Cámara de monitoreo de vista frontal

Manual de usuario

TECNOLOGÍA CO., LTD DE LA VISIÓN DE ZHEJIANG DAHUA V1.0.1

Prefacio

General

Este manual presenta las funciones y operaciones de la cámara de monitoreo de vista frontal (en lo sucesivo, "la cámara").

Modelos

DHI-DAE-CFM5210, DHI-DAE-CFM5211

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
PELIGRO	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría resultar en daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.1	Formato manual actualizado.	Septiembre 2021
V1.0.0	Primer lanzamiento.	Marzo 2021

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar los datos personales de otras personas, como su rostro, huellas dactilares y número de placa del automóvil. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcione la información de contacto requerida.

Acerca del manual

- El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No nos hacemos responsables de las pérdidas incurridas debido a la operación del producto en formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final. Actualice
- el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.
- Si existe alguna duda o controversia, nos reservamos el derecho a una explicación final.

Advertencias y salvaguardias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Dispositivo, la prevención de peligros y la prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo, cumpla con las pautas al usarlo y guarde el manual en un lugar seguro para futuras consultas.

Requisitos de operación

- Asegúrese de que la fuente de alimentación del dispositivo funcione correctamente antes de
- usarlo. No tire del cable de alimentación del dispositivo mientras está encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Transporte, utilice y almacene el dispositivo en condiciones de humedad y temperatura permitidas. Evite que los
- líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido en la parte superior del dispositivo para evitar que los líquidos fluyan hacia él.
- No desmonte el dispositivo.

requerimientos de instalación

 **ADVERTENCIA**

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente las normas de seguridad eléctrica locales y asegúrese de que el voltaje en el área sea constante y se ajuste a los requisitos de alimentación del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, el dispositivo podría dañarse.

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido provisto para su uso mientras trabaja en alturas.
- No exponga el dispositivo a la luz solar directa ni a fuentes de calor. No
- instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo. Utilice el adaptador de
- corriente o la fuente de alimentación de la carcasa proporcionada por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma IEC 62368-1 y no debe ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo. Conecte los aparatos
- eléctricos de clase I a una toma de corriente con toma de tierra de protección.

Tabla de contenido

1 Información del producto

1.1 Descripción general del producto

La cámara cumple con los estándares Dahua HDCVI, y admite la transmisión de datos con alta velocidad y sin demora. Debe ser controlado por HCVR, que cumple con los estándares HDCVI.

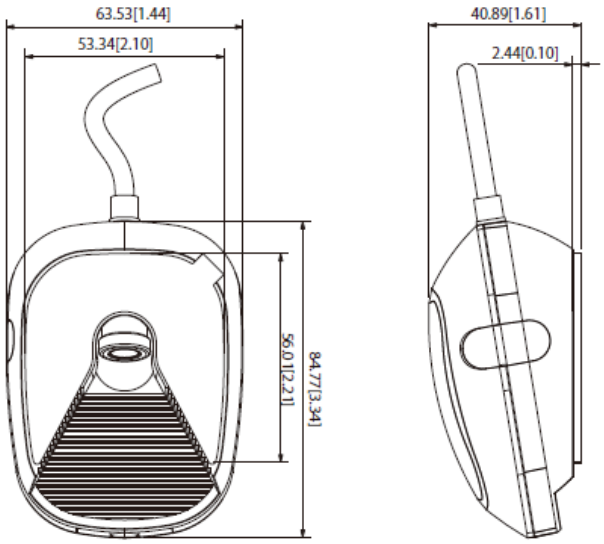
1.2 Función

- El sensor de imagen CMOS de alto rendimiento asegura imágenes de alta definición.
- Admite salida de video HDCVI.

2 Estructura

2.1 Dimensiones

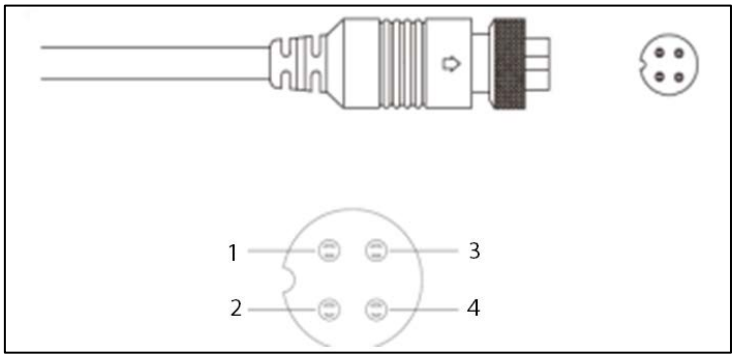
Figura 2-1 Dimensiones (mm [pulgadas])



2.2 Cable

Los cables son solo de referencia y pueden diferir del dispositivo real.

Figura 2-2 Cable



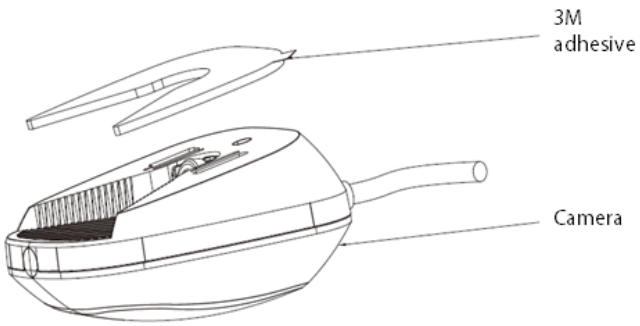
- 1: Video (amarillo).
- 2: Fuente de alimentación (rojo).
- 3: Línea de tierra de la fuente de alimentación
- (negra). 4: Línea de tierra de video (blanco).

3 Instalación

- Instale la cámara a tiempo después de desembalarla para evitar que el núcleo de la cámara quede expuesto en un ambiente húmedo durante mucho tiempo.
- La superficie de instalación, con cierto grosor, debe ser capaz de soportar al menos un peso 3 veces superior a la cámara.
- No rasgue ni tire la película adhesiva estática en la cubierta transparente, evitando que la lente se dañe, antes de completar la instalación y la puesta en servicio. No toque la cubierta después de romper la película. Asegúrese de que no queden huellas en la cámara.
- Esta sección toma algunos modelos como ejemplo. Son solo para referencia y pueden diferir del modelo real.

3.1 Instalación de la cámara

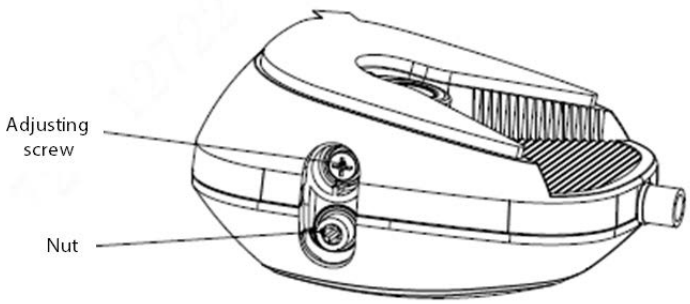
Figura 3-1 Instalación de cinta adhesiva



Paso 1 Saque la cámara y rompa la película protectora adhesiva 3M. Pegue la cámara a
Paso 2 la superficie de instalación de acuerdo con el rango de monitoreo. Conecte la
Paso 3 cámara al HCVR.
Etapa 4 Ajuste el ángulo de la cámara cuando la imagen de monitoreo se muestre en HCVR.

3.2 Ajuste de la cámara

Figura 3-2 Ajuste de la cámara



Paso 1 Quite el tapón de rosca y afloje el tornillo de ajuste. Asegúrese de que la cámara no

escabullirse.

Paso 2 Ajuste del campo de visión de la cámara a través de la tuerca.

Paso 3 Apriete los tornillos y vuelva a colocar la tapa después de completar el ajuste.

Para una calibración detallada de la cámara, consulte el manual del DVR.

Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación, se muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No incluya el nombre de la cuenta o el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc .;
- No utilice caracteres superpuestos, como 111, aaa, etc .;

2. Actualice el firmware y el software cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de dispositivos extraíbles (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Configure y actualice la información de restablecimiento de contraseñas oportunamente

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilite el bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión con la contraseña incorrecta varias veces, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio en cualquier conjunto de números entre 1024 ~ 65535, reduciendo el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilite HTTPS

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7. Enlace de dirección MAC

Le recomendamos que vincule la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

8. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda apagar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzones de correo.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, le recomendamos que utilice la función de transmisión encriptada, para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada provocará alguna pérdida en la eficiencia de transmisión.

11. Auditoría segura

- Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda que habilite la función de registro de red para asegurarse de que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP / MAC para limitar el rango de hosts permitidos para acceder al dispositivo.

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