

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 16 Videostreams in der Multiview-Ansicht anzeigen. Es bietet eine kostengünstige Lösung für die Videoüberwachung, bei der Live-Videos ohne Verwendung eines PCs angezeigt werden können. Es kann mit Monitoren verwendet werden, die HDMI unterstützen, und es kann Werbung oder allgemeine Informationen mit oder ohne Ton anzeigen. 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**
- > **Audio-Ausgang**
- > **Übergangslose Sequenzierung und Multiview-Ansicht**
- > **Intuitive Axis Bedienoberfläche**



IT-Sicherheitskennzeichen

Bundesamt für Sicherheit in der Informationstechnik

Der Hersteller versichert:
Das Produkt entspricht den Anforderungen des BSI.

Das BSI informiert:
Aktuelles zum Produkt
bsi.bund.de/it-sik/03149



AXIS D1110 Video Decoder 4K

System-on-Chip (SoC)

Modell

i.MX8 QuadPlus

Speicher

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

Bildfrequenz

Bis zu 60 Bilder pro Sekunde je nach Auflösung

Video-Streaming

Bis zu 16 Videostreams (acht mit VPU, acht mit CPU)

Videoausgang

Alle 16:9-Formate:

UHD

3840 x 2160 bei 25/30 Bildern pro Sekunde (50/60 Hz)

FHD 1080p

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

Ausgang

Audio-Ausgang, HDMI (Stereo)

Netzwerk

Netzwerkprotokolle

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, PTP, 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

Anwendungsprogrammierschnittstelle (engl. Application Programming Interface)

Offene API für Softwareintegration, einschließlich VAPIX® und AXIS Camera Application Platform (ACAP). Technische Daten auf axis.com/developer-community One-Click Cloud Connect

Videoverwaltungssysteme

Kompatibel mit AXIS Camera Station Pro, AXIS Camera Station 5 und Video Management Software von Axis Partnern, erhältlich unter axis.com/vms.

Ereignisbedingungen

IP-Adresse entfernt, Livestream aktiv, Netzwerk-Verlust, neue IP-Adresse, Systembereitschaft

Edge Storage: Speicherunterbrechung, Speicherintegritätsprobleme erkannt

E/A: manueller Auslöser, virtueller Eingang

MQTT: zustandslos

Geplant und wiederkehrend: Zeitplan

Ereignisaktionen

MQTT: veröffentlichen

Benachrichtigung; HTTP, HTTPS, TCP und E-Mail

SNMP-Traps: senden, senden während die Regel aktiv ist

Status LED: Blinken, bei aktiver Regel blinken

Zulassungen

Produktkennzeichnungen

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

Lieferkette

Entspricht TAA

1. Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit. (openssl.org) entwickelt wurde, sowie kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

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 Klasse A
Kanada: ICES-3(A)/NMB-3(A)
Japan: VCCI Klasse A
Korea: KS C 9835, KS C 9832 Class A
USA: FCC Teil 15 Abschnitt B Klasse A

Sicherheit

IEC/EN/UL 62368-1 ed. 3,
CAN/CSA C22.2 Nr. 62368-1 Ausg. 3

Umgebung

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

ETSI EN 303 645, BSI IT-Sicherheitskennzeichen,
FIPS-140

Cybersicherheit

Edge-Sicherheit

Software: Signiertes OS, Verzögerungsschutz gegen Brute-Force-Angriffe, Digest-Authentifizierung und OAuth 2.0 RFC6749 Client Credential Flow/OpenID Authorization Code Flow für zentrales ADFS-Kontomanagement, Kennwortschutz, Axis Kryptographie-Modul (FIPS 140-2 Stufe 1)
Hardware: Axis Edge Vault Cybersicherheitsplattform Secure Element (CC EAL 6+), System-on-Chip-Sicherheit (TEE), Axis Geräte-ID, sicherer Schlüsselspeicher, sicherer Systemstart, verschlüsseltes Dateisystem (AES-XTS-Plain 256Bit)

Netzwerksicherheit

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), X.509 Certificate PKI, hostbasierte Firewall

Dokumentation

AXIS OS Hardening Guide
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 auf axis.com/cybersecurity

Allgemeines

Gehäuse

Schutzart IP30
Aluminiumgehäuse
Farbe: NCS S 9000-N
Sicherheitsschlitz

Montage

AXIS T91A03 DIN Rail Clip A, Montagehalterung, kompatibel mit VESA-Montagelochbildern

Strom

Power over Ethernet (PoE) IEEE 802.3af/802.3at Typ 2 Klasse 4
10 bis 28 V DC, max. 17 W

Anschlüsse

Audio: Audioausgang 3,5 mm, Stereo
Datenübertragung: 2x USB Typ A, unterstützte USB-Klasse: HID, Mass Storage
Netzwerk: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE
Stromversorgung: Gleichstromeingang, Anschlussblock Einschub für SD-Speicherkarten (Highspeed/UHS-1) HDMI Typ A³, CEC unterstützt

Speicherung

Unterstützt SD-Speicherkarten des Typs microSD, microSDHC und microSD UHS-1

Betriebsbedingungen

0 °C bis +40 °C (32 °F bis 104 °F)
Luftfeuchtigkeit 10 bis 85 % (nicht kondensierend)

Lagerbedingungen

-20 °C bis 65 °C
Relative Luftfeuchtigkeit 5 bis 95 % (nicht kondensierend)

2. Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit. (openssl.org) entwickelt wurde, sowie kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.
3. ATC-zertifiziert

Abmessungen

Die Gesamtabmessungen des Produkts sind dem Maßbild in diesem Datenblatt zu entnehmen.

Gewicht

500g

Inhalt des Kartons

Video-Decoder, Installationsanleitung,
Anschlussklemmenblock

Optionales Zubehör

AXIS TU9001 Control Board, 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
Erhältlich 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 Gewährleistung finden Sie
auf axis.com/warranty

Artikelnummern

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

Material

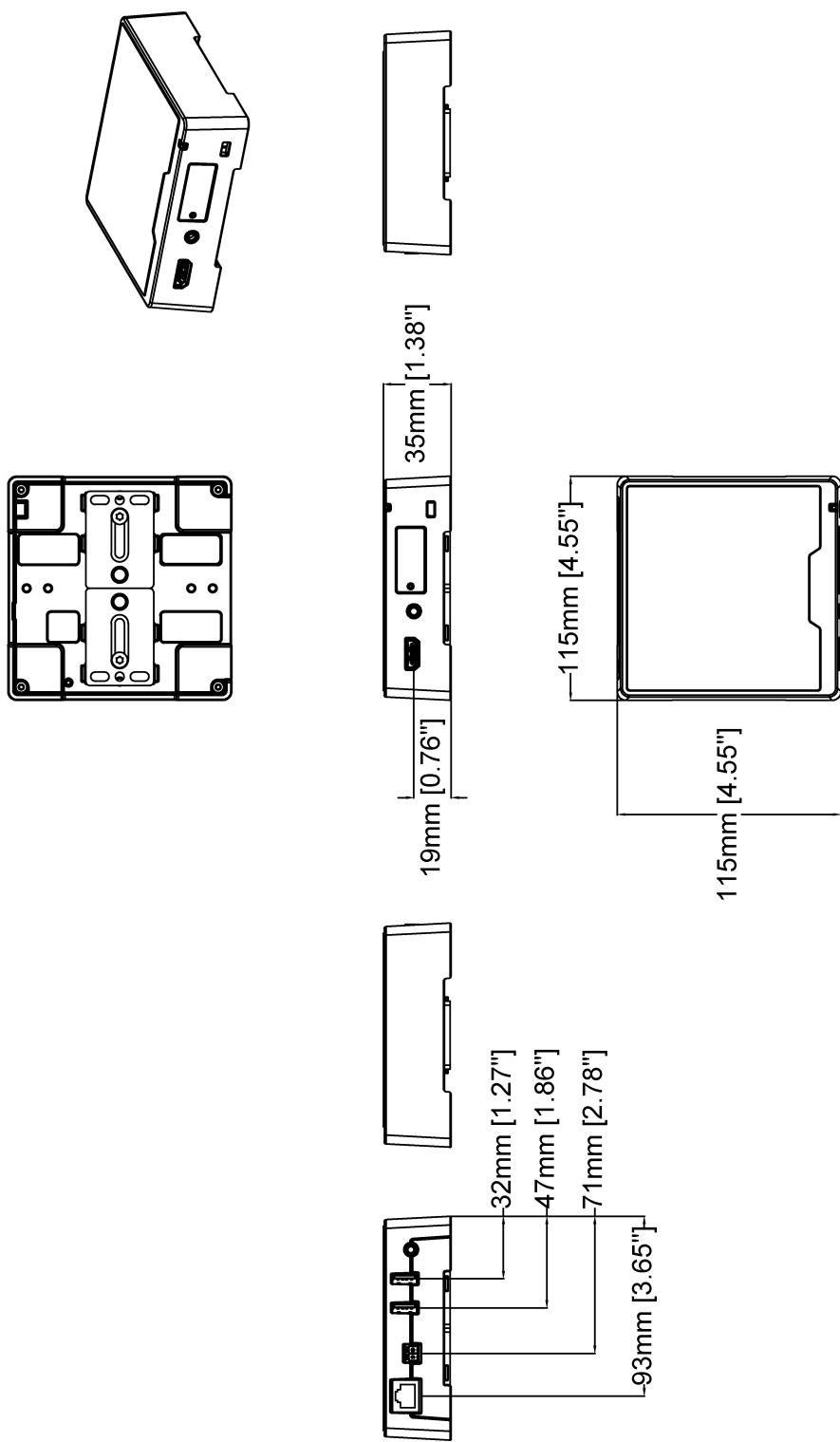
Auf Konfliktmineralien gemäß OECD-Leitfaden
überprüft
Weitere Informationen zum Thema Nachhaltigkeit bei
Axis finden Sie auf axis.com/about-axis/sustainability

Verantwortung für die Umwelt

axis.com/environmental-responsibility

Axis Communications nimmt am UN Global Compact teil. Weitere Informationen hierzu finden Sie auf unglobalcompact.org

Maßbild



AXIS[®]
COMMUNICATIONS

www.axis.com

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

© 2021 Axis Communications

Hervorgehobene Funktionen

Axis Edge Vault

Axis Edge Vault ist die hardwarebasierte Cybersicherheitsplattform zum Schutz des Axis Geräts. Sie bildet die Grundlage für jedweden sicheren Betrieb und bietet Funktionen zum Schutz der Identität des Geräts, zur Sicherung seiner Integrität und zum Schutz vertraulicher Daten vor unbefugtem Zugriff. Beispielsweise sorgt der **sichere Systemstart** dafür, dass ein Gerät nur mit **signiertem Betriebssystem** gestartet werden kann. Dies verhindert konkrete Manipulationen der Bereitstellungskette. Ein Gerät mit signiertem Betriebssystem kann außerdem neue Geräte-Software validieren, bevor es zulässt, dass sie installiert wird. Und 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 Zutrittskontrolle usw.) verwendet werden, vor einem Missbrauch bei Sicherheitsverletzungen. Der sichere Schlüsselspeicher wird über ein gemäß dem Common Criteria oder FIPS 140 zertifiziertes, hardwarebasiertes, kryptografisches Rechenmodul bereitgestellt.

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

Weitere Informationen finden Sie auf axis.com/glossary