PROGRAMMING MANUAL

SUPERIA SERIES

Multi-functional hybrid intrusion detection system control units

Addressee for this information: U User | I Installer

1 GENERAL DESCRIPTION

The control units of the SUPERIA series can be configured in two different, complementary ways: with BrowserOne software and via keypad.
BrowserOne software allows the complete configuration of the parameters of the intrusion detection system:

- management of zones, areas, outputs and users;
- access to system options;
- management of phone dialler, wireless sirens, weekly programmer;
- configuration of serial and control devices;
- view control panel status.

The configuration from keypad allows the configuration of only part of such parameters via a **user menu** (that grants the access to a "basic maintenance") and an **installer menu** (for more extensive programming). It also grants access to some operations that can be performed from keypad only, such as:

- wireless devices learning;
- system lock and system test.

This manual details control unit programming through:

- BrowserOne software: description of the functions and parameters that can be changed in each page;
- keypad menus dedicated to the user and to the installer.

Guide to the first configuration > chapter 27 *p. 76*

This section describes the basic configuration operations.
Use this section as starting point for control unit configuration.

2 SETUP

SUPERIA control units require BrowserOne 3.25.3 or above with SUPERIA control unit module.
The installation of BrowserOne requires a PC with Windows operating system.
Note: these instructions refer to the first installation of BrowserOne. Installing BrowserOne in a computer where it is already installed causes the loss of all software settings: update it instead. See paragraph 4.7.1 *p. 7*.
The first installation of requires BrowserOne an Internet connection.
– login to the www.elmospa.com website
– from BrowserOne page, download the following file:

BrowserOne_[version number]_web.exe

– open the file and follow the displayed instructions
– from BrowserOne page, download the following file:

[Control unit model] [version number]_setup.exe

– open the file to install the module
Once done, click on BrowserOne icon to run it.
To familiarise yourself with the interface of BrowserOne, see chapter 3 *p. 3*.
– click on **Modules** button on menu bar and load the right module
– select the operation mode: base (simplified, with access to the main options) or advanced (including all the options)

⚠ *The mode can also be changed later: click on the proper button in the command bar.*

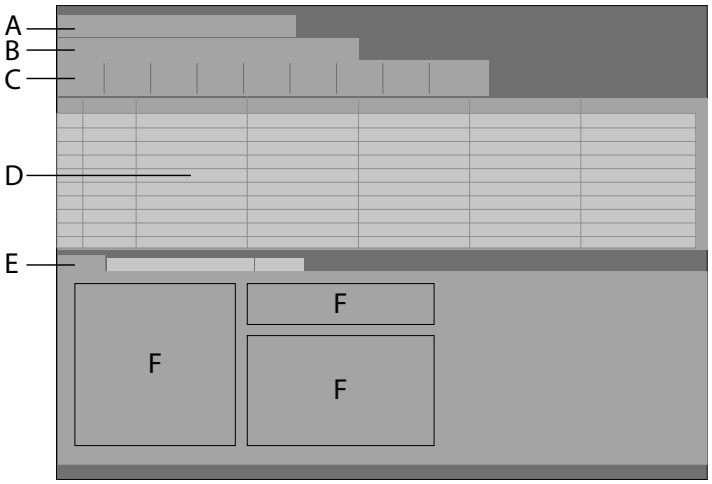
– press OK
– connect to the unit (see paragraph 4.3 *p. 4*)

Uninstalling BrowserOne

– from BrowserOne software launch path, click on "Uninstall..." and follow the displayed indications
Note: uninstalling the software also automatically removes any installed modules. The configuration files are saved in a separate folder instead: [Letter_HDD]:\Documents and Settings\User_Name\Documents\BrowserOne

3 SOFTWARE INTERFACE

BrowserOne software interface includes:



- menu bar (A) (see 4 *p. 3*);
- controls bar (B): quick commands;
- "pages" bar (C): grants the access to pages grouping data according to their operating function.

Each page may include:

- in top area (D), a grid whose rows are elements of a list (of zones, outputs, users, functions, etc. according to the page selected), columns are changeable parameters;
- in bottom area (E), a series of tabs (subpages): by clicking on a tab users can see a series of parameters related to the row selected in the grid. Inside tabs, options can be grouped in areas called panes (F).

Some pages do not show grids, but only tabs including parameters to change.
Status page will only be available when connected to the unit.

Hide/display columns

Right click on a column heading: it will display a menu where users can select columns to be displayed.

Multiple change of data

The software also allows selecting multiple rows for data change simultaneously (example: connect zones with a single action).
Select the first cell to modify, hold SHIFT key down and select the last cell of the interval to modify.
Change the content of the last cell selected, then press ENTER: the content of all cells selected will be changed accordingly.
Use CTRL instead of SHIFT to add or remove single rows to/from selection.

Quit

To quit software, click on closing icon top right, or click on **File** > **Exit** on menu bar.
Either close only the current module, or the application.

4 MENU BAR

4.1 File

▼ **New**

Load a default configuration:

- Factory default (supplied by manufacturer);
- defined by the User (saved with the command **Save as User Default...**).

▼ **Open...**

Load a configuration from a file previously saved to the PC, with *.stp: [file name].stp extension
As default, configuration files are saved to the following path: C:\Users\user_name\Documents\BrowserOne\
We recommend not to select automatic save files (AutoSavedSetup_dd.mm.yyyy_hh.mm.ss.stp).

▼ **Open history...**

It opens log files (*.hst format) previously created.

Such files, saved to the page **Events History** (see 19 *p. 56*), are backup files of the unit history event log.

▼ **Import**

Load a configuration file saved as an old format.

▼ **Save**

Save: it saves the changes to the current configuration.

Save As...: it saves the current configuration to a new *.stp file.

Save as User Default...: it saves the configuration in order to load it with **New** > **User Default**.

Save for Supervisor...: save the configuration, so it can be loaded to a supervision software.

▼ **Print Settings...**

It sets parameters for the displayed page printing (page format, source, orientation, margins).

All printers installed to the PC can be used.

▼ **Print**

It sets the parts of the module to print: **Current Page** (the whole page displayed), **All Pages**, one specific **Page** (and/or a tab of such page).

Note: not all pages/displayed data can be printed.

▼ **Compare with**

It compares current configuration with one of the following:

- **Factory Default** configuration
- **User Default** configuration
- **Other Setup...** (previously saved to file)

A printable list of different items will be displayed.

▼ **Exit**

Exit BrowserOne application.

Using **File** menu, it is also possible to load quickly one of the four most recent configuration files used, and its module as well.

4.2 Modify

▼ **Undo**

Undo the last change(s).

▼ **Redo**

Redo an action previously undone.

4.3 Connect

Unit connection has to be activated by the user. If the user does not activate the connection, the installer will not be able to connect to the unit and configure it via BrowserOne.

The user has to provide the installer with temporary or permanent access using keypad menu AUTHORIZATION: see chapter 21 *p. 60*.

Once authorised, the installer can start connection to the unit using options **Connect to...** or **Detect panels**.

Note: In case of USB connection: if you connect the unit before and then open BrowserOne, upon opening of the software a wizard for automatic connection via USB will be opened too. Click on the pop-up window displayed to start the wizard.

4.3.1 Connect to...

Option to start the wizard for unit connection.

The appropriate module will be loaded automatically.

– click on **Connect to...** (available on controls bar too)

– select **Connection type**

USB connection requires miniB USB optional cable. This connection allows also the update of firmware and voice synthesis function.

– click on **Next**

In the example below, the use of USB and TCP/IP connection will be described. For other connection types, see BrowserOne manual

USB connection

– connect the unit to the PC using mini B USB cable
– wait for the COM port virtualization software to be loaded
– in the **Serial connection** window click to update the available communication ports
– select "ELMO Virtual COM" from drop-down menu
– select **Next**: the software will attempt to start the connection
– when the connection is fine, enter installer code and press OK: a bar will be displayed on the bottom of the page

If the connection is impossible (because of communication port error, installer code error, or lack of connection authorization), error windows will be displayed. After a unit reset with USB connection active, it may happen that the connection is impossible: disconnect and reconnect the cable.

TCP/IP connection

– connect the control unit and the PC to the same LAN
• use the Remote Manager software to view the list of all connected EL.MO. devices

Note: Remote Manager is available for download from the product page of the control unit.

Until the first writing of the configuration, SUPERIA Series will be in Discovery mode and will broadcast its name on the LAN, making it easy to recognize it in the list

– select the row corresponding to SUPERIA Series
– change the network parameters ot the control unit to bring it inside the PC's subnet

Network parameters caon only be changed this way if the control unit is in Discovery mode and the user code is the default one.

– in window **TCP/IP connection**, enter control unit IP address and connection port
– select **Next**: the software will attempt to start the connection
– when the connection is fine, enter installer code and press OK: a bar will be displayed on the bottom of the page

If the connection is impossible (because of communication port error, installer code error, or lack of connection authorization), error windows will be displayed.

4.3.2 Detect panels

This option allows detecting units already connected to the PC.

– click on **Detect panels** (available on controls bar too)
– click on **Refresh** button
– select the COM port used by the unit
– click on **Connect to the device...** button

4.3.3 Close connection

Click to close the connection.
Click on **Detect panels** to re-activate the connection later.

4.4 Actions

This menu is available only when the keypad is connected.

▼ **Read setup**
Button available also on controls bar.
Click to load to BrowserOne the current unit configuration. A progress bar will display reading status.
This function is necessary in case of first connection to the unit to read proximity key codes and codes of radio detectors and remote controls learnt to RIVERRF concentrators or to GATEWAY2K.

▼ **Write setup**
Button available also on controls bar.
Click to save the configuration set in BrowserOne onto the unit. A progress bar will display writing status.

▼ **Read only radio codes self-learnt by devices**
Click to read only the configuration of radio codes previously learnt by the unit.

4.4.1 485 Devices Management

Click to open a window for detecting devices connected over serial line.
For all devices (with 8/4/2/1 zones) it is possible to select All, Only Configured or None.

In pane **Operations** on the right the following actions are available:

- **Read**
  Read selected devices.
- **Diagnostics**
  Start a diagnostic tool to detect possible address setting problems.

Select zones to be tested (all or a range of zones) and press OK.
When the procedure is finished, a window will open and display green LED indicators in case of successful diagnostic procedure.

4.4.2 Clock

Click to set unit date and time.
To modify parameters in the window, select the date and set the time with the relevant functions.
Select **Sync with System Clock** to synchronize unit clock with used PC clock.
Select **Write Date/Time** to write date and time to control unit.

4.5 View

This button allows accessing configuration pages.
For direct access to pages, use "pages" bar below.

4.6 Modules

Function used to load a module to be used with the control unit.

- **Load Module**
  Show installed modules.
  Select the desired module, then press OK.
- **Close Module**
  Close the module currently loaded.
  Below the two commands, the latest modules used are displayed.

Once the suitable module has been installed, it will be loaded automatically when the connection to the control unit is started.

4.7 Tools

- **Plant Management**
  Function to manage installed plants, saving data and configurations onto a database.
  For further information see BrowserOne manual.
- **Users Management**
  Function to manage operators who can access BrowserOne.
  For further information see BrowserOne manual.
- **Create Local Database Backup**
  It creates a backup copy of the local database containing plants and users; it will be saved in *.bak format.
- **Restore Local Database Backup**
  It loads a backup copy of the local database previously saved, and will replace the current local database with it.
- **Software Updates**
  Install new versions of the BrowserOne software or modules present.
  For further information, see 4.7.1 *p. 7*.
- **Firmware Update Panel**
  It updates control unit firmware (selecting an update file from a local archive or from a path on the PC).
  See control unit technical manual.
- **Firmware Update Device**
  It allows to update the firmware of a connected device (via RS-485 serial line or USB).
  See the relevant manuals indications.
- **Voice Synthesis Management**
  It allows recording voice messages onto devices that support voice synthesis.
  For further information, see 4.7.2 *p. 7*.

▼ **Options**

It allows setting data and messages to be displayed on printed pages.

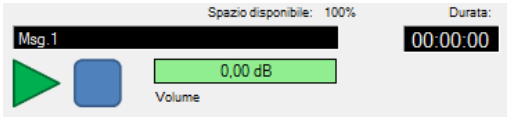
4.7.1 Software updates

Function to update BrowserOne software and modules to the latest version available.
Table rows show installed modules, columns show current version and latest released version: if the two versions are not the same (row highlighted red), the update will be suggested.
Click on **Perform Update** button to download and install all available updates.
Click on **Add components** (N available) (in the left pane) to choose updates to launch.
To exclude the update for a single module:
– select the corresponding row
– in the left pane **Actions**, check **Ignore this update**
To uninstall the update for a single module:
– select the corresponding row
– in the left pane **Actions**, check **Uninstall component**

4.7.2 Voice synthesis management

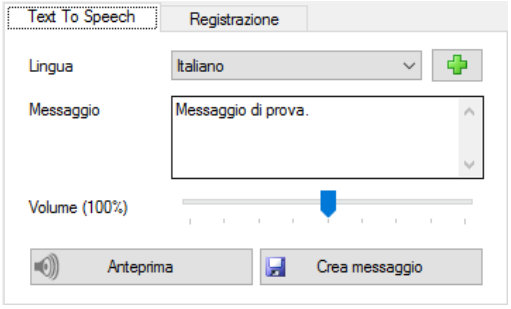
To manage voice synthesis messages select:
- **Voice Synthesis for Panel**, to record voice messages for the control unit;
- **Voice Synthesis for Leda485VOX**, to record voice messages for the siren.

The window **Voice Synthesis Management** will open.
– open a new project (**Open project** button) or create a new project (**New project** button), and enter a name for the project
– a project can contain 64 messages max: select a message to manage the recording using controls on right pane **Audio Elaboration**
In pane **Audio Elaboration**, use the top area options to listen to/stop/adjust the volume of a recorded message.



The messages can be recorded in **Text To Speech** or **Recording** mode: select the corresponding tab.

Text To Speech



– write the message in the field **Message**
– adjust the **Volume** using the cursor below: the message will be pronounced by a female voice, into the Language selected

in drop-down menu or selected pressing the button which detects languages available
– click on **Preview** to hear the message
– click on **Create message** to save it with a name (with which it will be displayed in the left list)

Recording

⚠ *Before recording, check PC sound card operation (if it is the case, start Windows hardware test). Record messages with headphones featuring a high-quality microphone in a noiseless environment.*

– to start recording, select REC (the vertical bar shows the signal level in recording mode)
– to stop recording, select STOP
– record all messages desired

Messages can be imported, exported and deleted by selecting the corresponding options below.
When finished, select **Save project** to save the project.
To transfer the file with the recorded messages to the unit (siren) memory, select **Write to panel** (**Write to Siren**).
File transfer can be made only if directly connected via USB-C cable.

4.8 Language

Select the language to be used for BrowserOne interface.

4.9 Information (?)

This menu provides information about the version of BrowserOne and the loaded modules.
It also allows to register the license for BrowserOne Enterprise and to display additional functions.

***

The following chapters will provide details on configuration pages.
To open configuration pages, click on the relevant icon on "pages" bar.

5 ZONES

Page for zones parameters configuration.
To operate on a single zone:
– select the zone row on the grid
– modify the zone parameters using options in the tabs below the grid and/or changing values in the grid columns
The following sections refer to tabs in the page **Zones**.

5.1 General

Tab that includes the general properties of each zone.

▼ **Zone Name**
Assign a name to the zone.

▼ **Info**
Additional information (example: device type and model).

▼ **Authorization level**
Select an authorisation level for the selected zone, from 0 (min) to 20 (max).

▼ **Connected**
Select the checkbox to enable the device connected to the zone.
Zones not connected will not signal alarms or tamper events.

▼ **Zone Type**
Select the type of the zone connected from the drop-down menu:
Normally Open: zone with C-NO contact (open when idle, closes upon alarm condition).
Normally Closed: zone with C-NC contact (closed when idle, opens upon alarm condition).
Balanced: double-balanced zone (monitored conditions: idle status, alarm status, tampering).
Triple Balanced: triple-balanced zone (monitored conditions: idle status, alarm status, tampering, fault).
Split: select split when two split contacts are connected to the same line: the zone associated to the first one will have address n (number of the row seleced on the grid), the other one will have address n+16. Only for zones 1 to 16.
Extended Split: select Extended Split when two extended split contacts are connected to the same line: the zone associated to the first one will have address n (number of the row seleced on the grid), the other one will have address n+16. The Extended Split mode adds to the split mode the monitoring of short circuit and line cut events. Only for zones 1 to 16.
Fast: zone used to connect sensors for roll-up shutters, inertial or magnetic sensors. Only for zones 1 to 12.
River RF: zone used to connect sensors learned on to RIVERRF concentrator.
Wired Concentrator: zone used to connect sensors learned on to wired concentrators.
Sensor 485: zone to which a sensor with serial interface has been connected; it occupies one address.
Output Status: the zone follows the corresponding output (having the same number). If the output is enabled, the zone enters alarm condition; if the output is disabled, the zone remains idle.

⚠ *An output has to remain in the same logic status for at least 300 ms in order to ensure that the zone take the same status. On the contrary, below 100 ms interval, the status will not be applied to the zone.*

Remote: the zone is controlled with commands sent via a supervision software directly connected (for domotic applications).

⚠ *For proper operation of the "Remote" function with Home & Building Automation gateways, it is necessary to enable the "Basic maintenance" property for the user associated to domotics functions.*

Progr. balance n: zone configured with one of the balancing programmed in tab Programmable Balance (see paragraph 5.3 *p. 13*).
Logic elaboration: zone to which the result of a logic function processing defined using the output function editor (see paragraph 7.1 *p. 18*) is applied.
e-Vision AI alarm: zone to which a camera supporting the D-Pulse-technology AI functions is connected.

Note: a number of SUPERIA devices equal to the number of control unit zones can be wired to a single D-Pulse control unit.

▼ **Zone Timer**
Timer to be used for some functions (example **Pre-alarm** and **Delayed**).

▼ **Zone Event**

Additional event generated upon alarm event.

When an alarm event occurs, a general “zone alarm” event is always generated, combined with the event selected in this menu (if it has been set).

Example: if the event Medical alarm is associated to a zone, when an alarm event occurs for that zone, two events will be generated: “zone alarm” and “medical alarm”.

Special selections:

No Events: upon zone alarm event, no events are generated except tamper event in case of zone tampered with.

Simple Zone: upon zone alarm event, only the generic zone alarm event will be generated.

Intrusion, tamper, assault, perimeter, emergency door alarm: such events prevent system arming when the zone is alarmed. The green LED (arming status) is off (normally, when a zone not associated to such events is in alarm condition, the green LED indicator blinks).

Technological N: events associated to zones to which devices other than intrusion devices are connected (ex. fridge control, tanks level, etc.).

Technological events do not generate alarms, but only SMS, data and phone communications. They will be saved to control unit history log.

▼ **AND with zone**

Select a zone from the list.

The two zones (the selected one and the active one) will generate an alarm event only if both detect an alarm condition within a set time interval (**Zone AND time**, see paragraph 10.3 *p. 35*).

The first zone generates the event "trigger AND", the second one generates the alarm event.

▼ **Alarms per Zone (Max)**

Maximum number of alarms generated by each zone: when the max is reached, the zone will be excluded.

Set a number between 1 and 15, or set **Unlimited**.

The counter is reset each time one of the pertaining sectors is armed (or, for multi-group zones, if all sectors are armed).

Select **Copy on all zones** to copy the max number for the current zone to all zones.

Only alarm events will be counted (not tamper events).

▼ **Fast**

This pane is only available for inputs with the **Fast** property.

Set **Sensitivity** (pulse number to detect within a set time interval in order to trigger an alarm) and **Pulse Count** (time interval to detect set pulse number).

Zone Options

Properties that can be assigned to single zones.
Select the checkboxes to enable the options.

▼ **24H**

If selected, the zone is always active no matter if its sectors are armed: alarms can be generated also when sectors are disarmed.

Option necessary to connect special sensors (smoke detectors, gas detectors, flood detectors, etc.).

▼ **Exit Path**

If selected, the zone is included in the exit path in order to allow leaving the premises within the time interval set (see **Exit Time**, paragraph 6.1 *p. 16*) after having armed the system.

Within such time, alarms from zones included in the exit path will be ignored. On the contrary, alarms from zones not included in the exit path will generate alarm events.

If an armable zone not included in the exit path is in anomaly status when arming the unit/area, the arming command will be cancelled.

▼ **Pre-alarm**

If selected, the zone prevents the generation of alarms for the set time interval (**Zone Timer**) starting from the entrance in the protected area.

This property allows defining "entry areas": users that enter protected premises walking through such areas have the time to reach a control device and disarm the system. If the time runs out without disarming the system, a tamper alarm will be generated.

⚠ *Pre-alarm property is not compatible with Delayed property.*

▼ **Delayed**

If selected, the zone has to remain in anomaly status longer than the time set (**Zone Timer**) for the control unit to generate an alarm.

If the anomaly status ends before the end of the time set, the zone does not generate an alarm ("zone activity monitor" function).

⚠ *Delayed property is not compatible with Pre-alarm property.*

▼ **Auto-Bypass**

If selected, the zone is automatically bypassed when the Exit Time of one of the pertaining sectors has elapsed and the zone is alarmed.

If a zone also has the Multi-group property, all sectors it belongs to must be armed for the auto-bypass to be performed.

Autobypass property will be reset:

- for non multi-group zones: when all the sectors pertaining to the zone are disarmed;
- for multi-group zones: when one of the sectors pertaining to the zone is disarmed;
- for 24H zones: upon arming, if they are in idle mode;
- when zones go back to normal status, if the option **Cancel auto-bypass at zone reset** at zone reset has been selected (see 10.1 *p. 30*).

Zones auto-bypass event is saved to unit history log.

Auto-Bypass property is not compatible with **Dual** property.

If this property is selected for a zone, the system can be armed even if such zone is alarmed.

Example: the zone is associated to a window detector. If users want to go out and wish to arm the system leaving the window open (= alarmed zone), they will have to select auto-bypass option for the corresponding zone.

▼ **Multi-group**

If selected, the zone will generate an alarm event only when all the sectors it has been assigned to are armed.

▼ **Exit Port**

Property selectable only if the zone is part of an exit path.

If selected, the remaining time of exit time interval will be reduced to 5 seconds (if it is longer) when anomaly condition for the zone ends before the end of the exit time.

▼ **Chime**

If selected, the keypad controlling sectors associated to the zone will emit an acoustic signal when the zone triggers an alarm

- while the corresponding sectors are disarmed, or
- while the zone has **24H** property.

In **Options** page it is possible to set a single acoustic signal (**Single Chime**, paragraph 10.1 *p. 30*) and the time interval (**Chime interval**, paragraph 10.3 *p. 35*).

▼ **Walk Test**

If selected, the zone will be included in the zones test during the next system test.

It is required that at least one zone has Walk Test property, otherwise system test will not be performed.

▼ **Follow On**

If selected, the zone will generate the pre-alarm event if another zone in the same sector is in pre-alarm. Otherwise, it generates an alarm.

Example: a room is protected with a door detector and a volumetric detector, and the door detector has **Pre-alarm** property (that is, is included in an entry path).

If users want the volumetric detecto “to follow” the door detector (that is, do not generate alarm durin entry time), select the property **Follow On** for the zone associated to the volumetric detector.

▼ **Dual**

If selected, to this zone is assigned an associated zone, which will be

- the following one (ex. 44), when the dual zone is odd (ex. 43)
- the previous one (ex. 1), when the dual zone is even (ex. 2)

The dual zone and the associate one have to belong to the same sectors.

For dual zones the following rules apply:

- as long as the associated zone is in idle mode or bypassed, the alarm condition of the dual zone will be ignored: the system can be armed even if the dual zone is alarmed.

- if a dual zone has pre-alarm property and the associate one does not, the prealarm property will be ignored when the associate zone is alarmed.

Dual property is not compatible with **Auto-Bypass** property.

Dual zones are suitable for protecting windows with shutters, where a zone protects the window, and another zone protects the shutter.

When selecting dual property for both, they become each other's associated zone: until one is kept close, the other can be left open without triggering an alarm.

Moreover, if the window contact has the pre-alarm property and the shutter contact does not, the window contact generate an instant alarm if the unit has been armed while the shutter was open. If the unit has been armed while the shutter was closed, and it still is, the window contact generates a pre-alarm.

▼ **Anomaly**

If selected, when the zone is in alarm condition the yellow anomaly LED blinks. This property is normally selected for 24H zones whose function is not tied to intrusion detection.

▼ **Key Zone**

If selected, the zone acquires the key property. A key zone causes the switching of the arming status of the associated sectors when it enters anomaly condition.

For the proper functioning of the property:

– select the 24H property for a key zone;
– connect the key zone to an impulsive control device with NO contacts, normally idle.

The transition between closed and open contact generates an arming command (BrowserOne will suggest wiring).

If the key zone is controlled by a contact that has no backup battery, it is essential that the contact is idle while not powered. Otherwise, a power fault would cause an unintended switching.

If selected, in **Zone Options** window will appear **Key zone set/reset** checkbox: select it to use a state control device instead of an impulsive one.

▼ **Tamper excludable**

An excluded zone does not generate intrusion alarms but it will keep generating tamper alarms.

Check this box to disable also tamper alarm signals given by this device when excluded.

▼ **AI server supervision**

Flag to enable the supervision of the zone to which a camera supporting the D-Pulse-technology AI functions is connected.

5.1.1 Radio code

The area displays the class of NG-TRX radio devices learnt to that zone:
- "Alarm" for volumetric detectors;
- "Alarm/reset" for perimeter detectors;
- "Not learnt" when the zone has no NG-TRX radio devices.

Learn the radio codes of NG-TRX devices on GATEWAY2K using the FAST ACQUIRE or LEARN RADIO DET. menu items (see paragraph 22 *p. 64*).
Then, select **Read setup** to read unit setup.
In **Zone Type** column, "Radio" will appear.
To set a zone type different from "Radio" for an already used zone, select **Delete Radio Code** radio code first to cancel the previous code.

5.1.2 Technological name

If a **Technological N** event has been associated to a zone (see **Zone Event**), you can also define a name for it.

5.2 Assign areas/sectors

Window to associate zones to sectors.
Select sector checkboxes in each column.
By default, 16 areas are available with 4 sectors each; to change number of area sectors, see **Sectors per area mode** in panel **General Options** (paragraph 10.1 *p. 30*).

▼ **Select All**

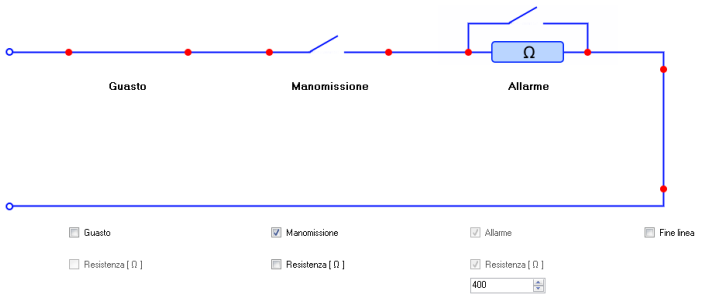
Click to associate the selected zone to all available sectors.

▼ **Deselect All**

Click to remove all the sectors associated to the selected zone.

5.3 Programmable balancing

Use this tab to define up to 4 balancing configurations that can be freely applied to the zones.
This function is useful, in particular, in case you need to integrate the control unit in an already existing system including zones that are not balanced according to the EL.MO. standard.



– click on a row to enter the editor pertaining to that specific balancing
– to add a fault or tamper contact, check the relevant box (the alarm contact is already available by default)
– once a contact has been added, check the **Resistance** box to add its resistance
– set the resistance value in the field

You can choose a resistance value between 400 Ω and 12 kΩ.
The software will automatically check configuration validity.
To associate one of the 4 balancing configurations to a zone:
– go to page **Zones** > **General**
– select the grid row corresponding to the zone
– from **Zone Type** drop-down menu, select **Progr. balance n** (1, 2, 3, 4 according to the balancing to be applied)

5.4 Ultrabus/Terabus devices

This tab allows managing wired devices with RS-485 serial interface.
Options of this menu will be available only selecting **Wired Concentrator** or **Sensor 485** from **Zone Type** drop-down menu.

▼ **Zone Type**

Select the connected zone type from drop-down menu.

Device type

Define the number of zones of the connected device (8/4/2 for wired concentrators, 1 for 485 sensor).
The graphic next to the field will display the settings on the address dip switch and jumpers.

Input properties

Select the connection type (Normally Open / Normally Closed / Balanced).

Fast

Select it to enable the menu.
Set here sensitivity and integration for compatible sensors connected.

RiverTH - Zone N

Menu to adjust parameters of tools for analogue values measurement (gas detectors, probes) connected to a RIVERTH concentrator.

Advanced devices configuration

Pane available only if in **Zone Type** type drop-down menu the option **Sensor 485** is selected..
This pane allows managing volumetric detectors with serial interface (ex. GRIFOX485, STRIXO485, TRIAL485): select

Open configuration form.
Select the device when required.
This menu allows:
- displaying the device operating status;
- setting device working parameters and enable/disable functions;
- using noise detection function and record its waveform for 4 hours max.

See manuals of detectors for further information on this subject.

5.5 Radio devices NG-TRX

SUPERIA control units series supports NG-TRX radio devices through the connection to GATEWAY2K device (up to 4) over serial line.
To configure GATEWAY2K serial line connection see chapter 12 *p. 44* and the relevant technical manual.
Detectors and transmitters of NG-TRX system can be learnt to GATEWAY2K using the options FAST ACQUIRE or LEARN RADIO DET. in installer menu on keypad (see paragraph 22 *p. 64*).

Options NG-TRX

General parameters of NG-TRX devices.
Options in this pane are the same for all NG-TRX devices.

▼ **Buzzer activation**
It enables/disables the device buzzer for alarm and/or reset.
If disabled, error tone will be sent anyway.

▼ **Performance tuner**
It adjusts the consumption/power balance used for transmission: Automatic, Minimum consumption, Maximum power.

▼ **Supervision interval**
It sets the frequency of supervision transmissions sent by the unit to check device functioning.

▼ **Delay supervision anomaly**
Select this option to delay the supervision time (by 6 times) for the anomaly signalling for lack of supervision.

▼ **Tx Boost**
Select this option to increase the transmission power of the device (real range increase: 10–30%).

⚠ *It may affect battery life substantially.*

Sensor options [SENSOR NAME]

It allows setting parameters specific to NG-TRX sensors connected.
See manuals of NG-TRX detectors for further information.

5.6 Radio devices River RF

Window to manage compatible radio devices memorized to RIVERRF series concentrators

⚠ *RIVERRF concentrators are not compatible with NG-TRX devices.*

▼ **Zone Type**
Select the connected zone type from drop-down menu.
See **Zone Type** in paragraph 5.1 *p. 9*.

▼ **Supervision Time**
If the option **Supervised** (in **Radio Code on River RF** pane) is selected, supervision time intervals can be set.

▼ **Associated User**
User associated to the remote control learnt to RIVERRF concentrator.

Device setup

Address of the concentrator to which this zone has been learnt.

Radio Code on River RF

Class of the radio device learnt to the concentrator.

▼ **Delete Detector Code**

Click to delete the code of the device learnt to this zone.

▼ **Supervised**

Select to enable the supervision of the device connected to this zone.

Set the supervision interval in **Supervision Time** drop-down menu on the left.

6 AREAS

Page to configure area parameters.
SUPERIA series control units are multiarea units that allow managing up to 64 sectors.
Sectors are grouped in a number of areas.
The number of areas can be changed in page **System Options** > **General** using option **Sectors per area mode** (see paragraph 10.1 *p. 30*).
Keypads and readers can be used as control devices for various areas.
One or more pertaining areas can be associated to each keypad (see paragraph 11.1 *p. 42*).
Each keypad

- shows information on currently operating area and allow changing operating area. With sector keys users can arm/disarm sectors of keypad pertaining areas and also pertaining to the user who performs the operation. In idle mode, LEDs indicate the status of the area.
- can be configured as system keypad: in such case the keypad indicates the general status of the system, and its sector keys indicate areas arming status. In idle mode, LEDs indicate system status.

Recommendations for proper management:

- for each area, set at least one user with authorizations and configure at least one keypad;
- configure from software at least one keypad as system keypad (normally number 1).

For further information on sector keys operating mode in 8/16/32/64 sectors per area, see paragraph 10.2 *p. 34*.
When displaying the log file on keypad, it is possible to view only events pertaining to the keypad and the user.

6.1 Areas

On the grid, select the row of the desired area.
Areas tab below displays properties common to all sectors included in such area.

▼ **Area Name**
Define a name for the area.

▼ **Exit Time**
Maximum time to exit the area once the system has been armed.
Option used with the function **Exit Path** (page **Zones** > **General**, pane **Zone Options**).

7 OUTPUTS

Page for outputs parameters configuration.
To operate on a single output:
– select the corresponding row on the grid
– assign a function to the output by selecting it from the **Output function** drop-down menu

▼ **Output function**

Outputs can be associated a specific function: the output will follow the status of such function.
Select the output function from the drop-down menu.
In detail, outputs with "Manual control" function can be enabled/disabled with OUTPUT CONTROL option in user/installer menu on keypad (see paragraph 21 *p. 60*).
When the output is not used, select "Output disabled": it will be deleted from the list of controllable outputs.

– once selected, set required parameters for the function in pane **Output functions settings** below

▼ **Mode**

Switching mode: the output switches at every new event of the output function.
NRT positive pulse: the output is usually disabled, it activates for the set time (**Timer**) at every new event of the output function. The time is not extended by new events.
RT positive pulse: the output is usually disabled and it activates for the set time (**Timer**)at every new event of the output function. The time is extended by new events.
NRT negative pulse: the output is usually enabled and it disables for the set time (**Timer**) at every new event of the output function. The time is not extended by new events.
RT negative pulse: the output is usually active and it disables for the set time (**Timer**) at every new event of the output function. The time is extended by new events.
Status: the output follows the output function status.
Reversed status: the output follows the opposite of the output function status.
Set/Reset: the output is activated by the set event and deactivated by the reset event.
Reset/Set: the output is activated by the reset event and deactivated by the set event.

▼ **Timer**

In case of pulsed mode, it is possible to set pulse duration here.

▼ **Parameter**

Additional options for some specific output functions.
Select zone / user / keypad for the output function.

▼ **Area N**

Select areas / sectors to apply the output function to.

On the left of the page, additional parameters concerning the selected output can be set.

▼ **Name**

Assign a name to this output.

▼ **Authorization level**

Select an authorisation level for the selected output, from 0 (min) to 20 (max).

▼ **Do not put in history output movements**

If selected, the activation/deactivation of this output will not be logged.

▼ **Interlock with output n**

If selected, a pair of outputs will be set, including the output selected and
- the following one, if the selected output is odd;
- the previous one, if the selected output is even.

This function allows to interlock pairs of outputs: they cannot be enabled simultaneously.
If either output is already active, activating the other one will cause the deactivation of the active one.
The aim of this function is to provide protection for home automation and prevent failures of the connected devices in case of incorrect programming of the outputs.

Note: despite the interlock, the outputs may still activate simultaneously for a few milliseconds due to the physical characteristics of the relays. Configure the output parameters correctly, in order to avoid overlapping.

▼ **Output for presence simulation**

If selected, this output will be used in "Enable presence simulation" and "Disable presence simulation" weekly programmer functions.

▼ **Control output manual**

Function available only when Mode is not set to "Status" or "Reversed status".

If selected, it allows also the manual control for outputs whose output function is not "Manual control".

▼ **Activated without authentication**

If selected, this output can be activated without user code request.

▼ **Logic elaborations editor**

Click to open a graphic output function editor.

7.1 Logic elaborations editor

Besides associating functions to single outputs, BrowserOne allows creating complex functions involving and interconnecting several outputs and zones.
This section provides a graphic editor to define them.
Click on

- **Add scheme** to create a schema in a new page.
- **Open scheme** to open a previously saved schema.

To modify the name assigned to the schema, enter it in the **Scheme name** field.
Up to 255 logic schemes can be defined, using up to 1024 logical elements.
To add an element:

– click on an item in the **Functions** list on the left
– drag it in the area on the right
– double click on an item to configure its parameters

The following logic elements are available:

▼ **Generator**

Event controlling the logical function.

Settable parameters: Output function, Mode, Timer, Parameter, Area N.

The parameters actually available depend on the selected event.

⚠ *A generator to which the "Manual control" function is assigned must be connected to at least one "Output" element.*

▼ **Input**

Zone affected by the function.

▼ **Output**

Output affected by the function.

▼ **Vault output**

Vault whose inputs or outputs you want to control.

The "Suspend connection event temporarily disconnects the control unit from the vault, which is necessary to let the vault's configurator software connect to the vault.

▼ **AND**

“AND” logical element: its output activates when all its used inputs are active.

▼ **OR**

“OR” logical element: its output activates when at least one of its used inputs is active.

▼ **XOR**

“XOR” logical element: its output activates when an odd number of its used inputs is active.

▼ **NOT**

"NOT" logical element: its output is the negation of the input.

▼ **Counter**

Each time the counting input "C" switches from 0 to 1, the counting value increases by 1.

Once the value set in "Counter" has been reached, the output activates and remains active until the "Autoreset time" expires.

If the reset input "R" switches from 0 to 1, the counter is reset and the output is disabled.

If Autoreset time is set to 0, the output does not deactivate by itself but only upon a transition of input "R".

If "Input reset to status" is flagged, the transitions of input "C" are not accepted as long as input "R" is active.

▼ **Up-Down Counter**

Each time the counting input "C" switches from 0 to 1, the counting value increases by 1.

Once the value set in "Activation counter" has been reached, the output activates.
Conversely, each time the decrease input "D" switches from 0 to 1, the counting value decreases by 1.
Once the value set in "Deactivation threshold" has been reached, the output deactivates.
Note: the value "Deactivation threshold" is expressed as a percentage of the counting value "Activation counter".
If the reset input "R" switches from 0 to 1, the counter is reset and the output is disabled.
If "Input reset to status" is flagged, the transitions of input "C" are not accepted as long as input "R" is active.

▼ **Delay**

Delay element: it introduces a delay in the event elaboration.
When start input "S" switches from 0 to 1, a timer equal to "Waiting time" is started: when the set time expires, the output activates and remains active for a time equal to "Minimum output pulse time".
Once the "Minimum output pulse time" has expired, if input "S" is set to 0 the output deactivates; if input "S" is set to 1 the output follows the status of input "S" (active until input "S" switches to 0).
Other transitions of input "S" will recharge the time.
If the reset input "R" switches from 0 to 1, the time is stopped and the output is disabled.
If Minimum output pulse time is set to 0, it will be ignored: the output will follow the status of input "S" until input "R" switches from 0 to 1, then it will be deactivated.
If "Input reset to status" is flagged, the transitions of input "S" are not accepted as long as input "R" is active.

▼ **Timer**

Timer element: it starts a timer.
If "Confirmation time" has been set to 0, the transition of input "S" from 0 to 1 activates the output immediately.
If "Confirmation time" has been set to a value higher than 0, input "S" must remain equal to 1 for this time before the output activates.
In any case, the output activates for a time equal to the "Activation time".
If "Retriggerable activation time" is flagged, other transitions of input "S" from 0 to 1will extend the activation time.
If "Active rest state" is flagged, the output will be set to 1 when idle, 0 during activation time.
When input "R" switches from 0 to 1, the timer is reset and its output goes back to idle status.
If "Input reset to status" is flagged, the transitions of input "S" are not accepted as long as input "R" is active.

▼ **Flip-Flop**

When input "S" ("Set") switches from 0 to 1, the outputs activates.
When input "R" ("Reset") switches from 0 to 1, the outputs deactivates.
When input "T" ("Toggle") switches from 0 to 1, the outputs changes its status.
If "Input reset to status" is flagged, the transitions of inputs "T" and "S" are not accepted as long as input "R" is active.

▼ **Output node / Entry node**

They allow carrying a signal from one schema to another one or simplifying the connections on the schema.
An output node is connected to one or more input nodes.

▼ **Tools > Notes**

It allows to add notes that will be saved in the configuration.
Drag the note in the schema and double click on it.
Enter the desired text.
To increase or decrease font dimension, click on  .
Once done, press OK.

To connect elements:
– click on the triangle at the right side of the "start" element
– wire the arrow to one of the triangles at the left side of the "destination" element

Keep in mind the following rules:
1. all the logical signals must start from a generator;
2. all the logical elaborations must lead to an output or input.

The software constantly checks the correctness of the drawn schema. At the bottom left some notifications are shown (missing connections, multiple ooutputs etc.): click on the icon  to display them.
A tool is available to check a schema just drawn is properly operating: see paragraph 7.1.1 *p. 20*.
Once a schema has been completed, click on **Save scheme**.
Save the file to the desired path.
It will be possible to open it later using **Open scheme** button.
To delete all the elements added to the schema, click on **Clean up scheme**.

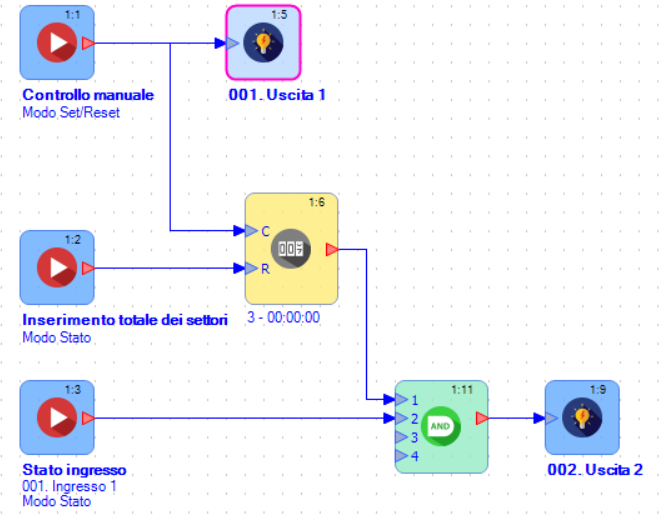
Example

One wants to activate two outputs under these conditions:

- output 1 must be activated at each manual interaction of the user;
- output 2 must be activated after 3 manual interactions of the user if zone 1 is active.

The user interaction can be implemented setting a generator with function "Manual control" and mode "Set/Reset".
"Manual control" generator is directly connected to output 1, that follows its status.
Interaction count can be implemented connecting the "Manual control" generator to a counter element with count value 3 and autoreset time 0. The count is reset at sector total arming.
An AND logical element allows activating output 2 if these conditions are both valid:

- 3 manual interactions have occurred;
- zone 1 is active.



⚠ *Signal acquisition times and control unit serial output update times depend from the devices' polling time, visible in the* **Status** > **Statistics 485** *page of BrowserOne if the control unit has firmware 1.3.10 or higher.*

7.1.1 Simulation mode

Click on **Start simulation** button to start the simulation.

⚠ *To start the simulation, the control unit must be connected to BrowserOne.*

It is possible to simulate the variation of the signal generated by any generator:

– right click on a generator
– for generators with RT or NRT mode, select **Activate**
– for generators with Status mode, select **Activate** or **Deactivate**
– for generators with Switching mode, select **Switch**

The  icon will appear to indicate the generator is being controlled manually.

⚠ *Until a generator is controlled manually, it will not be sensitive to external signals.*

The branches corresponding to the ongoing events will be highlighted in red.
to suspend the manual control of a generator:

– right click on a generator
– select **Release control**

Click on button **Stop simulation** to stop the simulation.

7.1.2 Protection

You can protect any number of schemas with a password.
A single password will be used for all protected schemas.
To set or modify the password protection:

- click on **Protection...** > **Add/edit password...** to set the password used to view the protected schemes;
- click on **Protection...** > **Delete security password** to delete the exisiting password;
- Click on **Protection...** > **Protect selected schema / Unprotect selected schema** to add or remove the protection from the currently visible scheme.

Protected schemas are identified by a closed lock icon.
If at least one schema is protected, opening the editor will prompt you to enter the password.
To continue without entering the password, press **Cancel**.
The **Protection...** button and the content of protected schemes are only visible if the right password has been used.

8 USERS

Page to configure users parameters.
SUPERIA control units support up to 2040 users.
To modify a single user's parameters:
– select the grid row corresponding to the user;
– set options in below tabs and/or grid columns.
The following sections will describe single tabs of users page.

8.1 General

Tab containing general properties of users.

▼ **User Name**
Define a name for the user selected.

User Code

Each user is assigned a 6-digits code to use, for example, to enter keypad menu.

▼ **Change User Code**
Click to modify this user's code.
Enter the code twice for confirmation.
It is not possible to enter a code that already exists for a different user or a code which last digit is 1 or 2 units bigger or smaller than the last digit of an already registered code (example: if the code 111111 already exists, then codes 111112, 111113, 111110 and 111119 will not be valid.)

▼ **Delete User Code**
Click to delete this user's code.

▼ **Enable code (...) control function**
Select to enable this user to use his code to enter user menu on keypad and for SMS remote control.
A user code not yet registered or a proximity key/remote control not yet learnt cannot be enabled (controls will be disabled).

Proxy Key Code

This pane allows checking if a proximity key associated to a user has been learnt.
If the key has been learnt, the message "Proxi key learned will appear", otherwise the message "Not Learned" will be displayed.
In installer menu, use LEARN PROXI R.C. (see paragraph 22 *p. 64*) to learn the key from keypad.

▼ **Enable Self-Learned Code**
Select to enable the code of a proximity key already learnt.

▼ **Delete Learned Code**
Click to delete a learnt code.

▼
Click to configure the card to be used to arm and disarm the system through MDARM.
A window will open: enter the card code and its PIN (if required); choose the protocol (Wiegand 26 or Wiegand 34).
Once done, press OK.
The user will be able to use the card to arm through MDARM the sectors set on page **Users**.

Card Code

Use this pane to manage the code of the card possibly given to the user for functions concerning access control.
– key in user code in the first field
– click on **Insert code** to associate the code to the user
In column **Code type**, "Card code" will appear.

▼ **Enable code**
Select to enable the code.

▼ **Delete code**
Click to delete a no more necessary card code.

User Options

- **Basic Maintenance**
  If selected, the user can access user menu on keypad.
- **No SMS/Voice for Arming/Disarming**
  If selected, no SMS/phone communications will be generated in case of arming/disarming commands.
  Digital communications will work anyway.
- **Enable user authorization management**
  If selected, users will be able to manage their own authorizations and those of other users: MANAGE USERS menu will be available on keypad to change users authorizations.
  See chapter 21 *p. 60*.
- **Deny arming authorization***
  If selected, users cannot arm the system.
- **Deny disarming authorization***
  If selected, users cannot disarm the system.
- **Enable Max security**
  If selected, users can use Max Security operations.
  If the unit is armed/disarmed in Max Security mode, only a user with Max Security property will be able to disarm/arm it.
  For further information on Maximum Security see chapter 23 *p. 69*.
- **Access-enabled user**
  Select to enable the user to gate zone control.
- **Temporary zones bypass**
  If selected, zones that have been excluded by the user will remain excluded only for the duration of an arming cycle.
  At the end, the exclusion will be automatically undone.
- **Euro Mode**
  Flag to enable the user to disarm single sectors using the keypad.
  The user will have the chance to select which sectors to disarm, with no need to disarm all its allowed sectors at the same time.

* Arming and disarming can also be denied simultaneously.

Radio zones associated to user

This pane shows the list of the remote controls associated to the user.
To learn remote controls use LEARN RADIO DET. installer menu item on keypad (see chapter 22 *p. 64*).

Authorization level

Select an authorisation level for the selected user, from 0 (min) to 20 (max).
This user will be able to control the zones and the outputs with a level equal to or lower than its own level, listed below.
The authorisation level can be set separately for each zone and each output from pages **Zones** > **General** and **Output** respectively.

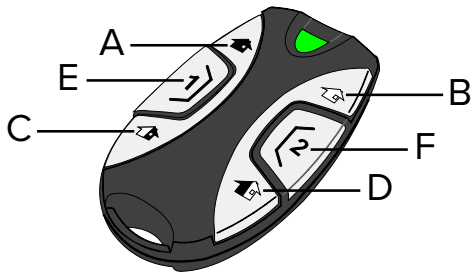
8.2 Sectors Authorised/Proposed

Use this tab to assign authorised and proposed sectors to users for each area.
Authorised sectors: sectors that can be operated by users. If a sector is not among authorised ones, users cannot arm/disarm it.
Proposed sectors: sectors that, during pre-arming time, are proposed to users for arming.
Select sectors inside columns. Each column controls one specific area.

- **Delete the sectors of not active users**
  Click to delete the sectors associated to a no longer active user.
- **Select All**
  Click to associate all available sectors to the user as both authorised and proposed.
- **Set as guard round user**
  Click to enable the user to make guard tours.
  See chapter 17 *p. 53* for further information.

Arming and disarming commands can be sent from keypad and remote controls, besides moving an electronic key to a

proximity key reader.



A Total arming
B Total disarming
C Partial arming 1
D Partial arming 2
E Central key 1
F Central key 2

8.2.1 Panic function on remote control

Press simultaneously “Partial arming 1” and “Partial arming 2” buttons to send a Panic alarm with activation of sirens or diallers
For the siren to activate upon panic alarm:
– go to page **System Options** > **Siren and Buzzer Options**
– flag **Panic Alarm to General Alarm Relay**
For the dialler to activate upon panic alarm:
– go to page **Telephone Dialler**, tab **Voice/Digital Dialler**
– select "Panic alarm" event on the grid
– in column **Associated Message**, select the message to send
– in column **Voice Phone Numbers Activation**, select the numbers to call

8.3 Remote control action (buttons 1 and 2)

Central buttons 1 and 2 of a remote control can be used to control two outputs (to which function "Keypads key 1" or "Keypads key 2" have been associated: see chapter 7 *p. 17*), or to arm/disarm sectors.
This tab allows associating arming/disarming commands of some sectors to central buttons 1 and 2.

⚠ *In this mode, these buttons cannot be used to control outputs 1 and 2.*

In column **Button 1 action** (for button 1) or **Button 2 action** (for button 2) select **Arm** (to use the button to arm sectors) or **Disarm** (to use the button to disarm sectors).
In other columns, select area sectors desired.
Example, to use button 1 to arm sectors 3 and 4 of area 2:
– select **Arm** in column **Button 1 action**
– in column **Sectors button 1 area 2**, select 3 and 4

8.4 Remote control action (buttons partial)

This tab allows associating arming/disarming commands of some sectors to remote control buttons “Partial arming 1” and “Partial arming 2”.
In column **Button partial 1 action** (for "Partial arming 1" button) or **Button partial 2 action** (for "Partial arming 2" button) select **Arm** (to use the button to arm sectors) or **Disarm** (to use the button to disarm sectors).
In other columns, select area sectors desired.
Example, to use partial arming 1 button to arm sectors 3 and 4 of area 2:
– select **Arm** in column **Button partial 1 action**
– in column **Sectors button partial 1 Area 2**, select 3 and 4.
If this tab is not used, by default partial arming 1 button arms sectors proposed, and partial arming 2 button arms sectors authorised but not the proposed ones.

8.5 Radio devices NG-TRX

Use this tab to set the parameters of a NG-TRX remote control.
It is possible to read information on remote control model and version from the columns.

▼ **Buzzer activation**

Select the activation condition of the remote control built-in buzzer: total mode, for error signals only, disabled.

▼ **Tx Boost**

Select it to increase radio section range.

The activation of Tx Boost option diminishes batteries life: we recommend the use of Tx Boost option only if the range is really poor.

Avoid activating it and then reducing remote control range.

9 TELEPHONE DIALLER

Page to configure telephone dialler parameters.
The phone dialler allows sending alarm communications: when an alarm is triggered, the dialler starts calling the numbers saved by the users (one at a time), and transmits a pre-recorded message.
The following sections will describe single tabs of users page.

9.1 General

First select to enable the 4G module.
The options below and those included in the next tabs will activate as a consequence.

▼
Select to enable data connection.
Set the options on below panel.

GSM/LTE Dialler Options

▼
Select if the GPRS connection to the selected provider is unavailable.
Function useful near country borders.

▼ **APN for GPRS internet access**
Enter the name of the network access point (according to SIM provider).
Most common italian APNs:
- Vodafone: mobile.vodafone.it
- TIM: ibox.tim.it
- Wind: internet.wind

Using a wrong APN address might cause unwanted high costs.

▼ **No GSM/LTE Registration Delay**
Set a time interval (1 to 15 min) after which the event "No GSM registration" will be triggered and the "GSM anomaly" condition set.
Communications will be attempted even if in anomaly condition.
In case of no GSM registration, calls are placed on hold until the registration is available again or until the delay time expires.

▼ **Max Number of SMS/Voice Events per Day**
Maximum number of voice/SMS event sent per day.
All messages will be counted, without distinction.

▼ **Radio access technology for 4G module**
Select the mobile network access technology for the 4G module (if installed).
Several options are available, single (4G only / 3G only / 2G only) or combined.

Notification options

▼ **No SMS/Voice for (...) control point**
If selected, the dialler will not activate in case of arming/disarming of the control unit from a Key Zone.
Useful in case of frequent unit arming/disarming.

▼ **No SMS/Voice for (...) Fast Arming**
If selected, the dialler will not activate in case of fast arming.

▼ **No SMS/Voice for (...) programmer**
If selected, the dialler will not activate in case of automatic arming/disarming from the weekly programmer.
Function available also on page **Weekly prog.** (see paragraph 14.1 *p. 47*).

▼ **Number of dialer (...) Relay+ event**
Max number of dialler activations for each "General Alarm Relay+" event.
Function useful in case of repeated alarm events while the General Alarm Relay+ is active.
As a standard, the dialler activates when the General Alarm Relay+ activates, and until the relay resets other alarms will not generate further events or dialler activations.
By setting a number of dialler activations higher than 1, further alarms from General Alarm Relay+ will activate the dialler (until they reach the number set).

The number of dialler activations for the tamper relay is fixed to 1: if the tamper event is repeated to the general alarm relay, the dialler will activate only once even when a higher number is set in this field.

9.2 Voice/digital

To activate dialler voice/digital functions select **Activate Voice Dialler** / **Activate Digital Dialler**.
Below pane **Voice Dialler Options** / **Digital Dialler Options** will be active.
The dialler activates when an event set to activate it occurs.
If the dialler is busy, events will be left in queue waiting to be processed when the dialler is available again.
Different types of communications will be managed with different priority by the dialler.
"Assault" and "Remote listening call back" events have the maximum priority.

Voice Dialler Options

Once the voice dialler has been activated, up to 32 phone numbers can be associated to an event (set in tab **User Telephone Number List**, see paragraph 9.5 *p. 28*).
– select the grid row corresponding to the event
– select phone numbers to activate checking the relevant boxes in **Voice Phone Numbers Activation**
The dialler calls set numbers in progressive order, from 1 to 32.
Options that can be configured in this pane:

▼ **Activate Common Message (Message 1)**
Select it to add message 1 after the message associated to the event.
Useful because some information that would need to be repeated in every recording (e.g. the address of the protected building) can be recorded only once this way.

▼ **Priority voice calls over digital calls**
Select it to give priority to voice calls delivery over digital calls to security companies.

▼ **Voice Call Duration**
Message duration (max 1 min 30 s).

▼ **Voice Call Repetitions**
Number of call repetitions.

▼ **Associated Message**
It associates a message to the selected row.
The message can be a predefined message or a recorded message.
Four messages are predefined and cannot be modified: "Warning alarm", "Warning tamper", "Warning anomaly", "Warning".
Each event will generate one of the 4 predefined messages.
Example:
- events "Medical alarm" and "Intrusion alarm area 1" will generate "Warning alarm";
- events "Tamper alarm area #" will generate "Warning tamper";
- events "230V Power failure" and "Commmunication failed" will generate "Warning anomaly";
- event "Technological #" will generate "Warning".

Digital Dialler Options

Select row corresponding to the event in the grid above.
Options that can be configured in this pane:

▼ **Priority SMS over Digital Protocol**
Select it to give priority to SMS messages delivery over digital calls.

▼ **Activate Double Digital Notification**
Select it to send a digital event notification both to the primary and the secondary number.

▼ **Primary/Secondary ID Code, Primary/Secondary Number**
When the alarm system is managed by one or more alarm centralization service(s), enter its/their primary/secondary numbers (20 digits) in these fields.
Enter primary/secondary ID codes (6 digits) for users identification.

▼ **Digital Protocol**
Select communication protocol: Fast Format DTMF, ContactID (Dec), ContactID (Hex).
Type and **Channel** fields vary according to the protocol selected.

▼ **Type**

Enter decimal values 1 to 9 (0 value deletes type and channel).

▼ **Channel**

Enter digital report code (hexadecimal value).

Type has to be defined first.

Note: codes list for Ademco Contact ID protocol can be found at control unit page on www.elmospa.com website (registration required).

9.3 SMS

Use this tab to set the parameters of SMS sending via the MD4GE optional module.

SMS Options

Select **Activate SMS Transmission Upon Event** to activate this pane.

Once the voice dialler has been activated, up to 32 phone numbers can be associated to an event (set in tab User Telephone Number List, see paragraph 9.5 *p. 28*).

– select the grid row corresponding to the event

– select phone numbers to activate checking the relevant boxes in **SMS Phone Numbers Activation**

▼ **SMS Heading**

Set the heading (i.e. the first part) of each SMS message. The forwarded SMS messages have a heading too.

The heading can be left blank.

It cannot begin with "C.": any "C." will be replaced by "*.".

Some special symbols can be used (select the row below the field to open a new window).

▼ **SMS Repetitions**

Set the number of SMS messages to be sent for each event.

▼ **Priority SMS over Digital Protocol**

See similar function in pane **Digital Dialler Options** (paragraph 9.2 *p. 27*).

▼ **Associated SMS**

Select SMS to send, "Auto-Composed" or one of the 64 editable messages.

User Numbers for SMS Forwarding

The 4G module can receive SMS texts different from control unit messages (e.g. SMS sent by mobile service providers).

Such "forwarding messages" can be forwarded to **User Numbers for SMS Forwarding**.

Select such numbers checking the corresponding boxes (up to 32).

The control unit can forward up to 5 SMS messages per day to each phone number.

Further SMS texts received will be ignored.

9.4 SMS text

Create the body of customized SMS texts (max 64 characters each) in the grid rows.

It is possible to use special symbols: when SMS are sent by the unit, symbols will be replaced with info on the current status of unit, therefore info that cannot be set initially (ex. armed sectors, temperature, etc.).

Example: heading is

Clarks Home /A1

the SMS sent by the user for mains failure could be the following:

Clarks Home DISARMED: Mains Failure PANEL

On page bottom, an estimate of the available space for customised SMS messages is reported.

9.5 User telephone number list

Enter in column **User Telephone Number** the numbers to be used for control unit communications.

Allowed digits are: all figures, symbols # and * , and the P character to insert a 1 second pause.

Up to 32 phone numbers containing each 20 figures can be configured.

To assign a name to phone numbers, enter it in column **Name Assigned to the Phone Number**.

After having received and listened to a call users can stop the call and press on phone keypad:

5: to stop the current call; the unit calls the following number.

0: to stop the current call; the unit does not make other calls until the next event occurs.

9.6 SIA DC-09

The dialler can transmit events via IP according to the SIA IP Reporting (TCP-2007) standard using the supported ADM-CID protocol.
Use this tab to set communication parameters.
To activate SIA DC-09 dialler select .
The panels below will be enabled.

▼ **Double Notification**
If flagged, messages will be sent to both servers.

▼ **Uses a "link-test" packet instead of the "periodic call" event**
If checked, the contol unit will use the proper SIA DC-09 connection health check.
If not checked, the control unit will instead send "periodic call" events, which are saved in the events log.

Primary Server

Use this pane to set the parameters of the primary server that will receive the event notifications.

▼ **IP Address**
Set the IP address of the primary server.

▼ **TCP port**
Set the TCP port of the primary server.

▼ **Encryption key**
Set an hexadecimal password to protect the messages.
The field is enabled only if the **Enable Encrypted Transmission on Primary** is flagged in the **General Options** side pane.

▼ **Account Number**
Device identification number.

▼ **Digital Protocol**
Select the protocol format (decimal/hexadecimal) from the drop-down menu.

▼
Flag this checkbox to protect the event messages with a password.
Set the password in the**Encryption key** field located in the **Primary Server** (Secondary) pane.

▼
If flagged, the control unit event sending date and time will be sent to the server in case unencrypted messages are used.
Such time can be later than the actual time the event occurred at (e.g. in case of temporary control unit disconnection).

▼
If flagged, the precise event occurrency date and time will be sent to the server.

▼
If flagged, additional information (zone and area names) will be sent to the server.

Note: if the GPRS connection is used and e-Connect is using this connection mode too, a failure of the connection to the server may imply a temporary disconnection from the e-Connect service.

Secondary Server /

You can also use a second backup server: use this panes to set the parameters and options of the secondary server.
The parameters are the same as the primary server ones.

10 OPTIONS

Page to configure system options parameters.
The following sections will describe single tabs of users page.

10.1 General

Installer Code

Default installer code **88888888**.
Select **Modify** to change it.
The code can be modified also from one of the keypads connected to the unit.

Enable secondary installer code

Flag to enable a secondary installer to access the control unit both via keypad and via BrowserOne.
To enable or disable the secondary installer:
– enter primary installer code
– press Ok
The secondary installer will be able to access the control unit with his own code (default: 00000000). To change the code:
– click on “Modify" key
– enter the new secondary installer code twice
– press Ok to confirm
If a secondary installer is disabled and, later, enabled again, he will be given the last used code.
Note: the secondary installer is not allowed to change primary installer's code.

⚠ *Attention: user authorisation is always required to enable primary and secondary installers to programming functions.*

Enable tertiary installer code

Similar function to enable a third installer code.

General Options

⚠ *Some of the functions listed below are only available if the PRXGDO key or the ETRVARCO module are being used.*

▼ **Welcome Message**
Insert the welcome message that will appear on the display of connected keypads.

▼ **Programmable Relay Settings 1, Programmable Relay Settings 2**
The unit features two relays with terminal outputs.
Set here the relay activation functions.
General Alarm Relay, Tamper Relay: the relay repeats the corresponding relay (alarm/tamper), and activates for the time set (positive safety logic).
Max Temperature, Min Temperature: the relay activates when the maximum/minimum threshold is reached.
Monitor program: the relay will be used as logic output in the programmable logic output functions and will follow its status.
Out 1 / 2 / 127 / 128 Follow On: the relay replicates the status of the set output.

▼ **Output Monitor (P+) Settings**
Output P+ can be used to signal control unit proper operation (default: Output Monitor (P+) Settings).
If this signalling is not requried, it is possible to change the output activation event: configure the output using the drop-down menu.
The available options are the same as the ones available for programmable relays 1 and 2.

▼ **Direct Connection Address**
Set the address for unit connection to network over RS485 serial line.

▼ **Sectors per area mode**
Select the number of sectors per area.
Total number of sectors will always be 64, however they partition may vary as follows:
4 sectors: 16 areas with 4 sectors each;

8 sectors: 8 areas with 8 sectors each;
16 sectors: 4 areas with 16 sectors each;
32 sectors: 2 areas with 32 sectors each;
64 sectors: 1 area with 64 sectors.

▼ **Lock Dialler at Disarming Event**
If selected, dialler voice/digital transmissions to arm/disarm sectors/areas pertaining to the user will be blocked.

▼ **Reverse output monitor, Reverse Programmable Relay 1, Reverse Programmable Relay 2**
Select to reverse the operating logic of output P+ or of the programmable relay.

▼ **RF Interference as Tamper**
If selected, the control unit generates a tamper event if the interference (reception of signals from non-memorized codes) lasts longer than 1 minute on the frequency used by Villeggio and Helios protocols.

Note: for NG-TRX system radio devices, see **Enable detection RF interference** (paragraph 10.8 *p. 39*).

▼ **Deactivate keypads tamper**
Select it to disable all keypad tamper events communications.

▼ **Silence Keypads during Exit Time**
If selected, it silences the buzzer of the built-in keypad during the exit time.

▼ **Disable phone numbers editing from keypad**
If selected, users cannot modify programmed phone numbers from keypad.
The function affects only users and not the installer.

▼ **Reset Periodic Call Time after a Digital Call**
If selected, the periodic call timer will be reset after each digital call.

▼ **Input alarm excluded on red LED of alarm**
If selected, the red LED lights up when an excluded device generates an alarm.
If deselected, the alarm event will only be logged since the device is excluded.

▼ **Display inputs on alarm during keypad inactivity**
If it is flagged, the names of the zones in alarm state will be shown on the keypad display when the keypad is idle.
The names will be shown cyclically one after another.
The area name or the welcome message will be also shown.
This function only applies to the first 8 control devices.
This function has no effect if **Visualization Protection** is active.

▼ **Zone tamper 24h NC**
If selected, the terminal zone of the tamper line will be set to NC (instead of 1500 Ω single balanced).

Note: we advise against activation.

▼ **Enable fast arming**
If selected, users will be able to arm a sector without entering their user code on keypad.

To perform fast arming:
– press a sector key: the unit requires confirmation for fast arming
– press OK within 5 seconds (beyond this time the procedure is cancelled)
Press a different sector button to change the sector you want to arm.
Only disarmed sectors that are not being armed can be armed this way, provided they are associated to at least one user.

▼ **"Fast arming/output maneuver" pressing (...)**
If selected, users can use the fast arming by pressing the sector button twice.

▼ **Alarm generation on status for fast inputs**
This function can be used when one wants to wire fast zones (rolling shutter contacts) in series with magnetic contacts.
Flag this function to properly manage alarm generation in such configuration.

▼ **Zones autoexclusion on yellow anomaly LED**
If selected, the yellow LED will light on when an excluded device enters anomaly condition.

▼ **Single Chime**
If selected, the control unit emits a single acoustic signal whenever a zone with "**Chime**" property (pane **Zone Options**, see paragraph 5.1 *p. 9*) passes from idle to alarm condition.

▼ **Simplified codes mode**
If not selected, user number will be required before user/installer code in order to enter user/installer menu.
If selected, only user/installer code will be required to enter user/installer keypad menu.

▼ **Disable green LED blinking (...) not intrusion alarm**

If selected, the green LED blinking will be disabled when zones non programmed as “intrusion zones” (ex. key points) enter alarm condition.

▼ **Cancel auto-bypass at zone reset**

If selected, the exclusion of a bypassed zone (with **Auto-Bypass** function on pane **Zone Options**, see paragraph 5.1 *p. 9*) in idle mode for 5 secs will be cancelled.

▼ **Reverse Area Arm/Disarm Logic**

Select to reverse the logic for area arm/disarm communication sending (digital, voice/SMS).

Standard logic: an area arming communication will be sent after arming of sectors if no sectors are initially armed; vice versa, an area disarming communication will be sent after disarming sectors, resulting in no sectors armed.

Reversed logic: an area arming communication is sent after arming sectors only if all sectors will be armed; an area disarming communication will be sent after disarming sectors if all sectors are initially armed.

▼ **Send all sectors arm/disarm events**

If selected, area arming/disarming communications will be sent at every arming/disarming, even for partial ones.

▼ **Repeat tamper alarm to general alarm relay**

If selected, a single output relay will be used for signalling general and tamper alarms.

Function useful to control optical-acoustic devices with a single relay.

▼ **Show passage status on I8/I9/Passlight**

If selected, the status of the gate zones associated to I8/Passlight devices will be displayed on them.

▼ **Disable max security after alarm**

If selected, a control unit armed in Maximum Security can be disarmed by a user without Maximum Security property only once and only within a defined time after an alarm.

This time can be programmed in field **Enable disarming with active max security after an alarm event** (see paragraph 10.3 *p. 35*).

▼ **Enable force arming zones**

If selected, the users equipped with "basic maintenance" property can arm the system even in case there are zones in persistent anomaly status. Such zones will be temporarily excluded during arming.

In case of tampered zones, the system cannot be armed.

▼ **Key zone even-arming/odd-disarming**

If not selected: at each alarm of a key zone, the armed pertaining sectors will be disarmed and vice-versa (standard).

If selected, the even zones generate only arming, the odd zones only disarming.

▼ **Enable compression on 485 protocol**

If selected, it improves ULTRABUS RS-485 serial line performances of the devices compatible with this mode.

▼ **Enable disarming/arming with door user**

If selected, a "passage" user will be allowed to perform arming and disarming operations with keypads and IZENITH.

To arm, keep the proximity key leaning on the reader for the duration of three acoustic signals.

EN50131 Options

▼ **Access Attempts Exceeded (...) Tamper Alarm**

If selected, the tamper relay will activate when the maximum number of attempts is exceeded.

If using wireless remote controls to arm/disarm the system, enable also their antiscramble function.

▼ **Activate general alarm/siren only (...) armed**

If selected, the general alarm relay and all sirens (integrated or external) will not activate if the system is disarmed.

However, the sirens will still activate for fire, gas or flood alarms.

▼ **Enable keypad locking for error code**

If selected, a keypad is locked for 90 seconds after entering three wrong codes consecutively.

The keypad remains locked until a valid code is entered.

If deselected, after 21 wrong codes are entered, the "Access attempts exceeded" event will be generated and displayed on keypad; in addition, if the function **Access Attempts Exceeded (...) Tamper Alarm** is enabled, the tamper event will be generated at the 7th wrong code.

▼ **Activate Arming Lock**

If selected, the following conditions prevent the system from being armed:

- simultaneous fault of phone dialler and sirens

⚠ *in such case, arming can be forced*

- lack of supervision for a radio device on a RIVERRF concentrator

⚠ *arming is refused only if the device really lacks supervision: supervision failure memories will be ignored*

- at the end of the exit time, a zone in the exit path is in alarm

⚠ *in such case, a failed arming event will be generated; arming can be tried again after having reset/excluded alarmed sensors*

Arming lock is also activated in event of:

- zone fault;
- fault occurrence within exit time;
- remote control low battery.

In case of arming lock, you can arm the system anyway by double-pressing the key.

▼ **Required authorization of the installer for (...)**

If selected, the unit complies with EN 50131 grade 3 standard.

It can be activated only if **Activate Arming Lock** function is selected.

▼ **Visualization Protection**

Select this option to activate the following visualization protections:

- LEDs indicating arming status (green), anomaly (yellow), alarm/tamper memory (red) are off when the system is armed.
- Icons area on LCD does not display information when the system is armed.
- Events do not generate messages on the display.
- To access the status visualization menu, one has to enter the user/installer code, then press arrow keys.

▼ **Dialer delay on pre-alarm**

Select it for the following effects:

- if, during the entry time, an intrusion alarm is generated by an instant zone with at least one sector in common with the areas included in the entry time, the dialler does not signal the alarm until one of the following conditions occur: the siren has been active for at least 30 s, or the entry time ends.
- dialler activations caused by a pre-alarm timer time out signal are not delayed.
- if, after the entry time has ended, an intrusion alarm is triggered by an instant zone, the dialler activation is immediate and the delay for all signallings with sectors in common with that instant zone is cancelled;
- all delayed alerts from sectors involved in a disarming command or in a system access will be cancelled.

▼ **Limit Log FIle Events**

Select it to limit to 10 the number of events logged for each arming/disarming cycle for each event source (zones, diallers, power supply unit, etc.).

Each source has a separate event counter. Once the limit is reached, events will be managed normally but are no longer logged.

▼ **Erasing memories (...) only by the installer**

Select it to authorize the installer only for tamper/fault memories cancellation.

▼ **Zone exclusion only from installer**

Select it to authorize the installer only for zones exclusion.

▼ **Hide arming state**

Select it to hide the arming status of the control unit by disabling LED indicators of connected keypads/readers.

▼ **Enable arm warning by time programmer**

If flagged, the keypads will emit beep tones one minute before weekly programmer activation.

Date and time

The following functions allow to set control panel date and time and their updates.

▼ **Time zone**

Choose the time zone from drop-down menu.

▼ **Enable manual time update**

Flag to allow control unit time manual update.

If flagged, it will be possible to set the time manually from **Actions** > **Clock** menu or from **CLOCK SETUP** keypad menu.

▼ **Enable clock update from...**

Choose, as an alternative to the manual update, which time to take as reference for time update (access controller, CEIABI supervisor, e-Connect, NTP).

In case of update from NTP, set the urls of the reference servers (default: google services).

Power Saving

The following options allow power saving.

▼ **Yellow LED OFF when there are no anomalies**

Select it to disable the yellow LED when there are no anomalies.

Valid also for readers connected to the keypad.

▼ **Sectors Keys OFF when inactive**

Select it to disable the backlight of sector buttons in case of inactivity.

▼ **Reader arming LED OFF when inactive**

Select it to disable the LED of the reader connected to the unit in case of inactivity.

Geolocation

▼ **Plant Latitude/Longitude**

Filling this field is necessary to be able to use the sunrise and sunset times of the correct geographical position in the logic elaborations editor.

Enter the GPS coordinates of the system.

In order to enter the correct values we suggest you to open Google Maps, right click on the geographical position of the installed system and click the coordinates shown in the right-click menu; this will copy the coordinates, paste them in the field.

10.2 Sector buttons

This tab allows associating sectors to keypad sector keys when one of the following modes have been selected: 8, 16, 32 or 64 sectors per area.
In 4 sectors per area mode, each key is associated to a sector in a univocal way, therefore the configuration cannot be modified.
Select sectors to be associated checking the corresponding boxes.
For example, in 8 sectors per area mode the configuration of area 1 sectors in the following image

	Tasti settore	Settori area 1
▶	Tasto settore 1	1 2 _ _ _ _ _ _
	Tasto settore 2	_ _ 3 4 _ _ _ _
	Tasto settore 3	_ _ _ _ 5 6 _ _
	Tasto settore 4	_ _ _ _ _ _ 7 8

indicates that sectors 1 and 2 are associated to sector key 1, sectors 3 and 4 are associated to sector key 2, sectors 5 and 6 to sector key 3, and sectors 7 and 8 to sector key 4.

10.2.1 Sector keys in 8/16/32/64 sectors per area mode

Information in this paragraph only applies to usage with standard keypads.
Some types of keypads (i.e. the touch screen ones) do not feature sector keys and allow to arm/disarm single sectors through dedicated menu items.

Standard operating mode

Each sector key shows the **overall** arming status of associated sectors.

Condition	Sector key indication
All associated sectors disarmed	OFF
All associated sectors armed	Steady light
All associated sectors armed in max security	Fast blinking
At least one sector armed (but not all)	Fast blinking alternate to steady on (only steady on when visualization protection is on)
At least one sector in exit time	Slow blinking

On the display of the keypad connected to the unit, the arming status is indicated as follows:

8 sectors: Arm: 123--67-

16 sectors: Arm: 123--67-AB----G

where numbers represent armed sectors, hyphens disarmed ones.
The numbers of sectors armed in max security will blink.
Display dimensions typically allow visualisation of the first 32 sectors.

Pre-arming

Sector keys provide information on associated sectors proposed for arming:

Proposed for arming	Sector key indication
No sectors (regardless of arming status)	OFF
At least one sector, but not all	Slow blinking
All sectors	Fast blinking

Press a sector key to change sectors proposed:

At least one sector, but not all	→	All sectors
All sectors	→	No sectors proposed for arming

During pre-arming time, sectors proposed for arming can be changed (if authorised) as follows:
- in **8 sectors per area** mode: press keys 1 to 8;
- in **16/32/64 sectors per area** mode: press keys 1 to 9, *(=A), 0(= B), #(= C) corresponding to the first 12 sectors; for sectors from the 13th on, the arming proposal cannot be changed.

Sectors arming status will be displayed on keypad: numbers indicate sectors proposed for arming, hyphens sectors not proposed.
If the fast arming is enabled, when pressing one sector key, sectors in use associated to that key will be armed.

10.3 Timers

Timer

This tab provides timers for general usage.

▼ **General Alarm Relay Time**
Time interval for general alarm relay activation.

▼ **Tamper Alarm Relay Time**
Time interval for tamper alarm relay activation.

⚠ *In case of multi-area management, general alarm and tamper alarm events are seen as system events. This means that when the relay resets, all alarm conditions of all areas will be reset.*

▼ **Mains Failure Delay**
Delay interval for the mains failure alert.
0 minute value means that the alert will be immediate.

▼ **System Test Interval**

Time interval for system tests (default: 52 weeks).

See chapter 24 *p. 72* for further information.

▼ **Supervision software control timeout**

Timer to evaluate the reactivity of the supervision software.

▼ **Emergency Light Time**

Duration of backlight on for keypads connected to the unit in case of mains failure.

Once the timeout has expired, the display will blink for 30 seconds to indicate its imminent turning off.

The display of the connected keypad will be switched off anyway when the battery is discharged.

▼ **Zone AND time**

Time interval within which two zones with AND property (see AND with zone option in paragraph 5.1 *p. 9*) have to be alarmed (both) to trigger an alarm event.

▼ **Periodic Call Interval**

Time interval for the control unit to place digital test calls to the alarm centralization service.

These test calls are sent on all the set channels, regardless of the selected interval.

▼ **Reduced periodic call interval**

Time interval for the control unit to place digital test calls to the alarm centralization service.

These test calls are only sent through the SIA DC-09 protocol channels and allow reaching compliance to performance levels DP3 and DP4 according to EN50136-1.

In detail, when the periodic call interval is set to 90 seconds, the communicator is compliant to level DP4, while if the interval is set to 3 minutes the communicator is compliant with level DP3.

If the interval is set to a value ranging from 3 minutes to 30 minutes, the communicator is compliant with level DP2.

If one communication channel only has been configured, compliance decreases from DP (Dual Path) to SP (Single Path).

▼ **Double confirmation time for duress**

Time interval to be used for "Double Confirmation" function: all disarming performed by remote controls or proximity keys shall be confirmed by entering a code at keypad.

If the timeout expires and no codes have been entered, a duress alarm will be generated.

All areas feature a timer for double confirmation function; any disarming involving more areas activates all pertaining timers.

Each user can block only the timers of his own pertaining areas.

▼ **Exit delay**

Time interval for **Reduce exit delay** function (see paragraph 11.2 *p. 42*).

At arming command (from keypad, reader or remote control), the exit time will be reduced to set time.

Exit time intervals already started will not be affected.

▼ **Chime interval**

Time interval for acoustic signals associated to Chime function (see option **Chime** on paragraph 5.1 *p. 9*).

A signal will be repeated when such time interval expires.

▼ **Max opening passage**

Maximum opening time for "Passage" zones.

Once the time expires, if the zone is still open (anomaly condition) an alarm event will be triggered.

▼ **Reintegration warning time**

Time (in seconds) for automatic system re-arming after a disarming performed by a user (**Reintegration time**, see chapter 8 *p. 22*).

If automatic re-arming has been set, an acoustic notification will be emitted some time before re-arming. This time can be set here.

▼ **Enable disarming with active max security after an alarm event**

Time used by **Disable max security after alarm** function (see paragraph 10.1 *p. 30*), if enabled.

After an alarm, an user without Maximum Security property will be able to disarm the control unit armed in Maximum Security within this time.

▼ **e-Vision AI device supervision time**

Set the supervision time for the cameras that support the D-Pulse-technology AI functions.

If the supervision of a "e-Vision AI alarm" zone has been enabled (option **AI server supervision** flagged for that zone), zone supervision will take place with a period equal to the set supervision time.

The following table reports the supervision time and the "Control message interval" (settable on the devices) suggested depending on the number of D-Pulse devices in use.

N. of D-Pulse devices	Supervision time e-Vision AI devices	Control message interval
up to 60	5 min	60 s
up to 120	15 min	120 s
more than 120	45 min	240 s

10.4 Siren and Buzzer Options

Use this tab to set acoustic signals of the internal siren associated to some events.

General

- **Panic Alarm to General Alarm Relay**
  Select it to activate the general alarm relay for panic events.
  Option useful when using sirens for panic events.
- **Fire, Flood and Gas Alarms to General Alarm Relay**
  Select it to activate the general alarm relay for the listed events.
  Option useful when using sirens for such events.
  We recommend the activation of this option in addition to using the dialler, and not in its place.
- **Echo Arming/Disarming on external siren (+Rif Sir)**
  Select it to activate a wired external siren for arming (one beep) and disarming (two beeps).

10.5 Network parameters

Use this tab to set parameters of e-Connect service access and of the available connection types.
Enter in **Hostname** field the name of the control unit in the network.

Ethernet 1 / Ethernet 2

Use this sections to set the parameters of the on-board Ethernet module (1 or 2).

- **Enable DHCP**
  Select to allow the DHCP server to assign values to below fields in a dinamic way.
  Deselect to assign values manually.
  If deselected, enter all the required parameters in the fields.

e-Connect

The e-Connect service allows users to change arming settings of control units (e.g. arm/disarm sectors, enable/disable zones) and to check their status over the Internet.
It also allows installers to perform part of the configuration remotely.
To access e-Connect service, Internet connection is required through the on-board Ethernet module or using a 4G module.
For further information on how to configure the e-Connect service, see chapter 25 *p. 73*.

- **Enable connection to e-Connect**
  Select to enable access to e-Connect.
- **Default server**
  Select to keep the default server as access server.
  Recommended option.
- **Custom URL**
  Select to set a different URL from the default one.
  Enter the URL in the field.
- **IP static**
  Select to use a static IP.
  Enter the IP address in the field.
- **e-Connect server port**
  Enter server port number.

Direct connection ports

Set the communication ports for direct communication to external devices.
Enable the desired ports and set their number.
It is possible to define the maximum number of devices connected at the same time (up to 20).

Access control connection port

Set the communication ports to access control devices.
Enable the desired ports and set their number.
It is possible to define the maximum number of devices connected at the same time (up to 20).

e-Vision AI connection port

Set the connection port for the devices that support the D-Pulse-technology AI functions.

10.6 Scenarios Configuration

Use this tab to set scenarios parameters.
Scenarios are a series of actions to be automatically activated upon arming command.
It is possible to set up to 8 scenarios and a Max Security scenario.
Select the activation level fron the drop-down menu:

- sector wide: the scenario only applies to sectors affected by arming command;
- area wide: the scenario applies to all areas affected by arming command (also for sectors belonging to such areas armed later);
- panel wide: upon arming command, the scenario activates for the whole control unit (also for sectors armed later).

▼ **Show asterisk on LCD for active scenarios**

Define how the activation of a scenario is displayed.
If not selected, the keypad in use will show the name of the active scenarios alternated to armed sectors in sequence.
If selected, the control unit will indicate with an asterisk the sectors with at least one active scenario.
Example:

- system keypad: an asterisk appears before area(s) with at least one active scenario: *A1 *A2 A3 A4
- 4 sectors per area: an asterisk appears before sectors(s) with at least one active scenario: S1 *S2 *S3 *S4
- 8/16/32/64 sectors per area: an asterisk appears before sectors list if there is an active scenario before at least one of them: Area 1:*1234----

Scenario n

Enter a name for the scenario.
Each scenarios can be configured with one of the following properties (or more):

▼ **Disable zone in time**

Entry time of zones associated to groups where this scenario is active is cancelled.

▼ **Disable alarm switch (internal siren)**

The internal siren and the alarm relay do not activate because of intrusion events from sectors where the scenario is active.
Alarm relay does not activate phisically, but the "General alarm relay" event is normally generated and managed.
This property does not affect activation caused by tamper, panic or 24H events.

▼ **Disable external sirens**

External sirens do not activate in case of intrusion events from sectors where the scenario is active.
This property does not affect activation caused by tamper, panic or 24H events.

10.6.1 Arming and scenarios activation

Scenarios properties activate upon arming command that can be entered at keypad or with the weekly programmer.

Using a keypad

If arming from keypad (code + sector button), the name of the scenario is shown instead of the area name.
In case of area change, the area name is shown for about 2 seconds, then it goes back to the scenario name again.
If areas are changed with arrow keys while the scenario name is displayed: press arrow key once to see the name of the current area, press arrow key again to change the area.

The displayed information may vary according to selection of **Show asterisk on LCD for active scenarios** function.

From weekly programmer

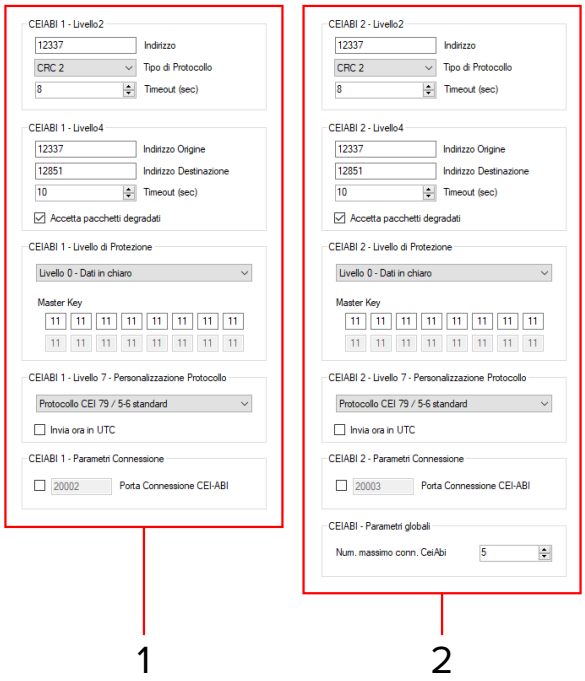
To activate a scenario with the weekly programmer, please follow below steps:

– go to page **Weekly prog.** > **Weekly programmer**
– on the above grid, select the row where to create the new program (Program #)
– select **Program enabled**
– in drop-down menu **Program function**, select "Arming scenario N" (or "Max Security arming" to activate the scenario in Max Security mode)

For further information, see paragraph 14.1 *p. 47*.
If a sector is already armed when the program is set, the scenario activates anyway.

10.7 CEI 79 / 5 - 6

Some applications require to communicate with control centers using CEI 79-5 or CEI 79-6 protocol.
Use this tab to configure connection parameters, in agreement with the alarm centralisation service provider.
Two communication channels are available and can be configured separately: the first using panes in the first column, the second using panes in the second column.



Drop-down menus allow selecting protocol protection levels (with relevant protection code) and customisation levels.
Some peculiar functions are described below.

▼ **Accept degraded packets**
Flag to allow the reception of packets also in case of uncrypted communication between the control unit and the surveillance centre.

▼ **Send time in UTC**
Select to enable the sending of the time as referred to the standard UTC time zone.

▼ **Max number CeiAbi conn.**
Set the maximum number of CeiAbi connections allowed at the same time (up to 20).

10.8 NG-TRX options

This tab allows setting some parameters for control unit - NG-TRX devices communication.

▼ **Receiving multichannel**
If active (ON), the control unit receives signals from all three NG-TRX communication channels at once.
If non active (OFF), the control unit receives signals from one channel at a time (default/preferential).
It is advisable to deactivate reception in case of disturbances over a channel.
The control unit may change channel in case of noise reception on the used channel, even when multi-channel mode is disabled.

▼ **Enable multi-channel sirens receiving**

Select to enable the sirens to receive on all three channels at once.

Options NG-TRX

▼ **Default channel**

Select a channel.

In case no interference is detected, the control unit will receive on this channel.

If there are disturbances, the control unit will switch to a preferential channel for reception (even different from default one) depending on disturbances presence.

▼ **Supervision interval**

Select the supervision interval that applies to all system devices for which a supervision interval has not been individually set.

When the time interval expires, devices will send a presence signal to the unit.

⚠ *Compliance to the EN50131 grade 1 standard requires a supervision interval of max 60 minutes; compliance to the EN50131 grade 2 standard requires a supervision interval of max 20 minutes.*

▼ **Delay supervision anomaly**

If selected, alerts for lack of supervision will be delayed for a time interval equal to six times the supervision interval.

⚠ *Compliance to the EN50131 grade 1 standard requires a supervision interval of max 10 minutes.*

▼ **Enable two-factor authentication for Remote Controls**

Select it to increase protection against remote control codes duplication attempts: two transmission will be sent for each command, thus implementing double authentication.

The activation of this option slows down the response of remote controls and increases battery consumption.

▼ **Delay low battery signaling**

If selected, peripherals will run additional controls before sending low battery alerts.

▼ **Enable detection RF interference**

Select it to enable interferences detection over 3 channels and log the corresponding event.

The control unit will automatically change the channel if the interfernce is detected and logged in the last 48 hours.

⚠ *Compliance to the EN50131-1 standard requires the activation of this function.*

▼ **RF Interference as Tamper**

If selected, interference events will generate also tamper events; such events will be managed normally.

▼ **Remote range NG-TRX**

Area to adjust NG-TRX remote controls range.

By default it is set at maximum; reduce the range in order to avoid accidentally activating the control unit from a long distance.

Do not reduce the range if **Tx Boost** option is active.

Transmissions of NG-TRX command

If there are multiple GATEWAY2K devices connected (up to 4), select which ones have to be enabled for commands transmission to other devices of the NG-TRX system.

Up to two GATEWAY2K can be enabled for command transmission.

10.9 Advanced settings GDO

This tab is available only if a key for MMR (Mass Market Retailers) function enable is being used. It allows defining the parameters of this function.
For further information see the manual of the key.

10.10 Historical events

This tab allows defining which events to log.
Check the events to be logged, uncheck the events not to be logged.

For the selected events, the event occurrence and its reset will be logged.

11 CONTROL DEVICES

Page for control device management.
Up to 64 control devices can be connected to the control unit (keypads, readers, control points).
To operate on a control device individually:
– select the corresponding row on the grid
– set options in below tabs and/or grid columns
The following sections will describe single tabs of users page.

11.1 Keypads

Control devices

▼ **Name**
Enter control device name.

▼ **Type**
Select control device type.
If you select **Advanced keyboard**, a new drop-down menu will appear.
Select the advanced keypad type from the new menu.
Click on **Open management** to open a configuration form.

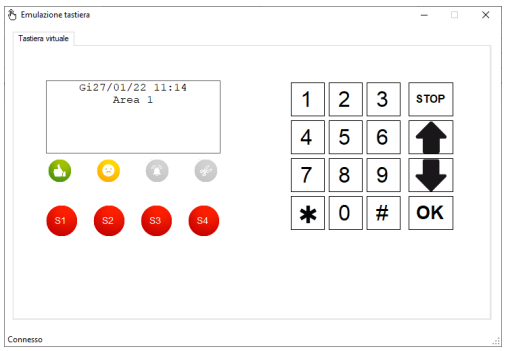
▼ **Address**
Set device address.

▼ **Area displayed (for keypads)**
Select which among the pertaining areas will be shown on keypad by default when the keypad is idle.
When idle, system keypads display system general status.

▼ **Pertaining area (for ETR Varco/I8/Passlight)**
Select the control device pertaining area.

Keypad emulation

Starting from control unit firmware version 1.0.7 and using BrowserOne 3.26.22 or above with module 1.1.4 or above, a tool for remote keypad emulation is available.
This tool allows to emulate a specific keypad phisically included in the system, in order to give the related commands from remote without actually using the keypad.
To open the tool for a specific keypad:
– select the keypad from the above grid
– on **Keypads** tab, click on **Open keypad emulation** button



The interface shows the same keys as the actual keypad and it repeats its display messages in real time.

11.2 Keypad options

Use the columns to set, for each keypad:
- any **Passage** zone connected to the keypad;
- if GDO functions are being used: a second passage zone and its maximum opening time;
- masks:

▼ **Mask authorized Sectors Area N**
Select which area N sectors to make available for arming/disarming using this keypad.

The user will be able to arm/disarm the sectors he has in common with this "mask" of sectors.

▼ **Mask proposed Sectors Area N**

Select which area N sectors to make available for arming using this keypad.

The user will be able to arm/disarm the sectors he has in common with this "mask" of sectors.

Other functions can be selected on below panel.

Insert options (control devices)

▼ **Show partial arm on sector buttons**

If selected, backlit keypad buttons will provide indications on partial arming.

▼ **Disable fast arming**

If selected, fast arming will not be allowed from this keypad/reader.

Users will have to use their codes (on a keypad) or their proximity keys (on a proximity reader) to arm sectors and areas.

▼ **Reduce exit delay**

Select it to reduce exit delay time for arming commands from this control device.

Set **Exit delay** in tab **Timer** on page **System Options** (see paragraph 10.3 *p. 35*).

▼ **Enable outputs fast activation**

Select it to enable outputs fast activation (without entering user code) from this keypad/reader.

The scenario deactivates when affected sectors are disarmed.

▼ **Enable predefined arming scenario**

If selected, default scenario (selectable from drop-down menu) will be activated when a sector is armed from this keypad/reader.

Default scenario

Select the default scenario to be activated.

11.3 Remote controls / Wireless keypads

▼ **Mask authorized Sectors**

Select which sectors are available for arming/disarming from remote controls.

The user will be able to arm/disarm the sectors he has in common with this "mask" of sectors.

▼ **Mask proposed Sectors**

Select sectors to propose for arming with remote controls “Partial arming 1” key.

The user will be able to arm/disarm the sectors he has in common with this "mask" of sectors.

▼ **Mask authorized - proposed Sectors**

Select sectors to propose for arming with remote controls “Partial arming 2” key.

The user will be able to arm/disarm the sectors he has in common with this "mask" of sectors.

Default scenario

Select the scenario to activate upon arming (only if **Enable predefined arming scenario** option is selected).

Insert options (remote controls)

These options are the same as the ones defined for keypads: see previous chapter.

11.4 SMS commands

The SMS command masks work as seen for the remote control masks described above.

12 ULTRABUS DEVICES

Page for serial devices management.
Up to 32 devices can be connected over serial line (sirens, power units, fog systems and GATEWAY2K).
To operate devices individually:
– select the corresponding row on the grid
– set options in below tabs and/or grid columns

12.1 Ultrabus devices

Set the parameters for serial line connection.

▼ **Device name**
Define a name for the device.

▼ **Type**
Select connected serial device type from drop-down menu:
- when selecting "Gateway GATEWAY2K" type, the **Read information** button appears: select it to see firmware, bootloader, NG-TRX radio module versions.
- when selecting a different device type, **Open management window** button appears: select it to open configuration window of device specific parameters.

For details, see devices technical manuals.

▼ **Address**
Select an address suitable for the device.

▼ **Pertaining areas**
Select device pertaining areas.

▼ **Parameter**
Select outputs to be reserved for a siren or for the activation of the output relay of a power supply unit.

13 NG-TRX DEVICES

Page to manage the NG-TRX radio peripheral devices connected to the control unit.
To operate a single device:
– select the corresponding row on the grid
– set options in below tabs and/or grid columns
The columns allow to:
- view **Type**, **Model**, **Version** of each radio device
- set the following parameters:

▼ **Supervision interval**
Select the time interval between two consecutive supervision communications.
The supervision is useful to signal siren proper operation to the control unit.

▼ **Delay supervision anomaly**
If selected, supervision loss notifications will be delayed of a time equal to 6 times the supervision interval.

13.1 NG-TRX devices

Management peripheral N

▼ **Peripheral name**
Assing a name to this device.

▼ **Delete peripheral**
Click to unlearn this device and delete its code.

▼ **Generate a new peripheral code**
Click to generate again the code of a radio device previously unlearnt.

This tab also features a specific pane that contains different options according to the type of radio peripheral device connected (NG-TRX actuator or siren).
See technical manuals of the single peripherals for further information.
For sirens, the pane described below will appear.

13.1.1 Radio sirens

NG-TRX options

Use this pane to set specific functions of NG-TRX sirens.

▼ **Supervision interval**
Select the time interval between two consecutive supervision communications.
The supervision is useful to signal siren proper operation to the control unit.
If this is set to default, the value set in page System Options > Options NG-TRX (see paragraph 10.8 *p. 39*) will be used instead.

▼ **Signalling zone in time**
Select the type of siren signal emitted during entry time.

▼ **Signalling exit delay**
Select the type of siren signal emitted during exit time.

▼ **Maximum activation interval**
Select maximum duration for siren activation.
The siren will remain active for such interval unless it receives a stop command from the unit before.

▼ **Maximum daily activation**
Select the maximum number of daily activations for the siren.
Useful to avoid excessive battery consumption.

▼ **Acoustic indication**
Select siren sound type.
Useful to single out sirens from other nearby ones or to signal specific events with special sounds.

▼ **Activation volume**
To set siren activation volume move cursor on the bar (8 levels).

▼ **Beep volume**
To set siren beep volume move cursor on the bar (4 levels).

▼ **Delay supervision anomaly**
If selected, supervision loss notifications will be delayed of a time equal to 6 times the supervision interval.

▼ **No active in tamper**
Select it to prevent the tamper event from triggering the siren.
Useful during maintenance sessions.

▼ **Light indication existence in life**
Select it to make the device flash every 60 seconds.
If **Light indication arm state** option (below) is enabled, flashing will only happen while the control unit is disarmed.

▼ **Light indication arm state**
Select it to make the device flash every 30 seconds while the control unit is armed.

▼ **Light indication memory alarm**
Select it to make the device flash 3 flashes every 30 s if there are alarm memories.

▼ **Light indication arm/disarm**
Select it to have the front LED light up every time a sector belonging to one of its pertaining areas is armed or disarmed.
- Arming: 3 flashes.
- Disarming: one long flash

▼ **Acoustic indication arm/disarm**
Select it to have the siren sound every time a sector belonging to one of its pertaining areas is armed or disarmed.
- Arming: 3 beeps
- Disarming: one long beep

Click on the dedicated buttons to select siren pertaining areas.
Other buttons:

▼ **Load default**
Reset to factory default.

▼ **Copy setup**
Create a copy of current setup.

▼ **Paste setup**
Paste setup copied previously.

14 WEEKLY PROG.

Page for weekly programmer management.
Up to 32 schedules can be set and activated.
To operate schedules individually:
– select the corresponding row on the grid
– set options in below tabs and/or grid columns

14.1 Weekly programmer

▼ **Program name**
Assign a name to the selected program.

All programs share the following functions:

▼ **No SMS/Voice for (...) programmer**
If selected, the dialler will not activate for automatic arming/disarming commands from the weekly programmer.
Function available also in page **Telephone Dialler**, tab **Generale**.

▼ **Disable Standard/Daylight saving time automatic switch**
If selected, the automatic switch between standard and daylight saving time (and viceversa) will be disabled.

▼ **Do not disarm (...) with a simple disarming**
If selected, the weekly programmer cannot disarm sectors armed in max security with a "simple" disarming command.

Select **Program enabled** to activate the programmer: below pane options will become available for selection.

Program settings

▼ **Editable by the user**
Select it to make the program editable from the keypad menu.
The user will be allowed to:
- enable/disable programs (information not in unit setup, the unit remembers this setting after being restarted);
- change program activation time (this setting is part of the control unit configuration, it is therefore affected by read/write operations).

If a program is “editable by the user”, the corresponding output will appear in the maintenance menu, under OUTPUT CONTROL option.

▼ **Days**
Select week days (either working days or holidays) for which the option has to be repeated.

▼ **Program function**
Select the function to be activated for the program.
Each function requires the selection of a Parameter (output, user) and/or area sector(s) for which the program will activate.

▼ **Start hour**
Select program starting time (hours and minutes) for selected days.

▼ **Parameter**
Select the parameter for the function (output, user).

▼ **Weekly day type**
Set a type for each day: working day, holiday or semi-holiday (A or B).
By default, the days from Monday to Friday are working days, Saturday is semi-holiday A, Sunday is holiday.
For example, for a shop closed on Monday mornings and on Sundays, the following settings shall be applied: semi-holiday A for Monday, weekday for days from Tuesday to Saturday, holiday for Sunday.

Having set a type for each day it is possible, for each program, to set which days to activate it:
– select the grid row corresponding to the program
– check/uncheck the checkboxes **Run if Holiday**, **Run if ferial**, **Run if Semi-holiday A**, **Run if Semi-holiday B**.

From the next tab **Schedule events** it is possible to select the sectors in each area affected by a program.

Weekly programmer and arming lock option

Arming from weekly programmer depends on the real possibility to arm sectors selected and on activation of **Activate Arming Lock** function (see paragraph 10.1 *p. 30*):
- if the arming lock option is deactivated and sectors cannot be armed due to alarmed zones, the arming will be forced

and an alarm for those zones will be generated;
- if the arming lock option is active and sectors cannot be armed due to alarmed zones or dialler/siren faults, no arming occurs and the corresponding event will be generated;
- if the arming lock option is active and sectors cannot be armed due to zones alarmed at the end of the exit time, the system disarms at the end of the exit time and a no arming event wil be generated.

Example

One wants to activate output 1 from Monday to Friday at 8.30.
The parameters in pane **Program settings** shall be set as follows:
– select days from Monday to Friday
– from drop-down menu **Program function** select "Enable output"
– set 8:30 as activation time
– set "Output 1" as parameter

14.2 Schedule events

This tab contains the programs configured in the previous tab.
This tab allows selecting the sectors of each area affected by the program (if required and if the program is enabled).
– select a program from the grid
– for each area, check or uncheck the boxes to select or deselect the sectors

14.3 Exception (Days)

Use this tab to define exceptions to program activations.
– select a grid row
– from column drop-down menus, select the activation month and day and the day type (workday, holiday, semi-holiday)
The programs will be suspended in the time intervals defined by the exceptions.
It is possible to define up to 32 exceptions, of which the first 16 are permanent (persistent in control unit memory), the next ones are volatile (not repeated).
Click on **Activate Fixed Holiday (Italian)** to automatically add the Italian holidays (with fixed date) as permanent exceptions.

⚠ *Fixed holidays replace any permanent exception already set.*

14.4 Exceptions (Holidays)

Use this tab to define exceptions to program activations due to holidays.
– select a grid row
– select beginning/end month and day and day type (workday, holiday, semi-holiday) from column drop-down menus
The programs will be suspended in the time intervals defined by the exceptions.
It is possible to define up to 8 exceptions.

14.5 Extraordinary

Overtime necessity may require temporary changes to program activation times.
Use this tab to define the parameters concerning overtime management.
The settable parameters apply to all the users and the programs at once.

▼ **Maximum advance time**
The weekly programmer will allow a program to start earlier than programmed. Set here the maximum amount of time allowed for the program to start in advance.

Requests for overtime

Use this pane to set the parameters concerning the overtime activation from keypad.

▼ **Definition of the hourly (...) overtime**
Overtime will be requested according to multiples of this time.

▼ **Number of hourly advancements (...) overtime**
For each single overtime request, the time can be extended a maximum number of times equal to this number.

▼ **Maximum number of overtime requests**

A maximum number of requests equal to the value set here will be accepted.

▼ **Maximum total demand for overtime**

Set here the total maximum time accepted for each overtime day.

To require overtime use OVERTIME REQUEST menu item in keypad user menu.
For details, please see 21 *p. 60*.

15 EMERGENCY EXITS

This page allows to manage the zones assigned to control passages called "Emergency exits", to assign a local signal to them and to arrange their testing.
The page is available for control units whose firmware version is 1.0.0 or above, using the latest version of BrowserOne and control unit module.
Select in the grid each zone assigned to emergency exit control (typically, magnetic contacts that control opening and closing of a door).
For such zones, it is necessary that the following options have been set on page **Zones** > **General**:

- select event “Emergency Door Alarm” from drop-down menu **Zone Event**;
- select "24H" from pane **Zone Options**.

15.1 General

Once you have selected a zone in the grid, use this tab to define its options.

▼ **Local signaling**
Select to enable an optical-acoustic device (e.g. a plate) to signal the alarm state of the "emergency exit" zone.
This signalling device must be wired to the output marked with the same number as the zone (e.g.: zone 0005 ➜ output 0005).

▼ **Reset local signaling on input reset**
Select to deactivate an optical-acoustic device indication when its associated "emergency exit" zone resets.

▼ **Emergency exit testable**
Select to make the zone testable.
If selected, it will be possible to define test parameters using tab **Emergency exit test** (see paragraph 15.2 *p. 50*).

▼ **Local signaling time**
Set a time: the local signalling device wired to the "emergency exit" zone will remain active for this time after the zone enters alarm state.

General options (valid for all zones)

The following options affect all the "emergency exit" zones at the same time.

▼ **Enable local signaling on general alarm**
Select to activate each local signalling device (if there is one) also in case of general alarm.

▼ **Play sound on zone tested**
If selected, a beep tone will be played to confirm zone testing (zone opening-closing).

▼ **Activate local signaling when testing an "emergency exit" zone**
If selected, the opening of an emergency exit activates the correspoding local signalling device even during the test.
The local signalling device stays active until the corresponding emergency exit gets closed again.

15.2 Test of emergency exits

This tab allows to configure the test parameters for the sectors to which "testable" zones are associated (i.e. zones for which the **Emergency exit testable** option is selected).
The test is defined in terms of sectors: make sure each "emergency exit" zone to be tested is actually assigned to a certain test sector.
Use page **Zones** > tab **Assign Area/Sector** for this purpose.

▼ **Emergency exit start mode**
Select the test starting mode for each sector.
If "Manual", the test for this sector can be started only manually: either accessing to the keypad user menu item **EMER. DOOR TEST**, or properly configuring a zone for this purpose.
If "Disarm + manual", the test for this sector will automatically be proposed when disarming it. It will also be possible to start it manually.
For all the details about test starting, see section 15.2.1 *p. 51*.

▼ **Test timeout**
Set the maximum amount of time after a test request (manual or at disarming) available to perform the test.

15.2.1 Details on "emergency exit" zone

Testing of a "emergency exit" zone is considered successful if the zone enters alarm state (door opened) and then returns idle (door closed).
In case there is a test request for a sector but the test has not been performed yet ("ongoing test" condition), the green system status LED will blink on the keypads controlling that sector.
The test is considered failed if the time set in field **Test timeout** expires or if the system is armed without performing the test.
If the test is failed for a sector, the anomaly LED will blink on the keypads controlling that sector; the related anomaly is reported in the status menu.

Starting the test manually

To start the test manually, enter user menu from keypad:
– key in user code
– type *
– use arrow keys to go to **EMER. DOOR TEST** option
– press OK
The test can be started by users with Basic Maintenance property.
See control unit user manual for detailed information on this menu.

Starting the test at disarming

If "Disarm + manual" mode has been selected for a sector, the test will be started when disarming it.
Go to each "emergency exit" zone to test, make it enter alarm state (door opened) and then idle state (door closed).
If set so, a beep tone will be played to confirm each single test completion.

Starting the test using an external zone

When a sector can be tested manually, the test starting command can also be given using a properly configured zone (a button typically).
Assign to this zone (having property "24H") the event "Test emergency exit start".
When the zone enters alarm state (button pressed), the test is started. Go to each "emergency exit" zone to test, make it enter alarm state (door opened) and then idle state (door closed).
If set so, a beep tone will be played to confirm each single test completion.
Similarly, it is possible to assign to another zone the "Test emergency exit end" event to manually stop the test.
When the zone enters alarm state (button pressed), the test is stopped. The test is considered failed for non tested zones.

Associated control outputs

It is possible to associate actions to specific outputs, so that these outputs activate to indicate the state of a certain sector testing.
For example, these outputs can be connected to light indicators that will turn on to indicate, for each single sector, different test states (ongoing, failed, passed).
Enter page **Outputs**, select each output of interest and select from drop-down menu **Output function** one of the available actions for the emergency exits.
For example, to have outputs 10, 11 and 12 activated to indicate the states of ongoing, passed or failed test (respectively) for sector 2 of area 1, assign:
- to output 10 the action “Emergency exit test started", selecting sector 2 of area 1 from below checkboxes;
- to output 11 the action “Emergency exit test passed", selecting sector 2 of area 1 from below checkboxes;
- to output 12 the action “Emergency exit test failed", selecting sector 2 of area 1 from below checkboxes.

16 VAULTS

This page allows to manage vaults (safes, lockboxes, security containers, etc.) that have a control board.
The page is available for control units whose firmware version is 1.0.7 or above, using the latest version of BrowserOne and control unit module.
Select every vault in the table, choose the model and input its connection data (IP address, port and password).
Use the monitoring (read only) password, which allows reading the input and output states of the board and controlling their activation but not to change the configuration parameters of the vault.
The management of the vaults configured in this tab happens exclusively through the logic elaborations editor (ch. 7.1 *p. 18*)

17 GUARD TOUR

It is possible to define a "guard tour", i.e. a defined closed path of sectors that will be disarmed temporarily one after another in order to allow a security guard to pass through the protected areas.
The path includes several sectors (called "stations"): the security guard will have to disarm and pass through them within a settable time.
The security guard must be an user with "Guard round" property: this property can be set in page **Users** > **Sectors Authorized/Proposed**.

Set the beginning sector

▼ **Sector to be deactivated to access the round tour**
Select the sector to disarm to begin the guard tour.

▼ **Disarm time to access the guard round**
Set a time. The sector selected in the previous menu will be disarmed for the set time to allow starting the guard tour.
Once this time has elapsed, the sector will be armed again.

Set the stations of the guard tour

▼ **Station**
Name of the station.

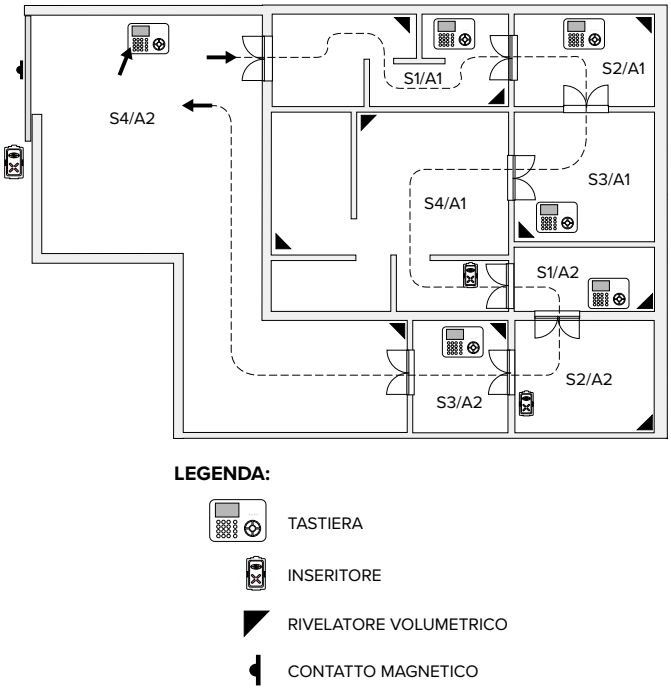
▼ **Time**
Set a time using arrow keys.
Columns **Input** and **Sector** will be available only if a time value higher than 0 has been set.
If the time has been set to 0, the station will not be considered.

▼ **Input**
Set the zone associated to the station.

▼ **Sector**
Set the sector associated to the station.

Example

One needs to configure the guard tour as shown in picture.



The guard tour shall begin from sector 4 of area 2.
– set "Sector S4.A2" in drop-down menu **Sector to be deactivated to access the round tour**
– set, for example, 30 s in field **Disarm time to access the guard round**
The path includes 8 stations, one for each sector.
For each station:
– click on the grid row corresponding to that station

– set the sector (from S1.A1) and the zones involved in each step
– set the allowed time to pass through each sector (e.g. 20 s for each sector)

Here follows the result of the above settings.

The user configured as "Guard round user" draws his proximity key close to the reader of sector S4.A2 keypad.

The control unit disarms sector S4.A2 and starts the timer: within the set time (30 s) the guard round user has to press OK to confirm he wants to start the guard tour, otherwise sector S4.A2 will be armed again.

Upon pressure of OK key the guard tour will begin: sector S1.A1 will be disarmed, the user has to pass through it within 20 seconds and draw the proximity key near the next keypad or reader.

Sector S2.A1 is disarmed, sector S1.A1 is armed again: the user has to pass through sector S2.A1 within 20 seconds and draw the key near the next keypad or reader.

These operations have to be repeated for all the tour steps.

To end the guard tour, the user returns to sector S4.A2: on its keypad the following message will be displayed

"RESET GUARD TOUR"

The user has 30 seconds to exit before S4.A2 re-arming.

18 TEMPERATURE

Page to manage functions of built-in temperature sensor.
The sensor is used to control temperature inside the case.
The temperature will be represented on a graphic as thermometer on page **Status**.

18.1 Options

Temperature options

▼ **Temperature Events Log**
Select to enable the log of temperature events on the control unit history file.

▼ **Temperature Max Threshold**
Set temperature maximum threshold for the thermostat function integrated.

▼ **Temperature Min Threshold**
Set temperature minimum threshold for the thermostat function integrated.

18.2 A-B temperatures management

▼ **Enable management of A and B temperatures**
Check to activate below panel.

Options for A and B temperatures

The control unit monitors the temperature that shall not rise above a prealarm and then an alarm threshold called A and that it does not go below a prealarm and then an alarm threshold called B.
Set prealarm and alarm thresholds in fields below.
To control if the temperature falls within thresholds set, set "A-B Temperature control function" to a unit output (see chapter 7 *p. 17*): the output will activate when the temperature reaches alarm thresholds A or B.
Alarm reset mode depends on selection/deselection of **Automatically restore (...) temperatures'** option.

▼ **Automatically restore (...) temperatures'**
If selected, the output will be reset when the temperature falls again within prealarm thresholds.
If deselected, A alarm (B alarm) resets if the temperature lowers below (rises higher) alarm threshold A (B) of the quantity set in **Temperature differential for A and B alarms**.

Manual reset

Users can also reset alarms manually as long as the temperature falls within thresholds set.
To configure this function: go to page **Outputs**, tab **Outputs**, select one output and associate "A-B Temperature control output function"; in area **Parameter** check sector boxes desired: S1, S2, S3 or S4.
To reset the output manually, user shall enter the following code at keypad

Code + SX

19 EVENTS LOG

Page to manage events history.
SUPERIA series control units can log up to 10000 events.
Each event is saved with date and time of generation.
In order to comply to the EN50131 standard enable **Limit Log FIle Events** function (in pane **EN50131 Options**, see paragraph 10.1 *p. 30*): the number of events logged for each arming/disarming cycle for each event source will be limited to 10.
Once the limit is reached, events are managed normally but will no longer be logged.
Unit internal clock is not equipped with a backup battery: events generated under mains and power failure conditions will be logged with default date (SAT 1/01/00) when mains or power supply is restored.

19.1 File and archive

Operations

▼ **Read**
To read unit history file previously saved and visualize events in the grid area.

▼ **Open...**
To open a saved .hst file and read it even while not connected to the control unit.

▼ **Save...**
To save unit history file as file format selected.
Click on the dropdown triangle to select a format:
- .hst to open it in BrowserOne;
- text, CSV or Excel formats for compatibility with word processors or spreadsheets.

Note: to use files saved, users shall login with same user name and password of the user who saved the file.

▼ **Archive**
Function available only if BrowserOne Plant Management function is active.

Archive

▼ **Load**
To display an archived log in the grid area.

▼ **Delete**
To delete an archived log.

Options

▼ **Swap order (most recent events at the top)**
Check this box to display the most recent events at the top.

▼
Select to display date and time in UTC standard time.

19.2 Event Filter

Use this tab to filter logged events and display only desired ones.
The area on the left lists all selectable events: check a box to display the log referring to that specific event (use **Select All** to display all events, **Deselect All** to see the display empty).
It is also possible to display only events in a time interval to be set: set start/end day using drop-down **To**/**From** menu (check the boxes to activate the menu).

20 STATUS

Page to control status of connected control unit.
The page is available only when control unit is connected.
It represents a useful tool for anomalies diagnostic.
These indicators are always visible:

▼ **GSM Signal**
It displays GSM signal strength, from 4 signs (excellent) to no signs (no signal).

20.1 Consulting the states

A series of tabs is available here with status info grouped according their type.
Status are represented by the following icons:

icon	Indication
(red)	Ongoing alarm/anomaly
(yellow)	Alarm/anomaly memory
(grey)	No alarm/anomaly (or memory of them)
(blue)	Exit time in progress
(red)	Fixed: sector armed Blinking: sector in exit time
(grey)	Sector disarmed
	Used in commands like "max security arming"

Memories will be reset as follows:
- per gli ingressi: all'inserimento dei settori associati;
- for areas/radio siren: upon arming of any sector assigned to the area/radio siren;
- for non-available areas (having no users with authorised sectors): upon any arming command.

Areas status

Area that displays the status of area sectors (arming, alarm tamper, anomaly status).
A series of options (**Arm selected sectors**, **Disarm selected sectors**, **Arm in max security**, **Disarm in max security**) allows sending commands to the connected unit: select sectors desired, then the option to be applied.

▼ **Delete memories**
Select to delete alarm, tamper and anomaly memories.
Memories will be reset at arming.

Zones status

Area that displays zones status (alarms, faults, anomalies).
Use **Zone included**/**Zone bypassed** options to include/bypass zones.

Output status

Area that displays output status (green LED: output enabled, grey LED: output disabled).
Use **Enable output**/**Disable output** options to enable/disable outputs.

Radio devices status

Area that displays the status of the radio sirens connected to the unit.

Users status

Area that displays battery status of remote controls used by users and learned to RIVERRF concentrators or via GATEWAY2K.

Modules status

Area that displays the status of the modules registered to the control unit in the available slots.

Control devices status

Area that displays the tamper status of the control devices connected to the control unit.

Serial devices status

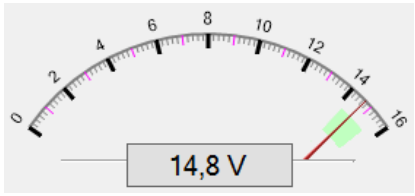
Area that displays the status of the serial devices (tamper, low battery, fault) connected to the control unit.

Analog values

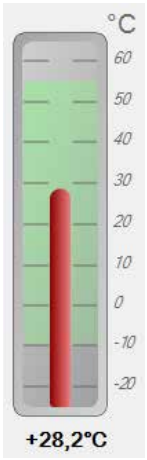
Tab containing analog values detected by RIVERTH concentrators connected to the control unit.
In column RIVERTH, a value preceded by symbols > o < indicates that the values are outside the tolerance range or that the device is disconnected.
Click on **Detect devices** to detect devices connected.
Click on **Refresh values** to refresh values on the page.
Check **Periodic refresh** box to make the page refresh automatically.

Operating parameters

Operating voltages are displayed with analog indicators



as well as the housing internal temperature.



NG-TRX

Status of NG-TRX system managed with GATEWAY2K.
The pane **Radio Signal NG-TRX** displays the strength of the radio signal for the three channels through vertical bars.
The pane **Remote controls statistics** displays the total number of packets transmitted and the percentage of packet re-transmitted and lost by remote controls.
Select **Remote controls details** to see statistics of remote controls (included the average signal).
The pane **Sensors/devices statistics** displays the total number of packets transmitted and the percentage of packet re-transmitted and lost by NG-TRX sensors and other NG-TRX devices (ex. radio sirens).
Select **Devices/sensors details** to see statistics of single devices.
Use **Reset all statistics** to delete all statistics.
Single devices statistics can be reset in detailed menu pages.
Statistics will be reset at control unit reset automatically.
Statistics shall be read as follows:

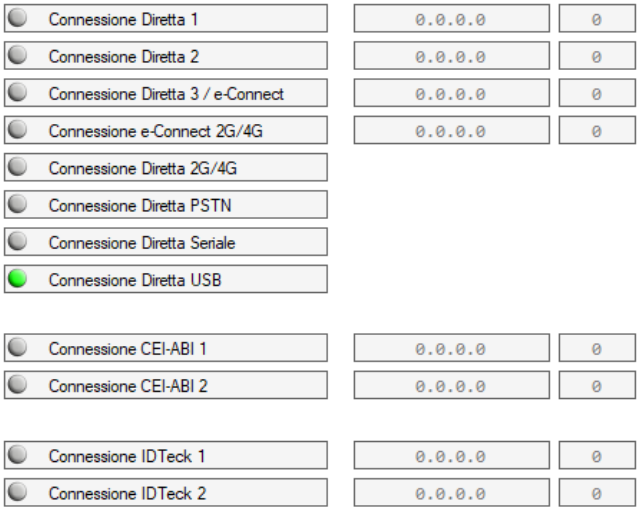
- Retransmission <5%: normal value.

- Several retransmissions (>5%), good signal = lots of contemporary transmissions, complex surroundings, high number of devices.
- Several retransmissions (>20%), low signal = problematic connection, increase transmission power.
- Data packets lost but supervision OK: sensor reception problems.
- Data packets lost and lack of supervision: out of order connection or sensor

Note: packet retransmission or loss for remote controls is to be expected if they are used outside their range.

Connection status

This tab shows the state of the active connections in real time, as well as the IP addresses and connection ports.



Statistics 485

Tte tab is available for control units with firmware version 1.0.7 or above, using BrowserOne 3.26.22 or above with module 1.1.4 or above.

It shows, separately for each serial line:

- The polling interval of inputs and control devices.
- The number of data packets that had to be sent a second time.
- The number of received but non valid packets.
- The date and time of the last reset.

Statistics can be reset with the designated buttons: the values refer to the period of time between the last reset and now.

The Zones / Peripherals / Control Deviced Details buttons allow to visualize the number of repeated transmissions of each single device.

A flag-shaped icon marks which serial line the device belongs to.

21 USER MENU

It allows the user to perform basic maintenance and to enable the installer to perform remote assistance operations.
By default, only user #1 can operate with control unit keypad: other users shall be authorised via software.
To enter the menu:
– if simplified code mode is not active: key in user number and then OK
– key in user code (default: 111111)

⚠ *It is strongly recommended to change the code to strenghten system security level. The installer cannot see it since it is represented by asterisks.*

– type *
The user menu lists the following items:

Maintenance

➔ BYPASS ZONES
➔ AUTHORIZATION
➔ OUTPUT CONTROL
➔ DAY TYPE
➔ OVERTIME REQUEST
➔ CLOCK SETUP
➔ WEEKLY PROGR.
➔ MANAGE USERS
➔ CHANGE CODE
➔ PHONE NUMBERS
➔ SYSTEM TEST
➔ MANAGE CHIME
➔EMER. DOOR TEST
➔ EVENT LOG

– press OK to enter a menu, STOP to exit setup
– use arrow keys ↑ or ↓ to browse menu items

BYPASS ZONES

This menu bypasses the selected zone.
– press OK to enter the menu
– use ↑ or ↓ keys to browse among zones, or enter the zone number directly
– press OK to bypass the zone and exit the menu, Stop to exit the menu without bypassing the zone
Note: if the option **Zone exclusion only from installer** is selected (see paragraph 10.1 *p. 30*), the menu will not be available.

AUTHORIZATION

This menu allows changing the authorization provided to the installer for:
• control unit access, connection to the BrowserOne software;
• the access (via BrowserOne) to the user images captured by VISIO2K, if there is one;
• remote control unit firmware update.
– press OK to enter the menu
– use arrow keys ↑ or ↓ to go to the authorisation you are interested in

Installer Access

Press OK repeatedly to change the authorisation to access the control unit:

▼ **TEMPORARY**
Until the end of the connection session.

▼ **NONE**
Access denied.

▼ **PERMANENT**
Access granted.

Image Installer

Press OK repeatedly to change the authorisation to access the user's images in BrowserOne:

▼ **NONE**
The installer cannot view the images.

▼ **LOCAL**
The installer can view the images only via USB connection (default).

▼ **ALWAYS**
The installer can view the images only via any type of connection.

Panel Update

Press OK repeatedly to change the authorisation to remotely update control unit firmware:

▼ **USER**
Each remote firmware update must be confirmed by the user.

▼ **AUTOMATIC**
Each remote firmware update will be completed automatically, no authorisation will required to the user.

⚠ *Setting the update to "AUTOMATIC" will cause the loss of the IMQ - Security Systems certification.*

– press Stop to save changes and exit the menu

OUTPUT CONTROL

The menu allows to change the status of the outputs programmed with "Manual control output" function (see chapter 7 *p. 17*).
– press OK to enter the menu
– use arrow keys ↑ or ↓ to browse among outputs, or key in output number directly
– press OK repeatedly to change output status
When all outputs are disabled, the message **No Out.Available** will be displayed
When an output is associated to an event, its status can be checked but not managed.
– press Stop to save changes and exit the menu

DAY TYPE

This menu allows to change day type (workday, holiday, semi-holiday A, semi-holiday B) temporarily.
This change will only be effective on current week: next week the configuration values set in BrowserOne will be restored.
– press OK to enter the menu
– press ↑ or ↓ to reach the desired day
– press * or # to change day type
– press Stop to save changes and exit the menu

OVERTIME REQUEST

This menu allows requiring overtime.
– press OK to enter the menu
– press ↑ or ↓ to reach the desired program
– press * to activate an overtime request and define its duration
The overtime duration is defined according to pre-defined time steps (which can be set via BrowserOne) and it depends on how many times the * button is pressed: each single pressure extends the duration of a quantity equal to the set time step. For example, if the set step is 30 minutes, pressing * 3 times an overtime of 1h 30min will be set.
– press # to cancel the ongoing overtime request
– press OK to save
– press Stop to exit the menu

CLOCK SETUP

Menu for date and time adjustment.

– press OK to enter the menu
– use number keys to set weekdays (1 = Monday ... 7 = Sunday), day/month/year, hour and minute
– use arrow keys ↑ or ↓ to move cursor along the row: data which are being modified will blink
– press OK to save changes and exit the menu, Stop to exit the menu without saving

WEEKLY PROGR.

This menu allows to suspend or modify a schedule set with the programmer.
This is possible as long as at least one schedule is available and the user is authorised for change (selected **Editable by the user**, see paragraph 14.1 *p. 47*).
– press OK to enter the menu
– press 1 to start modifying time
– use number keys to modify time, arrow keys ↑ or ↓ to move the cursor
– press OK to confirm
– press # to suspend a schedule, 1 to restart it
– press Stop to save changes and exit the menu

MANAGE USERS

This menu allows changing users authorizations for system access.
The user shall be enabled for users management: select **Enable user authorization management** in pane User Options (see paragraph 8.1 *p. 22*).
– press OK to enter the menu
– use arrow keys ↑ or ↓ to select the user
– press OK repeatedly to change the user's authorization:

▼ **FULL**
full authorisation

▼ **ARM ONLY**
arming only

▼ **DIS. ONLY**
disarming only

▼ **SUSPENDED**
authorisation denied

– press # key to suspend a user
The suspension can be set with weekly programmer too.
However, setup from keypad has priority over other settings.
– press Stop to save changes and exit the menu

PHONE NUMBERS

This menu allows changing phone numbers in users' phone number lists (see paragraph 9.5 *p. 28*).
– press OK to enter the menu
– press ↑ or ↓ to reach the number to be modified
– press OK to access the number
– use number keys, * and # to enter the number: the cursor will move rightwards
– press ↓ to cancel one digit, ↑ to enter an empty space, S4 to cancel the entire row
– press OK to save changes and exit the menu, Stop to exit the menu without saving

CHANGE CODE

This menu allows changing user codes.
– press OK to enter the menu
– use number keys to enter the code
Digits will be represented by asterisks (******).
– enter the code again
If the two codes match, the new code is memorized and the function exits the menu automatically.

SYSTEM TEST

This menu allows testing zones, outputs and diallers to check devices working.

– press OK to enter the menu
– use ↑ or ↓ to browse among available tests
– press OK to start the test

▼ **Zone test**

Alarm all connected zones with walk test property: the system beeps for confirmation and is now ready to test the following zone.

In case no zones have the walk test property, the message NOT EXECUTAB. will appear.

Press Stop to exit zones test and go to the following test.

▼ **Output test**

Press OK to start the test.

Press # to suspend the test, Stop to exit the test.

▼ **Dialler test**

Press OK, the message TEST CALL will be displayed.

Press OK to start the test.

Wait until the test is finished (if the dialler is not active, the message NOT EXECUTAB. will appear).

Press Stop to exit the test.

▼ **Battery test**

Press OK to start.

Press Stop to exit the test.

MANAGE CHIME

This menu allows enabling/suspending chime function.
– press OK to enter the menu
– press OK repeatedly to select ENABLED or SUSPENDED
– press Stop to save changes and exit the menu

EMER. DOOR TEST

Start emergency exit test.
See user manual.

EVENT LOG

This menu allows checking system events logged.
– press OK to enter the menu
The function will display the last event saved and the corresponding user.
– press ↑ or ↓ to browse among events
– press * to display date and time of the event
– press Stop to exit the menu

22 INSTALLER MENU

It allows more in-depth programming.
Access authorization has to be granted by a user with maintenance property.
The authorisation can be:

- **Permanent** (Default)
- **Temporary**: once for 15 minutes
- **None**: denied

To enter the menu:

– if simplified codes mode is not active: key in code 0 followed by OK
– enter installer code (default: 88888888)
– press OK

The installer menu includes the following items:

Programming

- ➔ ERASE MEMORIES
- ➔ FAST ACQUIRE
  - ➔ NEW REMOTE?
  - ➔ NEW SENSOR?
  - ➔ NEW SIREN?
- ➔ BYPASS ZONES
- ➔ SYSTEM LOCK
- ➔ RF MONITOR
- ➔ TERABUS
- ➔ LEARN PROXI R.C.
- ➔ LEARN RADIO DET.
- ➔ TX SIREN CODE
- ➔ NETWORK SETTINGS
- ➔ INTERNET ACCOUNT
- ➔ OUTPUT CONTROL
- ➔ CLOCK SETUP
- ➔
- ➔ WEEKLY PROGR.
- ➔ MANAGE USERS
- ➔ PHONE NUMBERS
- ➔ CHANGE CODE
- ➔ SYSTEM TEST
- ➔ MANAGE CHIME
- ➔ ZONES SCAN
- ➔ EVENT LOG

– press OK to enter a menu, STOP to exit setup
– use arrow keys ↑ or ↓ to browse among selections

ERASE MEMORIES

Menu to delete active memories.

– press OK to enter the menu
– press OK to delete active memories and exit the menu, Stop to exit the menu without saving

FAST ACQUIRE

Menu to learn a NG-TRX radio device (remote controls, sensors or sirens).
It requires connection and configuration of at least one GATEWAY2K device.

– press OK to enter the menu
– press Stop repeatedly to go to learning option of device desired (remote control, sensor or siren)
– press OK to go to the learning option submenu (NEW REMOTE? / NEW SENSOR? / NEW SIREN?)

The learning steps are illustrated below for each device individually.

– press Stop to exit submenu setup
– press Yes to save configuration, No to cancel changes made

▼ NEW REMOTE?

– press OK to enter level 2 menu
– the display will show ACTIVATE REM.C. option
– press and hold the central buttons of NG-TRX remote control for 10 s
– the display will show NAME?, press OK
– enter the name: press ⬇ to delete a character, 0 to move cursor leftward, # to move cursor rightward
– press OK to save and exit, Stop to exit submenu without saving

▼ NEW SENSOR?

– press OK to enter level 2 menu
– use ⬆ or ⬇ to go to the first zone to which learn the sensor
– press OK, the display will show ACTIV. DETECTOR
– press “learning” button of NG-TRX sensor to memorize
– press YES to confirm the code learned, NO to delete it

In case of multichannel sensor, each channel memorized will require the code confirmation.

– the display will show NAME?, press OK
– enter the name: press ⬇ to delete a character, 0 to move cursor leftward, # to move cursor rightward
– press OK to save and exit, Stop to exit submenu without saving

▼ NEW SIREN?

– press OK to enter level 2 menu
– set NG-TRX siren to “code learning” mode (coloured jumper closed, see technical manual)
– press OK to start siren code transmission

When code is transmitted correctly, the control unit will beep twice and the siren will signal it.
In case of wrong or missed transmission (AGAIN? displayed), press OK to repeat code transmission.

– once code transmission is complete, cut/open siren coloured jumper to save the code
– the display will show NAME?, press OK
– enter the name: press ⬇ to delete a character, 0 to move cursor leftward, # to move cursor rightward
– press OK to save changes and exit the menu, Stop to exit the menu without saving

BYPASS ZONES

See user menu.

SYSTEM LOCK

Menu to lock the system for maintenance sessions.

– press OK to lock the system

The keypad and proximity key reader LEDs will blink and the following message will appear:

SYSTEM LOCK
IDLE

– press Stop to exit the menu and restart the system

RF MONITOR

Menu to display signal strength of the 3 radio channels.

– press OK to enter the menu

Below each channel, signal strength is indicated by # characters (#### = excellent, ---- = poor).

– press Stop to exit the menu

TERABUS

It allows to address the concentrators equipped with TERABUS interface and to enable or disable their LEDs.

– press OK to enter the menu
– press ⬆ or ⬇ to browse among available options , , OPTIONS
– press OK to enter a menu item

Use items o to address the concentrator: see its manual for detailed information.
Item OPTIONS allows to enable or disable the concentrators' LEDs:

– select OPTIONS

– press OK to enter the menu
– press OK repeatedly to change state, choosing between and
– press Stop to exit the menu and save

LEARN PROXI R.C.

Menu to learn a NG-TRX remote control or a proxi key associated to a user.
– press OK to enter the menu
– use ↑ or ↓ to go to the user desired, or enter user number directly
– press OK
– if there are already remote controls or proxi keys associated to the user, press 1 to delete them, Stop to leave settings unchanged
– press 1 to memorize a remote control, 2 to memorize a proxi key
– to learn a NG-TRX remote control, press and hold for 10 seconds 1 and 2 buttons of remote control and wait for confirmation
– to learn a proxi key, draw it near the reader and wait for confirmation or error tone
– press Stop to exit setup
– press Yes to save configuration, No to cancel changes made

LEARN RADIO DET.

Menu to learn a detector on a zone.
– press OK to enter the menu
– use ↑ o ↓ to go to the zone desired, or enter zone number directly
– press OK
– if there are already detectors associated to the zone, press 1 to delete them, Stop to leave settings unchanged
– press OK to start learning a detector to that zone
– press 1 to learn NG-TRX sensors (GATEWAY2K connected required), 2 to learn wireless sensors of previous generation (RIVERRF connected required)
– the message ACTIV. DETECTOR will be displayed: activate the sensor (see related manual), and wait for confirmation or error tone
– press Stop to exit setup
– press Yes to save configuration, No to cancel changes made

TX SIREN CODE

Menu to learn NG-TRX sirens.
It requires connection and configuration of at least one GATEWAY2K device.
First, close configuration coloured jumper to set the siren to “code self-learning” mode.
– press OK to enter the menu
– use ↑ o ↓ to go to the siren desired, or enter siren number directly
– press OK
– select button 2 for NG-TRX sirens: the following message will be displayed

Sir.X NG-TRX

– when required, press Stop to exit, OK to save changes

NETWORK SETTINGS

Menu to display Ethernet board network settings.
– press OK to enter the menu
– press ↑ or ↓ to choose VIEW or DISCOVERY
– **VIEW**: use ↑ or ↓ to browse among items: MAC ADDRESS / IP ADDRESS / SUBNET / GATEWAY / DNS1 / DNS2
– **DISCOVERY**: enable or disable the propagation of the control unit's name on the LAN (used to identify a specific control unit when using the Remote Manager software)

The Discovery function is active by default and is is automatically deactivated during the first writing of the configuration.
If the Discovery function is active and the user code is still the default one, the Remote Manager software can change the network parameters of the control unit, port included, to simplify first installation procedures.
– press Stop to exit the menu

INTERNET ACCOUNT

Menu for the registration to e-Connect service.
It requires that the connection to e-Connect has been enabled (panel **e-Connect**, see paragraph 10.5 *p. 37*).
– press OK to enter the menu
– press 1 to start recording, Stop to exit the menu
– enter registration code (9 digits) received via email for the registration to e-Connect
– press OK
When the procedure is complete, the message REGISTERED will be displayed followed by a confirmation beep.
In case of error, the message ERROR # will be displayed: for error codes see chapter 25 *p. 73*.
– press Stop to exit the menu

OUTPUT CONTROL

See user menu.

CLOCK SETUP

See user menu.

It allows to change keypad menu item language.
– press OK to enter the menu
– use ↑ or ↓ to choose a language
– press OK to set the selected language

WEEKLY PROGR.

See user menu.

MANAGE USERS

See user menu.

PHONE NUMBERS

See user menu.

CHANGE CODE

See user menu.

SYSTEM TEST

See user menu.

MANAGE CHIME

See user menu.

ZONES SCAN

It opens a diagnostics tool to measure the resistance value perceived at each onboard zone.
– press OK to enter the menu
– enter the number of the desired zone
– press OK

The resistive value is indicated at the top right corner of the screen.
If the zone is open ("infinite" resistive value), - - - - is shown.

EVENT LOG

See user menu.

TERABUS

It allows to address the devices equipped with TERABUS interface.

– press OK to enter the menu
– press ↑ or ↓ to browse among available options
– press OK to enter a menu item
– Address the device: see its manual for more detailed information.

23 MAX SECURITY

Sectors can be armed with **Max Security** property.
Such property can be set by the installer during configuration.
When a sector is armed in Max Security mode it can only be disabled

- by a user with 'max security' property (enabled via BrowserOne during configuration)
- via weekly programmer
- by the installer via software.

To set the Max Security property for a user:

– go to page **Users**, tab **General**, pane **User Options** (see paragraph 8.1 *p. 22*)
– flag **Enable Max security**

To arm one or more sectors in Max Security, users shall enter their user codes followed by '#'.
Sector keys corresponding to sectors armed with Max Security property will blink quickly.

⚠ *Users without Max Security property cannot disarm sectors until at least one of sectors authorised for them or for the keypad are armed with Max Security.*

23.1 Maximum Security Property

A sector can be armed with Max Security property:

- by a user with Max Security property: in such case the sector is armed in **User Max Security** mode;
- by the weekly programmer: in such case is armed in **Weekly Programmer Max Security** mode.

The User Max Security property is reset at any disarming; when a sector armed with Max Security property is disarmed the property is reset.
On the contrary, the Weekly Programmer Max Security property is reset by **Max Security Set** and **Max Security Reset** weekly programmer functions only.

⚠ *In detail, if a sector is armed in Weekly Programmer Max Security mode and a user with max security property performs a disarm, the Weekly Programmer Max Security property remains active. Therefore, at the next control unit arming it will be armed with Max Security property, even if the arming is performed by a user without the Max Security property. However, if the disarming is performed via weekly programmer Max Security Reset function, the sector property will be reset and the sector can be armed in the standard way.*

The following icons indicate sectors arming status:

	Sector disarmed, no Max Security
	Sector disarmed, Weekly Programmer Max Security
	Sector armed, no Max Security
	Sector armed, Weekly Programmer Max Security
	Sector armed, User Max Security
	Sector armed, User Max Security + Weekly Programmer Max Security

The following table illustrates Max Security operating mode for arming/disarming events:

Starting condition	Action	End status

	Arming made by user / weekly programmer without Max Security	
	Arming made by user with Max Security	
	Arming made by weekly programmer with Max Security	
	Arming made by user without Max Security	
	Arming made by user with Max Security	
	Arming made by weekly programmer with/without Max Security	
	Disarming made by user / weekly programmer	
	Disarming made by user with Max Security or weekly programmer without Max Security	
	Disarming made by weekly programmer with Max Security	
	Disarming made by user with Max Security or by weekly programmer with/ without Max Security	
	Disarming made by user with Max Security	
	Disarming made by weekly programmer without Max Security	
	Disarming made by weekly programmer with Max Security	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Set Max Security by weekly programmer	
	Set Max Security by weekly programmer	
	Set Max Security by weekly programmer	

Special cases

- A max security arming can be performed while the sectors cannot be armed or are already armed; in such case the arming is denied but the max security property is set and the corresponding event is saved on to the system log.
- When a weekly programmer activates a max security arming but the sectors cannot be armed and feature the arming lock option, the sectors will not be armed but the weekly programmer max security property will be set anyway.
- When a max security arming command is sent via remote control to already armed sectors, such sectors will remain armed and will be assigned the User Max Security property.

24 SYSTEM TEST

The control unit uses System Test tool to verify system proper working.
By default, interval between tests is 4 weeks. The system test interval can be increased by the installer (52 weeks max, parameter **System Test Interval**, see paragraph 10.3 *p. 35*) only as a result of an explicit request of the user, which has to be informed of the resulting assumption of responsibility.
Users are required to periodically check the system and quickly report any functional failure to the installer.
Go to SYSTEM TEST menu in installer menu on keypad (see chapter 21 *p. 60*).
The test includes 4 steps: ZONES TEST, OUTPUTS TEST, DIALLER TEST, BATTERY TEST.
For the test to be considered valid, all four steps have to be run in sequence, without exiting the menu.
Please wait for each step to be completed (with messages TEST OK, TEST EXECUTED or NOT EXECUTAB.) and go to the next one. If Stop is pressed before the end of a step, the test will be stopped and considered invalid.
Note: the system test request is saved to the events log. If the test is not performed, the request is repeated every month. The display will show the message TEST EXECUTED, until the complete test of zones, outputs an dialler is performed.

1. Zones test

Zones test function controls the operating status of sensors connected to zones.
Only sensors with the walk test property are tested: first set walk test property for zones desired (see **Walk Test** on paragraph 5.1 *p. 9*).
If no zones have the walk test property, the zone test can not be performed and will automatically be considered passed.
Each time a zone is successfully tested, the control unit produces a confirmation beep: a zone is considered successfully tested when the control unit sees both alarm and idle conditions, in any sequence.
The completion of the zone test is marked by three consecutive beeps.
There is no time-out to exit test functions, the control unit remains in test mode until the test is completed or until the user exits manually.

2. Output test

Output test function allows the temporary activation of:
- Programmable relays (if activated for general or tamper alarm);
- External sirens;
- RS-485 siren (if installed);
- NG-TRX siren (if installed).

3. Dialler test

Dialler test function generates a “periodic call” event and activates the GSM/GPRS dialler.
The test cannot be performed in the following situations:
- if GSM/GPRS module is idle;
- if voice dialler is deactivated;
- if the “periodic call” event is not set correctly.

To set the event correctly follow below steps:
– go to page **Telephone Dialler**, tab **Voice/Digital Dialler**
– flag **Activate Voice Dialler**
– select "Periodic Call" event from the grid
– select message from column **Associated Message**
– in column **Voice Phone Numbers Activation**, select the numbers to call

4. Battery test

Battery test function controls the operating status of backup batteries.
When the test is positive, the message TEST EXECUTED will appear.
The interval between battery tests shall be at least 2 minutes.
In case of battery replacement, start a new battery test to reset the anomaly signal.

Configure the connection

The connection to the e-Connect service can be carried out through the built-in Ethernet module or through an optional 4G module.
In case there are both, the priority will be given to the built-in Ethernet module.

- if you are using the built-in Ethernet module: on page **System Options** > **Network parameters**, configure the network options on pane **Ethernet** 1 or 2;
- if you are using a 4G module: on page **Telephone Dialler** > **General**, select options and and set the parameters on below panel.

To configure the connection to e-Connect:
– go to page **System Options** > **Network parameters**
In **e-Connect** pane:
– select **Enable connection to e-Connect**
– set parameters (see paragraph 10.5 *p. 37*)

Register the control unit

After a new e-Connect user has been created, a 9-digit code will be sent via e-mail:
– enter INTERNET ACCOUNT menu item in keypad installer menu
– type the received 9-digit code
Once the connection has been registered, in BrowserOne on page **System Options** > **Network parameters** the following message will appear:

"Registered e-Connect account: installer_name\unit_name"

Now press **Read setup** to avoid losing settings.
Access e-Connect via App or via web page to check connection proper operation.

Error codes

Once users have entered the 9-digit code, if the registration is incorrect some error messages may appear:
Error 1: DNS resolution error or connection opening error.

- For GPRS connection only: verify that the proper APN for Internet access is set, make sure that the SIM tariff plan includes internet traffic, check the remaining card balance.
- If using a custom URL for the e-Connect server, verify that the URL is correct.
- For LAN connection only: if a static IP is not used, check the DNS servers settings, verify the correctness of DNS servers IP addresses from control unit **Network parameters** menu.
- If using a static IP for e-Connect server, verify the correctness of the IP entered.
- For LAN connection only: if a static IP is used, check the setting of the internet access gateway, verify the correctness of the gateway IP address in control unit **Network parameters** menu.

Error 2: connection opening error.

- For GPRS connection only: verify that the proper APN for Internet access is set, make sure that the SIM tariff plan includes Internet traffic, check the remaining card balance.
- If using a static IP for e-Connect server, verify the correctness of the IP entered.
- For LAN connection only: if a static IP is used, check the setting of the Internet access gateway, verify the correctness of the gateway IP address in control unit **Network parameters** menu.
- For LAN connection only: verify that the 15000 port is open on the proxy/firewall.
- Check the functioning of e-Connect server through the Web interface connection at the address: https://connect.elmospa.com

Error 3: error in data exchange with the e-Connect server.

- For GPRS connection only: verify that the proper APN is set, make sure that the SIM tariff plan includes Internet traffic, check the card balance.
- Check the functioning of e-Connect server through the Web interface connection at the address: https://connect.elmospa.com

Error 4: invalid registration code.

- Generate a new registration code and repeat the procedure with the new code.

Internet security

The use of the Internet for connection to security systems may expose system components to hackers attacks.
Use protection tools suitable to protect the systems against such attacks.
Among the available solutions, we suggest the following two:

- install a physical Firewall between the Internet connection and the control unit; configure the router so that only the ports actually used for the TCP/IP connection are open;
- create a VPN (Virtual Private Network) including only the device and the remote supervision centre in order to isolate the system and protect it against unauthorised accesses.

26 ANOMALY EVENTS

Event	Possible causes	Actions to do
Anom. power serial device	Device not powered correctly. Power supplied below nominal value or battery discharged.	Check device power supply.
No GSM registration	No SIM card or non-activated SIM card. SIM PIN code not disabled.	Check SIM card is in place and active; check SIM PIN code is disabled.
Mains failure	No mains power.	Reconnect mains power and check it is working properly.
No battery	Undetected or faulty battery. Power below release value (9 V).	Check battery status with a charge connected. Replace it if necessary.
Discharged battery	Low battery charge level. Power below battery discharged threshold (10,5 V).	Recharge battery. Replace it if necessary.
Failed communication	The digital dialler cannot communicate with the surveillance centre.	Check dialler working. Contact the surveillance centre.
Fault	A fault referring to a zone has been set.	Check BrowserOne Status page.
Detector/device fault	Detection of a sensor, siren or serial line anomaly.	Check devices status on BrowserOne Status page to view devices affected.
RF Interference	Interference detected on a channel.	Check for radio disturbances in the surroundings.
No supervision	At least one radio device has not replied to the periodic control made by the unit.	Check device working (electrical wiring, battery).
Arming failure	No arming completed. Lock arming function active.	Check anomalies active (dialler/sirens fault, alarmed zones) and reset them.
System test failed	System test incomplete (ZONES TEST, OUTPUTS TEST, DIALLER TEST, BATTERY TEST). One step interrupted before completion. One sensor does not reply during ZONES TEST.	Check zones status. Restart system test and complete it.

27 GUIDE TO THE FIRST CONFIGURATION

This section includes the most common configuration operations.
In case of first configuration, follow steps in the order given to configure the unit so that it will already manage the fundamental functions of the intrusion detection system.
The operations require the installer to access the keypad menu and use BrowserOne software.

⚠ *We recommend, in any case, consulting the previous chapters for details on all the available configuration options.*

Access to the keypad installer menu

To access installer menu from a keypad:
– if simplified codes mode is not active: key in code 0 followed by OK
– key in installer code (8 digits, default: 88888888)
– press OK
– use arrow keys ↑ or ↓ to browse among available options
– press OK to enter a menu item, Stop to exit setup
– if you press Stop repeatedly after an operation, you may be asked to save changes

BrowserOne installation

The first installation of requires BrowserOne an Internet connection.
– login to the www.elmospa.com website
– in the BrowserOne page, download the BrowserOne_[version number]_web.exe file, run it and follow the on-screen instructions
– from BrowserOne page, download [Control unit model][version number]_setup.exe file: launch it to install the module
– open BrowserOne

27.1 Connect the unit to Browserone

Follow these instructions to connect the control unit via USB to the PC that runs BrowserOne.
Other types of connections are available.
– open BrowserOne
– go to **Connect** > **Connect to...** menu
– select the **Connection type**, e.g. "Serial" or "USB"
– click on **Next**
– connect the unit to the PC by using a USB-C cable (not supplied)
– wait for the COM port virtualization software to be loaded
– the window **Serial connection** will open: click on the icon to update the available communication ports
– select "ELMO Virtual COM" from drop-down menu
– select **Next**: the software will attempt to start the connection
– when the connection is fine, enter installer code and select OK
– load control unit module using **Modules** menu

27.2 Connect keypads and readers

– connect at least one keypad to the unit serial line and configure it as indicated in its manual
– connect proximity key readers if needed
– open BrowserOne
– go to page **Control devices** > **Keypads**
– select the grid row corresponding to the keypad/reader
– select the type of keypad or proximity key reader from **Type** drop-down menu
– check that the address is correct in the **Address** field (number 1 if the keypad is the only one connected)
– configure the advanced keypads (if present) clicking on **Open management**
For keypads:
– select the keypad presentation area from column **Area displayed**
– select the keypad pertaining areas from column **Pertaining areas**
For proximity key readers:

– select the proximity key reader pertaining area from column **Pertaining area**
– select the proximity key pertaining sectors within the selected area from column **Pertaining sectors**

27.3 Connect RIVER and serial line detectors

Connect RIVER concentrators and serial line detectors.
Configure them as indicated in their technical manuals.

⚠ *In particular, for RIVER concentrators balance zones using the 4 dedicated switches group and set the address using the 8 dedicated switches group. Leave switch number 8 set to OFF.*

– open BrowserOne
– read unit configuration using the dedicated button on the controls bar
– go to **Zones** > **Ultrabus/Terabus devices** page
In case of concentrator:
– in **Zone Type** drop-down menu select **Wired Concentrator**
– in panel **Device type**, select the number of inputs (8, 4, 2)
If case of serial line detector:
– in **Device type** drop-down menu select **Sensor 485**
– in **Advanced devices configuration** pane, click on **Open configuration form**: a window will open to manage several detector functions
For further information, see detectors manual.

27.4 Register modules

Install each module directly on control unit main board, as shown in its technical manual.
Proceed with registration:
– enter keypad installer menu
– use arrow keys ↑ and ↓ to go to REGISTER MODULES option
– press OK to enter the menu
The already registered modules will be shown: use arrow keys ↑ or ↓ to display them.
– press OK to update modules registration
The installed modules (that are not in the list yet) will be registered.
The modules that are not present anymore will be deleted.
At the end, the unit will beep for confirmation.
– press Stop to exit the menu

27.5 System partition

The control unit can manage up to 64 sectors grouped in areas.
Select grouping mode according to the dimension of the areas to be protected, to the access points of such area, and to the access authorizations planned for users.
– open BrowserOne
– in page **System Options** > **General**, select the operating mode in **Sectors per area mode** drop-down menu
Each zone can be associated to more than one sector.
In **Zones** > **Assign Area/Sector** page:
– select the row of the desired zone
– in column**Area N Sectors**, select sectors of area N to which associate the zone (e.g, if you want to associate the zone to sectors 2 and 3 of area 1, in column Sectors Area 1 check boxes 2 and 3)
When finished, write the configuration to the unit by pressing the relative button in command bar.

27.6 Learn devices to RIVERRF

RIVERRF is compatible with first-generation wireless devices.
It is possible to learn both detectors and remote controls.
Wire RIVERRF concentrator and set its address as indicated in its technical manual.
– enter keypad installer menu
– use arrow keys ↑ and ↓ to go to LEARN RADIO DET. option

– press OK to enter the menu
– use arrow keys ↑ or ↓ to go to the zone desired, or enter the zone number directly
– press OK
– if there is already a detector learned for that zone, press 1 to cancel it or Stop to leave it unchanged
– press OK to start learning a new detector for that zone
– press 2 (wireless detector of Villeggio/Helios system)
– make the detector transmit an event (normally by pressing and releasing tamper button: see the relevant manual)
– wait for the confirmation or error beep sound
– press Stop to exit setup
– press Yes to save configuration, No to cancel changes made
– open BrowserOne
– connect the unit to BrowserOne
– read unit configuration using the dedicated button on the controls bar
– go to page **Zones** > **Radio devices River RF**
– select the grid row corresponding to the zone used to learn the device
– from **Zone Type** drop-down menu, select River Rf
– set supervision time using **Supervision Time** drop-down menu
– in case of remote control devices learning, select the user from the drop-down menu **Associated User**

27.7 Learn devices to GATEWAY2K

GATEWAY2K is necessary for the connection of NG-TRX devices.
Wire GATEWAY2K concentrator and configure it as indicated in its technical manual.
– open BrowserOne
– go to **Peripherals Ultrabus** page
– select the grid row corresponding to GATEWAY2K
– in column **Type**, select "Gateway GATEWAY2K" from the drop-down menu
– write the configuration to the unit selecting the relevant button on command bar
– enter keypad installer menu
– use arrow keys ↑ or ↓ to go to **FAST ACQUIRE** option
– press OK to enter the menu
– press Stop repeatedly to browse among second level items, OK to enter items menu:

▼ **NEW REMOTE?**
Option to learn NG-TRX remote controls.

▼ **NEW SENSOR?**
Option to learn NG-TRX detectors.

▼ **NEW SIREN?**
Option to learn NG-TRX sirens. Sirens have to be set to "Code Self-Learning" mode during learning (coloured jumper kept close).

See programming manual for configuration steps details.
– open BrowserOne
– read unit configuration using the dedicated button on the controls bar
– in page**Zones** > **Radio Devices NG-TRX**, set device parameters
See the detector's technical manual.
When finished, write the configuration to the unit by pressing the relative button in command bar.

27.8 Configure zones

A zone can be connected to a wired or wireless device (detector, contact, etc.).
Wire the device (if wired) or learn the device (if wireless, as indicated in paragraphs 27.6 *p. 77* and 27.7 *p. 78*).
– open BrowserOne
– go to **Zones** page
– select the grid row corresponding to the zone (for example, if you are operating on zone 1 click on row 01)
In **General** tab:
– enter an identifying name in **Zone Name** field
– from drop-down menu **Zone Type**, select the type of connected zone

– in panel **Zone Options**, assign properties to the zone by checking the desired boxes
Example: check **Exit Path** box if you want to include the zone into the exit path set for leaving the area within a set time.

⚠ *For detailed information, please see programming manual.*

– when finished, check **Connected** box to enable the zone
– repeat the procedure for all zones used
To write configuration to the unit, click on the specific button on controls bar.

27.9 Configure users

– open BrowserOne
– go to page **Users** > **General**
– select the row of the user desired (example: the row 01 for the user 01)
– enter an identifying name in **User Name** field
In **User Code** pane:
– click on **Change User Code** to assign a 6-digit code to a user
– flag **Enable code (...) control function**
In **User Options** pane:
– check **Basic Maintenance** to enable access to keypad user menu for the specific user
When finished, write the configuration to the unit by pressing the relative button in command bar.

27.10 Assign sectors to a user

It is possible to associate to each user:
• sectors authorised: sectors that users can set. Users cannot arm/disarm unauthorised sectors.
• sectors proposed: sectors proposed to users for arming during pre-arming time.
– open BrowserOne
– go to page **Users** > **Sectors Authorized/Proposed**
– select the row of the user desired (example: the row 01 for the user 01)
– select sectors authorised and proposed for each area in the dedicated columns
Example: to assign to user 1 sector 2 of area 3 as authorised sector:
– select user row
– click on column Sectors authorised Area 3
– check box 2
To write configuration to the unit, click on the specific button on controls bar.

27.11 Configure outputs

– open BrowserOne
– go to **Outputs** page
– select an output row (example: row 01 if you want to manage output 01)
– assign to outputs a specific function (if needed): select it from drop-down menu **Output function**
Once an output function has been selected, some editable parameters concerning this function may appear at the bottom of the page.
– click on **Logic elaborations editor** to open a graphic editor to create advanced functions
When finished, write the configuration to the unit by pressing the relative button in command bar.

27.12 Learn and configure remote controls

– enter installer menu on keypad (installer code + OK)
To learn non-NG-TRX remote controls:
– use arrow keys ↑ or ↓ to go to **LEARN RADIO DET.** option
– press OK then follow configuration steps
To learn NG-TRX remote controls:
– use arrow keys ↑ or ↓ to go to **FAST ACQUIRE** > **NEW REMOTE?** option or to **LEARN PROXI R.C.** option
– press OK then follow configuration steps
Once the remote control has been learned:

– open BrowserOne
– assign sectors authorised and proposed to the user to whom the remote control is associated, see 27.10 *p. 79* section

27.13 Configure the telephone dialler

– install and register the MD4GE module
MD4GE module supports voice/digital call and SMS texting.
– open BrowserOne
– go to **Telephone Dialler** page
– on tab **General**, select
– on tab **User Telephone Number List**, enter phone numbers to send messages to (up to 16) in column **User Telephone Number**

Enable calls

– go to tab
– flag **Activate Voice Dialler**
– select the row of the event for which the calls will be started
– in column **Associated SMS**, select the message to play during the call (Predefined, or one of 64 messages recordable using the built-in voice synthesis module)
– in column **Voice Phone Numbers Activation**, check the boxes (1 to 32) corresponding to numbers to call for such event
– repeat the procedure for all events desired.

Enable SMS

– go to tab **SMS**
– flag **Activate SMS Transmission Upon Event**
– select the row of the event for which SMS will be sent
– in drop-down menu **Associated SMS**, select the message to be sent for such event (Auto-composed, or one of 64 messages definable in tab Customized SMS)
– in column **SMS Phone Numbers Activation**, check box(es) (1 to 32) corresponding to numbers to send SMS to
– repeat the procedure for all events desired.
When finished, write the configuration to the unit by pressing the relative button in command bar.

27.14 Connect the unit to e-Connect

– open BrowserOne
– go to page **System Options** > **Network parameters**
In **e-Connect** pane:
– select **Enable connection to e-Connect**
– set below parameters
If you are using the built-in Ethernet module: on page **System Options** > **Network parameters**, configure the network options on pane **Ethernet** 1 or 2.
If you are using a 4G module: on page **Telephone Dialler** > **General**, select options and and set the parameters on below panel.
– write the configuration to the unit selecting the relevant button on command bar
– enter installer menu on keypad (installer code + OK)
– use arrow keys ↑ and ↓ to go to INTERNET ACCOUNT option
– press OK to enter the menu
– press 1 to start recording, Stop to exit the menu
– enter registration code (9 digits) received via email for the registration to e-Connect
– press OK
– when finished, the message REGISTERED will appear
– press Stop to exit the menu
– open BrowserOne
– read unit configuration using the dedicated button on the controls bar

27.15 Lock the system

It is possible to lock the system before maintenance sessions or device installation.
– enter installer menu on keypad (installer code + OK)
– use arrow keys ↑ and ↓ to go to SYSTEM LOCK option
– press OK to enter the menu
– press OK to lock the system
The keypad and proximity key reader LEDs will blink and the following message will appear:

SYSTEM LOCK
IDLE

– once done, press Stop to exit this menu and unlock the system

27.16 System test

A system test to check system functioning will be perodically necessary.
The system will propose a system test at defined time intervals (settable, default: 4 weeks).
In order for the test to be completed, at least one zone shall have Walk Test property
This property can be enabled in page **Zones** > **General**, pane **Zone Options**: check **Walk Test** box.
– enter user menu on keypad (user code + *)
– use arrow keys ↑ and ↓ to go to SYSTEM TEST option
The following elements will be fully tested: zones, outputs, dialler.

27.17 Update

Control unit / device firmware update

– open BrowserOne
– in menu bar, select **Tools**
– select **Firmware Update Panel** or **Firmware Update Device**
Follow displayed instructions thoroughly.
See unit or device technical manuals.

Update BrowserOne and modules

– make sure the PC is connected to Internet
– open BrowserOne
– in menu bar, select **Tools**
– select **Software Updates**
In the newly opened window, available updates (both for BrowserOne and the respective modules) are highlighted in red.
– if the unit module is not on the components list, select **Add components**, select the component, then press OK
– click on **Perform Update**

Table of contents

EU DECLARATION OF CONFORMITY

The product complies with current European EMC and LVD directives.
The full text of the EU declaration of conformity is available at the following internet address: www.elmospa.com – registration is quick and easy.

GENERAL WARNINGS

This device has been designed, built and tested with the utmost care and attention, adopting test and inspection procedures in compliance 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:
Multi-functional hybrid control units for intrusion detection 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 components adopted are 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 performedonly 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).

INSTALLER WARNINGS

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.
Work involved in the design, installation and maintenance of systems incorporating this product should be performedonly 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).

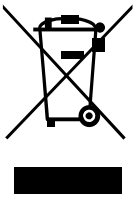
USER WARNINGS

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...)

MAIN SAFETY RULES

The use of the device is forbidden for children and unassisted disabled individuals.
Do not touch the device when bare footed, or with wet body parts. Do not directly spray or throw water on the device.
Do not pull, remove or twist the electric cables protruding from the device even if the same is disconnected from the power source.

DISPOSAL WARNINGS



IT08020000001624

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.
This product needs batteries for correct functioning. Exhausted batteries have to be delivered to dumping grounds authorised for battery collection. The materials used for this product are very harmful and polluting if dispersed in the environment.

EL.MO. Spa - Via Pontarola, 70 - 35011 Campodarsego (PD) - Italy
Ph. +39 049.9203333 - Fax +39 049.9200306 - Help Desk +39 049.9200426 - www.elmospa.com - international@elmospa.com