Zutrittskontrolle – ein lohnender Einstieg

H. Petereins, Berlin

Zutrittskontrollsysteme haben sich in letzter Zeit wie kein anderes Sicherheitssystem eine breite Akzeptanz erworben. Mit noch umfassenderen Funktionen und Identifikationskriterien setzt sich dieser Trend fort. Der Beitrag beschreibt den gegenwärtigen Stand der technischen Entwicklung. Er stellt wesentliche Grundlagen vor und erleichtert den Einstieg in diese Thematik.

Marktchancen durch Rationalisierungspotential

Zutrittskontrolle ist heute mehr als nur ein „Pförtner-Ersatz“. Sie ist eine Komponente der Sicherheitstechnik, die durch ihre verschiedensten Identifikationsmerkmalträger (ID-Karte) universell einsetzbar ist. Es sind Kombinationen mit Einbruchmeldeanlagen, Zeiterfassungssystemen, Betriebsdatenerfassung, innerbetrieblichem Zahlungsverkehr in Kantinen oder der Steuerung von Parkplätzen und Tiefgaragen möglich.

Ob als Einzellösung oder als vernetztes System – Zutrittskontrolle stellt ein wirksames Mittel zur Erhöhung der Sicherheit dar. Verbunden mit der rasanten Hard- und Softwareentwicklung gibt es immer komplexere Anwendungen und völlig neue, z. B. biometrische, Identifikationsmöglichkeiten. Die Einsatzgebiete für Zutrittskontrollsysteme sind vielfältig:

– Außenbereichsabsicherung
– Parkplätze und Tiefgaragen
– Eingangsbereiche von Banken und Geschäftshäusern, Behörden und Verwaltungen
– Objekte mit erhöhtem Sicherheitsbedarf, z. B. Rechenzentren, Forschungseinrichtungen, Flughäfen und Atomkraftwerke
– Sport- und Veranstaltungsstätten

In Parkhäusern oder Tiefgaragen ermöglichen sie eine ungehinderte Ein- und Ausfahrt, in Sportstätten gewährleisten sie zusammen mit Personenvereinzelungsanlagen (z.B. Drehkreuzen) den sicheren und kontrollierten Zugang vieler Menschen. Durch den kontrollierten Zugang lassen sich auch aktuelle Besucherzahlen generieren. So kann gerade auf Großveranstaltungen bei Gefahrensituationen gezielt gehandelt werden. Neben der erheblichen Einsparung von Personal geben die anfallenden Daten für den jeweiligen Betreiber Auskunft über Auslastung seiner Einrichtungen sowie andere interessante Informationen für die innerbetriebliche Organisation. Dabei werden immer mehr berührungslose ID-Karten und Chip-ID-Karten eingesetzt. Sie bestimmen heute mit ca. 80 Prozent bei neu errichteten Zutrittskontrollsystemen das Erscheinungsbild.

Die Analysten Frost & Sullivan in London prognostizierten 1999 dem Teilmarkt Zutrittskontrolle in Deutschland eine durchschnittliche Wachstumsrate von jährlich rund 5,7 Prozent bis zum Jahr 2005. Dabei wird betont, dass der Markt für Zutrittskontrollsysteme in Deutschland seine volle Reife noch nicht erreicht hat.

Autor

Dipl.-Ing. *Harald Petereins* ist Geschäftsführer des Ingenieurbüros für Sicherheitstechnik Petereins in Berlin.

Komponenten eines Zutrittskontrollsystems

Das Zutrittskontrollsystem besteht im einfachsten Fall aus:

- Steuereinheit, als Schaltzentrale mit entsprechender Intelligenz direkt vor Ort und der dazu notwendigen Software
- ein oder mehrere Leser, angeschlossen an die Steuereinheit
- elektromechanische Sperr-, Verriegelungs- oder Öffnungseinrichtungen für jede Tür
- Alarmgeber für die Signalisierung
- Stromversorgung, meistens mit Akku für Netzausfall sowie einer Stützbatterie gegen Datenverlust bei Netzausfall

Bei einer Vernetzung mit weiteren Steuereinheiten kommen die entsprechenden Schnittstellen für die Datenübertragung sowie eine Zentraleinheit für die Steuerung des Gesamtsystems mit Bedien- und Überwachungsfunktionen hinzu. Die Zentraleinheit verfügt über entsprechende Speichermöglichkeiten, Bedien- und Anzeigeeinheiten sowie einen Druckeranschluss.

Die Einzellösung

Die Zutrittskontrolle als Einzellösung besteht meistens aus einer Steuereinheit (Controller) und ein oder zwei Lesern sowie den notwendigen Steuerausgängen für die elektromechanischen Sperr- oder Öffnungselemente der Eingangstüren. Im einfachsten Fall verfügt der Controller über einen Speicher für eine bestimmte Anzahl von ID-Karten, welche mit einer sogenannten Masterkarte eingelesen werden können. Solche Systeme verfügen meistens über keinen Speicher für Ereignisse, d.h. alle Ereignisse werden nicht protokolliert und sind als ein wesentlicher Nachteil nicht nachvollziehbar.

Ein weiterer Nachteil besteht darin, dass bei Verlust einer ID-Karte der Speicher gelöscht werden muss. Alle Karten müssen dann neu eingelesen werden. Solche Systeme sind heute veraltet und werden nur noch als einfache Zugangsvariante (z. B. für Parkplätze) eingesetzt. Bei diesen einfachen Lösungen findet man den Leser und den Controller oft als eine Einheit, d.h. in einem Gehäuse, vor. Diese Lösung ist zwar praktisch, bietet aber – da sich Leser und Controller auf der Außenseite befinden – Möglichkeiten zur Manipulation.

Eine Einzellösung sollte heute mindestens nachfolgende Forderungen erfüllen:

- Aufnehmen und Überprüfen der elektronischen Signale der Leser beim Erkennen einer ID-Karte
- Steuern der elektromechanischen Einrichtungen an der Tür, z. B. Elektrotüröffner, Sperrelemente, Motorriegelschlösser, Haftmagnete sowie Schranken bzw. Drehkreuze
- Überwachen der Tür auf Verschluss und der Öffnungsvorgänge
- Signalisierung von Störungen und Alarmen sowie Manipulationsversuchen

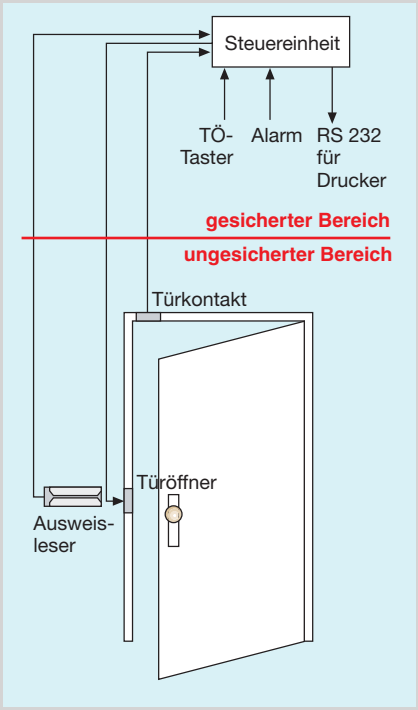
Eine Einzellösung verfügt über einen Controller, der für mehrere hundert ID-Karten geeignet ist und optional erweiterbar ist. Ein sogenannter Buchungspuffer, welcher die letzten 1000 bis 2000 Ereignisse speichert, eine Schnittstelle für den Anschluss eines Laptop zur Programmierung und zum Auslesen des Buchungspuffers sowie Schnittstellen für die Verriegelung und die Freigabe der Türen gehören dazu.

Über diese Schnittstellen gibt der Controller bei richtiger Identifikation den Zugang frei und überwacht bei geschlossener Tür diese auf unberechtigtes Öffnen. Bei unberechtigtem Öffnen der Tür kann der Controller einen Signalgeber zur Alarmierung ansteuern. Weitere Funktionen der Einzellösung können die optionale Nachrüstung mit freiprogrammierbaren Relaiskarten, eine Zutrittswiederholsperre sowie die 2-Personen-Zutrittskontrolle (Vieraugenprinzip) sein.

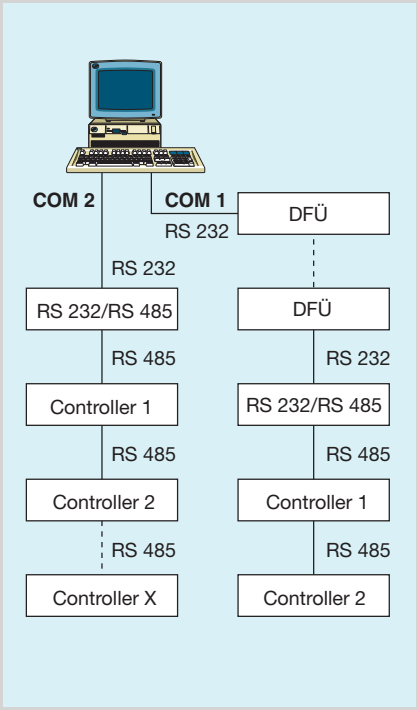
Eine Programmierung der Zutrittszeiten und der Türfreigabezeiten ist bei den meisten Controllern ebenso möglich wie die Programmierung von Sonn- und Feiertagen zur Einschränkung der Zutrittsmöglichkeit.

Eine Einzellösung muss auch bei Stromaus-

fall sicher funktionieren. Die meisten Hersteller bieten für ihre Systeme dazu ein entsprechendes Netzteil mit einem Akku an. Auch der Einsatz einer geeigneten USV ist möglich. Bild ❶ zeigt ein einfaches Beispiel für eine Einzellösung.



❶ **Einfache Zutrittskontrollsystemlösung an der Außenseite des Bereiches und Steueinheit auf der Innenseite des Bereiches (geschützter Bereich)**



❷ **Beispiel für ein vernetztes Zutrittskontrollsystem mit Leitstellenrechner, abgesetzte Steuereinheiten (Controllern) über ein DFÜ und lokalen Steuereinheiten (Controllern)**

Vernetzte Systeme

Vernetzte Systeme bestehen aus mehreren Steuereinheiten (Controllern) und einem PC-System, welche mit verschiedenen Bussystemen oder mittels DFÜ miteinander verbunden sein können (Bild ❷). An diese Controller können je nach Fabrikat und Typ mehrere Leser angeschlossen werden. Es kann jedoch nur immer ein Fabrikat verwendet werden, da die Hersteller ihre eigenen Protokolle und Übertragungssysteme verwenden, die untereinander nicht kompatibel sind. Die Controller stellen ein voll intelligentes Zutrittskontrollsystem dar, was bei Ausfall der Busverbindung, des PC-Systems oder bei einem abgesetzten System voll funktionsfähig bleibt. Nach erneuter Herstellung der Verbindung über das Bussystem oder bei einem abgesetzten System mittels DFÜ werden die Daten zum PC-System übertragen. Der Controller sollte folgende Anforderungen erfüllen:

- Intelligentes Zutrittskontrollsystem für XX (z. B. 6) Türen mit Software
- Speicher für XXX (z. B. 300) Personen und die zugeordneten ID-Karten sowie ggf. PIN-Code
- Buchungsspeicher für mindestens 2000 Ereignisse
- Steuerfunktionen für Türsteuerung sowie für Störung und Alarm
- DFÜ-Schnittstelle (optional)
- Druckerschnittstelle (optional)
- Hostschnittstelle
- Zutrittswiederholsperre
- Möglichkeit der 2-Personen-Zutrittskontrolle
- erweiterbar mit freiprogrammierbaren Relaiskarten

Das PC-System hat die Aufgabe, alle Daten des Systems zu verwalten und die entsprechenden Berechtigungen für die einzelnen ID-Karten zu vergeben. Darüber hinaus muss es die einzelnen Ereignisse (Buchungen) an allen Lesern registrieren und auswerten sowie die entsprechenden Steuerungen tätigen. Bei einem vernetzten System können vom PC-System als übergeordnete Zentrale alle Eigenschaften und Berechtigungen programmiert und verändert werden. Der Verlust einer ID-Karte oder die Änderung einer Berechtigung ist so unkompliziert und schnell möglich.

Das PC-System ermöglicht auch die Erweiterung des Zutrittskontrollsystems. Mit geeigneten Softwaremodulen ist eine Erweiterung zur Zeiterfassung, Betriebsdatenerfassung und zum innerbetrieblichen Abrechnungssystem möglich. Mittels dafür vorhandener Schnittstellen in der Software kann eine Übergabe der Daten an andere Programme erfolgen. Der Hardwareaufwand besteht für diese Anwendungen meistens nur im Austausch der jeweiligen einfachen Leser gegen Leser mit Tastatur bzw. gegen ein entsprechendes Terminal.

Die Software für das PC-System besteht je nach Hersteller aus einzelnen Modulen. Ein Grundmodul ermöglicht je nach System die Verwaltung von 200 bis 500 Personen mit den dazu gehörigen ID-Karten. Für eine Erweiterung der Personenanzahl müssen entsprechende Module käuflich erworben werden. Für die effektive Verwaltung der Daten ist eine entsprechende Datenbank (ORACLE, IBM DB2, Access o.ä.) und ein entsprechendes Betriebssystem, meistens Windows 95/98, Windows NT oder UNIX erforderlich.

Als Schnittstellen zwischen PC-System und Controllern werden verwendet:

- RS 232
  Leitungslänge: 15 bzw. 30 Meter
  Kabeltyp: LiCY 3 x 01,14 mm^2
- RS 485
  Leitungslänge: ca. 1500 Meter
  Kabeltyp: LifYCY 3 x 2 x 0,20 mm^2
  oder LiYCY-CY 3 x 2 x 0,25 mm^2
  meist max. 32 Geräte bei einem Bussystem, unbedingt paarig verseiltes Kabel verwenden
- Current-Loop
  Leitungslänge: ca. 2000 Meter
  Kabeltyp: LifYCY 2 x 2 x 0,20 mm^2
  oder LiYCY-CY 2 x 2 x 0,25 mm^2
  oder JY(St)Y 2 x 2 x 0,6 mm^2

ID-Karten und Ausweisleser

Jede ID-Karte ist mit einer lesbaren und auswertbaren Information in Form einer Codierung versehen. Diese Information wird auch als Identifikationsmerkmal und die ID-Karte als Identifikationsmerkmalträger bezeichnet. Als Identifikationsmerkmale werden eingesetzt:

– Magnetstreifen
– Induktionsprinzip
– Infrarotprinzip
– Wiegand-Prinzip
– berührungslos
– integrierter Microchip.

Im Folgenden werden die einzelnen Kartensysteme detailiert erläutert.

Magnetkarten und -kartenleser

Magnetkarten sind durch entsprechende DIN-Vorschriften (DIN 9781 und DIN 9785) hinsichtlich ihrer Maße und der Anordnung des Magnetstreifens auf der Karte genormt. Durch die Nutzung als Geld- und Kreditkarten sind sie weit verbreitet. Der Magnetstreifen ist in drei Spuren aufgeteilt und enthält je nach Nutzer und Hersteller

entsprechende Daten. Die Codierung der Magnetkarten erfolgt mit einem speziellen Codiergerät. Magnetkarten gibt es bezüglich der Magnetisierbarkeit des Magnetstreifens in zwei Ausführungen. Man unterscheidet zwischen HICO (high-energy) mit 4000 Oersted und LOCO mit 300 Oersted. Magnetkartenleser besitzen einen Magnetlesekopf und eine entsprechende Leseelektronik.
Bei den meisten Systemen wird nur eine Spur gelesen und ausgewertet (z. B. Spur 2). Für spezielle Zutrittskontrollsysteme bzw. Anwendungen (Banksysteme) werden auch Zweispurleser mit entsprechenden Leseköpfen und entsprechender Leseelektronik eingesetzt. Beim Lesen der Magnetkarte hat der Magnetlesekopf direkten Kontakt mit der Magnetkarte. Dies führt durch entsprechende Umwelteinflüsse zu einer Verschmutzung des Magnetlesekopfes (Staub, Schmutz, Fett, Öl) und erfordert eine Pflege und Wartung des Lesekopfes. Der Magnetstreifen der Karte muss vor mechanischer Beschädigung geschützt werden und von starken elektromagnetischen Feldern ferngehalten werden. Magnetkarten können einseitig bedruckt werden und sind so, versehen mit entsprechenden Daten, auch als Betriebsausweis u.ä. kombiniert verwendbar.
Magnetkartenleser gibt es in den Varianten
– Durchzugsleser
– Einsteckleser
– Motoreinzugsleser
als Aufputz- oder auch als Unterputzvariante.

Induktivkarten und -kartenleser
Induktivkarten bestehen aus einem Kunststoffträgermaterial, in dem sich eine Kupferfolie mit entsprechenden Lochungen befindet, die über die gesamte Fläche angeordnet sind. Diese Codierung ist statisch und kann nicht verändert werden. Induktivkarten sind mechanisch sehr stabil und erfüllen hohe mechanische Anforderungen. Durch ihren Aufbau ist die Induktivkarte strapazierfähig und unempfindlich gegen Öl, Benzin und normalem Staub. Eine Verschmutzung der Induktivkarte hat keinen Einfluss auf den Lesevorgang. Durch die innen liegende Kupferfolie mit ihrer Codierung ist die Induktivkarte von beiden Seiten bedruckbar und als Betriebsausweis mit Foto o. ä. nutzbar. Da bei der Induktivkarte die Codierung auf der ganzen Karte symetrisch angeordnet ist, kann die Karte in jeder Lage in den Leser eingesteckt werden. Induktivleser gibt es nur als Einsteckleser. Die Induktivkarte wird im Ruhezustand im Induktivleser gelesen.

Infrarotkarten und -kartenleser
Infrarotkarten bestehen aus einem Kunststoffträgermaterial, in das ein Codeträger aus Papier integriert ist. Das Leseverfahren basiert auf der Auswertung von Hell-Dunkel-Unterschieden mittels einer Infrarotlichtquelle in einem vorgegebenen Rasterbereich. Infrarotkarten sind empfindlich in ihrem Leseverhalten gegen Staub, Schmutz, Öl und Fett. Infrarotkarten können nur teilweise bedruckt werden. Der Teil der Infrarotkarte, in welchem sich die Codierung befindet, darf nicht bedruckt werden. Infrarotkartenleser gibt es als Einsteckleser, Durchzugsleser und Motoreinzugsleser. Im Infrarotkartenleser befinden sich IR-Lichtschranken, welche die Codierung beim Lesevorgang erkennen und auslesen.

Wiegandkarten und -kartenleser
Die Codierung der Wiegandkarten besteht aus einer Anordnung von Drahtstücken einer speziellen Legierung. Die Drahtstücken sind ca. 7 mm lang und werden nach einem speziellen Verfahren magnetisiert. Die Codierung ist statisch und nicht veränderbar. Die Wiegandkarte ist mechanisch sehr stabil und kann durch den Einsatz spezieller Kunststoffe sehr biegefest und praktisch bruchsicher gestaltet werden. Den Wiegandkartenleser gibt es nur als Durchzugsleser, wobei der Lesekopf durch sein magnetisches Prinzip gegen Schmutz, Öl u.a. relativ unempfindlich ist. Der Lesekopf hat beim Lesen keinen Kontakt zur Karte.

Berührungslose Karten und Kartenleser
Berührungslose Karten besitzen eine Empfangsantenne und eine Elektronik (Chip), die in das Kunststoffträgermaterial eingebettet sind (Passivkarte). Berührungslose Karten gibt es im Scheckkartenformat und als Schlüsselanhänger. Die Lesedistanz wird von der Antennengröße des Lesers (Sender) bestimmt.
Der Gestaltung der Karten und der Schlüsselanhänger sind keine Grenzen gesetzt, da die äußere Form für den berührungslosen Lesevorgang unerheblich sind.
Ein berührungsloser Kartenleser besitzt eine Sendeantenne, welche unterschiedliche Frequenzen sendet. Diese Aussendungen werden von den Karten oder Schlüsselanhängern in einem entsprechenden Abstand (Leseabstand) gedämpft und führen dabei zur Kartenidentifikation. Der Durchmesser der Sendeantenne entspricht ca. dem Leseabstand. Für große Lesereichweiten werden die Antennen der Leser auf geeignete Flächen aufgebracht oder im Mauerwerk eingelassen.
Da die Hersteller für ihre berührungslosen Karten unterschiedliche Codierungen und Frequenzen benutzen, sind diese untereinander nicht kompatibel. Ein bestehendes System kann daher im Regelfall nur durch Komponenten des gleichen Herstellers erweitert werden. Für spezielle Anwendungsfälle gibt es berührungslose Karten mit eigener Energiequelle (Batterie). Diese Aktivkarten verfügen über eine größere Lesereichweite.

Chipkarten und -kartenleser

Chipkarten im Scheckkartenformat besitzen einen Prozessorchip. Dieser Chip kann entweder nur als Träger von Identifikationsmerkmalen dienen oder aber als statischer Speicher die Identifikationsmerkmale speichern und multifunktional mit Daten beschrieben werden.
Anwendungsbeispiele, die jeder kennt, sind heute die Krankenkassenkarte, die Telefonkarte oder die aufladbare Geldkarte. Die Chipkartenleser haben einen ähnlichen Aufbau wie die Magnetkartenleser, nur das der Lese- bzw. Schreibprozess über Kontakte erfolgt.
Chipkartenleser arbeiten mit einer Clock-Data Schnittstelle. Es gibt sie als Einsteckleser und in einigen Anwendungsfällen als Einzugsleser. Chipkartenleser sind genau wie Magnetkartenleser empfindlich gegen Staub, Schmutz, Öl und Fett, da diese Stoffe den sicheren Kontakt zwischen Leser und Chip beeinflussen können.

Biometrische Identifikation

In den letzten zwei bis drei Jahren hat sich die biometrische Identifizierung enorm entwickelt. Obwohl biometrische Identifikationssysteme heute noch um Größenordnungen teurer als herkömmliche ID-Karten und Leser sind, scheint ihnen die Zukunft zu gehören. Die Vorteile sind einfach zu groß. So können zum Unterschied zu ID-Karten oder schlüsselbasierten Systemen die Merkmale weder verloren gehen, noch von anderen Personen entwendet werden. Die Merkmale sind einer Person permanent zugeordnet und eindeutig. Die meisten zur Identifizierung herangezogenen Merkmale sind beständig, d.h. sie ändern sich auch mit der natürlichen menschlichen Alterung nicht und sind somit über die gesamte Lebensdauer vorhanden. Je nach Art des zur Identifizierung heran gezogenen Merkmals ist die Fälschungssicherheit sehr hoch oder aber ein Missbrauch mit einem sehr hohen Aufwand verbunden.
Die Nachteile der biometrischen Systeme sind die schon erwähnten hohen Beschaffungskosten und der größere Aufwand an Technik vor Ort. Auch sollte der Persönlichkeitsschutz in diesem Zusammenhang nicht unbeachtet bleiben. Bestimmte biometrische Merkmale können nicht nur der Verifikation dienen, sondern eignen sich auch zur eindeutigen Identifikation einer Person und lassen sich ggf. gegen den Willen der Person missbrauchen. Auch hygie-

nische Bedenken und Einwände wurden schon mit Erfolg gegen den Einsatz solcher Systeme geltend gemacht.
Im Folgenden werden die bekannten biometrischen Identifikationen vorgestellt.

Gesichtserkennung
Zur Gesichtserkennung gibt es mehrere Verfahren. Diese Methode der Identifizierung wird von den meisten Personen problemlos akzeptiert. Der rechentechnische Aufwand bei diesem Verfahren ist weitaus größer als bei anderen Verfahren und die entsprechenden Musterdateien betragen bis zu 20 Kilobyte. Damit sind autonome Identifikationsgeräte erst mit den hohen Rechnergeschwindigkeiten möglich geworden. Ein Problem stellt jedoch der Datenschutz dar. Die angelegten Musterdateien können auch ohne Zustimmung der Person zu Identifizierungsmaßnahmen verwendet werden. Dies ist bei hand- oder fingerbasierenden Systemen nicht möglich.

Handgeometriekontrolle
Dabei werden die Abmessungen der Finger erfasst und die Dicke der Haut gemessen. Damit lässt sich eine Falscherkennungsrate von 1 zu 1.000 erreichen. Die Gründe für die relativ geringe Falscherkennungsrate ist in den nicht genügend vorhandenen Unterschieden in der Handgeometrie begründet.

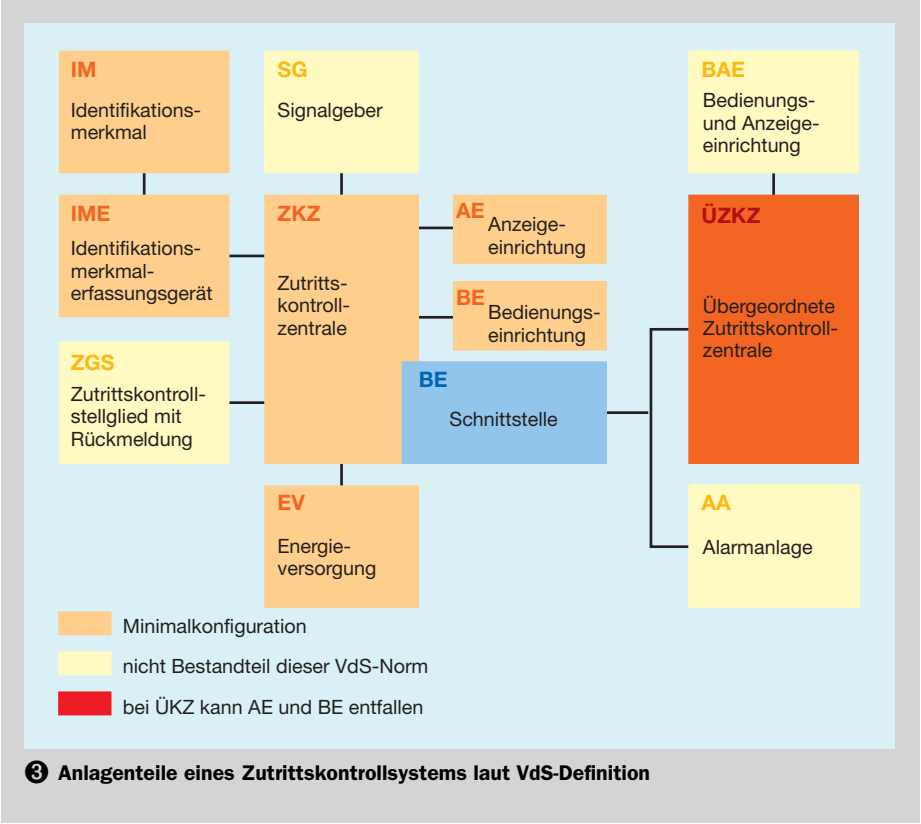
Fingerabdruckerkennung
Ein Fingerabdruck weist sehr viele individuelle Merkmale auf. Aufgrund dieser Unterschiede können Falscherkennungsraten von 1 zu 1.000.000 erreicht werden. Zusätzlich zum Fingerabdruck wird mittels Infrarotsensoren die Haut und Körpertemperatur detektiert. Die Größe der notwendigen Musterdateien beträgt zwischen 150 bis 2.000 Bytes.

Netzhauterkennung
Der Leser tastet mit Hilfe eines Laserstrahls die unterschiedlichen Strukturen der Netzhaut ab und fertigt davon ein Muster mit einer Länge von 256 Bytes an. Die Falscherkennungsrate liegt hier bei 1 zu 1.000.000. Der Vorteil dieses Verfahrens liegt in seiner Fälschungssicherheit, da die Netzhaut sich von außen nicht erkennen lässt. Aufgrund der Detektion der Netzhaut mit einem Laserstrahl, welche ungefährlich für den Menschen ist, wird dies von den meisten Menschen abgelehnt. Aus diesem Grund konnte sich dieses System bisher nur im militärischen Bereich durchsetzen.

Iriserkennung
Die Iriserkennung stellt offensichtlich eines der sichersten Verfahren dar. Als schwierig erweist sich die Erfassung der Iris, d.h. die unterschiedliche Position der Person und der Augen zum Identifikationsgerät.
Aus diesem Grund muss das Identifikationsgerät einen aufwendigen Suchvorgang ausführen. Hinzu kommt noch das generelle Problem menschlicher Hemmungen bei auf den Augen basierenden Identifikationsverfahren. Diese Technologie wird weiter entwickelt und hat Aussicht, ein dominierendes biometrisches Identifikationssystem zu werden.

Spracherkennung
Das Verfahren nutzt die Spektralanalyse eines bestimmten, gesprochenen Wortes und vergleicht diese Werte mit einer Musterdatei. Als negativ bei diesem Verfahren erweisen sich physische und psychische Stimmungen, welche die Sprache verfälschen und damit zu einer hohen Fehlerquote führen.

Schrifterkennung
Das Verfahren vergleicht das Schriftbild der Unterschrift und die Dynamik im Moment der Unterschrift. Als negativ bei diesem Verfahren erweisen sich ebenfalls physische und psychische Stimmun-



❸ **Anlagenteile eines Zutrittskontrollsystems laut VdS-Definition**

gen der Person, welche die Unterschrift und ihre Dynamik beim Unterschreiben beeinflussen.
Ein weiteres Problem stellt der relativ große Zeitaufwand für diese Art der Identifizierung dar.
In den meisten Fällen scheidet dieses Verfahren schon aus diesem Grund für eine Zutrittskontrolle aus.

Zutrittskontrolle und VdS

1997 erschien der Richtlinienentwurf für Zutrittskontrollanlagen, VdS 2358. Im August 1999 waren die Zutrittskontrollsysteme der Firmen AZS Technology AG und Häfele nach dieser Richtlinie zertifiziert.
Vier weitere Hersteller hatten zu diesem Zeitpunkt ihre Anlagen beim VdS eingereicht bzw. bereiteten diese vor.
Die Ursache für das zögerliche Herangehen an die Zertifizierung durch die Hersteller scheint jedoch darin begründet zu sein, dass der Markt die VdS-Zertifizierung nicht fordert. Dennoch soll an dieser Stelle darauf verwiesen werden, wie der VdS die Anlagenteile eines Zutrittskontrollsystems (ZKS) definiert. Bild ❸ zeigt ein Zutrittskontrollsystem als Blockbild mit den vom VdS dafür vorgesehenen Begriffen und Abkürzungen. Die Klassifizierung des VdS für Zutrittskontrollanlagen geht von 3 Klassen aus:

- **Klasse A:** Verfügt nur über einen einfachen Schutz gegen Überwindungsversuche und eine mittlere Verfügbarkeit des Systems. Eine Zuordnung der Benutzer ist vorhanden.
- **Klasse B:** Verfügt über einen höheren Schutz gegen Überwindungsversuche und eine hohe Verfügbarkeit des Systems. Eine Zuordnung der Benutzer ist vorhanden, die Zutrittsmöglichkeiten werden auf den geschlossenen Zustand überwacht.
- **Klasse C:** Verfügt über einen hohen Schutz gegen Überwindungsversuche und eine hohe Verfügbarkeit des Systems. Eine eindeutige Zuordnung der Benutzer ist vorhanden, nur berechtigen Personen ist der Zutritt möglich. Die Zutrittsmöglichkeiten werden auf den geschlossenen Zustand überwacht.

Neu ist der Aspekt und die Möglichkeit der Kopplung und Verknüpfung einer Einbruchmeldeanlage und eines Zutrittskontrollsystems mit der Möglichkeit, die Einbruchmeldeanlage mittels Zutrittskontrollsystem scharf bzw. unscharf zu schalten. Dies wird in der Praxis bereits bei Anlagen realisiert, die keine VdS-Zertifizierung erfordern.
Nun wird es definierte Schnittstellen auch für VdS-Anwendungen geben.

Planung eines Zutrittskontrollsystems

Für die Planung eines Zutrittskontrollsystems sind mehrerem Faktoren zu beachten. Neben der reinen Sicherheitsplanung mit der Bestimmung von Schutzzielen müssen alle organisatorischen und innerbetrieblichen Abläufe überprüft werden. Dazu gehört, dass der Personenfluss in den Hauptzeiten nicht beeinflusst wird, die Flucht- und Rettungswege weiterhin ihre Funktion uneingeschränkt erfüllen und die innerbetriebliche Abläufe nicht behindert werden. In Zusammenarbeit mit dem Kunden sind nachfolgende Daten zu erarbeiten und als Mengengerüst für die zu errichtende Anlage festzuhalten.

- Wieviele Türen, Tore oder Einfahrten sind zu überwachen?
- Wieviele Personen werden dieses System nutzen?
- Wieviele unterschiedliche Raumzonen- und Zeitzonenzulassungen sind erforderlich?
- Sind an den Zugängen zusätzliche Maßnahmen notwendig? (Drehkreuz, Schranke, Türöffner u.a.)
- Wird trotz dieser Maßnahmen der zügige Personenfluss gewährleistet?
- Werden die Bedingungen/Bestimmungen zu Flucht- und Rettungswegen noch eingehalten?
- Welche Türen, Tore oder Einfahrten sind auch auf Austritt bzw. Ausfahrt zu überwachen?
- Wo ist eine Aufenthaltsdauerüberwachung notwendig?

All diese Fragen müssen mit dem Kunden im Rahmen einer Sicherheitsanalyse geklärt werden. Erst danach kann das für diese Aufgabenstellung passende System ausgewählt werden.

Installation eines Zutrittskontrollsystems

Auch für die Installation eines Zutrittskontrollsystems gelten entsprechende Normen und Richtlinien. Manches ähnelt dabei der Installation einer Einbruchmeldeanlage.
Die geltenden europäischen Normen EN 50133-1 (Systemanforderungen), EN 50133-2-1 (Allgemeine Anforderungen an Anlagenteile) und EN 50133-7 (Anwendungsregeln) stellen wesentliche Grundlagen dar. Auf diesen Normen bauen die Richtlinien das VdS auf, gehen jedoch in einigen Punkten mit höheren Anforderungen über sie hinaus. Die VdS-Richtlinien VdS 2358 (Anforderungen) und VdS 2367 (Planung und Einbau) sollten jedoch bei einem Neueinstieg und der Erarbeitung notwendiger Grundkenntnisse für die Installation von Zutrittskontrollsystemen mit berücksichtigt werden.