AXIS D1110 Video Decoder 4K

4K-Video-Decoder mit HDMI™-Ausgang

Mit diesem 4K-Video-Decoder lassen sich Live-Videos in der Sequenzansicht und bis zu 8 Videostreams in der Multiview-Ansicht anzeigen. Er bietet eine kostengünstige Videoüberwachungslösung zur Anzeige von Live-Videos ohne PC. Das Gerät kann mit HDMI-fähigen Monitoren eingesetzt werden und ermöglicht außerdem die Anzeige von Werbeeinblendungen oder allgemeinen Informationen mit oder ohne Audio. Für eine schnelle und unkomplizierte Installation ist darüber hinaus sowohl die Stromversorgung über PoE als auch mit Gleichstrom möglich.

- > 4K-Video-Decoder mit HDMI™-Ausgang
- > PoE- oder DC-Stromversorgung
- > Audioausgang
- > Übergangslose Sequenzierung und Multiview-Ansicht
- > Intuitive Axis Bedienoberfläche

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

System-on-Chip (SoC)

Modell	i.MX8 QuadPlus
Arbeitsspeicher	2 GB RAM, 1 GB Flash

Video

Videokomprimierung	H.264/AVC (MPEG-4 Part 10/AVC Baseline, Main und High Profile [ohne Unterstützung von B-Rahmen und Interlaced Rendering]) H.265/HEVC, Main Profile
Bildrate	Bis zu 60 Bilder pro Sekunde je nach Auflösung
Videostreaming	Bis zu acht Videostreams in der VPU (Video Processing Unit)
Video-Ausgang	Alle 16:9-Formate: **UHD** 3840 x 2160 bei 25/30 Bildern pro Sekunde (50/60 Hz) **FHD 1080 px** 1920 x 1080 bei 50/60 Bildern pro Sekunde (50/60 Hz) 1920 x 1080 bei 25/30 Bildern pro Sekunde (50/60 Hz) **HD 720 px** 1280 x 720 bei 50/60 Bildern pro Sekunde (50/60 Hz) **SD** 720 x 576 bei 50 Bildern pro Sekunde (50 Hz) 720 x 480 bei 60 Bildern pro Sekunde (60 Hz)

Audio

Audioausgang	Audio-Ausgang, HDMI (Stereo)

Netzwerk

Netzwerkprotokolle	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, verbindungslokale Adresse (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Systemintegration

Programmierschnittstelle	Offene API zur Software-Integration einschließlich VAPIX® und AXIS Camera Application Platform (ACAP). Technische Daten auf *axis.com/developer-community*. ACAP enthält Native SDK. Cloud-Anbindung mit einem Mausklick
Video Management Systeme	Kompatibel mit AXIS Companion, AXIS Camera Station und Video Management Software von Axis Application Development Partnern, erhältlich unter *axis.com/vms*.
Ereignisbedingungen	IP-Adresse entfernt, Livestream aktiv, Netzwerk-Verlust, neue IP-Adresse, Systembereitschaft Edge Storage: Speicherstörung, Erkennung von Speicherintegritätsproblemen Ein- und Ausgänge: manueller Auslöser, virtueller Eingang MQTT: statuslos Geplant und wiederkehrend: Zeitplan
Ereignisaktionen	MQTT: veröffentlichen Benachrichtigung per: HTTP, HTTPS, TCP und E-Mail SNMP-Traps: Senden, Senden bei aktiver Regel Status-LED: Blinklicht, Blinklicht bei aktiver Regel

Zulassungen

Produktkennzeichnungen	UL/cUL, UKCA, CE, KC, VCCI, RCM
Lieferkette	TAA-konform
EMV	CISPR 35, CISPR 32 Class A, EN 55035, EN 55032 Class A, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2 **Australien/Neuseeland:** RCM AS/NZS CISPR 32 Class A **Kanada:** ICES-3(A)/NMB-3(A) **Japan:** VCCI Klasse A **Korea:** KS C 9835, KS C 9832 Class A **USA:** FCC Part 15 Subpart B Class A
Sicherheit	IEC/EN/UL 62368-1 ed. 3, CAN/CSA C22.2 Nr. 62368-1 Ed. 3
Umwelt	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
Netzwerk	NIST SP500-267

Cybersicherheit

Edge-Sicherheit	**Software:** Signierte Firmware, Verzögerungsschutz gegen Brute-Force-Angriffe, Digest-Authentifizierung, Kennwortschutz **Hardware:** Cybersicherheitsplattform Axis Edge Vault Secure Element (CC EAL 6+), Axis Geräte-ID, sicherer Schlüsselspeicher, sicheres Hochfahren
Netzwerk-Sicherheit	IEEE 802.1X (EAP-TLS)[a], IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], Network Time Security (NTS), X.509 Certificate PKI, IP-Adressen-Filterung
Dokumentation	*AXIS OS Systemhärtungsanleitung* *Axis Vulnerability Management-Richtlinie* *Axis Security Development Model* Diese Dokumente stehen unter *axis.com/support/cybersecurity/resources* zum Download bereit. Weitere Informationen zum Axis Cybersicherheitssupport finden Sie unter *axis.com/cybersecurity*

Allgemein

Gehäuse	Schutzart IP30 Aluminiumgehäuse Farbe: NCS S 9000-N Sicherheitseinschub
Montage	AXIS T91A03 DIN Rail Clip A, Montagehalterung, kompatibel mit VESA-Montagelochbildern
Power	Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 2 Class 4 10 bis 28 V DC, max. 17 W
Anschlüsse	Netzwerk: RJ-45 10BASE-T/100BASE-TX/1000BASE-T PoE Audio: Audioausgang 3,5 mm, Stereo Stromversorgung: DC-Eingang, Anschlussblock 2x USB Typ A Einschub für SD-Speicherkarten (Highspeed/UHS-1) HDMI Typ A[b], CEC-unterstützt
Speicher	Unterstützt SD-Speicherkarten des Typs microSD, microSDHC und microSD UHS-1
Betriebsbedingungen	0 °C bis 40 °C Relative Luftfeuchtigkeit 10 bis 85 % (nicht kondensierend)
Lagerbedingungen	-20 °C bis 65 °C Relative Luftfeuchtigkeit 5 bis 95 % (nicht kondensierend)
Abmessungen	Die Gesamtabmessungen des Produkts sind dem Maßbild in diesem Datenblatt zu entnehmen.
Gewicht	500 g
Inhalt des Kartons	Video-Decoder, Installationsanleitung, Anschlussklemmenblock
Optionales Zubehör	AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards Weiteres Zubehör finden Sie unter *axis.com/products/axis-d1110#accessories*
System-Tools	AXIS Site Designer, AXIS Device Manager, Produkt-Auswahlhilfe, Zubehör-Auswahlhilfe, Objektivrechner Verfügbar auf *axis.com*
Sprachen	Englisch, Deutsch, Französisch, Spanisch, Italienisch, Russisch, Chinesisch (vereinfacht), Japanisch, Koreanisch, Portugiesisch, Polnisch, Chinesisch (traditionell), Niederländisch, Tschechisch, Schwedisch, Finnisch, Türkisch, Thailändisch, Vietnamesisch
Gewährleistung	Informationen zur 5-jährigen Axis Gewährleistung finden Sie unter *axis.com/warranty*
Teilenummern	Abrufbar unter *axis.com/products/axis-d1110#part-numbers*

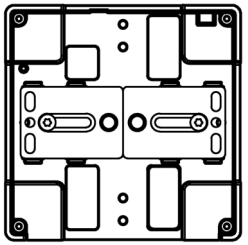
Nachhaltigkeit

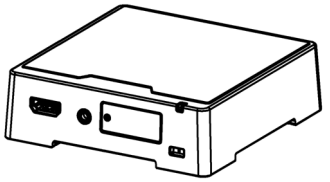
Substanzkontrolle	RoHS gemäß RoHS-Richtlinie 2011/65/EU und EN 63000:2018 REACH gemäß Verordnung (EG) Nr. 1907/2006. Informationen zu SCIP UUID finden Sie auf *echa.europa.eu*.
Materialien	Auf Konfliktmineralien gemäß OECD-Leitfaden überprüft Weitere Informationen zum Thema Nachhaltigkeit bei Axis finden Sie auf *axis.com/about-axis/sustainability*
Verantwortung für die Umwelt	*axis.com/environmental-responsibility* Axis Communications nimmt am UN Global Compact teil. Weitere Informationen dazu finden Sie auf *unglobalcompact.org*

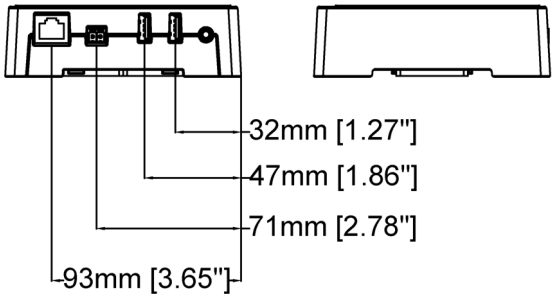
a. *Dieses Produkt enthält Software, die durch das OpenSSL-Projekt für die Nutzung innerhalb des OpenSSL-Toolkits entwickelt wurde. (openssl.org), sowie von Eric Young (eay@cryptsoft.com) geschriebene Verschlüsselungssoftware.*

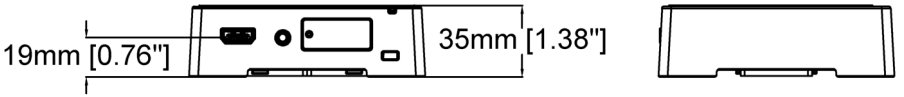
b. *ATC-zertifiziert*

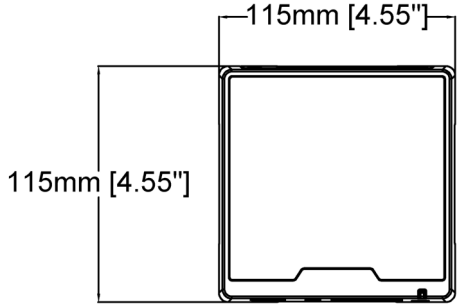
Maßbild











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

www.axis.com

Wesentliche Merkmale und Technologien

Axis Edge Vault

Axis Edge Vault ist die hardwarebasierte Cybersicherheitsplattform zum Schutz des Axis Geräts. Sie bildet die Grundlage für alle sicheren Vorgänge und bietet Funktionen zum Schutz der Identität des Geräts, zur Sicherung seiner Integrität ab Werk und zum Schutz vertraulicher Daten vor unbefugtem Zugriff.

Die Herstellung der Root of Trust beginnt bereits beim Hochfahren des Geräts. Bei Axis Geräten wird das Betriebssystem (AXIS OS), von dem das Gerät hochgefahren wird, durch das hardwarebasierte **sichere Hochfahren** überprüft. AXIS OS wiederum wird beim Build-Prozess kryptografisch signiert (**signierte Firmware**). Das sichere Hochfahren und die signierte Firmware greifen ineinander und stellen sicher, dass die Firmware während des gesamten Lebenszyklus des Geräts nicht manipuliert wurde und das Gerät nur von autorisierter Firmware hochgefahren werden kann. Auf diese Weise erhält man eine ununterbrochene Kette von kryptografisch validierter Software für die Vertrauenskette, von der jedweder sicherer Betrieb abhängig ist.

Hinsichtlich der Sicherheit ist der **sichere Schlüsselspeicher** der entscheidende Faktor für den Schutz kryptografischer Daten, die für die sichere Kommunikation (IEEE 802.1X, HTTPS, Axis Geräte-ID, Schlüssel für die Zugriffskontrolle usw.) verwendet werden, vor einem Missbrauch bei Sicherheitsverletzungen. Der sichere Schlüsselspeicher wird über ein gemäß dem Common Criteria und/oder FIPS 140 zertifiziertes, hardwarebasiertes, kryptografisches Rechenmodul bereitgestellt. Je nach Sicherheitsanforderungen kann ein Axis Gerät entweder über ein oder mehrere solcher Module verfügen, wie z. B. ein TPM 2.0 (Trusted Platform Module) oder ein sicheres Element, und/oder eine in ein System-on-Chip (SoC) integrierte Trusted Execution Environment (TEE).

Weitere Informationen zu Axis Edge Vault finden Sie auf *axis.com/solutions/edge-vault*.

Weitere Informationen finden Sie auf *axis.com/glossary*