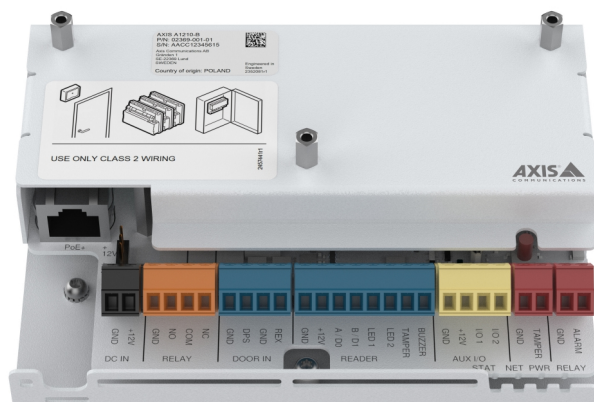


# AXIS A1210-B Network Door Controller

## Kompakte Tür-Steuerung (Barebone)

AXIS A1210-B umfasst alles, was zur Steuerung eines Zugangs erforderlich ist. Die Stromversorgung erfolgt dabei über ein PoE-Kabel. Dieses Produkt ist vollständig in End-to-End-Lösungen von Axis integriert und sowohl für kleine als auch für große Installationen optimiert. Unterstützt wird eine flexible Authentifizierung mit unterschiedlichen Zugangsmodellen. Das kompakte und kostengünstige Barebone-Gerät kann überall installiert werden und gewährleistet eine schnelle und einfache Wandmontage. Durch ihre Stapelbarkeit eignen sich die Geräte außerdem ideal für den Einbau in kleinen Räumen wie z. B. bestehende oder neue Schaltschränke. Integrierte Cybersicherheitsfunktionen verhindern darüber hinaus unbefugte Zugriffe und schützen Ihr System.

- > **Komplette Türsteuerung für einen Zugangspunkt**
- > **Flexible Installationsmöglichkeiten**
- > **Intelligente Edge-Funktionen**
- > **Integrierte Cybersicherheitsfunktionen**
- > **Vollständige Integration in End-to-End-Lösungen von Axis**



# AXIS A1210-B Network Door Controller

## Türcontroller

<b>Lesegeräte</b>	Bis zu 2 OSDP-Leser (Multi-Drop) oder 1 Wiegand-Leser pro Controller Unterstützung von OSDP Secure Channel Integrierbar mit der drahtlosen Schließtechnologie ASSA ABLOY Aperio®.
<b>Türen</b>	Bis zu 16 Funktüren
<b>Anmeldeinformationen</b>	Für bis zu 250.000 lokal gespeicherte Zugangsdaten
<b>Ereignispuffer</b>	Geeignet für bis zu 250.000 lokal gespeicherte Ereignisse

## Power

Stromeingang: 12 V Gleichstrom, max. 36 W oder Power over Ethernet (PoE) IEEE 802.3at, Typ 2 Klasse 4.  
Relais: 1 x Relais NO/NC, max. 2 A Gleichstrom  
Leistungsabgabesperre: 12/24 V, über Steckbrücken konfigurierbar  
Stromversorgung über PoE: max. 900 mA bei 12 V Gleichstrom, max. 450 mA bei 24 V Gleichstrom  
Gleichstromversorgung: max. 1600 mA bei 12 V Gleichstrom, max. 800 mA bei 24 V Gleichstrom  
Stromausgang Leser: 12 V Gleichstrom, max 500 mA  
Gesamtes Leistungsbudget für Peripheriegeräte (Schlösser, Lesegeräte, etc.): 2100 mA bei 12 V über Gleichstrom, 1400 mA bei 12 V über PoE Class 4

## E/A-Schnittstelle

<b>Leser</b>	DC-Ausgang: 12 V, max. 500 mA Daten: OSDP, Wiegand Ein- und Ausgänge: Drei Open-Drain-Ausgänge, max. 30 V, je 100 mA Ein überwachter Eingang
<b>Zugangspunkt</b>	DC-Ausgang: 12/24 V, Brücke konfigurierbar Stromausgang: Siehe Abschnitt „Stromversorgung“ Ein- und Ausgänge: Überwachte REX- und Türpositionssensor-Eingänge Ausgangsrelais: ein Relais, C-Kontakte: 2 A bei 30 V DC, resistiv
<b>Zusatzanschlüsse</b>	DC-Ausgang: 12 V, 50 mA Ein- und Ausgänge: Zwei Ports, konfigurierbare Ein- oder Ausgänge
<b>Extern</b>	Externer manipulationsüberwachter Eingang Überwachter Alarmeingang
<b>Überwachter Eingang</b>	Konfigurierbarer Eingang für Leserschnittstelle, REX-Eingang für Zugangspunkt, Eingang für Türpositionssensor und AUX Programmierbare Abschlusswiderstände, 1 K, 2,2 K, 4,7 K und 10 K, 1 %, 1/4-Watt-Standard Ein unüberwachter Eingang zur Erkennung von Gehäusemanipulationen

## Kabelanforderungen

Kabelquerschnitte für Steckverbinder: CSA: AWG 28–16, CUL/UL: AWG 30–14  
DC-Stromversorgung und Relais: AWG 18-16  
Ethernet und PoE: STP CAT 5e oder höher  
Leserdaten (RS-485): 1 verdrehtes Doppelkabel mit Abschirmung, 120-Ohm-Impedanz, ausgelegt für bis zu 1000 m  
Leserdaten (Wiegand): Für bis zu 150 m ausgelegt  
Stromversorgung des Lesers über den Controller (RS485): AWG 20-16, je nach Spannungs- und Strombereich des Lesers für bis zu 200 m<sup>a</sup>  
Stromversorgung des Lesers über den Controller (Wiegand): AWG 20-16, je nach Spannungs- und Strombereich des Lesers für bis zu 150 m<sup>b</sup>  
E/As als Eingänge: Für bis zu 200 m ausgelegt

## System-on-Chip (SoC)

**Arbeitsspeicher** 512 MB RAM, 2 GB Flash

## Netzwerk

**Netzwerkprotokolle** IPv4, IPv6, HTTP, HTTPS, TLS, QoS Layer 3 DiffServ, SMTP, mDNS (Bonjour), UPnP, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, SOCKS, SSH, MQTT v3.1.1, Syslog

## Systemintegration

<b>Programmierschnittstelle</b>	Offene API zur Integration von Software, einschließlich VAPIX®, Metadaten und AXIS Camera Application Platform (ACAP). Technische Daten auf <a href="https://axis.com/developer-community">axis.com/developer-community</a> . ACAP enthält Native SDK. Anbindung an die Cloud mit einem Klick
<b>Video Management Systeme</b>	Kompatibel mit XIS Camera Station und Video Management Software von Axis Entwicklungspartnern für Anwendungen, auf <a href="https://axis.com/vms">axis.com/vms</a> erhältlich.
<b>Manipulationserkennung</b>	Entfernen der Geräteabdeckung / manipulationsgesicherten Vorderseite Manipulationsgesichertes Lesegerät Neigen, Vibration

## Zulassungen

<b>Produktkennzeichnungen</b>	UL/cUL, KC, EAC, VCCI
<b>Lieferkette</b>	Entspricht TAA
<b>EMV</b>	EN 55035, EN 55032 Klasse B, EN 61000-3-2, EN 61000-3-3 Korea: KC KN32 Klasse B, KC KN35
<b>Sicherheit</b>	IEC/EN/UL 62368-1, IEC/EN 60950-1, UL 2043, UL 294

## Cybersicherheit

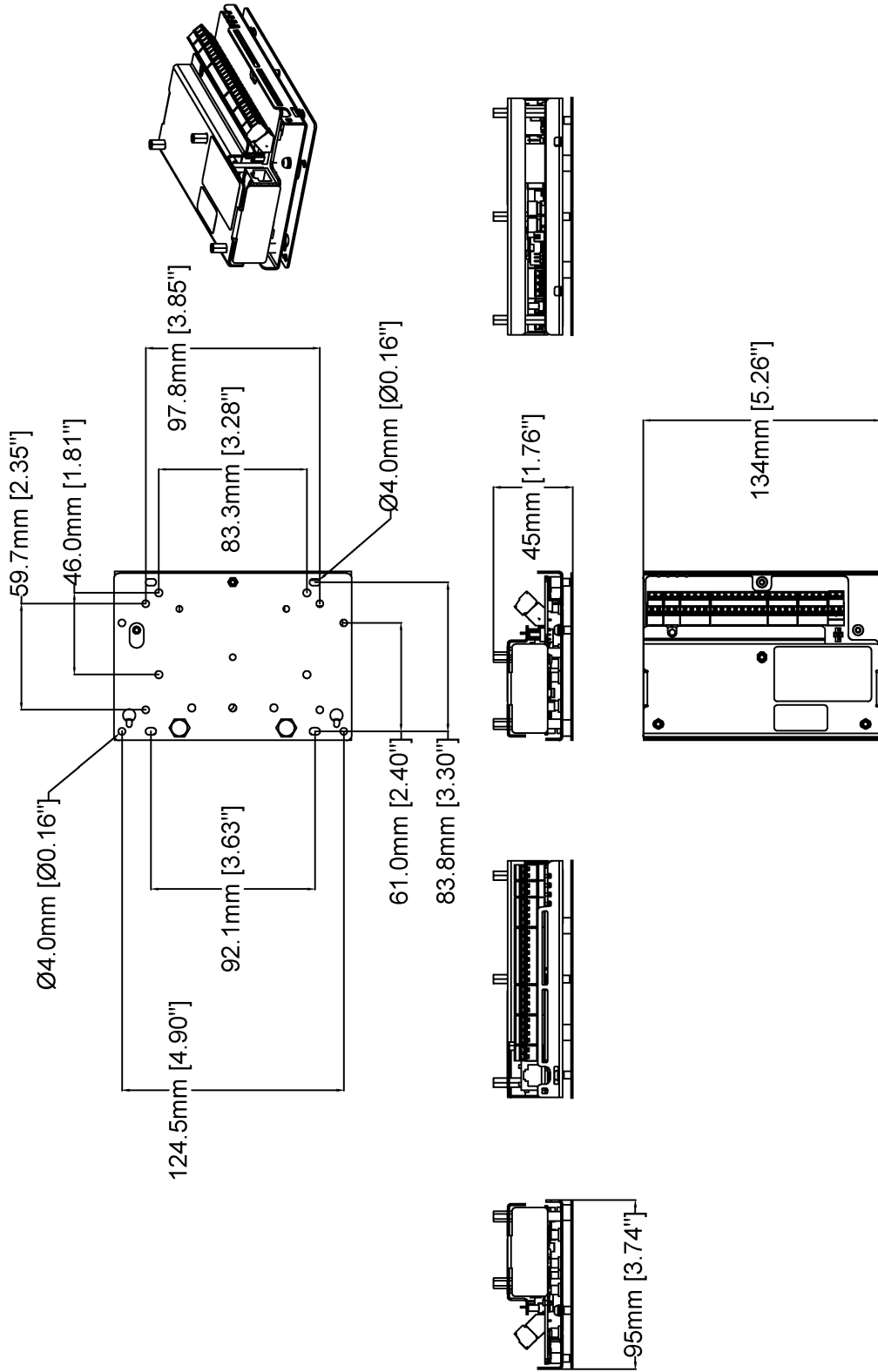
<b>Edge-Sicherheit</b>	Software: Signierte Firmware, Verzögerungsschutz gegen Brute-Force-Angriffe, Digest-Authentifizierung, Kennwortschutz Hardware: Cybersicherheitsplattform Axis Edge Vault Secure Element (CC EAL 6+), sicherer Schlüsselspeicher, sicheres Hochfahren
<b>Netzwerk-Sicherheit</b>	IEEE 802.1X (EAP-TLS) <sup>c</sup> , IEEE 802.1AR, HTTPS/HSTS <sup>c</sup> , TLS v1.2/v1.3 <sup>c</sup> , Network Time Security (NTS), X.509 Certificate PKI, IP-Adressen-Filterung
<b>Dokumentation</b>	<i>AXIS OS Systemhärtungsanleitung</i> <i>Axis Vulnerability Management-Richtlinie</i> <i>Axis Security Development Model</i> Diese Dokumente stehen unter <a href="https://axis.com/support/cybersecurity/resources">axis.com/support/cybersecurity/resources</a> zum Download bereit. Weitere Informationen zum Axis Cybersicherheitsupport finden Sie auf <a href="https://axis.com/cybersecurity">axis.com/cybersecurity</a>

## Allgemein

<b>Gehäuse</b>	Aluminium Farbe: Weiß NCS S 1002-B
<b>Montage</b>	Schaltschrankmontage <sup>d</sup> DIN-Schiennenmontage <sup>d</sup> Stapelmontage <sup>d</sup>
<b>Anschlüsse</b>	Netzwerk: RJ-45 für 10BASE-T/100BASE-TX/1000BASE-T PoE (geschirmt) Ein-/Ausgänge: Anschlussblöcke für Gleichstrom, Ein-/Ausgänge, RS485/Wiegand, Relais. Abnehmbare und farbkodierte Anschlüsse für eine einfache Installation. Kabelquerschnitte für Steckverbinder: CSA: AWG 28-16, CUL/UL: AWG 30-14
<b>Betriebsbedingungen</b>	0 °C bis 70 °C Relative Luftfeuchtigkeit 20 bis 85 % (nicht kondensierend)
<b>Lagerbedingungen</b>	-40 °C bis 70 °C
<b>Abmessungen</b>	Die Abmessungen des gesamten Produkts finden Sie in der Bemaßungszeichnung in diesem Datenblatt.
<b>Gewicht</b>	425 g
<b>Inhalt des Kartons</b>	Türsteuerung, Installationsanleitung, Anschlusset (montiert), Erdungsset, Kabelbinder

<b>Optionales Zubehör</b>	AXIS TA4701 Access Card AXIS TA4702 Key Fob AXIS TA1801 Top Cover AXIS TA1901 DIN Rail Clip AXIS TA1902 Access Control Connector Kit <sup>e</sup> AXIS TQ1808-VE Surveillance Cabinet <sup>e</sup> AXIS 30 W Midspan <sup>e</sup> AXIS 30 W Midspan AC/DC <sup>e</sup> AXIS T8006 PS12 <sup>e</sup> Weiteres Zubehör finden Sie auf <a href="http://axis.com/products/axis-a1210-b">axis.com/products/axis-a1210-b</a>
<b>System-Tools</b>	AXIS Site Designer, AXIS Device Manager, Produkt-Auswahlhilfe, Zubehör-Auswahlhilfe Auf <a href="http://axis.com">axis.com</a> verfügbar
<b>Sprachen</b>	Englisch, Deutsch, Französisch, Spanisch, Italienisch, Russisch, Chinesisch (vereinfacht), Japanisch, Koreanisch, Portugiesisch, Chinesisch (traditionell), Polnisch
<b>Gewährleistung</b>	Informationen zur 5-jährigen Gewährleistungsfrist finden Sie auf <a href="http://axis.com/warranty">axis.com/warranty</a>
<b>Teilenummern</b>	Auf <a href="http://axis.com/products/axis-a1210-b#part-numbers">axis.com/products/axis-a1210-b#part-numbers</a> verfügbar

<b>Nachhaltigkeit</b>	
<b>Substanzkontrollen</b>	PVC-frei, BFR/CFR-frei gemäß JEDEC/ECA JS709 RoHS gemäß RoHS-Richtlinie 2011/65/EU und EN 63000:2018 REACH gemäß Verordnung (EG) Nr. 1907/2006. Informationen zu SCIP UUID finden Sie auf <a href="http://echa.europa.eu">echa.europa.eu</a> .
<b>Materialien</b>	Auf Konfliktmineralien gemäß OECD-Leitfaden überprüft Weitere Informationen zum Thema Nachhaltigkeit bei Axis finden Sie auf <a href="http://axis.com/about-axis/sustainability">axis.com/about-axis/sustainability</a>
<b>Verantwortung für die Umwelt</b>	<a href="http://axis.com/environmental-responsibility">axis.com/environmental-responsibility</a> Axis Communications nimmt am UN Global Compact teil. Weitere Informationen hierzu finden Sie auf <a href="http://unglobalcompact.org">unglobalcompact.org</a>
a. . Mit A4020-E und A4120-E geprüft. b. . c. Dieses Produkt enthält Software, die im Rahmen des OpenSSL-Projekts für die Nutzung innerhalb des OpenSSL-Toolkits entwickelt wurde. ( <a href="http://openssl.org">openssl.org</a> ), sowie von Eric Young ( <a href="mailto:ey@cryptsoft.com">ey@cryptsoft.com</a> ) erstellte kryptografische Software. d. Montage in UL-gelisteten UL 294-Gehäusen mit Sabotagekontakt. e. Nicht für UL 294 geeignet	



Revision	v.01	Revision date	2022-11-16
Paper size	A4	Release date	2022-11-16
Created by	MSS	Scale	1:3

## Hervorgehobene Funktionen

### Axis Edge Vault

Axis Edge Vault ist die hardwarebasierte Cybersicherheitsplattform zum Schutz des Axis Geräts. Sie bildet die Grundlage für alle sicheren Vorgänge und bietet Funktionen zum Schutz der Identität des Geräts, zur Sicherung seiner Integrität ab Werk und zum Schutz vertraulicher Daten vor unbefugtem Zugriff.

Die Herstellung der Root of Trust beginnt bereits beim Hochfahren des Geräts. Bei Axis Geräten wird das Betriebssystem (AXIS OS), von dem das Gerät hochgefahren wird, durch das hardwarebasierte **sichere Hochfahren** überprüft. AXIS OS wiederum wird beim Build-Prozess kryptografisch signiert (**signierte Firmware**). Das sichere Hochfahren und die signierte Firmware greifen ineinander und stellen sicher, dass die Firmware während des gesamten Lebenszyklus des Geräts nicht manipuliert wurde und das Gerät nur von autorisierter Firmware hochgefahren werden kann. Auf diese Weise erhält man eine ununterbrochene Kette von kryptografisch validierter Software für die Vertrauenskette, von der jedweder sicherer Betrieb abhängig ist.

Hinsichtlich der Sicherheit ist der **sichere Schlüsselspeicher** der entscheidende Faktor für den Schutz kryptografischer Daten, die für die sichere Kommunikation (IEEE 802.1X, HTTPS, Axis Geräte-ID, Schlüssel für die Zugriffskontrolle usw.) verwendet werden, vor einem Missbrauch bei Sicherheitsverletzungen. Der sichere Schlüsselspeicher wird über ein gemäß dem Common Criteria und/oder FIPS 140 zertifiziertes, hardwarebasiertes, kryptografisches Rechenmodul bereitgestellt. Je nach Sicherheitsanforderungen kann ein Axis Gerät entweder über ein oder mehrere solcher Module verfügen, wie z. B. ein TPM 2.0 (Trusted Platform Module) oder ein sicheres Element, und/oder eine in ein System-on-Chip (SoC) integrierte Trusted Execution Environment (TEE).

Weitere Informationen zu Axis Edge Vault finden Sie auf [axis.com/solutions/edge-vault](https://axis.com/solutions/edge-vault).

Weitere Informationen finden Sie auf [axis.com/glossary](https://axis.com/glossary)