

AXIS D1110 Video Decoder 4K

Descodificador de vídeo 4K con salida HDMI™

Este decodificador de vídeo 4K se puede utilizar para mostrar vídeo en directo en vista de secuencia y hasta 9 transmisiones de vídeo multiventana. Es una solución rentable para la supervisión por vídeo, con la posibilidad de visualizar vídeo en directo sin la necesidad de utilizar un PC. Se puede usar con monitores compatibles con HDMI y, además, puede mostrar anuncios o información general con o sin audio. Además, admite alimentación PoE y CC para una instalación rápida y sencilla.

- > [Vídeo 4K con salida HDMI](#)
- > [Alimentación PoE o CC](#)
- > [Salida de audio](#)
- > [Secuencias perfectas y transmisión multiventana](#)
- > [Interfaz Axis intuitiva](#)



AXIS D1110 Video Decoder 4K

Sistema en chip (SoC)	
Modelo	i.MX8 QuadPlus
Flash	2 GB de RAM, 1 GB de memoria flash
Vídeo	
Compresión de vídeo	H.264/AVC (MPEG-4 Parte 10/AVC Base Profile, Main Profile y High Profile (los fotogramas B y la renderización entrelazada no son compatibles)) H.265/HEVC Main perfil
Velocidad de fotogramas	Hasta 60 imágenes por segundo en función de la resolución
Transmisión de vídeo	Hasta nueve secuencias (ocho usando VPU, una usando CPU)
Salida de vídeo	Todos los formatos 16:9: UHD 3840x2160 a 25/30 imágenes por segundo (50/60 Hz) FHD 1080p 1920x1080 a 50/60 fps (50/60 Hz) 1920x1080 a 25/30 fps (50/60 Hz) HD 720p 1280x720 a 50/60 fps (50/60 Hz) SD 720x576 a 50 fps (50 Hz) 720x480 a 60 fps (60 Hz)
Audio	
Salida de audio	Salida de línea, HDMI (estéreo)
Red	
Protocolos de red	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, dirección de enlace local (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR
Integración del sistema	
Interfaz de programación de aplicaciones	API abierta para la integración de software, incluidos VAPIX [®] y AXIS Camera Application Platform (ACAP); las especificaciones están disponibles en axis.com/developer-community . La ACAP incluye Native SDK Conexión a la nube con un clic
Sistemas de gestión de vídeo	Compatible con AXIS Companion, AXIS Camera Station y el software de gestión de vídeo de socios desarrolladores de aplicaciones de Axis disponible en axis.com/vms
Condiciones de evento	Dirección IP eliminada, secuencia en directo activa, pérdida de red, nueva dirección IP, sistema preparado Almacenamiento local: alteración del almacenamiento, detección de problemas de estado del almacenamiento E/S: disparador manual, entrada virtual MQTT: sin estado Programados y recurrentes: programador
Acciones de eventos	MQTT: publicar Notificación: HTTP, HTTPS, TCP y correo electrónico Trampas SNMP: enviar, enviar mientras la regla esté activa LED de estado: iluminar, iluminar mientras la regla esté activa
Homologaciones	
Marcas de productos	UL/cUL, UKCA, CE, KC, VCCI, RCM
Cadena de suministro	Cumple los requisitos de TAA
EMC	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 Australia/Nueva Zelanda: RCM AS/NZS CISPR 32 Clase A Canadá: ICES-3(A)/NMB-3(A) Japón: VCCI Clase A Corea: KS C 9835, KS C 9832 Clase A EE. UU.: FCC Parte 15 Subparte B Clase A
Seguridad	IEC/EN/UL 62368-1 ed. 3, CAN/CSA C22.2 No. 62368-1 ed. 3
Entorno	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

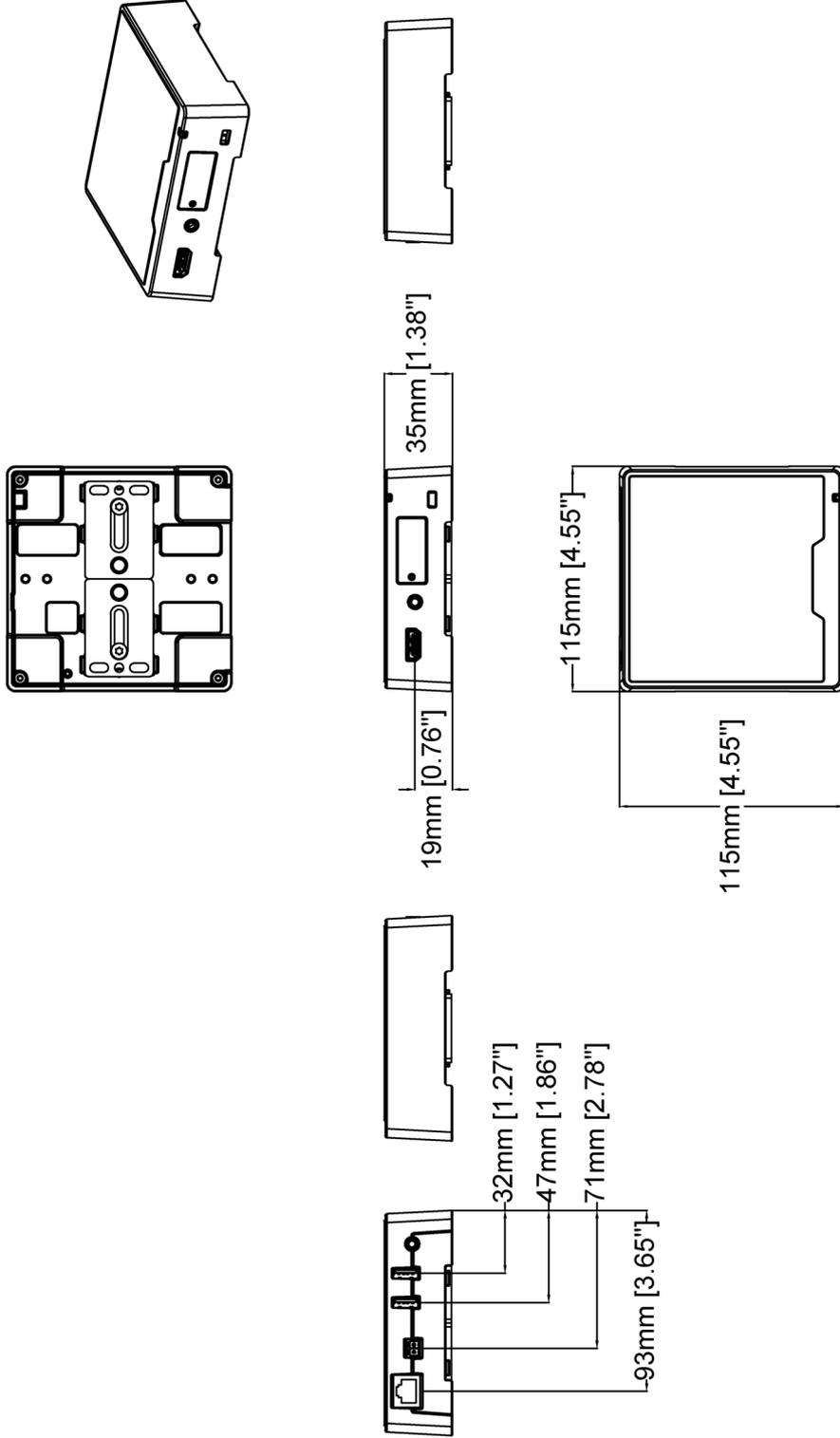
Red	NIST SP500-267
Ciberseguridad	ETSI EN 303 645
Ciberseguridad	
Seguridad perimetral	Software: sistema operativo firmado, protección contra retrasos de fuerza bruta, autenticación digest y flujo de código de autorización OpenID OAuth 2.0 RFC6749 para la gestión centralizada de cuentas ADFS, protección de contraseñas Hardware: Plataforma de ciberseguridad Axis Edge Vault Elemento seguro (CC EAL 6+), seguridad de sistema en un chip (TEE), ID de dispositivo de Axis, almacén de claves seguro, arranque seguro, sistema de archivos cifrado (AES-XTS-Plain 256 bits)
Seguridad de red	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), Certificado pki x.509, firewall basado en host
Documentación	<i>Guía de seguridad de sistemas de AXIS OS</i> <i>Política de gestión de vulnerabilidades de Axis</i> <i>Axis Security Development Model</i> Para descargar documentos, vaya a axis.com/support/cybersecurity/resources Para obtener más información sobre el servicio de asistencia para ciberseguridad de Axis, vaya a axis.com/cybersecurity .
General	
Carcasa	Clasificación IP30 Carcasa de aluminio Color: NCS S 9000-N Ranura de seguridad
Montaje	AXIS T91A03 DIN Rail Clip A, escuadra de montaje, compatible con diseños de orificios de montaje VESA
Alimentación	Alimentación a través de Ethernet (PoE) IEEE 802.3af/802.3at Tipo 2 Clase 4 10-28 V CC, 17 W máx.
Conectores	Red: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE Audio: salida de línea de 3,5 mm, estéreo Alimentación: Entrada CC, bloque de terminales 2 USB Tipo A Ranura para tarjetas SD (alta velocidad/UHS-1) HDMI tipo A ^b , compatible con CEC
Almacenamiento	Compatibilidad con tarjetas microSD/microSDHC/microSD UHS-1.
Condiciones de funcionamiento	De 0 °C a 40 °C (de 32 °F a 104 °F) Humedad relativa del 10 al 85 % (sin condensación)
Condiciones de almacenamiento	De -20 °C a 65 °C Humedad relativa del 5 al 95 % (sin condensación)
Dimensiones	Para obtener información sobre las dimensiones generales del producto, consulte el dibujo de dimensiones de la hoja de datos
Peso	500 g (1,10 lib)
Contenido de la caja	Decodificador de vídeo, guía de instalación, conector de bloques de terminales
Accesorios opcionales	AXIS TU9001 Control Board, AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards Para obtener más información sobre accesorios, vaya a axis.com/products/axis-d1110#accessories
Herramientas de sistema	AXIS Site Designer, AXIS Device Manager, selector de productos, selector de accesorios Disponibles en axis.com
Idiomas	Alemán, chino (simplificado), chino (tradicional), coreano, español, finés, francés, holandés, inglés, italiano, japonés, polaco, portugués, ruso, sueco, tailandés, turco, vietnamita
Garantía	Garantía de 5 años; consulte axis.com/warranty
Referencias	Disponible en axis.com/products/axis-d1110#part-numbers
Sostenibilidad	
Control de sustancias	RoHS de conformidad con la directiva europea RoHS 2011/65/UE/ y EN 63000:2018 REACH de conformidad con (CE) no 1907/2006. Para SCIP UUID, consulte echa.europa.eu

Materiales Análisis de minerales conflictivos conforme a las directrices de la OCDE
Para obtener más información sobre la sostenibilidad en Axis, vaya a axis.com/about-axis/sustainability

Responsabilidad medioambiental axis.com/environmental-responsibility
Axis Communications es firmante del Acuerdo Mundial de las Naciones Unidas, obtenga más información en unglobalcompact.org

- a. Este producto incluye software desarrollado por OpenSSL Project para su uso en el kit de herramientas OpenSSL (openssl.org) y software criptográfico escrito por Eric Young (ey@cryptsoft.com).
- b. Certificación de ATC

Esquemas de dimensiones



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

www.axis.com

Funciones destacadas

Axis Edge Vault

Axis Edge Vault es la plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Constituye la base de la que dependen todas las operaciones seguras y ofrece características para proteger la identidad del dispositivo, proteger su y proteger la información confidencial frente a accesos no autorizados. Por ejemplo, el **arranque seguro** garantiza que un dispositivo solo puede arrancar con el **sistema operativo firmado**. De esta forma, se evita la manipulación de la cadena de suministro física. Con el SO firmado, el dispositivo puede validar también el nuevo software antes de aceptar instalarlo. El **almacén de claves se-**

guro es la pieza clave para proteger la información criptográfica que se utiliza para una comunicación segura (IEEE 802.1X, HTTPS, ID de dispositivo Axis, claves de control de acceso, etc.) contra la extracción maliciosa en caso de una infracción de la seguridad. El almacén de claves seguro y las conexiones seguras se proporcionan a través de un módulo de cálculo criptográfico basado en hardware certificado por FIPS 140 o criterios comunes.

Para obtener más información sobre Axis Edge Vault, vaya a axis.com/solutions/edge-vault.

Para obtener más información, consulte axis.com/glossary