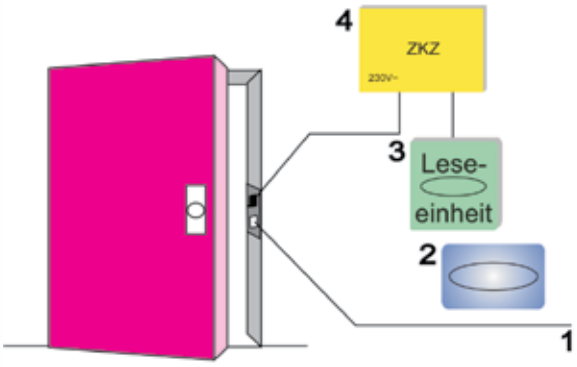
Zutrittssteuerung

Erkennen der Benutzer einer Zutrittssteuerungsanlage

Die grundlegende Aufgabe einer Zutrittssteuerungsanlage besteht darin, zu entscheiden, wer wo und wann in einen durch eine Zutrittssteuerung gesicherten Bereich eintreten darf. Während das **Wo** und **Wann** auf der Einteilung in Raum- und Zeitzonen und damit auf organisatorischen Festlegungen beruht, steht hinter dem **Wer** die Identifikation, d.h. die Erkennung des Benutzers.
Der Sicherheit der Identifikation kommt eine herausragende Bedeutung zu. Sie ist deshalb in der Norm EN 50133-1 „Alarmanlagen, Zutrittskontrollanlagen für Sicherungsanwendungen (DIN VDE 0830-8-1), Teil 1: Systemanforderungen“ ein eigenständiges Kriterium der Sicherheitsklassifizierung. Auch in IEC 60839-11-1 „Elektronische Zutrittskontrollanlagen – Anforderungen an Systeme und Geräte“ ist sie ein wichtiges Kriterium.

Einfaches Zutrittssteuerungssystem



1 Elektrischer Türöffner, Motorschloss, Schranke, Schleuse o. Ä.

2 Ausweis, codierter Schlüssel, Zahlenkombination o. Ä.

3 Ausweisleseeinheit, Tastatur, biometrischer Sensor

4 Zentrale

Mechatronische Produkte vereinen die Funktionen 1, 3 und 4 in einer baulichen Einheit

Im Rahmen von Zutrittssteuerungssystemen kann die Erkennung der Benutzer erfolgen über:

- den Besitz der Person (Ausweis, codierter Schlüssel, Tag, o.ä.)
- das Wissen der Person (PIN-Code: die Persönliche Ident-Nummer)
- die Eigenschaften der Person (Biometrisches Merkmal)

In der Praxis wird häufig der „Besitz“, also ein Ausweis oder ein Transponder eingesetzt, weiter zunehmend gewinnt auch die Biometrie an Bedeutung. Das „Wissen“, also die PIN, wird als alleiniges ID-Mittel in Mitteleuropa in der Zutrittssteuerung nur selten eingesetzt.
Bei erhöhten Sicherheitsanforderungen werden auch Kombinationen aus „Wissen“, „Besitz“ und „Eigenschaften“ verwendet. So ist eine verlorene und noch nicht gesperrte Karte bei der Kombination mit „Wissen“ vom Kartenfinder nicht verwendbar.

Ein biometrisches Erkennungsverfahren, z.B. Fingerabdruck, Handgeometrie, Gesichts-, Venen- oder Iriserkennung, ist das einzige Mittel, den zu einem Ausweis gehörenden Besitzer auf Grund des hinterlegten biometrischen Merkmals zu „erkennen“. Wird ausschließlich ein biometrisches Merkmal verwendet, so handelt es sich um Identifikation - die Person wird durch ein biometrisches Merkmal identifiziert.

Wird vor der biometrischen Erkennung ein ID-Mittel eingelesen oder ein Wissensmerkmal (PIN) eingegeben, handelt es sich um Verifikation.

Heutzutage erkennt ein Zutrittssteuerungssystem in den meisten Fällen das „**Wer**“ aus dem Lesen einer Ausweis-Codierung.

Leseverfahren

Die folgende Darstellung gibt einen Überblick über gängige Leseverfahren, deren Hauptkriterien, Vor- und Nachteile sowie Kombinationen mehrerer Verfahren.

RFID mit passiven Transpondern	
Leseverfahren:	Radio Frequency Identification: Karte oder Transponder/Tag (jeweils ein Chip und eine Antenne in einem ID-Träger) wird durch ein hochfrequentes elektromagnetisches Feld mit Energie versorgt und überträgt Daten, auch bidirektional Weitere Bezeichnungen: berührungslos/Proximity (für Distanzen bis ca. 10 cm), Midrange (für Distanzen > 10 - 30 cm) und Handsfree (Vicinity) (für Distanzen > 30 cm) Diese Systeme werden als Nurlese-Systeme oder auch als Schreib-Lese-Systeme angeboten, wobei das Schreiben/Ändern von Daten auch im Feld erfolgen kann. Es gibt mehrere Verfahren und viele Hersteller (marktführend und mit jeweils mehreren Technologie-Varianten sind: Mifare DESFire EV1, Legic advant® und im außereuropäischen Raum noch i-Class). Drei Generationen von RFID-Chips unterscheiden sich nach Frequenzbereich, Speicherkapazität und insbesondere Sicherheitsmaßnahmen, nämlich • RFID der ersten Generation, meist 125 kHz-Systeme, die über eine werkseitige einmalige Chip-Seriennummer und teilweise über zusätzliche Daten identifiziert werden. Sie besitzen keine Authentifizierung und keine Verschlüsselung auf der Luftstrecke sowie keinen Zugriffsschutz auf den Speicher und weisen relativ kleine Datenmengen auf (ca.100-300 bit). • RFID der zweiten Generation (z. B. Legic prime, Mifare classic; i-Class,Hitag (125 kHz)) – meist 13,56 MHz Systeme, die über geheime Verschlüsselungsverfahren und Zufallszahlen authentifizieren (challenge/response Verfahren) und Zugriffsschlüssel mit speziellen Zugriffsverfahren besitzen. Die Kommunikation auf der Luftstrecke ist verschlüsselt. Die Datenmengen bewegen sich im Kilobit- bzw. unteren Kilobyte-Bereich. • RFID der dritten und jetzt aktuellen Generation (z. B. Legic advant, Mifare DESFire EV1) - meist 13,56 MHz-Systeme neuester Technik. Sie besitzen im Gegensatz zur zweiten Generation anerkannte Kryptoalgorithmen (z.B. AES oder 3DES) und mindestens 128 bit Schlüssellängen und sind somit nach heutigen Erkenntnissen sicher. Die Ablage der Schlüssel in den Lesestationen ist in sogenannten „secure elements“ (SAM) möglich und gilt ebenfalls als sicher. Die Datenmengen können viele Kilobit bzw. mehrere Kilobyte betragen.
Lesedistanz:	Abhängig von der Baugröße der Antenne in Empfänger/Sender i.d.R. 5 - 10 cm, einige Systeme bis über 50 cm, mit Verstärkern/Boostern auch i.d.R. 50 - 150 cm
Lesegeschwindigkeit:	Abhängig vom Verfahren und der Speicherkapazität
Frequenzen:	Überwiegend 125 kHz und 13,56 MHz (ISO/IEC 14443 und 15693)
Speichergröße:	Bis mehrere kByte; hersteller- und verfahrensabhängig Neben flexiblen Schreib-Lese-Systemen sind am Markt auch Nur-Lese-Systeme verfügbar.
Dateninhalt und Speicherorganisation:	Herstellerspezifisch in Bereiche eingeteilt; einige Verfahren sind multiapplikationsfähig, bei anderen wird nur die Unikats- bzw. Seriennummer verwendet

Vorteile:	Lesung erfolgt berührungslos und praktisch verschleißfrei; hoher Bedienkomfort, hohe Lese-Sicherheit; Lesen ist weitgehend lageunabhängig; ID-Mittel sind in verschiedensten Bauformen verfügbar; unempfindlich gegen Feuchtigkeit, Staub, Schmutz, Fremdlicht; bei einigen Verfahren hohe Datenverschlüsselung möglich
Nachteile:	Funktioniert nicht hinter Metall und im Bereich starker Magnetfelder
Kombination mit	kontaktbehafteten Chipkarten, Barcode, Magnetstreifen, Infrarot, Induktiv, ...

RFID mit aktiven Transpondern

Leseverfahren:	Transponder-Karte oder Tag wird durch eine integrierte oder angeschlossene Spannungsquelle mit Energie versorgt und sendet Daten an die Leseeinheit, wenn die Karte/Tag in deren elektromagnetisches Nahfeld kommt Diese Systeme werden meist als Nurlese-Systeme angeboten. Andere Transponder-Bauformen werden vom Benutzer per Taste aktiviert.
Lesedistanz:	I.d.R. einige Meter (Longrange)
Frequenzen:	< 150 kHz, 433 MHz, 868 MHz, 2,45 GHz
Speichergröße:	10 - 20 kByte
Dateninhalt:	Anbieterspezifisch
Vorteile:	Große Reichweite durch aktiven Sender
Nachteile:	Begrenzte Batterielebensdauer; größere Kartenstärke von einigen Millimetern
Kombination mit	passiven RFID-Chips möglich

Biometrie

Leseverfahren:	Unterschiedliche Verfahren: Fingerabdruck, Gesichtserkennung, Handvenenmuster, Iris, ...
Speichergröße:	Keine „Datenträger“ ist die zu identifizierende Person.
Dateninhalt:	Meist höherer Speicherbedarf im Zutrittssteuerungssystem oder auf der Chipkarte, wenn diese als persönlicher Datenträger verwendet wird, jedoch abhängig vom Speicherbedarf des persönlichen Merkmals (Template)
Vorteile:	Höheres Sicherheitsniveau; bei einigen Verfahren kein Ausweis erforderlich; Biometrie wird aber meist als Verifikation betrieben in Verbindung mit Identkarte oder PIN-Code
Nachteile:	Meist höherer Preis; längere Erkennungs-Zeiten möglich; eine 100 % Identifikations- und Verifikationsrate ist systembedingt (wie bei allen Erkennungsverfahren) nicht gegeben
Kombination mit	nahezu allen Leseverfahren möglich Abhängig von der Bauform der Antenne können auch RFID-Verfahren, z.B. Hitag mit Mifare, kombiniert werden.

Verfahren mit heute geringer Bedeutung für die Zutrittssteuerung:

Chipkarte	
Leseverfahren:	Kontaktbehafteter Einsteckleser; statisches Leseverfahren
Speichergröße:	bis mehrere kByte (MByte); read/write
Dateninhalt:	Anbieterspezifisch (bei Mikroprozessor-Chip erfolgt Datenaustausch meist nach ISO 7816-3/4 mit den Protokollen T=0, T=1, früher auch T=14)
Vorteile:	Speicherung größerer Datenmengen; hohes Sicherheitsniveau; Datenverschlüsselung bei Prozessorchips möglich
Nachteile:	Anbieterspezifischer Datenaufbau; kritisch: mechanischer Abrieb/Verschleiß der Kontakte, Kontakte empfindlich gegen Verschmutzung
Kombination mit	Barcode, Magnetstreifen, RFID

Magnetstreifen	
Leseverfahren:	Dynamisch; Einsteck- und Durchzugsleser
Speichergröße:	75, 127, 210 Bit/Inch; read/write
Dateninhalt:	Spur 2: bis 37 numerische Nutzzeichen
Vorteile:	Sehr preisgünstiger Ausweis; weit verbreitet; preisgünstiger Leser
Nachteile:	Empfindlich gegen Magnetfelder, Staub, Schmutz; Code leicht zu ändern, zu verfälschen, zu duplizieren; niedriges Sicherheitsniveau; hoher Verschleiß der Identkarten
Kombination mit	Barcode, Induktiv, Infrarot, Berührungslos, Chipkarten

Barcode	
Leseverfahren:	Optisch (Infrarot-/Rotlicht), dynamisch; als Stift, Durchzugsleser oder Scanner
Speichergröße:	In praktischer Anwendung bis zu 15 Zeichen; read only
Dateninhalt:	Numerisch/alphanumerisch
Vorteile:	Sehr einfach mit Drucker zu erstellen; Ausweis oder Belege sehr preisgünstig; unempfindlich gegen elektromagnetische Felder; Kopierschutz durch Infrarotfolie
Nachteile:	Keine Bedeutung bei Neuentwicklungen
Kombination mit	Magnetstreifen, Induktiv, Infrarot, Berührungslos, Chipkarten

Proprietäre Verfahren, heute ohne Bedeutung:

Wiegand, Infrarot, Induktiv	
Leseverfahren:	Nur lesend
Speichergröße:	Mehrere Zeichen
Dateninhalt:	Interpretation meist anbieterspezifisch
Vorteile:	Individuelle Vorteile; rauer Einsatz
Nachteile:	Praktisch keine Bedeutung mehr bei Neuentwicklungen

Die besondere Bedeutung der RFID-Technologie

Wegen der einfachen Handhabung, des verschleißfreien, zuverlässigen Einsatzes und der großen Flexibilität bevorzugen Anwender heute auf RFID-basierende Identverfahren.

Die verschiedenen Verfahren werden von unterschiedlichen Herstellern angeboten. Alle anerkannten Verfahren funktionieren in der Praxis zuverlässig. Wenn mehr als die Serien-/Unikatsnummer UID eines Ausweises gelesen werden soll, so sind einige wichtige Parameter zu beachten:

Verfahren:

Ist abhängig von individuellen Sicherheitsanforderungen. Die erzielbare Sicherheit lässt sich im Rahmen der technischen Optionen des gewählten RFID-Verfahrens noch variieren durch kryptierte Datenaufzeichnung, Datenübertragung, Zugriffschutz über Schlüssel und ähnliche Mechanismen bis hin zu RFID-Prozessorkarten und eigenen Verschlüsselungs- und Sicherungstechniken.
Einige Verfahren haben bereits weltweite Verbreitung, andere haben ihren Anwendungsschwerpunkt im deutschsprachigen Raum oder in Europa.

Lesen und Schreiben:

Nur Lesen: ausreichend für online-Zutrittssteuerung, Zeiterfassung.
Lesen/Schreiben: für Bezahl- Dienste, Produktverfolgung, komplexe online- und offline-Zutrittssteuerung mit dynamischen/temporären Zutrittsrechten für die offline-Terminals auf dem Ausweis oder biometrischen Daten bzw. Templates auf der Karte.

Antikollision:

Bedeutung: mehrere Karten befinden sich gleichzeitig im elektromagnetischen Empfangsfeld. Sie werden automatisch sequenziell gelesen.

Normen:

- ISO 14443 (Proximity Card, < 10cm): beschreibt die physikalischen Charakteristika (Abmessung [nur referenziert, da sie in anderen Normen festgelegt ist], Frequenz, Initialisierung, Antikollision, Übertragungsprotokoll) sowie den Einsatz von Shortrange-Ident-Karten
- ISO 15693, (Vicinity Card, < 1,5m), entsprechend für Vicinity Cards
- ISO 18000, Referenz-Architektur für alle Frequenzen (135 kHz - 5,8 GHz) speziell für den Einsatz von RFID in der Logistik

Zusammenfassung

- Der zuverlässigen, sicheren und schnellen Identifikation der Benutzer einer Zutrittssteuerung kommt eine herausragende Bedeutung zu. Besonders auf eine ergonomisch gute Bedienung des Systems ist zu achten, um bereits mit der Systemeinführung die Akzeptanz der Anwender zu gewinnen.
- Relevante Kriterien bei dem ausgewählten Lese-/Identifikationsverfahren sind u.a. Flexibilität, Verschleiß/Haltbarkeit, Sicherheit, einfache Handhabung und der Gesamtaufwand zur Erstellung und logistischen Betreuung der Ausweise über einen i.d.R. längeren Zeitraum.
- Das gebräuchlichste Identifikationsmittel (ID-Mittel) im Bereich der professionellen Zutrittssteuerung ist der Ausweis. Zunehmend werden Transponder (z.B. als Schlüsselanhänger) in unterschiedlichen Bauformen genutzt, die sich durch ihre Robustheit auszeichnen. Allerdings ist dabei die reduzierte Lesedistanz (< 5 cm) und geringe äußere Beschriftungsmöglichkeit zu beachten.
  Die Karte wird, besonders als berührungsloser RFID-Ausweis bzw. als -Smartcard, auch in Zukunft eine führende Rolle spielen. Die meisten anderen Verfahren werden nur dort eingesetzt, wo besondere Umweltbedingungen oder Projekt-Kriterien vorliegen.

- Durch die Kombination mehrerer Codierungen auf einer Karte, werden die Eigenschaften, Funktionen und Einsatzmöglichkeiten dieser verschiedenen Technologien vereint. So können die unterschiedlichsten kartengesteuerten Anwendungen, z.B. Zutrittskontrolle, Zeit- und Kantinendatenerfassung, auf einem Mitarbeiterausweis vereint werden, um dem Bediener mehrere ID-Träger in seinem Betrieb zu ersparen. Solche Kombinationsmöglichkeiten sind unbedingt mit dem Geräte- und Kartenhersteller zu klären.

- Biometrische Verfahren werden verwendet, wenn aufgrund der Sicherheitsanforderungen die Erkennung eines Ausweises allein nicht ausreicht, sondern der Benutzer selbst mit seiner Karte authentifiziert werden soll. Hier dient die Biometrie als Erkennungsverfahren für den Benutzer - statt für dessen „Sekundär-ID-Mittel“.
- Wie bereits erwähnt, wird ein PIN-Code als alleiniges ID-Mittel in Deutschland kaum eingesetzt. Ein PIN-Code als geistiges Merkmal in Verbindung mit einer Karte kommt dagegen häufiger bei Verifikation zum Einsatz.

BHE - Feldstraße 28 **Telefon: 06386 9214-0** **Internet: www.bhe.de**
66904 Brücken **Telefax: 06386 9214-99** **E-Mail: info@bhe.de**