

AXIS C1310-E Mk II Network Horn Speaker

Außenlautsprecher für klare Ansagen mit großer Reichweite

Der AXIS C1310-E Mk II Network Horn Speaker ist unter den meisten klimatischen Bedingungen ideal für den Einsatz im Außenbereich geeignet. Er ermöglicht Benutzern, unerwünschte Aktivitäten aus der Ferne zu verhindern, im Notfall Anweisungen zu erteilen oder allgemeine Sprachnachrichten zu senden. Der integrierte Speicher unterstützt bereits aufgezeichnete Nachrichten oder Sicherheitspersonal kann direkt auf Benachrichtigungen antworten. Offene Standards unterstützen die einfache Integration in Netzwerk-Video, Zutrittskontrolle, Analysen und VoIP (Unterstützung von SIP). Die digitale Signalverarbeitung (DSP) gewährleistet einen klaren Klang. Über das integrierte Mikrofon lassen sich per Fernzugriff Integritätstests durchführen, und es ist eine Zwei-Wege-Kommunikation möglich. Darüber hinaus unterstützt die integrierte Audio Management Software die Verwaltung von Benutzern, Inhalten, Zonen und Zeitplänen.

- > **Umfassendes Lautsprechersystem**
- > **Lässt sich mit dem Standardnetzwerk verbinden**
- > **Einfache Installation dank PoE**
- > **Fernüberwachung des Systemzustands**
- > **Skalierbar und leicht zu integrieren**



IT-Sicherheitskennzeichen

Bundesamt für Sicherheit in der Informationstechnik

Der Hersteller versichert:
Das Produkt entspricht den
Anforderungen des BSI.

Das BSI informiert:
Aktuelles zum Produkt
bsi.bund.de/it-sik/03141



AXIS C1310-E Mk II Network Horn Speaker

Audio-Hardware

Gehäuse

Gefalteter Hornlautsprecher mit Kompressionstreiber

Max. Schalldruckpegel

>121 dB

Frequenzgang

280 Hz bis 12,5 kHz

Erfassungsbereich

70° horizontal um 100° vertikal (bei 2 kHz)

Audio-Eingang/-Ausgang

Integriertes Mikrofon (kann mechanisch deaktiviert werden)

Integrierter Lautsprecher

Technische Daten des integrierten Mikrofons

50 Hz bis 12 kHz

Beschreibung des Verstärkers

Integrierter Verstärker (7 W, Klasse D)

Digital Signal Processing

Integriert und vorkonfiguriert

Audio-Management

AXIS Audio Manager Edge

Integriert:

- Zonenverwaltung zum Aufteilen von bis zu 200 Lautsprechern in 20 Zonen
- Content Management für Musik und Live- sowie aufgezeichnete Durchsagen.
- Planungsmöglichkeit für Zeit und Ort der Wiedergabe von Inhalten.
- Priorisierung dringender Inhalte
- Statusüberwachung zur Erkennung von Systemfehlern aus der Ferne
- Benutzerverwaltung zur Steuerung des Zugriffs auf Funktionen.

Weitere Einzelheiten finden Sie im Datenblatt unter axis.com/products/axis-audio-manager-edge/support

AXIS Audio Manager Pro

Für größere und komplexere Systeme. Separat erhältlich.

Technische Daten finden Sie im Datenblatt unter axis.com/products/axis-audio-manager-pro/support

AXIS Audio Manager Center

AXIS Audio Manager Center ist ein Cloud-Dienst, über den sich Systeme mit mehreren Standorten per Fernzugriff verwalten lassen.

Technische Daten finden Sie im Datenblatt unter axis.com/products/axis-audio-manager-center/support

Audiosoftware

Audio-Streaming

Uni-/bidirektionale Audioübertragung mit optionaler Halbduplex-Echounterdrückung. Mono.

Audiocodierung

AAC LC 8/16/32/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Axis μ -law 16 kHz, WAV, MP3 in Mono/Stereo von 64 kBit/s bis 320 kBit/s. Konstante und variable Bitrate. Abtastrate von 8 kHz bis zu 48 kHz.

Systemintegration

Anwendungsprogrammierschnittstelle (engl. Application Programming Interface)

Offene API für Softwareintegration, einschließlich VAPIX®, Cloud-Anbindung mit einem Mausklick und AXIS Camera Application Platform (ACAP).

Videoverwaltungssysteme

Kompatibel mit AXIS Camera Station Edge, AXIS Camera Station Pro, AXIS Camera Station 5 und Video Management Software von Axis Partnern, erhältlich unter axis.com/vms.

Massenbenachrichtigung

Singlewire InformaCast®, Intrado Revolution, Lynx, Alertus

Vereinheitliche Kommunikation

Geprüfte Kompatibilität:

SIP-Clients: 2N, Yealink, Cisco, Linphone, Grandstream
PBX/SIP-Server: Cisco Call Manager, Cisco BroadWorks, Avaya, Asterix, Grandstream
Cloud-Dienstanbieter: Webex, Zoom

SIP

Unterstützte SIP-Merkmale: Sekundärer SIP-Server, IPv6, SRTP, SIPS, SIP TLS, DTMF (RFC2976 und RFC2833), NAT (ICE, STUN, TURN)
RFC 3261: INVITE, CANCEL, BYE, REGISTER, OPTIONS, INFO
DTMF (RFC 4733/RFC 2833)

Ereignisbedingungen

Audio: Audio-Clips wiedergeben, Lautsprechertestergebnis
Anruf: Status, Statusänderung
Gerätestatus: IP-Adresse blockiert/entfernt, Livestream aktiv, Netzwerk-Verlust, neue IP-Adresse, Systembereitschaft
Edge Storage: laufende Aufzeichnung, Speicherunterbrechung, Speicherintegritätsprobleme erkannt
E/A: digitaler Eingang, manueller Auslöser, virtueller Eingang
MQTT: abonnieren
Geplant und wiederkehrend: Zeitplan

Ereignisaktionen

Audio: automatischen Lautsprechertest ausführen
Audioclips: abspielen, anhalten
E/A: E/A umschalten
Licht und Sirene: laufen, anhalten
MQTT: veröffentlichen
Benachrichtigung: HTTP, HTTPS, TCP und E-Mail
Aufzeichnungen: Audio aufnehmen
SNMP-Trap-Meldungen: Senden von Meldungen
Status-LED: Blinken

Eingebaute Installationshilfen

Überprüfen und Identifizieren per Testton

Funktionsüberwachung

Automatischer Lautsprechertest (Überprüfung durch integriertes Mikrofon)

Zulassungen

Produktkennzeichnungen

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

Lieferkette

Entspricht TAA

EMV

EN 55035, EN 55032 Klasse B, EN 50121-4, EN 61000-6-1, EN 61000-6-2
Australien/Neuseeland: RCM AS/NZS CISPR 32 Klasse B
Kanada: ICES-3(B)/NMB-3(B)
Japan: VCCI Klasse B
Korea: KS C 9835, KS C 9832 Klasse B
USA: FCC Abschnitt 15 Teil B Klasse B
Bahnanwendungen: IEC 62236-4

Sicherheit

CAN/CSA C22.2 Nr. 62368-1 Ausg. 3, IEC/EN/UL 62368-1 ed. 3

Umgebung

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 Typ 4X, MIL-STD-810G 509.5, MIL-STD-810H 509.7

Cybersicherheit

ETSI EN 303 645, BSI IT-Sicherheitskennzeichen, FIPS-140

Netzwerk

Netzwerkprotokolle

IPv4/v6¹, HTTP, HTTPS², SSL/TLS², QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP, SIP

Cybersicherheit

Edge-Sicherheit

Software: Signiertes Betriebssystem, Brute-Force-Verzögerungsschutz, Digest-Authentifizierung, Kennwortschutz, Axis Cryptographic Module (FIPS 140-2 Level 1)

Hardware: Axis Edge Vault Cybersicherheitsplattform Secure Element (CC EAL 6+), Axis Geräte-ID, sicherer Schlüsselspeicher, sicheres Hochfahren

Netzwerksicherheit

IEEE 802.1X (EAP-TLS)², IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS², TLS v1.2/v1.3², Network Time Security (NTS), X.509 Certificate PKI, hostbasierte Firewall

1. Audio-Synchronisierung nur mit IPv4.

2. Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit. (openssl.org) entwickelt wurde, sowie kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Dokumentation

AXIS OS Hardening Guide

Axis Vulnerability Management-Richtlinie

Axis Security Development Model

AXIS OS Software Bill of Material (SBOM)

Diese Dokumente stehen unter axis.com/support/cybersecurity/resources zum Download bereit.

Weitere Informationen zum Axis

Cybersicherheitssupport finden Sie auf axis.com/cybersecurity

System-on-Chip (SoC)

Modell

NXP i.MX 8M Nano

Speicher

1024 MB RAM, 1024 MB Flash

Allgemeines

Gehäuse

Zertifiziert nach IP66 und NEMA 4X

Backbox aus Aluminium und Halterung aus rostfreiem Stahl

Farbe: Weiß RAL 9010

Stromversorgung

Power over Ethernet (PoE) IEEE 802.3af/802.3at Typ 1 Klasse 3

Normal 2 W, max. 12,95 W

Anschlüsse

Netzwerk: RJ-45 für 10BASE-T/100BASE-TX, PoE

Eingänge/Ausgänge: 4-poliger Anschlussblock (2,5 mm) für 2x überwachte, konfigurierbare I/Os

LED-Anzeigen

Status-LED, frontseitige LED

Zuverlässigkeit

Zuverlässiger Betrieb rund um die Uhr.

Betriebsbedingungen

Temperatur: -40 °C bis +60 °C (-40 °F bis +140 °F)

Luftfeuchtigkeit: 10 bis 100 % rF (kondensierend)

Lagerbedingungen

Temperatur: -40 °C bis +65 °C (-40 °F bis +149 °F)

Luftfeuchtigkeit: 5 bis 95 % (nicht kondensierend)

Abmessungen

Die Gesamtabmessungen des Produkts sind dem Maßbild in diesem Datenblatt zu entnehmen.

Gewicht

1,3 kg

Inhalt des Kartons

Hornlautsprecher, Installationsanleitung,

Anschlussblock, Anschlusschutz, Kabeldichtung,

Ringanschluss, Eigentümer-Authentifizierungsschlüssel

Optionales Zubehör

AXIS T91B47 Pole Mount, AXIS T91F67 Pole Mount,

Cable Gland M20 x 1,5, RJ45, Cable Gland A M20,

Midspans für AXIS Power over Ethernet, T94R01B

Corner Bracket, T94P01B Corner Bracket, T94S01P

Conduit Back Box

Weiteres Zubehör finden Sie auf axis.com/products/axis-c1310-e-mk-ii#accessories

Sprachen

Englisch, Deutsch, Französisch, Spanisch, Italienisch,

Russisch, Chinesisch (vereinfacht), Japanisch,

Koreanisch, Portugiesisch, Polnisch, Chinesisch

(traditionell), Niederländisch, Tschechisch, Schwedisch,

Finnisch, Türkisch, Thailändisch, Vietnamesisch

Gewährleistung

Informationen zur 5-jährigen Gewährleistung finden Sie auf axis.com/warranty

Artikelnummern

Abrufbar unter axis.com/products/axis-c1310-e-mk-ii#part-numbers

Nachhaltigkeit

Substanzkontrolle

PVC-frei gemäß JEDEC/ECA JS709

RoHS gemäß RoHS-Richtlinie 2011/65/EU und EN

63000:2018

REACH gemäß Verordnung (EG) Nr. 1907/2006.

Informationen zu SCIP UUID finden Sie auf echa.europa.eu

Material

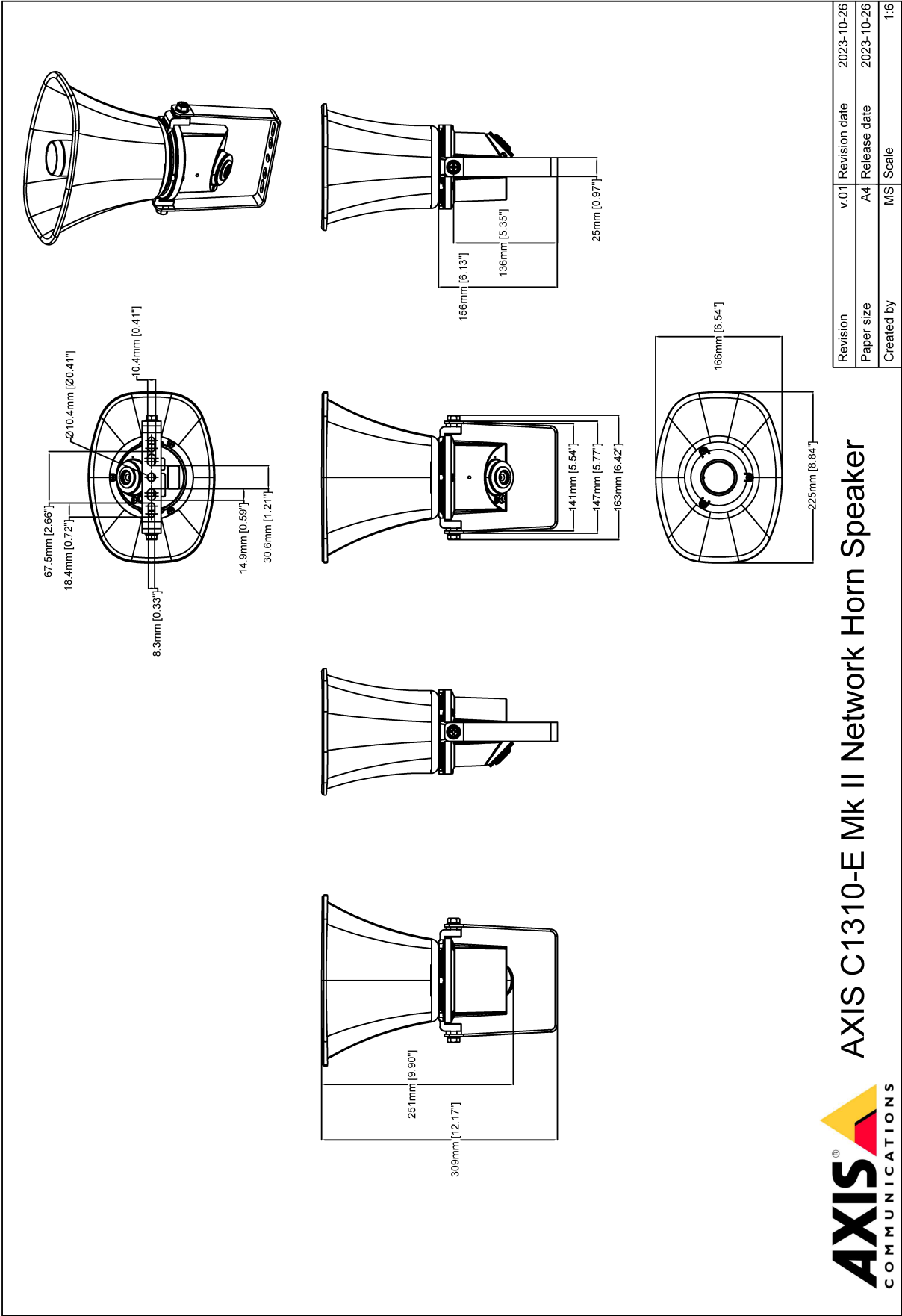
Auf Konfliktmineralien gemäß OECD-Leitfaden überprüft

Weitere Informationen zum Thema Nachhaltigkeit bei Axis finden Sie auf axis.com/about-axis/sustainability

Verantwortung für die Umwelt

axis.com/environmental-responsibility

Axis Communications nimmt am UN Global Compact teil. Weitere Informationen hierzu finden Sie auf *unglobalcompact.org*



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

Hervorgehobene Funktionen

Axis Edge Vault

Axis Edge Vault ist die hardwarebasierte Cybersicherheitsplattform zum Schutz des Axis Geräts. Sie bildet die Grundlage für jedweden sicheren Betrieb und bietet Funktionen zum Schutz der Identität des Geräts, zur Sicherung seiner Integrität und zum Schutz vertraulicher Daten vor unbefugtem Zugriff. Beispielsweise sorgt der sichere Systemstart dafür, dass ein Gerät nur mit signiertem Betriebssystem gestartet werden kann. Dies verhindert konkrete Manipulationen der Bereitstellungskette. Ein Gerät mit signiertem Betriebssystem kann außerdem neue Geräte-Software validieren, bevor es zulässt, dass sie installiert wird. Und hinsichtlich der Sicherheit ist der sichere Schlüsselspeicher der entscheidende Faktor für den Schutz kryptografischer Daten, die für die sichere Kommunikation (IEEE 802.1X, HTTPS, Axis Geräte-ID, Schlüssel für die Zutrittskontrolle usw.) verwendet werden, vor einem Missbrauch bei Sicherheitsverletzungen. Der sichere Schlüsselspeicher wird über ein gemäß dem Common Criteria oder FIPS 140 zertifiziertes, hardwarebasiertes, kryptografisches Rechenmodul bereitgestellt.

Weitere Informationen zu Axis Edge Vault finden Sie unter axis.com/solutions/edge-vault.

Weitere Informationen finden Sie auf axis.com/glossary