



# Handheld Metal Detector

## User's Manual








# Foreword

## Model

DHI-ISC-H103

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

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

## Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2021

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the Detector, hazard prevention, and prevention of property damage. Read these contents carefully before using the Detector, comply with them when using, and keep the manual well for future reference.

## Operation Requirements



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

## Electrical Safety



- Do not connect the power adapter to the Detector after powering on. Connect the power adapter to the Detector when the power is off.
- Conform to the local electrical safety standards strictly to ensure that the ambient voltage is stable and meets the Detector power supply requirements.
- Do not provide two or more power supply methods to the device simultaneously, otherwise, it may cause Detector damages or safety risks.



- Safety helmets, safety belts, and protective measures are required for personnel working at heights to ensure personal safety.
- Do not place and install the Detector in direct sunlight or near heating devices.
- Do not install the Detector in a humid, dusty or soot place.
- Install the Detector in a well-ventilated place, and do not block its vents.
- Use the adapter or chassis power supply provided by the product manufacturer.
- The power source shall conform to the requirements of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirements according to GB8898 (IEC60065) or GB4943.1 (IEC60950-1). Please note that the power supply requirements are subject to the device label.
- Connect the I-type structure to the power socket with protective earthing.

# Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Overview</b> .....	<b>5</b>
1.1 Introduction .....	5
1.2 Operating Condition.....	5
1.3 Appearance.....	5
<b>2 Components</b> .....	<b>6</b>
2.1 Packing List .....	6
2.2 Components.....	6
<b>3 Parameters and Operations</b> .....	<b>7</b>
3.1 Parameters .....	7
3.2 Structure.....	7
3.3 Indicator .....	8
3.4 Detection Mode.....	8
3.5 Buttons .....	9
<b>Appendix 1 Cybersecurity Recommendations</b> .....	<b>11</b>

# 1 Overview

## 1.1 Introduction

- Model: DHI-ISC-H103
- Dimension:360\*82\*34 (length x width x height, mm)

## 1.2 Operating Condition

- Operating temperature:  $-25^{\circ}\text{C}\sim+60^{\circ}\text{C}$
- Relative humidity: 0~95%, non-condensing.
- Power requirement: 2\* AA batteries

## 1.3 Appearance

Figure 1-1 Product Appearance



# 2 Components

## 2.1 Packing List

Table 2-1 Checking list

Name	Quantity
Handheld Metal Detector	1
Charger	1
2 batteries	1

## 2.2 Components

Figure 2-1 Power adapter



# 3 Parameters and Operations

## 3.1 Parameters

Parameters	Descriptions
Dimension	360x82.5x 42.5 mm
Weight	270g
Battery	2* AA battery, standard equipment
Charger	Universal 5V USB charger (Applicable for mobile phone charger plug, PC USB port, etc.); NiMH AA battery charger
Power consumption	<60 Mw
Shell material	Mainly ABS and rubber
Operating temperature	-25C ~+60C
Relative humidity	0~95%, non-condensing.

## 3.2 Structure

Figure 3-1 Structure

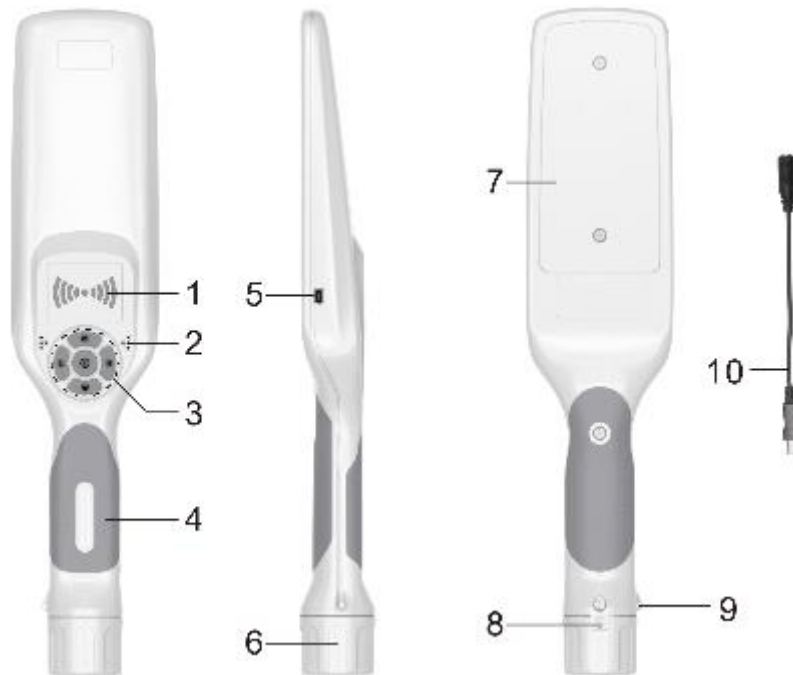


Figure 3-2 Structure descriptions

No.	Structure descriptions
1.	Indicator. For details, see 3.3Indicator.



No.	Structure descriptions
2.	Speaker
3.	Buttons. For details, see 3.5Buttons.
4.	Handle
5.	USB port
6.	Battery cover
7.	Detection area
8.	Fixing screws of battery cover
9.	Lanyard hole
10.	Conversion cable between USB and 3.5mm headphone

### 3.3 Indicator

Low battery: when in low battery status, the middle indicator quickly flashes.

Figure 3-3 Low battery indicator



Power status: when in charging status, the indicator circularly flashes as shown in Figure 3-4; when finishing charging, the indicator turns off.

Figure 3-4 Indicator in charging status



Alarm: 3-level alarm selectable. The larger and the closer the metal, the higher level of the metal alarm.

Figure 3-5 Alarm indicator

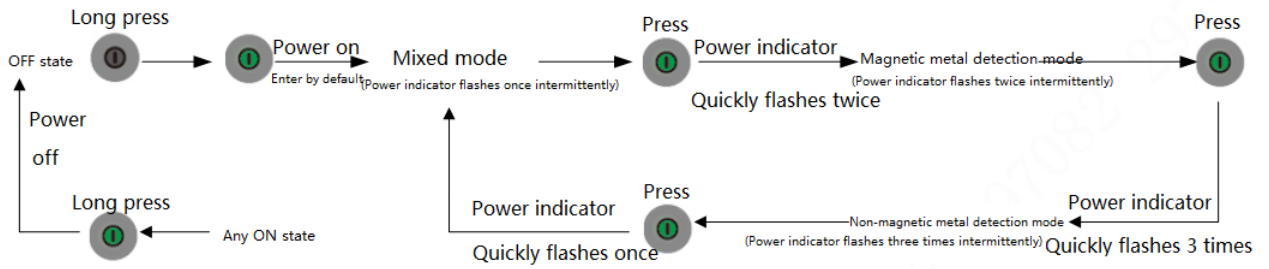


### 3.4 Detection Mode

Three detection modes:

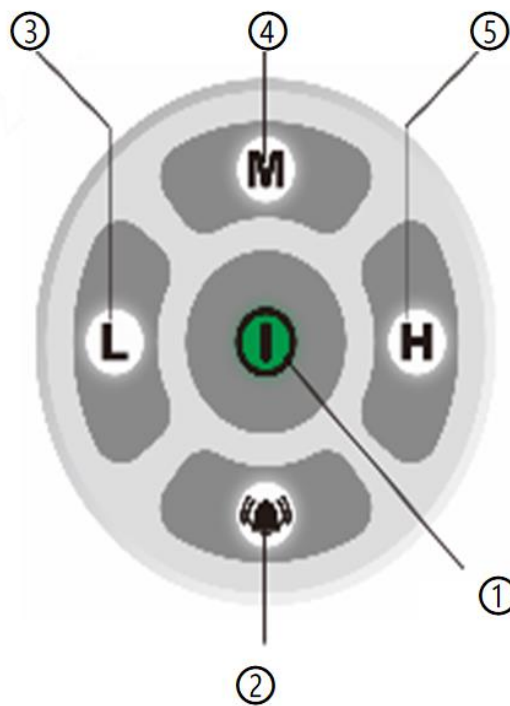
- Magnetic metal detection mode (no alarm for non-magnetic metals),
- Non-magnetic metal detection mode (no alarm for magnetic metals),
- Mixed mode (alarm for magnetic and non-magnetic metals).

Figure 3-6 Detection modes



### 3.5 Buttons


Figure 3-7 Buttons



One indicator per button to indicate the Detector working status.

Figure 3-8 Buttons

No.	Buttons	Descriptions
1.	① Power button	<ul style="list-style-type: none"> <li>• Long press to power on;</li> <li>• When Device is in working status, long press to power it off;</li> <li>• The Indicator flashes once every 3 seconds in working status.</li> </ul>

No.	Buttons	Descriptions
2.	② Alarm mode conversion button	<ul style="list-style-type: none"> <li>● Press the button for alarm mode circle switch as shown in the following order: sound-vibration-sound&amp;vibration-sound .</li> <li>● When in sound&amp;light alarm mode, no indicator flashes;</li> <li>● When in vibration&amp; light alarm mode, the indicator flashes every 3 seconds;</li> <li>● When in sound&amp;vibration&amp;light alarm mode, the indicator flashes every 1.5 seconds.</li> </ul>
3.	Sensitivity adjustment button ③ Low sensitivity button ④ Middle sensitivity button ⑤ High sensitivity button	<ul style="list-style-type: none"> <li>● 4-level sensitivity selectable: low, middle, high, and extra-high.</li> <li>● Select sensitivity level by pressing corresponding sensitivity adjustment button. The corresponding indicator flashes every 3 seconds:  </li> <li>● There is no direct button for extra-high sensitivity. If you want to select extra-high sensitivity, first press the high sensitivity button to select high sensitivity, and then long press the high sensitivity button for 3 seconds to switch to extra-high sensitivity.</li> <li>● In extra-high sensitivity status, no indicator will flash.</li> </ul>

# Appendix 1 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 procedures toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations 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;
- Do not use overlapped characters, such as 111;

### **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.) 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).

### **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 tunnel.

### **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.

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](http://www.dahuasecurity.com) | Postcode: 310053

Email: [overseas@dahuatech.com](mailto:overseas@dahuatech.com) | Fax: +86-571-87688815 | Tel: +86-571-87688883