# Alarm Controller

## User’s Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V2.0.0

# Foreword

## General

This manual introduces the installation, functions and operations of the alarm controller (hereinafter referred to as "controller"). Read carefully before using the device, and keep the manual safe for future reference.

## Models

DHI-ARC3008C

## Safety Instructions

The following signal words might appear in the manual.

| Signal Words | Meaning |
|---|---|
| ⚠ DANGER | Indicates a high potential hazard which, if not avoided, will result in death or serious injury. |
| ⚠ WARNING | Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury. |
| ⚠ CAUTION | Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results. |
| TIPS | Provides methods to help you solve a problem or save time. |
| NOTE | Provides additional information as a supplement to the text. |

## Revision History

| Version | Revision Content | Release Time |
|---|---|---|
| V2.0.0 | ● Updated images.<br>● Updated arming and disarming, and user menu operations. | April 2022 |
| V1.0.1 | Updated arming and disarming. | October 2020 |
| V1.0.0 | First release. | May 2020 |

## Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

# About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This section introduces content covering the proper handling of the controller, hazard prevention, and prevention of property damage. Read carefully before using the controller, and comply with the guidelines when using it.

## Transportation Requirements

⚠

- Transport the controller under allowed humidity and temperature conditions.
- Pack the controller with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the controller, violently vibrate or immerse it in liquid during transportation.

## Storage Requirements

⚠ WARNING

- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting a battery might result in an explosion
- Leaving a battery in an environment with extremely high temperatures might result in an explosion or the leakage of flammable liquids and gas.
- Subjecting a battery to extremely low air pressure might result in an explosion or the leakage of flammable liquids and gas.

⚠

- Store the controller under allowed humidity and temperature conditions.
- Do not place the controller in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or unstable illumination.
- Do not place heavy stress on the controller, violently vibrate or immerse it in liquid during storage.

## Operation Requirements

⚠ WARNING

- Change the default access code after installation to protect the controller from being stolen.
- Use the controller within the rated range of power input and output.

⚠

- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the controller while the adapter is powered on.
- Operate the controller within the rated range of power input and output.
- Transport, use and store the controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the controller, and make sure that there is no object filled with liquid on the controller to prevent liquid from flowing into it.
- Do not disassemble the controller.

## Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the controller.
- Do not connect the controller to two or more kinds of power supplies, to avoid damage to the controller.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the controller in a place exposed to sunlight or near heat sources.
- Keep the controller away from dampness, dust, and soot.
- Put the controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the controller label.
- The controller is a class I electrical appliance. Make sure that the power supply of the controller is connected to a power socket with protective earthing.
- Do not install or place the controller in a location that exposes it to sunlight or heat sources.
- Keep the controller away from dampness, dust, and soot.
- Keep the controller installed on a stable surface to prevent it from falling.
- Do not drop or splash liquid onto the controller, and make sure that there is no object filled with liquid on the controller to prevent liquid from flowing into it.
- Do not disassemble the controller.
- Transport, use and store the controller under the allowed humidity and temperature conditions.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).
- Affix the controller securely to the building before use.
- The power supply must be installed inside the controller.
- When installing the controller, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- The rated power of the controller is 40 W.
- Prevent liquid from dripping or splashing on the controller. Do not put any objects filled with liquid, such as a vase, on top of the controller.
- Do not expose the battery to overheated environments such as with direct sunlight and fire.

**Electrical Safety**

⚠ WARNING

- Improper use of the battery might result in a fire or explosion.
- Replace unwanted batteries with new batteries of the same type and model.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- Make sure the power supply meets the SELV (Safety Extra Low Voltage) requirements, and rated voltage conforms to the IEC60950-1 standard. The requirements of the power supply are subject

to the controller label.

- The controller is a class I electrical appliance. Make sure that the power supply of the controller is connected to a power socket with protective earthing
- The appliance coupler is a disconnection controller. Keep it at a convenient angle when using it.

Before acting on a system component, or while you are installing or servicing the controller, make sure to disconnect both the primary (mains power) and secondary (battery) power supply of the system. Also, to avoid damage from electrostatic discharge, handle the controller with care and avoid any contact with its electronic components.

**Power Supply**

⚠ WARNING

The power supply of the controller meets the EN 50131-6 standard, and performs the following controls in compliance to the standard:

- Every 24 hours, the status of the alternative power supply is checked. The battery test is executed under load.
- In the absence of mains voltage, the test is not executed.
- Every 10 seconds, the output voltage is checked.
- The output voltage is checked every 10 seconds.
- The battery is disconnected if voltage drops below 10.8 V (protection against the deep discharge).

**Battery**

⚠ WARNING

The battery of the controller meets the EN 50131-6 standard, and performs the following controls in compliance to the standard:

- The controller must be equipped with a battery that has 12 V/12 Ah capacity.
- We recommend using a FG 21201 battery.
- The battery is designed with special lead calcium tin alloy grid that is built to resist corrosion and provide a short recharge time.
- The battery adopts VRLA AGM technology and uses low resistance high microporous fiberglass separators.
- The battery uses leak resistant post seal, faston, flag and threaded female, terminals with high conductivity and maximum torque resistance.
- The battery is designed with one-way safety relief valves that allow gas to escape, and prevent the ingress of oxygen
- The battery uses ABS plastic (from FGHL range flame retardant ABS plastic to IEC 707 FV0 and UL94 FV0 - LOI greater than 28%).
- The battery supports installation in any orientation, except being permanently inverted. The batteries can only be replaced by qualified personnel.
- The electrolyte is absorbed in fiberglass separators with 99% internal gas recombination efficiency. Blocs are grants non-spillable and maintenance free, so their electrolytes do not require topping up during its lifetime. Also, low self-discharge allows it a shelf life of 6 months.

**Wire**

⚠ WARNING

- Ground connection

The ground connection must comply with the valid European standards. It is required that the ground conductor be connected between the casing and the door.

- External circuit breaker

The power supply of the controller is not equipped with a circuit breaker. To ensure that controller installation meets the local standards, an external circuit breaker or a bipolar mains switch (16A curve C, opening stroke min. 3 mm) must be connected to an accessible part of the electric installation (240 VAC). Also, the circuit breaker must be installed close to the controller and must be clearly labeled.

- Mains connection (240 VAC)

  The mains cable is not included. To reduce the risk of electric shock in normal operating conditions, observe the following precautions:

  - Use a double insulation cable (with shielding) for the connection to mains power.
  - The mains cable should have a minimum diameter of 3 x 1.5 mm$^2$ and, once it has been connected to the corresponding power input, it should be attached with a cable tie to the mounting base of the power supply.
  - To ensure electrical safety and correct functioning of the controller, always connect the ground conductor to the corresponding terminal between the base and the door of the casing.
- Mains and ground connection
  - Connect the mains conductor and the ground conductor.
  - The mains conductor must be wired in the absence of voltage.
  - The ground conductor must be connected to the ground terminal of the power supply and to the faston connector soldered to the casing.
  - It is required that the ground conductor be connected between the casing and the door.
  - For safety reasons, attach the connection cable with a cable tie to the mounting base of the power supply.

## Maintenance Requirements

⚠ WARNING

- Dispose used batteries strictly according to its instructions and local regulations.
- Power off the controller before maintenance.
- To prevent explosion or fire, replace battery with the same size.

⚠

- In the planning phase, to ensure the autonomy of the service requested by the standards, it is important to size the primary (mains power) and secondary (battery) power supply correctly. Consider that, in case of power failure, the system Is ensured to continue functioning by means of batteries for a limited period of time, the length of which depends on the capacity and the state of efficiency of the batteries.
- To ensure the efficiency of the burglar alarm system, it is necessary to provide an appropriate maintenance program. The frequency of the maintenance depends on different aspects, however, it is recommended to have the system serviced at least once every 6 months. The maintenance operations should be made by specialized technical staff, the same who designed and installed the system. The European standards series EN 50131 includes the possibility of remotely executing one of the two required annual inspections.

- Replace the batteries with the correct model and dispose of the unwanted ones as instructed to avoid failing to meet the requirements of the safeguards. Some types of lithium batteries are not acceptable.
- The most important controls:
  - ◇ The status of the power supplies and batteries.
  - ◇ The status of the batteries and self-powered devices (sirens and transmitters).
  - ◇ The functional efficiency and coverage of the movement and perimeter detectors.
  - ◇ The efficiency of the control units and procedures for arming of the program.
  - ◇ The efficiency of the alarm transmission equipment (e.g. activation of the telephone call cycle).
  - ◇ The efficiency of the warning devices.
  - ◇ The correct detection and management of the tamper alarms.
  - ◇ The other secondary functions (for example, activation of the hold-up alarm).
  - ◇ The correct connection of the cables to the terminals.
  - ◇ The final inspection report.

# Table of Contents

# 1 Introduction

## 1.1 Overview

The alarm controller is a high performance anti-theft controller designed for the middle and small alarm solution application. Adopting embedded Linux operation system and relying on embedded platform, the system can run steadily with advanced controlling technology and strong data transmission ability. The embedded design also supports the product with high security and excellent stability.

The controller can work both independently and with professional app in mobile phone, which is convenient for remote viewing and alarm status controlling. The product can also be connected to the network to form the strong security monitoring network, working with the professional alarm platform software to show the strong networking and remote monitoring ability.

The controller can be widely applied in the store, warehouse, family, and so on for security protection.

## 1.2 Features

The functions might be different depending on the software and hardware version of the model you purchased.

- 8 onboard wired zones.
- Support 1-way siren control and 2-way MOS transistor output on the controller.
- With the expansion module (consists of 8 input modules and 8 output modules), alarm input and alarm output channels are increasing to 72 and 82 respectively.
- Outputs operation follows system events, zone events, area, link and scheduling programs.
- 1 case tamper port for the alarm controller.
- 1 siren tamper input.
- Up to 8 areas, and every area with 2 partitions.
- Up to 8 keypads.
- Up to 100 users with 8 authority levels for different users (supervisor, manager, master, user, temporary, duress, patrol, and technician).
- 1000 events log.
- Supports more than 11 zone types.
- 7 sorts of zone terminations, including closed-circuit (NC), open-circuit (NO), end-of-line (EOL) resistors, double end-of-line (DEOL) resistors, triple end-of-line (3DEOL) resistors, inertial type for vibration detector and pulse type for roller shutter.
- Configurable zone resistance (2K7, 4K7, and 6K8).
- With 2 RS-485 ports for keypads connection and extended connections.
- With PSTN port for alarm event report function, supporting CID (Contact ID).
- 3 telephone numbers for monitor station (PSTN), 8 telephone numbers for vocal message, and 8 telephone numbers for SMS.

- With GSM/GPRS/LTE network ports for events SMS reporting and remote control, events vocal message reporting by dialing and remote control, and mobile phone app connection ability when Ethernet connection is failed.
- With 10/100M self-adaptive Ethernet port.
- Supports abnormality alarm, including network disconnected alarm, PSTN fault alarm, tampering alarm, low battery alarm, battery loss alarm, power loss alarm, and keyboard faults alarm.
- In-field firmware upgradable.
- App-based system control through DMSS.
- Arm and disarm areas with RFID cards.
- Access to the third party platform with SIA.

## 1.3 Technical Specifications

This section contains technical specifications of the controller. Please refer to the ones that correspond with your model.

Table 1-1 Technical specifications

| Type | Parameter | Description |
|---|---|---|
| Port | Alarm Input | 8 channels, can be expanded to 72 for zone alarm input |
| | Alarm Output | 2 channels, can be expanded to 82 (channel 1–2: MOS outputs, channel 3–82: Relay outputs) |
| | Network | 1 RJ-45 10M/100M self-adaptive Ethernet port |
| | PSTN | One group of PSTN RJ-11 ports that support contact ID protocol (with PSTN module)<br>3 telephone numbers for monitor station (PSTN) |
| | RS-485 | 2-channel RS–485 ports, support keyboard (A1B1) and expansion module (A2B2) access |
| | 2G | Operating frequency: GSM850/GSM900/DCS1800/PCS1900 MHz |
| | 4G | LTE-FDD: B1/B3/B5/B7/B8/B20<br>LTE-TDD: B38/B40/B41<br>GSM/EDGE: B3/B8 |
| | Siren | 1 × 12 V/1 A siren output port |
| | Battery | 12 V battery port |
| | Auxiliary Power Output | 2 × 12 V/1 A AUX power output ports |
| | Tamper | 1 case tamper port for the alarm controller<br>1 siren tamper input |
| Function | SMS Notification | Supports up to 8 telephone numbers for SMS and remote control (with 2G or 4G module) |
| | Phone Call Notification | Supports up to 8 telephone numbers for vocal message (with 2G or 4G module) |
| | Network Protocol | TCP/IP, DHCP, static IP, P2P |

| Type | Parameter | Description | |
|---|---|---|---|
| | Configuration Method | Keypad and client software | |
| | Arm and Disarm Method | Keyboard, swipe card, DMSS app, SMS, DSS Professional, and VTH | |
| | External Agreement | Supports customized access to the third parties by SIA | |
| | Number of Keypads | Max. 8 keypads | |
| | Area | 8 areas | |
| | Partition | Each area includes 2 partitions | |
| | Timers | 8 timers, can be used for user authorization restrictions, output linkage control, automatic arming and disarming control, and more | |
| | Power Management | Automatic switching between main power supply and backup power supply | |
| | | Alarm for main power loss | |
| | | Alarm for battery loss and battery voltage fault | |
| | Event Logs | Max. 1000 | |
| | Component data for non-volatile memory components (duration of data maintenance) | Flash: More than 20-year data retention | |
| | User Management | Max. 100 users<br>7 user levels: Supervisor, Manager, Master, User, Temporary, Duress, and Patrol<br>1 Technician | |
| | Query | Query for zone fault, system fault, program version, signal strength detection, and GPRS | |
| | Language | English, Italian | |
| | App | DMSS app and DMSS Plus app not certified IMQ-Security system | |
| | RFID Card | Arm and disarm by swiping card (with ASR1101A/ASR1101A-D) | |
| | Electrical specific cations CPU board | CPU consumption | 360 mA@14.5 V |
| | | Output voltage control | 9–16 VDC |
| | | Detector power supply | 14.5 VDC |
| | | Siren power supply | 14.5 VDC |
| Power Supply | Main Power | Type A: 110–240 VAC, 50/60 Hz | |
| | Conformity | EN 50131-6 | |
| | Max. Consumption | 800 mA@230 VAC; 1300 mA@ 115 VAC | |

| Type | Parameter | Description |
|---|---|---|
| | Max. Output Voltage | 2.76 A@14.5 VDC |
| | Max. Current Available | 2.76 A |
| | Max. Ripple | Max. 30 mV |
| | Power Consumption | Max. 40 W |
| | Max. Output Voltage | 12 V; 1A |
| | Mains fuse (non - replaceable) | RT21: 5 A |
| Battery | Battery Capacity | 1 x 12 V/7.2 Ah |
| | Battery Flame Class | UL94 FV0 |
| | Standards | IEC 60896 Part 21 - VRLA methods of testing<br>IEC 60896 Part 22 - VRLA requirements<br>Eurobat 3-5 years standard commercial for FG FGH<br>FGC and 10-12 years long life for FGHL<br>UL Recognized |
| | Battery Low Battery Threshold | 11.8 VDC |
| | Battery Restore Threshold | 12.3 VDC |
| | Battery Standby | Up to 12 hrs<br>440 mA as max load in order to have autonomy of 12 h. |
| | Release Voltage | < 10.8 V |
| | Failure Signaling | < 5 V |
| | Overcharge Signaling | 14.5 V |
| | Battery Recharge Time | 80% approx. 48 h |
| ARC Signaling | ATS Category | SP2 (PSTN or GSM)<br>DP1 (PSTN + GSM) |
| | Acknowledgement Operation | Pass through |
| | Primary Transmission Path | LAN (NO 50136-2) |
| | Secondary Transmission Path | GPRS/4G /PSTN |
| | Notification Equipment | B/C/E |
| General | Operating Temperature | –10 °C to +55 °C (+14 °F to +131 °F) |
| | Relative Humidity | 10%–90% (RH) |
| | Product Dimensions | 275.0 mm× 275.0 mm× 77.0 mm (10.83" × 10.83" × 3.03") (L× W× H) |
| | Installation | Wall mount |

| Type | Parameter | Description |
|---|---|---|
| | Net Weight (without battery) | ≤3 kg |
| | Expansion Bolts | Outer diameter: 5.5 mm<br>Inner diameter: 2.9 mm<br>Length: 24.5 mm<br>Quantity: 4 |
| | Self-tapping Screw | Diameter: 4 mm<br>Length: 25 mm<br>Quantity: 4 |
| ACE Classification | | Type A |
| Certifications | | CE: 4789104635<br>EN 50131-3, EN 50131-6, EN 50136-2<br>Security Grade 2<br>Environment Class II |

Table 1-2 ATE category

| ATE Category | Reporting Time | Protocols | Communication Devices | | | Communication Device to be Used |
|---|---|---|---|---|---|---|
| | | | PSTN | 2G/3G | IP | |
| SP2 | 25 h | Standard | √ | — | — | The check marked communication device |
| SP3 | 30 min | Standard | — | √ | √ | Only one of the two check marked communication devices |
| SP4 | 3 min | Encrypted | — | √ | √ | Only one of the two check marked communication devices |
| SP5 | 90 s | Encrypted | — | √ | √ | Only one of the two check marked communication devices |
| DP1 | 25 h | Standard | √ | √ | √ | Only two of the three check marked communication devices |
| DP2 | 30 min | Standard | √ | √ | √ | Only two of the three check marked communication devices |
| DP3 | 3 min | Encrypted | — | √ | √ | The two check marked communication devices |

<table>
<tr><th rowspan="2">ATE Category</th><th rowspan="2">Reporting Time</th><th rowspan="2">Protocols</th><th colspan="3">Communication Devices</th><th rowspan="2">Communication Device to be Used</th></tr>
<tr><th>PSTN</th><th>2G/3G</th><th>IP</th></tr>
<tr><td>DP4</td><td>90 s</td><td>Encrypted</td><td>—</td><td>√</td><td>√</td><td>The two check marked communication devices</td></tr>
<tr><td colspan="7">ATE: Alarm transmission equipment.<br>SPx (Single Path): A value that indicates the performance level achieved by a single communication device, according to the EN 50136–1 standard.<br>DPx (Double Path): A value that indicates the performance level achieved by a combination of two communication devices, according to the EN 50136–1 standard.<br>Reporting time: The reporting time is prescribed based on the standard of each level of performance. Reporting time is the maximum time available to report when an alarm transmission device fails. Alarm transmission devices meet this requirement by regularly reporting their status through a specific symbolic test function.<br>Protocols: Indicates the security level of the protocols to be used for the notification of failures. Standard protocols and voice protocols are encrypted. High security protocols are encrypted with an AES 128 bit or AES 256 bit encryption key.<br>Communication devices: Implemented communication devices.<br>Communication devices to be used: Indicates the number of and which communication devices are to be used based on the ATE category.</td></tr>
</table>

Table 1-3 Terms and definitions

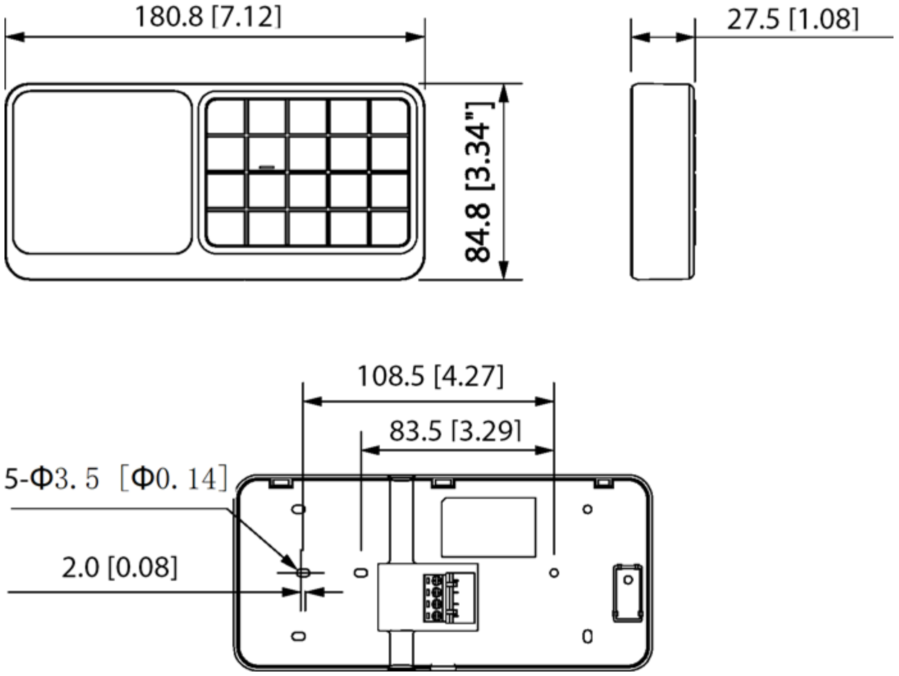
| Term | Description |
|---|---|
| Area | 8 areas that can be armed. |
| Zone | Protection zones under area. |
| Partition | The scope of partition is larger than zone and under area. |
| Numeric key | Key 0–9 on the keypad. |
| Function key | Other keys except numeric keys, such as ESC and ENTER. |
| Key combination | Total Fn + numeric key. |
| User menu | Menus programmed by the user. |
| Installer menu | Menus programmed by the technician. |
| Access code | A specified code, from 4 to 6 digits, that allows the user to operate the keypad. |
| 1 EOL | The detector type can be NC, and returns three status: normal, alarm and short circuit. |
| 2 EOL | The detector type can be NC, and returns four status: normal, alarm, tamper, and short circuit prevention. |
| 3 EOL | The detector type can be NC, and returns five status: normal, alarm, tamper, anti-masking, and short circuit prevention. |

# 2 Keypad

This chapter introduces the dimensions, main functions, indicators, keys operations, and installation of the keypad.

## 2.1 Dimensions

Figure 2-1 Dimensions (unit: mm [inch])



## 2.2 Installation

### Prerequisites

Make sure to prepare following expansion bolts and self-tapping screws first.

- Expansion bolts

  Outer diameter: 6.5 mm; inner diameter: 2.5 mm; length: 28.1 mm; quantity: 4.

- Self-tapping screw:

  Diameter: 3 mm; length: 18 mm; quantity: 4.

### Procedure

Step 1 Unpack the box and take out the expansion bolts and self-tapping screws.

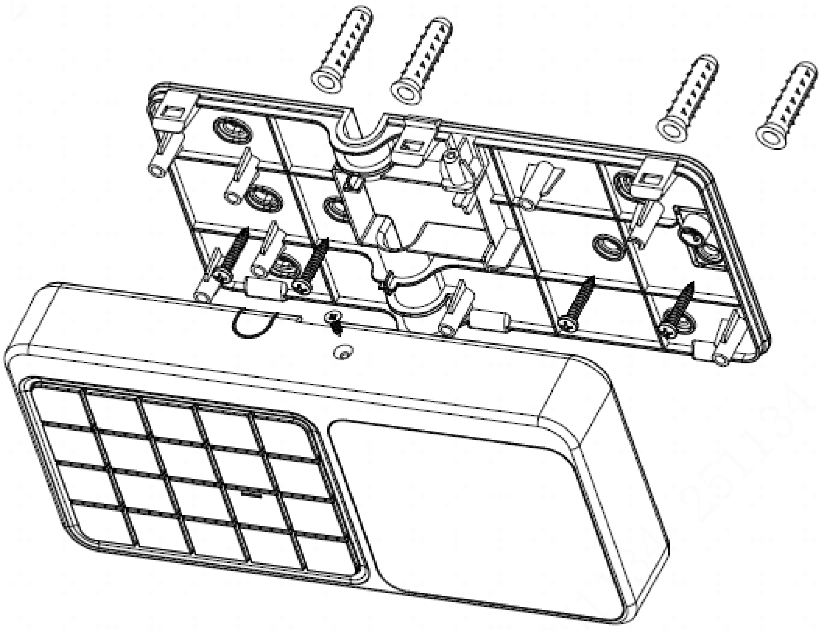
Step 2 Drill screw holes with a diameter of about 6.35 mm and a depth of about 28.1 mm on the mounting surface.

Step 3 Insert expansion bolts into the drilled screw holes.

Step 4 Align the holes in the rear panel of the alarm keypad with the expansion bolts, and then put in and fasten the self-tapping screws.

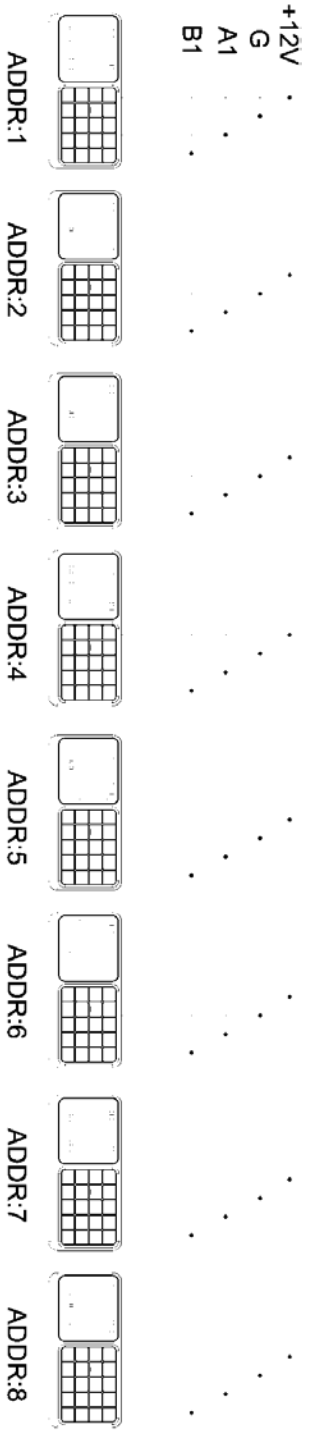
Step 5 Attach the keypad front panel and rear panel together.

Figure 2-2 Install the controller



## 2.3 Wiring

Figure 2-3 keypad connection



## 2.4 Structure

Figure 2-4 Structure

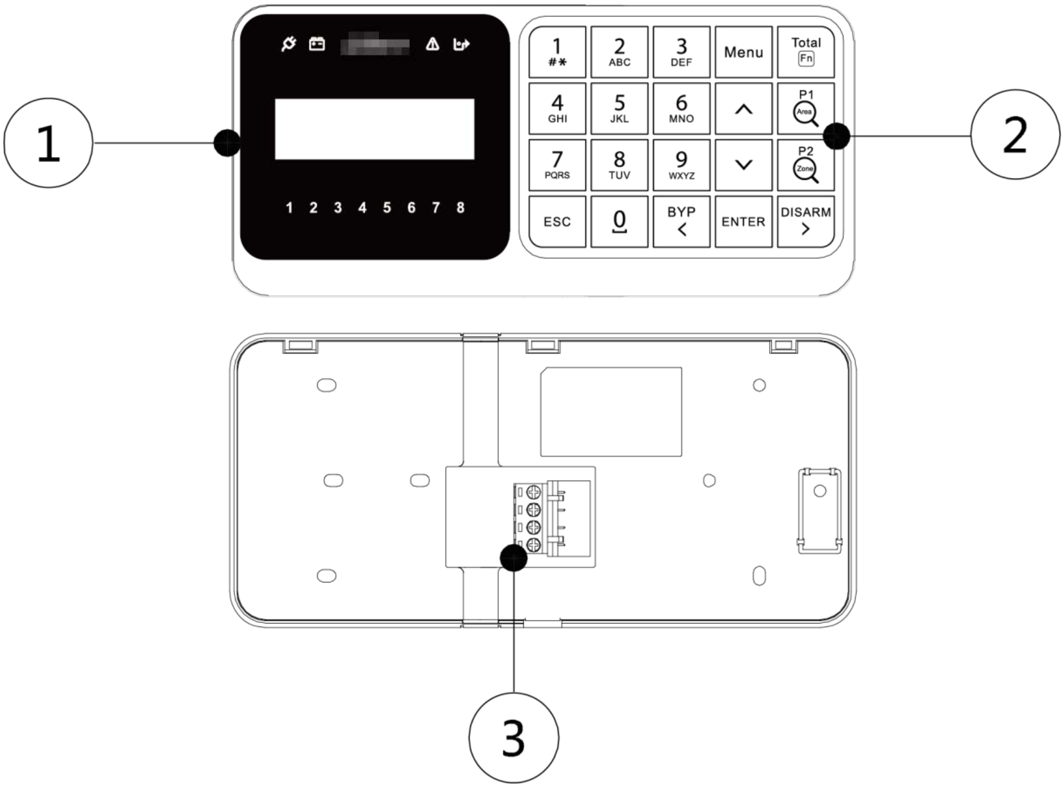


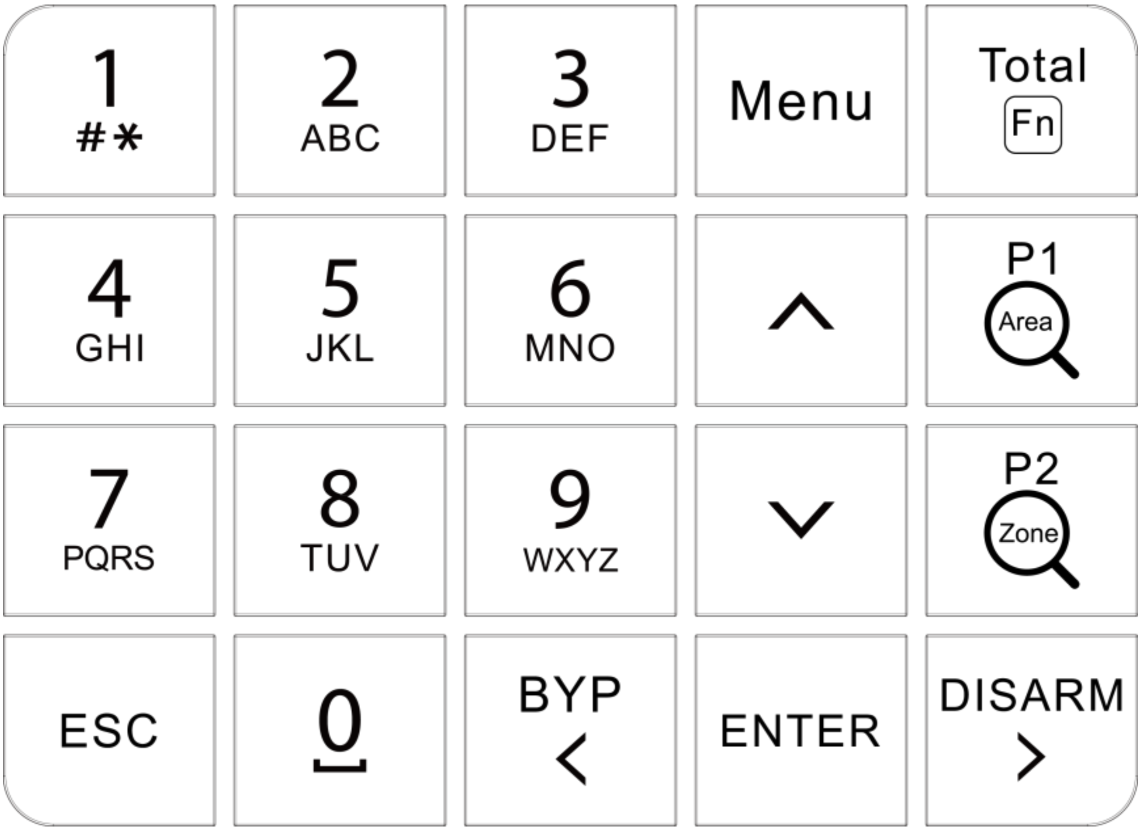
Table 2-1 Function

| No. | Name | Function |
|---|---|---|
| 1 | LCD display | Displays all the system information including management and programming. For details, see "2.7 LCD Display". |
|  | LED indicators | Displays information about power status, battery status, failures, bypass, and alarm status of each area. For details, see "2.6 LED Indicators". |
| 2 | Keys | Each key has specific function. For details, see "2.5 Keys". |
| 3 | Ports | ● +12V: Supplies 12 VDC.<br>● GND: Ground.<br>● RS485_A1<br>● RS485_B1 |

## 2.5 Keys

Each key of the keypad has a specific function.

Figure 2-5 Keys



## 2.5.1 Numeric Keys (from 0-9)

The numeric keys have following functions.

- Enter access codes as required to access programming (technician or user) or to arm/disarm.
- The keys from 1 to 8 represent eight areas. When the zone is not ready, you can press and hold the key to show the **NOT READY** details, and when the key LED light slowly flashes or quickly flashes, press and hold the key to show the alarm details.
- The keys from 0 to 9 can be used to enter or edit alphanumeric descriptions.
- Press 1 to enter #, *, and .. Press 0 to enter space.

## 2.5.2 Function Keys

Table 2-2 Function keys

| Key | Function |
|---|---|
| ESC | Exit from the current menu or return to the previous menu. |

| Key | Function |
|---|---|
| BYP < | - Move the pointer to the left when you edit.<br>- Press and hold BYP < to delete the text.<br>- Bypass the zones as follows.<br>1. Enter the access code.<br>2. Press BYP <, and then the screen of setting the bypass zones is displayed.<br>3. Press the corresponding numeric key of the zones that you want to bypass. For example, if you want to bypass zone 12, press key 1 and then press key 2.<br>4. Press Enter to confirm the setting. |
| Menu | - Enter the user menu or the installer menu.<br>- Quick enter. For example, if you enter 130, press immediately to confirm, otherwise it will become invalid.<br>- Quick jump. For example, if there are 300 logs and you want to view the 200th log, enter 200, and then press immediately to jump to the 200th log page. |
| ^ v | - Increase or decrease numbers.<br>- Navigate between the options on the screen.<br>- Turn pages.<br>- Enter the password, and press ^, and then enter the authorization mode. |
| ENTER | - Enter the sub menu.<br>- Switch to the next menu of the same level in editing mode.<br>- Confirm. |
| Total Fn | - Arm the whole areas.<br>- Rapid global arming of the whole areas.<br>- Key combination operations. |
| P1 Area | - Arm the partition 1.<br>- Rapid arming of the partition 1.<br>- Key combination operations. |
| P2 Zone | - Arm the partition 2.<br>- Rapid arming of the partition 2.<br>- Key combination operations. |
| DISARM > | - Disarm.<br>- Move the pointer to the right when you edit number or letter. |

## 2.5.3 Key Combination Operations

Press keys in sequence.

For example, if you need to press Total Fn + 0, press Total Fn first, and then press 0.

Table 2-3 Key combination operations

| Key | Function |
|---|---|
| Total Fn + 0 (F0) | ● On the main screen, press Total Fn + 0 (F0) to view the GSM connection status, which is shown with eight bars.<br>● Press Total Fn + 0 (F0) again to return to the main screen.<br>The system automatically returns to the main screen within 2 minutes if no operations are performed. |
| Total Fn + 1 (F1) | ● Panic activation (silent activation or with sirens and keypad buzzer).<br>● On the menu of **ZONE TROUBLES**, **ZONE MANAGER**, and **CHIME ZONES**, press Total Fn + 1 (F1) to go to the area selection screen to select, search and filter through areas.<br>● On the **OUTPUTS** menu, press Total Fn + 1 (F1) to do a test to the output circuit, and active is shown. |
| Total Fn + 2 (F2) | ● Robbery activation (silent activation).<br>There is no response on the screen but this event is recorded in the log.<br>● On the menu of **ZONE TROUBLES**, **ZONE MANAGER**, and **CHIME ZONES**, you can select, search and filter through zones.<br>● Edit text on the screen such as description of module, zone, user code, output, timer and display.<br>● Edit telephone number, SMS number, and SIM number on the **TEL NUMBER** menu, and PSTN number on **MONITOR STATION** menu. |
| Total Fn + 3 (F3) | ● Medical activation (with keypad buzzer)<br>● On the **WALK TEST** menu, switch between individual test and multiple test.<br>● On the **TEL NUMBER** menu, start a phone call test or message test. |
| Total Fn + 4 (F4) | ● Fire alarm activation (with keypad buzzer and siren).<br>● On the **TEL NUMBER** menu, stop a phone call test. |
| P1 Area + (1-8) | Search for specified zones under the specified area. |
| P2 Zone + (01-99) | Search for areas to which the specified zone belongs. |

# 2.6 LED Indicators

There are 12 LED indicators on the keypad that respectively shows information about power status, battery status, faults, bypass, and alarm status of each area.

## 2.6.1 Overview

Table 2-4 LED indicators

| Icon | Color | Meaning |
|---|---|---|
| 🔌 | Green | Power status. |
| 🔋 | Green | Battery status. |
| ⚠ | Red | Fault status. |
| ↪ | Green | Bypass. |
| 1 2 3 4 5 6 7 8 | Red | Alarm status of eight areas. |

## 2.6.2 Status

### Power LED Indicator (🔌)

- Glows green: The system operates with normal power supply.
- Slowly flashes green: The system does not operate normally due to a lack of power supply. Make sure to check the power.
- Quickly flashes green: The system is in installer programming mode or in the walk test zone mode. If a lack of power supply occurs when the system is in either of these two modes, the LED indicator also quickly flashes.

### Battery LED Indicator (🔋)

If power supplies normally, the indicator will not be ON in case of low battery.

- Slowly flashes green: Battery faults such as low power and powering off quickly.
- Off: Battery operates normally.

### Fault LED Indicator (⚠)

- Glows green: System faults (main power loss, battery low voltage or missing), and you can view the details on the **SYSTEM TROUBLES** menu of **User** menu.
- Slowly flashes green: Tampering is happening to the controller, siren, or keypad.
- Off: The system operates normally.

### Bypass LED Indicator (↪)

- Glows green: There is at least one bypassed zone.
- Off: There is no bypassed zone.

### 1-8 LED Indicators

There are eight LED indicators located below the LCD display representing the status of the areas. From left to right, there is the alarm status of area 1 to area 8.

Figure 2-6 Area status LED indicators

- Glows red: The area is armed.
- Slowly flashes red: The alarm is in progress or the alarm has occurred.
- Quickly flashes red: The area is in alarm condition and the linkage is in progress. This condition disappears when the area is disarmed. The indicator starts to flash slowly and is cancelled when a valid user code is entered again followed by the command **DISARMED**.
- Off: The area is disarmed.

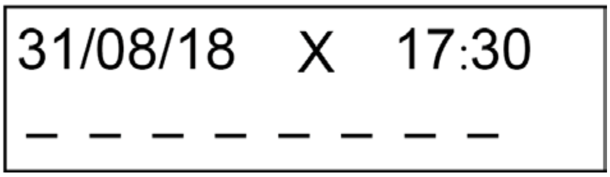
By pressing and holding the number key corresponding to each area for three seconds, you can view where exactly the alarm is in the area. For example, when the area 5 indicator quickly flashes, press and hold key 5, then * shows where the alarm is located exactly. This operation can only view the zone-related alarms, but cannot view the system faults alarms.

## 2.7 LCD Display

The keypad is equipped with a back-lit LCD display that shows all the system information including management and programming.

When the display is off and everything is working properly, the first line shows the date and time, and the second line contains a series of data that represent area in use in the system.

Figure 2-7 Example of keypad with 8 areas assigned



```
31/08/18   X   17:30
_ _ _ _ _ _ _ _
```

Each dash can represent a different meaning according to the event activated by the area. Refer to Table 4-6 for the event description and symbol of each event.

### Symbols on the First Line of Display

Table 2-5 Symbols on the first line of display

| Symbol | Meaning |
|---|---|
| 31/08/18 | Day/Month/Year |
| x | ● **H**: Holiday period active.<br>● **T**: Telephone dialer calling.<br>● **P**: Disarming period for patrol user. |
| 17:30 | Hour: Minutes. |

| Symbol | Meaning |
|---|---|
| ▯▯▯▯▯... | Level of GSM signal. Each ▯ is equivalent to one bar, and maximum eight bars. |

## Symbols on the Second Line of Display

Table 2-6 Symbols on the second line of display

| Symbol | Event |
|---|---|
| Upper case **T** | Total arming. |
| 1 | Partition arming 1. |
| 2 | Partition arming 2. |
| Upper case **P** | Partition 1 + Partition 2 arming. |
| Lower case **t** | Total forced arming. |
| Upper case **A** | Alarm. |
| **<** | Entry delay time |
| **>** | Exit delay time |
| * | Area not ready (zones open). |
| **!** | Alarm delay. |

## Alarm Message Display

During an alarm, the main screen shows the general reason description for the alarm in the first line, for example, **ZONE ALARM**. The alarm message remains displayed for the entire duration of the alarm.

To verify the event that caused the alarm, you can press and hold the corresponding numeric key (from 1 to 8) to show the event details. The display will show the zone or the event that triggered the alarm.

To examine whether any other zones are involved in the alarm, press ˄ and ˅ to scroll up and down the page. Normally, the display shows the last zone affected by the event.

- If there is a call in progress, the display will show the question: 31/08/18 T 17:30 STOP TELEPHONE? when you enter the user code, and press DISARM >. Press ENTER again to confirm the end of the call, or press ESC to return to the main screen and continue the call.
- Alarm messages on the keypad will not be displayed until the system enters authorization mode.

## Display of GSM Signal Strength

By pressing Total Fn + 0 (F0), the value of GSM signal strength and connection status will be displayed on the main screen for about two minutes, or you can press Total Fn + 0 (F0) again to exit. You can also monitor the GSM signal strength during a call in progress.

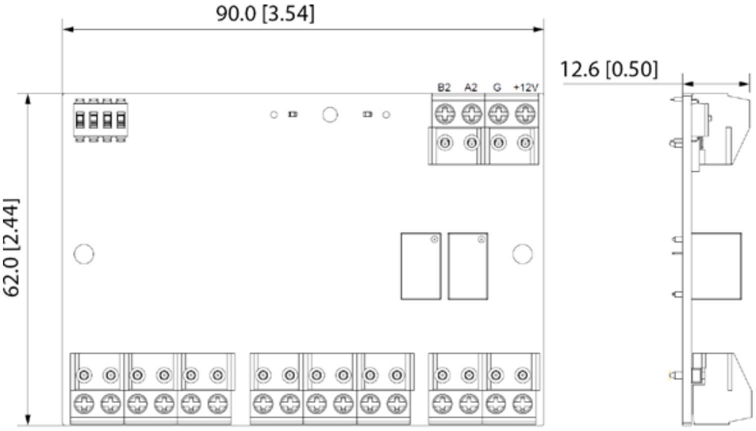
- None ▯: No GSM signal.
- One ▯: Minimum GSM signal.
- Eight ▯: Maximum GSM signal.

# 3 Expansion Module (Optional)

The expansion module is not provided, and you need to purchase it as needed.

## 3.1 Dimensions

Figure 3-1 Dimensions (unit: mm [inch])



## 3.2 Wiring

Figure 3-2 Wiring of detectors

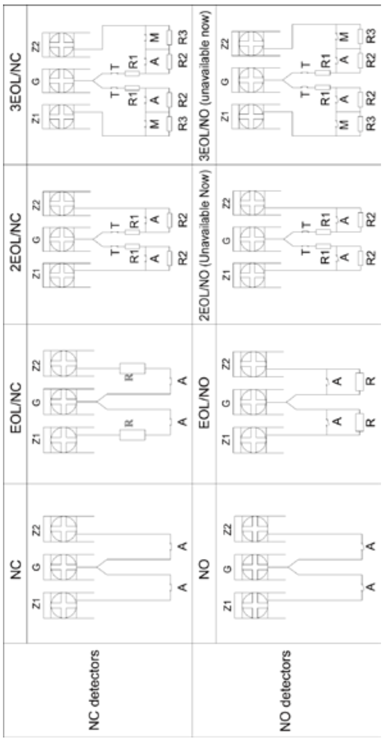
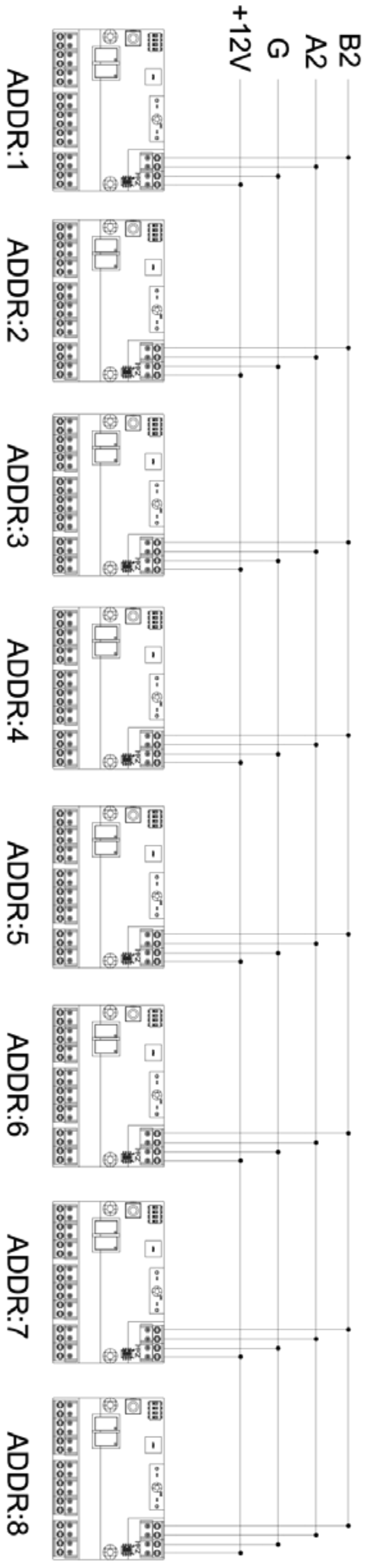


Figure 3-3 Expansion module connections



## 3.3 Module Functions

Dip switch addresses of the expansion modules (including alarm input and output modules) are from 1 to 8.

## Alarm Input Module

8 alarm inputs and 2 alarm outputs are supported with alarm input modules. The alarm input module with Dip switch address 1 receives alarm input signals from wired zones of 9–16, and connects to alarm output devices of 3–4. Other alarm input modules are connected by analogy till the module addressed 8, which receives alarm input signals from wired zones of 65–72, and connects to alarm output devices of 17–18.

## Alarm Output Module

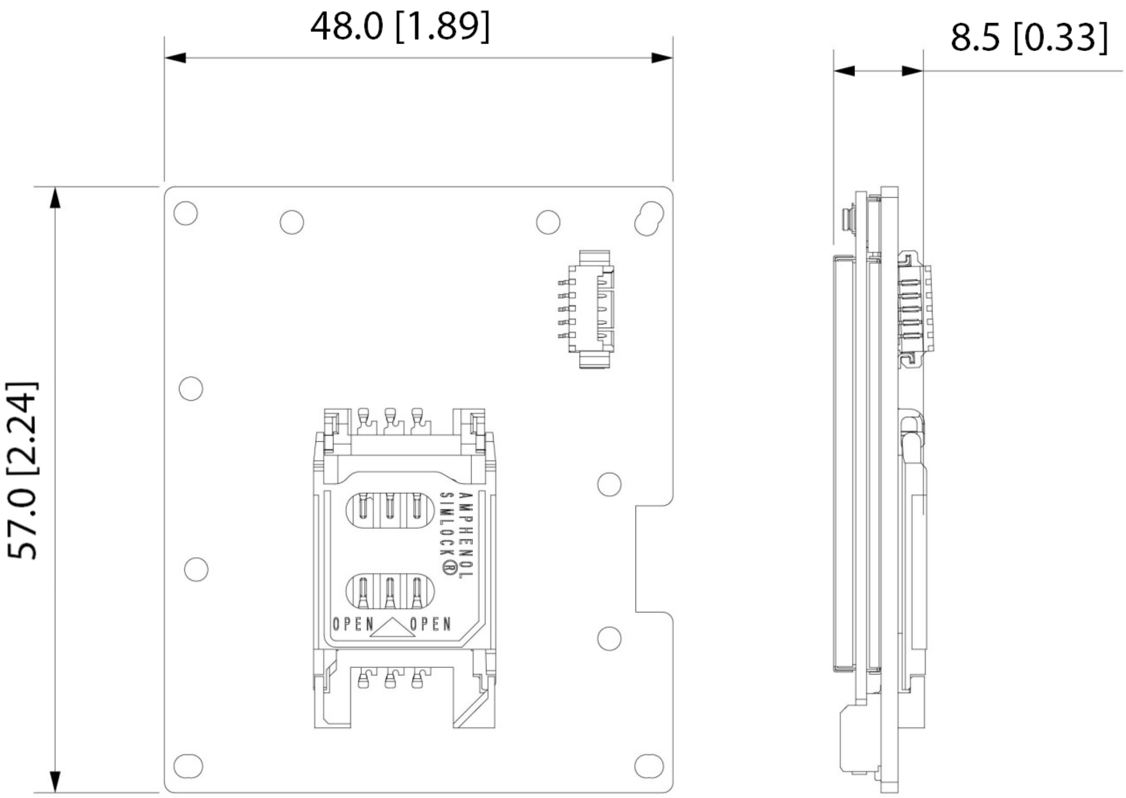
8 alarm outputs are supported with alarm output modules. The alarm output module with Dip switch address 1 connects to alarm output devices of 19–26. Other alarm output modules are connected by analogy till the module addressed 8, which connects to alarm output devices of 75–82.

# 4 4G Module (Optional)

The 4G module is not provided, and you need to purchase it as needed.

## 4.1 Dimensions

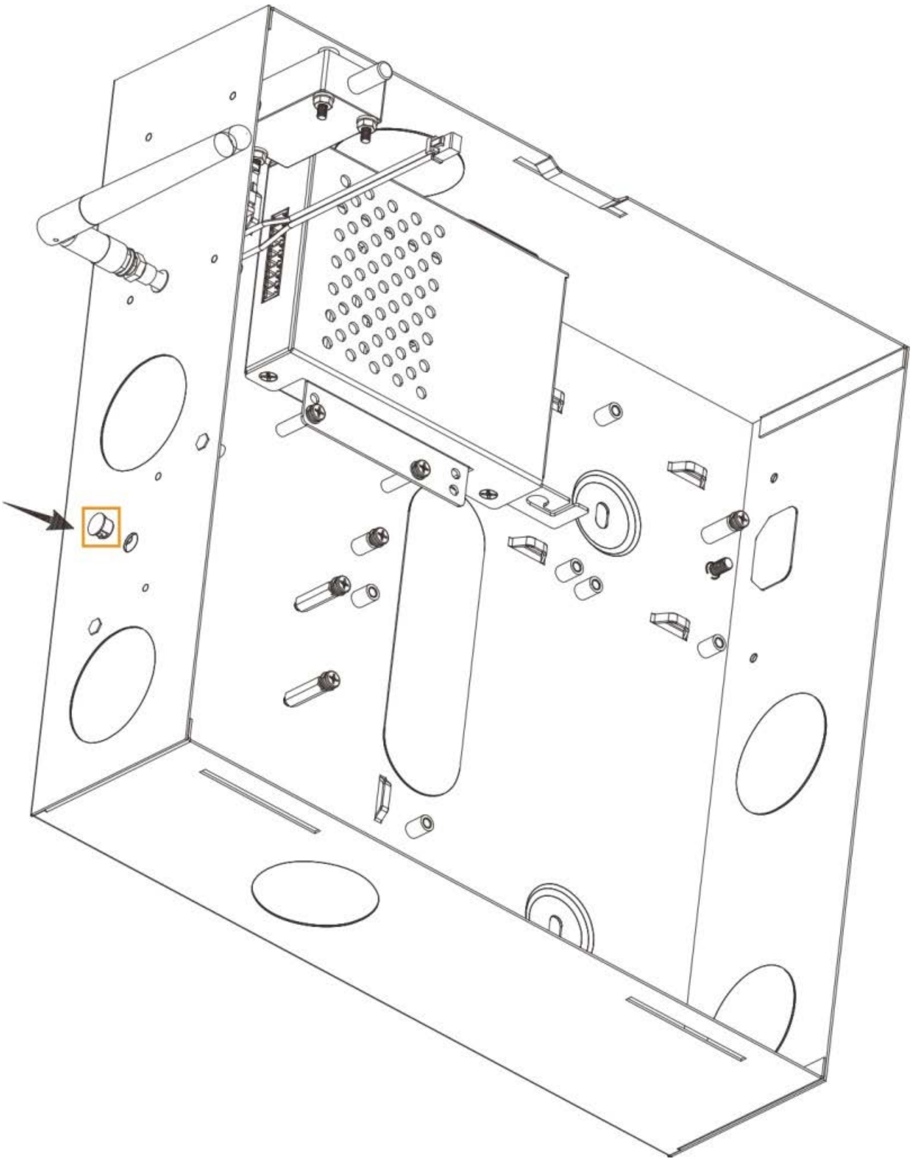
Figure 4-1 Dimensions (unit: mm[inch])



## 4.2 Installing 4G Modules

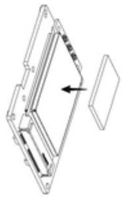
Step 1 Remove two plugs on the controller.

Figure 4-2 Remove plugs



Step 2 Attach the thermal pad to the 4G module.

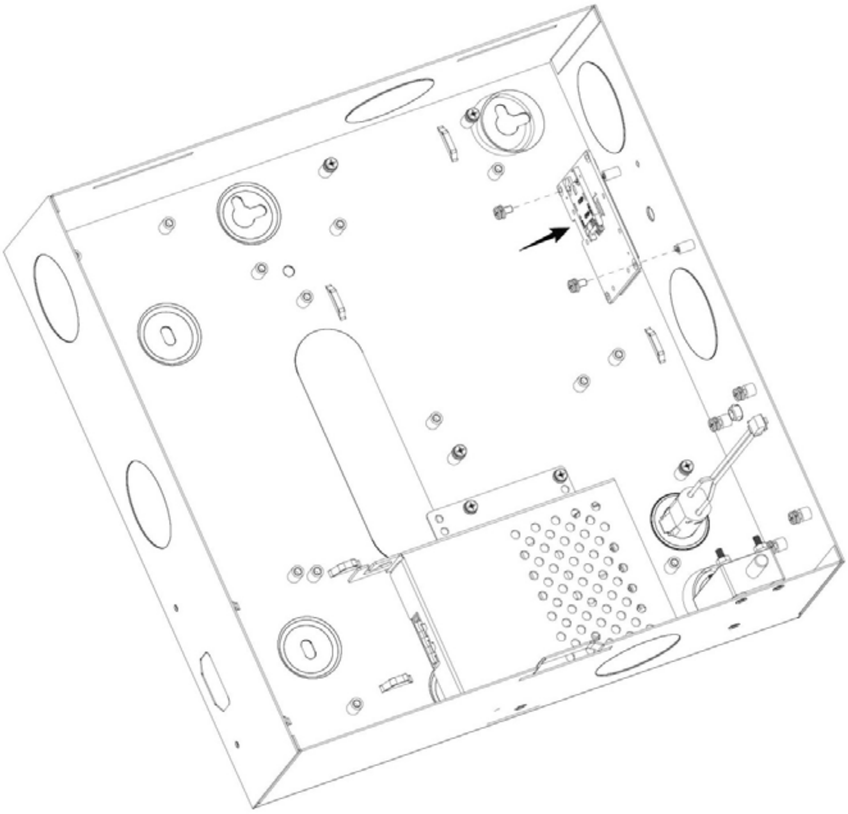
Figure 4-3 Install the thermal pad



Step 3 Attach one end of the antenna patch cord to the main port of the 4G module.

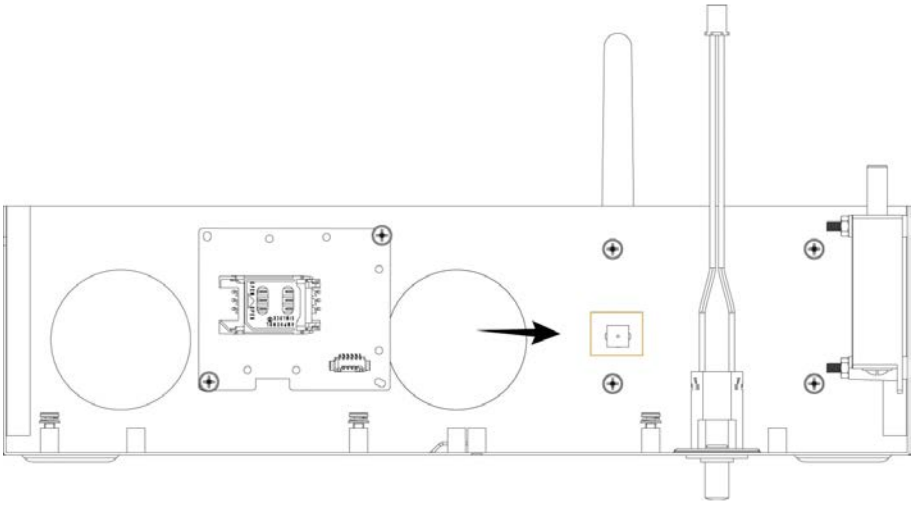
Step 4 Secure the 4G module to the controller with screws.

Figure 4-4 Secure the 4G module



Step 5 Secure the other end of the antenna patch cord to the antenna hole, and then install the external antenna on the hole.

Figure 4-5 Secure the antenna patch cord



Step 6 Connect the 4G module to the 4G port on the main board with the provided wire.

Step 7 Inset the SIM card into the 4G module.

# 5 Arming and Disarming

## 5.1 Arming

When you arm the system, the detectors that are connected to it are activated. If an alarm event occurs, the detectors will trigger an alarm.

When any of the scenarios listed below occur, the system cannot be armed. The keypad will display which zone or area is abnormal, and will give you the option to continue arming. You need to confirm your operations again either by pressing ENTER to arm the system, or by pressing ESC to cancel arming.

- Non 24-hour zone is open.

  ◇ When the zone is not set to allow bypass operations, you will not be given the option to confirm your operations again.

  ◇ When 1 EOL, 2 EOL and 3 EOL zone masking, zone short circuit, or zone tamper are triggered, you will not be given the option to confirm your operations again.

- The intrusion alarm is triggered for an area or zone, but is not cancelled afterwards.
- The medical alarm, fire alarm or other alarms are triggered for an area or zone, but are not cancelled afterwards.

  When robbery alarm is triggered for an area or zone, but is not cancelled afterwards, you will not be given the option to confirm your operations again.

- Controller tamper is triggered.
- Main power failure or battery fault are triggered.

  When power failure and low battery voltage are triggered, you will not be given the option to confirm your operations again.

- PSTN or GSM fault are triggered.

The system supports the following types of arming:

- Total Arming
- Partition 1 Arming
- Partition 2 Arming
- Partition 1+2 Arming
- Forced Arming
- Rapid Arming
- Arming through Timer
- Arming from dialing or SMS, VTH, card, DSS Professional app, DMSS app
- Key Zone Arming

### 5.1.1 Total Arming

Total arming activates protection for the entire alarm system and is used when there are no persons on the premise.

Step 1 Confirm that all zones are ready to be armed, which means that an * must not be placed in place of the dash in the second line of the LCD display.

To identify which zone is not ready, do the following:

1) Press and hold the numeric key (from 1 to 8) where the * character appears.
2) The first open zone is shown on the display.
3) Press ⌃ ⌄ to scroll up and down the screen to show other zones that are not ready.
4) After these zones are identified, you can send a person to do the onsite examination or go to the **ZONE MANAGER** menu to set bypass for these zones.

Step 2 Enter your user code, and then press Total Fn.

The numbers of areas that are ready for arming are shown on the second line of the LCD display.

Step 3 Select the areas that need to be armed by pressing the corresponding numeric key (from 1 to 8).

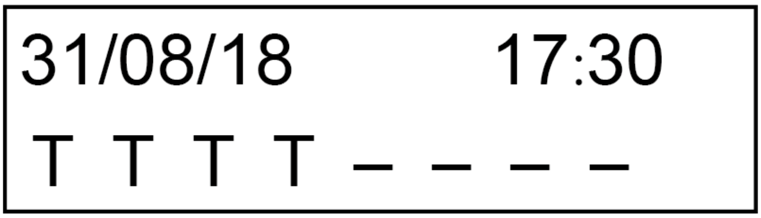
Step 4 Press ENTER to arm the system.

The keypad emits a confirmation buzzer.

The armed area shows an upper case **T**, and the corresponding LED indicator lights up. The areas that are not armed continue to show a dash. You can arm other areas at any time.

If exit delay is active, the buzzer sound for the keypad will keep going off for the entire programmed exit delay period.

Figure 5-1 Total arming



```
31/08/18          17:30
T T T T – – – –
```

### 5.1.2 Partition 1 Arming

Partition arming 1 activates partial protection by arming part of the system and activating a predefined group of detectors.

Step 1 Confirm that all zones are ready to be armed, which means that an * must not be in place of the dash in the second line of the LCD display.

To identify which zone is not ready, do the following:

1) Press and hold the numeric key (from 1 to 8) where the * character appears.
2) The first set of open zones are shown on the diaplay.
3) Press ⌃ ⌄ to scroll up or down the page to show other zones that are not ready.
4) After these zones are identified, you can send person to do the onsite examination or

go to the **ZONE MANAGER** menu to set bypass for these zones.

Step 2 Enter your user code, and then press P1.

The numbers of areas that are ready to be armed are shown on the second line of the LCD display.

Step 3 Select the areas that need to be armed by pressing the corresponding numeric key (from 1 to 8).

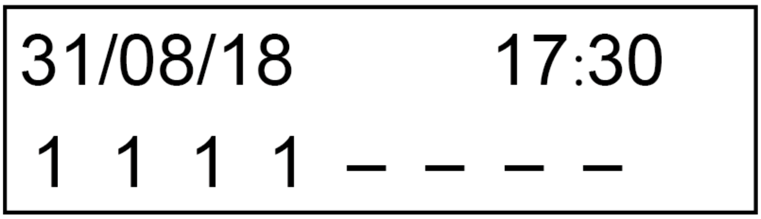
Step 4 Press ENTER to arm the system.

The keypad emits a confirmation buzzer.

The armed area shows the number **1**, and the corresponding LED indicator lights up. The areas that are not armed continue to show a dash. You can arm other areas at any time.

If exit delay is active, the keypad keeps sounding a buzzer for the entire programmed exit delay period.

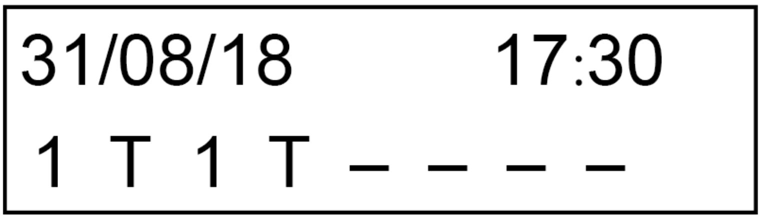
Figure 5-2 Partition arming 1



```
31/08/18        17:30
1 1 1 1 – – – –
```

The areas can be armed in different and mixed modes, for example, you can have 2 areas that are in total arming mode and 2 other areas that have partition arming 1.

Figure 5-3 Mixed arming 1



```
31/08/18        17:30
1 T 1 T – – – –
```

### 5.1.3 Partition 2 Arming

Partition arming 2 activates partial protection by arming part of the system and activating a predefined group of detectors.

Step 1 Confirm that all zones are ready to be armed, which means there must not be any * character in the place of dash in the second line of the LCD display.

To identify which zone is not ready, do the following:

1) Press and hold the numeric key (from 1 to 8) where the * character appears.
2) The first open zone shows on the display.
3) Press ˄ ˅ to scroll up or down the page to show other not ready Zones.
4) After these zones are identified, you can send person to do the onsite examination or go to **ZONE MANAGER** menu to set bypass for these zones.

Step 2 Enter your user code, and then press P2 Zone.

The numbers of areas ready for arming are shown on the second line of the LCD display.

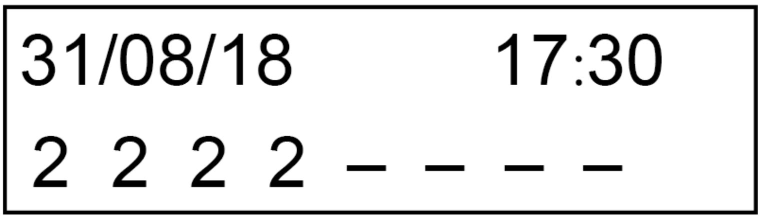
Step 3 Select the areas that need to be involved in the arming by pressing the corresponding numeric key (from 1 to 8).

Step 4 Press ENTER to do the arming.

The keypad emits a confirmation buzzer. The armed area shows the number **2**, and the corresponding LED indicator lights up. The areas that are not armed continues to show a dash. You can add other areas to the arming at any time.

If the exit delay is active, the keypad keeps sounding a buzzer for the entire programmed exit delay period.

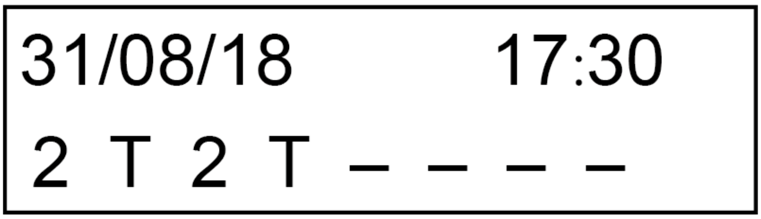
Figure 5-4 Partition arming 2



```
31/08/18        17:30
2 2 2 2 – – – –
```

The areas can be armed in different and mixed modes, for example, you can have two areas have total arming mode, and two areas have partition arming 2 mode.

Figure 5-5 Mixed arming 2



```
31/08/18        17:30
2 T 2 T – – – –
```

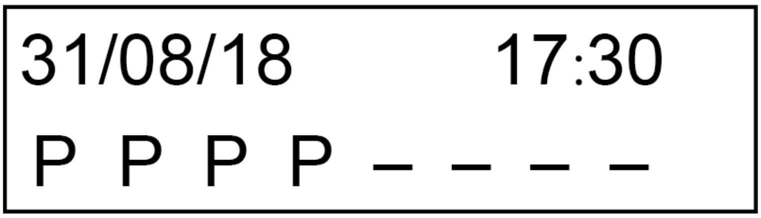
## 5.1.4 Partition 1+2 Arming

Partition arming 1 + partition arming 2 activates partial protection by arming part of the system and activating the detectors that belong to these two partitions.

To perform partition arming 1 + partition arming 2, you must arm one of the two partitions while the other is already armed (the order does not matter).

After the arming operation is complete, the armed area shows the upper case **P**.

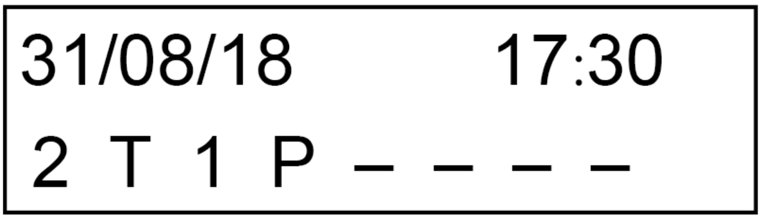
Figure 5-6 Partition arming 1 and partition arming 2



```
31/08/18        17:30
P P P P – – – –
```

The areas can be armed in different and mixed modes, for example, you can apply partition arming 1, partition arming 2 and total arming mode for different section at the same time.

Figure 5-7 Mixed arming



31/08/18 17:30

2 T 1 P – – – –

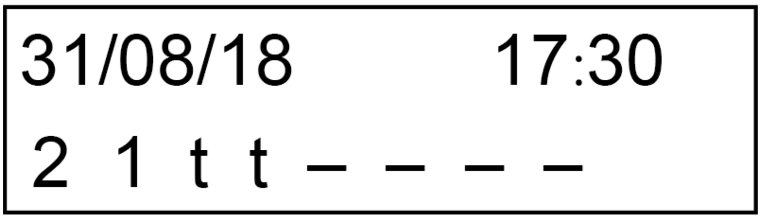
## 5.1.5 Forced Arming

Forced arming allows you to override when the system is not ready to be armed because of open zones, without any additional operations. This type of arming can be useful when zones, such a windows or door, are open or not ready to be armed, and you know their status ad wish to leave them open. Another instance where forced arming is useful is when one or more sensors are in a **TROUBLE** condition but you do not want to put them into bypassed status.

After forced arming has been set, the bypass LED indicator lights up showing that some detectors are set to automatically bypassed. If forced arming is set for the whole area, a lower case **t** is shown on the LCD display.

- Forced arming could inhibit sensors that you did not wish to bypass from arming without you realizing it.
- After they are disarmed, all the detectors involved in forced arming will become available for arming again.
- You cannot operate forced arming if the following alarms were triggered:
  - ◇ Zone masking alarm, zone short circuit alarm, and zone tamper alarm.
  - ◇ Power failure alarm and low battery voltage alarm.
  - ◇ Hold-up alarm or robbery alarm.

Figure 5-8 Forced arming



31/08/18 17:30

2 1 t t – – – –

## 5.1.6 Rapid Arming

To use rapid arming, the technician must have programmed the keypad. Otherwise, the keypad cannot perform the rapid arming.

Rapid arming allows you to arm the alarm system without entering the user code. The only difference between rapid arming and arming with the code is the practicality of performing the operation quickly. To disarm the system, you must type in a valid code.

Step 1 Press and hold Total Fn for the arming that you require on the areas that belong to the keypad.

You can also arm the system with **IMMEDIATE** or **DELAYED** exit time for rapid arming if this is programmed by the technician.

Step 2 (Optional) To disarm from rapid arming, you need to type in a valid user code.

### 5.1.7 Arming through Timer

You can arm the alarm system by timer that is set on the **SYSTEM TIMER** menu.
This setting can be managed and programed by the technician, supervisor, and manager.
The system also supports programming **HOLIDAYS** during which the timer will not have any effect.

### 5.1.8 Arming from Remote

The alarm system can also be armed from your phone through a specific procedure with an interactive vocal guide or through SMS messages.

## 5.2 Disarming

When you disarm the system, all the connected detectors are deactivated.
The system supports the following types of arming:

- Total Disarming
- Disarming through Timer
- Disarming through Telephone or SMS text
- Disarming under Duress
- Disarming from dialing or SMS, VTH, card, DSS Professional app, DMSS app

### 5.2.1 Total Disarming from the Keypad

You can perform disarming when there is an alarm or you just want to disarm.

Step 1 Enter the user code on the keypad.

Step 2 Press DISARM >.

The area that can be disarmed is shown on the LCD display.

Step 3 Press the corresponding key on the keypad to the area that you want to disarm.

Step 4 Press ENTER to fully disarm the area.

### 5.2.2 Total Disarming with the Timer

You can disarm the alarm system by a timer that is set on the **SYSTEM TIMER** menu.
This setting can be managed and programed by the technician and supervisor user.
The system also supports programming **HOLIDAYS** during which the timer will not have any effect.

## 5.2.3 Total Disarming through Telephone or SMS

The alarm system can also be disarmed from your phone through a specific procedure with an interactive vocal guide or through SMS text messages.

## 5.2.4 Disarming under Duress

You can perform disarming through a changed user code or a specific duress code to trigger a duress alarm. 1234 is an example of a normal user code. You can increase or decrease the last figure.

Step 1 Enter the changed user code, for example, 1235.

Step 2 Press DISARM >.

The area that can be disarmed is shown on the LCD display.

Step 3 Press the corresponding key on the keypad for the area that you want to disarm.

Step 4 Press ENTER to fully disarm the area.

# 6 User Menu

This chapter describes the operations included in the user menu.

The user menu consists of many menus for management and programming operations. They are as below:

- ZONE TROUBLES
- SYSTEM TROUBLES
- ZONES MANAGER
- LOGBOOK EVENT
- CHIME ZONES
- ACCESS CODES
- TECHNICIAN
- FIRMWARE VERSION
- WALK TEST
- SYSTEM TIMERS
- DATE/TIME
- HOLIDAY
- TEL NUMBERS
- REMOTE SERVICE
- SECURITY CODE
- RFID CARDS

To enter the user menu, you need an access code. So the user menu is accessible from the codes that have an appropriate security level. The factory default user code is 1234, which is also the user code of the supervisor user with the highest authority.

It is possible to scroll through the menus by the up and down arrow keys, or to go directly to the required menu by pressing the number of the menu + Menu.

To exit from the user menu, press ESC until the keypad requests **EXIT FROM MENU?**, then press ENTER to confirm or press ESC again to cancel.

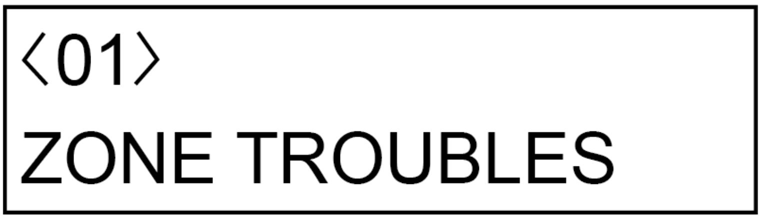
## 6.1 Zone Troubles

The **ZONE TROUBLES** menu examines which zones are in the **NOT READY** status and the reason for the fault. It then judges if it is necessary to close it or bypass it.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLES** menu is shown on the LCD display.

Figure 6-1 Zone troubles


〈01〉

ZONE TROUBLES

Step 2 Press ENTER to enter the menu.

- If there are no fault zones, the screen shows **NO TROUBLE**.
- If there are zones in trouble, then any of these 3 categories will appear: **TAMPER**, **SHORT**, and **MASK**.

Step 3 Press ENTER to enter programming mode.

Table 6-1 Zone troubles programming

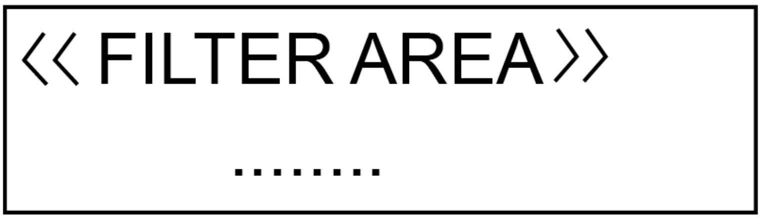
| Option | Description |
|---|---|
| Trouble type | Shows the type of trouble.<br>● **TAMPER**: Tampering detectors.<br>● **SHORT**: Short circuit.<br>● **MASK**: Anti-shielding. |
| STATUS | ● A: **ACTIVE**<br>The Zone is in normal condition.<br>● I: **ISOLATE**<br>The zone is excluded (removed) permanently and can be brought back only by switching to **ACTIVE**.<br>● B: **BYPASSED**<br>The zone is temporarily bypassed from arming of the system. The zone can be re-armed when the area is disarmed. |

If there are many trouble zones, you can set a search filter by **AREA** and **ACTIVATION STATUS** as below.

- Filter by **AREA**: Press Total Fn + 1 (F1).

Press the corresponding numeric keys of areas that you want to search for, and then press ENTER to start filtering.

Figure 6-2 Filter by Area

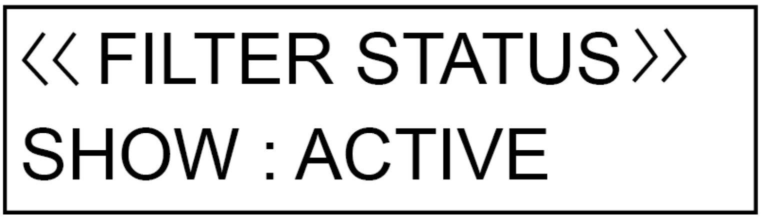

〈〈 FILTER AREA 〉〉

........

- Filter by **ACTIVATION STATUS**: Press Total Fn + 2 (F2).

  Press ∧ ∨ to set the searching criterion: **ALL**, **BYPASSED**, **TEST**, **ISOLATE**, and **ACTIVE**.

Figure 6-3 Filter by activation status



《 FILTER STATUS 》
SHOW : ACTIVE

Step 4 Press ENTER to confirm the setting, and then press ESC to return to the **ZONE TROUBLES** menu.

Then you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

## 6.2 System Troubles

The **SYSTEM TROUBLES** menu examines which faults are present in the alarm system. If the fault LED indicator glows or flashes, a system fault might be present.
To find what the fault is, you need to enter the **SYSTEM TROUBLES** menu as below:

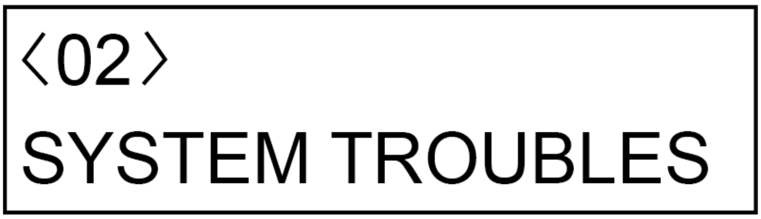
Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display

Step 2 Press ˄ ˅ to scroll up or down until you reach the **SYSTEM TROURBLES** menu, and then press ENTER.

- No system faults.

Figure 6-4 System troubles



〈02〉
SYSTEM TROUBLES

- If there are system troubles, then any of these 3 categories will appear: **TAMPER**, **TROUBLE**, and **COM TROUBLE**.

Table 6-2 System troubles programming

| Option | Description |
|---|---|
| TAMPER | ● **Panel Tamper**<br>● **Siren Tamper**<br>● **Module Tamper** |

| Option | Description |
|---|---|
| TROUBLE | ● System date and time<br>● 220 VAC main supply<br>● Low battery<br>● Battery trouble<br>● PSTN line<br>● GSM line<br>● Antenna fault<br>● SIM expiration<br>● PWD default |
| COM TROUBLE | Device fault (such as keypad and module) |

Step 3 Press ENTER to confirm the setting, and then press ESC to return to the **SYSTEM TROUBLES** menu.

Then you can press ∧ ∨ to move to the next menu or press ESC to exit from the user menu.

## 6.3 Zone Manager

The **ZONES MANAGER** menu allows any zone of the system to be placed in bypassed regardless of its current status (open or trouble).

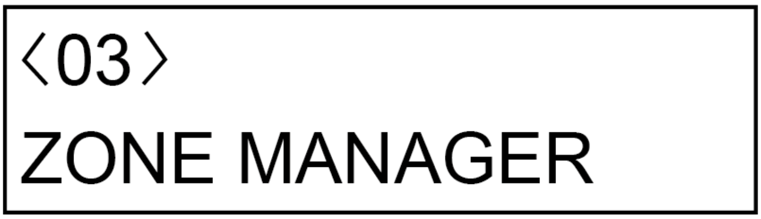
Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ∧ ∨ to scroll up or down until you reach the **ZONE MANAGER** menu, and then press ENTER.

The **ZONE MANAGER** menu is shown on the LCD display.

Figure 6-5 Zone manager



〈03〉

ZONE MANAGER

Step 3 Press ∧ ∨ to select the desired zone, and then press ENTER.

The submenu for changing status is shown.

Step 4 Press ∧ ∨ to select the status for the desired zone.

- **ACTIVE**: The zone is in normal condition.
- **ISOLATE**: The zone is excluded permanently and can be brought back only by switching to **ACTIVE**.
- **BYPASSED**: The zone is temporarily bypassed from arming of the system. The zone can be re-armed when the area is disarmed.

Step 5 Press ENTER to confirm the setting, and then press ESC to return to the wired zones selection menu.

Then you can continue with programming other wired zones, or press ESC to return to the **ZONE MANAGER** menu from where you can press ^ ˅ to move to the next menu or press ESC to exit from the user menu.

- Repeat the previous steps to manage other zones if needed.
- If there are many trouble zones that you want to manage, you can set a search filter by **AREA** and **ACTIVATION STATUS**.

## 6.4 Logbook Event

The **LOGBOOK EVENT** menu contains all the controller events with their respective date and time, such as alarms, arming and disarming, faults.

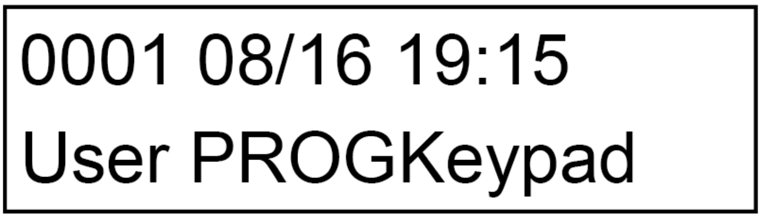
The events are shown from the most recent to the oldest, and when the event memory is full, the oldest events make room for the most recent ones.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display

Step 2 Press ^ ˅ to scroll up or down until you reach the **LOGBOOK EVENT** menu, and then press ENTER to enter the screen that shows the latest stored event.

Figure 6-6 The latest stored event



```
0001 08/16 19:15
User PROGKeypad
```

- The first line shows the event with its number and the date and time.
- The second line shows event details.

Step 3 Press ^ ˅ to select the event, and then press ENTER to extend the display to view more details on the event.

Step 4 Press ESC to return to the log event selection menu.

Then you can continue viewing other log events, or press ESC to return to the **LOGBOOK EVENT** menu from where you can press ^ ˅ to move to the next menu or press ESC to exit from the user menu.

# 6.5 Chime Zones

The **CHIME ZONES** menu is useful for obtaining a keypad buzzer sound whenever a specific zone is affected while the system is disarmed. This function is particularly useful for monitoring the presence of persons in particular zones or the opening of a door or window.

The **CHIME ZONES** menu activates chime mode for an individual zone. Only the zones defined by the technician as **CHIME Zones** can be activated in chime mode.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **CHIME ZONES** menu, and then press ENTER.

- If the technician did not program any zone with chime mode, the screen shows **NO FOUND**.
- If the technician programmed the zone with chime mode, continue the operations.

Step 3 Press ˄ ˅ to select **YES** or **NO**.

Step 4 Press ENTER to confirm the setting, and then press ESC to return to the **CHIME ZONES** menu.

Then you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

- Repeat the previous steps to set chime mode for other zones if needed.
- If there are many zones that you want to set chime mode for, you can set a search filter by **AREA** and **ACTIVATION STATUS**.

# 6.6 Access Codes

The **ACCESS CODES** menu allows you to customize the user codes for accessing the controller. Each user is assigned with a code that is linked with an authority level. Users with high authority can perform most operations in the system, and those with low authority are restricted to certain operations.

## 6.6.1 Authority Level

Table 6-3 Authority level

| User type | Authority level |
|---|---|
| Supervisor | Full control over all operations of all areas. Factory default setting is 1234. |
| Manager | Control over operations in areas allowed by the keypad. The manager can change his own code, and codes and authorities of lower levels, but cannot change the supervisor code. |

| User type | Authority level |
|---|---|
| Master | Only has control over operations assigned to the master. The master can only change his own code and those of a lower level and access the user menu up to option 9. |
| User | Only has control over operations assigned to the user. The user can only change his own code and access the user Menu up to option 8. |
| Temporary | Only has control over arming and disarming operations. Temporary does not have access to the user menu. |
| Duress | Only has control over arming and disarming operations and automatic report of the duress alarms. Duress does not have access to the user menu. |
| Patrol | Only has control over disarming operations. When the patrol time ends, the zones are automatically armed again. |

## 6.6.2 Configuring Authority Level

Step 1 Enter the access code, and then press Menu.

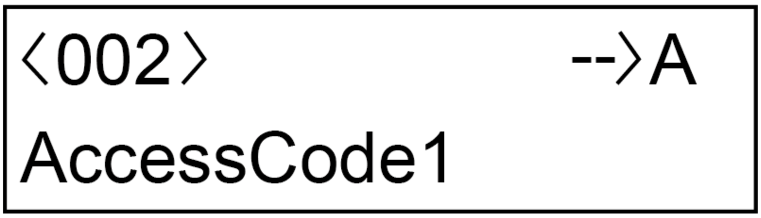
The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **ACCESS CODES** menu, and then press ENTER.

The access code 1 submenu is shown.

Access code 1 is always the supervisor code. From 2 onwards it is possible to program users with an authority level. You can set up to 99 access codes.

Figure 6-7 Access Code 1



```
<002>          -->A
AccessCode1
```

Step 3 Press ˄ ˅ to select a desired access code, and then press ENTER to enter the programming mode.

Step 4 Set the authority parameters.

- For supervisor and manager, you only need to set **STATUS**, **LEVEL**, **ARMING**, **FORCED ARM**, and **LINK** submenus. For master, user, temporary, and duress, you must set all the submenus.
- In each submenu, press ˄ ˅ to alter the options. After setting each submenu, press ENTER to enter the next submenu.

Table 6-4 Access code level and submenus

| Submenu | Setting |
|---|---|
| STATUS | Set the code to an operating or non-operating status.<br>● **ACTIVE**<br>● **ISOLATE** |
| LEVEL | Give an authority level to the user. |
| AREAS | Establish which areas the access code can be used for. |
| PART1 | Establish whether the access code can operate partition 1 and partition 2 arming types under the selected areas. |
| PART2 | |
| ARM | Establish whether the access code has the authority to arm or disarm the controller.<br>● **YES**<br>● **NO**<br>● **YES LINK 4**: The access code can link output 4 when arming or disarming. |
| DISARM | Establish whether the access code has the authority to arm or disarm the Control Panel.<br>● **YES**<br>● **NO**<br>● **YES LINK 4**: The access code can link output 4 when arming or disarming. |
| ARMING | Establish whether the code, when armed, can grant access to activate the system immediately or leaving area exit delays.<br>● **IMMEDIATE**<br>● **DELAYED**<br>📖<br>During delayed periods, the keypad buzzer will beep once every second. When you disarm in the same way, delayed arming will be cancelled. |
| FORCED ARM | Establish whether the code can grant access to arm the system even with alarm detectors in a not ready status. For example, windows left open deliberately or defective sensors.<br>● **YES**<br>● **NO** |
| STOP CALL | Establish whether the access code can grant access to answer or stop a phone call when there is a telephone call in progress.<br>● **YES**<br>● **NO** |
| ZONE STATUS | Establish whether the access code can grant access to change the zone status, for example, from **ACTIVE** to **DISALED**.<br>● **YES**<br>● **NO** |

| Submenu | Setting |
|---|---|
| REMOTE | Establish whether the access code can grant access to control the controller through a phone call or SMS.<br>● **YES**<br>● **NO** |
| TIMER | Establish whether the access code is limited to operation only during certain time periods.<br>There are 4 timers that can be set for the access code, and each timer can select from eight timers that are configured in the system. If you select 0, the access code can operate during the whole period instead of during limited time periods. |
| LINK 1, 2, 3, 4 | Establish whether the access code can grant access to the authorization to activate command outputs (maximum 4) and set the number of outputs to be activated.<br>● This function is valid only when the Link type is selected in the **OUTPUT** menu of the installer menu.<br>● The output to be activated must set the categories item to **LINK** type by the technician on the **OUTPUTS** menu. |
| NEW CODE | Enter a new code that contains from 4 to 6 digits. It cannot start with 0. |

Step 5 Press ENTER to confirm all the settings, and then press ESC to return to the access codes selection menu.

Then you can continue with programming other access codes, or press ESC to return to the **ACCESS CODES** menu from where you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

## 6.6.3 Configuring Access Code

### 6.6.3.1 Setting an Access Code

If you want to set or change an access code, follow the steps described in "6.6.3 Configuring Access Code" to enter the **NEW CODE** submenu.

Step 1 In the **NEW CODE** menu, enter the new code, and then press ENTER.

The confirmation text **PWD VALID** is displayed.

Step 2 Enter the new code again, and then press ENTER to save the new code.

If the code is not valid or was entered incorrectly, the operation will not successful and 2 beeps will be sounded with the text **PWD INVALID** to confirm the error. In this case, repeat the operation correctly.

Step 3 Press ESC to exit.

### 6.6.3.2 Deleting an Access Code

Access code 1 cannot be deleted.

Step 1 On the **ACCESS CODE** submenu, for example, access code 2, press and hold BYP < for at least three seconds.

The **NO PRESENT** message is shown to indicate that the access code was deleted.

Step 2 Press ESC to exit.

A cancelled access code is no longer operational but can be reactivated by a user with an appropriate authority level such as supervisor.

### 6.6.3.3 Customizing the Description of Access Code

You can customize the factory default description (access code no.) if needed.

Step 1 On the **NEW CODE** submenu, for example, access code 2, and press Total Fn + 2 (F2) to enter the editing status.

Step 2 Press BYP < and DISARM > to move to the position of the description, and then enter the character by using the specific key (0 to 9).

Step 3 Press ENTER to save the description.

Step 4 Press ESC to exit from the submenu or press ENTER to continue.

## 6.7 Technician

The purpose of the **TECHINCIAN** menu is to authorize the technician to access the installer menu. Otherwise, the technician cannot make any programming changes to the controller without your authorization.

In practice, for the technician to be able to access programming, the **TECHINCIAN** must be authorized by a valid user code (temporary, duress and patrol are not valid).

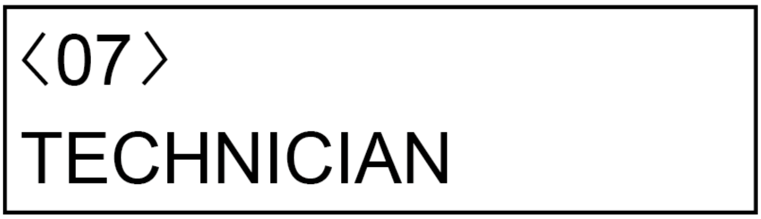
The operation is confirmed with the sound of 3 beeps and makes the technician code operational, authorizing it for set period of time. The period can be set from 1 hour to 10 hours in the **SYSTEM TIMING** menu of the installer menu.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ^ ˅ to scroll up or down until you reach the **TEHCNICIAN** menu.

Figure 6-8 Technician menu



〈07〉
TECHNICIAN

Step 3 Press ENTER.

3 beeps confirms that the technician code is operational, authorizing it for a set period of time.

Step 4 Press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

## 6.8 Firmware Version

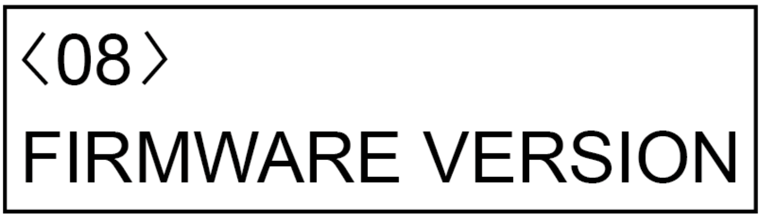
The **FIREWARE VERSION** examines the version of software installed in the controller and the keypad. If necessary, specify it to your technician. The controller can be updated to more recent versions.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **FIRMWARE VERSION** menu.

Figure 6-9 Firmware version



〈08〉
FIRMWARE VERSION

Step 3 Press ENTER to show the controller's version, and then press ENTER again to switch to show the keypad version.

Step 4 Press ESC to return to the **FIREWARE VERSION** menu.

Then you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

## 6.9 Walk Test

The **WALK TEST** menu tests the functionality of the installed detectors and examines the response of the **OPEN/CLOSED/TAMPER/FAILURE** status to the controller.

- Only the zones with the **ACTIVE** status can be tested.

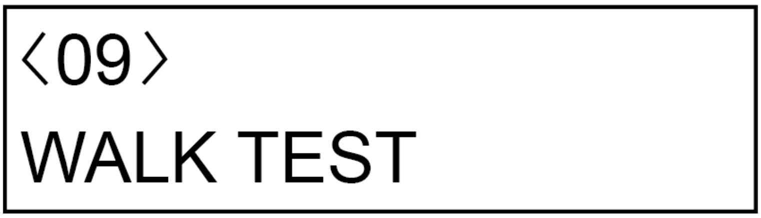
- When the system is in the armed status, entering **WALK TEST** menu prompts the unauthorized message.
- When one Keypad has entered the walk test mode, other keypads shows **OUT OF USE**.
- The **WALK TEST** menu cannot return to the main screen automatically.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ∧ ∨ to scroll up or down until you reach the **WALK TEST** menu.

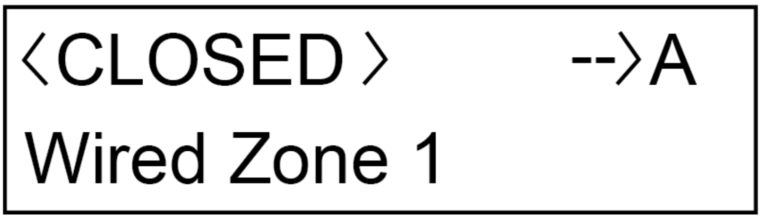
Figure 6-10 Walk test



〈09〉
WALK TEST

Step 3 Press ENTER to enter the screen that shows the status of the connected detectors: **CLOSED**, **OPEN**, **TAMPER**, **SHORT**, and **MASK**.

Figure 6-11 Test menu



〈CLOSED〉 --〉A
Wired Zone 1

Step 4 Press Total Fn + 3 (F3) to switch between A (multiple test) and B (individual test).

- If you select A, only triggered zones are shown.
- If you select B, you can press ∧ ∨ to select another zone to be tested.

Step 5 Press ESC to return to the **WALK TEST** menu.

Then you can press ∧ ∨ to move to the next menu or press ESC to exit from the user menu.

## 6.10 System Timers

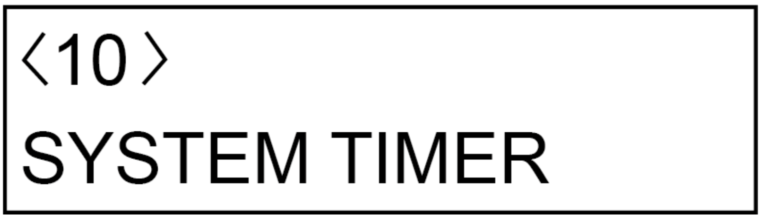
**SYSTEM TIMERS** sets the start and stop time and days of the week for each timer. **SYSTEM TIMERS** can be used in other submenu settings named timer. The timer can be used for timed arming and disarming of specific areas, authorizing codes to work within time limits, and timed activation and deactivation of specific controller outputs.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ∧ ∨ to scroll up or down until you reach the **SYSTEM TIMERS** menu.

Figure 6-12 System timer



〈10〉

SYSTEM TIMER

Step 3 Press ENTER to enter the submenu from where you can select a desired timer that you want to set (8 timers in total).

By pressing Total + 2 (F2), you can enter **EDITING** mode to change the description of timer.

Step 4 Press ˄ ˅ and ˄ ˅ to select a timer, and then press ENTER to enter programming mode.

Step 5 Configure timer settings.

On each submenu, press ˄ ˅ to alter the options. After each submenu is set, press ENTER to enter the next submenu.

Table 6-5 Timer settings description

| Submenu | Setting |
|---|---|
| STATUS | ● **ACTIVE**: Timer enabled.<br>● **ISOLATE**: Timer enabled by temporarily locked, but you can still continue to configure other settings.<br>● **OFF**: Timer is completely disabled, and you cannot continue to the next pages of settings. |
| TYPE | ● **START ONLY**: Used only for automatic arming operations.<br>● **STOP ONLY**: Used only for automatic disarming operations.<br>● **START/STOP**: Used only for both automatic arming and disarming operations. |
| START TIME | Enter the start time for automatic arming by pressing the corresponding keys and then press Menu to confirm the value. You can also press ˄ ˅ to change the value. |
| STOP TIME | Enter the start time for automatic disarming by pressing the corresponding keys and then press Menu to confirm the value. You can also press ˄ ˅ to change the value. |
| DAYS | Select the week days to be active for the Timer.<br>Press Key 1 to 7 to select the days (**M T W T F S S**). |

| Submenu | Setting |
|---|---|
| HOLIDAYS | Establish whether the timer being programmed.<br>● **YES**: The timer is blocked during the holiday periods. For example, if associated with the arming/disarming of areas, it no longer causes disarming during the holiday period. If associated with a code, remote controls or outputs, these will no longer be operative during the holiday period.<br>● **NO**: The timer does not follow the holiday conditions, and therefore remains active regardless of what is associated with it. |
| ARMING | Select the type of arming for the timer.<br>● **DELAYED**<br>● **IMMEDIATE** |
| FORCEDARM | Select whether the timer arming will be forced.<br>● **YES**<br>● **NO** |

Step 6 Press ESC to return to the timer selection menu.

Then you can continue with programming other timers, or press ESC to return to the **SYSTEM TIMER** menu from where you can press ∧ ∨ to move to the next menu or press ESC to exit from the user menu.

📖

You will be notified 1 minute before timed arming begins, and the keypad will beep once every 2 seconds. Press ESC to cancel arming.

## 6.11 Date and Time

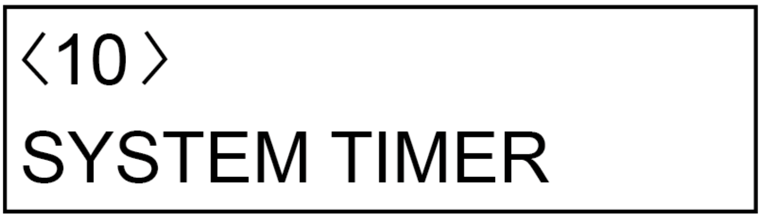
The **DATE/TIME** menu sets the time of the controller.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ∧ ∨ to scroll up or down until you reach the **DATE/TIME** menu.

Figure 6-13 Date and time



〈10〉

SYSTEM TIMER

Step 3 Press ENTER to enter programming mode.

Enter the value, press Menu to show the value, then press ENTER to confirm the value. You can also press ˄ ˅ to change the value, and press ENTER to move to the next editing.

Table 6-6 Date and time settings

| Submenu | Setting |
|---|---|
| TIME | Set the time for the controller. |
| DATE | Set the date for the controller (day/month/year). |
| DST ENABLE | Enable the DST function. You can select from **YES** and **NO**. |
| SOL TO LEG | Set the day and the month for the automatic change of time from **Solar** to **Legal**. |
| LEG TO SOL | Set the day and the month for the automatic change of time from **Legal** to **Solar**. |
| EXPIRY | This function is supported only when the **SIM TYPE** is set to **CONTRACT** in the **COMMUNICATIOR** menu.<br>Set the expiration date of the SIM card installed in the GSM telephone communicator.<br>It is suggested to set a minimum period of 10 days before the real expiration of the SIM card so as to have adequate warning time to recharge it and extend its validity.<br>At the set date, the failure status LED indicator will light up. If programmed, SMS can be sent to an external phone number. Auxiliary outputs can also be activated for connection to local devices. |

Step 4 Press ENTER to confirm the settings.

Step 5 Press ESC to return to the **DATE/TIME** menu from where you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

## 6.12 Holiday

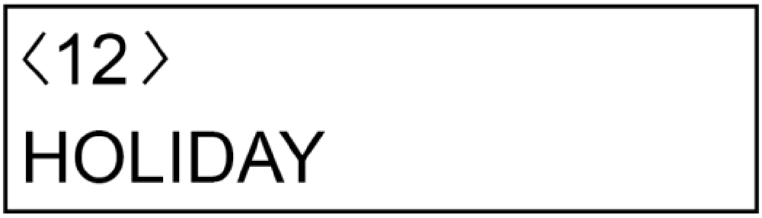
The **HOLIDAY** menu sets the holiday dates of the year when the timers must not affect the system. You can program up to 20 holidays, and a holiday period can consist of just one day.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **HOLIDAY** menu.

Figure 6-14 Holiday

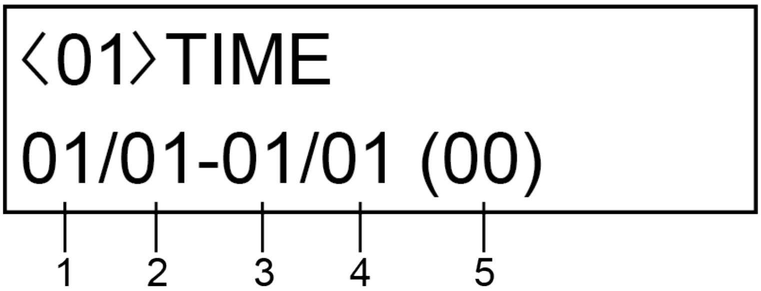

〈12〉
HOLIDAY

Step 3 Press ENTER to enter the submenu from where you can select a holiday that you want to program.

By pressing Total Fn + 2 (F2), you can enter **EDITING** mode to change the description of the holiday.

Step 4 Press ˄ ˅ to select a holiday, and then press ENTER to enter programming mode

Figure 6-15 Holiday programming



- 1: Holiday start day
- 2: Holiday start month
- 3: Holiday end day
- 4: Holiday end month
- 5: Holiday year

Step 5 Enter the value, press Menu to show the value, and then press ENTER to confirm the value. You can also press ˄ ˅ to change the value, and then move on to the next field.

Step 6 Press ENTER to confirm the setting.

Step 7 Press ESC to return to the holiday selection menu.

Then you can continue with programming other holidays, or press ESC to return to the **HOLIDAY** menu from where you can press ˄ ˅ to move to the next menu or press ESC to exit from the user menu.

To delete a holiday, on the holiday selection screen where the Holiday name is shown, press and hold BYP ‹ for at least three seconds.

## 6.13 Telephone Number

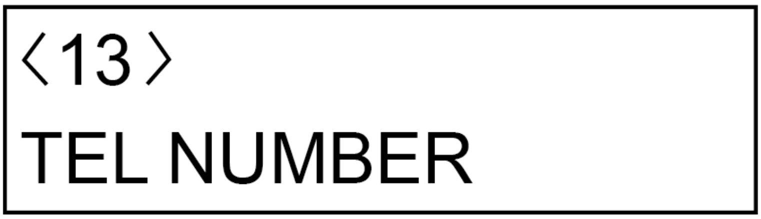
The **TEL NUMBER** menu sets the telephone numbers that will be used by the dialer for voice calls and SMS. You can program up to 8 different telephone numbers for audio messages, and 8 numbers for text SMS. You can also record the SIM card number that is installed in the controller.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **TEL NUMBER** menu,

Figure 6-16 Telephone number



⟨13⟩

TEL NUMBER

Step 3 Press ENTER to enter the screen from where you can select the submenus from **TEL NUM**, **SMS NUM**, and **SIM NUM** by pressing ˄ ˅.

Step 4 Configure the phone number submenu settings.

- **TEL NUM**
  1. On the **TEL NUM** submenu, press ENTER to enter the screen from where you can select a telephone number that you want to program by pressing ˄ ˅.
  2. After selecting a phone number, press ENTER to enter programming mode.
  3. Configure phone number settings.

Table 6-7 Telephone number setting

| Submenu | Setting |
|---|---|
| STATUS | ● **ACTIVE**: Allow the phone number to be called.<br>● **ISOLATE**: Do not allow the call in and out of the phone number. |
| STOP CYCLE | ● **YES**: When the alarm event occurs, if the event is programmed to link multiple telephone numbers, press # key on your phone to hang up the call, the calling will not link to other phone numbers.<br>● **NO**: When the alarm event occurs, if the event is programmed to link multiple phone numbers, the calling will continue to call other phone numbers although pressing # key on your phone. |

- **SMS NUM**
  1. On the **SMS NUM** submenu, press ENTER to enter the screen from where you can select a phone number that you want to program by pressing ˄ ˅.
  2. After selecting a telephone number, press ENTER to enter programming mode.
  3. Configure SMS number settings.

Table 6-8 SMS number setting

| Submenu | Setting |
|---|---|
| STATE | ● **ACTIVE**: Allow the SMS to be sent and received.<br>● **ISOLATE**: Do not allow the SMS to be sent and received. |
| SYSTEM | Press 1 to 7 to select the corresponding week days to send the system status message to this SMS number. |
| CREDIT | Press 1 to 7 to select the corresponding week days to send the balance information of the SIM card that is installed in the controller. |
| SMS TIME | Enter the specific time for **SYSTEM** and **CREDIT**. |

| Submenu | Setting |
|---|---|
| AREA | Press 1 to 8 to select the alarm event from which areas can be sent to this SMS number. |
| EVENT | Press 1 to 5 to select which event can be sent to this SMS number.<br>● 1: **S-system event**<br>● 2: **M-module**<br>● 3: **E-Emergency**<br>● 4: **I-Arm/Disarm**<br>● 5: **Z-Zones** |

4. Perform other actions

   ◇ Press Total Fn + 2 (F2) to enter **EDITING** mode to change phone number. You can enter up to a maximum of 24 digits. Use the horizontal cursor keys to move within the number. Any of the digits can be overwritten. By positioning at any point in the number (for example, at the start) and holding down, it is possible to delete all the digits from that point onwards (for example, deletion of the entire number).

   ◇ Press Total Fn + 3 (F3) to do a test call on this number.

   ◇ Press Total Fn + 4 (F4) to interrupt a call in progress at any time.

- **SIM NUM**

  Record the SIM card number that is installed in the controller.

Step 5 Press ESC to return to the **TEL NUMBER** menu.

Then you can press ⌃ ⌄ to move to the next menu or press ESC to exit from the user menu.

## 6.14 Remote Service

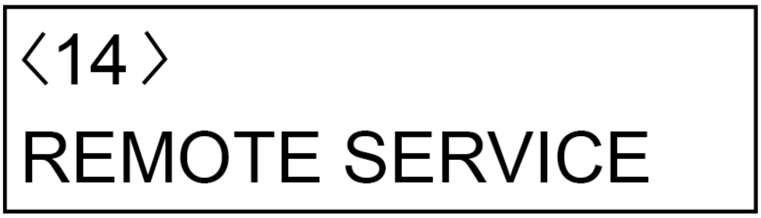
The **REMOTE SERVICE** menu gives the possibility to activate the alarm controller remotely by telephone from the control center of your installer.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ⌃ ⌄ to scroll up or down until you reach the **REMOTE SERVICE** menu.

Figure 6-17 Remote service



〈14〉

REMOTE SERVICE

Step 3 Press ENTER to enter programing mode.

Step 4 On the **STATE** submenu, select **YES** and **NO**.

- **YES**: Allows remote control by the Installer from telephone call, SMS, app, or platform.
- **NO**: Do not allow remote control by the Installer.

Step 5 Press ESC to return to the **REMOTE SERVICE** menu.

Then you can press ⌃ ⌄ to move to the next menu or press ESC to exit from the user menu.

## 6.15 Security Code

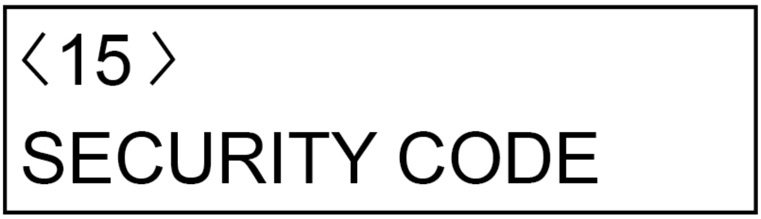
The **SECURITY CODE** menu sets the code that is used to protect your alarm controller from connecting with personal computers locally or remotely.

Step 1 Type in the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ⌃ ⌄ to scroll up or down until you reach the **SECURITY CODE** menu.

Figure 6-18 Security code

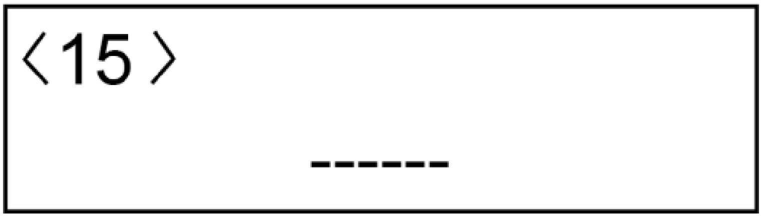


〈15〉

SECURITY CODE

Step 3 Press ENTER to enter programming mode.

Figure 6-19 Security code programming



〈15〉

------

Step 4 Enter a 4 to 6 digit code, and then press Menu.

The code is shown.

Step 5 Press ENTER to confirm and close code programing mode.

If the code has already been programmed, 6 asterisks will appear instead of dashes.

Step 6 Press ESC to return to the **SECURITY CODE** menu.

Then you can press ⌃ ⌄ to move to the next menu or press ESC to exit from the user menu.

## 6.16 RFID Cards

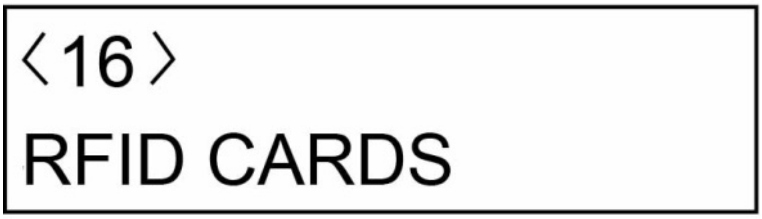
After adding Radio Frequency Identification (RFID) cards, you can use them to arm and disarm your areas by using a combination of card or card swiping with a password.

Step 1 Enter the access code, and then press Menu.

The **ZONE TROUBLE** menu is shown on the LCD display.

Step 2 Press ˄ ˅ to scroll up or down until you reach the **RFID CARDS** menu.

Figure 6-20 RFID cards

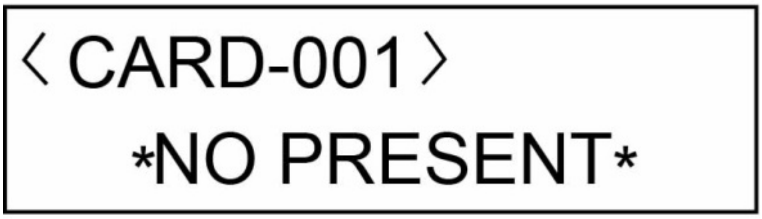


〈16〉

RFID CARDS

Step 3 Press ENTER to enter programing mode.

Figure 6-21 screen entered



〈CARD-001〉

*NO PRESENT*

Step 4 Configure the RFID card parameters.

- Up to 100 RFID cards can be set. Press ˄ ˅ to select one as needed, or you can press the card number and then press Menu to go to the desired card directly. For example, press 50 and then press Menu to go to CARD-050.
- For each card, press ENTER to enter the configuring screen. Press ˄ ˅ to alter the options. Press ENTER to confirm the setting and move to the next parameter. Press and hold BYP < to restore the configured card to default (**NO PRESENT** status).
- Press ESC to return to the upper menu.

Table 6-9 RFID card parameter descriptions

| Submenu | Descriptions |
|---|---|
| STATE | Set the card to an operating or non-operating status.<br>● A: **ACTIVE**<br>The RFID card is in normal condition.<br>● I: **ISOLATE**<br>The RFID card cannot be used, and can be activated again after it is switched to **ACTIVE** state. |

| Submenu | Descriptions |
|---|---|
| AREAS | Set one or multiple areas where the RFID card can be used. |
| ARMING | Set the arming status.<br>● **IMMEDIATE**<br>The area is immediately armed.<br>● **DELAYED**<br>The area is armed after the exit delay time, which can be set by the installer. |
| FORCED ARM | Set whether the area can be armed when alarm detectors are in a not ready status. For example, the window is open or in case of defective sensors.<br>● **YES**<br>● **NO** |
| ARMING METHOD | Set the arming method by using a combination of card swiping with a password.<br>● **CARD**<br>Swipe the card to arm the selected area.<br>● **CARD + PWD**<br>Swipe the card, and then enter the set password within 30 s to arm the selected area. |
| PASSWORD | If you select **CARD + PWD**, set a password with 4 to 6 digits. |
| PLEASE SWIPE | When the system prompts **Please swipe**, swipe the card on the card reader to register the card number, and the number will be displayed on the keypad LCD screen. |

# Appendix 1 Keypad Buzzer Sound

Appendix Table 1-1 Keypad sound

| Buzzer sound | Description |
|---|---|
| One slight beep | Keypad pressing. |
| One beep | Menu entering. |
| Continuous three beeps | ● Switching between the first menu and the last menu after log in to the system.<br>● Authorizing the technician to access installer menu. |
| Two beeps, first short and second long | ● Login fault.<br>● Access code modification fault.<br>● Bypass failed. |

# Appendix 2 Event Log Messages

Appendix Table 2-1 Event log messages

| Event message | Description | Event message | Description |
|---|---|---|---|
| AL.SF | Siren Fault | — | — |
| P1.Arm | Partitial1 Arm | AL. | Alarm |
| P2.Arm | Partitial2 Arm | S.T.RES | Siren Tamper Restore |
| AL.PAN. | Panic Alarm | AL.S.T | Siren Tamper Alarm |
| AL.ROB. | Robbery Alarm | TAM. | Tamper |
| AL.MED. | Medical Alarm | Keypad TAM. RES. | Keypad Tamper Restore |
| AL.Fire | Fire Alarm | AL.K.T | Keypad Tamper Alarm |
| WD.Zone | Wired Zone | COMM. | Communication |
| WD.Z |  | COMM.Restore | Communication Restore |
| AL.TAM. | Tamper Alarm | AL.C.T | Communication Trouble Alarm |
| AL.AM. | Anti-Mask Alarm | AL.COMM.Trouble |  |
| LOWBAT. | Low Battery | 2G/4G COMM.RES. | 2G/4G Communication Restore |
| WL.Zone | Wireless Zone | PSTN COMM.RES. | PSTN Communication Restore |
| WL.Z |  | PSTN ACT. | PSTN Activation |
| Access Code ERR. | Access Code Error | IN.MODU.TAM.RES. | Input Module Tamper Restore |
| PROG.Mode End | User Program Mode End | IN.M.T | Input Module Tamper |
| TECH.AUT.Expired | Technician Authorization Expired | AL.IN.Module TAM | Input Module Tamper Alarm |
| Technician AUT. | Technician Authorization | IN.Module | Input Module |
| User PROG.Mode | User Program Mode | OUT.MODU.TAM.RES | Output Module Tamper Restore |
| TECH.PROG.M | Technician Program Mode | OUT.M.T | Output Module Tamper |
| TECH.PROG.Mode |  | OUT.Module TAM. |  |
| TROU. | Trouble | WL. | Wireless |
| SYS.BAT.TROU. | System Battery Trouble | WL.IN.M.T.RES. | Wireless Input Module Tamper Restore |

| Event message | Description | Event message | Description |
|---|---|---|---|
| SYS.BAT.Low.VOL. | System Battery Low Voltage | WLI.M.T | Wireless Input Module Tamper |
| SYS.BAT. Restore | System Battery Restore | WL.IN.MODU.TAM | |
| SYS. | System | WL IN.Module | Wireless Input Module |
| RES. | Restore | — | |

When the following faults occur at the same time, the priority is as follows: A>B>C>D>E. In the same level, the subsequent time will be reported first.

A： Fire alarm, panic alarm, robbery alarm, medical alarm

B： Zone alarm

C： Fire trouble, zone short, zone tamper, zone mask, siren fault

D： System trouble

E： Modules tamper, modules trouble

# Appendix 3 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

**Mandatory actions to be taken for basic device network security:**

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

**"Nice to have" recommendations to improve your device network security:**

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

## More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883