AXIS D1110 Video Decoder 4K

Descodificador de vídeo 4K con salida HDMI™

Este descodificador de vídeo 4K se puede utilizar para mostrar vídeo en directo en vista de secuencia y hasta 8 transmisiones de vídeo multiventana. Este producto ofrece una solución de supervisión de vídeo rentable en la que se puede mostrar vídeo en directo sin necesidad de usar un ordenador. Puede utilizarse con monitores compatibles con HDMI, 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

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

Sistema en chip (SoC)

Modelo	i.MX8 QuadPlus
Memoria	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 profile
Velocidad de imagen	Hasta 60 imágenes por segundo en función de la resolución
Transmisión de vídeo	Hasta ocho transmisiones en VPU (unidad de procesamiento de vídeo)
Salida de vídeo	Todos los formatos 16:9: **UHD** 3840x2160 a 25/30 fps (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, Link-Local address (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*. ACAP incluye Native SDK. Conexión a la nube con un solo 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 en el extremo: alteración del almacenamiento, problemas de estado de almacenamiento detectados E/S: activación manual, entrada virtual MQTT: sin estado Programado y recurrente: programador
Acciones de eventos	MQTT: publicar Notificación: HTTP, HTTPS, TCP y correo electrónico Trampas de 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 N.º 62368-1 ed. 3
Ambiental	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:** Firmware firmado, protección contra retardo por 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+), ID de dispositivo Axis, almacén de claves seguro, arranque seguro
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), X.509 Certificado PKI, firewall basado en host
Documentación	*Guía de seguridad de sistemas de AXIS OS* *Política de gestión de vulnerabilidades de Axis* *Modelo de desarrollo de la seguridad de Axis* 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

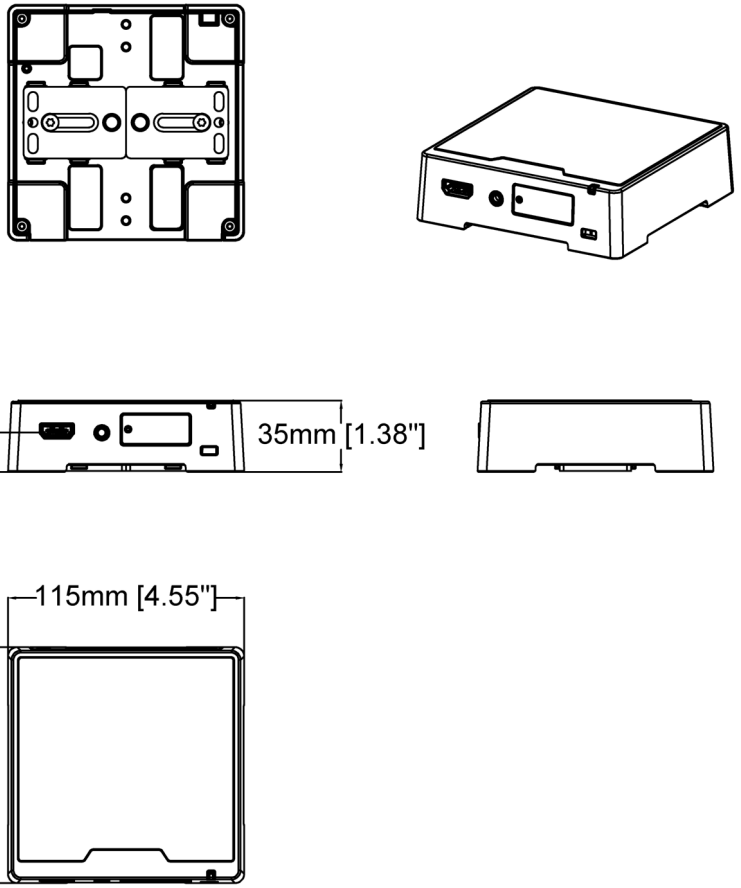
Carcasa	Clasificación IP30 Carcasa de aluminio color: NCS S 9000-N Ranura de seguridad
Montaje	AXIS T91A03 DIN Rail Clip A, escuadra de montaje, compatible con diseños de orificios de montaje VESA
Alimentación	Alimentación a través de Ethernet (PoE) IEEE 802.3af/802.3at Tipo 2 Clase 4 10-28 V CC, 17 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	0 °C a 40 °C 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
Contenido de la caja	Decodificador de vídeo, guía de instalación, conector de bloques de terminales
Accesorios opcionales	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, calculadora de objetivos 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	Se ha evaluado para encontrar minerales en conflicto de acuerdo con las guías 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, lea más 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 (eay@cryptsoft.com).*
b. *certificación 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

Características y tecnologías clave

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 integridad de fábrica y proteger la información confidencial frente a accesos no autorizados.

La base de la confianza comienza en el proceso de arranque del dispositivo. En los dispositivos Axis, el mecanismo de **arranque seguro** basado en hardware verifica el sistema operativo (AXIS OS) desde el que se está iniciando el dispositivo. El SO de AXIS, a su vez, tiene firma criptográfica (**firmware firmado**) durante el proceso de compilación. El arranque seguro y el firmware firmado están vinculados entre sí; se aseguran de que no se haya manipulado el firmware durante el ciclo de vida del dispositivo y que el dispositivo solo arranque con firmware autorizado. De este modo se crea una cadena de software validado criptográficamente para la cadena de confianza de la que dependen todas las operaciones seguras.

Desde un aspecto de seguridad, la **pulsación de tecla segura** 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. La pulsación de tecla segura se proporciona a través de un módulo de cálculo criptográfico basado en hardware certificado por FIPS 140 o criterios comunes. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios de estos módulos, como un TPM 2.0 (Módulo de plataforma de confianza) o un elemento seguro, o un entorno de ejecución de confianza (TEE) integrado en el sistema en un chip (SoC).

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

Para obtener más información, consulte *axis.com/glossary*