

## 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 9 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](#)
- > [Überganglose Sequenzierung und Multiview-Ansicht](#)
- > [Intuitive Axis Bedienoberfläche](#)



# AXIS D1110 Video Decoder 4K

<b>System-on-Chip (SoC)</b>	
Modell	i.MX8 QuadPlus
Speicher	2 GB RAM, 1 GB Flash
<b>Video</b>	
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 neun Videostreams (acht mit VPU, einer 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)
<b>Audio</b>	
Audio-Ausgang	Audio-Ausgang, HDMI (Stereo)
<b>Netzwerk</b>	
Netzwerkprotokolle	IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS <sup>a</sup> , HTTP/2, TLS <sup>a</sup> , CIFS/SMB, SMTP, mDNS (Bonjour), UPnP <sup>®</sup> , 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
<b>Systemintegration</b>	
Anwendungsprogrammierschnittstelle (engl. Application Programming Interface)	Offene API für Softwareintegration, einschließlich VAPIX <sup>®</sup> und AXIS Camera Application Platform (ACAP). Technische Daten auf <a href="http://axis.com/developer-community">axis.com/developer-community</a> One-Click Cloud Connect
Videoverwaltungssysteme	Kompatibel mit AXIS Camera Station Pro, AXIS Camera Station 5 und Video Management Software von Axis Partnern, erhältlich unter <a href="http://axis.com/vms">axis.com/vms</a> .
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
<b>Zulassungen</b>	
Produktkennzeichnungen	UL/cUL, UKCA, CE, KC, VCCI, RCM
Lieferkette	Entspricht TAA
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

## Cybersicherheit

**Edge-Sicherheit** Software: Signiertes Betriebssystem, Verzögerungsschutz gegen Brute-Force-Angriffe, Digest-Authentifizierung und OAuth 2.0 RFC6749 OpenID Authorization Code Flow für zentrale ADFS-Kontoverwaltung, Kennwortschutz  
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)<sup>a</sup>, IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS<sup>a</sup>, TLS v1.2/v1.3<sup>a</sup>, 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](http://axis.com/support/cybersecurity/resources) zum Download bereit.  
Weitere Informationen zum Axis Cybersicherheitssupport finden Sie auf [axis.com/cybersecurity](http://axis.com/cybersecurity)

## Allgemeines

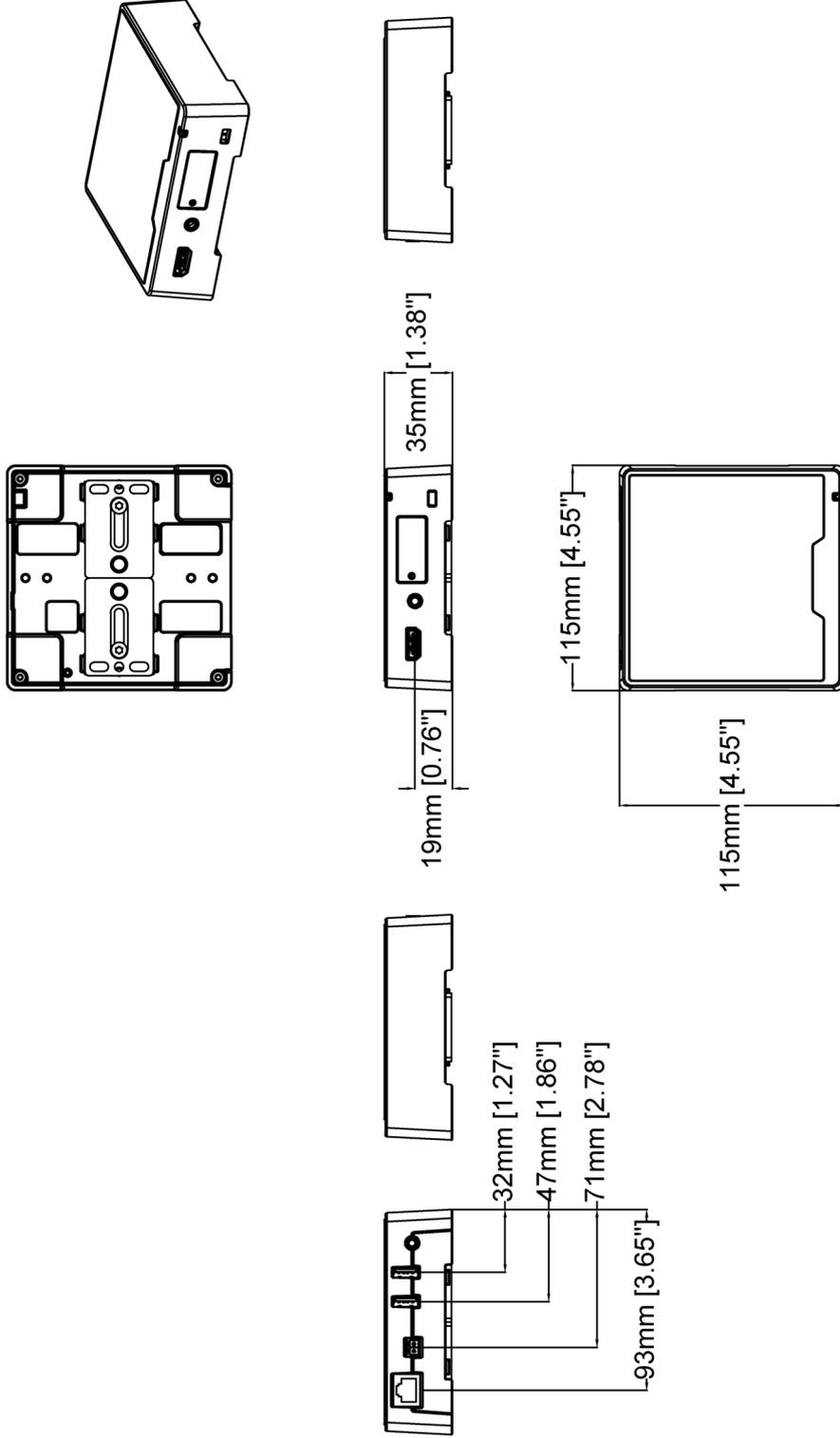
Gehäuse	Schutzart IP30 Aluminiumgehäuse Farbe: NCS S 9000-N Sicherheitsschlitze
Montage	AXIS T91A03 DIN Rail Clip A, Montagehalterung, kompatibel mit VESA-Montagelochbildern
Stromversorgung	Power over Ethernet (PoE) IEEE 802.3af/802.3at Typ 2 Klasse 4 10 bis 28 V DC, max. 17 W
Anschlüsse	Netzwerk: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE Audio: Audioausgang 3,5 mm, Stereo Stromversorgung: Gleichstromeingang, Anschlussblock 2x USB Typ A Einschub für SD-Speicherkarten (Highspeed/UHS-1) HDMI Typ A <sup>b</sup> , CEC unterstützt
Speicherung	Unterstützt SD-Speicherkarten des Typs microSD, microSDHC und microSD UHS-1
Betriebsbedingungen	0 °C bis +40 °C 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	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 <a href="http://axis.com/products/axis-d1110#accessories">axis.com/products/axis-d1110#accessories</a>
System-Tools	AXIS Site Designer, AXIS Device Manager, Produkt-Auswahlhilfe, Zubehör-Auswahlhilfe Erhältlich auf <a href="http://axis.com">axis.com</a> .
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 <a href="http://axis.com/warranty">axis.com/warranty</a>
Artikelnummern	Abrufbar unter <a href="http://axis.com/products/axis-d1110#part-numbers">axis.com/products/axis-d1110#part-numbers</a>
<b>Nachhaltigkeit</b>	
Substanzkontrolle	RoHS gemäß RoHS-Richtlinie 2011/65/EU und EN 63000:2018 REACH gemäß (EG) Nr. 1907/2006. Für SCIP UUID siehe <a href="http://echa.europa.eu">echa.europa.eu</a>

**Material** Auf Konfliktmineralien gemäß OECD-Leitfaden überprüft  
Weitere Informationen zum Thema Nachhaltigkeit bei Axis finden Sie auf [axis.com/about-axis/sustainability](https://axis.com/about-axis/sustainability)

---

**Verantwortung für die Umwelt** [axis.com/environmental-responsibility](https://axis.com/environmental-responsibility)  
Axis Communications nimmt am UN Global Compact teil. Weitere Informationen hierzu finden Sie auf [unglobalcompact.org](https://unglobalcompact.org)

- a. *\*Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit ([openssl.org](https://openssl.org)) entwickelt wurde, sowie kryptografische Software, die von Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)) geschrieben wurde.*
- b. ATC-zertifiziert



# 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

© 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 hinsicht-

lich 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](https://axis.com/solutions/edge-vault).

Weitere Informationen finden Sie auf [axis.com/glossary](https://axis.com/glossary)