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 8 strumieni wideo w widoku złożonym. Dekoder stanowi oszczędne rozwiązanie do monitoringu wideo, umożliwiające wyświetlanie podglądu na żywo bez konieczności używania komputera PC. Można go używać w połączeniu z monitorami obsługującymi HDMI, a dodatkowo pozwala on wyświetlać reklamy lub ogólne informacje z dźwiękiem lub bez dźwięku. Ponadto, dekoder obsługuje 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**

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

System on chip (SoC)

Model	i.MX8 QuadPlus
Pamięć	2 GB RAM, 1 GB Flash

Wideo

Kompresja wideo	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
Poklatkowość	Do 60 kl./s zależnie od rozdzielczości
Strumieniowanie wideo	Do ośmiu strumieni w VPU (jednostce przetwarzania wideo)
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, HTTPS[a], HTTP/2, TLS[a], 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

Integracja systemu

Interfejs programowania aplikacji (ang. Application Programming Interface, API)	Open API do integracji oprogramowania, w tym VAPIX®, AXIS Camera Application Platform (ACAP); dane techniczne są dostępne pod adresem *axis.com/developer-community.* ACAP zawiera macierzysty zestaw SDK Łączenie w chmurze jednym kliknięciem
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*
Warunki zdarzeń	usuwanie adresu IP, aktywne przesyłanie strumienia na żywo, utrata połączenia sieciowego, gotowość systemu, nowy adres IP Zasób lokalny: zakłócenie zasobu pamięci masowej, wykryto problemy z kondycją pamięci masowej We/Wy: wyzwalacz ręczny, wirtualne wejście MQTT: bez stanu Zaplanowane i cykliczne: harmonogram
Mechanizmy zdarzeń	MQTT: publikacja Powiadomienie: HTTP, HTTPS, TCP i e-mail Pułapki SNMP: wysyłanie, wysyłanie gdy reguła jest aktywna Wskaźnik LED stanu: świecenie, świecenie gdy reguła jest aktywna

Certyfikaty

Oznaczenia produktów	UL/cUL, UKCA, CE, KC, VCCI, RCM
Łańcuch 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
Zabezpieczenia	IEC/EN/UL 62368-1 wyd. 3, CAN/CSA C22.2 nr 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

Cyberbezpieczeństwo

Bezpieczeństwo na obwodzie	**Oprogramowanie:** Podpisane oprogramowanie sprzętowe, 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 +), ID urządzenia Axis, bezpieczny magazyn kluczy, bezpieczne uruchamianie
Bezpieczeństwo w sieci	IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2)[a], IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], 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* 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*

Ogólne

Obudowa	Stopień ochrony IP30 Aluminiowa obudowa Kolor: NCS S 9000-N Gniazdo bezpieczeństwa
Montowanie	AXIS T91A03 DIN Rail Clip A, uchwyt montażowy, kompatybilny z układem otworów montażowych VESA
Zasilanie	Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 2 klasa 4 10–28 V DC, maks. 17 W
Złącza	Sieć: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE Audio: 3,5 mm wyjście liniowe, stereo Zasilanie: Wejście DC, blok złączy 2 USB typu A Gniazdo kart SD (o dużej szybkości/UHS-1) HDMI typu A[b], obsługa CEC
Pamięć masowa	Obsługa kart microSD/microSDHC/microSD UHS-1
Warunki robocze	Od 0°C do 40°C (od 32°F do 104°F) Wilgotność 10–85% RH (bez kondensacji)
Warunki przechowywania	Od -20°C do 65°C (od -4°F do 149°F) Wilgotność 5–95% RH (bez kondensacji)
Wymiary	Ogólne wymiary produktu można znaleźć na rysunku wymiarowym w niniejszym arkuszu danych
Masa	500 g (1,10 lb)
Zawartość opakowania	Dekoder wideo, Instrukcja instalacji, zestaw złączy, blok złączy
Akcesoria opcjonalne	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, kalkulator obiektywów 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*

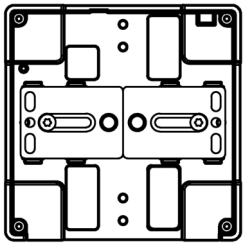
Zrównoważony rozwój

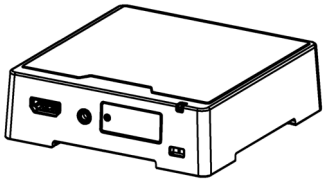
Kontrola substancji	Zgodność z unijną dyrektywą RoHS 2011/65/UE/ i EN 63000:2018 Zgodność z rozporządzeniem REACH (KE) nr 1907/2006. Informacje o obsłudze protokołu SCIP UUID można znaleźć na stronie *echa.europa.eu*
Materiały	Sprawdzono pod kątem nienabywania surowców z terenów objętych konfliktami zbrojnymi zgodnie z wytycznymi OECD Aby dowiedzieć się więcej o proekologicznych działaniach Axis, odwiedź stronę *axis.com/about-axis/sustainability*

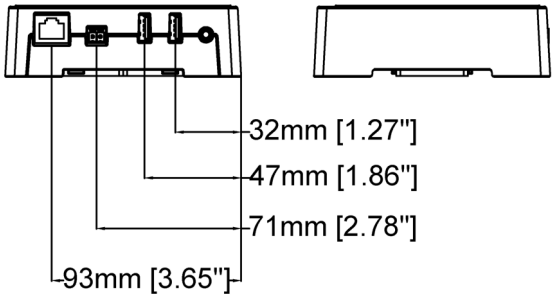
Odpowiedzialność za środowisko	*axis.com/environmental-responsibility* Axis Communications jest sygnatariuszem programu UN Global Compact. Więcej można się dowiedzieć pod adresem *unglobalcompact.org*.

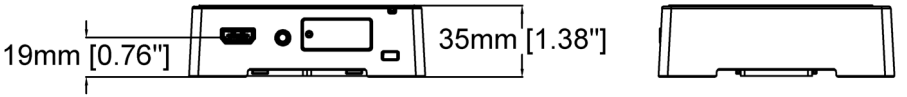
a. *W produkcie zainstalowano oprogramowanie opracowane przez OpenSSL Project do stosowania z OpenSSL Toolkit. (openssl.org) oraz oprogramowanie szyfrujące autorstwa Erica Younga (eay@cryptsoft.com).*
b. *Certyfikat ATC*

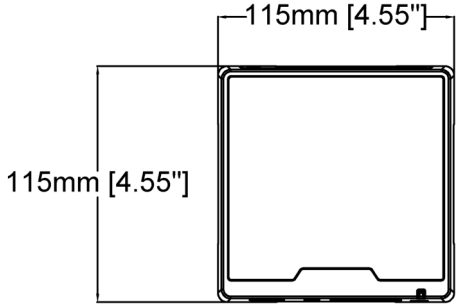
Rysunek wymiarowy











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

Najważniejsze funkcje i technologie

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 przed zresetowaniem do ustawień fabrycznych oraz ochrony poufnych informacji przed nieautoryzowanym dostępem.

Ustanawianie źródła zaufania rozpoczyna się w trakcie rozruchu urządzenia. W urządzeniach Axis sprzętowy mechanizm **bezpiecznego uruchamiania** weryfikuje system operacyjny (AXIS OS), z którego urządzenie się uruchamia. Z kolei system operacyjny AXIS OS jest kryptograficznie podpisywany (**podpisane oprogramowanie sprzętowe**) w trakcie kompilowania. Funkcje bezpiecznego uruchamiania i podpisanego oprogramowania sprzętowego ściśle ze sobą współpracują w celu zapewnienia, że przez cały cykl życia urządzenia nie ingerowano w jego oprogramowanie sprzętowe, a urządzenie jest uruchamiane tylko z autoryzowanego oprogramowania sprzętowego. W ten sposób powstaje nieprzerwany łańcuch kryptograficznie zweryfikowanego oprogramowania dla łańcucha zaufania, na którym będą polegać wszystkie bezpieczne operacje.

W kontekście bezpieczeństwa 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**. Ów bezpieczny magazyn kluczy jest realizowany za pomocą wspólnych kryteriów oraz/lub sprzętowego kryptograficznego modułu obliczeniowego mającego certyfikat FIPS 140. Zależnie od wymaganego poziomu bezpieczeństwa urządzenie Axis może być wyposażone w jeden lub kilka takich modułów, np. TPM 2.0 (Trusted Platform Module) lub zabezpieczony element, oraz/lub układ SoC (system-on-chip) z wbudowanym zaufanym środowiskiem wykonawczym (TEE).

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*