AXIS C1310-E Mk II Network Horn Speaker

Altavoz exterior para una voz sin límites

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
- > Se conecta 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

Sistema en chip (SoC)

Modelo	i.MX 8M Nano
Memoria	1024 MB de RAM, 1024 MB de memoria flash

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 integrado (puede ser desactivarse mecánicamente) Altavoz integrado
Especificación del micrófono integrado	50 Hz - 12 kHz
Procesamiento de señales digitales	Integrado y preconfigurado
Descripción del amplificador	Amplificador 7 W Clase D integrado

Gestión de audio

AXIS Audio Manager Edge	Integrado: – Gestión de contenido de música y de anuncios en directo o pregrabados. – Funciones de programación que permiten determinar el momento y el lugar en el que se reproducirá un contenido concreto. – Priorización del contenido para garantizar que los mensajes urgentes interrumpan el contenido programado. – Gestión de zonas que permite dividir hasta 200 altavoces en 20 zonas. – Supervisión del estado que hace posible la detección remota de errores del sistema. – Gestión de usuarios para controlar quién tiene acceso a funciones determinadas. Consulte la hoja de datos aparte para obtener más información.
AXIS Audio Manager Pro	Para sistemas grandes y avanzados. Se vende por separado. Consulte las especificaciones en la hoja de datos aparte.

Software de audio

Transmisión de audio	Unidireccional/bidireccional con cancelación de eco half-duplex 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.

Red

Protocolos de red	IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS[a] HTTP/2, TLS[a], QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SSH, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), dirección de enlace local (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Integración del sistema

Interfaz de programación de aplicaciones	API abierta para la integración de software, incluidos VAPIX®, metadatos y AXIS Camera Application Platform (ACAP); las especificaciones están disponibles en *axis.com/developer-community*. La ACAP incluye Native SDK. Conexión a la nube con un solo clic Compatibilidad con el protocolo de inicio de sesión (SIP) para la integración con sistemas de voz por IP (VoIP), de punto a punto o integrados con SIP/PBX.
Sistemas de gestión de vídeo	Compatible con AXIS Companion, AXIS Camera Station y el software de gestión de vídeo de socios desarrolladores de aplicaciones de Axis disponible en *axis.com/vms*
Audio inteligente	Auto Speaker Test
Condiciones de evento	Audio: reproducción de clip de audio, resultado de la prueba del altavoz Estado del dispositivo: dirección IP bloqueada/eliminada, secuencia en directo activa, pérdida de red, nueva dirección IP, sistema preparado Almacenamiento en el extremo: grabación en curso, alteración del almacenamiento, problemas de estado de almacenamiento detectados E/S: entrada digital, activación manual, entrada virtual MQTT: suscribirse Programado y recurrente: programador
Acciones de eventos	Audio: ejecutar comprobación automática del altavoz Clips de audio: reproducir, detener E/S: activar E/S Luz y sirena: ejecutar, detener MQTT: publicar Notificación: HTTP, HTTPS, TCP y correo electrónico Grabaciones: grabar audio Mensajes SNMP trap: enviar mensaje LED de estado: flash
Ayudas de instalación integradas	Verificación e identificación del tono de prueba
Supervisión funcional	Auto Speaker Test, verificación de conexión, registro de sistema integrado

Homologaciones

Marcas de productos	CSA, UL/cUL, UKCA, CE, KC, EAC, VCCI, RCM
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
Ambiental	IEC 60068-2-1, IEC 60068-2-2, 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

Ciberseguridad

Seguridad perimetral	**Software:** Firmware firmado, protección contra retrasos de fuerza bruta, autenticación Digest, protección con contraseña **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)[a], IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], Network Time Security (NTS), X.509 Certificado PKI, firewall basado en host
Documentación	*Guía de seguridad de sistemas de AXIS OS* *Política de gestión de vulnerabilidades de Axis* *Modelo de desarrollo de la seguridad de Axis* 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, ir a *axis.com/cybersecurity*.

General

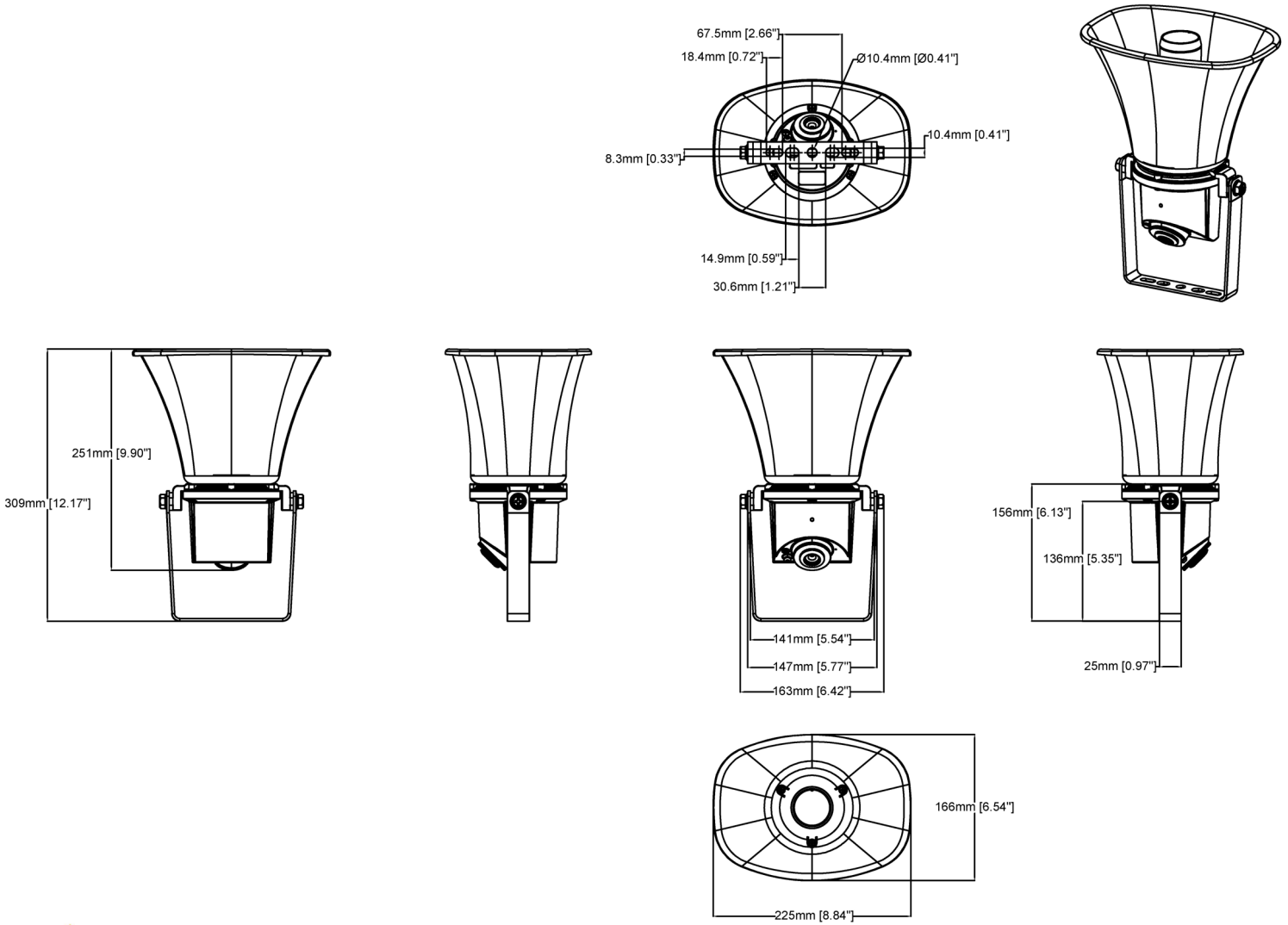
Carcasa	Clasificación IP66 y NEMA 4X Lata trasera de aluminio y soporte de acero inoxidable. color: blanco RAL 9010
Alimentación	Alimentación a través de Ethernet (PoE) IEEE 802.3af/802.3at Tipo 1 Clase 3 2 W típicos, 12,95 W máx.

Conectores	Red: RJ45 10BASE-T/100BASE-TX PoE. I/O: Bloque de terminales de 4 pines de 2,5 mm para 2 E/S configurables supervisadas
Fiabilidad	Diseñado para un funcionamiento ininterrumpido.
Condiciones de funcionamiento	Temperatura: De -40 °C a 60 °C Humedad relativa del 10 al 100 % (con condensación)
Condiciones de almacenamiento	Temperatura: de -40 °C a 65 °C Humedad relativa del 5 al 95 % (sin condensación)
Dimensiones	Para obtener información sobre las dimensiones generales del producto, consulte el dibujo de dimensiones de la hoja de datos.
Peso	1,3 kg
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, alimentación AXIS 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
Garantía	Garantía de 5 años; consulte *axis.com/warranty*
Referencias	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	Se ha evaluado para encontrar minerales en conflicto de acuerdo con las guías 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, lea más en *unglobalcompact.org*

a. *Este producto incluye software desarrollado por OpenSSL Project para su uso en el kit de herramientas OpenSSL. (openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).*



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

Características y tecnologías clave

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 integridad de fábrica y proteger la información confidencial frente a accesos no autorizados.

La base de la confianza comienza en el proceso de arranque del dispositivo. En los dispositivos Axis, el mecanismo de **arranque seguro** basado en hardware verifica el sistema operativo (AXIS OS) desde el que se está iniciando el dispositivo. El SO de AXIS, a su vez, tiene firma criptográfica (**firmware firmado**) durante el proceso de compilación. El arranque seguro y el firmware firmado están vinculados entre sí; se aseguran de que no se haya manipulado el firmware durante el ciclo de vida del dispositivo y que el dispositivo solo arranque con firmware autorizado. De este modo se crea una cadena de software validado criptográficamente para la cadena de confianza de la que dependen todas las operaciones seguras.

Desde un aspecto de seguridad, la **pulsación de tecla segura** 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. La pulsación de tecla segura se proporciona a través de un módulo de cálculo criptográfico basado en hardware certificado por FIPS 140 o criterios comunes. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios de estos módulos, como un TPM 2.0 (Módulo de plataforma de confianza) o un elemento seguro, o un entorno de ejecución de confianza (TEE) integrado en el sistema en un chip (SoC).

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

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