AXIS C1310-E Mk II Network Horn Speaker

Altavoz para exterior de largo alcance y gran nitidez

El AXIS C1310-E Mk II Network Horn Speaker es perfecto para entornos de exterior en la mayoría de climas. Permite a los usuarios prevenir de forma remota actividades no deseadas, dar instrucciones durante una emergencia o enviar mensajes de voz generales. La memoria integrada admite mensajes grabados previamente, o el personal de seguridad puede responder a notificaciones con voz en directo. Los estándares abiertos son compatibles con la integración sencilla con el vídeo en red, el control de acceso, el análisis y la voz por IP (VoIP) (compatible con SIP). El procesamiento de señal digital (DSP) garantiza un sonido claro. El micrófono integrado permite realizar pruebas remotas del estado del sistema y comunicación bidireccional. Además, el software de gestión de audio integrado permite gestionar los usuario, el contenido, las zonas y la programación.

- > Sistema de altavoz integral
- > Conexión a la red estándar
- > Instalación sencilla con PoE
- > Pruebas remotas de estado del sistema
- > Ampliable y fácil de integrar

AXIS C1310-E Mk II Network Horn Speaker

Hardware de audio

Carcasa
Altavoz de bocina reentrante con motor de compresión

Nivel de presión de sonido máximo
>121 dB

Respuesta de frecuencia
280 Hz - 12.5 kHz

Patrón de cobertura
70° horizontal 100° vertical (a 2 kHz)

Entrada/salida de audio
Micrófono incorporado (puede ser desactivarse mecánicamente)
Altavoz integrado

Especificación del micrófono integrado
50 Hz - 12 kHz

Descripción del amplificador
Amplificador 7 W Clase D integrado

Procesamiento de señales digitales
Integrado y preconfigurado

Gestión del audio

AXIS Audio Manager Edge
Integrado:
– Gestión de zonas que permite dividir hasta 200 altavoces en 20 zonas.
– Gestión de contenido de música y de anuncios en directo o pregrabados.
– Programación para decidir cuándo y dónde reproducir contenido.
– Priorización del contenido para garantizar que los mensajes urgentes interrumpan el contenido programado.
– Supervisión del estado que hace posible la detección remota de errores del sistema.
– Gestión de usuarios para controlar quién tiene acceso a funciones determinadas.
Para más detalles, consulte la hoja de datos de *axis.com/products/axis-audio-manager-edge/support*

AXIS Audio Manager Pro
Para sistemas grandes y avanzados. Se vende por separado.
Para especificaciones, consulte la hoja de datos de *axis.com/products/axis-audio-manager-pro/support*

AXIS Audio Manager Center
AXIS Audio Manager Center es un servicio en la nube que ofrece acceso remoto y gestión de sistemas multisitio.
Para especificaciones, consulte la hoja de datos en *axis.com/products/axis-audio-manager-center/support*

Software de audio

Transmisión de audio
Unidireccional/bidireccional con cancelación de eco semidúplex opcional. Mono.

Codificación de audio
AAC LC 8/16/32/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Axis µ-law 16 kHz, WAV,
MP3 en mono/estéreo de 64 kbps a 320 kbps.
Velocidad de bits variable y constante.
Frecuencia de muestreo de 8 kHz a 48 kHz.

Integración del sistema

Interfaz de programación de aplicaciones
API abierta para la integración de software, incluidos VAPIX®, conexión a la nube con un solo clic,
AXIS Camera Application Platform (ACAP).

Sistemas de gestión de vídeo
Compatible con AXIS Camera Station Edge,
AXIS Camera Station Pro, AXIS Camera Station 5 y software de gestión de vídeo de socios de Axis disponible en *axis.com/vms*.

Comunicación general
Singlewire InformaCast®, Intrado Revolution, Lynx, Alertus

Comunicaciones unificadas
Compatibilidad verificada:
Clientes SIP: 2N, Yealink, Cisco, Linphone, Grandstream
Servidores PBX/SIP: Cisco Call Manager, Cisco BroadWorks, Avaya, Asterix, Grandstream
Proveedores de servicios en la nube: Webex, Zoom

SIP
Funciones de SIP admitidas: Servidor SIP secundario, IPv6, SRTP, SIPS, SIP TLS, DTMF (RFC2976 y RFC2833), NAT (ICE, STUN, TURN)
RFC 3261: INVITE, CANCEL, BYE, REGISTER, OPTIONS, INFO
DTMF (RFC 4733/RFC 2833)

Condiciones de evento
Audio: reproducción de clip de audio, resultado de la prueba del altavoz
Llamada: estado, cambio de estado
Estado del dispositivo: dirección IP bloqueada/eliminada, secuencia en directo activa, pérdida de red, nueva dirección IP, sistema preparado
Almacenamiento local: grabación en curso, alteración del almacenamiento, problemas de estado de almacenamiento detectados
E/S: entrada digital, disparador manual, entrada virtual
MQTT: suscripción
Programados y recurrentes: programador

Acciones de eventos
Audio: ejecutar comprobación automática del altavoz
Clips de audio: reproducir, detener
E/S: alternar E/S
Luz y sirena: iniciar, detener
MQTT: publicar
Notificación: HTTP, HTTPS, TCP y correo electrónico
Grabaciones: grabar audio
Mensajes de trampa SNMP: envío de mensaje
LED de estado: parpadeo

Ayudas de instalación integradas
Verificación e identificación del tono de prueba

Supervisión funcional
Auto Speaker Test (verificación a través del micrófono incorporado)

Homologaciones

Marcas de productos
CSA, UL/cUL, UKCA, CE, KC, EAC, VCCI, RCM, BSMI

Cadena de suministro
Cumple los requisitos de TAA

EMC
EN 55035, EN 55032 Clase B, EN 50121-4, EN 61000-6-1, EN 61000-6-2
Australia/Nueva Zelanda: RCM AS/NZS CISPR 32 Clase B
Canadá: ICES-3(B)/NMB-3(B)
Japón: VCCI Clase B
Corea: KS C 9835, KS C 9832 Clase B
EE. UU.: FCC Parte 15 Subparte B Clase B
Ferrocarril: IEC 62236-4

Seguridad
CAN/CSA C22.2 N.º 62368-1 ed. 3, IEC/EN/UL 62368-1 ed. 3

Entorno
IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66, NEMA 250 Tipo 4X, MIL-STD-810G 509.5, MIL-STD-810H 509.7

Ciberseguridad
ETSI EN 303 645, etiqueta de seguridad informática BSI, FIPS-140

Red

Protocolos de red
IPv4/v6[1], HTTP, HTTPS[2], SSL/TLS[2], QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, PTP, RTSP, RTP, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP, SIP

Ciberseguridad

Seguridad perimetral
Software: Sistema operativo firmado, protección contra retrasos de fuerza bruta, autenticación Digest, protección por contraseña, módulo criptográfico Axis (FIPS 140-2 nivel 1)
Hardware: Plataforma de ciberseguridad Axis Edge Vault
Elemento seguro (CC EAL 6+), ID de dispositivo Axis, almacén de claves seguro, arranque seguro

Seguridad de red
IEEE 802.1X (EAP-TLS)[2], IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS[2], TLS v1.2/v1.3[2], Network Time Security (NTS), certificado PKI x.509, firewall basado en host

1. *Sincronización de audio solo con IPv4.*
2. *Este producto incluye software desarrollado por OpenSSL Project para su uso en el kit de herramientas OpenSSL (openssl.org) y software criptográfico escrito por Eric Young (eay@cryptsoft.com).*

Documentación
Guía de seguridad de sistemas de AXIS OS
Política de gestión de vulnerabilidades de Axis
Axis Security Development Model
Lista de materiales del software AXIS OS (SBOM)
Para descargar documentos, vaya a *axis.com/support/cybersecurity/resources*
Para obtener más información sobre el servicio de asistencia para ciberseguridad de Axis, vaya a *axis.com/cybersecurity*.

Sistema en chip (SoC)

Modelo
NXP i.MX 8M Nano

Flash
1024 MB de RAM, 1024 MB de memoria flash

General

Carcasa
Clasificación IP66 y NEMA 4X
Lata trasera de aluminio y soporte de acero inoxidable.
Color: blanco RAL 9010

Alimentación
Alimentación a través de Ethernet (PoE)
IEEE 802.3af/802.3at Tipo 1 Clase 3
2 W típicos, 12,95 W máx.

Conectores
Red: RJ45 10BASE-T/100BASE-TX PoE
E/S: Bloque de terminales de 4 pines de 2,5 mm para 2 E/S configurables supervisadas

Indicadores LED
LED de estado, LED delantero

Fiabilidad
Diseñado para un funcionamiento ininterrumpido.

Condiciones de funcionamiento
Temperatura: De -40 °C a 60 °C (de -40 °F a 140 °F)
Humedad relativa: Humedad relativa del 10 al 100 % (con condensación)

Condiciones de almacenamiento
Temperatura: De -40 °C a 65 °C (de -40 °F a 149 °F)
Humedad relativa: Humedad relativa del 5 al 95 % (sin condensación)

Dimensiones
Para conocer las dimensiones totales del producto, consulte el plano de dimensiones de esta ficha técnica.

Peso
1,3 kg (2,9 lib)

Contenido de la caja
Altavoz exponencial, guía de instalación, conector de bloque de terminales, protector del conector, junta de cable, terminal de anillo, clave de autenticación del propietario

Accesorios opcionales
AXIS T91B47 Pole Mount, AXIS T91F67 Pole Mount, Cable Gland M20x1.5, RJ45, Cable Gland A M20, AXIS Power a través de Ethernet Midspans, T94R01B Corner Bracket, T94P01B Corner Bracket, T94S01P Conduit Back Box
Para obtener más información sobre accesorios, vaya a *axis.com/products/axis-c1310-e-mk-ii#accessories*

Idiomas
Alemán, chino (simplificado), chino (tradicional), coreano, español, finés, francés, holandés, inglés, italiano, japonés, polaco, portugués, ruso, sueco, tailandés, turco, vietnamita

garantia
Garantía de 5 años; consulte *axis.com/warranty*

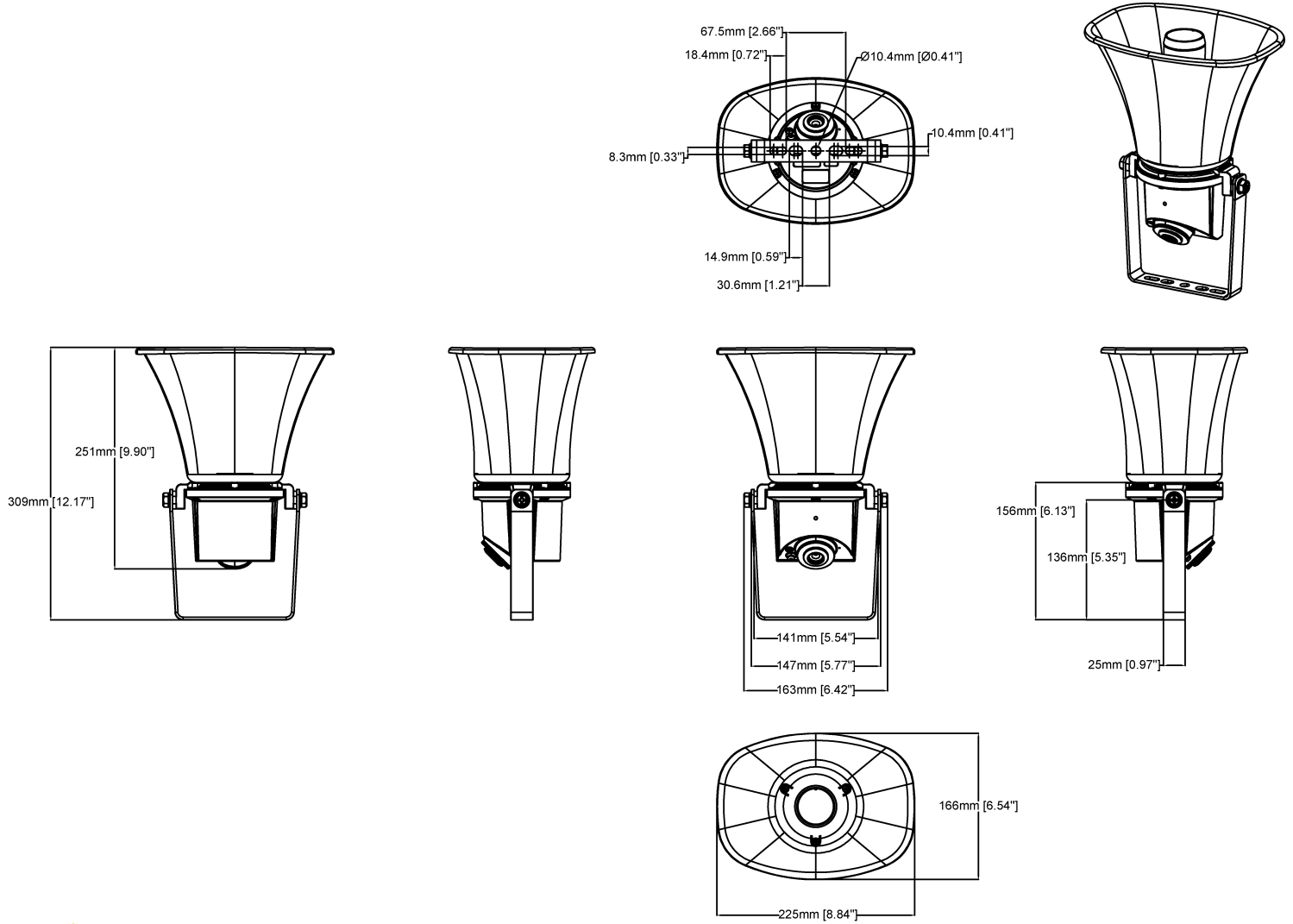
Números de pieza
Disponible en *axis.com/products/axis-c1310-e-mk-ii#part-numbers*

Sostenibilidad

Control de sustancias
Sin PVC de conformidad con la norma JEDEC/ECA, JS709
RoHS de conformidad con la directiva europea RoHS 2011/65/UE/ y EN 63000:2018
REACH de conformidad con (CE) no 1907/2006. Para SCIP UUID, consulte *echa.europa.eu*

Materiales
Análisis de minerales conflictivos conforme a las directrices de la OCDE
Para obtener más información sobre la sostenibilidad en Axis, vaya a *axis.com/about-axis/sustainability*

Responsabilidad medioambiental
axis.com/environmental-responsibility
Axis Communications es firmante del Acuerdo Mundial de las Naciones Unidas, obtenga más información en *unglobalcompact.org*



AXIS C1310-E Mk II Network Horn Speaker

Revision	v.01	Revision date	2023-10-26
Paper size	A4	Release date	2023-10-26
Created by	MS	Scale	1:6

© 2023 Axis Communications

Funciones destacadas

Axis Edge Vault

Axis Edge Vault es la plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Constituye la base de la que dependen todas las operaciones seguras y ofrece características para proteger la identidad del dispositivo, proteger su y proteger la información confidencial frente a accesos no autorizados. Por ejemplo, el **arranque seguro** garantiza que un dispositivo solo puede arrancar con el **sistema operativo firmado**. De esta forma, se evita la manipulación de la cadena de suministro física. Con el SO firmado, el dispositivo puede validar también el nuevo software antes de aceptar instalarlo. El **almacén de claves seguro** es la pieza clave para proteger la información criptográfica que se utiliza para una comunicación segura (IEEE 802.1X, HTTPS, ID de dispositivo Axis, claves de control de acceso, etc.) contra la extracción maliciosa en caso de una infracción de la seguridad. El almacén de claves seguro y las conexiones seguras se proporcionan a través de un módulo de cálculo criptográfico basado en hardware certificado por FIPS 140 o criterios comunes.

Para obtener más información sobre Axis Edge Vault, vaya a *axis.com/solutions/edge-vault*.

Para obtener más información, consulte *axis. com/ glossary*

© 2023 – 2025 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC y VAPIX son marcas comerciales registradas de Axis AB en diferentes jurisdicciones. Todas las demás marcas comerciales son propiedad de sus respectivos titulares.Nos reservamos el derecho de introducir modificaciones sin previo aviso.