Wachstumsmarkt: Segment Zutrittskontrolle

Der Beitrag gibt einen Einblick in den gegenwärtigen Entwicklungsstand dieses Marktsegmentes und in die wichtigsten geltenden Normen. Mit diesen Ausführungen soll der Umgang mit Zutrittskontrollsystemen und biometrischen Erkennungsmethoden erleichtert werden.

Wachsende Akzeptanz

Zutrittskontrollsystemen begegnet man heute zunehmend auf Schritt und Tritt. In den letzten 5 Jahren haben sie sich wohl wie kein anderes Sicherheitssystem eine breite Akzeptanz erworben. Das Marktsegment Zutrittskontrolle verfügt neben der Videotechnik über die größten Zuwachsraten. Das dürfte vor allem an den immer umfassenderen Funktionen und Identifikationskriterien, den Integrationsmöglichkeiten in andere Systeme und sinkenden Investitionskosten liegen. Zutrittskontrolle ist heute mehr als nur ein Ersatz für den Pförtner oder Wachmann. Sie ist heute eine Komponente der Sicherheitstechnik, die durch ihre verschiedensten Identifikationsmerkmalträger (ID-Karte) universell einsetzbar ist und mit Einbruchmeldeanlagen (EMA) genau so kombiniert werden kann wie mit Systemen der Haustechnik, mit Zeiterfassungssystemen, Betriebsdatenerfassung, innerbetrieblichem Zahlungsverkehr in Kantinen oder der Steuerung von Parkplätzen und Tiefgaragen.
Ob als Einzellösung oder als vernetztes System stellt die Zutrittskontrolle ein wirksames Mittel zur Erhöhung von Sicherheit und Schutz von Eigentum dar.

Normen im Vergleich

Aus der Entwicklung der letzten Jahre resultieren auch die Bemühungen, das Regel- und Normenwerk für Zutrittskontrolltechnik dieser Entwicklung anzupassen. In der Praxis sind hier die Normen EN 50133-1 (1998), 50133-2-1 (2001) und 50133-7 (2000) sowie die VdS-Richtlinie VdS 2358 von Bedeutung. Diese Normen unterscheiden sich jedoch in der Darstellung und Herangehensweise. Die Euro-Norm beschreibt in ihren Funktionsdiagrammen die Relationen der Zutrittskontrollanlage (ZKA) zu ihrem Stellglied, einschließlich Rückmeldung, ihren Benutzern, ihren Betreibern/Bedienern und zu anderen verbundenen Systemen.

EN 50133. Hier wird ein Zutrittspunkt in beiden Begehungsrichtungen klassifiziert, d.h. es wird zwischen Betreten und Verlassen eines Sicherungsbereiches bzw. einer Raumzone unterschieden. Die Sicherungsklassifizierung der EN 50133 (Bild ❶) unterscheidet zwischen zwei voneinander nur bedingt abhängigen Teilen, der Identifikationsklassifizierung und der Zutrittsklassifizierung.

VdS 2358. In der VdS werden in erster Linie die Schutzfunktionen und Bedrohungsarten einer Zutrittskontrollanlage dargestellt. Die Klassifizierung (Bild ❷) geht wie bei den bekannten VdS-Richtlinien für Einbruchmeldeanlagen von einer Einteilung in die Gefahrenklassen A, B und C aus. In der VdS-Richtlinie wird die Gefährdung/Bedrohung der ideellen und materiellen Güter im Sicherungsbereich hinter dem Zutrittspunkt betrachtet. So wird in den Klassen A und B der Austritt aus dem Sicherungsbereich nicht berücksichtigt. Lediglich in der Klasse C wird obligatorisch eine Ein- und Austrittskontrolle im Verbund mit einer Personenvereinzelung gefordert. Die Wahl einer entsprechenden VdS-Klasse beinhaltet somit bereits die Anforderungen an die Begehungsrichtung und die damit verbundenen Anforderungen.
Weitere, jedoch teilweise nur unwesentliche, Unterschiede ergeben sich aus den unterschiedlichen Betrachtungsweisen bei den Forderungen an die ID-Mittel und die ID-Auswertung, an den Zugang bzw. Zugriff auf den Datenbestand und auf die Programmierung sowie an das Stellglied und die Rückmeldung. Höhere Maßstäbe stellt die VdS-Richtlinie 2358 jedoch bei den Anforderungen an die Installation der Verkabelung und die Energieversorgung. Hier verlangt die VdS-Richtlinie für die Klassen B und C z. B. 2 Energiequellen, eine Notstromversorgung für bis zu 12 Stunden sowie einen Datenerhalt von 8 Tagen bei der Klasse B und 30 Tagen für die Klasse C. Datum und Uhrzeit müssen für 120 Stunden weiter funktionsfähig bleiben.
Die VdS-Richtlinie 2358 beschreibt auch die Schnittstelle zwischen EMA und ZKA, eine Anwendung, die immer häufiger in der Praxis genutzt wird. In der EN 50133 wird hinsichtlich einer Verbindung mit anderen Systemen nur auf die Forderung nach einen Melderausgang verwiesen, der für jeden Zutrittspunkt für die Meldung eines erlaubten Zutritts an andere Systeme vorhanden sein soll.

Einsatzgebiete

Zutrittskontrollsysteme findet man heute nicht nur zur Außenbereichsabsicherung und an Parkplätzen und Tiefgaragen, an den Eingängen von Banken und Sparkassen und großen Unternehmen, sondern auch bei Behörden und Verwaltungen, bei Gewerbeeinrichtungen, im Privatbereich sowie bei Objekten mit einem erhöhten Sicherheitsbedarf, wie Rechenzentren, Forschungseinrichtungen, Flughäfen und Atomkraftwerke. Sie ermöglichen in Parkhäusern oder Tiefgaragen eine ungehinderte Ein- und Ausfahrt, in Sportstätten gemeinsam mit Personenvereinzelungsanlagen (z. B. Drehkreuzen) den sicheren, kontrollierten Zutritt vieler Menschen und in Messehäusern den kontrollierten Zugang und Ausgang. Gleichzeitig geben sie dem Betreiber eine Übersicht darüber, wie viele Menschen sich im Messehaus aufhalten, um auch in einer Gefahrensituation gezielt handeln zu können.

Nutzen. Neben der erheblichen Einsparung von Personal geben die anfallenden Daten auch für den jeweiligen Betreiber Auskunft über Auslastung seiner Einrichtungen sowie andere interessante Informationen für die innerbetriebliche Organisation.

Trends. Neben den herkömmlichen Identifikationsmerkmalträgern, wie sie jeder als Geldkarte kennt, gelangen immer mehr berührungslose ID-Karten und Chip-ID-Karten zum Einsatz und bestimmen heute mit über 80 % bei neu errichteten Zutrittskontrollsystemen das Erscheinungsbild. Immer stärker werden von Nutzern und Betreibern biometrische Identifikationssysteme angenommen. Diese beruhen auf der Untersuchung der Handform, des Fingerabdruckes, der Iris, der Netzhaut, der Unterschrift oder der Sprache. Diese Identifikationen erfordern einen weitaus größeren rechentechnischen Aufwand, was den Speicherumfang und die Rechengeschwindigkeit betrifft, und eine umfangreichere Software. Sie erlebten aber durch die rasante Entwicklung der Rechentechnik in den letzten 3 Jahren einen großen Aufschwung. Auch wenn gegenwärtig die Lösungsvarianten für eine biometrische Identifikation noch kostenintensiver sind als herkömmliche ID-Karten und Leser, stellen sie für hohe Sicherheitsanforderungen bereits heute exzellente Lösungen dar, denen unbestritten die Zukunft gehören wird.
Die Analysten Frost & Sullivan in London prognostizierten bereits 1999 dem Teilmarkt Zutrittskontrolle in Deutschland eine durchschnittliche Wachstumsrate von jährlich rund 5,7 % bis zum Jahr 2005.

EN 50133-1: Sicherungsklassifizierung

– Identifikationsklassifizierung
  0: keine Identifikation
  1: geistige Merkmale (PIN-Code, Passwort, Parole)
  2: ID-Mittel oder Biometrie
  3: Kombination ID und PIN oder ID und Biometrie oder PIN und Biometrie
– Zutrittsklassifizierung
  A: wer und wo
  B: wer, wo und wann (mit Protokollierung)

❶ **Sicherungsklassifizierung nach EN 50133-1**

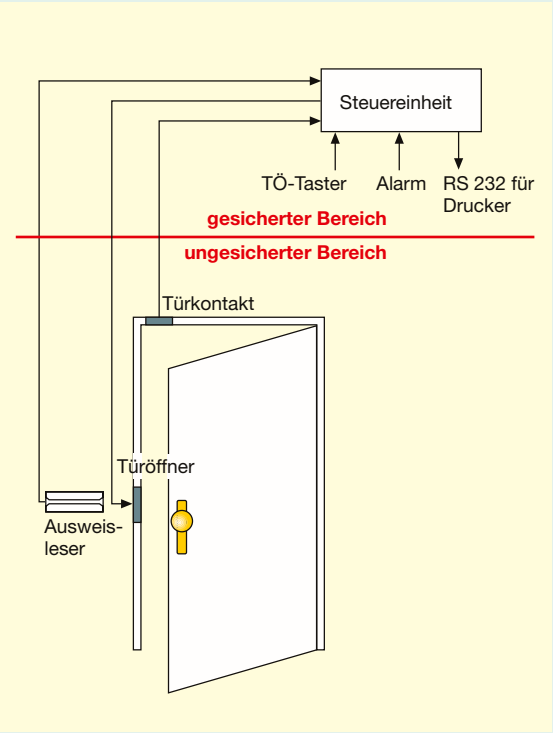
Anlagenklassifizierung nach VdS 2358

Klasse A
– einfacher Schutz, mittlere Verfügbarkeit
– keine individuelle Zuordnung des Benutzers
– keine Türüberwachung

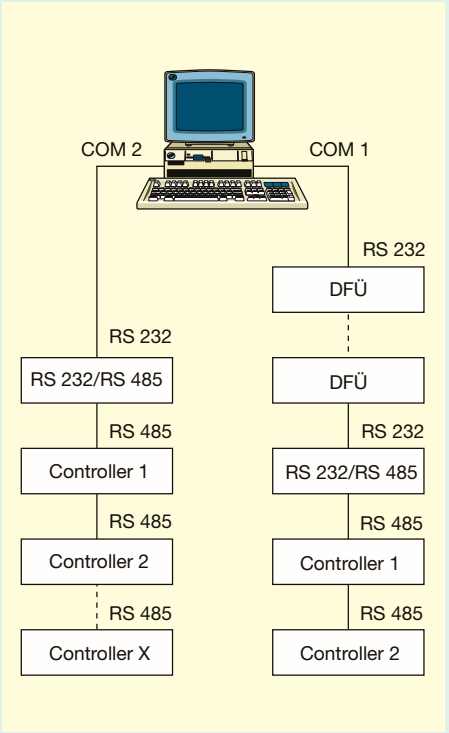
Klasse B
– mittlerer Schutz, hohe Verfügbarkeit, Zeitzonen
– individuelle Zuordnung des Benutzers
– Türüberwachung

Klasse C
– hoher Schutz, hohe Verfügbarkeit, Zeitzonen
– individuelle, eindeutige Zuordnung des Benutzers
– Türüberwachung, Vereinzelung, Ein-/Aus-Kontrolle

❷ **Anlagenklassifizierung nach VdS 2358**



❸ Einfache Zutrittskontrollsystemlösung mit Ausweisleser auf der Außenseite und Steuereinheit auf der Innenseite des Bereichs



❹ Beipiel für ein vernetztes Zutrittskontrollsystem mit Leitstellenrechner, abgesetzten Steuereinheiten über eine DFÜ und lokalen Steuereinheiten

Komponenten

Das Zutrittskontrollsystem besteht im einfachsten Fall aus:

- Steuereinheit, als Schaltzentrale mit entsprechender Intelligenz direkt vor Ort und der
- dazu notwendigen Software
- ein oder mehrere Lesern, angeschlossen an die Steuereinheit
- Elektromechanischen Sperr-, Verriegelungs- oder Öffnungseinrichtungen für jede Tür
- Rückmeldung über Magnet-Reed-Kontakt o.ä.
- Alarmgeber für die Signalisierung
- Stromversorgung, meist 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.

Anzeige

Einzellösung

Die Zutrittskontrolle als Einzellösung (Bild ❸) besteht meistens aus einer Steuereinheit (Controller) und 1 - 2 Lesern sowie den notwendigen Steuerausgängen für die elektromechanischen Sperr- oder Öffnungselemente der Eingangstüren. 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 überwachen der Öffnungsvorgänge
- Signalisierung von Störungen und Alarmen sowie Manipulationsversuchen.

Weitere Funktionen der Einzellösung können die optionale Nachrüstung mit einem biometrischen Erkennungssystem, freiprogrammierbaren Relaiskarten, eine Zutrittswiederholsperre sowie die 2-Personen-Zutrittskontrolle (Vier-Augen-Prinzip) 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 Stromausfall sicher funktionieren. Die meisten Hersteller bieten für ihre Systeme dazu ein entsprechendes Netzteil mit einem Akku an, aber auch der Einsatz einer geeigneten USV ist möglich.

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 ❹). 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, welche untereinander nicht ohne weiteres 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.

Anforderungen an den Controller

- Intelligentes Zutrittskontrollsystem für z. B. 6 Türen mit Software
- Speicher für 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
- Erweiterbar mit biometrischem Erkennungssystem
- Zutrittswiederholsperre
- Möglichkeit der 2-Personen-Zutrittskontrolle
- Erweiterbar mit freiprogrammierbaren Relaiskarten.

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

ID-Karten und Leser

Jede ID-Karte ist mit einer mit technischen Mitteln lesbaren und auswertbaren Information in Form einer Codierung versehen. Diese Information wird auch als Identifikationsmerkmal (Tafel ❶) und die ID-Karte als Träger der Information als Identifikationsmerkmalträger bezeichnet.

Tafel ❶ Verwendete Identifikationsmerkmale

- ID-Karten mit Magnetstreifen – Magnetkarte
- ID-Karten nach dem Induktionsprinzip – Induktivkarte
- ID-Karten nach dem Infrarotprinzip – Infrarotkarte
- ID-Karten nach dem Wiegand-Prinzip – Wiegandkarte
- ID-Karten, berührungslos – Berührungslose Karte
- ID-Karten mit integriertem Mikrochip

Tafel ❷ Bekannte biometrische Identifikationsmethoden

Gesichtserkennung
Es gibt mehrere Verfahren. Diese Methode der Identifizierung wird von den meisten Personen problemlos akzeptiert. Der rechentechnische Aufwand bei diesem ist weitaus größer als bei anderen Verfahren. Die entsprechenden Musterdateien betragen bis zu 20 kByte. Damit sind autonome Identifikationsgeräte erst mit den hohen Rechnergeschwindigkeiten möglich geworden.

Handgeometrie
Dabei werden die Abmessungen der Finger erfasst und die Dicke der Haut gemessen. Damit lässt sich eine Falscherkennungsrate von 1 zu 1000 erreichen. Die Gründe für diese relativ geringe Falscherkennungsrate ist in den nicht genügend vorhandenen Unterschieden in der Handgeometrie begründet. Wird in der Praxis nicht bzw. kaum angewendet.

Fingerprinterkennung
Ein Fingerabdruck weist sehr viele individuelle Merkmale auf. Aufgrund dieser Unterschiede können Falsch-erkennungsraten von 1 zu 1Million erreicht werden. Zusätzlich zum Fingerabdruck wird mittels Infrarotsensoren die Haut und die Körpertemperatur („Lebenderkennung“) detektiert. Der Fingerabdruck wird optisch, infrarot oder kapazitiv ausgemessen. Die Größe des biometrischen Referenz-Datensatzes beträgt zwischen 250 bis 3000 Bytes. Als kostengünstige biometrische Erkennung immer weiter verbreitet.

Iris-, Augenhintergrund- und Rentinaerkennung
Diese Erkennung stellt offensichtlich eines der sichersten Verfahren dar. Das generelle Problem menschlicher Hemmungen bei auf den Augen basierenden Identifikationsverfahren wirkte sich lange Zeit hemmend auf die Verbreitung dieser sicheren Erkennungsmethode aus. Die Abtastung erfolgt mit einem Licht- bzw. Infrarotstrahl und nicht, wie oft behauptet, mit einem Laserstrahl. Moderne Systeme nutzen hochauflösende Videotechnik für den Erkennungsprozess. Diese Technologie hat beste Aussichten, das dominierende biometrische Identifikationssystem zu werden.

Sprachmustererkennung
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. Diese Methode findet kaum Anwendung.

Biometrische Identifikation

In den letzten 3 Jahren hat sich die biometrische Identifizierung (Tafel ❷) weiter entwickelt und in zunehmenden Maße durchgesetzt. Die Vorteile der biometrischen Erkennung sind sehr vielfältig. So können zum Unterschied zu ID-Karten oder schlüsselbasierten Systemen die Merkmale nicht 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 kaum und sind somit fast über die gesamte Lebensdauer vorhanden. Je nach Art des zur Identifizierung herangezogenen Merkmals ist die Fälschungssicherheit sehr hoch. Betrachtet man noch die Entwicklung, die zur Identifizierung notwendigen Daten auf der Chipkarte des Nutzers mit einer Dateigröße von wenigen kByte geschützt abzuspeichern, so erscheinen auch komplizierte Identifikationen innerhalb eines kurzen Zeitraumes von unter 2 Sekunden als realistisch. Die Nachteile der biometrischen Systeme sind die schon erwähnten höheren Anschaffungskosten, der Aufwand für die Programmierung und Hinterlegung der personenbezogenen Merkmale sowie der erhöhte Aufwand an Technik vor Ort. Auch sollten die Probleme des Persönlichkeits- und Datenschutzes in diesem Zusammenhang nicht unbeachtet bleiben. Bestimmte biometrische Merkmale können nicht nur der Verifikation dienen, sondern auch zur eindeutigen Identifikation einer Person und ggf. gegen den Willen der Person missbraucht werden.

Fazit

Zutrittskontrollsystemen mit biometrischer Erkennung und sicheren, dem Stand der Technik entsprechenden Karten, z. B. Mifare-Karte, gehören die Zukunft. Diese ID-Karten bieten zunehmend die Möglichkeit, die Vergleichsdaten für die gewählte biometrische Erkennung zu speichern. Mit dieser technischen Lösung ergeben sich besonders für Großunternehmen, auch mit dezentralen Strukturen, neue und effiziente Lösungsmodelle. Jeder Installateur sollte sich heute an Systemen orientieren, welche den aufgeführten Euro-Normen entsprechen. Werden höhere Anforderungen, basierend auf den Richtlinien des VdS gestellt, ist Technik mit VdS-Anerkennung einzusetzen, wobei diese VdS-Anlagen dann von entsprechenden Errichterfirmen errichtet und attestiert werden müssen.

H. Petereins