Zutrittskontrolle integriert in Systemlösungen

H. Petereins, Berlin

Die Zutrittskontrolle als ein Marktsegment der Sicherheitstechnik verzeichnet gegenwärtig gute Zuwachsraten. Die Kenntnis der zu beachtenden Normen und das Verständnis beim Umgang mit Zutrittskontrollsystemen sowie biometrischen Erkennungsmethoden sind wichtige Voraussetzungen, sich dieses Geschäftsfeld zu erschließen. Das betrifft ebenfalls die bereits am Markt angebotenen Möglichkeiten, Einbruchmeldetechnik, Zutrittskontrolle und Videoüberwachung in eine Systemlösung zu integrieren.

1 Zutrittskontrollsysteme

Zutrittskontrollsystemen begegnet man heute zunehmend auf Schritt und Tritt. In den vergangenen fünf Jahren haben sich Zutrittskontrollsysteme wohl wie kein anderes Sicherheitssystem eine breite Akzeptanz erworben. Das Marktsegment Zutrittskontrolle verfügt neben der Videotechnik über die größten Zuwachsraten im Marktsegment Sicherheitstechnik. Das dürfte vor allem an den immer umfassenderen Funktionen und Identifikationskriterien von Zutrittskontrollsystemen, den Integrationsmöglichkeiten in andere Systeme und dies bei 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 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 – die Zutrittskontrolle stellt ein wirksames Mittel zur Erhöhung von Sicherheit und Schutz von Eigentum dar.

1.1 Richtlinien und Normen

Aus der Entwicklung der vergangenen zehn 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 zu nennen. Diese Normen unterscheiden sich jedoch in der Darstellung und Herangehensweise voneinander.

Autor
Dipl.-Ing. *Harald Petereins,* Ingenieurbüro für Sicherheitstechnik Petereins, Berlin.

EN 50133. Die Euro-Norm beschreibt in den dargestellten Funktionsdiagrammen die Relationen der Zutrittskontrollanlage zu ihrem Stellglied, einschließlich Rückmeldung, ihren Benutzern, ihren Betreibern/Bedienern und zu anderen verbundenen Systemen. In der EN 50133 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 differenziert zwischen zwei voneinander nur bedingt abhängigen Teilen, der Identifikationsklassifizierung und der Zutrittsklassifizierung. Die Sicherungsklassifizierung nach EN 50133-1 ist in Bild ❶ dargestellt.

VdS 2358. In der VdS 2358 werden in erster Linie die Schutzfunktionen und Bedrohungsarten einer Zutrittskontrollanlage dargestellt. Die Klassifizierung 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 (Bild ❷).

Euro-Norm und VdS-Richtlinie im Vergleich. Weitere, jedoch teilweise nur unwesentliche, Unterschiede ergeben sich aus den unterschiedlichen Betrachtungsweisen bei den Forderungen an die ID-Mittel und die ID-Auswertung, bei den Anforderungen an den Zugang bzw. Zugriff auf den Datenbestand und auf die Programmierung sowie den Anforderungen an das Stellglied und die Rückmeldung.

Höhere Anforderungen stellt die VdS-Richtlinie 2358 jedoch bei den Anforderungen an die Installation der Verkabelung und die Energieversorgung. Hier fordert die VdS-Richtlinie für die Klassen B und C, z. B. zwei 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.

1.2 Anwendungen

Zutrittskontrollsysteme findet man heute nicht nur zur Außenbereichsabsicherung, an Parkplätzen und Tiefgaragen oder an den Eingängen von Banken und Sparkassen und großen Unternehmen, sondern auch bei Behörden und Verwaltungen, bei Gewerbeeinrichtungen und im Privatbereich sowie bei Objekten mit einem erhöhten Sicherheitsbedarf, wie Rechenzentren, Forschungseinrichtungen, Flughäfen und Atomkraftwerken.

In Parkhäusern oder Tiefgaragen ermöglichen sie eine ungehinderte Ein- und Ausfahrt, in Sportstätten ermöglichen sie gemeinsam mit Personenvereinzelungsanlagen (z. B. Drehkreuzen) den sicheren und kontrollierten Zugang vieler Menschen, in Messehäusern den kontrollierten Zugang und Ausgang. Der Be-

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**

treiber erhält gleichzeitig damit eine Übersicht, wie viele Besucher sich im Messehaus aufhalten, um auch in einer Gefahrensituation gezielt handeln zu können.

1.3 Biometrische Systeme

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. 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 weit 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, des Gesichts, der Unterschrift oder der Sprache. Diese Identifikationen erfordern einen weitaus größeren rechentechnischen Aufwand, was den Speicherumfang und die Rechengeschwindigkeit der Auswerteeinheiten betrifft.

Durch die rasante Entwicklung der Rechentechnik in den vergangenen Jahren sind die realisierbaren Möglichkeiten enorm gestiegen. 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 und vor allem finanzierbare Lösungen dar, denen unbestritten die nahe Zukunft gehören wird. Die Analysten Frost & Sullivan in London prognostizierten bereits 1999 dem Teilmarkt Zutrittskontrolle in Deutschland eine durchschnittliche jährliche Wachstumsrate von etwa 5,7 % bis zum Jahr 2005 und darüber hinaus.

1.4 Komponenten eines Zutrittskontrollsystems

Das Zutrittskontrollsystem besteht im einfachsten Fall aus:

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

tionen hinzu. Die Zentraleinheit verfügt über entsprechende Speichermöglichkeiten, Bedien- und Anzeigeeinheiten sowie einen Druckeranschluss.

2 Einzellösung

Die Zutrittskontrolle als Einzellösung besteht meistens aus einer Steuereinheit (Controller) und ein bis zwei Lesern sowie den notwendigen Steuerausgängen für die elektromechanischen Sperr- oder Öffnungselemente der Eingangstüren. Eine Einzellösung sollte heute mindestens diese 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
- Signalisieren 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.

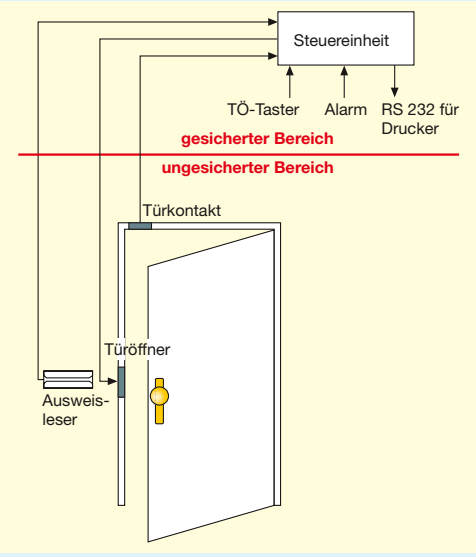
Eine Programmierung der Zutrittszeiten und der Türfreigabezeiten ist bei den meisten Controllern ebenso möglich wie die Programmierung von Sonn- und Feiertagen zur Einschränkung der Zutrittsmöglichkeit.

Eine Einzellösung (Bild ❸) 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.

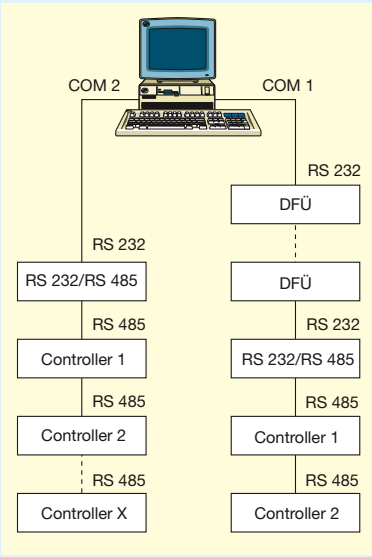
3 Vernetzte Systeme

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.



❸ Beispiel für eine Einzellösung



❹ Beispiel für ein vernetztes Zutrittskontrollsystem

Anforderungen an den Controller:

- 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 2 000 Ereignisse
- DFÜ-Schnittstelle (optional)
- Druckerschnittstelle (optional)
- Hostschnittstelle
- erweiterbar mit biometrischem Erkennungssystem
- Zutrittswiederholsperre
- Steuerfunktionen für Türsteuerung sowie für Störung und Alarm
- 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 oder der Änderung einer Berechtigung ist so unkompliziert und schnell ein Austausch möglich.

4 ID-Karten und Ausweisleser

Jede ID-Karte ist mit einer mit technischen Mitteln lesbaren und auswertbaren Information in Form einer Codierung versehen. Diese Information wird auch als Identifikationsmerkmal und die ID-Karte, als Träger der Information – als Identifikationsmerkmalträger bezeichnet. Diese Identifikationsmerkmalträger werden heute üblicherweise verwendet:

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

5 Biometrische Identifikation

In den vergangenen drei Jahren hat sich die biometrische Identifizierung rasch weiter entwickelt und zunehmend durchgesetzt (siehe auch Im Überblick).

5.1 Vorteile

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 Kilobyte geschützt abzuspeichern, so sind heute auch komplizierte Identifikationen innerhalb eines kurzen Zeitraumes von unter zwei Sekunden möglich.

5.2 Nachteile

Die Nachteile der biometrischen Systeme sind die höheren Anschaffungskosten, der höhere Aufwand für das Programmieren und Hinterlegen der personenbezogenen Merkmale sowie der erhöhte Aufwand an Technik vor Ort. Auch sollten die Probleme des Persönlichkeitsschutzes/Datenschutzes in diesem Zusammenhang nicht unbeachtet bleiben. Bestimmte biometrische Merkmale können nicht nur der Verifikation dienen, sondern können auch zur eindeutigen Identifikation einer Person dienen und ggf. gegen den Willen der Person missbraucht werden.

5.3 Wachsende Bedeutung der biometrischen Systeme

Jeder Installateur sollte sich heute an Systemen orientieren, die den aufgeführten Euro-Normen entsprechen und einem Mindestsicherheitsstandard entsprechen.
Werden höhere Anforderungen, basierend auf den Richtlinien des VdS gestellt, muss auf Technik mit VdS-Anerkennung orientiert werden. Dabei sollten diese als reine VdS-Anlagen dann von entsprechenden Errichterfirmen bzw. gemeinsam mit diesen errichtet werden.

6 Übergreifende Systeme

In zunehmenden Maße sind heute Einbruchmeldeanlagen mit Zutrittskontrollfunktionen anzutreffen. Diese Anlagen verfügen meist über eine Einbruchmeldeanlage nach den Richtlinien des VdS und eine Zutrittskontrollfunktion. Dabei wird der aus der Einbruchmeldetechnik bekannte Leser für die Scharf-/Unscharfschaltung der Einbruchmeldeanlage gleichzeitig als Lesegerät für die Zutrittskontrolle benutzt. Für den Anwender bzw. Nutzer besteht der Vorteil auch darin, für die Einbruchmeldeanlage und die Zutrittskontrolle nur eine ID-Karte benutzen zu können. Komfortable Lösungen verwenden neben den Lesern für die Scharf-/Unscharfschaltung auch Bedienteile der Einbruchmeldeanlage zur Eingabe von Codes oder zur Aktivierung von Steuerfunktionen.

IM ÜBERBLICK – Biometrische Identifikationsmethoden

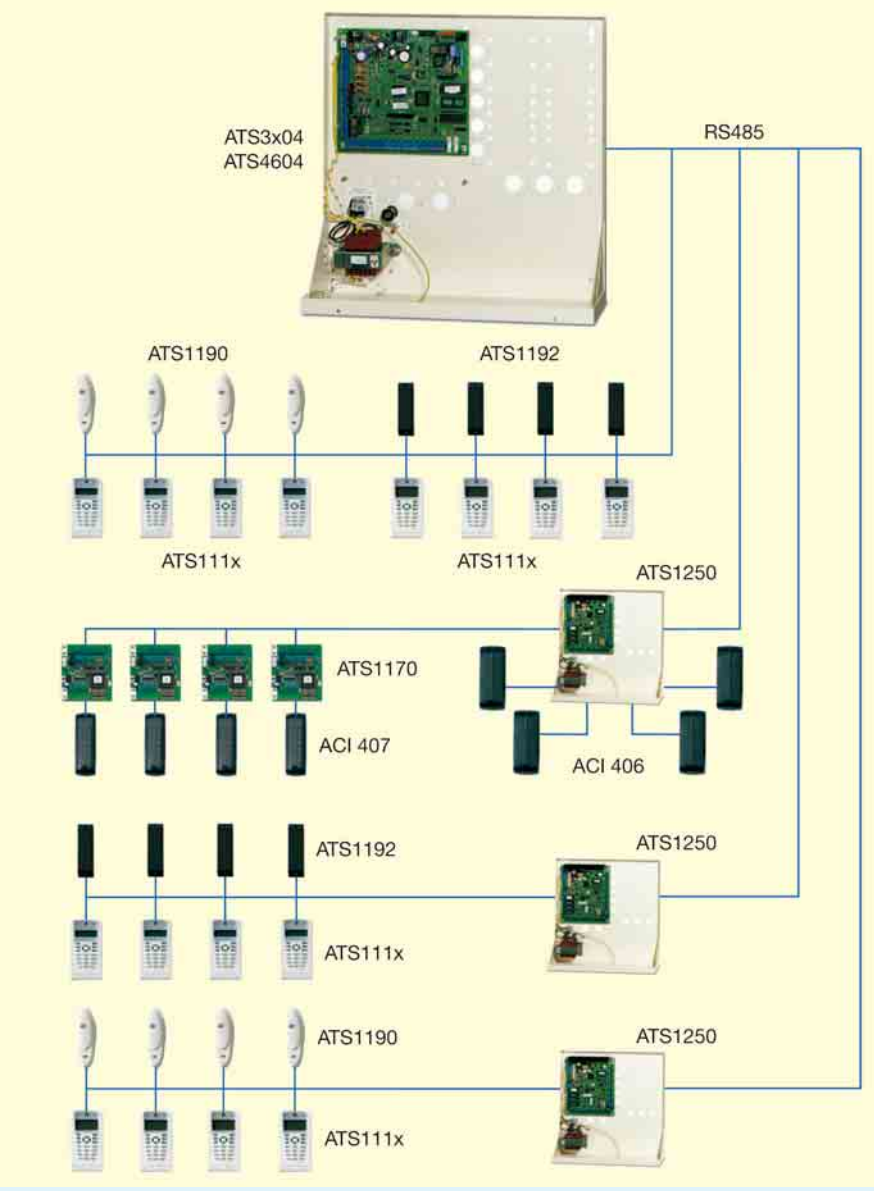
Gesichtserkennung
Zur Gesichtserkennung gibt es mehrere Verfahren. Diese Methode der Identifizierung wird von den meisten Personen problemlos akzeptiert. Der rechentechnische Aufwand bei diesem Verfahren ist weitaus größer als bei anderen Verfahren und die entsprechenden Musterdateien betragen bis zu 20 Kilobyte. Damit sind autonome Identifikationsgeräte erst mit den hohen Rechnergeschwindigkeiten möglich geworden. Großversuche, z. B. für Jahreskarteninhaber für Museen oder Tierparks, haben die theoretischen Aussagen in der Praxis überzeugend bestätigt und wurden von den Anwendern akzeptiert.

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. Sie wird in der Praxis nicht bzw. kaum angewendet.

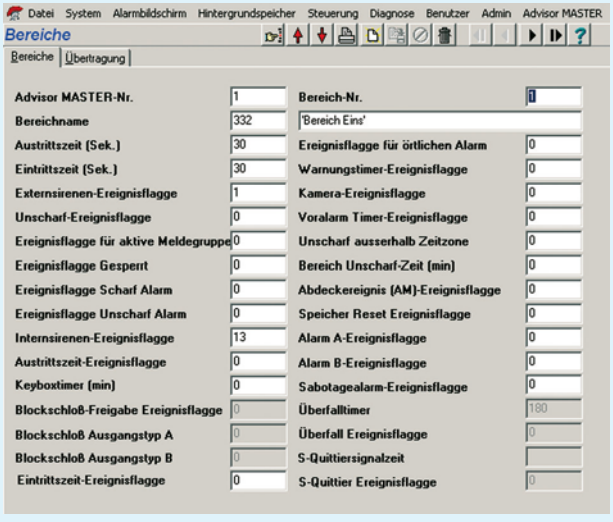
Fingerprinterkennung
Ein Fingerabdruck weist sehr viele individuelle Merkmale auf. Aufgrund dieser Unterschiede können Falscherkennungsraten von 1 zu 1000000 erreicht werden. Zusätzlich zum Fingerabdruck wir mittels Infrarotsensoren die Haut und die Körpertemperatur („Lebenderkennung“) detektiert. Der Fingerabdruck wird optisch, infrarot oder kapazitiv ausgemessen. Die Größe des biometrischen Referenz-Datensatzes beträgt zwischen 250 bis 3000 Bytes. Als kostengünstige biometrische Erkennung wird diese immer weiter verbreitet und ist heute oft bis in den Home-Security-Bereich anzutreffen.

Iris-, Augenhintergrund- und Retinaerkennung
Diese Erkennung stellt offensichtlich eines der sichersten Verfahren dar. Das generelle Problem menschlicher Bedenken 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. Praktische Großversuche, z. B. bei der Sicherheitsabfertigung auf Flughäfen, haben die Sicherheit des Verfahrens bestätigt und die Akzeptanz weiter erhöht.

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, die die Sprache verfälschen und damit zu einer hohen Fehlerquote führen. Diese Methode findet kaum Anwendung.



❺ System ATS von GE Security – ein praktisches Beispiel für die Integration von Einbruchmeldeanlagen, Zutrittskontrolle und teilweiser Video-Überwachung in einem System



❻ Das Beispiel der Software Titan vermittelt einen Eindruck der Softwareoberfläche

6.1 Zusammenwirken der Systeme

Da durch die Entwicklung der Rechentechnik die technischen Möglichkeiten erheblich gestiegen sind, können heute große und leistungsstarke Systeme errichtet werden, die Einbruchmeldeanlagen, Zutrittskontrolle und teilweise Video-Überwachung kostengünstig verschmelzen lassen. Das im Bild ❺ dargestellte System ist dafür ein gutes praktisches Beispiel.

6.2 Leitstellensoftware

Wird dieses System mit einer Leitstellensoftware (Bild ❻) ergänzt, mit der selbstverständlich auch das gesamte System programmiert und gesteuert werden kann, erhält man ein universelles System für den Einbruchschutz und die Zutrittskontrolle.

Die Software ermöglicht es, neben den Programmier-, Steuer- und Recherche-Funktionen auch eine Person beim Betreten eines Sicherungsbereiches zu identifizieren, indem der Name der Person, deren Sicherheitsstatus bzw. deren Berechtigung sowie – wenn im Programm hinterlegt – ein Foto der Person auf dem Bildschirm dargestellt wird.

Damit kann eine Sicherungskraft neben der automatischen Kontrolle des Zutritts durch das System auch eine manuelle Überwachung und Kontrolle vornehmen.

7 Zusammenfassung

Zutrittskontrollsysteme können wesentlich zur Erhöhung der Sicherheit in Behörden und öffentlichen Einrichtungen, in Unternehmen, aber auch im Home-Bereich beitragen.

Die Investitionskosten für Zutrittskontrollsysteme sind in den vergangenen Jahren gesunken – und dies bei stetig steigender Leistungsfähigkeit und höherer Sicherheit der Systeme.

Die Integration von Zutrittskontrolle, Einbruchmeldetechnik und Videotechnik in einem System mit einer professionellen Leitstellensoftware für alle Komponenten wurde auch besonders auf der Fachmesse Security im Herbst 2006 verdeutlicht.

Es wurden damit neue Perspektiven für umfassende Systemlösungen aufgezeigt. Auch für das Elektrohandwerk ergibt sich damit die Chance, neue interessante Geschäftsfelder zu erschließen. ■