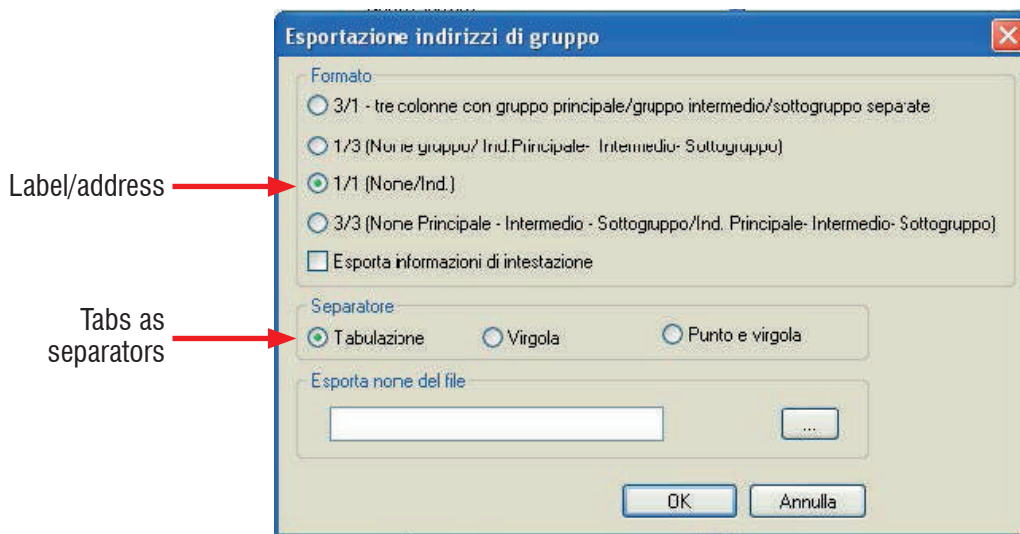
This type of file can be generated manually (for example using Microsoft Excel), or automatically using the ETS software. In the latter, the following will be necessary:

1. Select the group address branch to export
2. Select "EXPORT GROUP ADDRESSES" ("Esporta Indirizzi di Gruppo..." in the picture below) from the relevant menu





3. Specify the following options:
- Data organised in 2 columns (label + address)
 - Tabs as column separators



Note: CSV import can also be useful to quickly create new KNX objects in ELMOGWAY without having to go through ETS: simply enter group address and label information in a new file and start the import procedure.



10. SCS PROTOCOL

The gateway can be connected to a SCS/MyHOME system and interact bidirectionally with home automation functions, sending status notifications to the control unit and receiving commands on as many communication addresses. The SCS protocol requires IP interfacing with a Bticino device operating as gateway.

10.1 SCS connection

With enabled models, it is possible to connect the gateway to the SCS bus through the network using an appropriately configured *OpenWebNet gateway* (configured using the *MyHome Suite* software by Bticino).

The compatible model is the F454 gateway, which is the only one OpenWebNet branded.

Operation using F459, MH202, MH200N has been tested, nevertheless functional limits exist: their usage is not advisable. Operation using other gateway models is neither tested nor guaranteed.

The procedure for interfacing the control unit with an SCS / MyHOME system requires the following steps:

- Creation of objects and their addressing;
- Association between SCS objects and the control unit functions through one or more *gateway rules* (see "11. GATEWAY RULES" on page 42).

10.2 Communication configuration

In order to configure the communication with the OpenWebNet gateway of the MyHOME system, first of all access the "SCS" detail tab of the side menu using the "three dots" at the side of the name (once selected), or by clicking "EDIT" on the bottom toolbar.

The communication can be configured in the initial section of the page by entering the following parameters:

IP ADDRESS	IP address assigned to the OpenWebNet gateway.
PORT	Enter the port for communication with the OpenWebNet gateway. Unless in case of specific needs, the preset value 20,000 should be left unchanged.
OPENWEBNET PASSWORD	Enter the password for access to the Open protocol, if different from the preset password (12345).
ENABLE COMMUNICATION	Select this item to enable communication with the OpenWebNet gateway. Otherwise, the configuration will not be applied.
EXECUTION STATE CONNECTION STATUS	They indicate respectively the execution status of the communication driver (which must be activated by pressing START after completing the configuration), and the actual status of the communication with the OpenWebNet gateway.

After completing the configuration, start the communication by pressing START and check that the "Connection status" is "connected".



The SCS devices that may be connected to the gateway can be split into three categories: **lights**, **automation** and **CEN buttons**.

10.3 Adding lights

It is possible to include one or more SCS lights in the gateway, and then control them (or react to their switching on). From the "SCS" configuration page, access "Lighting" and proceed as follows:

1. Enter the number of lights to create in the appropriate field at the side of "ADD" (default: 1);
2. Click "ADD".

At the end of the procedure, the new light controls are listed as in the following figure:

Lighting

Name	Addressing	RO	LP	GR	Tipology	State
Light 1	Point	1	1		ON/OFF	Off
Light 2	Point	1	1		ON/OFF	Off
Light 3	Point	1	1		ON/OFF	Off
Light 4	Point	1	1		ON/OFF	Off

For each item, it is possible to specify the following:

NAME	Identification label of the light control within the project.
ADDRESSING	Specify if the control must be: <ul style="list-style-type: none"> • Point (or a "direct" control for a single light point); • Room (control for all the devices of a set area); • Group (control for all the devices belonging to a group); • General (control for the whole system).
RO LP GR	Based on the type of addressing, specify the address to control by entering: <ul style="list-style-type: none"> • RO: ambient number; • LP: light point number; • GR: group number;
TYPE	Specify if the control must be ON/OFF or dimmer.
STATUS	It gives the possibility of viewing the updated status in real time, or to control the light (after pressing "UPDATE").

After configuring the desired light controls, press "UPDATE" to restart communication.

10.4 Adding automations

Automations may be added in a similar way as the lights. However, differently from lights, it will be possible to also specify:

TYPE	Specify if the control must be roll-up shutter (UP/DOWN) or ON/OFF type.
-------------	--

Automations

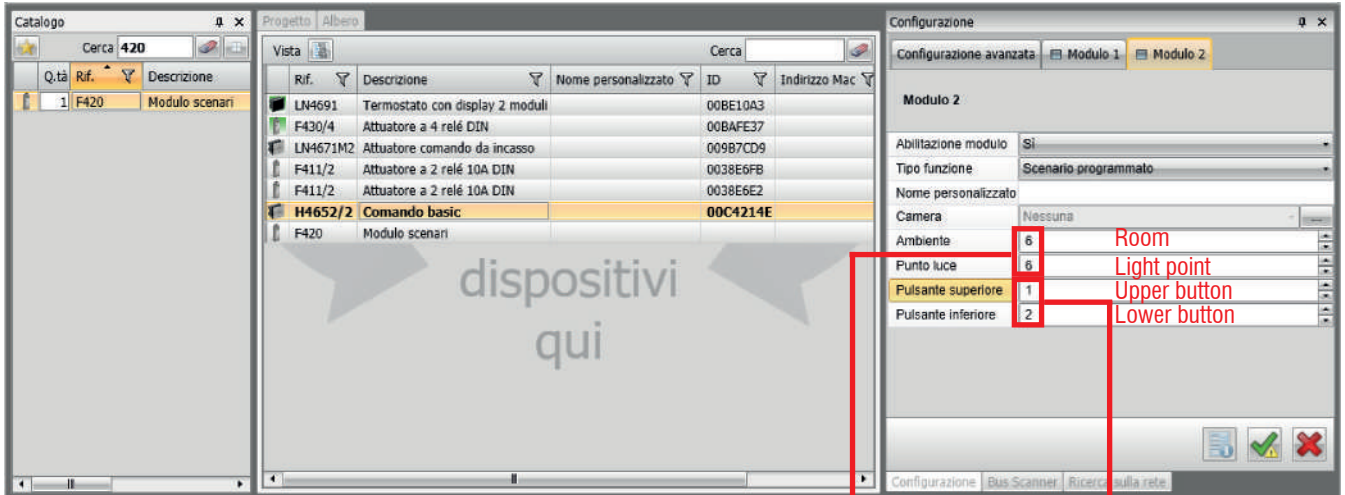
Name	Addressing	RO	LP	GR	Tipology	State
Roll-up shutter 3	Point	1	3		Up/Down	Stop
Roll-up shutter 4	Point	1	4		Up/Down	Stop



10.5 Addition of CEN Pushbuttons

This section can be used to configure within the gateway one or more MyHOME buttons, associating to their pressure a command to be sent to the control unit. For this purpose, buttons must first be configured (through jumper or through the MyHome Suite software) for CEN or CEN PLUS scenario control.

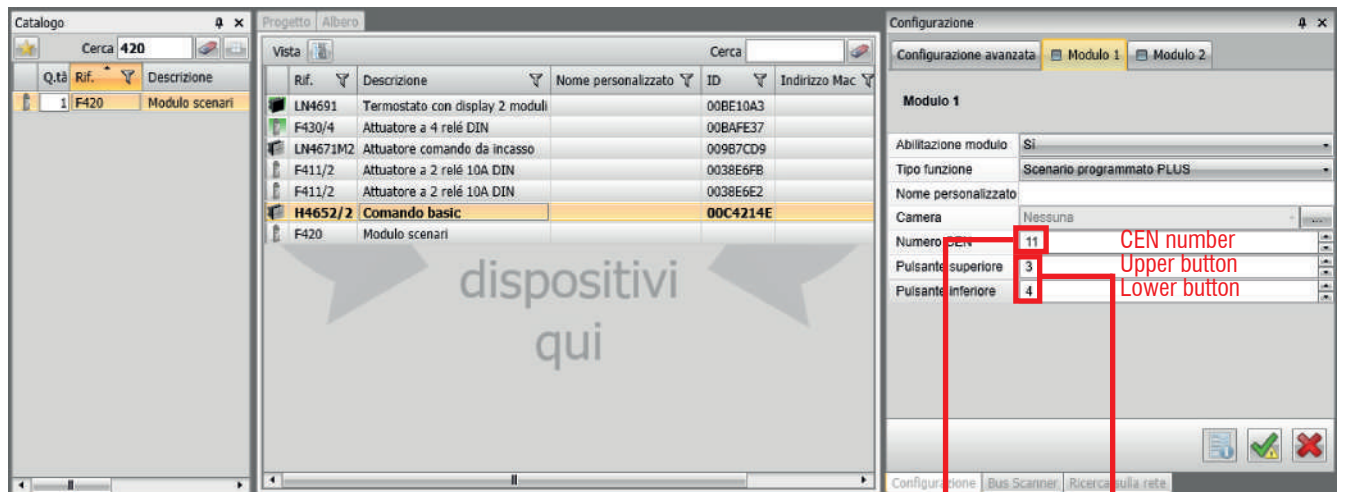
In case of CEN pushbuttons, it will be necessary to enter their address (RO and LP) and the button number in the gateway:



CEN Pushbuttons

Name	Scene type	RO	LP	CEN	Button	State
Scenario 1	CEN	6	6		1	Idle
Scenario 2	CEN	6	6		2	Idle

Vice-versa, in case buttons for the recalling of CEN PLUS programmed scenarios, the CEN number and the button number must be specified:



CEN Pushbuttons

Name	Scene type	RO	LP	CEN	Button	State
Scenario 1	CEN PLUS			11	3	Idle
Scenario 2	CEN PLUS			11	4	Idle

11. GATEWAY RULES

After creating KNX or SCS type objects as discussed in the previous chapters, these can be used to set specific rules. *Gateway rules* are graphic associations between the commands and states of the control unit (for Tacóra units, only states), and KNX or SCS type objects.

They specify which statuses and commands must be exchanged, and in which conditions; each rule may contain any number of objects and connections. However, to make things easier to read, we recommend separate rules for the different gateway functions.

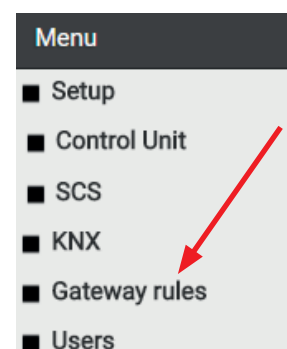
Note: Gateway rules are not required for Modbus interfacing, as this is pre-configured on the appropriate register mapping (see chapter “7. MODBUS PROTOCOL - INTRUSION DETECTION CONTROL UNITS”).

Note for creation of rules with KNX elements: in order to make reaction and signal propagation correct, at least power supply on KNX bus is required.

11.1 Creation of a rule

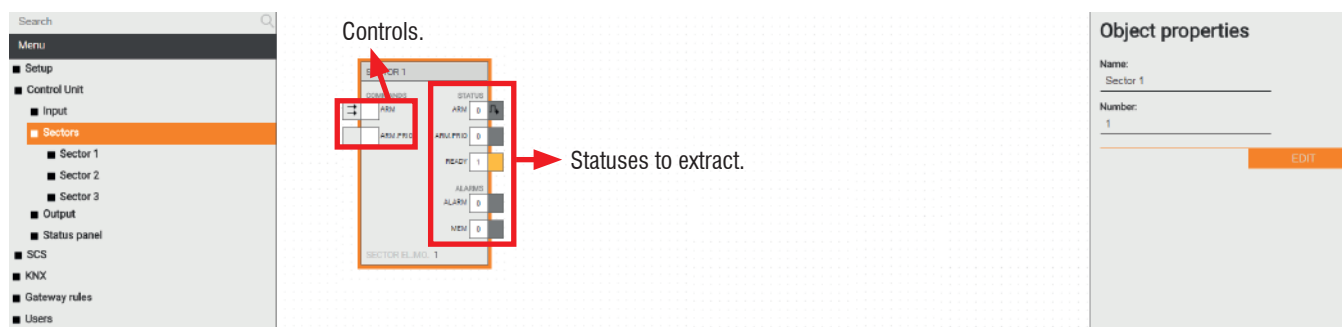
In order to add a new gateway rule, proceed as follows:

1. Identify the **"Gateway rules"** section in the menu (figure on the side);
2. Click "ADD" on the toolbar;
3. Select the new rule;
4. Press the "three dots" at the side, or the "EDIT" button on the toolbar. Accessing the rule will show a page that is initially empty, in which to drag the objects to interconnect. Clicking the right mouse key will open a detail panel (on the right of the screen), which can be used to assign a name to the rule.
5. On the side menu, identify the "input", "sector" and "output" objects, as well as the KNX group addresses or the SCS objects to add, and drag them to the empty area. It is also possible to search for the desired objects using the search bar, and then drag them (one at the time) from the search results. The objects are represented as **blocks** with one or more **nodes** on the left (inputs) and right (outputs). Input nodes may be connected to other objects in order to control the object in question, while output nodes can themselves control other objects. Commands among objects in the gateway rules are always on value variation only.



Example with intrusion detection control units

In order to interact with sector 1 of the control unit, simply identify it in the **"Control unit → Sectors"** section and drag it as shown in the following image:



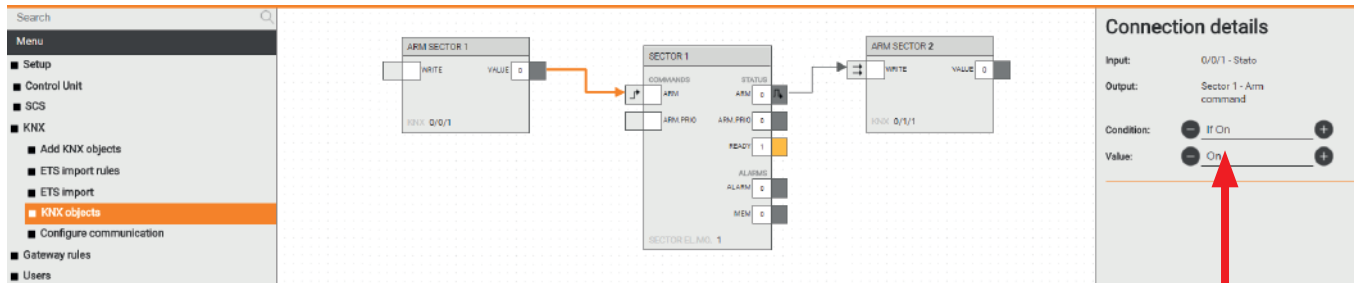
In order to control sector 1 of the control unit from the appropriate KNX control address and, at the change of its arming status, notify its status on the status address (both previously created as shown in chapter “9. KNX PROTOCOL”), proceed as follows:

1. Drag sector 1 from the **"Control unit → Sectors"** section;
2. Drag the **"Arm sector 1"** object to the left of sector 1;
3. Drag the **"Arm sector 2"** object to the right of sector 1;
4. Press and hold down the left mouse button with the pointer on the control node of the first KNX object and, keeping the mouse button down, connect it to the "ARM" node of the sector (in this way, when the KNX address status changes



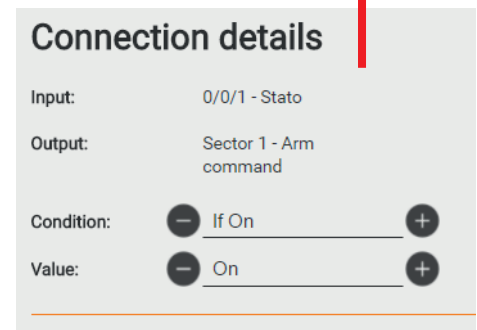
the sector receives a command);

5. In the same way, connect the "ARM" output node to the KNX status object. In this way:
 - When a value 1 is received on the 0/0/1 group address, the sector is armed; vice-versa, the sector is disarmed when a value of 0 is received;
 - When the arming status of the sector changes (not only due to the activity of the gateway, but also following a field command), the arming status (1 or 0) is sent through the bus to the group address 0/1/1.



It is possible to change the preset behaviour of a connection by pressing the right button above the same, which will cause the opening of a side panel (as seen in the figure on the side), where it will be possible to specify:

- **Condition:** The value of the source object that determines the command for the destination object. This can be "ALWAYS" (therefore no filter is applied), or one of the following values for the selected object;
- **Value:** Value to send to the destination object. It can be:
 - CURRENT VALUE: the value of the source object is transferred to the destination object;
 - INVERTED VALUE: the value of the source object is inverted before being transferred to the destination object;
 - A specific value among those available for the destination object.



Looking at the previous example, in order to only arm sector 1 when receiving a value of 1 on group address 0/0/1, but not to disarm it when a value of 0 is entered:

- Enter "If ON" as condition;
- Enter "ON" as value.

The graphic indicators of the nodes affected by the connection change accordingly, to provide a graphic view of the connection itself.

It is also possible to simulate the operation of the gateway rules in real time, interacting with the control nodes (right side) of KNX and SCS objects. To do this:

- Double click on the node numeric value (white box);
- In case of ON/OFF nodes, a value is sent immediately;
- However, in case of numerical nodes, the user is given the possibility of entering a value (enter the value and press SEND).



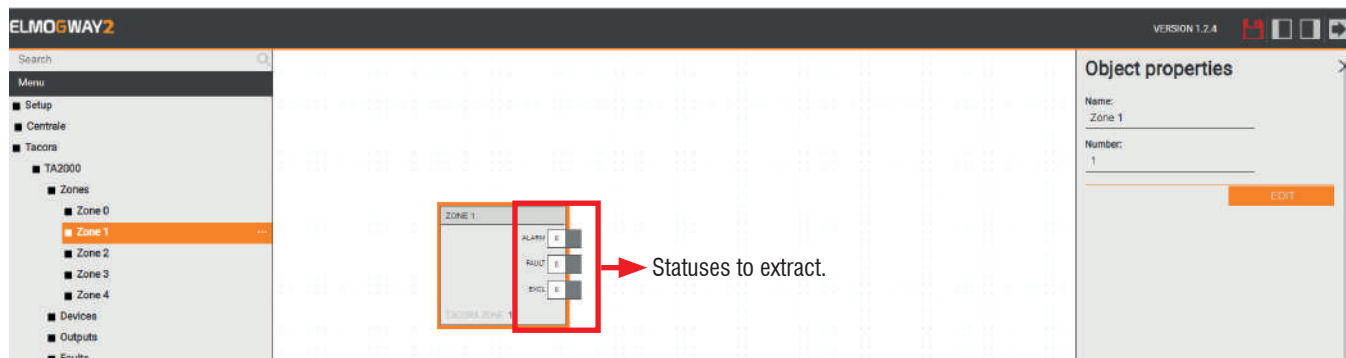
Example with Tacóra fire detection control units

Starting from firmware version 1.2.4, the gateway rules that involve Tacóra fire control units allow to drag blocks related to:

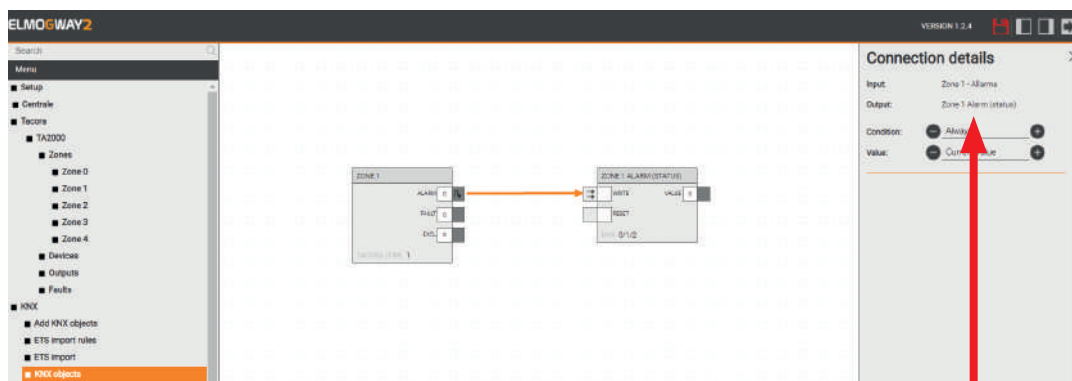
- zones (alarm, fault, exclusion)
- devices (exclusion, reset request, onboard output state)
- outputs (managed by the control unit)
- faults (managed by the control unit)

with possibility to manage their states (indicated in brackets).

It is not possible to perform command operations on the previously described elements.

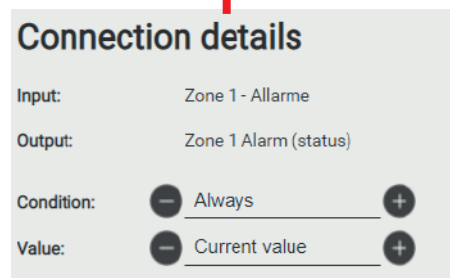


In the following example, when the alarm state of zone 1 changes, the alarm state (1 or 0) is sent to the group address 0/1/2.



It is possible to change the preset behaviour of a connection by pressing the right button above the same, which will cause the opening of a side panel (as seen in the figure on the side), where it will be possible to specify:

- **Condition:** The value of the source object that determines the command for the destination object. This can be “ALWAYS” (therefore no filter is applied), or one of the following values for the selected object;
- **Value:** Value to send to the destination object. It can be:
 - CURRENT VALUE: the value of the source object is transferred to the destination object;
 - INVERTED VALUE: the value of the source object is inverted before being transferred to the destination object;
 - A specific value among those available for the destination object.



Note: if you try to add an object for which rules are not supported, or whose parameters are partially incomplete (e.g. group addresses etc.), the “Object not supported by gateway rules” message appears on top of the page.



12. USERS



12.1 Change of credentials

The access credentials of the admin user may be changed in the following way:

1. In the "**Users**" section of the menu select "admin";
2. Access its tab by clicking on the "three dots" or the "EDIT" button on the toolbar;
3. Change the username as desired: it must not contain spaces or special characters;
4. Change the password, making sure to enter it twice.

Object properties

General information

Username:

Password:

Repeat password:

CLOSE



NOTES



NOTES

13. TABLE OF CONTENTS

1. GENERAL FEATURES	3
2. FEATURES	3
3. ELMOGWAY STRUCTURE	4
4. ELMOGWAY2 STRUCTURE	5
5. INSTALLATION AND RESET	6
5.1 Installation	6
5.2 Wiring	6
5.3 Wiring examples: ELMOGWAY	7
5.4 Wiring examples: ELMOGWAY2	12
5.5 Reset procedures	16
5.5.1 Factory IP address reset	16
5.5.2 Total factory configuration reset	16
6. SOFTWARE CONFIGURATION	17
6.1 ACCESS TO THE CONFIGURATION SOFTWARE	17
6.2 GENERAL OVERVIEW OF THE USER INTERFACE	18
6.3 SETUP MENU	20
6.3.1 LANGUAGE	20
6.3.2 NETWORK	20
6.3.3 BACKUP/RESTORE	20
6.3.4 DATE/TIME	20
6.3.5 SOFTWARE UPDATE	21
6.3.6 MAINTENANCE	21
6.4 CONTROL UNIT MENU - INTRUSION DETECTION CONTROL UNIT	22
6.4.1 GENERAL SETTINGS	22
6.4.2 INPUTS	23
6.4.3 SECTORS	24
6.4.4 OUTPUTS	25
6.4.5 CONTROL UNIT STATUSES	25
6.5 CONTROL UNIT MENU - FIRE DETECTION CONTROL UNIT	26
6.5.1 GENERAL SETTINGS	26
6.5.2 ZONES	27
6.5.3 DEVICES	27
6.5.4 OUTPUTS	28
6.5.5 FAULTS	28
7. MODBUS PROTOCOL - INTRUSION DETECTION CONTROL UNITS	29
7.1 COMMUNICATION SETTINGS FOR INTRUSION DETECTION CONTROL UNITS	29
7.2 REGISTERS FOR INTRUSION DETECTION CONTROL UNITS	30
7.3 PROTECTION OF COMMANDS	31
8. MODBUS PROTOCOL - TACÓRA FIRE DETECTION CONTROL UNITS	33
8.1 COMMUNICATION SETTINGS FOR INTRUSION DETECTION CONTROL UNITS	33
8.2 REGISTERS FOR FIRE DETECTION CONTROL UNITS	34
9. KNX PROTOCOL	35
9.1 CONNECTION TO THE KNX BUS	35
9.2 CREATION OF GROUP ADDRESSES	35
9.3 LIST OF KNX OBJECTS	36
9.4 COMMUNICATION CONFIGURATION	36
9.5 IMPORT FROM ETS (OPTIONAL)	37
9.5.1 ESF + PHD FORMAT	37
9.5.2 CSV FORMAT	37
10. SCS PROTOCOL	39
10.1 SCS CONNECTION	39
10.2 COMMUNICATION CONFIGURATION	39
10.3 ADDING LIGHTS	40
10.4 ADDING AUTOMATIONS	40
10.5 ADDITION OF CEN PUSHBUTTONS	41
11. GATEWAY RULES	42
11.1 CREATION OF A RULE	42
12. USERS	45
12.1 CHANGE OF CREDENTIALS	45
13. TABLE OF CONTENTS	48