

Keine Chance für Unbefugte

Systemvielfalt und -integration

Dipl.-Ing. Werner Störmer ist Leiter der Geschäftsstelle Essen der PCS Systemtechnik GmbH

Aufgrund des zunehmenden Sicherheitsbedürfnisses werden in Unternehmen immer häufiger elektronische Zutrittskontrollsysteme eingesetzt. Nur Personen, die sich identifizieren können und über eine Berechtigung verfügen, erhalten den Zutritt zum Werksgelände, zu Gebäuden und Sicherheitsbereichen. Da die Identträger – meist Mitarbeiterausweise – auch für andere kartengesteuerte Anwendungen, wie Kantinen- und Personalzeiterfassung, genutzt werden, kommt der Auswahl des Identifikationssystems besondere Bedeutung zu. Zur Zutrittskontrolle (ZK) mit hohen Sicherheitsanforderungen werden verstärkt biometrische Verfahren eingesetzt.



Bild 1 (links): An Eingängen mit Vereinzelungseinrichtungen kann eine Kopplung von ZK und PZE erfolgen [Aufnahme bei Bosch Siemens Hausgeräte GmbH]

Je nach Sicherheitsgrad eines Anwenders werden zur Zutrittskontrolle unterschiedliche Funktionen und Systemkomponenten benötigt. Am einfachsten sind Türöffnungssysteme, bei denen nach Prüfung des Ausweises ein Zutritt gewährt wird. Jeder Firmenangehörige, der eine freigegebene Karte hat, kann zu jeder Zeit die Türen öffnen. Es wird nur die Ausweisnummer, aber nicht nach Personengruppen oder zeitlichen Kriterien abgeprüft.

Trend zur Systemvielfalt

Soweit nur eine oder wenige Zutrittsstellen für eine geringe Mitarbeiteranzahl gesichert werden müssen, kann eine standalone-Lösung eingesetzt werden. Ein ZK-Terminal steuert die Zutrittsberechtigungen über gespeicherte Tabellen. Die Zeitprofile für Personengruppen oder einzelne Mitarbeiter werden z.B. über einen mobilen oder vernetzten PC geladen. Gemäß dieser Logik wird einem bestimmten Mitarbeiter nur dort der Zugang gestattet, wo das Lesegerät die positive Lesung durch



Bild 2 (unten): Die ZK im Fahrstuhl verhindert das Anfahren verbotener Etagen

ein Türöffnungssignal bestätigt. Die weitergehende Zutrittskontrolle arbeitet mit der Verknüpfung von definierten Personengruppen sowie einer Zeit- und Raumzonensteuerung. Erst nach erfolgreicher Prüfung der zeitlichen und örtlichen Zutrittsparameter wird die Tür geöffnet. Die Öffnungszeiten werden über die Tabellen im System verwaltet und

Thema: Trends bei Identifikations- und Zutrittskontrollsystemen

Problemstellung: Über ZK-Systeme verfügen heute bereits die meisten Unternehmen. Es kommen dabei die unterschiedlichsten Prinzipien zum Einsatz.

Lösung: Der Beitrag stellt die verschiedenen Identiträger sowie Lesesysteme vor und gibt einen Überblick über die verstärkt zum Einsatz kommenden biometrischen Identifikationssysteme. Im Vordergrund steht allerdings immer der Kunde mit seinen spezifischen Sicherheitsanforderungen.

über ein entsprechendes Programm in die entsprechenden Terminals verteilt.

Kostengünstig sind PC basierende Systeme mit Funktionen einer übergeordneten ZK-Zentrale, an der stern- oder busförmig abgesetzte ZK-Leser angeschlossen werden. Diese Systeme bieten bereits komfortable Programmiermöglichkeiten, Dokumentation und Stammdatenverwaltung an. Dabei ist die mögliche Anzahl und Art der Vernetzbarkeit der anzuschließenden ZK-Geräte zu beachten. Es kann im System auch eingestellt werden, dass eine oder mehrere Türen zu bestimmten Tageszeiten ohne Zutrittssteuerung geöffnet werden können.

Ein zusätzliches Modul der ZK-Software ist die Speicher- und Protokollierungsfunktion. Es wird gespeichert, welcher Mitarbeiter zu welcher Zeit an welchem Ort (z.B. Tür, ZK-Gerät etc.) eine zulässige oder unberechtigte Zu-

trittsbuchung vorgenommen hat. Auf diese Weise kann man feststellen, wer wann welchen Raum betreten hat und eventuell auch, wer es – zumindest mit welchem Identiträger – versucht hat.

Bei Systemen mit Alarmfunktion wird ereignisabhängig, z.B. unzulässiger Zutrittsversuch oder Ausfall von ZK-Einrichtungen, ein Alarm ausgelöst. Die jeweiligen Reaktionen werden über entsprechende Konfigurations-Tools definiert. Dabei sind auch technische Probleme (z.B. defekter Leser) oder Bedienfehler zu berücksichtigen. Alarmlösungen können direkt an eine Zentrale zur Bearbeitung weitergeleitet oder lediglich protokolliert und archiviert werden. Letzteres empfiehlt sich bei unberechtigten Zutrittsversuchen, weil es ja bei dem Versuch bleibt und die Person über die Buchung identifizierbar ist.

Überwachungssysteme kontrollieren das Verlassen (nach berechtigtem Zutritt) von Räumen, die vorhandene oder zulässige Zahl von Personen pro Raum, den Raumwechsel (Person B darf nicht von Raum Y nach Raum Z) oder die Zutrittswiederholspanne.

In allen Fällen sind die organisatorischen Maßnahmen zu beachten, z.B. wenn sich nicht mehr als drei Personen gleichzeitig in einem Raum aufhalten sollen und eine vierte Person Einlass verlangt: Wenn die Anwesenden aufgefordert werden sollen, den Raum zu verlassen, ist eine optische oder akustische Signalgebung erforderlich. Auch für den Einlassbegehrenden muss eine Anzeige erfolgen, warum er nicht ein-

treten darf. Hier ist der Einsatz eines ZK-Terminals mit mehrzeiligem Display, auf dem eine entsprechende Bedienerführung angezeigt wird, sinnvoll.

Trend zu Integrationslösungen

Die ZK ist meist Teil eines integralen Sicherheitskonzepts mit Alarmanlagen, Einbruchmeldesystemen und zentraler Leittechnik. Hinzu kommt die Anbindung und Steuerung von Vereinzelungseinrichtungen wie z.B. Schranken, Drehkreuze und -türen. Verstärkt findet auch die Integration in andere kartengesteuerte Anwendungen, wie die Kantinendaten- (KDE) und Personalzeiterfassung (PZE), statt. Aus Kostengründen ist hier die Nutzung des gleichen Netzwerks sowie Ausweis- und Identifikationssysteme, unter Umständen auch des gleichen Terminals, sinnvoll. Bei derart verknüpften Systemen werden mit nur einem Buchungsvorgang die Zutrittsberechtigung erteilt sowie die Anwesenheit und der Arbeitsbeginn des Mitarbeiters erfasst (Bild 1).

Gerade bei Kombination von ZK mit PZE empfehlen sich standalone-Terminals, die bei Ausfall des PCs oder bei Unterbrechung der Datenleitung selbständig die Buchung speichern, die Zutrittsanforderung prüfen und den Zugang freigeben oder sperren können. Um sicher zu gehen, dass unbefugtes Personal nicht auf bestimmte Etagen gelangt, kann eine Aufzugssteuerung eingerichtet werden: Ein im Aufzug installiertes ZK-Terminal erlaubt oder untersagt dann das Anfahren dieser Stockwerke (Bild 2). Die ZK am Park-



Bild 3: Beispiel für ZK- und PZE-Terminal mit Fingerprint in Kombination mit einem Chipkartenleser

platz- oder Tiefgarageneingang vermittelt zusätzlich einen Überblick über die Stellplatzbelegung.

Die Chipkartentechnologie ermöglicht auch die Verknüpfung mit anderen Anwendungen. Beispielsweise kann auch die Geldkarte der deutschen Kreditwirtschaft zusätzlich zur Identifikation bei der ZK, PZE und KDE genutzt werden. Auf dem freien Speicherplatz des Karten-Chips wird eine Ausweisnummer hinterlegt, mittels der die Überprüfung von Berechtigungen gesteuert wird. Der Vorteil besteht vor allem darin, dass die betreffenden Unternehmen oder Behörden keine Investitionen in die Karten leisten müssen, weil sie bereits bundesweit verbreitet sind. Für die Geldkarte spricht auch, dass das Schlüssel-Management für gesichertes Auslesen der Daten und damit eine effiziente Karten-Echtheitsprüfung bereits auf dem Chip implementiert ist.

Kontaktlose Identifikation

Bei vielen kartengesteuerten Anwendungen ist es notwendig, die Ausweisdaten nicht nur speichern und lesen, sondern auch kontrolliert verändern zu können. Daher muss der Ausweis mit

entsprechenden Fähigkeiten und Funktionen ausgestattet sein. Deshalb werden die herstellereigenen und statischen Codierungen wie Infrarot-, Induktiv- oder Wiegand-Ausweise an Bedeutung verlieren. Magnetstreifenkarten bieten weniger Speicherkapazität als Chipkarten, die wiederum in reine Speicher- und Mikroprozessor-Chipkarten zu unterscheiden sind. Im Unterschied zu anderen Technologien besitzt die Chipkarte eine integrierte Schaltung zur Informationsspeicherung mit Datenschnittstellen nach außen.

Dieses Speichermedium bietet hohe Datensicherheit und in der Variante als Prozessor-Chipkarte eine zusätzliche Verarbeitungskapazität. Beim Einsatz biometrischer ID-Verfahren wie Fingerprint oder Gesichtserkennung bietet die Chipkarte die Möglichkeit, die Referenzdaten in einem entsprechend großen und gegen unerlaubten Zugriff gesicherten Speicher der Karte zu hinterlegen. Am weitesten standardisiert und verbreitet ist die mit Kontakten versehene Chipkarte. Bedingt durch die Art der Datenübertragung und den Aufbau des Lesesystems ist die kontaktbehaftete Chipkarte aber nicht für alle Umgebungen (schmutzige oder feuchte Umgebungen) geeignet.

Günstiger ist hier die kontaktlose Chipkarte, bei der die Energieversorgung des Identträgers und der Datenaustausch vom/zum Lesegerät unter Verwendung elektromagnetischer Felder erfolgen. Neben der Karte werden auch Transponder in diversen Formen und Größen z.B. als Schlüsselanhänger angeboten. Abstandsleser werden als integrierte Module für PZE-/ZK-Terminals wie auch als abgesetzte oder eigenständige ZK-Leser angeboten. Hierbei kann die Identifikation im "Vorbeigehen" erfolgen, unabhängig davon, ob es regnet, schneit oder ob die Karte verschmutzt ist. Dabei hängt die Lesereichweite vom verwendeten System und dessen Empfindlichkeit ge-

genüber Störungen, aber auch von der Größe und Art der Antenne im Lesegerät ab.

Während ein herkömmlicher Kartenleser durch Kaugummi, Büroklammern, Papierstückchen oder eingeschüttete Flüssigkeiten einfach außer Funktion gesetzt werden kann, so vermögen es die Abstandsleser, den Ausweis oder Transponder selbst durch Mauerwerk hindurch zu identifizieren; dadurch lässt sich der Leser vandalismusgeschützt installieren.

Mittlerweile gibt es eine Vielfalt an herstellereigenen, kontaktlosen Chipkartentypen, wobei sich die Systeme mit einer Übertragungsfrequenz von 125 kHz/13,56 MHz durchgesetzt haben. Für kontaktlose Mikroprozessor-High-End-Chipkarten (Proximity Cards) und Transpondersysteme für geringe Lesereichweiten bis ca. 20 cm wurde mit der ISO 14443 ein Standard definiert. Diese Norm beschreibt die physikalischen und datentechnischen Eigenschaften der Übertragungsstrecke zwischen einem Lesegerät und dem Datenträger.

Die Zukunft gehört wohl der Dual-Interface- oder Kombikarte, die sowohl den kontaktlosen als auch den kontaktbehafteten Datenaustausch erlaubt. Dadurch werden die Vorzüge beider Technologien miteinander verbunden: zum einen der Sabotageschutz und der Komfort bei der Identifikation und zum anderen die Sicherheit bei Lese-/Schreibvorgängen mit vielen Daten, insbesondere bei Zahlungsfunktionen. Zusätzlich können Dual-Interface-Karten mit Magnetstreifen, Barcodes oder anderen Codierungen versehen werden.

Für Hochsicherheitsbereiche

Bei höheren Sicherheitsanforderungen werden biometrische Authentisierungssysteme eingesetzt, die Personen anhand physiologischer und verhaltensbedingter Merkmale eindeutig erkennen. Diese biometrischen Merkmale sollen die Schwächen anderer Identifikationsarten, wie vergessener PIN oder Ausweis, eliminieren. Bislang waren biometrische Authentisierungssysteme

Systeme noch relativ teuer, weshalb sie hauptsächlich für polizeiliche oder militärische Sicherheitsanwendungen genutzt wurden.

Inzwischen wurde die Technik - und damit auch die Akzeptanz dieser Systeme - soweit verbessert, dass der Einsatz für eine sichere und zuverlässige Erkennung genutzt werden kann. Um die Identität einer Person authentifizieren zu können, werden die biometrischen Merkmale als Referenzdaten in Datenbanken gespeichert und zur Berechtigungsprüfung aufgerufen. Empfehlenswert ist die Speicherung der umfangreichen Referenzdaten mittels Datenkompression auf einer Chipkarte. Bei der Ausweisidentifizierung entfällt die Suchzeit in der Datenbank. Mittlerweile werden folgende Verfahren eingesetzt:

- Verfahren, die statische physiologische Attribute (z.B. Fingerabdrücke, Handgeometrie, Netzhautmuster) erfassen.
- Verfahren, die variable bzw. dynamische physiologische Attribute (z.B. Gesicht, Stimme) oder verhaltensabhängige Merkmale wie Schreibrhythmus auf einer Computertastatur oder eine Unterschrift per Hand zur Überprüfung heranziehen.
- Multimodale Verfahren, die mehrere Merkmale, sowohl statische als auch dynamische, kombiniert erfassen, um eine höhere Erkennungsgenauigkeit zu erreichen.

Die wichtigsten biometrischen Authentisierungs-Systeme und ihre Eigenschaften:

• **Fingerprint**

Die neuartigen Module zur Fingererkennung arbeiten anstelle von teuren und schmutzanfälligen optischen Scannern mit billigen pflegeleichten Silizium-Chips:

Winzige Kondensatorzellen registrieren die Mikrostruktur der Haut und ermöglichen z.B. die Integration in Tastaturen, Kartenlesern und Handys. Der aufgelegte Finger ersetzt also die Ausweis- und/oder PIN-Eingabe. Gegen Ungenauigkeiten durch Narben, Schmutzpartikel oder Fingerverletzungen werden Fehlerkorrektur-Algorithmen eingesetzt (Bild 3).

Um kurze Erkennungszeiten sicherzustellen und den Zugriff zur Datenbank zu ersparen, werden die Daten des Fingerabdrucks im System so codiert, dass sie auf einer Chipkarte gespeichert werden können.

• **Gesichts- und Spracherkennung**

Zur Gesichtserkennung wird am Kontrollpunkt mittels Kamera automatisch ein Bild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen. Auch bei unterschiedlicher Mimik oder Position des Gesichts vermag das System, aus der Bildverarbeitung die Person sicher zu identifizieren.

Beim Spracherkennungssystem werden verschiedene Merkmale der Stimme des Betreibers abgespeichert. Im Überwachungsmodus wird gewährleistet, dass nur Personen einen Zutritt erhalten, deren Sprache, nach Nennung ihres Passwortes, wiedererkannt wird. Zur Erhöhung der Erkennungssicherheit kann zusätzlich eine Analyse der Lippenbewegung bei der Spracheingabe erfolgen. Für die Bewegungsanalyse extrahiert das Verfahren einzelne Bilder aus einer Videosequenz. Mit der Berechnung optischer Flussvektoren entsteht ein charakteristisches biometrisches Muster.

Um die Sicherheit noch mehr zu erhöhen, können auch verschiedene biometrische Merkmale wie Gesicht, Sprache und Mimik kombiniert

überprüft werden. Solche Systeme können auch so programmiert werden, dass bei Ausfall einer Erkennungsart (z.B. durch laute Geräusche oder grelles Licht) zwei eindeutig erkannte Merkmale ausreichen.

Sorgfältige Auswahl

Die Auswahl des ZK-Systemtyps ist abhängig von der erforderlichen Sicherheit.

Bei der Entscheidung für ein bestimmtes Identifikationssystem sind vorrangig die Akzeptanz bei der Belegschaft und die Frequentierung (z.B. pro Zutrittsstelle) zu beachten. Die kartengebundene Identifikation geht meist sehr viel schneller als die Erkennung personenspezifischer Merkmale. Dagegen bieten die biometrischen Verfahren eine wesentlich höhere Sicherheit, sind jedoch nicht für alle Einsatzarten geeignet. Die Auswahl muss also entsprechend den jeweiligen Anforderungen und Umgebungsbedingungen sorgfältig erwogen werden.

PCS Systemtechnik GmbH, Pfälzer-Wald-Str. 36, 815 39 München

Kontakt zum Autor:

Werner Störmer

Tel.: 0201-8941630, Fax: -89410

wstoermer@pcs.com