EL.MO. SPA

USER MANUAL

QHUBO

Wireless intrusion detection system

Q-TX e-Connect

1 DESCRIPTION

QHUBO is a series of multi-functional control units that support wireless devices.
The control units are compatible with:

- all devices using radio technologies Q-TX, Helios and Villeggio;
- all devices using NG-TRX radio technology, after connecting a hardware key CHQ2K.

Among the devices using NG-TRX technology, we would particularly like to highlight:

- actuators, which make it possible to control up to 32 outputs;
- the AURA2K keyboards, which allow to display the system status and limited configuration options (as indicated in the keyboard manual).

Only the QHUBOWF model has an integrated Wi-Fi module.
The control unit manages 4 sectors, allowing each user to only arm or disarm part of the system
The control units can be connected to e-Connect.
QHUBO control units are sold in a plastic housing protected against opening and removal from the wall.
Table-top installation is also possible using the special bracket, in which case the control unit loses its protection against removal from the wall.

Manual contents

2 FRONT LEDS

The three front LEDs indicate the operating status of the control unit.
In the order from left to right:

Green LED: input status

- On: no input in alarm/tamper status. The control unit can be armed.
- Off: at least one input not belonging to the exit path is in alarm.
- Flashing: the control unit is armed and at least one input belonging to the exit path shows an error; or at least one input is in alarm/tamper status but is generating an event other than an intrusion alarm.

Yellow LED: error status

- On: no errors. It is possible to ask the installer to set the control unit up so that the LED remains off in the absence of faults.
- Flashing: system fault (power failure, low battery, tamper open, error, etc.) or input fault. For information on how to view active faults, see 9.1 *p. 5*.

To reset memories, arm and disarm the system.

Red LED: arming status and alarm and tamper memory

- Off: system disarmed.
- On: system armed.
- Flashing: alarm or tampering alarm detected.

To reset memories, arm and disarm the system.

2.1 LED indicators

LED signals are also reproduced on any connected keyboards.

The meaning of the green (1) and yellow (2) LEDs is the same, but there are two separate red LEDs, one for alarm signalling (3) and one for fault signalling (4).

3. General alarm LED

It indicates general alarm.
- **OFF**: no alarm events.
- **ON**: alarm in progress (active relay).
- **Flashing**: alarm detected.

To reset memories, arm and disarm the system.

4. Tamper LED

It indicates tamper status.
- **OFF**: no tampering zones.
- **ON**: tamper alarm in progress (active relay).
- **Flashing**: tamper alarm detected.

To reset memories, arm and disarm the system.

3 GENERAL INFORMATION ON SYSTEM ARMING

In the configuration, the following may be assigned to each user:
- a user code, used for keyboard arming and disarming;
- a proximity key, used for keyboard arming and disarming;
- a remote control, used for remote arming and disarming (no keyboard required);
- a list of proposed sectors, used for partial arming using the remote control, keyboard or proximity (key) reader.

Partial arming procedures, which allow to only arm certain sectors, are detailed in the chapters on the use of remote controls, keyboards and proximity (key) readers.
Arming and disarming are confirmed by an acoustic signal emitted by the control unit.

⚠ *The control unit detects unauthorised access attempts: if within a arming/disarming cycle more than 20 attempts are detected (non-recognised keypad/key/remote control/remote access codes) the event* **Maximum access attempts exceeded** *will be generated. More consecutive access attempts with the same code will be counted as one.*

3.1 Exit path

In the configuration, some inputs may be included in an **exit path**.

After arming the system, the user can leave the premises within a set time **(exit time)** and walk the exit path without an alarm being generated.

3.2 Panic event

During the configuration, it is possible to make sure that the control unit triggers an alarm when certain keys of the keyboard or remote control are pressed at the same time.
This occurrence is recorded in the log as **Panic alarm**, with an indication of the generating keyboard or remote control.

3.3 Arming lock or forced arming

During the configuration, it is possible to set the arming lock function.
While the function is active, any request to arm the system made with the system showing an alarm or a fault will be denied.
For example, if a window protected by a magnetic contact is open, the control unit will prevent arming, rather than arm the system and then immediately detect an alarm situation.

⚠ *Bypassed detectors will not cause system lock.*

In order to be able to arm the system:
– resolve alarm or fault situations (possibly excluding the device concerned)
– repeat the arming procedure

System forced arming

If the arming lock was due to a dialler fault or lack of supervision, arming can be forced.
The forced arming procedures for arming required by a user are detailed in the chapters on the use of remote controls, keyboards and proximity keys.
If arming is done remotely using the software or by the hourly programmer, forced arming occurs automatically.
Forced arming will not be allowed in case of zones with anomaly events.

4 KEYPADS USAGE

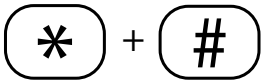
Control units QHUBO can be connected to keyboards VELAPLUS.
Control units QHUBO with key CHQ2K can be connected to keyboards AURA2K.
For a list of the available menus and functions, see the specific keyboard manual.
The meanings of the signalling LEDs are given in paragraph 2.1 *p. 2*.

Note: as the control unit only manages a single area, keyboards set as system keyboards show the arming status of the sectors and not of the areas.

4.1 Operating mode from keypad

Before proceeding, please see arming general information (paragraph 3 *p. 2*).
Arming and disarming operations are described in the keyboard manual.

4.1.1 Panic event



– Press keys * and # on keypad simultaneously.

4.1.2 System forced arming

If forced arming is possible, keyboards with display the "FORCED ON?" message.
– Press **OK** within 15 seconds to start forced arming, **STOP** to cancel it.

5 PROXIMITY KEYS USAGE

Proximity keys can be used to quickly arm and disarm the system. Simply bring them close to the readers on the keyboards.

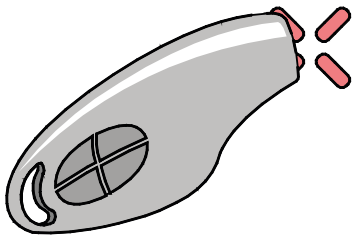
⚠ *The keys shall be registered to the control unit.*

5.1 Proximity keys usage

Before proceeding, please see arming general information (paragraph 3 *p. 2*).

5.1.1 System arming

– Place the proximity key on the reader.



– Wait for the arming LED to come on (continuous flashing).
– Leave the protected areas within the set time (if any has been set) walking through the path set.

When exit time elapses, the unit status LED will light up.

5.1.2 Disarming

When system is armed:
– Place the proximity key near the sensitive area onto reader.
– Wait a few seconds until the unit status LED switches OFF.

5.1.3 System forced arming

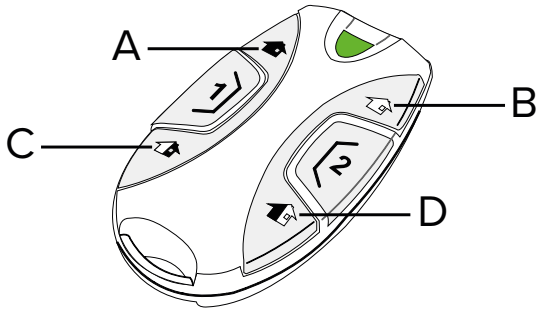
If forced arming is possible, keyboards with display the "FORCED ON?" message.
– Within 15 seconds, move the proximity key close again to force arming.

6 REMOTE CONTROLS USAGE

Remote control devices can be used to arm (either totally or partially) and disarm systems.

6.1 Function keys

The picture refers to the ATLANTE-Q model.



A Key "TOTAL ARMING"
B Key "TOTAL DISARMING"
C Key "PARTIAL ARMING 1"
D Key "PARTIAL ARMING 2"

During the configuration, it is possible to customise the keys so that they arm and disarm specific sectors.
Please refer to the manual of the remote control in use for information on keys and LED indications.

6.2 Operation with remote controls

Before proceeding, please see arming general information (paragraph 3 *p. 2*).

6.2.1 System arming

To arm the system, press one of the following keys:
- "Total arming" (A): arms **all sectors**
- "Partial arming 1" (C): arms **sectors proposed** for the user
- "Partial arming 2" (D): arms **the sectors not proposed to the user**

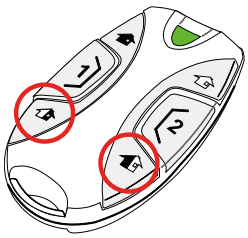
⚠ *For some remote control models, the installer can*

customise the "partial arming 1" and "partial arming 2" buttons so that each one arms/disarms specific sectors (instead of the proposed or not proposed sectors respectively, as set by default).

6.2.2 Disarming

– Press "total disarming" (B) key.

6.2.3 Panic event



Press and briefly hold the "partial arming 1" (C) and "partial arming 2" (D) buttons together.

6.2.4 System forced arming

– Press the desired arming key again within 15 seconds.

7 PHONE COMMUNICATIONS

The GSM or LTE module integrated in the control unit allows connection to the GSM-GPRS or LTE network, for sending voice messages and SMS.
If the system is disarmed while multiple telephone calls are being sent, any calls that have not yet been sent will be cancelled.

7.1 Calls reception

Users will receive calls or SMS texts when specific alarm events occur (defined during setup.)
Events can also be used for transmissions to surveillance centres.
When users receive a phone call, they can use one of the following keys on the phone keypad:

5	The call is interrupted, the unit will call the following number (if set).
0	The call is interrupted, the unit will not call other numbers until a new event occurs.

7.2 Receiving SMS from control units

During configuration it is possible to activate SMS sending upon events (alarms, arming/disarming commands, anomalies).
Users with their phone number on the list will receive a SMS text from the unit upon occurrence of such events.
SMS texts contain information on system status.
The unit can send maximum 1000 events / day.
During configuration, it is possible to also configure some "forwarding numbers", to which the control unit will forward any SMS messages (e.g. SMS sent by the mobile network operator).

7.3 Limits to dialler activations

Installers can program the control unit so that it limits the number of events that trigger the dialler.
When the max number is reached, the voice/SMS dialler ignores other calls until the next day.
This function is available in **Telephone Dialler** menu in BrowserOne.

⚠ *Limits refer to events, and not to calls: the amount of calls can be higher if events cause several calls. Moreover, the limit refers only to voice dialler and not digital dialler.*

For the **Low battery** event, using the software it is also possible to set a limit on the number of calls (both voice and digital) caused by the same.
In addition, such events will activate the dialler only if there are no discharged battery memories for the relevant device.

8 DIAGNOSTICS

In case of anomalies, the yellow LED indicator on keypads or readers will keep blinking.
To view faults...

- using keyboards AURA2K, please refer to the keyboard manual;
- using the supervision software, see chapter 9.1 *p. 5*.

Below messages that may be displayed.

ANOMALY	CAUSE
ANOMALY Low Battery	The battery charge is low or the battery is missing.
ANOMALY Mains Failure	Mains failure: the unit is powered by the battery only.
ANOMALY No GSM Registr.	SIM card missing or disabled, or PIN code active.
KEYP/RD TAMPER Keyp./Reader #	Keypad or reader (the number of which is indicated) signals a tamper event.
ANOMALY Sensor low volt.	One sensor (or more) is not powered correctly. Power voltage is below set threshold.
ANOMALY Sound. low volt.	One siren (or more) is not powered correctly. Power voltage is below set threshold.
ANOMALY R.C. Low Battery	One remote control (or more) signals low battery.

9 SUPERVISION SOFTWARE

e-Connect is a supervision services platform for EL.MO. intrusion detection systems.
e-Connect allows users to control and manage their systems via the Internet, a PC or a smartphone application.
Operations with e-Connect software:

- check control unit status (anomalies, tamper events,

alarms)
- arm / disarm procedures
- read events log
- enable/disable outputs

There are two types of e-Connect accounts: managed accounts and stand-alone accounts.

⚠ *A 9-digit numerical code is generated during the creation of the account, which the installer must enter in the programming software while connected via USB cable to the control unit; therefore, the account must be created before the installer completes the first programming of the control unit.*

Managed account

- It can only be offered by installers who use the e-Connect platform themselves;
- it is usually offered as part of a maintenance contract;
- the account is created by the installer, who provides the user with the credentials for first-time access and their own **installer profile name**;
- changing the time zone, deleting the log or updating the control unit details require the intervention of the installer;
- the installer can update the firmware remotely.

The user can perform supervision activities logging in...

- a web browser, going to connect.elmospa.com/**installer-profile-name**;
- the app e-Connect.

The e-Connect app:

- is compatible with Android and iOS operating systems and can be downloaded from their respective stores;
- it allows the management of intrusion, fire and video surveillance systems, storing the access credentials;
- it allows the creation and import of e-Connect accounts connected to EL.MO. intrusion and fire detection control units;
- it allows the association of e-Vision video surveillance systems to DVR and NVR accounts;
- it lists the accounts created or imported, allowing access to the account interface without having to enter the credentials;
- it lists DVRs and NVRs, allowing access to the video surveillance system monitoring interface;
- it provides push notifications of alarms and InstaVision video verification, which forwards video recordings of the alarm event to the app.

Stand-alone account

- It can be offered by any installer;
- allows all controllable parameters to be changed independently;
- the account is created directly by the user, either by using the appropriate command in the app or by pressing Register on the website;
- updating the control unit requires on-site intervention by the installer (remote support is not available).

The user can perform supervision activities logging in...

- from connect.elmospa.com/qhubo on a web browser;
- using the free app MYQHUBO

The MYQHUBO app:

- is compatible with Android and iOS operating systems and can be downloaded from their respective stores;
- it allows the creation and import of e-Connect accounts linked to QHUBO control units;
- it lists the accounts created or imported, allowing access to the account interface without having to enter the credentials;

The MYQHUBO app does not provide push notifications; it is recommended to ask the installer to enable SMS notifications directly from the control unit.

9.1 Instructions for the use of apps and websites

App for managed accounts

To use the e-Connect app, please refer to the Intrusion Detection app manual, available for download from the product page of e-Connect at www.elmospa.com.

App for stand-alone accounts

For the use of the MYQHUBO app, please refer to chapter 10 *p. 6*.

account interface

The account interface is the screen that can be reached by tapping one of the accounts listed in the app or by logging in to the websites listed in Chapter 9 *p. 4*.

Instructions on how to use the interface can be found in the e-Connect user manual, which can be downloaded from the e-Connect product page at www.elmospa.com.

In addition to what is described in that manual, the Account Options menu (top right) contains the following items, which can only be accessed after logging into the control unit:

▼ **Change user code**

It allows to change the 6-digit code used to access the control unit.

▼ **Edit user name**

It allows to change the name assigned to the control unit access code, which is displayed on the remote control page and in the log.

If any items are selected without first logging into the control unit, the control unit's login interface appears immediately, as if the **Login** button had been pressed.

The navigation menu contains the following additional pages:

▼ **Remote controls**

It lists the remote controls assigned to users, identified by the user name.

▼ **Peripherals**

It lists the devices connected to the control unit.

The Inputs, Remote Controls and Peripherals pages have a Status column with short descriptions of the current types of errors (yellow border) or faults (red border).
The colours match those of the control unit's LEDs.
Since narrow screens initially do not show all the columns, the field containing the name of the input, remote control or peripheral device shows a yellow "sad face" icon in case of error, and red scissors in case of fault.
A list of possible errors can be found in Chapter 8 *p. 4*.
Click or tap the + symbol at the beginning of the line to expand the line and display the status description.
Error and fault reminders are listed on the **Log** page.

10 MYQHUBO

The MYQHUBO app allows to manage the QHUBO series control units registered on the e-Connect platform.
In particular, it allows to:

- create a new account and generate the key to be communicated to the installer for registration (**Create a new account**, chap. 10.3 *p. 6*);
- import existing accounts (**Import account**, chap. 10.3 *p. 6*);
- access the interface of the accounts created or imported, for the supervision of the intrusion detection system.

During the creation of the account, select the credentials (username and password) required to access the account from both the app and the website.
When importing the account, it will be necessary to enter the credentials of the account to be imported.
In both cases, the credentials are stored in the app, allowing access to the account without having to enter them again.
If the account credentials are changed from the account interface (that can be accessed from connect.elmospa.com/qhubo), the credentials saved in the app must be updated manually: **Edit account** (Chap. 10.6 *p. 7*).
Access to the accounts from apps may require biometric authentication: **Log in with biometric authentication** (ch. 10.6 *p. 7*).

10.1 Installation

– download the app from the Android or iOS store
– install the app

10.2 Startup

– tap the app icon

If biometric authentication has been enabled (see 10.3 *p. 6*), this will be requested when opening the app.
At the first access, it will be necessary to allow this type of authentication using the "Settings" menu (or similar) of the smartphone.

⚠ *The available authentication type (fingerprint, face recognition etc.) depends on the used device.*

10.3 General menu

To access the general menu, tap the ⋮ icon at the top right, next to the app name.

▼ **Create new account**

It allows to create a new account to be connected to a QHUBO series control unit.
Once the account has been created, a nine-digit code will automatically be sent to the indicated e-mail address, to be forwarded to the installer, who will then enter it in the control unit.
This also creates a profile within the app (see chapter 10.5 *p. 7*), already set up with the chosen credentials.

▼ **Add existing account**

It allows to create a profile in the app or import into the app an account already stored in another Android or iOS device.
In this way, it is possible to grant access to supervisory functions to several different people, e.g. all family members.

▼ **Manuals**

It allows to download an up-to-date copy of this manual or the e-Connect website interface manual.
Only open the manuals you need, in order not to exceed in data consumption.

▼ **Settings**

It opens the settings menu (chap. 10.4 *p. 6*)

▼ **Privacy**

It shows the privacy policy of the app.

10.4 Settings menu

▼ **Change page with slide**

It allows switching between pages of the account interface by swiping your finger to the right or left.
Disabled by default.

▼ **Enable PIN**

It allows setting a PIN code for APP access.
Disabled by default.
The code will be required when activating the function.

▼ **Biometric authentication**

It allows setting APP access through biometric authentication.
This mode is an alternative to PIN insertion.
Disabled by default.
The available authentication type (fingerprint, face recognition etc.) depends on the used device.

▼ **Edit Server**

Edit server (e-Connect server address).

▼ **Language**
Select language in drop-down menu.

▼ **Feedback and Suggestion**
Send suggestions to the developers.

▼ **About**
It displays application information

10.5 Account list

Each account created or imported as seen in the general menu (chap. 10.3 *p. 6*) is represented by a rectangular icon (profile) containing a profile picture and user name.
Tap on the ⋮ icon on the right of the profile to access the profile customisation menu (see chapter 10.6 *p. 7*).
Tap on the rest of the profile to access the account interface.
The interface that opens is the same as the one accessed from the connect.elmospa.com/qhubo website.

10.6 Account menu

▼ **Edit account**
This screen can be used to change the credentials that the app uses to connect to the control unit's account in the e-Connect platform.
If the credentials do not match those already in the account, the connection will fail.
Use the screen to correct any wrong credentials, to update the credentials, or enter data from a different account.
To change accounts e-mail or password, go to the account interface (that can be accessed from connect.elmospa.com/qhubo).

▼ **Delete account**
It removes the account from the app.
This operation does not deactivate the account

▼ **Set profile image**
Choose an image from the gallery.

▼ **Set as default account**
There can be only one default account at a time.
A yellow star appears in the account pane.
Such account will immediately be opened when starting the APP.

▼ **Login with biometric data**
Activating this function causes the app to request biometric authentication when logging in.
The available authentication type (fingerprint, face recognition etc.) depends on the used device.

11 ENERGY SAVING

Installers can activate functions for energy saving:

▼ **Yellow LED OFF when there are no anomalies**
The yellow LED will be off (at keypads and readers connected) when there are no anomalies.

▼ **Disable GSM**
If QHUBOWF is connected to a WiFi network, the GSM module can be switched off.

12 ACOUSTIC SIGNALS

Installers can customize acoustic signals.

▼ **Buzzer Volume for arming/disarming**
The buzzer volume can be adjusted for arming and disarming commands: **Normale**, **Attenuato** and **Spento**.

▼ **Built-in Siren Activation Status**
It is possible to select which events will trigger the built-in siren and set different volumes.

13 PARTS CLEANING

Clean the unit and the keypads with a damp cloth, using suitable non-corrosive cleansers.
Do not spray any liquid substance directly on the case.

EU DECLARATION OF CONFORMITY

Hereby, EL.MO. Spa declares that the radio equipment QHUBO / QHUBOWF is in compliance with Directive 2014/53/EU.
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:
Wireless intrusion detection system.
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).

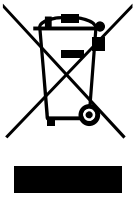
USER WARNINGS

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