

AXIS D1110 Video Decoder 4K

Dekoder wideo 4K z wyjściem HDMI™

Tego dekodera wideo 4K można używać do wyświetlania wideo na żywo w widoku sekwencyjnym i do 9 strumieni wideo w widoku złożonym. Stanowi ekonomiczne rozwiązanie do monitoringu wizyjnego, w ramach którego przekazywany na żywo materiał wizyjny może być wyświetlany bez użycia komputera. Urządzenie może być używane z monitorami obsługującymi format HDMI, a ponadto może wyświetlać reklamy lub informacje ogólne z dźwiękiem lub bez niego. Ponadto, dekodery obsługują zarówno zasilanie PoE, jak i DC, co upraszcza i przyspiesza jego instalację.

- > **Wideo 4K i wyjście HDMI**
- > **Zasilanie PoE lub DC**
- > **Wyjście audio**
- > **Płynne działanie widoku sekwencyjnego i złożonego**
- > **Intuicyjny interfejs Axis**



AXIS D1110 Video Decoder 4K

System on chip (SoC)

Model

i.MX8 QuadPlus

Pamięć

2 GB RAM, 1 GB Flash

Nagranie wideo

Kompresja obrazu

H.264/AVC (MPEG-4 część 10/AVC profile Baseline, Main i High (ramka B i rendering z przeplotem nie są obsługiwane))

H.265/HEVC Main profile

Liczba klatek przesyłanych w ciągu zadanej jednostki czasu

Do 60 kl./s zależnie od rozdzielczości

Strumieniowanie wideo

Maksymalnie dziewięć strumieni (osiem z użyciem VPU, jeden z użyciem procesora)

Wyjście wideo

Wszystkie formaty 16:9:

UHD

3840x2160 przy 25/30 kl./s (50/60 Hz)

FHD 1080p

1920x1080 przy 50/60 kl./s (50/60 Hz)

1920x1080 przy 25/30 kl./s (50/60 Hz)

HD 720p

1280x720 przy 50/60 kl./s (50/60 Hz)

SD

720x576 przy 50 kl./s (50 Hz)

720x480 przy 60 kl./s (60 Hz)

Audio

Wyjście audio

Wyjście liniowe, HDMI (stereo)

Sieć

Protokoły sieciowe

IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS¹, HTTP/2, TLS¹, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP, v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, DHCPv4/v6, SSH, LLDP, CDP, MQTT v3.1.1, Syslog, adres Link-Local (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

integracji systemu;

Application Programming Interface (interfejs programowania aplikacji)

otwarty interfejs API do integracji oprogramowania, obejmuje platformy aplikacyjne kamer VAPIX® i AXIS Camera Application Platform (ACAP); specyfikacje znajdują się na stronie axis.com/developer-community One-click cloud connection (łączenie w chmurze jednym kliknięciem)

Systemy zarządzania dozorem wizyjnym

Zgodność z oprogramowaniem AXIS Camera Station Pro, AXIS Camera Station 5 i oprogramowaniem do zarządzania materiałem wizyjnym od partnerów Axis dostępnym na stronie axis.com/vms.

Warunki zdarzeń

usuwanie adresu IP, aktywne przesyłanie strumienia na żywo, utrata połączenia sieciowego, gotowość systemu, nowy adres IP

Pamięć masowa typu Edge: zakłócenie pamięci masowej, wykryto problemy z kondycją pamięci masowej

We/Wy: wyzwacz ręczny, wejście wirtualne

MQTT: bezstanowy

Zaplanowane i cykliczne: harmonogram

Mechanizmy zdarzeń

MQTT: publish

Powiadomienia: HTTP, HTTPS, TCP i poczta e-mail

Pułapki SNMP: wysyłanie, wysyłanie, gdy reguła jest aktywna

Dioda statusu: miganie, miganie, gdy reguła jest aktywna

1. Urządzenie zawiera oprogramowanie opracowane przez organizację OpenSSL Project do zastosowań w zestawie narzędzi OpenSSL Toolkit (openssl.org) oraz oprogramowanie szyfrujące opracowane przez Erika Younga (eyay@cryptsoft.com).

Aprobaty

Oznaczenia produktów

UL/cUL, UKCA, CE, KC, VCCI, RCM

Łącuch dostaw

Zgodność ze standardami TAA

EMC

CISPR 35, CISPR 32 klasa A, EN 55035,
EN 55032 klasa A, EN 61000-3-2, EN 61000-3-3,
EN 61000-6-1, EN 61000-6-2

Australia / Nowa Zelandia:

RCM AS/NZS CISPR 32 klasa A

Kanada: ICES-3(A)/NMB-3(A)

Japonia: VCCI klasa A

Korea: KS C 9835, KS C 9832 klasa A

USA: FCC część 15 podczęść B klasa A

Bezpieczeństwo

IEC/EN/UL 62368-1 wyd. 3,
CAN/CSA C22.2 No. 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 IP30

Sieć

NIST SP500-267

Cyberbezpieczeństwo

ETSI EN 303 645, etykieta bezpieczeństwa IT BSI

Cyberbezpieczeństwo

Bezpieczeństwo na obwodzie

Oprogramowanie: Podpisany system operacyjny, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem

Sprzęt: Platforma cyberbezpieczeństwa Axis Edge Vault Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia Axis, bezpieczny magazyn kluczy, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain 256-bitowe)

Bezpieczeństwo sieci

IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2)²,
IEEE 802.1AE (MACsec PSK / EAP-TLS), IEEE 802.1AR,
HTTPS / HSTS², TLS v1.2 / v1.3², Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta

Dokumentacja

Przewodnika po zabezpieczeniach systemu AXIS OS
zasadach zarządzania lukami przez Axis
Axis Security Development Model

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

Zapisy ogólne

Obudowa

Stopień ochrony IP30

Aluminiowa obudowa

Kolor: NCS S 9000-N

Gniazdo bezpieczeństwa

Montaż

AXIS T91A03 DIN Rail Clip A, uchwyt montażowy, kompatybilny z układem otworów montażowych VESA

Zasilanie

Zasilanie przez sieć Ethernet (PoE)

IEEE 802.3af / 802.3at typ 2 Klasy 4

10–28 V DC, maks. 17 W

Złącza

Sieć: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE

Audio: wyjście liniowe 3,5 mm, stereo

Zasilanie: Wejście DC, blok złączy

2 USB typu A

Slot kart SD (o dużej szybkości/UHS-1)

Obsługa HDMI typu A³, CEC

Przechowywanie

Obsługa kart microSD/microSDHC/microSD UHS-1

Warunki eksploatacji

0 ÷ +40°C

Wilgotność 10–85% RH (bez kondensacji)

Warunki przechowywania

-20°C – 65°C (-4°F – 149°F)

wilgotność względną: 5 – 95% (bez kondensacji)

2. Urządzenie zawiera oprogramowanie opracowane przez organizację OpenSSL Project do zastosowań w zestawie narzędzi OpenSSL Toolkit (openssl.org) oraz oprogramowanie szyfrujące opracowane przez Erika Younga (eyay@cryptsoft.com).

3. Certyfikat ATC

Wymiary

Ogólne wymiary produktu można znaleźć na rysunku wymiarowym w niniejszym arkuszu danych

Waga

500 g (1,10 lb)

Zawartość opakowania

Dekoder wideo, Instrukcja instalacji, zestaw złączy, blok złączy

Akcesoria opcjonalne

AXIS TU9001 Control Board, AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards
Więcej akcesoriów znajduje się na stronie axis.com/products/axis-d1110#accessories

Narzędzia systemowe

AXIS Site Designer, AXIS Device Manager, selektor produktów, selektor akcesoriów
Dostępne na stronie axis.com

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-d1110#part-numbers

Zrównoważony rozwój

Kontrola substancji

Zgodność z unijną dyrektywą RoHS 2011/65/UE i EN 63000:2018
REACH zgodnie z (WE) nr 1907/2006. Identyfikator SCIP UUID znajduje się na stronie echa.europa.eu

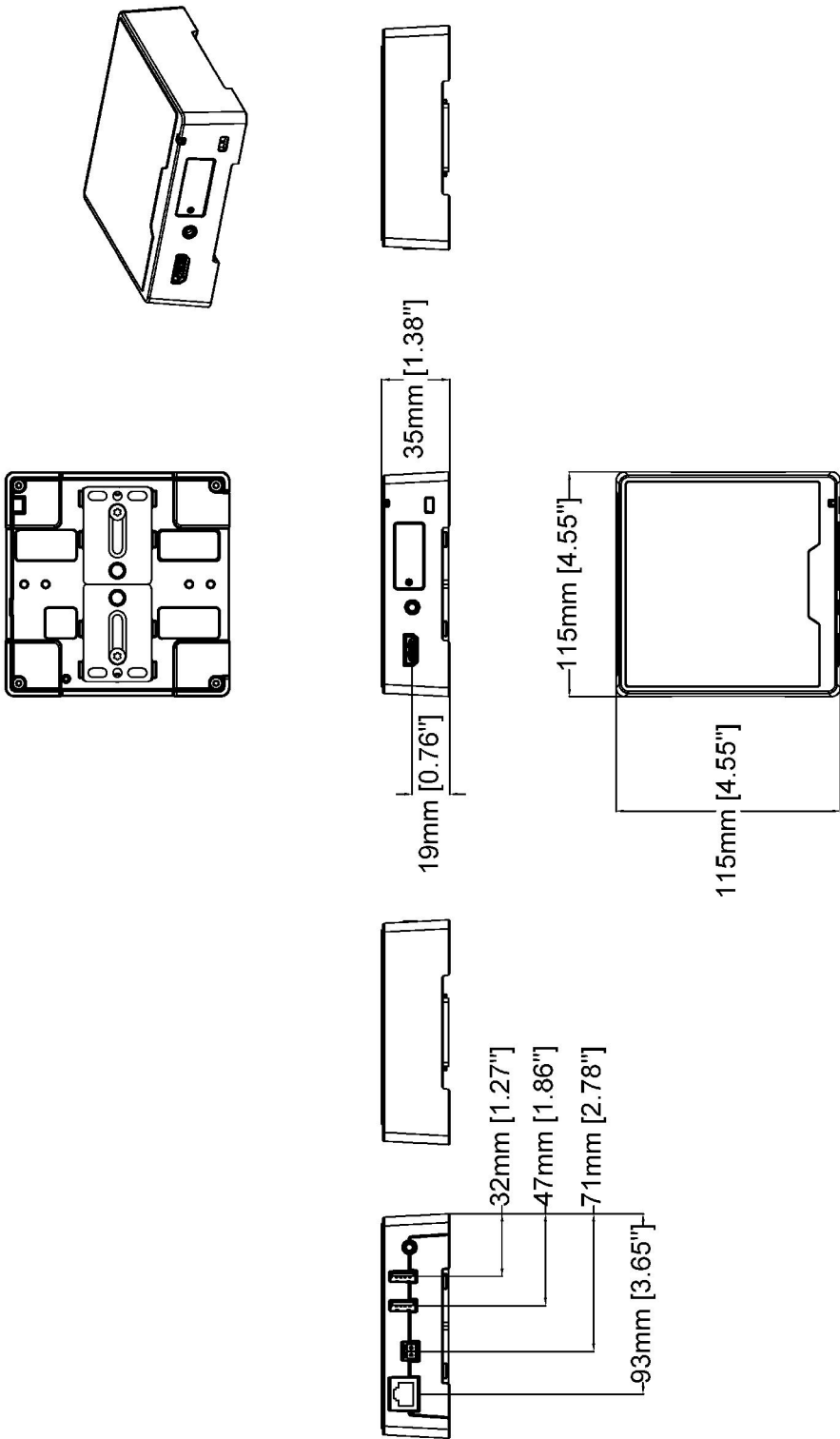
Materiały

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/odpowiedzialnosc-za-srodowisko

Axis Communications jest sygnatariuszem programu UN Global Compact. Więcej można się dowiedzieć pod adresem unglobalcompact.org.



AXIS D1110 Video Decoder 4K

Revision	v.01	Revision date	2021-06-07
Paper size	A4	Release date	2021-06-07
Created by	JSK	Scale	1:3

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 swoje 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