

AXIS C1310-E Mk II Network Horn Speaker

Głośnik zewnętrzny zapewniający czytelność głosu z dużej odległości

AXIS C1310-E Mk II Network Horn Speaker doskonale się nadaje do zastosowań zewnętrznych w prawie każdym klimacie. Umożliwia zdalne zapobieganie niepożądanemu zachowaniu i przekazywanie instrukcji w sytuacjach awaryjnych lub wysyłanie ogólnych wiadomości głosowych. Wbudowana pamięć obsługuje wiadomości nagrane uprzednio. Personel odpowiedzialny za bezpieczeństwo może też reagować na wydarzenia i mówić na żywo. Otwarte standardy umożliwiają prostą integrację sieciowego dozoru wizyjnego, kontroli dostępu, analiz oraz VoIP (obsługa SIP). Procesy cyfrowego przetwarzania sygnałów (CPS) zapewniają dobrą jakość dźwięku. Wbudowany mikrofon umożliwia zdalne testowanie stanu i zapewnia 2-kierunkową komunikację. Ponadto wgrane oprogramowanie do obsługi systemów audio jest wyposażone w funkcje zarządzania użytkownikami, zawartością, strefą, planowanie i inne.

- > **Kompletny system głośników**
- > **Łączenie z siecią standardową**
- > **Łatwa instalacja dzięki PoE**
- > **Zdalne testowanie kondycji systemu**
- > **Skalowalność i łatwa integracja**



AXIS C1310-E Mk II Network Horn Speaker

Sprzęt audio	
Obudowa	Głośnik tubowy z przetwornikiem kompresyjnym
Maks. poziom ciśnienia dźwięku	>121 dB
Charakterystyka częstotliwości	od 280 Hz do 12,5 kHz
Wzór zasięgu	70° w poziomie 100° w pionie (przy 2 kHz)
Wejście/wyjście audio	Wbudowany mikrofon (możliwość mechanicznego wyłączenia) Wbudowany głośnik
Specyfikacja wbudowanego mikrofonu	od 50 Hz do 12 kHz
Opis wzmacniacza	Wbudowany wzmacniacz 7 W klasy D
Przetwarzanie sygnału cyfrowego	Wbudowane i wstępnie skonfigurowane

Zarządzanie dźwiękiem	
AXIS Audio Manager Edge	Wbudowane funkcje: – Zarządzanie strefami umożliwiające podzielenie maks. 200 głośników na 20 stref. – Zarządzanie muzyką i ogłoszeniami w czasie rzeczywistym oraz nagraniami wcześniej. – Planowanie czasu i lokalizacji odtwarzania zawartości. – Ustawianie priorytetów zawartości, tak aby pilne komunikaty miały zawsze pierwszeństwo przed zaplanowanym programem odtwarzania zawartości. – Monitorowanie kondycji w celu zdalnego wykrywania błędów systemu. – Zarządzanie użytkownikami w celu kontrolowania ich dostępu do poszczególnych funkcji. Więcej informacji można znaleźć w arkuszu danych dostępnym na stronie axis.com/products/axis-audio-manager-edge/support
AXIS Audio Manager Pro	W przypadku większych i bardziej zaawansowanych systemów. Sprzedawane oddzielnie. Specyfikacje można znaleźć w arkuszu danych dostępnym na stronie axis.com/products/axis-audio-manager-pro/support
AXIS Audio Manager Center	AXIS Audio Manager Center jest usługą chmurową umożliwiającą zdalny dostęp i zarządzanie systemami obejmującymi wiele lokalizacji. Specyfikacje można znaleźć w arkuszu danych dostępnym na stronie axis.com/products/axis-audio-manager-center/support

Oprogramowanie audio	
Strumieniowanie audio	Jedno-/dwukierunkowe z opcjonalną minimalizacją echa w systemie half-duplex. Mono.
Kodowanie dźwięku	AAC LC 8/16/32/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Axis μ -law 16 kHz, WAV, MP3 mono/stereo od 64 kb/s do 320 kb/s. Stała i zmienna przepływność. Częstotliwość próbkowania od 8 kHz aż do 48 kHz.

Integracja systemu	
Interfejs programowania aplikacji (ang. Application Programming Interface, API)	Otwarty interfejs API umożliwiający integrację oprogramowania, w tym VAPIX®, Łączenie w chmurze jednym kliknięciem, AXIS Camera Application Platform (ACAP).
Systemy zarządzania dozorem wizyjnym	Zgodność z aplikacjami AXIS Companion i AXIS Camera Station oraz oprogramowaniem do zarządzania materiałem wizyjnym od partnerów rozwijających aplikacje firmy Axis dostępnym na stronie axis.com/vms
Masowe powiadomianie	Singlewire InformaCast®, Intrado Revolution, Lynx, Alertus
Ujednolicona komunikacja	Sprawdzona zgodność: Oprogramowanie klienckie SIP: 2N, Yealink, Cisco, Linphone, Grandstream Serwery PBX/SIP: Cisco Call Manager, Cisco BroadWorks, Avaya, Asterix, Grandstream Dostawcy usług w chmurze: Webex, Zoom

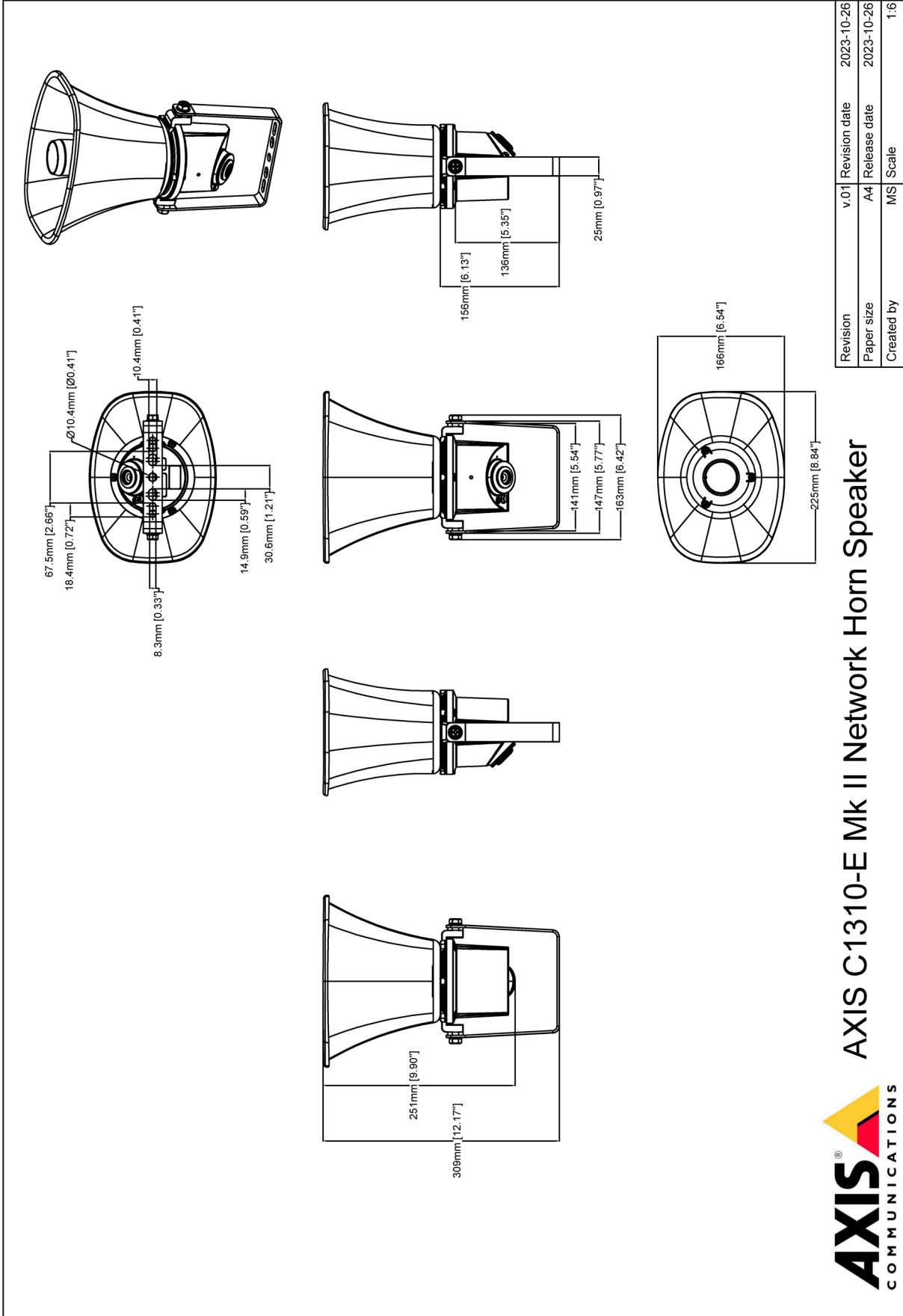
SIP	Obsługiwane funkcje SIP: pomocniczy serwer SIP, IPv6, SRTP, SIPS, SIP TLS, DTMF (RFC2976 i RFC2833), NAT (ICE, STUN, TURN) RFC 3261: INVITE, CANCEL, BYE, REGISTER, OPTIONS, INFO (zapraszanie, anulowanie, pożegnanie, rejestracja, opcje, informacje) DTMF (RFC 4733/RFC 2833)
Warunki zdarzeń	Audio: odtwarzanie klipu audio, wynik testu głośnika Nawiązanie połączenia: stan, zmiany stanu Status urządzenia: blokowanie/usuwanie adresu IP, aktywne przesyłanie strumienia na żywo, utrata połączenia sieciowego, gotowość systemu, nowy adres IP Zasób lokalny: rejestrowanie w toku, zakłócenie pamięci masowej, wykryto problemy z kondycją pamięci masowej We/Wy: wejście cyfrowe, wyzwalacz ręczny, wejście wirtualne MQTT: subskrypcja Zaplanowane i cykliczne: harmonogram
Mechanizmy zdarzeń	Audio: uruchamianie automatycznego testu głośnika Klipy audio: odtwarzanie, zatrzymanie We/Wy: połączenie We/Wy Światło i syrena: uruchomienie, zatrzymanie MQTT: publikacja Powiadomienie: HTTP, HTTPS, TCP i e-mail Nagrania: zapis audio Wiadomości pułapki SNMP: wysłanie wiadomości Wskaźnik LED stanu: miga
Wbudowana pomoc podczas montażu	Weryfikacja i identyfikacja testowa tonowa
Monitorowanie funkcjonalne	Auto Speaker Test (automatyczny test głośników z użyciem wbudowanego mikrofonu)
Certyfikaty	
Oznaczenia produktów	CSA, UL/cUL, UKCA, CE, KC, EAC, VCCI, RCM, BSMI
Łańcuch dostaw	Spełnia wymogi TAA
EMC	EN 55035, EN 55032 klasa B, EN 50121-4, EN 61000-6-1, EN 61000-6-2 Australia / Nowa Zelandia: RCM AS/NZS CISPR 32 klasa B Kanada: ICES-3(B)/NMB-3(B) Japonia: VCCI klasa B Korea: KS C 9835, KS C 9832 klasa B USA: FCC część 15 podczęść B klasa B Koleje: IEC 62236-4
Zabezpieczenia	CAN/CSA C22.2 nr 62368-1 wyd. 3, IEC/EN/UL 62368-1 wyd. 3
Środowisko	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
Cyberbezpieczeństwo	ETSI EN 303 645
Sieć	
Protokoły sieciowe	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
Cyberbezpieczeństwo	
Bezpieczeństwo na obwodzie	Oprogramowanie: podpisany system operacyjny, ochrona przed atakami brute force, uwierzytelnianie szyfrowane, ochrona hasłem Sprzęt: platforma cyberbezpieczeństwa Axis Edge Vault zabezpieczony element (CC EAL 6 +), ID urządzenia Axis, bezpieczny magazyn kluczy, bezpieczne uruchamianie
Bezpieczeństwo w sieci	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), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta

Dokumentacja	Przewodnik po zabezpieczeniach systemu operacyjnego AXIS Polityka AXIS zarządzania podatnością na ataki Model rozwoju zabezpieczeń AXIS Wykaz materiałów oprogramowania dla systemu operacyjnego AXIS (SBOM) Aby pobrać dokumenty, przejdź do strony axis.com/support/cybersecurity/resources Aby przeczytać więcej o wsparciu w zakresie cyberbezpieczeństwa oferowanym przez Axis, przejdź do strony axis.com/cybersecurity
System on chip (SoC)	
Model	NXP i.MX 8M Nano
Pamięć	1024 MB RAM, 1024 MB Flash
Ogólne	
Obudowa	Stopień ochrony IP66 i NEMA 4X Aluminiowa puszką tylna i wspornik ze stali nierdzewnej Kolor: biały RAL 9010
Zasilanie	Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3 Typowo 2 W, maks. 12,95 W
Złącza	Sieć: RJ45 10BASE-T/100BASE-TX PoE We/Wy: 4-pinowy blok złączy 2,5 mm dla 2x nadzorowanych konfigurowalnych We/Wy
Wskaźniki LED	Wskaźnik LED stanu, przednia dioda LED
Niezawodność	Przeznaczone do pracy ciągłej.
Warunki robocze	Temperatura: Od -40°C do 60°C (od -40°F do 140°F) Wilgotność: 10–100% RH (z kondensacją)
Warunki przechowywania	Temperatura: Od -40°C do 65°C (od -40°F do 149°F) Wilgotność: 5–95% RH (bez kondensacji)
Wymiary	Ogólne wymiary produktu można znaleźć na rysunku wymiarowym w niniejszym arkuszu danych.
Masa	1,3 kg (2,9 lb)

Zawartość opakowania	Głośnik tubowy, instrukcja instalacji, blok złączy, osłona złączy, uszczelka kablowa, zacisk pierścieniowy, klucz uwierzytelniania właściciela
Akcesoria opcjonalne	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 Więcej akcesoriów znajduje się na stronie axis.com/products/axis-c1310-e-mk-ii#accessories
Języki	angielski, niemiecki, francuski, hiszpański, włoski, rosyjski, chiński uproszczony, japoński, koreański, portugalski, polski, chiński tradycyjny, niderlandzki, czeski, szwedzki, fiński, turecki, tajski, wietnamski
Gwarancja	5-letnia gwarancja, zobacz axis.com/warranty
Numery części	Dostępne na stronie axis.com/products/axis-c1310-e-mk-ii#part-numbers
Zrównoważony rozwój	
Kontrola substancji	Nie zawiera PCW zgodnie z normą JEDEC/ECA JS709 Zgodność z unijną dyrektywą RoHS 2011/65/UE/ i EN 63000:2018 Zgodność z rozporządzeniem REACH (KE) nr 1907/2006. Informacje o obsłudze protokołu SCIP UUID można znaleźć na stronie echa.europa.eu
Materiały	Sprawdzono pod kątem nienabywania surowców z terenów objętych konfliktami zbrojnymi zgodnie z wytycznymi OECD Aby dowiedzieć się więcej o proekologicznych działaniach Axis, odwiedź stronę axis.com/about-axis/sustainability
Odpowiedzialność za środowisko	axis.com/environmental-responsibility Axis Communications jest sygnatariuszem programu UN Global Compact. Więcej można się dowiedzieć pod adresem unglobalcompact.org .

a. Synchronizacja dźwięku tylko przy adresacji IPv4.

Rysunek wymiarowy



Wyróżnione funkcje

Axis Edge Vault

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Stanowi podstawę, od której zależą wszystkie bezpieczne operacje; zapewnia funkcje ochrony tożsamości urządzenia, ochrony jego integralności oraz ochrony poufnych informacji przed nieautoryzowanym dostępem. Na przykład funkcja **bezpiecznego uruchamiania** zapewnia, że rozruch urządzenia jest możliwy wyłącznie za pomocą **podpisanego systemu operacyjnego**, co uniemożliwia fizyczne manipulacje na poziomie łańcucha dostaw. Dzięki podpisanemu systemowi operacyjnemu urządzenie może też zweryfikować nowe oprogramowanie, zanim zezwoli na jego instalację.

Newralgicznym elementem konstrukcyjnym systemu chroniącego informacje kryptograficzne wykorzystywane do zapewnienia bezpiecznej komunikacji (IEEE 802.1X, HTTPS, identyfikator urządzenia Axis, klucze kontroli dostępu itd.) przed wykradzeniem w razie naruszenia zabezpieczeń jest **bezpieczny magazyn kluczy**. Bezpieczny magazyn kluczy oraz bezpieczne połączenia są realizowane za pomocą wspólnych kryteriów oraz/lub sprzętowego kryptograficznego modułu obliczeniowego mającego certyfikat FIPS 140.

Więcej informacji o rozwiązaniu Axis Edge Vault można znaleźć na stronie axis.com/solutions/edge-vault.

Więcej informacji znajduje się na stronie axis.com/glossary