

AXIS C1310-E Mk II Network Horn Speaker

Alto-falante externo para clareza de voz em longa distância

O AXIS C1310-E Mk II Network Horn Speaker é perfeito para ambientes externos na maioria dos climas. Ele permite que os usuários evitem atividades indesejadas de maneira remota, forneçam instruções durante uma emergência ou façam comunicados gerais. A memória integrada oferece suporte a mensagens pré-gravadas, mas a equipe de segurança também pode responder a notificações falando em tempo real. Os padrões abertos possibilitam uma fácil integração com vídeo em rede, controle de acesso, análise e VoIP (suporte a SIP). O processamento digital de sinais (DSP) garante clareza no áudio. O microfone integrado permite realizar testes remotos de integridade e comunicação bidirecional. Além disso, o software de gerenciamento de áudio incorporado oferece suporte a gerenciamento de usuários, conteúdos, zonas e agendamento.

- > Sistema de alto-falantes tudo em um
- > Conexão a redes padrão
- > Instalação simples com PoE
- > Teste de integridade remoto
- > Expansível e fácil de integrar



AXIS C1310-E Mk II Network Horn Speaker

Hardware de áudio

Gabinete	Alto-falante de corneta regressante com driver de compactação
Nível de pressão sonora máximo	>121 dB
Resposta em frequência	280 Hz – 12,5 kHz
Padrão de cobertura	70° horizontal por 100° vertical (a 2 kHz)
Entrada/saída de áudio	Microfone integrado (pode ser desativado mecanicamente) Alto-falante integrado
Especificação do microfone integrado	50 Hz – 12 kHz
Descrição do amplificador	Amplificador integrado de 7 W Classe D
Processamento digital de sinais	Integrado e pré-configurado

Gerenciamento de áudio

AXIS Audio Manager Edge	Integrado: – Gerenciamento de zonas que permite dividir até 200 alto-falantes em 20 zonas. – Gerenciamento de conteúdo para música e comunicados ao vivo/pré-gravados. – Cronograma de quando e onde executar conteúdo. – Priorização de conteúdo para garantir que mensagens urgentes interrompam a programação. – Monitoramento de integridade para descoberta remota de erros do sistema. – Gerenciamento de usuários para controlar quem tem acesso a quais recursos. Para obter mais detalhes, consulte a folha de dados em axis.com/products/axis-audio-manager-edge/support
AXIS Audio Manager Pro	Para sistemas maiores e mais avançados. Vendido separadamente. Para obter as especificações, consulte a folha de dados em axis.com/products/axis-audio-manager-pro/support
AXIS Audio Manager Center	O AXIS Audio Manager Center é um serviço em nuvem para acesso remoto e gerenciamento de sistemas multissite. Para obter as especificações, consulte a folha de dados em axis.com/products/axis-audio-manager-center/support

Software de áudio

Streaming de áudio	Unidirecional/bidirecional com cancelamento de eco half duplex opcional. Mono.
Codificação de áudio	AAC LC 8/16/32/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Axis μ -law 16 kHz, WAV, MP3 em mono/estéreo de 64 kbps a 320 kbps. Taxa de bits constante e variável. Taxa de amostragem de 8 kHz a 48 kHz.

Integração de sistemas

Interface de programação de aplicativo	API aberta para integração de software, incluindo VAPIX®, One-Click Cloud Connection, AXIS Camera Application Platform (ACAP).
Sistemas de gerenciamento de vídeo	Compatível com AXIS Companion, AXIS Camera Station, software de gerenciamento de vídeo de parceiros de desenvolvimento de aplicativos Axis disponíveis em axis.com/vms
Notificação em massa	Singlewire InformaCast®, Intrado Revolution, Lynx, Alertus
Comunicação unificada	Compatibilidade verificada: Clientes SIP: 2N, Yealink, Cisco, Linphone, Grandstream Servidores PBX/SIP: Cisco Call Manager, Cisco BroadWorks, Avaya, Asterix, Grandstream Provedores de serviços na nuvem: Webex, Zoom
SIP	Recursos SIP com suporte: Servidor SIP secundário, 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)

Condições de eventos

Áudio: reprodução de clipes de áudio, resultado do teste de alto-falante
Chamadas: estado, mudança de estado
Status do dispositivo: endereço IP bloqueado/removido, stream ao vivo ativo, perda de rede, novo endereço IP, sistema pronto
Armazenamento de borda: gravação em andamento, interrupção do armazenamento, problemas de integridade do armazenamento detectados
E/S: entrada digital, acionador manual, entrada virtual
MQTT: assinar
Agendados e recorrentes: cronograma

Ações de eventos

Áudio: executar teste automático de alto-falante
Clipes de áudio: reproduzir, parar
E/S: alternar E/S
Luz e sirene: executar, parar
MQTT: publicar
Notificação: HTTP, HTTPS, TCP e email
Gravações: gravar áudio
Mensagens de interceptação SNMP: enviar mensagem
LED de status: piscando

Auxílios de instalação integrados

Verificação e identificação de tom de teste

Monitoramento funcional

Teste automático de alto-falante (verificação via microfone integrado)

Aprovações

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

Cadeia de suprimentos

Compatível com TAA

EMC

EN 55035, EN 55032 Classe B, EN 50121-4, EN 61000-6-1, EN 61000-6-2
Austrália/Nova Zelândia: RCM AS/NZS CISPR 32 Classe B
Canadá: ICES-3(B)/NMB-3(B)
Japão: VCCI Classe B
Coreia: KS C 9835, KS C 9832 Classe B
EUA: FCC Parte 15 Subparte B Classe B
Transporte ferroviário: IEC 62236-4

Segurança

CAN/CSA C22.2 N° 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

Segurança cibernética

ETSI EN 303 645

Rede

Protocolos de rede

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, NTCP, SIP

Segurança cibernética

Segurança de borda

Software: Sistema operacional assinado, proteção contra atrasos por força bruta, autenticação digest, proteção por senha
Hardware: Plataforma segurança cibernética AXIS Edge Vault
Elemento seguro (CC EAL 6+), ID de dispositivo Axis, repositório de chaves seguro, inicialização segura

Segurança de rede

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), PKI de certificado X.509, firewall baseado em host

Documentação

Guia de Fortalecimento do AXIS OS
Política de gerenciamento de vulnerabilidades da Axis
Modelo de desenvolvimento de segurança da Axis
Lista de materiais (SBOM) de software do AXIS OS
Para baixar documentos, vá para axis.com/support/cybersecurity/resources
Para saber mais sobre o suporte da Axis à segurança cibernética, acesse axis.com/cybersecurity

Sistema em um chip (SoC)

Modelo

NXP i.MX 8M Nano

Memória

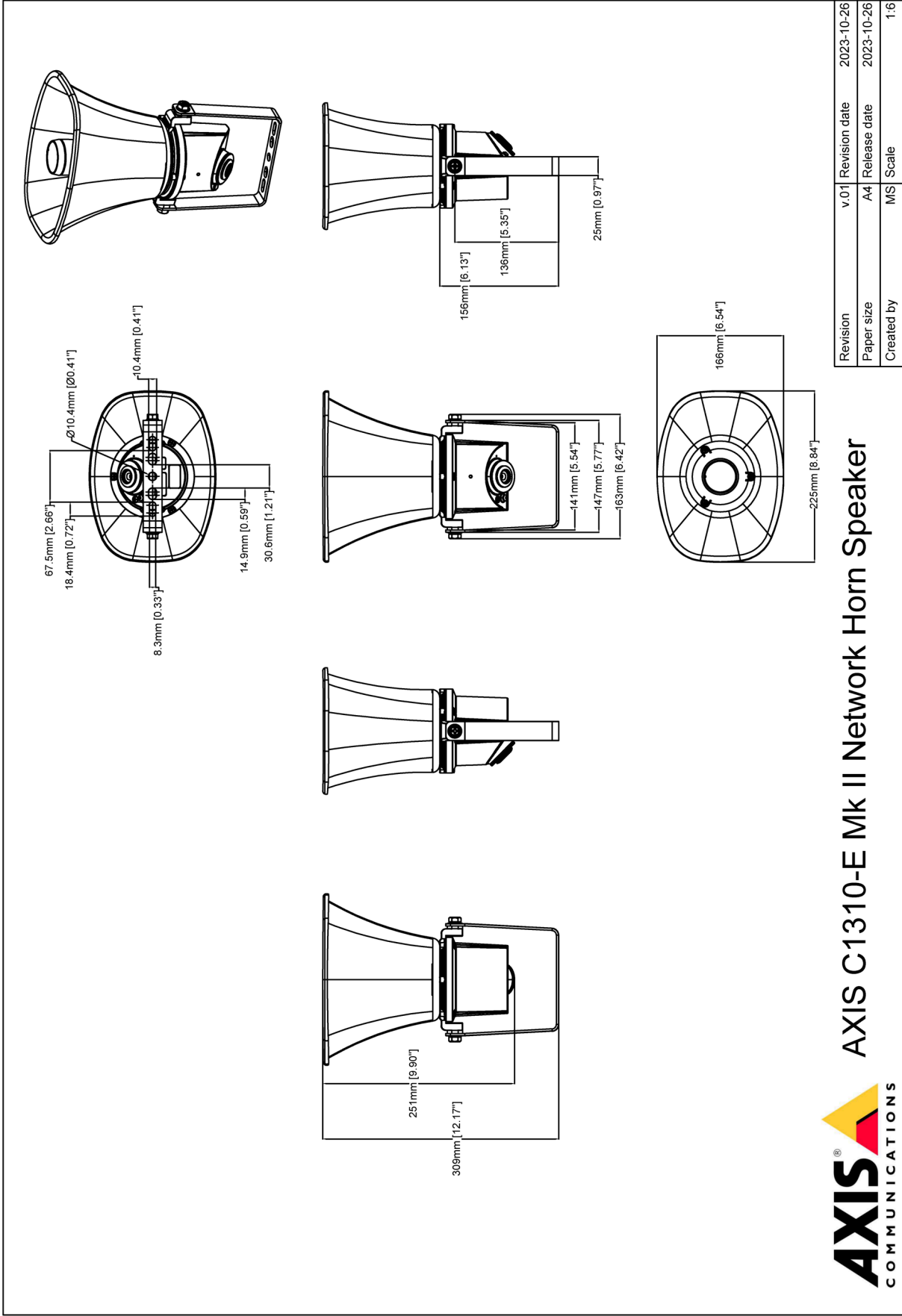
1024 MB de RAM, 1024 MB de flash

Geral	
Caixa	Classificações IP66 e NEMA 4X Lata traseira de alumínio e suporte de aço inoxidável cor: branco RAL 9010
Alimentação elétrica	Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 1 Classe 3 Típico 2 W, máx. 12,95 W
Conectores	Rede: RJ45 10BASE-T/100BASE-TX PoE E/S: Bloco de terminais com 4 pinos de 2,5 mm para 2 x E/S configuráveis supervisionadas
LEDs indicadores	LED de status, LED frontal
Confiabilidade	Desenvolvida para operação ininterrupta 24 horas por dia, 7 dias por semana.
Condições operacionais	Temperatura: -40 °C a 60 °C (-40 °F a 140 °F) Umidade: umidade relativa de 10%–100% (com condensação)
Condições de armazenamento	Temperatura: -40 °C a 65 °C (-40 °F a 149 °F) Umidade: umidade relativa de 5%–95% (sem condensação)
Dimensões	Para obter as dimensões gerais do produto, consulte os esquemas de dimensões nesta folha de dados.
Peso	1,3 kg (2,9 lb)
Conteúdo da embalagem	Megafone, guia de instalação, conector de bloco de terminais, protetor de conector, prensa-cabos, terminal de anéis, chave de autenticação do proprietário
Acessórios opcionais	AXIS T91B47 Pole Mount, AXIS T91F67 Pole Mount, Cable Gland M20x1.5, RJ45, Cable Gland A M20, AXIS Power over Ethernet Midspans, T94R01B Corner Bracket, T94P01B Corner Bracket, T94S01P Conduit Back Box Para conferir mais acessórios, acesse axis.com/products/axis-c1310-e-mk-ii#accessories

Idiomas	Inglês, alemão, francês, espanhol, italiano, russo, chinês simplificado, japonês, coreano, português, polonês, chinês tradicional, holandês, tcheco, sueco, finlandês, turco, tailandês, vietnamita
Garantia	Garantia de cinco anos, consulte axis.com/warranty
Números de peça	Disponível em axis.com/products/axis-c1310-e-mk-ii#part-numbers
Sustentabilidade	
Controle de substâncias	Livre de PVC de acordo com o Padrão JS709 JEDEC/ECA RoHS de acordo com a diretiva RoHS da UE 2011/65/EU/ e EN 63000:2018 REACH de acordo com a (EC) No 1907/2006. Para SCIP UUID, consulte echa.europa.eu
Materiais	Triagem de minerais de conflito de acordo com as diretrizes da OCDE Para saber mais sobre a sustentabilidade na Axis, acesse axis.com/about-axis/sustainability
Responsabilidade ambiental	axis.com/environmental-responsibility A Axis Communications é signatária do Pacto Global da ONU, leia mais em unglobalcompact.org

a. *Sincronização de áudio somente com IPv4.*

Esquema de dimensões



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

Recursos em destaque

Axis Edge Vault

O AXIS Edge Vault é a plataforma segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele forma a base de que todas as operações seguras dependem e oferece recursos para proteger a identidade do dispositivo, proteger sua integridade e proteger informações confidenciais contra acesso não autorizado. Por exemplo, a **inicialização segura** garante que um dispositivo possa inicializar apenas com o **sistema operacional assinado**, o que impede a violação da cadeia de suprimentos física. Com o sistema operacional assinado, o dispositivo também é capaz de validar o novo software do dispositivo antes de aceitar instalá-lo. O **armazenamento de chaves seguro** é o bloco

de construção crítico para a proteção de informações de criptografia usadas para comunicação segura (IEEE 802.1 x, HTTPS, ID de dispositivo da Axis, chaves de controle de acesso, etc.) contra extração maliciosa em caso de violação de segurança. O armazenamento de chaves seguro e as conexões seguras são fornecidos através de um módulo de computação criptográfica com certificação de critérios comuns e/ou FIPS 140.

Para saber mais sobre o Axis Edge Vault, acesse axis.com/solutions/edge-vault.

Para obter mais informações, consulte axis.com/glossary