AXIS D1110 Video Decoder 4K

Décodeur vidéo 4K avec sortie HDMI™

Ce décodeur vidéo 4K peut être utilisé pour afficher une vidéo en direct dans une vue de séquence et jusqu'à 8 flux vidéo en multi-vues. Il propose une solution économique pour la vidéosurveillance lorsque la vidéo en direct peut être affichée sans recourir à une connexion via un ordinateur. Il peut être utilisé avec des moniteurs qui prennent en charge le format HDMI ; de plus, il peut afficher des publicités ou des informations générales avec ou sans audio. En outre, il prend en charge l'alimentation PoE et CC pour une installation rapide et facile.

- > Vidéo 4K avec sortie HDMI
- > Alimentation PoE ou CC
- > Sortie audio
- > Séquençage transparent et multi-vues
- > Interface Axis intuitive

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

Système sur puce

Modèle	i.MX8 QuadPlus
Mémoire	RAM de 2 Go, mémoire flash de 1 Go

Vidéo

Compression vidéo	H.264/AVC (MPEG-4 Partie 10/AVC Baseline, Main et High profile (la trame B et le rendu entrelacé ne sont pas pris en charge)) H.265/HEVC Main profile
Fréquence d'image	Jusqu'à 60 ips en fonction de la résolution
Diffusion vidéo	Jusqu'à huit flux en VPU (unité de traitement vidéo)
Sortie vidéo	Tous les formats 16:9 : **UHD** 3840x2160 @25/30 ips (50/60 Hz) **FHD 1080p** 1920x1080 @50/60 ips (50/60 Hz) 1920x1080 @25/30 ips (50/60 Hz) **HD 720p** 1280x720 @50/60 ips (50/60 Hz) **SD** 720x576 @50 ips (50 Hz) 720x480 @60 ips (60 Hz)

Audio

Sortie audio	Sortie de ligne, HDMI (stéréo)

Réseau

Protocoles réseau	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, Adresse lien-local (sans configuration), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Intégration système

Interface de programmation	API ouverte pour l'intégration de logiciels, avec VAPIX®, AXIS Camera Application Platform (ACAP) ; caractéristiques disponibles sur *axis.com/developer-community*. L'ACAP inclut un kit SDK natif Connexion Cloud en un clic
Systèmes de gestion vidéo	Compatible avec AXIS Companion, AXIS Camera Station et le logiciel de gestion vidéo des partenaires de développement d'applications d'Axis disponibles sur *axis.com/vms*
Conditions de l'événement	Adresse IP supprimée, flux de données vidéo en direct actif, perte du réseau, nouvelle adresse IP, système prêt Stockage edge : interruption du stockage, problèmes d'état du stockage détectés E/S : déclenchement manuel, entrée virtuelle MQTT : sans état Programmés et récurrents : planning
Déclenchement d'actions en cas d'événement	MQTT : publier Notification : HTTP, HTTPS, TCP et e-mail Déroutements SNMP : envoyer, envoyer tant que la règle est active LED d'état : clignotant, clignotant tant que la règle est active

Homologations

Marquages de produit	UL/cUL, UKCA, CE, KC, VCCI, RCM
Chaîne d'approvisionnement	Conforme aux exigences de la TAA
CEM	CISPR 35, CISPR 32 Classe A, EN 55035, EN 55032 Classe A, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2 **Australie/Nouvelle-Zélande :** RCM AS/NZS CISPR 32 Classe A **Canada :** ICES-3(A)/NMB-3(A) **Japon :** VCCI Classe A **Corée :** KS C 9835, KS C 9832 Classe A **États-Unis :** FCC partie 15 - sous-partie B, Classe A
Sécurité	IEC/EN/UL 62368-1 éd. 3, CAN/CSA C22.2 No. 62368-1 éd. 3
Environnement	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
Réseau	NIST SP500-267

Cybersécurité

Sécurité locale	**Logiciels :** firmware signé, protection contre les attaques par force brute, authentification Digest, protection par mot de passe **Matériel :** plateforme de cybersécurité Axis Edge Vault Secure element (CC EAL 6+), identifiant de périphérique Axis, keystore sécurisé, démarrage sécurisé
Sécurité réseau	IEEE 802.1X (EAP-TLS)[a], IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], sécurité de l'heure réseau (NTS), IGC de certification X.509, filtrage d'adresse IP
Documentation	*Guide de renforcement AXIS OS* *Politique de gestion des vulnérabilités d'Axis* *Modèle de développement de sécurité Axis* Pour télécharger des documents, rendez-vous sur *axis.com/support/cybersecurity/resources* Pour en savoir plus sur la prise en charge de la cybersécurité Axis, rendez-vous sur *axis.com/cybersecurity*

Général

Boîtier	Certification IP30 Boîtier en aluminium Couleur : NCS S 9000-N Fente de sécurité
Montage	AXIS T91A03 DIN Rail Clip A, support de fixation, compatible avec configurations de trous de montage VESA
Alimentation	Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 2 Classe 4 10–28 V CC, 17 W max.
Connecteurs	Réseau : RJ45 pour 10BASE-T/100BASE-TX/1000BASE-T PoE Audio : Sortie de ligne 3,5 mm, stéréo Alimentation : Entrée CC, bloc terminal 2 USB type A Emplacement pour carte SD (Highspeed/UHS-1) HDMI type A[b], CEC pris en charge
Stockage	Compatible avec les cartes microSD/microSDHC/microSD UHS-1
Conditions d'utilisation	0 °C à 40 °C (32 °F à 104 °F) Humidité relative 10 % à 85 % (sans condensation)
Conditions de stockage	-20 °C à 65 °C (-4 °F à 149 °F) Humidité relative de 5 % à 95 % (sans condensation)
Dimensions	Pour les dimensions du produit dans son ensemble, voir le plan coté dans cette fiche technique
Poids	500 g (1,10 lb)
Contenu de la boîte	Décodeur vidéo, guide d'installation, connecteur de bloc terminal
Accessoires en option	AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards Pour en savoir plus sur les accessoires, rendez-vous sur *axis.com/products/axis-d1110#accessories*
Outils système	AXIS Site Designer, AXIS Device Manager, sélecteur de produits, sélecteur d'accessoires, calculateur d'objectif Disponible sur *axis.com*
Langues	Anglais, Allemand, Français, Espagnol, Italien, Russe, Chinois simplifié, Japonais, Coréen, Portugais, Polonais, Chinois traditionnel, Néerlandais, Tchèque, Suédois, Finnois, Turc, Thaï, Vietnamien
Garantie	Garantie de 5 ans, voir *axis.com/warranty*
Références	Disponible sur *axis.com/products/axis-d1110#part-numbers*

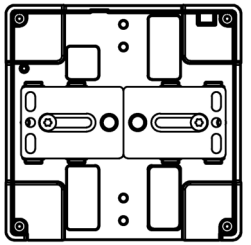
Développement durable

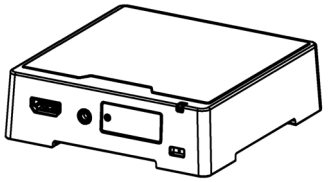
Contrôle des substances	RoHS conformément à la directive de l'UE RoHS 2011/65/EU/ et EN 63000:2018 REACH conformément à (CE) N° 1907/2006. Pour en savoir plus sur l'UUID SCIP, rendez-vous sur *echa.europa.eu*
Matériaux	Vérification conformément aux lignes directrices de l'OCDE concernant le devoir de diligence pour les chaînes d'approvisionnement en minerais provenant de zones de conflit Pour en savoir plus sur le développement durable chez Axis, rendez-vous sur *axis.com/about-axis/sustainability*
Responsabilité environnementale	*axis.com/environmental-responsibility* Axis Communications est signataire du Pacte mondial des Nations unies ; pour en savoir plus, accédez à *unglobalcompact.org*

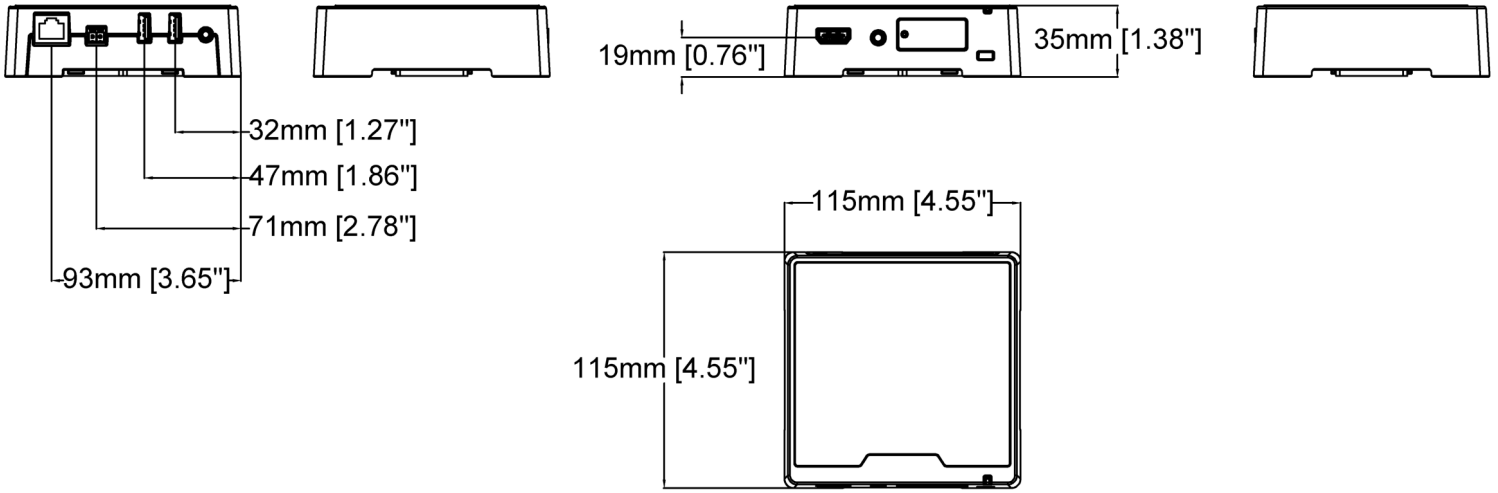
a. *Ce produit inclut un logiciel développé par le projet OpenSSL pour une utilisation dans la boîte à outils OpenSSL. (openssl.org), ainsi qu'un logiciel de cryptographie développé par Eric Young (eay@cryptsoft.com).*

b. *certifié ATC*

Plan coté







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

Principales fonctionnalités et technologies

Axis Edge Vault

Axis Edge Vault est la plate-forme de cybersécurité matérielle qui protège les périphériques Axis. Elle garantit leur identité et leur intégrité, et protège vos informations sensibles contre tout accès non autorisé.

Le processus de démarrage d'un périphérique est à la base de la chaîne de confiance. Sur un périphérique Axis, le mécanisme de **démarrage sécurisé** basé sur le matériel vérifie le système d'exploitation (AXIS OS) à partir duquel il démarre. Une signature cryptographique est associée à Axis OS (**firmware signé**) au cours du processus de création. Le processus de démarrage sécurisé et la signature du firmware sont liés ; ils assurent l'intégrité du firmware tout au long du cycle de vie du périphérique et garantissent que ce dernier ne démarre que depuis un firmware autorisé. Ainsi, tous les logiciels sont validés de manière cryptographique et forment une chaîne de confiance dont dépendent toutes les opérations sécurisées.

En termes de sécurité, le **keystore sécurisé** est un élément clé de la protection des informations cryptographiques utilisées dans le cadre des communications sécurisées (IEEE 802.1X, HTTPS, identifiant de périphérique Axis, clés de contrôle d'accès, etc.) contre toute extraction malveillante en cas de faille. Le keystore sécurisé est mis en œuvre via un module de calcul cryptographique basé sur du matériel certifié FIPS 140 et conforme aux critères courants. Selon les exigences de sécurité en vigueur, un périphérique Axis peut être doté d'un ou de plusieurs modules de ce type, tels qu'un module Trusted Platform Module (TPM 2.0) ou un élément sécurisé, et/ou un environnement TEE de confiance intégré sur un processeur (SoC).

Pour en savoir plus sur Axis Edge Vault, rendez-vous sur *axis.com/solutions/edge-vault*.

Pour en savoir plus, voir *axis.com/glossary*

©2022 - 2023 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC et VAPIX sont des marques déposées d'Axis AB dans diverses juridictions. Toutes les autres marques appartiennent à leurs propriétaires respectifs. Nous nous réservons le droit d'effectuer des modifications sans préavis.