

AXIS D1110 Video Decoder 4K

Decodificador de vídeo 4K com saída HDMI™

Este decodificador de vídeo 4K pode ser usado para exibir vídeo ao vivo na exibição em sequência e até 16 streams de vídeo em multiexibição. Ele oferece uma solução econômica para monitoramento de vídeo, em que o vídeo ao vivo pode ser exibido sem o uso de um PC. Pode ser usado com monitores compatíveis com HDMI, além de poder exibir anúncios ou informações gerais com ou sem áudio. Além disso, ela oferece suporte à alimentação PoE e CC para permitir uma instalação rápida e fácil.

- > **Vídeo 4K com saída HDMI**
- > **Alimentação PoE ou CC**
- > **Saída de áudio**
- > **Sequenciamento contínuo e multiexibição**
- > **Interface Axis intuitiva**



AXIS D1110 Video Decoder 4K

Sistema em um chip (SoC)

Modelo

i.MX8 QuadPlus

Memória

2 GB de RAM, 1 GB de flash

Vídeo

Compressão de vídeo

H.264/AVC (MPEG-4 Parte 10/AVC, perfis Baseline, Main e High (não há suporte a quadros B nem à renderização entrelaçada))
H.265/HEVC perfil Main

Taxa de quadros

Até 60 fps dependendo da resolução

Transmissão de vídeo

Até 16 fluxos (oito usando VPU, oito usando CPU)

Saída de vídeo

Todos os formatos 16:9:

UHD

3840 x 2160 a 25/30 fps (50/60 Hz)

FHD 1080p

1920 x 1080 a 50/60 fps (50/60 Hz)

1920 x 1080 a 25/30 fps (50/60 Hz)

HD 720p

1280 x 720 a 50/60 fps (50/60 Hz)

SD

720 x 576 a 50 fps (50 Hz)

720 x 480 a 60 fps (60 Hz)

Áudio

Saída

Saída de áudio, HDMI (estéreo)

Rede

Protocolos de rede

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, endereço local do link (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Integração de sistemas

Interface de programação de aplicativo

API aberta para integração de software, incluindo VAPIX® e AXIS Camera Application Platform (ACAP); especificações disponíveis em axis.com/developer-community
Conexão com a nuvem com apenas um clique

Sistemas de gerenciamento de vídeo

Compatível com AXIS Camera Station Pro, AXIS Camera Station 5 e software de gerenciamento de vídeo dos parceiros da Axis, disponível em axis.com/vms.

Condições do evento

Endereço IP removido, transmissão ao vivo ativa, perda de rede, novo endereço IP, sistema pronto
Armazenamento de borda: interrupção no armazenamento, problemas de integridade de armazenamento detectados
E/S: acionador manual, entrada virtual
MQTT: sem estado
Agendados e recorrentes: programação

Ações de eventos

MQTT: publicar
Notificação: HTTP, HTTPS, TCP e e-mail
Interceptações SNMP: enviar, enviar enquanto a regra está ativa
LED de status: piscar, piscar enquanto a regra está ativa

Aprovações

Marcações de produtos

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

Cadeia de suprimentos

Compatível com TAA

1. Este produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (openssl.org) e software de criptografia desenvolvido por Eric Young (ey@cryptsoft.com).

EMC

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

Austrália/Nova Zelândia:

RCM AS/NZS CISPR 32 Classe A

Canadá: ICES-3(A)/NMB-3(A)

Japão: VCCI Classe A

Coreia: KS C 9835, KS C 9832 Classe A

EUA: FCC Parte 15 Subparte B Classe A

Proteção

IEC/EN/UL 62368-1 ed. 3,

CAN/CSA C22.2 No. 62368-1 ed. 3

Ambiente

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

Rede

NIST SP500-267

Segurança cibernética

ETSI EN 303 645, selo de segurança de TI do BSI, FIPS-140

Segurança cibernética

Segurança de borda

Software: Sistema operacional assinado, proteção contra atrasos por força bruta, autenticação digest e OAuth 2.0 RFC6749 Client Credential Flow/OpenID Authorization Code Flow para gerenciamento centralizado de contas ADFS, proteção por senha, Axis Cryptographic Module (FIPS 140-2 nível 1)

Hardware: Plataforma de segurança cibernética Axis Edge Vault

Elemento seguro (CC EAL 6 +), segurança de sistema em chip (TEE), ID de dispositivo Axis, repositório de chaves seguro, inicialização segura, sistema de arquivos criptografado (AES-XTS-Plain 256bit)

Segurança de rede

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), PKI de certificado X.509, firewall baseado em host

Documentação

Guia para aumento do nível de proteção do AXIS OS
Política de gerenciamento de vulnerabilidades da Axis
Axis Security Development Model

Para baixar documentos, vá para axis.com/support/cybersecurity/resources

Para saber mais sobre o suporte da Axis à segurança cibernética, acesse axis.com/cybersecurity

Geral

Caixa de proteção

Classificação IP30

Caixa de proteção de alumínio

Cor: NCS S 9000-N

Slot de segurança

Montagem

AXIS T91A03 DIN Rail Clip A, suporte de montagem, compatível com padrões de furos de montagem VESA

Alimentação

Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 2 Classe 4

10 – 28 VCC, máx. 17 W

Conectores

Áudio: saída de linha de 3,5 mm, estéreo

Transferência de dados: 2x USB Tipo A, classe de USB compatível: HID, Mass Storage

Rede: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE

Alimentação: Entrada CC, bloco de terminais

Entrada para cartão SD (Highspeed/UHS-1)

HDMI tipo A³, suporte a CEC

Armazenamento

Suporte a cartões microSD/microSDHC/microSD UHS-1

Condições operacionais

De 0 °C a 40 °C (32 °F a 104 °F)

Umidade relativa de 10 – 85% (sem condensação)

Condições de armazenamento

-20 °C to 65 °C (-4 °F to 149 °F)

Umidade relativa de 5 – 95% (sem condensação)

Dimensões

Para obter as dimensões gerais do produto, consulte os esquemas de dimensões nesta folha de dados

Peso

500 g (1,10 lb)

2. Este produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (openssl.org) e software de criptografia desenvolvido por Eric Young (eay@cryptsoft.com).

3. Certificado pelo ATC

Conteúdo da embalagem

Decodificador de vídeo, guia de instalação, conector de bloco de terminais

Acessórios opcionais

Placa de controle AXIS TU9001, protetor contra tensão AXIS TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards
Para a porta USB: AXIS TU9001 Control Board, AXIS TU9002 Joystick, AXIS TU9003 Keypad, armazenamento USB, tela sensível ao toque, mouse
Para mais acessórios, acesse axis.com/products/axis-d1110#accessories

Ferramentas do sistema

AXIS Site Designer, AXIS Device Manager, seletor de produtos, seletor de acessórios
Disponível em axis.com

Idiomas

Inglês, alemão, francês, espanhol, italiano, russo, chinês simplificado, japonês, coreano, português, polonês, chinês tradicional, holandês, tcheco, sueco, finlandês, turco, tailandês, vietnamita

Garantia

Garantia de 5 anos, consulte axis.com/warranty

Números de peças

Disponível em axis.com/products/axis-d1110#part-numbers

Sustentabilidade

Controle de substâncias

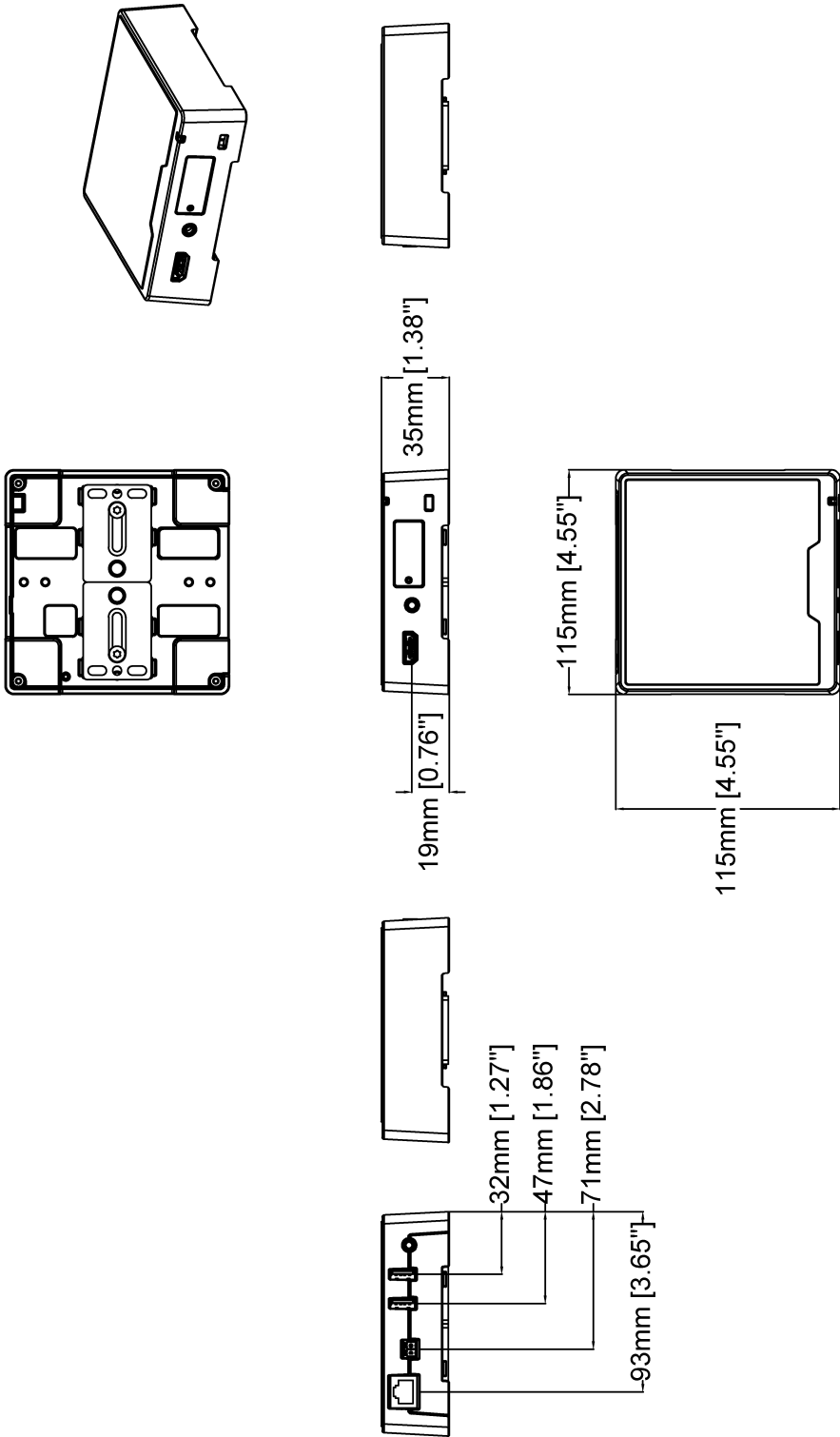
RoHS de acordo com a diretiva RoHS da UE 2011/65/EU e EN 63000:2018
REACH de acordo com a (EC) No 1907/2006. Para SCIP UUID, consulte echa.europa.eu

Materiais

Triagem de minerais de conflito de acordo com as diretrizes da OCDE
Para saber mais sobre a sustentabilidade na Axis, acesse axis.com/about-axis/sustainability

Responsabilidade ambiental

axis.com/environmental-responsibility
A Axis Communications é signatária do Pacto Global da ONU, leia mais em unglobalcompact.org



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

Recursos em destaque

Axis Edge Vault

O Axis Edge Vault é a plataforma de segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele forma a base de que todas as operações seguras dependem e oferece recursos para proteger a identidade do dispositivo, proteger sua integridade e proteger informações confidenciais contra acesso não autorizado. Por exemplo, a **inicialização segura** garante que um dispositivo possa inicializar apenas com o **sistema operacional assinado**, o que impede a manipulação física da cadeia de suprimentos. Com o SO assinado, o dispositivo também é capaz de validar o novo software do dispositivo antes de aceitar instalá-lo. O **armazenamento de chaves seguro** é o bloco de construção crítico para a proteção de informações de criptografia usadas para comunicação segura (IEEE 802.1 x, HTTPS, ID de dispositivo da Axis, chaves de controle de acesso, etc.) contra extração maliciosa em caso de violação de segurança. O armazenamento de chaves seguro e as conexões seguras são fornecidos através de um módulo de computação criptográfica com certificação Common Criteria ou FIPS 140.

Para saber mais sobre o Axis Edge Vault, acesse axis.com/solutions/edge-vault.

Para obter mais informações, consulte axis.com/glossary