Zentrale Ansprechstellen

Siemens Schweiz AG
Building Technologies
Freilagerstrasse 40
8047 Zürich
Schweiz
Tel. +41 585 578 700

Gebäudesicherheit
Siemens Schweiz AG
Building Technologies
Safety Technology
Industriestrasse 22
8604 Volketswil
Schweiz
Tel. +41 585 578 700

Gebäudeautomation
Siemens Schweiz AG
Building Technologies
Comfort Technology
Sennweidstrasse 47
6312 Steinhausen
Schweiz
Tel. +41 585 579 200

HLK/KNX für Systemhäuser und Integratoren, Planer, Wiederverkäufer und OEM
Siemens Schweiz AG
Building Technologies
Control Products & Systems
Sennweidstrasse 47
6312 Steinhausen
Schweiz
Tel. +41 585 579 220

Niederlassung Basel
Duggingerstrasse 23
4153 Reinach
Schweiz
Verkauf
Tel. +41 585 567 111
Service Center
Tel. +41 842 842 013

Niederlassung Bern
Obere Zollgasse 73
3072 Ostermundigen
Schweiz
Verkauf
Tel. +41 585 576 111
Service Center
Tel. +41 842 842 013

Niederlassung Luzern
Platz 3
6039 Root D4
Schweiz
Verkauf
Tel. +41 585 576 565
Service Center
Tel. +41 842 842 013

Niederlassung Tessin
In Tirada 34
6528 Camorino
Schweiz
Verkauf
Tel. +41 585 567 780
Service Center
Tel. +41 842 842 000

Niederlassung Lausanne
Avenue des Baumettes 5
1020 Renens
Schweiz
Verkauf
Tel. +41 585 575 677
Service Center
Tel. +41 842 842 033

Niederlassung Genf
Chemin du Pont-du-Centenaire 109
1228 Plan-les-Ouates
Schweiz
Verkauf
Tel. +41 585 575 100
Service Center
Tel. +41 842 842 033

Niederlassung Zürich
Industriestrasse 22
8604 Volketswil
Schweiz
Verkauf
Gebäudesicherheit
Tel. +41 585 578 900
Gebäudeautomation
Tel. +41 585 578 278
Service Center
Tel. +41 842 842 023

Niederlassung St. Gallen
Industriestrasse 149
9201 Gossau
Schweiz
Verkauf
Tel. +41 585 578 578
Service Center
Tel. +41 842 842 023

Niederlassung Löschung
Dornierstrasse 18
9423 Altenrhein
Schweiz
Verkauf
Tel. +41 585 575 575
Service Center
Tel. +41 842 842 023

Die Informationen in diesem Dokument enthalten allgemeine Beschreibungen der technischen Möglichkeiten, die im Einzelfall nicht immer vorliegen müssen. Die gewünschten Leistungsmerkmale sind daher im Einzelfall bei Vertragsschluss festzulegen. Das Dokument beinhaltet eine allgemeine Produktübersicht. Die Verfügbarkeit kann je nach Land variieren.
Für detaillierte Produktinformationen kontaktieren Sie bitte die lokale Firmenvertretung oder autorisierte Partner.

© Siemens Schweiz AG, 2016 • Bestell-Nr. BT-10863D/CH-AN • Änderungen vorbehalten

SIEMENS

Zutrittskontrolle mit SiPass

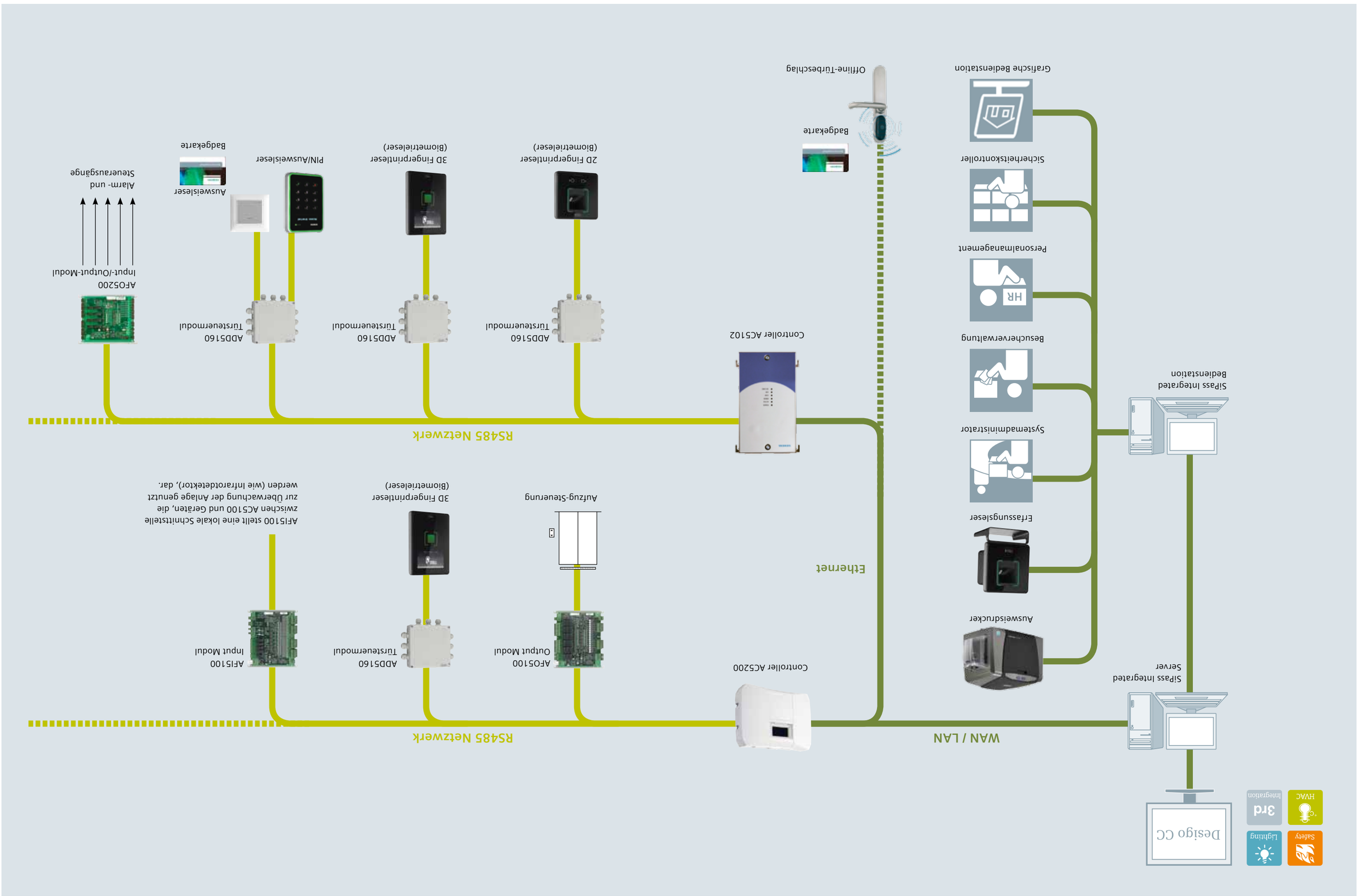
Unsere Welt erfährt Veränderungen, die uns zu einem neuartigen Denken zwingen: demografischer Wandel, Urbanisierung, globale Erwärmung und Ressourcenknappheit. Maximale Effizienz hat deswegen höchste Priorität – und das nicht nur in puncto Energie. Zusätzlich werden wir noch mehr Komfort für das Wohlbefinden der Nutzer schaffen müssen. Auch der Bedarf nach Schutz und Sicherheit wird immer grösser. Für unsere Kunden ist Erfolg dadurch definiert, wie gut sie diese Herausforderungen meistern. Siemens hat die Antworten dazu.

«Wir sind der zuverlässige Technologiepartner für energieeffiziente, sichere und geschützte Gebäude und Infrastruktur.»

www.siemens.ch/zutrittskontrolle

www.siemens.ch/zutrittskontrolle

Zutrittskontrolle – Grafische Übersicht



Zutrittskontrolle

Die Zutrittskontrolle (Zuko) regelt den Zutritt zu Gebäuden oder schützenswerten Bereichen nach den Vorgaben «Wer, wann, wo?» und allenfalls «mit wem?» Ein Zutrittskontrollsystem ist ein elektronisches Hilfsmittel, das für die Zutrittskontrolle verantwortlich ist und automatisch prüft, ob die Berechtigungen einer Person vorhanden sind, um ein bestimmtes Gebäude, einen Bereich oder Raum betreten zu dürfen. Gleichzeitig mit der Zutrittsberechtigung wird auch die Dauer dieser Berechtigung festgelegt. Diese kann also einmalig, zeitlich begrenzt oder unbegrenzt sein. Ein Zutrittskontrollsystem erhöht die Sicherheit erheblich und unterstützt betriebliche Abläufe.

Aufgabe einer Zutrittskontrolle

Ein Zutrittskontrollsystem organisiert den Zutritt über ein vom Betreiber festgelegtes Regelwerk. Dabei werden Berechtigungen nach personenbezogenen, räumlichen und zeitlichen Kriterien zugewiesen. Somit ist es möglich, dass nur Personen Zutritt gewährt wird, die sich mit einem Identifizierungsmerkmal (z. B. mit Karte, Ausweis, PIN-Code oder biometrischen Merkmalen) zu erkennen gegeben haben.

Ziele der Zutrittskontrolle

- Ein Zutrittskontrollsystem gewährt ausschliesslich autorisierten Personen ordnungsgemässen Zutritt
- Es regelt wer, wann, wo und allenfalls mit wem Zutritt hat

Heutige Zutrittskontrollsysteme basieren auf elektronischen, organisatorischen und baulichen Massnahmen. Sie schützen damit Gebäude, Einrichtungen und vor allem Menschen vor Übergriffen und Bedrohungen durch Unbefugte und verhindern Diebstahl von geistigem Eigentum. Die besondere Herausforderung bei der Zutrittskontrolle liegt vor allem darin, Berechtigte so wenig wie möglich in ihrer Bewegungsfreiheit einzuschränken, Unberechtigten aber den Zutritt lückenlos zu verwehren. Somit kommt der Zutrittskontrolle auch eine wichtige präventive Aufgabe zu, indem sie potenzielle Täter abschreckt. Sie verhindert zwar keine Übergriffe von Berechtigten, ermöglicht aber deren Identifizierung im Ereignisfall.

Aufbau eines Zutrittskontrollsystems

Ein System besteht mindestens aus den folgenden drei Komponenten:

- **Sensor:** Der Sensor nimmt die Identifizierung oder Verifizierung des Benutzers auf und übermittelt diese der Zentrale.
- **Aktor:** Sobald eine positive Prüfung in der Zentrale vorliegt, wird der Zutritt freigeschaltet.
- **Zutrittskontrollzentrale:** Die Zentrale prüft ein Zutrittsbegehren nach spezifischen Parametern entweder selbst (Offline-System) oder lässt sich dieses von einer zentralen Kontrollinstanz erst bestätigen (Online-System).

Offline-Zutrittskontrolle

Bei Offline-Lösungen werden die Zutrittsrechte auf die digitalen Türkomponenten oder auf die Identifikationsmedien (Ausweis, Anhänger, Schlüssel) geschrieben.

Offline-Zutrittskontrolle mit Zutrittsrechten auf dem Medium: «Grün» hat seine Berechtigungen am Update-Leser auf sein Medium geladen und aktualisiert, «Rot» nicht.

Zutrittsrechte auf dem ID-Medium

Eine Software verwaltet zentral die Zutrittsrechte und Zeitprofile und schreibt sie mithilfe eines Update-Lesers auf die ID-Medien wie Ausweise, Anhänger etc. Dabei können die Zutrittsrechte verändert und wieder auf die unterschiedlichen Medien geschrieben werden. Geht ein Medium verloren, wird es im System gesperrt. Mit einem Programmer oder einem ID-Medium wird die Sperrung an die Offline-Türkomponente übermittelt.

Vorteile

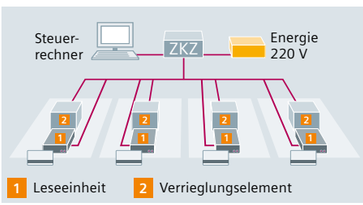
- Keine Verkabelung notwendig
- Geringer Montage- und Installationsaufwand
- Einfaches Nachrüsten von Türen
- Zutrittsrechte werden auf das ID-Medium geschrieben

Nachteile

- Zutrittsrechte sind nicht sofort verfügbar
- Kartensperrungen müssen vor Ort auf die Türkomponenten geladen werden und sind erst dann wirksam

Online-Zutrittskontrolle

Bei Online-Lösungen wird die Entscheidung, ob eine Person Zutritt oder keinen Zutritt erhält, in der Zentrale gefällt. Die Zutrittsrechte liegen meist redundant in der Zentrale sowie auf dem Zutrittsserver. Zutrittskontrollsysteme treten meist in zentraler oder dezentraler Topologie oder in einer Mischform auf.



Zentrale Installation mit Leser und Verriegelungselementen

Zutrittsrechte online bei den Türkomponenten

Eine Software verwaltet zentral die Zutrittsrechte und Zeitprofile und lädt sie über das IT-Netzwerk in die Zentrale. Dies ermöglicht es, Zutrittsrechte online zu ändern und z. B. verlorene Ausweise sofort zu sperren. Alle Türsteuereinheiten und Zutrittsleser sind über ein Bussystem mit der Zentrale vernetzt, wobei sich die Türsteuereinheiten zentral oder dezentral verkabeln lassen.

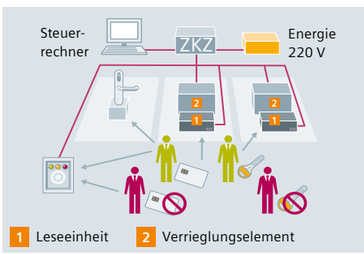
Vorteile

- Zutrittsrechte sofort verfügbar
- Kartensperrungen sofort wirksam
- Zentrale Türüberwachung möglich
- Ereignismeldungen sofort verfügbar

Nachteile

- Verkabelungsaufwand

Heutzutage können moderne Zutrittskontrollsysteme Zutrittsrechte sowohl offline als auch online verwalten. Die Betreiber einer Anlage müssen sich dabei nicht für oder gegen eine Lösung entscheiden, sondern profitieren von den Vorteilen der verschiedenen Varianten.

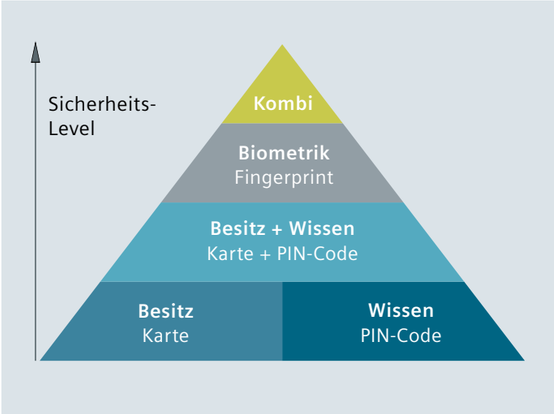


Moderne Zutrittskontrollsysteme mit Online- und Offline-Lösung

Medium

Der Leser, oder aber auch Sensor, übermittelt die erfassten Identifikationsmerkmale eines Benutzers an die Zentrale. Um einen Benutzer identifizieren zu können, muss er sich durch Besitz (einer Karte, eines Tags), durch Wissen (PIN, Kennzahl), personenspezifische Merkmale (Biometrie) oder eine Kombination davon ausweisen. Die unterschiedlichen Verfahren unterliegen dabei einer mehr oder weniger hohen Sicherheitsstufe.

Die Sicherheit eines Zutrittskontrollsystems kann den Anforderungen des Nutzers angepasst werden. Werden nur der Besitz (eines Mediums) oder das Wissen geprüft, ist die Sicherheit tief. Das Medium (z. B. eine Karte) kann einfach weitergegeben oder gestohlen werden. Dasselbe gilt für das Wissen (den PIN-Code), dieses kann einfach ausspioniert oder ebenfalls weitergegeben werden. Wenn die beiden Verfahren aber miteinander kombiniert werden, führt dies zu einer deutlichen Steigerung der Sicherheit. Aber auch hier gilt: Wissen und Besitz sind nicht an eine Person gebunden, die Sicherheit ist also nur so gut, wie der Umgang damit. Die Biometrie schliesslich bietet die höchste Sicherheitsstufe, weil personengebundene Merkmale weder weitergegeben oder ausspioniert noch gefälscht werden können. In diesem Abschnitt wird auf die am häufigsten eingesetzten Medien eingegangen.



Sicherheitsstufen der unterschiedlichen Verfahren

Karte im Kreditkartenformat mit Chip

Schlüsselanhänger und Armband mit RFID-Chip

Die Biometrie bietet die höchste Sicherheitsstufe

SiPass Integrated: Bewegungsfreiheit in aller Sicherheit

SiPass Integrated ist ein leistungsstarkes und nahezu unendlich flexibles Zutrittssystem, das höchste Sicherheit ohne Einschnitte bei Komfort und Anwenderfreundlichkeit bietet. Es ist auch möglich, SiPass Integrated als Sicherheits-Management-Station (SMS) zu nutzen und so Zutrittskontrolle, Einbruchmeldetechnik und Videoüberwachung in einem System zu integrieren.

Mit seiner modularen Struktur fügt sich SiPass Integrated in jede moderne IT-Umgebung ein und ist bei wachsenden Anforderungen schnell und flexibel erweiterbar.

Bereits heute setzen weltweit tausende Unternehmen, Flughäfen, Häfen, Behörden, aber auch Krankenhäuser und Universitäten auf SiPass Integrated von Siemens, wenn verlässliche Zutrittskontrolle gefragt ist.

SiPass Integrated: Komponenten

Hardwarekomponenten

SiPass Integrated lässt sich komplett auf die individuellen Anforderungen der Einrichtung anpassen. So können je nach Bedarf nur Eingänge oder Ein- und Ausgänge (Antipassback) und/oder die Nutzung von Fahrstühlen kontrolliert werden. Gebäudebereiche, in denen ein erhöhter Sicherheitsbedarf besteht, können zusätzlich mit Videoüberwachungstechnologie abgesichert werden.

Ein SiPass-Integrated-System setzt sich aus mehreren verschiedenen Hardwarekomponenten zusammen: Advanced Central Controllers (als ACCs oder ACC-Lites bezeichnet), Türmodule, Signalmodule, Leser und Ausweiskarten. Die automatische Sicherung und Wiederherstellung der Systemdatenbank sorgt für maximale Systemintegrität. Die über den gesamten Übertragungspfad – von der Ausweiskarte bis zum Server – gesicherte Datenübertragung bietet durchgehend hohe Sicherheit.

■ Kontroller

Der «Advanced Central Controller» AC5102 (ACC) und der AC5200 (ACC-Lite) spielen im SiPass-Integrated-System eine entscheidende Rolle, denn sie bilden die Schnittstelle zwischen der SiPass-Integrated-Software und den über das Gebäude verteilten Geräten (Schnittstellenmodule für Ausweisleser, Eingangs- und Ausgangsmodule). Der AC5200 bietet annähernd alle Funktionen des AC5102. Beide Arten von Kontroller können am gleichen Standort, und kombiniert eingesetzt werden. Die Kommunikation zwischen allen Kontrollern im System erfolgt Peer-to-Peer und vom SiPass-Integrated-Server unabhängig. Der grosse Vorteil davon ist, dass das System selbst dann unbeeinträchtigt bleibt, wenn die Verbindung zum Server abreisst.

Der AC5102 wird generell bei grösseren Anlagen verwendet, während sich der AC5200 ideal für kleinere Installationen eignet. Er baut auf der SR35i-Hardware des SiPass-Entro-Systems auf und kann bis zu acht Türen kontrollieren. Das macht den AC5200 zur kostengünstigen Alternative für Zweigstellen und dezentrale, kleine Niederlassungen.

■ Leser und Ausweiskarten

Dank der speziellen Siemens Schnittstelle kann pratisch jeder Standardleser an das SiPass Integrated-System angebunden werden. Unterschiedliche Lesertechnologien können frei untereinander zu einem System kombiniert werden, das auf die individuellen Sicherheitsanforderungen der jeweiligen Einrichtung (einschliesslich Funktionen wie z. B. sichere Anmeldung über PC, Fahrzeugidentifizierung und bargeldlose Bezahlung) massgeschneidert ist.

Biometrische Authentifizierung, z. B. mit 3D und 2D Fingerprint Lesern

Elektronischer Türbeschlag und Zylinder in SiPass integriert

Highlights

- Modulare Systemarchitektur erlaubt massgeschneiderte Anpassung an jeden Bedarf
- Fortschrittliches Identitätsmanagement mit Biometrie-integration und DESFire Verschlüsselung
- Advanced Security Programming (ASP) für automatisierte Sicherheitsabläufe
- Intuitiv gestaltete, benutzer- und verwaltungsfreundliche Software
- Modernes, interaktives Reporting
- Unterstützung von Salto-Offline-Komponenten
- Mit TCP/IP über WAN/LAN in einer bestehenden IT-Umgebung einsetzbar

Kernfunktionen

■ Interaktives Berichts-Tool

Der SiPass-Integrated-Explorer sorgt für schnelle Identifizierung und Einstufung von Ereignissen im System. Die Software umfasst ein Tool zum Erstellen von grafischen Online-Berichten, Datenbankberichten, Vorgangsberichten, parallelen Berichten sowie erweiterte Such- und Filteroptionen und eine Baumansicht, die für eine schnellere Übersicht sorgt. Das System erlaubt es, Berichte auf einen Klick zu erstellen, die Informationsstruktur individuell anzupassen und die Daten nach Bedarf zu sortieren. Es ist ebenfalls möglich, Merklisten zu definieren und so Menschen, die möglicherweise ein Sicherheitsrisiko darstellen, zu überwachen.

■ Erweitertes Alarmmanagement

Das standardisierte Alarmmanagement-System von SiPass Integrated erlaubt es, bis zu 1000 Alarmklassen zu konfigurieren. Um ein schnelleres Reagieren zu ermöglichen, werden alle Alarme entsprechend ihrer Priorität angezeigt und gekennzeichnet. Zur Unterstützung des Sicherheitspersonals können zudem individuelle Anweisungen eingerichtet werden, die im Alarmfall zu befolgen sind.

■ Antipassback und Anwesenheitskontrolle (Roll-call)

Die Aufgabe der Antipassback-Funktion besteht darin zu verhindern, dass ein Ausweis mehrmals genutzt wird, um mehreren Personen Zutritt zu verschaffen. Ist ein Ausweisinhaber als im Antipassback-Bereich anwesend erfasst, ist seine Ausweiskarte für weitere Zutritte zu diesem Bereich gesperrt. Mit der Antipassback-Funktion wird zudem die Anwesenheitskontrolle (Roll-call) möglich, die exakt erfasst, wie viele und welche Mitarbeitende sich zu einem gegebenen Zeitpunkt in einem Bereich aufhalten. Solche Informationen können sich in Notfällen als lebensrettend erweisen. SiPass Integrated umfasst darüber hinaus eine Antipassback-Funktion für Arbeitsgruppen, mit der nach Festlegung eines Antipassback-Bereichs kontrolliert werden kann, wie viele Angehörige einer bestimmten Arbeitsgruppe zum gleichen Zeitpunkt maximal den betreffenden Bereich betreten dürfen. Diese Limitierung kann mit weiteren Zutrittsbeschränkungen zum betreffenden Bereich kombiniert werden.

■ Verwaltung der Ausweisinhaber

Informationen zu einem Ausweisinhaber können in SiPass Integrated sehr einfach hinzugefügt werden. Falls erforderlich können sogar mehrere Ausweise zu einer einzigen Person zugeordnet werden. Die benutzerdefinierte Design-Vorlage erlaubt das Erstellen von einem eigenen Layout mittels Drag-and-drop-Konfiguration und einschliesslich Parameter Einstellung für einzelne Felder und Schaltflächen. Es ist auch möglich, benutzerdefinierte Seiten in XML-Format innerhalb SiPass Integrated-Systemen zu importieren oder exportieren.

■ Türverriegelung

Mit dieser Funktion kann eine Gruppe von Türen definiert und sichergestellt werden, dass keine zweite Tür der anderen Gruppe geöffnet werden kann, solange eine Tür der Gruppe geöffnet ist. So können Personenfallen und Schleusen eingerichtet werden, wie sie besonders in medizinischen und biotechnologischen Einrichtungen, Flughäfen und weiteren sicherheitskritischen Einrichtungen benötigt werden.

■ Schnittstelle zu Videomanagement SiNVR

Diese Schnittstelle ermöglicht die Anbindung von SiPass Integrated an das Siemens Videomanagement System SiNVR und erlaubt die Aufzeichnung der Kamerabilder aufgrund von Zutrittsereignissen.

Zusatzfunktionen

■ Salto-Offline-Komponenten

Mit dieser Funktion können Salto-Offline-Komponenten (Türen) zu einem SiPass-Integrated-System hinzugefügt werden. Zutrittsberechtigungen können sowohl für Online- als auch Offline-Komponenten in der SiPass-Integrated-Software zugeteilt werden.

■ Personalisierte Ausweise und Bildvergleich

Mit dieser Option können erweiterte Sicherheitsmerkmale wie Fotos und Unterschriften erfasst und gespeichert werden.

■ Exportieren von Zeit- und Anwesenheitsdaten

Diese Funktion macht es leicht, alle in SiPass Integrated protokollierten Vorgangsdaten im benötigten Format zu exportieren und in die im Unternehmen genutzte Anwendung für Zeit- und Anwesenheitserfassung zu übernehmen.

■ Aufzugssteuerung

SiPass Integrated bietet zwei Möglichkeiten von Aufzugssteuerung an. Wird die Option Aufzugssteuerung angewendet, wird jedes Stockwerk wie ein normaler Zugangspunkt in SiPass Integrated behandelt, für den eigene Zutrittskontrolloptionen gelten, wie etwa Zeiträume, in denen der Zutritt möglich ist, tägliche Überprüfung des Zutrittscodes, der PIN oder sogar Bildvergleich für maximale Sicherheit.

■ Nachrichtenweiterleitung

Mit der Nachrichtenweiterleitungsoption kann das System individuell festgelegte Texte automatisch an die Pager, Mobiltelefone oder E-Mail-Adressen definierter Beauftragter weiterleiten, wenn ein Sicherheitsverstoss oder sonstige relevante Vorfälle erfasst werden.

■ Personaldatenaustausch (HR-API)

Die Standard-HR-API ermöglicht es, Business-Anwendungen von Drittanbietern mit SiPass Integrated zu kommunizieren und allgemeine Daten auszutauschen. Dies verhindert die Notwendigkeit, identische Daten in mehreren Systemen eingeben zu müssen. Ausweisinhaber- und andere Zutrittskontrolldaten können z. B. über einen Web-Browser oder über ein HR-System gelesen und geändert werden.

■ Grafische Bedienung

Mit der Grafikoption können individuelle grafische Karten erstellt, importiert und aufgebaut werden, in denen Alarmsituationen für Sicherheitspersonal optisch angezeigt werden und der Status sämtlicher Sicherheitspunkte im System auf einen Blick überwacht werden kann.