

AXIS C1310-E Mk II Network Horn Speaker

Altoparlante a lungo raggio per esterni

AXIS C1310-E Mk II Network Horn Speaker è perfetto per ambienti esterni nella maggior parte dei climi. Consente agli utenti di prevenire da remoto attività indesiderate, fornire istruzioni durante un'emergenza o inviare messaggi vocali generali. La memoria integrata supporta i messaggi preregistrati. In alternativa, il personale di sicurezza può rispondere alle notifiche con messaggi vocali dal vivo. Gli standard aperti supportano facilità di integrazione con video di rete, controllo degli accessi, analisi e VoIP (supporto del protocollo SIP). L'elaborazione digitale del segnale (DSP) garantisce un suono nitido. Il microfono incorporato consente test sull'integrità da remoto e comunicazione bidirezionale. Per di più, il software per la gestione audio integrato supporta la gestione degli utenti, dei contenuti, delle aree e della pianificazione.

- > **Sistema di altoparlanti All-in-One**
- > **Connessione alla rete standard**
- > **Installazione semplice grazie all'alimentazione PoE**
- > **Diagnosi remota**
- > **Scalabile e facile da integrare**



AXIS C1310-E Mk II Network Horn Speaker

Hardware audio

Custodia	Altoparlante a tromba rientrante con driver a compressione
Livello di pressione sonora massimo	>121 dB
Risposta di frequenza	280 Hz - 12,5 kHz
Modello di copertura	70° orizzontale per 100° verticale (a 2 kHz)
Input/output audio	Microfono integrato (può essere disabilitato meccanicamente) Altoparlante integrato
Specifica microfono incorporato	50 Hz - 12 kHz
Descrizione dell'amplificatore	Amplificatore integrato 7 W Classe D
Elaborazione segnale digitale	Incorporato e preconfigurato

Gestione audio

AXIS Audio Manager Edge	Incorporato: - Gestione delle zone permette di suddividere fino a 200 altoparlanti in 20 zone. - Gestione dei contenuti per la musica e gli annunci in diretta/preregistrati. - Pianificazione per determinare gli orari e le zone in cui riprodurre contenuti. - Assegnazione di priorità ai contenuti, facendo in modo che i messaggi urgenti interrompano la pianificazione. - Monitoraggio dell'integrità per il rilevamento da remoto di errori di sistema. - Gestione degli utenti per controllare chi ha accesso a quali funzionalità. Per ulteriori dettagli, consultare la scheda tecnica in axis.com/products/axis-audio-manager-edge/support
AXIS Audio Manager Pro	Per sistemi più grandi e avanzati. Venduto separatamente. Per specifiche, consultare la scheda tecnica in axis.com/products/axis-audio-manager-pro/support
AXIS Audio Manager Center	AXIS Audio Manager Center è un servizio cloud per l'accesso e la gestione remota di sistemi multisito. Per specifiche, consultare la scheda tecnica in axis.com/products/axis-audio-manager-center/support

Software audio

Flussi audio	Unidirezionale/bidirezionale con cancellazione dell'eco half-duplex opzionale. Mono.
Codifica 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 in mono/stereo da 64 kbps a 320 kbps. Velocità di trasmissione in bit fissa e variabile. Velocità di campionamento da 8 kHz fino a 48 kHz.

Integrazione di sistemi

Application Programming Interface	API aperte per l'integrazione di software, tra cui VAPIX®, One-click cloud connection, AXIS Camera Application Platform (ACAP).
Sistemi di gestione video	Compatibile con AXIS Camera Station Edge, AXIS Camera Station Pro, AXIS Camera Station 5 e con il software per la gestione video di partner di AXIS, disponibile all'indirizzo axis.com/vms .
Avvisi di massa	Singlewire InformaCast®, Intrado Revolution, Lynx, Alertus
Comunicazioni unificate	Compatibilità verificata: Client SIP: 2N, Guaina, Cisco, Linphone, Grandstream Server PBX/SIP: Cisco Call Manager, Cisco BroadWorks, Avaya, Asterix, Grandstream Provider di servizi cloud: Webex, Zoom
SIP	Funzionalità SIP supportate: Server SIP secondario, IPv6, SRTP, SIPs, SIP TLS, DTMF (RFC2976 e RFC2833), NAT (ICE, STUN, TURN) RFC 3261: INVITE, CANCEL, BYE, REGISTER, OPTIONS, INFO DTMF (RFC 4733/RFC 2833)

Condizioni degli eventi	Audio: riproduzione di clip audio, risultato verifica altoparlante Chiamata: stato, cambiamento dello stato Stato dispositivo: indirizzo IP bloccato/rimosso, flusso dal vivo attivo, perdita di rete, nuovo indirizzo IP, pronto all'uso Archiviazione su dispositivi edge: registrazione in corso, interruzione dell'archiviazione, problemi di integrità dell'archiviazione rilevati I/O: input digitale, attivazione manuale, input virtuale MQTT: sottoscrizione Pianificato e ricorrente: pianificazione
--------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Azioni eventi	Audio: esegui test automatico dell'altoparlante Clip audio: riproduzione, arresto I/O: attiva/disattiva I/O Luce e sirena: esegui, arresta MQTT: pubblicazione Notifica: HTTP, HTTPS, TCP ed e-mail Registrazioni: registra audio Messaggi trap SNMP: invio messaggio LED di stato: lampeggiante
----------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Supporti di installazione incorporati	Verifica e identificazione test del tono
----------------------------------------------	------------------------------------------

Monitoraggio funzionale	Verifica automatica dell'altoparlante (verifica con microfono integrato)
--------------------------------	--------------------------------------------------------------------------

Approvazioni

Marche del prodotto	CSA, UL/cUL, UKCA, CE, KC, EAC, VCCI, RCM, BSMI
Catena di fornitura	Conformità a TAA
EMC	EN 55035, EN 55032 Classe B, EN 50121-4, EN 61000-6-1, EN 61000-6-2 Australia/Nuova Zelanda: RCM AS/NZS CISPR 32 Classe B Canada: ICES-3(B)/NMB-3(B) Giappone: VCCI Classe B Corea: KS C 9835, KS C 9832 Classe B Stati Uniti: FCC Parte 15 Sottosezione B Classe B Ferroviana: IEC 62236-4

Protezione	CAN/CSA C22.2 No. 62368-1 ed. 3, IEC/EN/UL 62368-1 ed. 3
-------------------	----------------------------------------------------------

Ambiente	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
-----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Cybersecurity	ETSI EN 303 645
----------------------	-----------------

Rete

Protocolli di rete	IPv4/v6 ^a , HTTP, HTTPS, SSL/TLS, 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
---------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Cybersecurity

Sicurezza edge	Software: SO firmato, protezione ritardo forza bruta, autenticazione digest, protezione mediante password Hardware: Piattaforma di cybersecurity Axis Edge Vault Secure element (CC EAL 6+), ID dispositivo Axis, archivio chiavi sicuro, avvio sicuro
Protezione della rete	IEEE 802.1X (EAP-TLS), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), X.509 PKI certificato, firewall basato su host

Documentazione	<i>AXIS OS Hardening Guide</i> <i>Axis Security Development Model</i> Distinta base del software AXIS OS (SBOM) Per il download dei documenti, vai a axis.com/support/cybersecurity/resources Per maggiori informazioni relativamente al supporto per la sicurezza informatica Axis, visitare axis.com/cybersecurity
-----------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

System-on-chip (SoC)

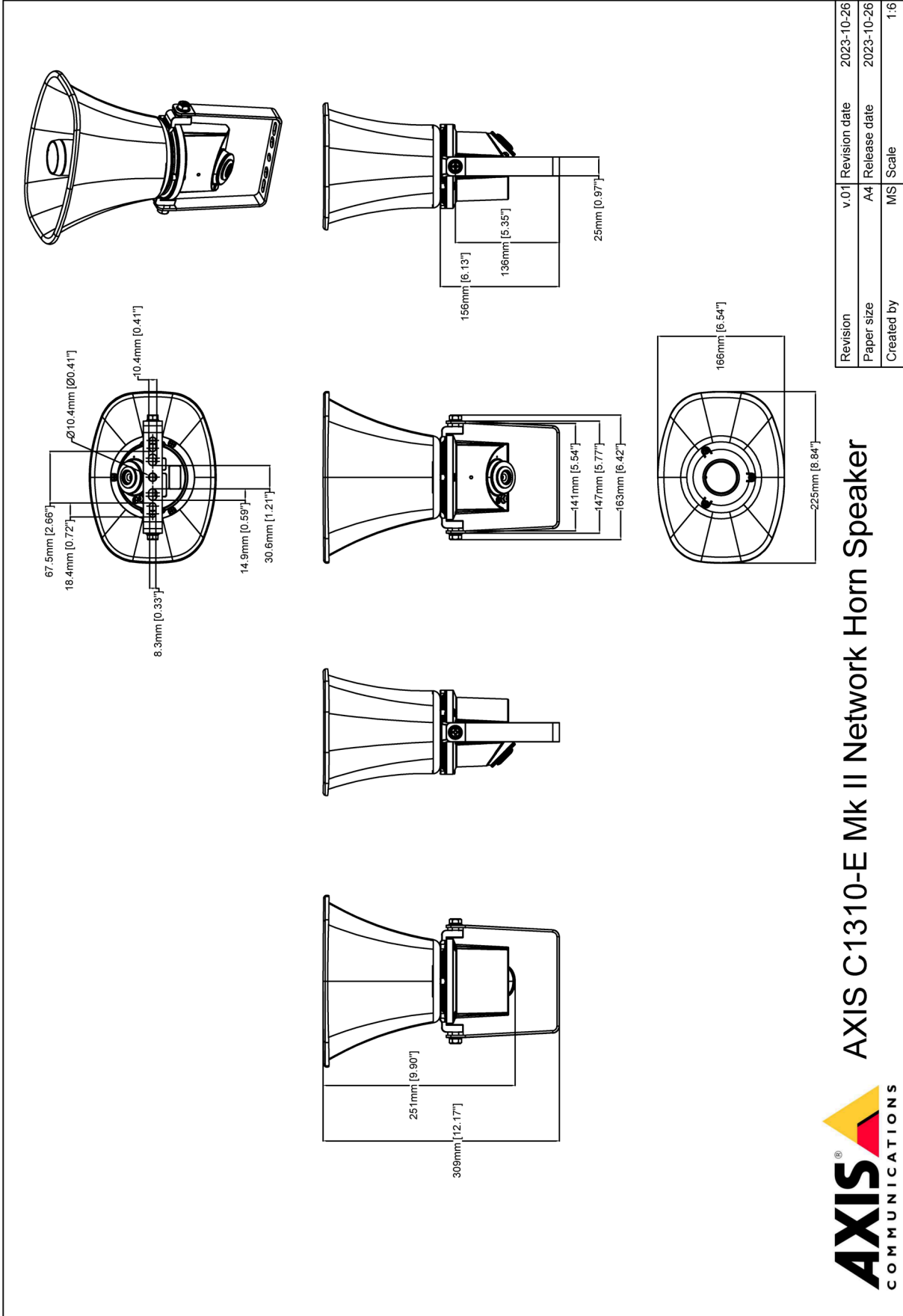
Modello	NXP i.MX 8M Nano
Memoria	RAM da 1024 MB, Flash da 1024 MB

Generale	
Alloggiamento	Classe IP66 e NEMA 4X Contenitore posteriore in alluminio e staffa in acciaio inossidabile Colore: bianco RAL 9010
Alimentazione	Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 1 Classe 3 Tipico 2 W, max 12,95 W
Connettori	Rete: RJ45 10BASE-T/100BASE-TX PoE I/O: Morsettiera a 4 pin da 2,5 mm per 2 I/O configurabili supervisionati
Indicatori LED	LED di stato, LED frontale
Affidabilità	Progettata per un funzionamento continuo.
Condizioni d'esercizio	Temperatura: Da -40 °C a 60 °C Umidità: relativa 10 - 100% (con condensa)
Condizioni di immagazzinaggio	Temperatura: Da -40 °C a 65 °C Umidità: Umidità relativa 5-95% (senza condensa)
Dimensioni	Per le dimensioni complessive del prodotto, vedere il disegno quotato in questa scheda tecnica.
Peso	1,3 kg (2.9 lb.)
Contenuto della scatola	Altoparlante a tromba, guida all'installazione, connettore morsettiera, protezione del connettore, guarnizione del cavo, terminale ad anello, chiave di autenticazione proprietario
Accessori opzionali	AXIS T91B47 Pole Mount, AXIS T91F67 Pole Mount, Cable Gland M20 x 1,5, RJ45, Cable Gland A M20, midspan AXIS Power over Ethernet Midspans, Corner Bracket T94P01B, Conduit Back Box T94S01P Per ulteriori accessori, vai a axis.com/products/axis-c1310-e-mk-ii#accessories

Lingue	Inglese, tedesco, francese, spagnolo, italiano, russo, cinese semplificato, giapponese, coreano, portoghese, polacco, cinese tradizionale, olandese, ceco, svedese, finlandese, turco, thailandese, vietnamita
Garanzia	Garanzia di 5 anni, visitare axis.com/warranty
Codici prodotto	Disponibile presso axis.com/products/axis-c1310-e-mk-ii#part-numbers
Sostenibilità	
Controllo sostanza	Senza PVC conformemente a JEDEC/ECA Standard JS709 RoHS conformemente alla direttiva UE RoHS 2011/65/UE/ e EN 63000:2018 REACH conformemente a (EC) N. 1907/2006. For SCIP UUID, consultare echa.europa.eu
Materiali	Sottoposto a controlli conformemente alle linee guida OCSE nell'ambito dei "conflict minerals" Per ulteriori informazioni relative alla sostenibilità presso Axis, visitare axis.com/about-axis/sustainability
Responsabilità ambientale	axis.com/environmental-responsibility Axis Communications è un firmatario del Global Compact delle Nazioni Unite, per maggiori informazioni vai su unglobalcompact.org

a. Sincronizzazione audio solo con IPv4.

Disegno quotato



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

www.axis.com

Funzionalità evidenziate

Axis Edge Vault

Axis Edge Vault è la piattaforma di cybersicurezza basata sull'hardware che protegge il dispositivo Axis. Rappresenta la base sulla quale poggiano tutte le operazioni sicure e mette a disposizione funzionalità per la tutela dell'identità del dispositivo, la salvaguardia della sua integrità e la protezione dei dati sensibili da accessi non autorizzati. Ad esempio, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con **SO firmato**, impedendo la manomissione fisica della catena di fornitura. Con il sistema operativo firmato, il dispositivo è anche in grado di convalidare il nuovo software del dispositivo prima di accettarne l'installazione.

Il **keystore sicuro** è l'elemento essenziale per proteggere le informazioni di crittografia utilizzate per una comunicazione sicura (IEEE 802.1X, HTTPS, ID dispositivo Axis, chiavi di controllo degli accessi e così via) contro malintenzionati in caso di violazione della sicurezza. Il keystore sicuro e le connessioni sicure vengono forniti tramite un modulo di elaborazione crittografico basato su hardware con certificazione FIPS 140 o Common Criteria.

Per maggiori informazioni relativamente ad Axis Edge Vault, visitare axis.com/solutions/edge-vault.

Per ulteriori informazioni, consulta axis.com/glossary