AXIS D1110 Video Decoder 4K

Decodificatore video 4K con uscita HDMI™

Questo decodificatore video in 4K può essere utilizzato per visualizzare video in diretta in visualizzazione in sequenza e fino a 9 flussi video in vista multipla. Offre una soluzione economica per il monitoraggio video che consente di visualizzare video in diretta senza l'uso di un PC. Può essere utilizzato con monitor che supportano HDMI e può visualizzare pubblicità o informazioni generali con o senza audio. Supporta l'alimentazione PoE e CC per un'installazione semplice e rapida.

- > Video 4K con uscita HDMI
- > Alimentazione PoE o CC
- > Uscita audio
- > Sequenziamento e visualizzazione multipla continui
- > Interfaccia Axis intuitiva

4K NETWORK VIDEO

AXIS D1110 Video Decoder 4K

System-on-chip (SoC)

Modello
i.MX8 QuadPlus

Memoria
RAM da 2 GB, flash da 1 GB

Video

Compressione video
H.264/AVC (MPEG-4 Parte 10/AVC Profilo di base, principale ed elevato (B-frame e il rendering interlacciato non sono supportati))
H.265/HEVC Main profile

Velocità in fotogrammi
Fino a 60 fps a seconda della risoluzione

Streaming video
Fino a nove flussi (otto con VPU, uno con CPU)

Output video
Tutti i formati 16:9:
UHD
3.840 x 2.160 a 25/30 fps (50/60 Hz)
FHD 1080p
1.920 x 1.080 a 50/60 fps (50/60 Hz)
1.920 x 1.080 a 25/30 fps (50/60 Hz)
HD 720p
1.280 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)

Audio

Output audio
Uscita linea, HDMI (stereo)

Rete

Protocolli di rete
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS[1], HTTP/2, TLS[1], 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, indirizzo di collegamento locale (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

Integrazione di sistemi

Application Programming Interface
API aperta per l'integrazione di software, compresi VAPIX® ed AXIS Camera Application Platform (ACAP); specifiche disponibili all'indirizzo *axis.com/developer-community*
Connessione al cloud con un clic

Sistemi di gestione video
Compatibile con AXIS Camera Station Pro, AXIS Camera Station 5 e con il software per la gestione video di partner di Axis, disponibile all'indirizzo *axis.com/vms*.

Condizioni degli eventi
Indirizzo IP rimosso, flusso dal vivo attivo, perdita di rete, nuovo indirizzo IP, pronto all'uso
Archiviazione edge storage: interruzione dell'archiviazione, problemi di integrità dell'archiviazione rilevati
I/O: attivazione manuale, input virtuale
MQTT: senza stato
Pianificato e ricorrente: pianificazione

Azioni eventi
MQTT: pubblicazione
Notifica: HTTP, HTTPS, TCP ed e-mail
Trap SNMP: invio, invio mentre la regola è attiva
LED di stato: lampeggio, lampeggio mentre la regola è attiva

Approvazioni

Marcature del prodotto
UL/cUL, UKCA, CE, KC, VCCI, RCM

Catena di fornitura
Conformità a TAA

1. *Questo dispositivo comprende il software sviluppato da OpenSSL Project per l'utilizzo con OpenSSL Toolkit (openssl.org) e il software di crittografia scritto da Eric Young (eay@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
Australia/Nuova Zelanda:
RCM AS/NZS CISPR 32 Classe A
Canada: ICES-3(A)/NMB-3(A)
Giappone: VCCI Classe A
Corea: KS C 9835, KS C 9832 Classe A
Stati Uniti: FCC Parte 15 Sottosezione B Classe A

Protezione
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

Rete
NIST SP500-267

Cybersecurity
ETSI EN 303 645, Etichetta sicurezza BSI IT

Cybersecurity

Sicurezza edge
Software: SO firmato, protezione ritardo forza bruta, autenticazione digest e OAuth 2.0 RFC6749 OpenID Authorization Code Flow per la gestione centralizzata dell'account ADFS, protezione mediante password
Hardware: Piattaforma di cybersecurity Axis Edge Vault Secure element (CC EAL 6+), sicurezza system-on-chip (TEE), ID dispositivo Axis, archivio chiavi sicuro, avvio sicuro, file system crittografato (AES-XTS-Plain 256bit)

Protezione della rete
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2)[2],
IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR,
HTTPS/HSTS[2], TLS v1.2/v1.3[2], Network Time Security (NTS), X.509 PKI certificato, firewall basato su host

Documentazione
AXIS OS Hardening Guide
policy di gestione delle vulnerabilità Axis
Axis Security Development Model
Per il download dei documenti, vai a *axis.com/support/cybersecurity/resources*
Per maggiori informazioni relativamente al supporto per la sicurezza informatica Axis, visitare *axis.com/cybersecurity*

Generale

Alloggiamento
Classe IP30
Custodia in alluminio
Colore: NCS S 9000-N
Slot di sicurezza

Montaggio
AXIS T91A03 DIN Rail Clip A, staffa di montaggio, compatibile con schemi dei fori di montaggio VESA

Alimentazione
Power over Ethernet (PoE) IEEE 802.3af/802.3at Tipo 2 Classe 4
10-28 V CC, max 17 W

Connettori
Rete: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE
Audio: uscita linea da 3,5 mm, stereo
Alimentazione: Morsettiera di ingresso CC
2x USB Tipo A
Slot per scheda di memoria (Highspeed/UHS-1)
HDMI Tipo A[3], CEC supportato

Archiviazione
Supporto per scheda di memoria microSD/microSDHC/microSD UHS-1

Condizioni d'esercizio
Da 0 °C a 40 °C
Umidità relativa compresa tra 10% e 85% (senza condensa)

Condizioni di immagazzinaggio
Da -20 °C a 65 °C (-4 °F a 149 °F)
Umidità relativa compresa tra 5% e 95% (senza condensa)

Dimensioni
Per le dimensioni complessive del prodotto, vedere il disegno quotato in questa scheda tecnica

Peso
500 g (1.10 lb)

Contenuto della scatola
Decodificatore video, guida all'installazione, connettore morsettiera

2. *Questo dispositivo comprende il software sviluppato da OpenSSL Project per l'utilizzo con OpenSSL Toolkit (openssl.org) e il software di crittografia scritto da Eric Young (eay@cryptsoft.com).*
3. *Certificato ATC*

Accessori opzionali
AXIS TU9001 Control Board, AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards
Per ulteriori accessori, vai a *axis.com/products/axis-d1110#accessories*

Strumenti di sistema
AXIS Site Designer, AXIS Device Manager, selettore prodotti, selettore accessori
Disponibile all'indirizzo *axis.com*

Lingue
Inglese, tedesco, francese, spagnolo, italiano, russo, cinese semplificato, giapponese, coreano, portoghese, polacco, cinese tradizionale, olandese, ceco, svedese, finlandese, turco, tailandese, vietnamita

Garanzia
Garanzia di 5 anni, visitare *axis.com/warranty*

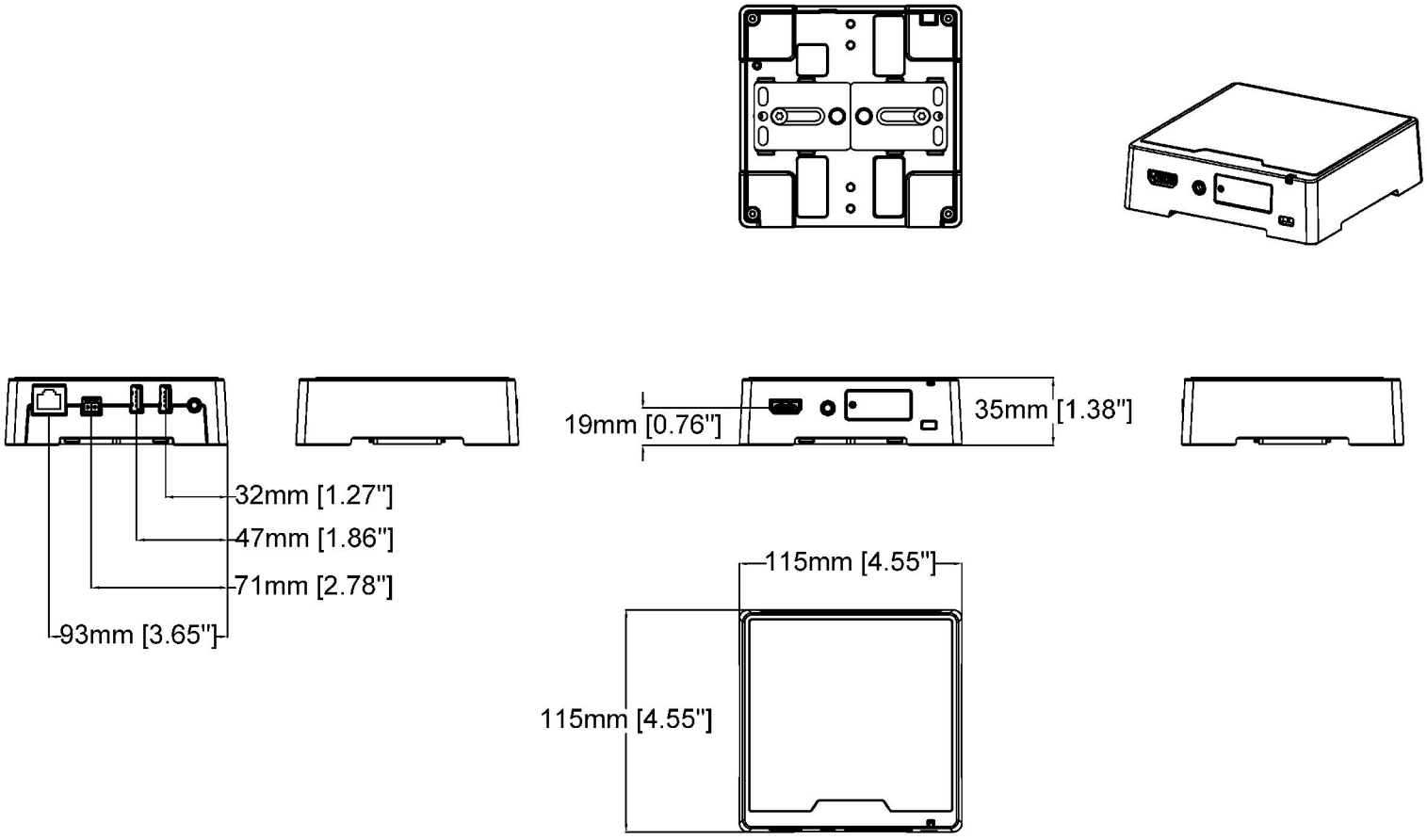
Codici prodotto
Disponibile presso *axis.com/products/axis-d1110#part-numbers*

Sostenibilità

Controllo sostanza
RoHS conformemente alla direttiva UE RoHS 2011/65/UE/ e EN 63000:2018
REACH in conformità con il regolamento (CE) n. 1907/2006. Per l'UUID SCIP, vedere *echa.europa.eu*

Materiali
Sottoposto a controlli conformemente alle linee guida OCSE nell'ambito dei "conflict minerals"
Per ulteriori informazioni relative alla sostenibilità presso Axis, visitare *axis.com/about-axis/sustainability*

Responsabilità ambientale
axis.com/environmental-responsibility
Axis Communications è un firmatario del Global Compact delle Nazioni Unite, per maggiori informazioni vai su *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

Funzionalità evidenziate

Axis Edge Vault

Axis Edge Vault è la piattaforma di cybersicurezza basata sull'hardware che protegge il dispositivo Axis. Rappresenta la base sulla quale poggiano tutte le operazioni sicure e mette a disposizione funzionalità per la tutela dell'identità del dispositivo, la salvaguardia della sua integrità e la protezione dei dati sensibili da accessi non autorizzati. Ad esempio, l'**avvio sicuro** assicura che un dispositivo possa essere avviato solo con **SO firmato**, impedendo la manomissione fisica della catena di fornitura. Con il sistema operativo firmato, il dispositivo è anche in grado di convalidare il nuovo software del dispositivo prima di accettarne l'installazione. Il **keystore sicuro** è l'elemento essenziale per proteggere le informazioni di crittografia utilizzate per una comunicazione sicura (IEEE 802.1X, HTTPS, ID dispositivo Axis, chiavi di controllo degli accessi e così via) contro malintenzionati in caso di violazione della sicurezza. Il keystore sicuro e le connessioni sicure vengono forniti tramite un modulo di elaborazione crittografico basato su hardware con certificazione FIPS 140 o Common Criteria.

Per maggiori informazioni relativamente ad Axis Edge Vault, visitare *axis.com/solutions/edge-vault*.

Per ulteriori informazioni, consulta *axis.com/glossary*