VIER-TÜREN-ZUTRITTSKONTROLLER — ETHERNET

IDE-DC300

Der IDE-DC300 verwaltet vier Türen und vier Leser mit einem einzigen, per Ethernet angebundenen Controller. Die Feldverdrahtung erfolgt über steckbare Schraubklemmen. Für Installationen, bei denen die Türen an einem gemeinsamen Punkt zusammenlaufen, gibt es ihn im Kunststoffgehäuse oder im Blechschrank mit integriertem Netzteil.

4
TÜREN

4
LESER

40.000
AUSWEISE

200.000
OFFLINE-EREIGNISSE

ZWEI GEHÄUSE, EIN CONTROLLER



150 × 130 × 27 mm

IDE-DC300

Vier-Türen-Zutrittskontroller, Kunststoffgehäuse; ohne Netzteil

GEHÄUSE ABS, UL94-HB	ABMESSUNGEN 150 × 130 × 27 mm
NETZTEIL Nicht enthalten	NETZEINGANG —
MONTAGE Aufputz, Innenbereich	BETRIEBSTEMPERATUR 0 bis +50 °C
LUFTFEUCHTIGKEIT 10–90 % r. F., nicht kondensierend	



300 × 320 × 75 mm

IDE-DC300-S

Vier-Türen-Zutrittskontroller, Metallschrank; integriertes 60-W-Netzteil

GEHÄUSE Blechschrank	ABMESSUNGEN 300 × 320 × 75 mm
NETZTEIL Enthalten, 12 V / 5 A / 60 W	NETZEINGANG 100–260 V AC, 50/60 Hz
MONTAGE Wandmontage, Innenbereich	BETRIEBSTEMPERATUR 0 bis +40 °C
LUFTFEUCHTIGKEIT 20–90 % r. F., nicht kondensierend	

Beide Varianten enthalten dieselbe Controllerelektronik und melden der Verwaltungssoftware denselben Gerätetyp. Das Suffix kennzeichnet Gehäuse und Netzteil. Die Fotos sind annähernd im gleichen Maßstab dargestellt.

WICHTIGE MERKMALE

Vier Türen an einem Controller
Vier Wechslerrelais, vier unabhängige Wiegand-Leserkanäle und sechs getrennte Eingänge bedienen vier Türen. Jede Tür hat einen Ausgang für Leser-LED und Summer. Ein einzelner Controller verringert die Zahl der Netzwerkanschlüsse und der zu konfigurierenden und zu wartenden Geräte.

Schleusenentscheidungen fallen lokal
Die Türschleuse wird im Controller als Teil der Zutrittsentscheidung ausgewertet. Eine Tür kann gesperrt werden, solange eine andere Tür ihrer Schleusengruppe offen ist oder gerade freigegeben wird – ohne Rückfrage beim Server.

Die Zutrittskontrolle läuft bei Netzwerkausfällen weiter

Ausweise, Berechtigungen und Zeitpläne sind im Controller gespeichert. Alle vier Türen treffen auch offline lokale Zutrittsentscheidungen. Der Controller puffert bis zu 200.000 Zutrittsereignisse und sendet sie, sobald die Verbindung zurück ist.

Automatische Erkennung des Kartenformats

Der Controller erkennt unterstützte 26-, 34-, 35- und 37-Bit-Formate, darunter HID H10306, H10304, Corp 1000, Honeywell/Northern und iCLASS. Für HID Prox, Mifare CSN und iCLASS UID stehen Rohwert-Alternativen zur Verfügung. Jeder Leser kann ein anderes unterstütztes Kartenformat verwenden.

Firmware-Updates aus der Ferne mit automatischer Wiederherstellung

Die Verwaltungssoftware kann Firmware auf viele Geräte gleichzeitig verteilen. Updates lassen sich automatisch mit einstellbarem Prüfintervall und Uhrzeit einspielen, damit sie außerhalb der Arbeitszeit installiert werden. Startet die neue Firmware nicht, kehrt der Controller automatisch zur vorherigen funktionierenden Version zurück.

„Warum ging die Tür nicht auf?“ – das Protokoll gibt die Antwort

Wird eine Anfrage abgelehnt, wird der Grund mitgespeichert: Karte unbekannt, fehlende Berechtigung, Versuch außerhalb der erlaubten Zeiten? Beschwerden und Vorfälle lassen sich direkt anhand dieser Einträge klären.

Steckbare Feldklemmen

Die Feldanschlüsse nutzen steckbare Schraubklemmen im Raster 3,5 mm. Jedes Relais hat NC-, COM- und NO-Anschlüsse, jeder Leser einen eigenen sechspoligen Klemmblock. Beim Tausch des Controllers wird der Klemmblock einfach abgezogen, ohne einzelne Adern zu lösen.

Notfreigabe für den ganzen Controller

Ein konfigurierter Eingang kann alle vier Türen für die Flucht freigegeben halten, bis der Eingangszustand endet.

Direkte Systemintegration

Der Controller bietet sowohl einen HTTP-Server als auch einen HTTP-Client. Er kann Live- und gepufferte Zutrittsereignisse an ein externes System senden, oder ein externer Server ruft sie im Abruf-und-Bestätigungs-Verfahren ab. Das veröffentlichte Protokoll enthält exakte Beispielnachrichten und einen lauffähigen Referenzempfänger.

Alarmfunktionen sind im Controller integriert

Ein Bewegungsmelder wird an einen Controllereingang angeschlossen, eine Sirene über einen Controllerausgang angesteuert. Alarmbereiche werden per Karte am Türleser scharf- und unscharfgeschaltet. Keine separate Alarmzentrale, keine Integration zwischen zwei Systemen.

Alle Standorte werden zentral verwaltet

Der Controller baut die gesicherte Verbindung zum Verwaltungsserver selbst auf. Keine feste öffentliche IP, keine Portweiterleitung, kein VPN; Controller in verschiedenen Gebäuden und Städten werden in derselben Oberfläche verwaltet.

TECHNISCHE DATEN

KAPAZITÄT

Ausweise (Karten, PINs und mobil)	40.000
Berechtigungsregeln	5.000
Zeitpläne	5.000
Nutzungsbegrenzte Ausweise	60.000
Speicher für Offline-Zutrittsereignisse	200.000

Karte, PIN und mobiler Ausweis derselben Person zählen als drei Ausweise. Sie teilen sich eine Identität, einen Berechtigungssatz und einen Anti-Passback-Status.

Das Verhalten bei vollem Protokoll ist wählbar. Beim Erhalt der Einträge werden die ältesten nie überschrieben und neue Anfragen abgelehnt; bei Vorrang für den Zutritt überschreiben neue Ereignisse die ältesten. Die erste Option schützt die vorhandene Audit-Historie, die zweite hält den Zutritt offen und protokolliert aktuelle Ereignisse weiter.

Die maximale Anzahl der **Berechtigungen pro Person** ist einstellbar. Höhere Grenzen verringern die Ausweiskapazität wie folgt:

Berechtigungen pro Person	16	32	48	64	128	255
Ausweise	40.000	40.000	29.000	23.000	12.500	6.500

TÜREN, LESER UND E/A

Türen	4
Kartenleser	4 × Wiegand, unabhängige Kanäle
Relaisausgänge	4 × Wechsler (NC / COM / NO), potenzialfreie Kontakte
Max. Schaltspannung	30 V DC
Max. Schaltstrom	5 A
Eingänge	6 × optisch getrennt, für potenzialfreie Kontakte; einstellbare Entprellung
Leserausgänge	8 Ausgänge: 4 × LED- und 4 × Summersteuerung
Integrierter Summer	Ja
Statusanzeige	2 × adressierbare RGB-LEDs
RTC	Bei Stromausfall batteriegepuffert; per NTP synchronisiert

Die Relaiskontakte haben einen Überspannungsschutz und sind für Schlosslasten mit Niederspannung ausgelegt. Das Schalten von Netzspannung wird nicht unterstützt.

FUNKTIONEN DER ZUTRITTSKONTROLLE

Zutrittsentscheidungen fallen im Controller, ohne Rückfrage beim Server.

Türschleuse (Interlock)	Beliebige der vier Türen können eine Schleusengruppe bilden. Der Zutritt an einer Tür wird verweigert, solange ein anderes Gruppenmitglied offen ist oder sich in einem aktiven Freigabezyklus befindet. Die Regel gilt in beide Richtungen.
Mehrpersonen-Freigabe	Innerhalb eines einstellbaren Zeitfensters von 1 Sekunde bis 1 Stunde sind Ausweise von 2–8 verschiedenen berechtigten Personen erforderlich. Lesergruppen lassen sich so einrichten, dass der Eintritt über zwei Leser und der Austritt über einen erfolgt. Das erneute Vorhalten desselben Ausweises zählt nicht.
Anti-Passback	Der Zonenstatus wird direkt zwischen den Controllern abgeglichen, ohne Serververbindung – das ermöglicht globales Anti-Passback am ganzen Standort. Pro Tür einstellbar; hartes und weiches Anti-Passback werden unterstützt.
Brand- und Notfreigabe	Ein konfigurierter Eingang hält alle vier Türen für die Flucht freigegeben, bis der Zustand endet.
Alarmbereiche	Szenarien werden in Bereiche gruppiert. Ein Bereich wird mit einem berechtigten Ausweis scharf- oder unscharfgeschaltet; Bewegung in einem unscharfen Bereich löst nichts aus.
Austrittstaster	Jeder Eingang kann direkt als Austrittstaster konfiguriert werden.
Türkontakt	Nimmt ein Drehsignal eines Drehkreuzes an und erkennt aufgebrochene sowie zu lange offene Türen mit einstellbarer Zeit. Ist kein Türkontakt montiert, steht der Eingang für eine andere Funktion zur Verfügung.
Zeitpläne	Zeitpläne, Feiertage und Datumsbereiche werden im Controller ausgewertet.
Nutzungsbegrenzte Ausweise	Ein Ausweis gilt für eine feste Anzahl von Zutritten, gezählt pro Tür.
Szenario-Engine	Im Controller gespeicherte Regeln, ausgelöst zu festen Zeiten oder durch Eingangszustände, Tür- und Zutrittsereignisse. Ein ausgelöstes Szenario kann ein Relais für eine bestimmte Zeit schalten, den Summer ertönen lassen, ein Relais an einem anderen Controller ansteuern oder ein anderes Szenario scharf- und unscharfschalten.
Detaillierte Zutrittsprotokolle	Bei abgelehntem Zutritt wird der Grund gespeichert: unbekannte Karte, fehlende Berechtigung, Nutzung außerhalb des Zeitplans, verbrauchtes Nutzungskontingent, Anti-Passback-Regel, inaktiver oder abgelaufener Eintrag, falscher Anlagencode, Offline-Zustand, Türschleuse und fehlgeschlagene Authentifizierung. Auch aufgebrochene und zu lange offene Türen sowie die Rückkehr in den Normalzustand werden protokolliert.
Prüfung des Anlagencodes	Pro Leser kann ein zulässiger Anlagencode festgelegt werden. Eine Karte mit abweichendem Code wird abgelehnt; als Grund wird ein falscher Anlagencode protokolliert.
Leser-Rückmeldung	Pro Leser lassen sich eigene LED- und Summermuster für gewährte und abgelehnte Versuche festlegen.

Kartennummernformat	Anlagencode und Kartennummer können als getrennte Felder oder als die auf der Karte aufgedruckte lange Nummer gelesen werden.
Vor der Uhrzeitsynchronisierung	Einstellbares Verhalten, bevor die Uhr synchronisiert ist.
Offline-Verhalten	Einstellbares Verhalten, wenn der Server nicht erreichbar ist.

EINSTELLUNGEN PRO TÜR

Jede Tür ist unabhängig einstellbar: Dauer des Öffnungsimpulses; Relaismodus (Impuls, Umschalten oder Halten); Grund- und Wiederanlaufzustand; vorzeitiges Verriegeln beim Öffnen der Tür; Zählung des Zutritts erst beim Öffnen der Tür; Offenhaltezeit; Anti-Passback-Modus und -Zone; Schleusengruppe; sowie Nutzungszählung.

INTEGRATION UND SCHNITTSTELLEN

Integrierter HTTP-Server	Nimmt direkte HTTP-Befehle an, um eine Tür freizugeben, den Status abzufragen und Einstellungen zu lesen oder zu ändern.
HTTP-Client — Push	Sendet Live- und gepufferte Zutrittsereignisse an einen externen Server, dazu Heartbeats und Eingangstelemetrie.
HTTP-Server — Pull	Ein externer Server kann Ereignisse in getrennten Schritten abrufen und bestätigen.
Verwaltungsprotokoll	MQTT über TLS. Der Controller baut die Verbindung auf; kein offener Port, keine Portweiterleitung, kein VPN nötig.
Serieller Bus	RS-485, Halbduplex; bis 500 kbit/s und 256 Teilnehmer; ±18 kV IEC-ESD.
Außerdem verfügbar	TCP und UDP
Geräteerkennung	mDNS / DNS-SD
Gerätezustand	Laufzeit, Neustartgrund, Prozessortemperatur und Speicherstatus werden gemeldet.
Netzwerk-Rückfall	Wird eine falsche statische IP gesetzt, bleibt der Controller erreichbar; er kehrt zu DHCP zurück.
Dokumentation	Veröffentlichte Protokollspezifikation, exakte Beispielnachrichten und ein lauffähiger Referenzempfänger.

KOMMUNIKATION

Ethernet	10/100, RJ45 mit integriertem Übertrager, geschirmt
WLAN / Bluetooth	Nicht vorhanden — kabelgebundene Installation
Gespeicherte Daten	Im Controller verschlüsselt

STROMVERSORGUNG

Eingang	12–24 V DC
Schutz	Schutz gegen Verpolung, Überspannung und Spannungsspitzen
Leistungsaufnahme Controller	1,0 W typisch, 3,1 W maximal — ca. 80 mA bzw. 260 mA bei 12 V
Leserversorgung	Gleiche Spannung wie der Controllereingang (12–24 V); maximal 250 mA pro Leser
Empfohlenes Netzteil	Mindestens 12 V / 2 A oder 24 V / 2 A
Pufferbatterie	CR1220-Knopfzelle; puffert nur die Echtzeituhr (RTC); versorgt nicht den Controller.

Mit vier Lesern à 250 mA nimmt der Controller bei 12 V etwa 1,26 A auf; deshalb werden mindestens 2 A empfohlen.

Die Relaiskontakte sind potenzialfrei. Das Schloss wird aus einer eigenen Versorgung gespeist und vom Kontakt nur geschaltet; der Schlossstrom ist daher nicht enthalten und muss separat bereitgestellt werden.

Die Variante **IDE-DC300-S** umfasst einen Blechschrank und ein integriertes Netzteil 12 V / 5 A / 60 W (100–260 V AC, 50/60 Hz, 85 % Wirkungsgrad, EN 62368-1).

ANSCHLÜSSE — STECKBARE SCHRAUBKLEMMEN, RASTER 3,5 MM

KLEMME	POLE	SIGNALE
Versorgungseingang	2	IN+, IN−
Relais 1–4	je 3	NC, COM, NO
Leser 1–4	je 6	D0, D1, LED, Summer, IN+, IN−
Eingänge	je 2	IN1–IN2, IN3–IN4, IN5–IN6
RS-485	2	A, B
Ethernet	RJ45	10/100, geschirmt

KABEL UND LÄNGE

VERBINDUNG	KABEL	MAXIMALE LÄNGE
Wiegand-Daten	Geschirmtes, verdrilltes Adernpaar AWG22	150 m
RS-485	Geschirmtes, verdrilltes Adernpaar AWG24 oder stärker; 120-Ω-Abschluss an beiden Enden	1.200 m bei standardmäßig 9.600 Baud; ca. 200 m bei 500 kbit/s
Ethernet	Cat-5e	100 m
Leserversorgung	Die Länge hängt vom Spannungsabfall ab; siehe unten	—

Leserversorgung. Der Leser wird aus der Controllerversorgung gespeist. Die maximale Kabellänge wird durch den Leiterwiderstand begrenzt. Bei 12 V Versorgung und maximal 2 V Spannungsabfall:

LESERSTROM	AWG22	AWG20	AWG18
100 mA	190 m	300 m	475 m
150 mA	125 m	200 m	315 m
250 mA	75 m	120 m	190 m

Prüfen Sie bei langen Strecken sowohl die Daten- als auch die Versorgungsgrenze und verwenden Sie die kürzere Länge. Die Klemmen nehmen Leiter bis AWG16 auf, sodass ein passendes Kabel direkt bis zum Controller geführt werden kann.

MECHANISCHE DATEN UND UMGEBUNGSBEDINGUNGEN

MERKMAL	IDE-DC300	IDE-DC300-S
Gehäuse	ABS, UL94-HB	Blechschrank
Abmessungen	150 × 130 × 27 mm	300 × 320 × 75 mm
Netzteil	Nicht enthalten	Enthalten, 12 V / 5 A / 60 W
Netzeingang	—	100–260 V AC, 50/60 Hz
Montage	Aufputz, Innenbereich	Wandmontage, Innenbereich
Betriebstemperatur	0 bis +50 °C	0 bis +40 °C
Luftfeuchtigkeit	10–90 % r. F., nicht kondensierend	20–90 % r. F., nicht kondensierend
Schutzart	Für den Innenbereich	Für den Innenbereich

Der engere Umgebungsbereich der Variante IDE-DC300-S ergibt sich aus dem integrierten Netzteil.

BESTELLUNG

IDE-DC300	**Vier-Türen-Zutrittskontroller, Kunststoffgehäuse; ohne Netzteil**
IDE-DC300-S	**Vier-Türen-Zutrittskontroller, Metallschrank; integriertes 60-W-Netzteil**

Beide Varianten enthalten dieselbe Controllerelektronik und melden der Verwaltungssoftware denselben Gerätetyp. Das Suffix kennzeichnet Gehäuse und Netzteil.

GARANTIE

Für das Produkt gilt ab Lieferdatum eine Garantie von zwei Jahren auf Material- und Verarbeitungsfehler.

Von dieser Garantie ausgenommen sind:

- Die Pufferbatterie der Echtzeituhr
- Schäden durch Spannungsspitzen, Blitzschlag, Überspannung oder eine Versorgung außerhalb des angegebenen Eingangsbereichs
- Beim IDE-DC300-S das integrierte Netzteil, für das eine separate Herstellergarantie gilt

IDE Smart Teknoloji A.Ş
Bilişim Vadisi Muallimköy Mah. Deniz Cad. No: 143-8 C1 Blok Gebze, Kocaeli, Türkei · info@idesmart.com · +90 (216) 909 0195