

Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses

Band: 83 (1992)

Heft: 17

Artikel: Datenschutz beginnt schon vor der Tür : das Zutrittsberechtigungssystem als Komponente des Sicherheitskonzeptes

Autor: Zobrist, Rudolf

DOI: <https://doi.org/10.5169/seals-902862>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 13.10.2024

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Datenschutz beginnt schon vor der Tür

Das Zutrittsberechtigungssystem als Komponente des Sicherheitskonzeptes

Rudolf Zobrist

Die Sicherheit und Integrität von Information ist für moderne Betriebe und Anlagen dermassen entscheidend, dass diese mit aktiven Schutzmassnahmen gewährleistet werden müssen. Eine erste wichtige Komponente der Risikoverminderung ist ein Zutrittsberechtigungssystem, das neben dem Informations- und Anlagenschutz noch weiteren Betriebsfunktionen wie der Präsenz- und Zeiterfassung dient. Der vorliegende Beitrag gibt einen Überblick über den heutigen Stand und die Technik dieser Systeme.

Pour les entreprises et installations modernes, la sécurité et l'intégrité de l'information sont à tel point décisives qu'il faut les garantir par des mesures de protection actives. Une première composante de la réduction du risque est le système d'autorisation d'accès qui, outre la protection de l'information et des installations, sert à d'autres fonctions dans l'entreprise tel que l'enregistrement de la présence et des heures. Les présent article donne un aperçu de l'état actuel et la technique de ces systèmes.

Adresse des Autors

Rudolf Zobrist, El.-Ing. HTL, Direktor der Zettler AG, 8752 Näfels.

Wenn der Computer nicht mehr läuft, läuft nichts mehr. Diese Erfahrung macht jeder einmal, der auf elektronische Datenverarbeitung angewiesen ist. Darüber hinaus sind die täglich übermittelten Informationen Geld wert, viel Geld, im Banken-Business gar Milliarden. Erstaunlich deshalb, dass trotz ausgeklügelten Datensicherungssystemen die Hardware oft nur unzureichend geschützt wird. EDV-Anlagen sind sensibler als man denkt, und Schäden gehen oft weit über das Materielle hinaus. Was für die EDV-Anlage gilt, ist bei einer CAD-Anlage nicht anders. Oft unbemerkt ist ein kleiner Arbeitsplatz zu einer Grossanlage geworden, und schnell sind Millionenwerte in Hard- und Software investiert, ohne das ein Schutzkonzept besteht. Wird aber einmal die Sicherheitsproblematik erkannt, wird oft der Ruf nach einem Zutrittskontrollsystem laut. Bevor in ein derartiges System aber investiert wird, empfiehlt es sich, neben den technischen Mög-

lichkeiten auch die organisatorischen Folgen und die psychologischen Aspekte zu überdenken, die mit der Einführung des kontrollierten Zutritts auftreten. Es gilt, die Prioritäten im Schutzbereich, das geeignete System sowie die bevorzugte Kartentechnologie zu eruieren, aber auch die Mitarbeiterinnen und Mitarbeiter von der Notwendigkeit und den Vorteilen des neuen Systems zu überzeugen. Für die Geschäftsleitung sind moderne Zugangssysteme nicht zuletzt ein wirksames Instrument, organisatorische Massnahmen effizient durchzusetzen.

Was sind Zutrittskontrollsysteme?

Zutrittskontrollsysteme schützen Objekte, Einrichtungen, Werte und geistiges Eigentum vor dem Zugriff unbefugter Personen (Bild 1). Gefahren können von Mitarbeitern und von externen Besuchern ausgehen, die in EDV-Räumen oder anderen sensiblen

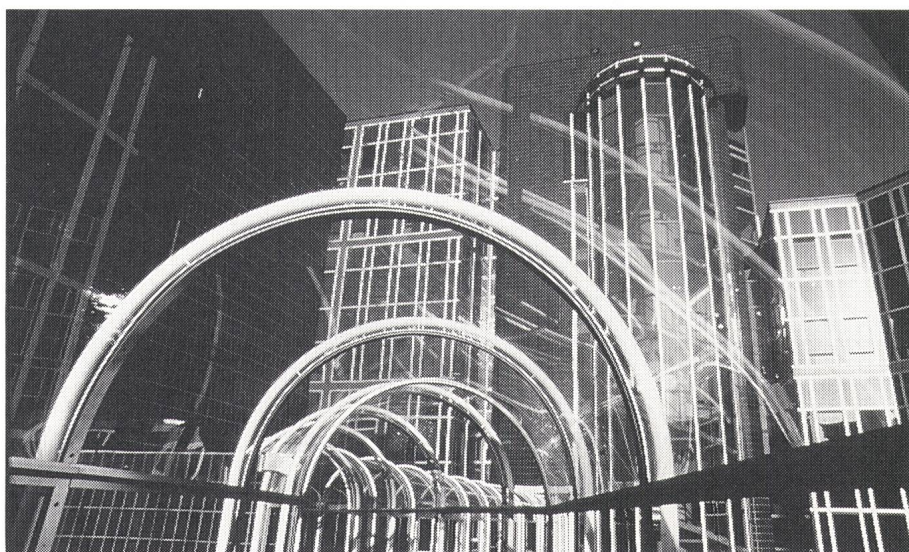


Bild 1 Im Sicherheitskonzept von wirtschaftlich genutzten Gebäuden spielt die Zutrittskontrolle eine zentrale Rolle

Räumen absichtlich oder unabsichtlich Schaden anrichten können. Elektronische Zutrittsberechtigungssysteme nehmen zusätzliche Aufgaben wahr, wie zum Beispiel die Freigabe von Zugängen zu bestimmten Tages- und Wochenzeiten oder die Aufklärung von Unregelmässigkeiten mit Hilfe einer lückenlosen Protokollierung aller gewährten Zutritte (Bild 2). Darüber hinaus vereinfachen sie die Organisation und Verwaltung von Schliessplänen und reduzieren Umtriebe und Kosten bei Verlust oder Diebstahl von Schlüsseln.

Bild 2
Die Funktionen Zutrittskontrolle und Zeiterfassung werden oft in das gleiche System integriert



Der Einsatz im Rahmen des Sicherheitskonzeptes

Zutrittskontrollsysteme sind weder Ersatz für ein Sicherheitskonzept noch für ein Einbruchmeldesystem. Die unterschiedlichen Aufgabenbereiche zeigen sich bereits in einem einfachen Vergleich: Brandmelde- und Einbruchmeldeanlagen sind Systeme, die sich passiv verhalten. Sie werden für die Belegschaft eines Unterneh-

mens erst bemerkbar, wenn ein Störfall eintritt. Dann müssen diese Anlagen auf Anrieb einwandfrei funktionieren, selbst wenn sie vorher möglicherweise Jahre «geschlafen» haben. Ein Zutrittskontrollsystem hingegen nimmt eine kontinuierliche aktive Rolle wahr. Die Mitarbeiter stehen

täglich mit ihm in Kontakt. Öffnungs-, Kontroll- und Aufzeichnungsvorgänge finden ständig statt, Mängel und Störungen werden sofort entdeckt. Viele Anwender sehen in diesen Anlagen im wesentlichen ein modernes, kontrollierbares Schliesssystem, das dem Mitarbeiter die nötige Bewegungsfreiheit gewährt und Betrieb, Personal und Werte vor fremden Zugriffen schützt.

Wie bereits angetönt, gilt es aber zu bedenken, dass für ein umfassendes Sicherheitskonzept weitere Massnahmen, wie der jeweiligen Sicherheitszone entsprechende bauliche und mechanische Vorkehrungen, zu realisieren sind. Eine der wichtigsten zusätzlichen Sicherheitsmassnahmen ist die Instruktion der Mitarbeiterinnen und Mitarbeiter. Sie sollen so früh wie möglich in das Sicherheitskonzept einbezogen werden und wissen, dass die Zutrittskontrolle ihrem Schutz und der Sicherung des Arbeitsplatzes dient.

Zur Akzeptanz von Zutrittskontrollsystemen

Der Ausdruck Zutrittsberechtigung ist dem Wort *Kontrolle* vorzuziehen, da dies der Funktion des Systems eher gerecht wird. Die Mitarbeiter erhalten einen modernen Schlüssel, mit dem sie ohne grosse Einschränkung ihrer Arbeit nachgehen können. Die Angst vor Schlüsselverlust und vergessenem Abschiessen entfällt. Mitarbeiter, die bislang keinen Schlüssel hatten, werden durch die Karte gleichberechtigt; eine motivierte Belegschaft ist umsichtig und bemerkt Unregelmässigkeiten. Zutrittsberechtigungssysteme können auch die Akzeptanz geschlos-

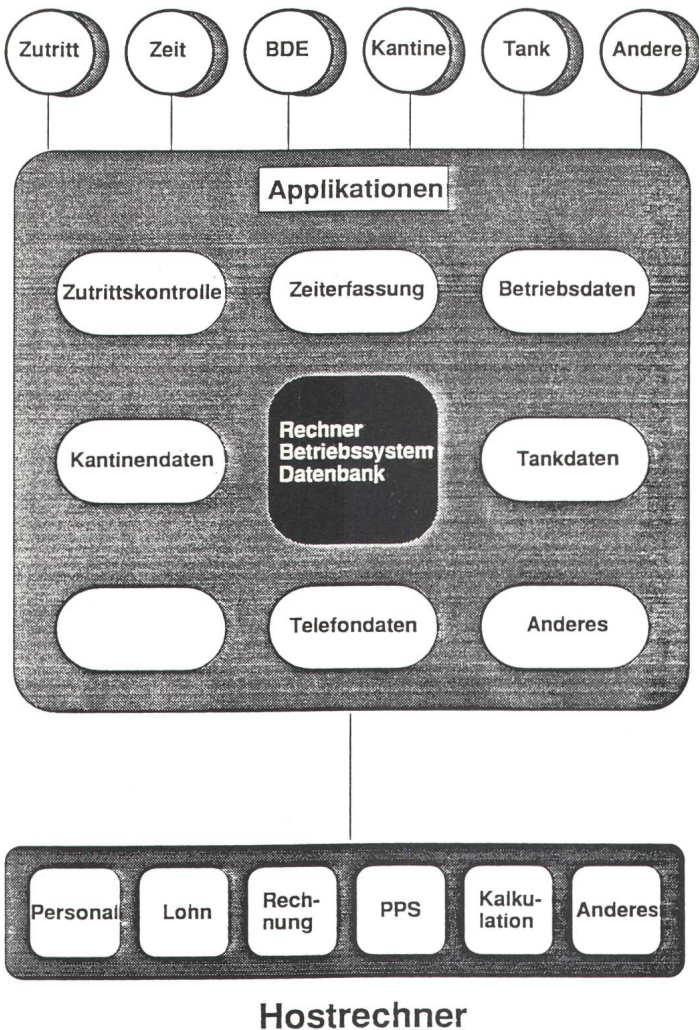


Bild 3
Das moderne Zutrittsberechtigungs-system ist Teilsystem eines übergeordneten Betriebssystems, das verschiedenste Anwendungen umfasst

sener Türen erhöhen, da deren Wichtigkeit manifestiert wird. Ein System wird zudem um so eher akzeptiert, je geringer die dadurch entstehende Behinderung ausfällt. Dies ist bei der Planung wie bei der Systemwahl zu berücksichtigen.

Wirkung und positive Nebeneffekte

Für die Unternehmensleitung eines Betriebes ist die Installation eines Zutrittsberechtigungssystems in mancher Hinsicht vorteilhaft und mit positiven Nebeneffekten verbunden. Die Möglichkeit, weitere Systeme und Funktionen wie Zeiterfassung und -bewirtschaftung integrieren zu können, hat die Hemmschwelle zur Einführung eines derartigen Systems in den letzten Jahren deutlich gesenkt. Ein elektronisches Zutrittsberechtigungssystem hat darüber hinaus eine spürbare präventive Wirkung und verhilft auch organisatorischen Massnahmen ohne grossen Aufwand zum Erfolg. Wie oft sind Türen nicht abgeschlossen «weil man ja in fünf Minuten wieder hinein muss», oder werden Türen nicht verschlossen, weil die zuständige Person gerade krank oder in den Ferien ist? Mit dem elektronischen Zutrittskontrollsystem ist die Tür grundsätzlich immer zu und nur mit der Karte zu öffnen. Damit erübrigt sich auch der ohnehin oft nur wenig wirksame Hinweis auf dem Schildchen «Türe ab 18.00 Uhr bitte schliessen!».

In Betrieben mit häufig wechselndem Personal ergibt sich ein weiterer wesentlicher Vorteil: Vergisst der Mitarbeiter nach Beendigung des Arbeitsverhältnisses seine Karte abzugeben, kann dessen Zutrittsberechtigung vom System umgehend gelöscht werden, was bei mechanischen Schliesssystemen nicht möglich ist.

Frühzeitige Planung notwendig

Die Zutrittsberechtigungssysteme sind, wie alle anderen Komponenten der Gebäudetechnik, schon früh in die Planung einzubeziehen (Bild 3). Ein in letzter Minute zu beschaffendes Zutrittskontrollsystem verursacht höhere Installationskosten und unter Umständen Einschränkungen in der Systemauswahl. Anhand eines Gebäudeplans müssen die verschiedenen Sicherheitszonen definiert werden, die unterschiedliche Schutzgrade erfordern. Dazu gehört auch der Miteinbe-

zug der Aussenanlagen wie Parkplatzzufahrten und Garagen.

Die Systemauswahl muss sich nach diesen spezifischen Anforderungen richten. Dabei sind einerseits die technischen Möglichkeiten, andererseits die Schnittstellen zu anderen Sicherheitsvorkehrungen wie Einbruch- und Brandmeldeanlagen sowie Gebäudeleitsystemen zu berücksichtigen. Aber auch ein späterer Ausbau der Anlage muss möglich sein.

Die technischen Möglichkeiten

Die heutige Systemvielfalt lässt Flexibilität in Grösse, Anwendungsbereich und Identifikationsart zu, so dass sich für Betriebe unterschiedlichster Grösse ein passendes System installieren lässt. Der potentielle Anwender muss sich dabei primär über die Vor- und Nachteile der Hauptunterscheidungsmerkmale zentraler oder dezentraler Steuerung und Kartentechnologie orientieren (Bild 4). Bei zentralen Konzepten besteht für mehrere Gebäude ein System, das alle Leser von einer Zentrale aus bedient und parametrisiert sowie die Türen steuert. Bei dezentralen Systemen hingegen funktioniert jedes Gebäude autonom, aber mit derselben Karte. Daneben bestehen mehrere Varianten für kombinierte Systeme, wobei die Gebäude vernetzt werden, die Unterzentralen jedoch teilweise autonom sind.

Die Vor- und Nachteile der verschiedenen Steuerungsoptionen zeigen sich bei den Türstationen. Im Falle einer zentralen Türsteuerung ist es der Zentralrechner, der die Entscheidungen trifft und die entsprechenden Aktionen an der Türstation auslöst. Nachteile: Die Zugriffszeit erhöht sich mit zunehmender Anzahl der Leser; bei einem Ausfall des Zentralrechners ist die Sicherheit an der Tür nicht oder nur teilweise gewährleistet, da in der Regel beim Zutritt nur noch der Firmencode, nicht aber die Zeitzone und die persönliche Zutrittsberechtigung geprüft wird.

Bei den dezentralen, vollautonomen, intelligenten Türsteuerungen werden die Programmierung und Parametrierung im Zentralrechner vorgenommen. Die Vorgaben werden dann an die Türstationen weitergeleitet und dort gespeichert. Bei der Kartenlesung entscheidet die Türstation autonom und löst die entsprechende Aktion aus. Damit verkürzt sich die Wartezeit wesentlich. Die Bewegun-

gen werden an den Zentralrechner zur Protokollierung weitergeleitet, wobei Alarmmeldungen mit höchster Priorität verarbeitet werden. Eine umfassende Sicherheit ist demnach auch bei Ausfall oder Wartung des Zentralrechners oder bei Unterbruch der Datenleitung gewährleistet.

Höchsten Ansprüchen in Anwendung und Sicherheit wird die kombinierte zentrale-dezentrale Türsteuerung gerecht. Im Online-Betrieb entscheidet die Zentrale, was Optionen wie Raumbilanzierung oder Doppeltutrittsberechtigung ermöglicht. Nach einem Ausfall der Zentrale schaltet das System um und arbeitet wie das dezentral gesteuerte System.

Kartentechnologien

Die meisten Zutrittskontrollsysteme arbeiten heute mit Kartentechnologien unterschiedlichster Art (Kreditkarten- und Badgekartenformat). Grundsätzlich unterscheidet man dabei zwischen magnetischer, optischer, induktiver, berührungsloser und Laserabtastung.

Magnetkarten: Sie sind preiswert und lassen mehrere Anwendungskombinationen zu. An die Sicherheit die-

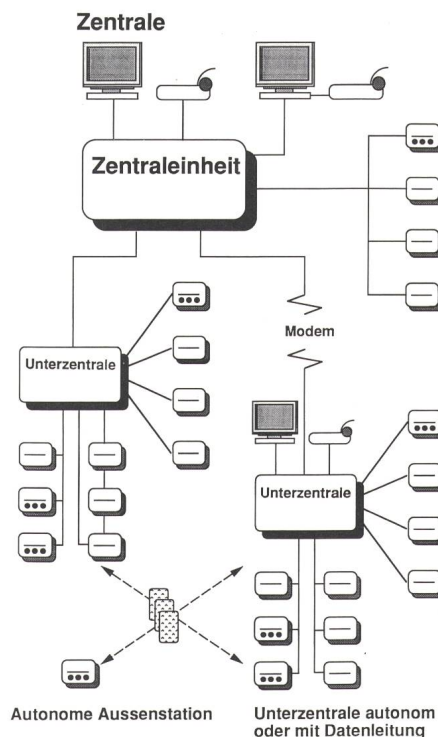


Bild 4 Elektronische Zutrittsberechtigungssysteme können zentral oder dezentral organisiert sein. Dezentrale Organisation setzt intelligente und autonome Türlesestationen voraus

ser Karten können keine hohen Ansprüche gestellt werden; die Karte ist relativ einfach zu lesen, zu kopieren oder abzuändern.

Optisch lesbare Karten (z.B. *Barcode*lösung): Sie können mit einem simplen Matrixdrucker hergestellt und einem einfachen Gerät verschweisst werden. Auch diese Ausweise sind äusserst einfach zu kopieren. Eine zusätzliche Sicherheit erbringt allenfalls eine mechanische Abdeckung des Codes, der dann mit einem Infrarot-Barcodeleser decodiert wird.

Induktive Karten: Sie werden hauptsächlich für höhere und höchste Sicherheitsansprüche benützt. Der sogenannte Wiegand-Code beispielsweise ist in die Karte eingegossen (Kombination von verschiedenen Ferrit-Drähtchen). Die Karte durchläuft im Leser folgende Stadien: Magnetisierung des Codes durch Induktion, Lesung, Entmagnetisierung des Codes. Zur Entschlüsselung des Codes müsste man die Karte sorgfältig öffnen und die Zusammensetzung (die chemische wie die geometrische) der einzelnen Ferrit-Drähtchen feststellen. Um auch dieses Restrisiko zu beseitigen, werden bei den Wiegand N-Crypt-Karten zusätzliche Verschlüsselungen vorgenommen, die nur vom System decodiert werden können.

Kombinierte Karten: Oft werden sie auch hergestellt, um den Sicherheits- und Universalitätsansprüchen gerecht zu werden. Diese beinhalten einen induktiven Code für die Zutrittskontrolle und eine weitere Codierung für zusätzliche Zwecke.

Handsfree-Karten: Handsfree-Karten und -Leser werden immer häufiger eingesetzt; sie sind bequemer in der Handhabung und können unter keinen Umständen manipuliert werden. Die Leser sind zudem sabotagesicher, weil sie keine mechanischen Teile und Schlitzlöcher aufweisen und meist unsichtbar montiert sind. Hier drängen sich besonders batteriefreie Karten auf, die mit passiver Elektronik ausgestattet sind. Sie verfügen über eine sehr lange Lebensdauer und sind sehr umweltfreundlich.

Chipkarten (Smart Card): Chipkarten werden mit mechanischem Kontakt oder berührungslos angeboten. Die berührungslos beschreib- und lesbaren, batteriefreien Multifunktions-Chip-Karten werden heute zum Beispiel in Skigebieten für die Handsfree-Bedienung der Drehkreuze sowie als Punktekarte eingesetzt. Die neueste

Generation dieser Karten, welche etwa ab Ende 1993 mit den entsprechenden Lese- und Schreibgeräten zur Verfügung stehen wird, kann zwei Funktionen übernehmen: ein fest programmierter, unkopier- und unzerstörbarer Code und ein beschreib- und auslesbarer 1-KBit-Speicher erlauben einen Einsatz als Mittel zur berührungslosen Identifikation bis 70 Zentimeter Lesedistanz und den Einsatz für Debit- und Kreditfunktionen.

Die Laserkarte: Sie ist der wichtigste Rivale der Chip-Karten. Sie besitzt zwar keine eingebaute Elektronik, verfügt jedoch über eine aussergewöhnlich hohe Speicherkapazität, welche diese Technologie für Zutrittsberechtigungssysteme interessant macht. Die Möglichkeit, über längere Zeit alle getätigten Transaktionen zu speichern oder speicherintensive, biometrische Daten des Karteninhabers zu integrieren, öffnen der Laserkarte den Weg zum Einsatz bei Gebührenabrechnungssystemen, Hochsicherheitsanlagen und zur Verwendung als Debitkarte.

Biometrische Systeme: Eine weitere Dimension der Berechtigungsprüfung stellen die biometrischen Systeme dar, welche anhand der Identifikation von gespeicherten physischen Personenmerkmalen Zutritt gewähren

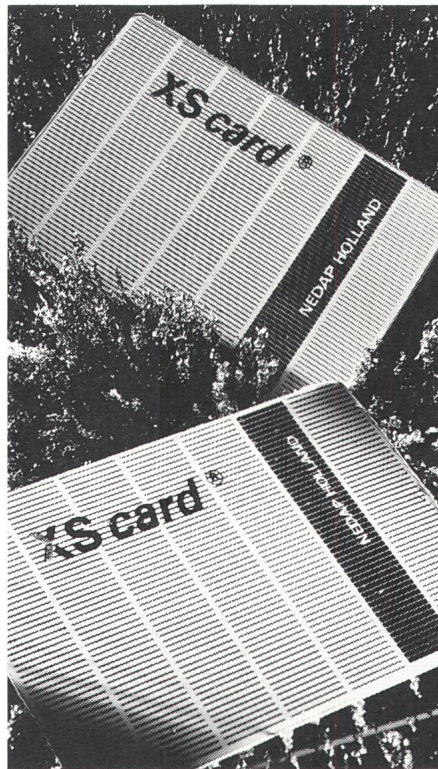


Bild 5 Bei den Kartentechnologien sind in den kommenden Jahren noch grosse Fortschritte zu erwarten

und punktuell vor allem im Hochsicherheitsbereich angewendet werden. Die Möglichkeiten der biometrischen Identifikation liegen im Porträt- oder Unterschriftenvergleich, in der Handgeometrie, in der Stimmenerkennung, in der Fingerabdruckidentifikation oder in der Erkennung der Augensignatur. Diese Art der Berechtigungsprüfung nimmt ziemlich viel Zeit in Anspruch und setzt eine grosse Speicherkapazität voraus. Erstaunlicherweise sind die vom Kunden gewünschten Identifikationsmerkmale gewissen Modeerscheinungen unterworfen. So wurde beispielsweise kürzlich von Sandia, den National Laboratories des US Departments of Energy, festgestellt, dass zurzeit die Identifikation der Handgeometrie im Trend liegt.

Zukunftsperspektiven

Die Zukunftsträchtigkeit des Marktes widerspiegelt sich in der grossen Anzahl Anbieter aus den unterschiedlichsten Branchen. Eindeutig im Vorteil befinden sich Unternehmen aus dem Bereich Sicherheitstechnik, da sie über die nötige Erfahrung im Haustechnik-Projektmanagement und die dafür notwendige Serviceinfrastruktur verfügen. Biometrische Systeme und die berührungslose Zutrittsberechtigung werden dank sinkender Preise und neuer Software weitere Verbreitung finden. Die grössten Veränderungen wird es aber bei den Karten geben (Bild 5). Die Zukunft gehört der kombinierten Chip-Karte (Smart Card), die verschiedene Technologien in sich vereint und universell für die Zutrittsberechtigung, Zeitwirtschaft, Betriebsdatenerfassung, Kantinenabrechnung usw. eingesetzt werden kann. Schnittstellen zur Verschlüsselung von Speicherinhalten werden auf der Karte Platz finden, die eine Identifikation des Kartenbesitzers mittels direkt auf der Karte abgespeicherten biometrischen Informationen ermöglichen. Vielleicht etwas voreilig, aber sicher nicht unrealistisch ist der Gedanke, dass alle heutigen Magnetstreifen-Karten wie Kredit- und Bankkarten durch die neuen Technologien ersetzt und mit neuen integrierten Funktionen wie Pass, Fahrausweis, medizinischer Ausweis usw. ergänzt werden. Ob diese Möglichkeiten dazu führen, dass wir nur noch eine einzige Plastikkarte auf uns tragen werden, wird der Markt entscheiden.



ERTECH



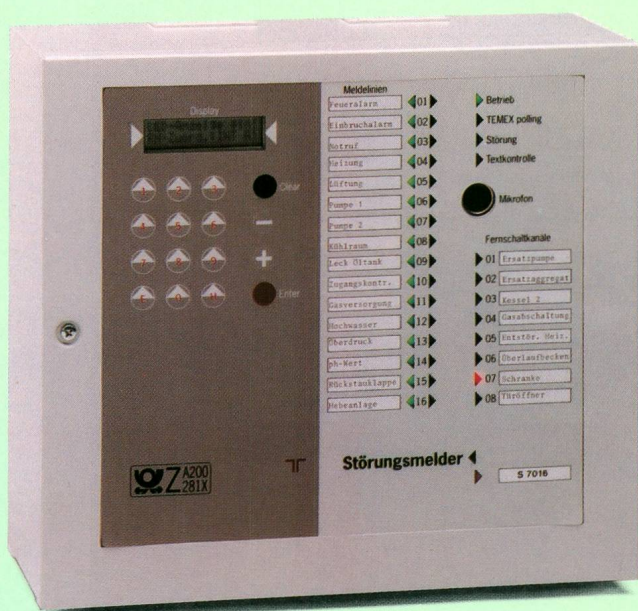
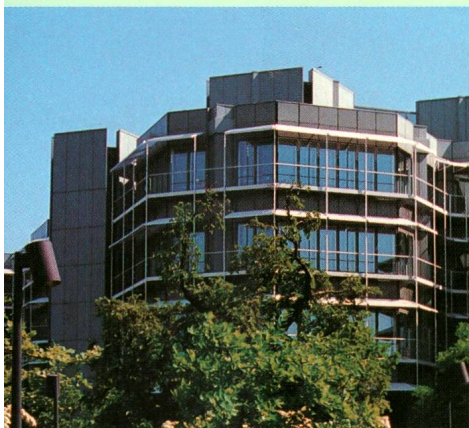
ELEKTRONIK AG

ERLENSTR. 10

CH-2555 BRÜGG

TEL. 032/53 45 46

FAX 032/53 48 64



Telefonalarm

Störungsmelder

Vollautomatisches Melden von Störungen, Zustandsänderungen und Gefahren über das öffentliche Telefonnetz.

ERTECH

ELEKTRONIK AG

ERLENSTR. 10

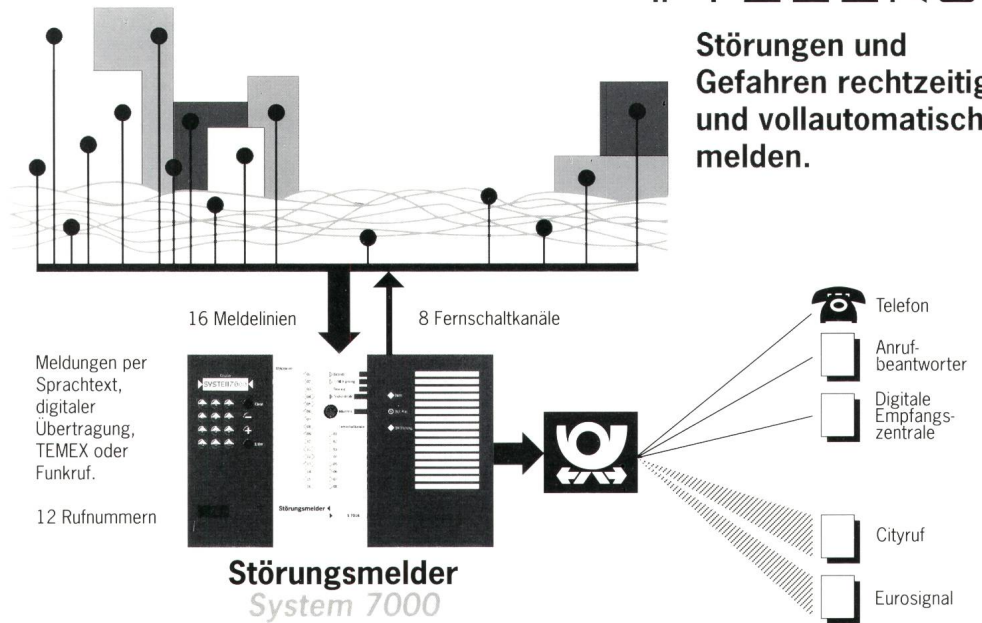
CH-2555 BRÜGG

TEL. 032/53 45 46

FAX 032/53 48 64

TELENOT

Störungen und Gefahren rechtzeitig und vollautomatisch melden.



Melden per Sprachtext oder Funkruf

Freie menügesteuerte Programmierung aller relevanten Funktionen

Besprechung der Meldetexte über ein Mikrofon

Betrieb direkt an bestehendem Telefonanschluss (keine zusätzliche Amtsleitung)

Kein Modem erforderlich

Textspeicherung mittels Sprachprozessor

Ausbau bis zu 16 Meldelinien und 8 Fernschaltkanäle

Freie Zuordnung der Rufnummern zu den Meldelinien

Echtzeituhr, automatische Umschaltung Sommer- Winterzeit

Ereignisspeicher mit Zeitanzeige

IWV- oder MFV-Wahl programmierbar

Fernabfrage der Meldelinienzustände

Alarmer über das Telefonnetz

Die Geräte der Serie S 7000 sind private Zusatzeinrichtungen, die an das öffentliche Telefonnetz angeschlossen werden können. Sie dienen der Übermittlung von technischen Alarmen (Betriebszustände, Grenzwerte, Störungen) sowie Hilferufe (Einbruch, Feuer, Überfall) über das Telefonnetz.

Die Meldungen werden in Form von Sprachtext übermittelt und können auf jeden beliebigen Telefonanschluss abgesetzt werden.

Der modulare Aufbau und das umfangreiche Zubehör bringen dem Anwender in jedem Fall eine optimierte Lösung. Der Sprachtext der 16 Meldelinien kann über ein Mikrofon vom Anwender gesprochen werden. Die Speicherung der Texte erfolgt in einem RAM-Speicher.

Durch Fernabfrage kann der Störungsmelder auf unquittierte Meldung überprüft werden.



Firma _____

Name _____

Abteilung _____

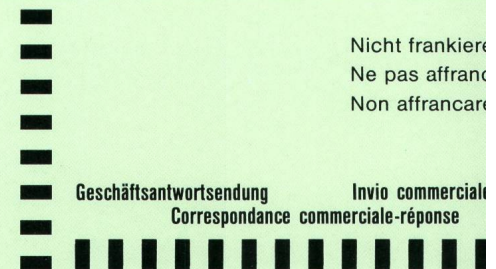
Strasse _____

Ort _____

Telefon _____

Bitte senden Sie uns Unterlagen über:

- Störungsmelder
- Einbruchmeldeanlagen
- Datenübertragung Fernwirktechnik
- Beratung, Vorführung



ERTECH
Elektronik AG
Erlenstrasse 10
CH-2555 Brugg