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 8 streams de vídeo em multiexibição. Ele oferece uma solução eficiente em termos de custos para monitorar vídeo, onde vídeo ao vivo pode ser exibido sem o uso de um PC. Ele pode ser usado com monitores compatíveis com HDMI e exibir anúncios publicitários 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

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

Sistema em um chip (SoC)

Modelo	i.MX8 QuadPlus
Memória	2 GB de RAM, 1 GB de flash

Vídeo

Compactação 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
Streaming de vídeo	Até oito streams na VPU (unidade de processamento de vídeo)
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 de áudio	Saída de áudio, HDMI (estéreo)

Rede

Protocolos de rede	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, endereço Link-Local (configuração zero), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Integração de sistemas

Interface de programação de aplicativo	API aberta para integração de software, incluindo VAPIX®, AXIS Camera Application Platform (ACAP); especificações disponíveis em *axis.com/developer-community*. A ACAP inclui um SDK nativo One-click Cloud Connection
Sistemas de gerenciamento de vídeo	Compatível com AXIS Companion, AXIS Camera Station, software de gerenciamento de vídeo de Parceiros de Desenvolvimento de Aplicativos Axis disponíveis em *axis.com/vms*
Condições de eventos	endereço IP removido, stream ao vivo ativo, 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: stateless Agendados e recorrentes: agendamento
Ações de eventos	MQTT: publicar Notificação: HTTP, HTTPS, TCP e email 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
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
Segurança	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

Segurança cibernética

Segurança de borda	**Software:** Firmware assinado, proteção contra atrasos por força bruta, autenticação Digest e OAuth 2.0 RFC6749 OpenID Authorization Code Flow para gestão centralizada de contas ADFS, proteção por senha **Hardware:** Plataforma segurança cibernética AXIS Edge Vault Elemento seguro (CC EAL 6 +), ID de dispositivo Axis, repositório de chaves seguro, inicialização segura
Segurança de rede	IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2)[a], IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS[a], TLS v1.2/v1.3[a], Network Time Security (NTS), PKI de certificado X.509, firewall baseado em host
Documentação	*Guia de Fortalecimento do AXIS OS* *Política de gerenciamento de vulnerabilidades da Axis* *Modelo de desenvolvimento de segurança da Axis* 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

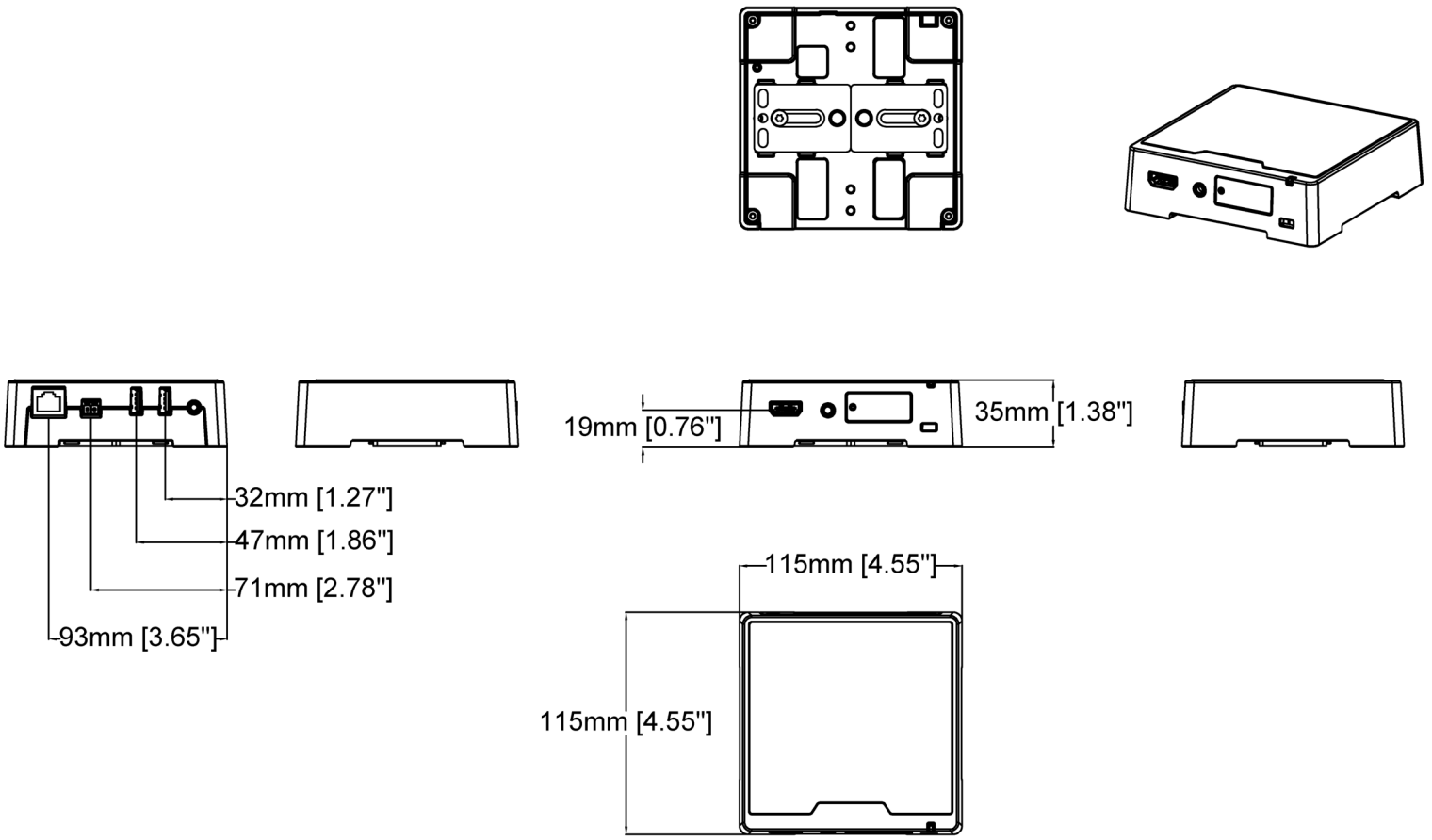
Caixa	Classificação IP30 Caixa em alumínio Cor: NCS S 9000-N Slot de segurança
Montando	AXIS T91A03 DIN Rail Clip A, suporte de montagem, compatível com padrões de furos de montagem VESA
Alimentação elétrica	Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 2 Classe 4 10 – 28 VCC, máx. 17 W
Conectores	Rede: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE Áudio: saída de linha de 3,5 mm, estéreo Potência: Entrada CC, bloco de terminais 2 x USB tipo A Entrada para cartão SD (Highspeed/UHS-1) HDMI tipo A[b], suporte a CEC
Armazenamento	Suporte a cartões microSD/microSDHC/microSD UHS-1
Condições operacionais	0 °C a 40 °C (32 °F a 104 °F) Umidade relativa de 10 – 85% (sem condensação)
Condições de armazenamento	-20 °C a 65 °C (-4 °F a 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)
Conteúdo da embalagem	Decodificador de vídeo, guia de instalação, conector de bloco de terminais
Acessórios opcionais	AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards 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, calculadora de lentes 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 peça	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	Avaliado quanto à presença de minerais de conflitos de acordo com as diretrizes da OECD 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*

a. *Este produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit. (openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).*
b. *Certificação ATC*



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

Principais recursos e tecnologias

Axis Edge Vault

O AXIS Edge Vault é a plataforma 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 de fábrica e proteger informações confidenciais contra acesso não autorizado.

Estabelecer a raiz de confiança começa no processo de inicialização do dispositivo. Nos dispositivos Axis, a **inicialização segura** do mecanismo com base em hardware verifica o sistema operacional (AXIS OS) do qual o dispositivo está sendo inicializado. O AXIS OS, por sua vez, é assinado criptograficamente (**firmware assinado**) durante o processo de compilação. A inicialização segura e o firmware assinado são vinculados uns aos outros e garantem que o firmware não seja violado durante o ciclo de vida do dispositivo e que o dispositivo só inicie a partir do firmware autorizado. Isso cria uma cadeia inquebrável de software criptografado criptograficamente para a cadeia de confiança de que todas as operações seguras dependem.

De um aspecto de segurança, 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 é fornecido através de um módulo de computação criptográfica com certificação de critérios comuns e/ou FIPS 140. Dependendo dos requisitos de segurança, um dispositivo Axis pode ter um ou vários módulos, como um TPM 2,0 (Trusted Platform Module) ou um elemento seguro, e/ou um ambiente de execução confiável (TEE) incorporado ao sistema em chip (SoC).

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

Para obter mais informações, consulte *axis.com/glossary*