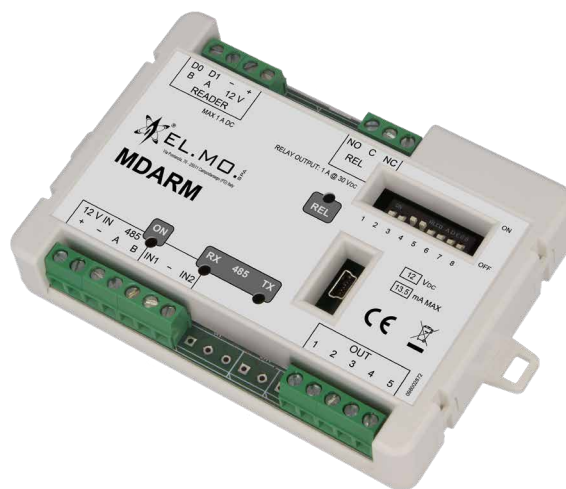


MDARM

**Arming module on RS-485 serial line
for intrusion detection systems to be
used with an external reader**



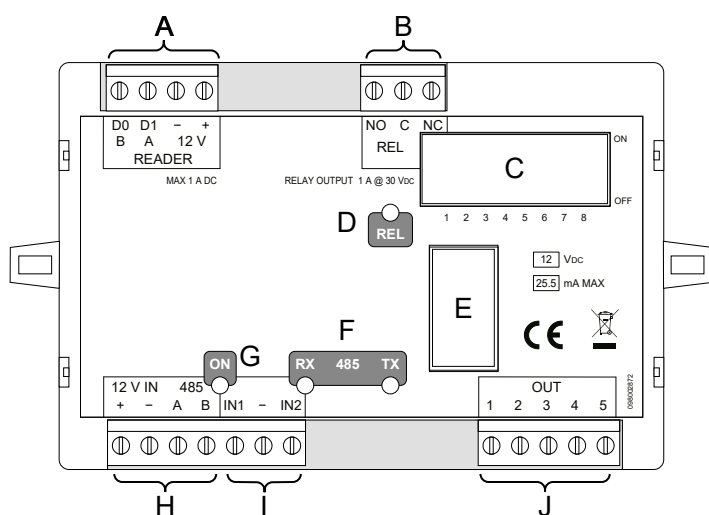
Addressee for this information: User | Installer

1 DESCRIPTION

MDARM allows arming and disarming an intrusion detection system using the same user identification method used by the access control system.

If the intrusion detection unit to which MDARM is connected supports access-enabled users, it can also be used to temporarily arm and disarm its gate.

MDARM and the access control system use different sets of Wiegand readers.



- | | |
|-------------------------------|---------------------------------|
| A Reader serial line* | F Serial status LEDs |
| B Relay outputs | G Power ON LED |
| C Dip switch selectors | H ULTRABUS serial line |
| D Relay status LEDs | I Zones |
| E USB port | J Open collector outputs |

* The product with code OCMIN0100100 is only compatible with Wiegand readers equipped with an internal pull-up on their communication lines, products with different codes are also compatible with Wiegand readers without internal

pull-ups.

MDARM is compatible with intrusion detection systems that use the ULTRABUS serial line.

2 TECHNICAL DATA

Model	MDARM		
General features			
Operating voltage	Power supply	12	V
	Consumption at power voltage		
	Idle mode	8.0	mA
	Maximum	14	mA
O.C. output maximum current		30	mA
Working temperature		-10 ÷ +55	°C
Relative humidity		max 93%	
Fixing centre distance		120.0	mm
Dimensions		W 129 × H 80 × D 20	mm
Weight		103	g


Parts supplied: technical manual.

3 INSTALLATION

 General warnings are at the end of this manual.

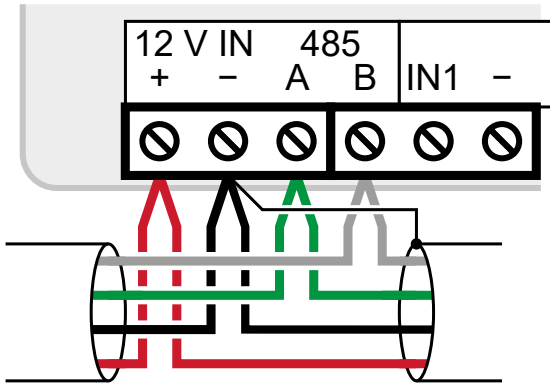
MDARM is designed to be installed in a box (e.g. a junction box) equipped with protection against opening carried out by the installer.

3.1 Wirings

 Wire devices while they are disconnected from power/mains.

! Make sure to be free of static charges and take all precautions needed to safely install MDARM.

3.1.1 Serial line wiring

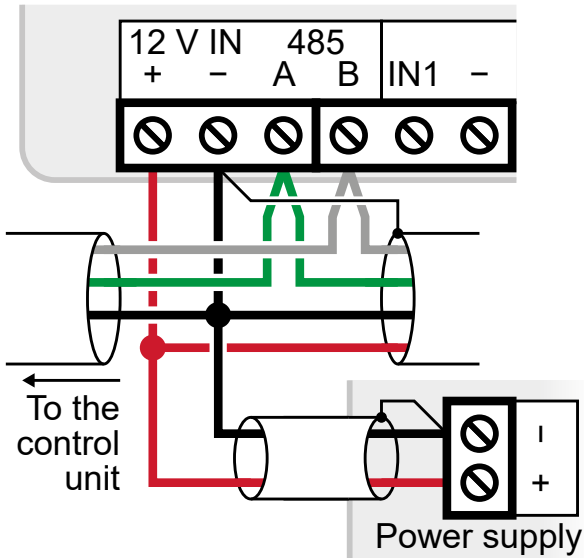


– wire detector power and serial line terminals
Use shielded cables with the following section: $2 \times 0.75 \text{ mm}^2$ (power) + $2 \times 0.22 \text{ mm}^2$ (signal).

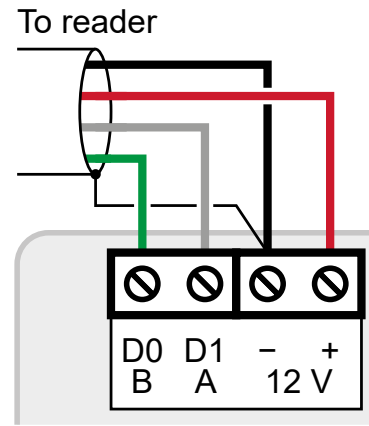
The serial line may be extended with branches, provided that the following rules are followed:

- the sum of the lengths of the branches must not exceed 1 km;
- 680Ω termination resistors must be connected to the ends of the two longest branches.

As an alternative, MDARM and all following devices can be powered by a power supply box wired as shown below.



3.1.2 Reader connection

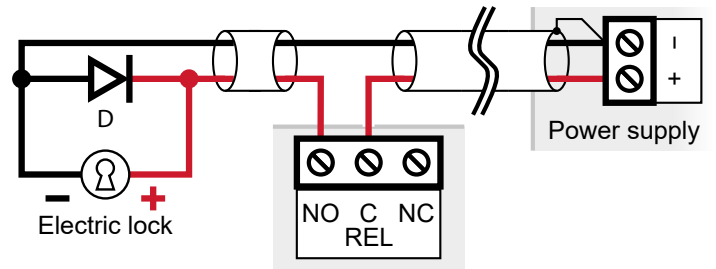


– see ch. 3.2 p. 3 for reader type configuration

3.1.3 Relay output wiring

Only carry this connection only if you want to use the Gate control function (ch 7.1 p. 6).

The REL output controls the electric lock that unlocks the gate.



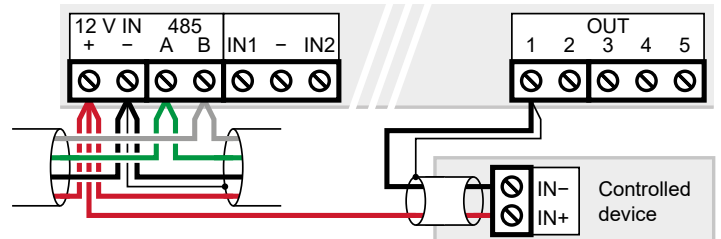
D = 1N4007 flyback diode to protect MDARM from the inductive voltage pulse.

3.1.4 Open collector output wiring

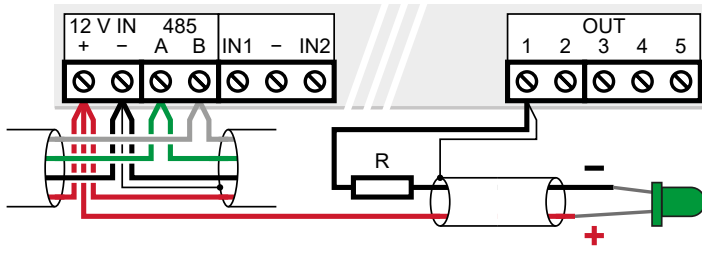
Outputs are assigned to the following functions:

1	Alarm or tamper alarm status
2	Anomaly status
3	Armability status
4	Arming state
5	Follows the activation of the buzzer

All outputs connected like shown for output 1 in the diagram.

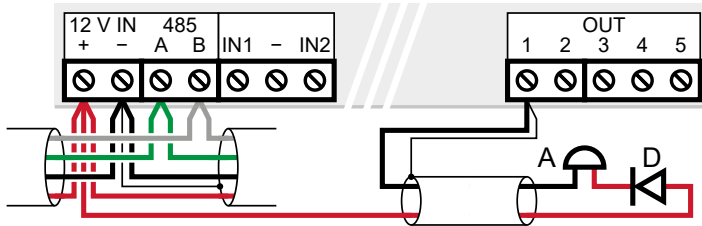


Example: LED control



R = Resistor suitable to protect the chosen LED

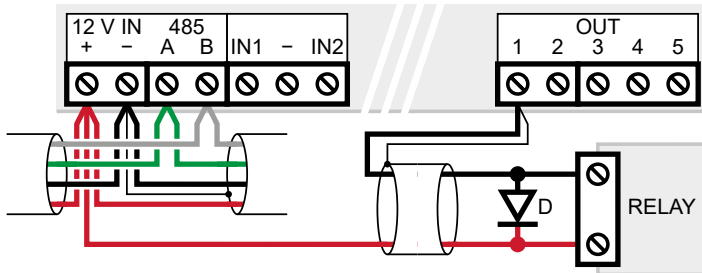
Example: sounder control



A = sounder

D = 1N4001 diode (if not built-in in the sounder)

Example: control of a relay (or other inductive load)



D = flyback diode to protect MDARM from the inductive voltage pulse. Only connect relays that can function with a command current of 25 mA or less.

3.2 Dip switches meaning

1-5: address setting

Device	DIP ON	Device	DIP ON	Device	DIP ON
1	-----	2	1----	3	-2---
4	12---	5	--3--	6	1-3--
7	-23--	8	123--	9	---4-
10	1--4-	11	-2-4-	12	12-4-
13	--34-	14	1-34-	15	-234-
16	1234-	17	---5	18	1---5
19	-2--5	20	12--5	21	--3-5
22	1-3-5	23	-23-5	24	123-5
25	---45	26	1--45	27	-2-45
28	12-45	29	--345	30	1-345

Device	DIP ON	Device	DIP ON	Device	DIP ON
31	-2345	32	12345		

6-8: other functions

Dip switch	ON	OFF
6	IZENITH	I8
7	34 bit Wiegand	26 bit Wiegand
8	PIN required	PIN not required

MDARM is seen by the control unit as either an IZENITH reader or as an I8 one.

The two types of reader use two separate address classes, i.e. IZENITH 1 is a different address than I8 2 (and so on).

The on-board buzzer only works if MDARM is in IZENITH mode.

MDARM in IZENITH mode can be programmed to arm/disarm the chosen areas only.

MDARM in I8 mode can be programmed to arm/disarm the chosen sectors only.

Only use the **PIN required** function with readers featuring a keypad.

3.3 Programming

BrowserOne is the configuration software of the intrusion detection system.

It is used for:

- link card codes to the users of the intrusion detection system and to their arming and disarming authorisations
- open the stand-alone TBSManager interface, which allows the configuration of MDARM's readers via USB, even before having connected MDARM to the system;

Once MDARM has been connected to the serial line (ch. 3.1.1 p. 2) BrowserOne can be also used to:

- choose which areas or sectors can be armed from each MDARM;
- enable the access-enabled user function that allows a user to temporarily disable an input protecting a passage.

Programming operations:

- open BrowserOne software
- update BrowserOne to the latest version available
- in order to program readers via USB, follow ch. 5 p. 4.
- to perform the remaining programming, even remotely, follow chapter 3.3.1 p. 3.

3.3.1 Configuration via browser

MDARM must be connected to the serial line (ch. 3.1.1 p. 2).

- load the latest module available for the control unit in use
- start control unit connection
- select **Read setup** key to read control unit setup
- go to **Control devices** page

For each MDARM:


- set the I8 or IZENITH type according to the position of dip switch 6
- choose which sectors or areas can be armed and disarmed using MDARM

In I8 mode, sectors can be selected.

In IZENITH mode, areas can be selected.

Gate control function

- update MDARM to the latest version available (ch. 6 p. 5)

 *The gate control function requires using a control unit that manages it, e.g. ETR, TITANIA or PROXIMA.*

In the context of this function, a passage is a door or a gate which is protected by a **24H** zone (alarmed even while the system is not armed) that is also referred to as **Passage**.

If an user with the **Access-enabled user** property authenticates at a MDARM which has been assigned to a passage, instead of arming/disarming the system MDARM temporarily disables the passage zone, making it possible for the user to open the passage and to keep it open for a predetermined time without triggering an alarm.

- open the **Keypad options** tab.
- in the **Passage 1** column, select the passage zone address
- In the **Max opening passage** column, set the time after which the gate must be closed or the gate opening request must be renewed
- go to **Users** page
- flag the **Access-enabled user** option of each user you want to authorize

If one or more individuals need to be able to both use the passage opening function and the arm/disarm function, they will have to use two different cards/codes (one for each function).

For each of those individuals:

- create two separate users in BrowserOne
- only authorise one of those two users to open the passage
- give the individual both cards or codes; they will use one to open the passage and one for disarming/arming the system

Alternatively, for PROXIMA control units only, it is possible to change the arming/disarming procedure, making it possible to perform both operations with a single card.

- open BrowserOne's **System options** page
- enable the general option **Enable disarming/arming with door opening**

All users, including those without the **Access-enabled user** flag, will have to pass the card thrice in order to disarm/arm the system.

4 DIAGNOSTICS

The first diagnostic operations consist in analyzing the LEDs

on MDARM's front.

To get more information, access to the TBSManager software is required (ch. 5 p. 4).


4.1 LED indicators

LED	Colour	Condition	Indication
ON	Green	Standard operating mode	Steady light
		Firmware update in progress	1 flash every 1 s
		Missing power supply	OFF
485 TX/RX	Red	Serial line transmission/reception	Blinking
REL	Yellow	Output enabled	Steady light
		Disabled output	OFF

5 TBSMANAGER

TBSManager is MDARM's diagnostics and configuration software.

- open BrowserOne software
- update BrowserOne to the latest version available

 *If MDARM is already connected to the control unit via ULTRABUS, activate the control unit's **system lock** before opening the box protected by the tamper and before connecting the USB cable.*

- connect the PC to the USB port of MDARM using an USB Mini-B cable 1 m long at most
- update MDARM to the latest version available (ch. 6 p. 5)

The 5 V power from the USB connection is enough to power MDARM but not the readers.

Reader diagnostics requires that MDARM is powered at 12 V (12 V IN terminals).

5.1 General

The window provides information on the device, on its configuration and addressing.

Info panel

Shows information about the connected device (type, firmware version, bootloader version).

It is normal that, if MDARM is powered through USB, the power parameters are too low..

DIP configuration

Shows the address and the current settings corresponding to the position of the onboard dip switches.


Each configuration variation will be shown in real time.

5.2 Setup

▼ Protocol
Normal: checks the parity bit (default).
No parity: does not check the parity bit.
▼ Enable keypad code
Enable this option to allow the user to input their card code by typing it manually on the reader's keypad.
▼ Load Default
Resets all parameters of this section to their default values (normal protocol , keypad code disabled).
▼ Read Configuration
Read the configuration data stored in MDARM and show it in this screen.
▼ Write Configuration
Writes the configuration data shown in this screen to MDARM.

5.3 Reader

This page is used to perform reading tests.

 *Reading tests can only be performed if the PIN mod is disabled: set dip 8 to OFF while testing.*

The test requires that MDARM is powered at 12 V (12 V IN terminals).

– input the coding, number and revision of the card used for testing and move it close to the reader

If the card gets read, the **Reading** icon lights up.

If the card matches the stated number and revision, the **Correspondence** icon also lights up.

– once the test has been performed, press **Seen**

if the reader has a keypad, typed digits will appear in the **Last key pressed** row.

Below the Wiegand code (decimal value that can be copied to paste it in BrowserOne) and the received code (equivalent hexadecimal code) are shown.

5.4 Zone status

This page contains diagnostic tools.

– activate the button or magnetic contact of the circuit and check that the **Status** and **Resistance** columns change as expected

5.5 Outputs control

This page allows checking the activation status of the outputs.

You can also click on the output names to activate or deactivate them.

The **Shutdown** column lets you limit the duration of the activation to the stated number of seconds.

6 FIRMWARE UPDATE



The following update modes are available:

1. **Update via BrowserOne in RS-485 connection:** it can be performed remotely, even via e-Connect, and it allows to automatically update several devices sequentially.
2. **Update using BrowserOne via USB:** it allows the update before the installation, powering up the device via USB.
3. **Update using TBSManager via USB:** it allows the update before the installation, powering up the device via USB.

We recommend performing the update with system locked or disarmed, to avoid alarm signalling in some situations.

If an update attempt does not end properly (for example, because of a disconnection during the update), the device will not lose its operativity.

Nevertheless, tamper signalling may be sent if the update procedure is not completed within 10 minutes, with reset once the update has been properly concluded.

6.1 Firmware update via BrowserOne and RS-485

It requires the connection of the control unit to BrowserOne and the connection of the device over serial line.

- open BrowserOne software
- update BrowserOne to the latest version available
- load the latest module available for the control unit in use
- start control unit connection
- select **Firmware update device** in **Tools** menu
- select "Bus 485" then press **Next**
- in the window displayed select the device to be updated:
 - in drop-down menu select the model

Note: choose the model according to how you position dip switch 6 (ch. 3.2 p. 3).

- click on **Next**
- the software application will search for all that type of devices connected over serial line: select the device to be updated on the list, then select **Next**

Note: If some MDARM are in IZENITH mode and some are in I8 mode the update must be repeated twice, once per mode.


Select the update file in the displayed window.

Select the download path:

- select **Sync with online archive** to download the file from a network archive: in the window displayed, select the update file then click on **Ok**
- click on **Browse** to select an update file already stored on the PC: find it and select **Open**
- click on **Next** to continue
- a summary window will open: select **Next**
- follow displayed instructions until the confirmation message pops up
- press **Update another device** to update another device, press **End** otherwise

6.2 Firmware update via BrowserOne and USB

It demands direct connection of the PC to the device.

 *If MDARM is already connected to the control unit via ULTRABUS, activate the control unit's **system lock** before opening the box protected by the tamper and before connecting the USB cable.*

- use a USB-MiniB cable to connect the device to a PC equipped with BrowserOne software
- open BrowserOne software
- update BrowserOne to the latest version available
- select **Firmware update device** in **Tools** menu
- select "USB" then press **Next**
- in the window displayed select the device to be updated: in drop-down menu select the model


Select the update file in the displayed window.

Select the download path:

- select **Sync with online archive** to download the file from a network archive: in the window displayed, select the update file then click on **Ok**
- click on **Browse** to select an update file already stored on the PC: find it and select **Open**
- click on **Next** to continue
- choose "Standard" update mode
- click on **Next** to continue
- select Virtual COM serial port to which USB Mini-B cable is connected to (if such port is not listed, select update icon) then select **Next**
- a summary window will open: select **Next**
- the communication will start and the device will be updated: select **Next**
- press **End**

6.3 Firmware update via TBSManager

It demands direct connection of the PC to the device via USB.

 *If MDARM is already connected to the control unit via ULTRABUS, activate the control unit's **system lock** before opening the box protected by the tamper and before connecting the USB cable.*

- use a USB-MiniB cable to connect the device to a PC equipped with BrowserOne software
- open BrowserOne software
- update BrowserOne to the latest version available
- go to **Tools > Run TBSManager** menu
- click on **Connect**
- on window top bar, click on **Update > Firmware**
- click on **Ok** button
- click on **Select** button

A window will appear that allows to select the path where the update file is located.

If a firmware update has already been performed before via RS-485 and option **Sync with online archive** was selected, the list of the available files can be found at this path.

C:\Users\user_name\Documents\BrowserOne\Download\Firmware\Devices

In case you got the update file in another way (e.g. downloading it from MDARM's product page on the EL.MO. website), select the path where it is located.

- select the update file and click on **Open**
- click on **Update** button

If the update is successful, the relative message will appear.

6.3.1 Emergency update

If the Connect button of TBSManager in direct connection mode does not work or does not appear, you can try performing an emergency firmware update.

- on TBSManager's top bar, click on **Update > Emergency**
- click on **Select** button
- select the update file and click on **Open**
- click on **Update** button

7 USE



To arm or disarm the system, authenticate yourself at the reader.

Authentication

The authentication procedure depends on the reader model that has been installed.

For instance:

- by placing a key card near to the reader;
- typing the card code, followed by "#", on the reader's keypad*;
- by placing a proximity key near to the reader;
- by placing a token or a tag near to the reader;
- by placing a smartphone near to the reader that communicates the key code using a wireless transmission technology;
- by showing to the reader's camera a specifically generated QR code;
- in any of the previous ways followed by typing a PIN on the reader's keypad.

*Requires activating the **Enable keypad code** function of MDARM (ch. 5.2 p. 5). The card code can be typed without the leading zeroes, e.g. 437020# instead of 00437020#. On systems based upon PROXIMA control units with the **Enable disarming/arming with door opening** option enabled, users with the **Access-enabled user** function enabled need to perform the authentication thrice in a row to arm the system.

7.1 Gate control function

Note: this function is only available if MDARM is connected to a control unit that has it

The gate control function temporarily authorizes the opening

of a gate which is normally monitored even while the system is disarmed.

- place a key card (or other identification device) specifically enabled for gate control near to the reader

The electric lock activates, making it possible to open the gate without generating an alarm.

The gate can stay open for the time chosen while programming the system.

An acoustic signal warns that the opening timer will expire in 10 seconds.

If the timer expires while the gate is still open, the control unit enters the alarm state.

- In order to reset the timer and lengthen the time available, bring the key card next to the reader again.

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:

Arming module on RS-485 serial line for intrusion detection systems to be used with an external reader

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 performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the mains and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply.

If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

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

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

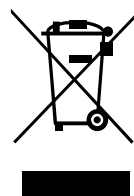


The use of the device is forbidden for children and unassisted disabled individuals.

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.