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

Sistema em um chip (SoC)	
Modelo	i.MX 8M Nano
Memória	1024 MB de RAM, 1024 MB de flash

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 a 12 kHz
Processamento digital de sinais	Integrado e pré-configurado
Descrição do amplificador	Amplificador integrado de 7 W Classe D

Gerenciamento de áudio	
AXIS Audio Manager Edge	Integrado: – Gerenciamento de conteúdo para música e comunicados ao vivo/pré-gravados. – Agendamento de quando e onde executar conteúdos específicos. – Priorização de conteúdo para garantir que mensagens urgentes interrompam a programação. – Gerenciamento de zonas que permite dividir até 200 alto-falantes em 20 zonas. – Monitoramento de integridade para descoberta remota de erros do sistema. – Gerenciamento de usuários para controlar quem tem acesso a quais recursos. Consulte folha de dados separada para obter mais detalhes.
AXIS Audio Manager Pro	Para sistemas maiores e mais avançados. Vendidos separadamente. Consulte folha de dados separada para obter especificações.
AXIS Audio Manager Center	O AXIS Audio Manager Center é um serviço em nuvem para acesso remoto e gerenciamento de sistemas multissite.

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.

Rede	
Protocolos de rede	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, Syslog seguro (RFC 3164/5424, UDP/TCP/TLS), endereço Link-Local (configuração zero), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Integração de sistemas	
Interface de programação de aplicativo	API aberta para integração de software, incluindo VAPIX®, metadados e AXIS Camera Application Platform (ACAP); especificações disponíveis em *axis.com/developer-community*. A ACAP inclui SDK nativo. Conexão com a nuvem com um clique Suporte a Session Initiation Protocol (SIP) para a integração a sistemas Voice over IP (VoIP), ponto a ponto ou integração a SIP/PBX.
Sistemas de gerenciamento de vídeo	Compatível com AXIS Companion, AXIS Camera Station, software de gerenciamento de vídeo de Parceiros de Desenvolvimento de Aplicativos da Axis disponíveis em *axis.com/vms*
Áudio inteligente	Teste automático de alto-falante
Condições de eventos	Áudio: reprodução de clipes de áudio, resultado do teste de alto-falante 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 de conexão, Log de sistema integrado

Aprovações	
Marcações de produtos	CSA, UL/cUL, UKCA, CE, KC, EAC, VCCI, RCM
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 Nº 62368-1 ed. 3, IEC/EN/UL 62368-1 ed. 3
Ambiente	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
Segurança cibernética	ETSI EN 303 645

Segurança cibernética	
Segurança de borda	**Software:** Firmware assinado, proteção forçada contra atrasos, autenticação de ingestão, proteção de 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)[a], IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], 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*

Geral	
Caixa	Classificações IP66 e NEMA 4X Lata traseira de alumínio e suporte de aço inoxidável cor: branco RAL 9010

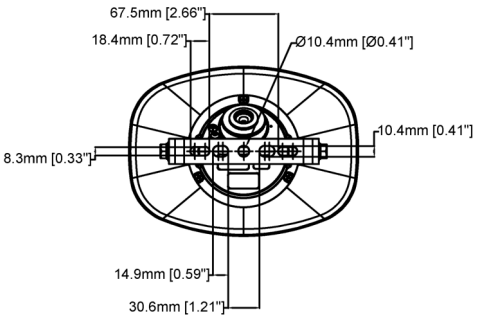
Alimentação elétrica	Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 1 Classe 3 Típico 2 W, máx. 12,95 W
Conectores	Rede: RJ45 10BASE-T/100BASE-TX PoE E/S: Bloco de terminais com 4 pinos de 2,5 mm para 2 x E/S configuráveis supervisionadas
Confiabilidade	Desenvolvida para operação ininterrupta 24/7.
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*

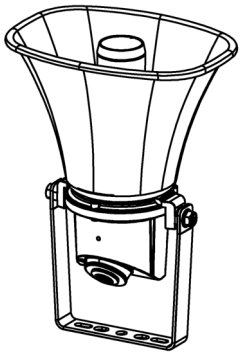
Sustentabilidade

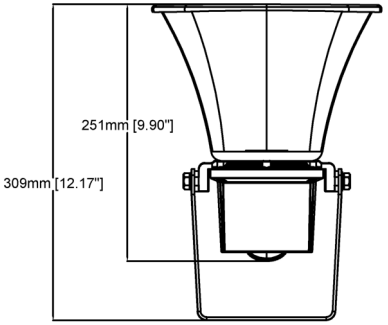
Controle de substâncias	Livre de PVC de acordo com o Padrão JS709 JEDEC/ECA RoHS de acordo com a diretiva RoHS da UE 2011/65/EU/ e EN 63000:2018 REACH de acordo com a (EC) No 1907/2006. Para SCIP UUID, consulte *echa.europa.eu*
Materiais	Avaliado quanto à presença de minerais de conflitos de acordo com as diretrizes da OECD 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*

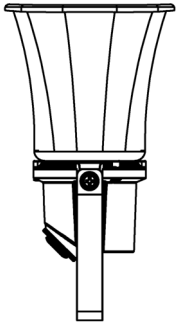
a. *Este produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit. (openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).*

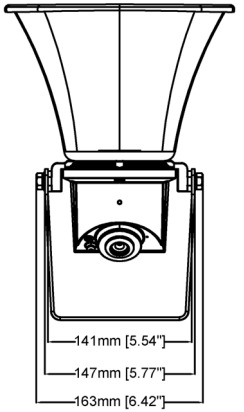
Esquema de dimensões

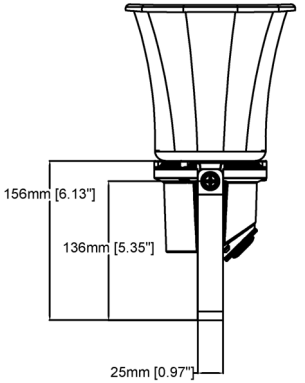


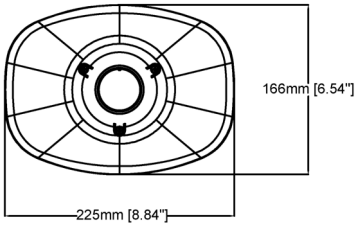












AXIS COMMUNICATIONS

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

www.axis.com

Principais recursos e tecnologias

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 de fábrica e proteger informações confidenciais contra acesso não autorizado.

Estabelecer a raiz de confiança começa no processo de inicialização do dispositivo. Nos dispositivos Axis, a **inicialização segura** do mecanismo com base em hardware verifica o sistema operacional (AXIS OS) do qual o dispositivo está sendo inicializado. O AXIS OS, por sua vez, é assinado criptograficamente (**firmware assinado**) durante o processo de compilação. A inicialização segura e o firmware assinado são vinculados uns aos outros e garantem que o firmware não seja violado durante o ciclo de vida do dispositivo e que o dispositivo só inicie a partir do firmware autorizado. Isso cria uma cadeia inquebrável de software criptografado criptograficamente para a cadeia de confiança de que todas as operações seguras dependem.

De um aspecto de segurança, 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 é fornecido através de um módulo de computação criptográfica com certificação de critérios comuns e/ou FIPS 140. Dependendo dos requisitos de segurança, um dispositivo Axis pode ter um ou vários módulos, como um TPM 2,0 (Trusted Platform Module) ou um elemento seguro, e/ou um ambiente de execução confiável (TEE) incorporado ao sistema em chip (SoC).

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

Para obter mais informações, consulte *axis.com/glossary*