

Neue Gebäude mit Sicherheit



Aus dem Inhalt

Das Berliner Verbundvorhaben sicheres Gebäude	2
Sicherheitspass für Gebäude	5
Gebäudeautomatisierung und Gebäudesicherheit – Hilfsmittel für Prävention, Gefahrenbekämpfung und Personenrettung	7
Terroristische Bedrohung und Gebäudesicherheit	9
Selbstorganisierende Gebäudeautomationssysteme Forschungsprojekt „SOGAS“	11/12

Seite

Editorial

Als die Stadt Berlin 2004 mit einer Technologieinitiative im Rahmen von Projekt Zukunft das Thema „Sicherheit mit IT“ aufgriff, war nicht unbedingt zu erwarten, dass rund zwei Jahre später mit dem „Verbundvorhaben sicheres Gebäude“ derart greifbare Ergebnisse vorliegen.

Im Verlauf dieses Zeitraumes hat sich erfreulicherweise gezeigt, dass Behörden, Unternehmen und Forschungseinrichtungen durchaus in der Lage sind, auf einer gemeinschaftlichen Interessensbasis nach neuen, innovativen Weiterentwicklungen eines Sicherheitsbegriffes sowie nach innovativen IT-Lösungen zu forschen, diese zu konzipieren und letztlich auch marktfähig zu erschließen.

Darüber hinaus beweist der heutige Stand des Projektes, dass das Interesse am Thema „sicheres Gebäude“ nicht nur auf Seiten der Projektmitarbeiter liegt, sondern sich in zunehmendem Maße auch den zukünftigen Anwendern – den Immobilienbetreibern und den Vermietern – erschließt. Die Sicherheit in Gebäuden besitzt heute einen gewachsenen Stellenwert.

Durch eine intensive und kooperative Zusammenarbeit wurden neue Erkenntnisse und Lösungen für ein verbessertes, auf funktionelle und wirtschaftliche Sicherheit zielendes Gebäudemanagement entwickelt. Die Verknüpfung der verschiedenen Sicherheitsaspekte einer Immobilie, deren Koordination und Verzahnung sind jetzt erfolgreich und praxisnah erprobt. Dem Erfordernis, eine engere Zusammenarbeit auf den Feldern Wirtschaft, Wissenschaft und Entwicklung zu erreichen, sind wir dank des „sicheren Gebäudes“ einen guten Schritt näher gekommen.

Das vorliegende Magazin gibt einen umfassenden Überblick und Einblick in die Aufgaben und Arbeiten der beteiligten Projektpartner. Beim Lesen wünsche ich Ihnen viele interessante Entdeckungen und Erkenntnisse.

Werner Gegenbauer
Ehrenpräsident der IHK zu Berlin



Neuere Herausforderungen in der Gebäudeautomation

Das Berliner „Verbundvorhaben sicheres Gebäude“

Gebäude können heute nicht mehr grundsätzlich als sicher bezeichnet werden. Diese Erkenntnis war der Ausgangspunkt für das Berliner „Verbundvorhaben sicheres Gebäude“ im Rahmen der Technologieinitiative „Sicherheit mit IT“. Sie gab zugleich den Anstoß für die Projektidee, bei deren Entwicklung die Technische Fachhochschule Wildau maßgeblich beteiligt war. Während der Durchführung übernahm sie die wissenschaftliche Begleitung sowie das Projektmanagement. Klares Ziel war es, aus dem Verbundvorhaben verwertbares Wissen zu gewinnen.

Der Standort Berlin ist für die Initiative von hoher Bedeutung. Im Zusammenhang mit der Hauptstadtfunktion und den Anforderungen an den Regierungssitz konzentrieren sich hier viele Gebäude auf engem Raum, bei denen das Thema Sicherheit besonders wichtig ist. Zudem haben sich Facility Management- und Sicherheits-Dienstleister etabliert, deren Wissen und Aktivitäten genutzt werden können. Verbände und Netzwerke wie der Arbeitskreis Unternehmenssicherheit Berlin-Brandenburg (AKUS) oder die Initiative „Sicherheitspartnerschaft mit der Berliner Polizei“ kommen als Partner für das Anwendungs-Szenario in Frage.

Entwicklungschancen

Schon heute gibt es in Gebäuden unterschiedliche Gebäudetechnik-Systeme und -Anlagen, Telekommunikations- und Informatiknetze, Sicherheits- und Alarmsysteme sowie komplexe Gebäudeleittechnik. Oft handelt es sich um unabhängige Systeme aus Hard- und Softwarekomponenten, deren Schnittstellen unzureichend gestaltet sind.

Die Stromausfälle („Blackouts“) in einer Reihe von hochindustrialisierten Staaten sind ein weiteres Beispiel für die Notwendigkeit, mit komplexen, oft weit verzweigten Automatisierungslösungen umzugehen zu lernen. Gäbe es beispielsweise einen Zugriff auf Echtzeit-Informationen der Energieversorger über den Zustand ihrer Netze, so könnten in einem „sicheren Gebäude“ bei einem sich ankündigenden Netzausfall Personenaufzüge noch gezielt bis zur nächsten Etage gefahren werden. So würde verhindert, dass Menschen in den Aufzügen stecken bleiben. Wenn mit den speziellen Methoden der modernen Informationstechnologie externe und interne Automatisierungssysteme verknüpft werden, die Sicherheit signifikant erhöht und im Katastrophenfall Leben gerettet werden.

Effektives Zusammenspiel aller Systeme

Wenn ganze Systeme oder einzelne Funktionen der komplexen Technik in modernen Gebäuden ausfallen, können durch unerwartete Kombinations- oder Synergie-Effekte multiplizierte Schadensbilder auftreten. Das kann unter Umständen die völlige Vernichtung des Gebäudes, seiner Bewohner oder von Teilen seiner Umwelt zur Folge haben. Moderne, ganzheitliche Sicherheitskonzepte sollen daher die Nutzer und die eingesetzte Technik schützen. Darüber hinaus sichern sie die dauerhafte Funktionserfüllung, bewahren die Bewohner vor materiellen und informellen Verlusten und schützen die Umwelt vor Schäden durch und aus dem Gebäude. Das effektive Zusammenspiel aller Systeme und ein integratives Gesamtbetriebskonzept sind die einzige Möglichkeit, auch in Zukunft einen maxi-

malen Nutzen für Eigentümer, Betreiber und Mieter zu erzielen und Risiken weitgehend auszuschließen.

Das „Verbundvorhaben sicheres Gebäude“ will keine neuen Hardware- oder Software-Schnittstellen für bereits existierende Produkte in den oben aufgezählten Systemen entwickeln. Vielmehr entsteht auf Basis der am Markt vorhandenen Hardware- und Software-Lösungen eine neue, ganzheitliche Plattform (ein DCS-System). Diese Plattform verwendet die zur Zeit separat erzeugten und gespeicherten Daten der diversen nicht interoperablen Systeme und stellt diese unterschiedlichsten Zielgruppen als komplexe, ganzheitliche Information für das jeweils betrachtete Gebäude zur Verfügung.

Alle in einem Gebäude anfallenden Daten sämtlicher relevanter Systeme werden so erstmalig über geschützte Zugriffsmechanismen den verschiedenen Dienstleistern unter Verwendung von Internet-Technologien bereitgestellt.

■ **Dieter Skrobotz**
Technische Fachhochschule Wildau
skrobotz@igw.tfh-wildau.de

Funktionsanalyse und intelligente Kombination

Grundlage des ganzheitlichen, innovativen Gebäudemanagements

In den letzten Jahren errichtete bzw. modernisierte Gebäudekomplexe sind nicht nur vielseitig in ihrer architektonischen Struktur, sie haben auch eine Fülle unterschiedlicher Systeme zur Wahrung der Gebäudesicherheit integriert.

Die Gebäudesicherheit beschränkt sich dabei meist auf einzelne Maßnahmen z. B. auf die visuelle Überwachung oder eine Zeit- und Zutrittskontrolle. Zudem sind die eingesetzten sicherheitsrelevanten Systeme spezialisierte Einzelanlagen, die in sich geschlossen sind und nur begrenzt Informationen untereinander austauschen. Konkret diente der bisherige Informationsaustausch meist nur der Weiterleitung von Störfunktionen. Lösungen, die die Gesamtfunktionalität eines Gebäudes absichern – also Gefahren durch Technik oder Menschen abwehren – werden derzeit nur unzureichend angeboten.



Quelle: Honeywell

Dieser unbefriedigenden Situation hat sich das „Verbundvorhaben sicheres Gebäude“ angenommen. Ein neuartiger ganzheitlicher Ansatz beim Gebäudemanagement ermöglicht es erstmals die Gesamtfunktion des Gebäudes als Einheit zu betrachten und sich nicht länger auf den autonomen Funktionserhalt jedes einzelnen Gewerkes zu beschränken. Ziele sind die uneinge-

schränkte Kommunikation aller Einzelanlagen untereinander, die technische Auswertung bislang ungenutzter Informationen sowie die Anwendung verknüpfter Verfahren um den Gesamtzustand des Gebäudesystems zu beschreiben. Zu diesem Zweck wurden Schnittstellen definiert, über die die Kommunikation aller Anlagen und Systeme eines modernen Gebäudes rea-

System	Sicherheitsbereich		Gebäudeinfrastruktur		Energiebereich		Gebäudeumgebung		Gebäudeinterior		Gebäudeexterior		Gebäudeanwendung	
	1	2	1	2	1	2	1	2	1	2	1	2	1	2
Kommunikation zwischen den Systemen (Zustandsmeldungen, Alarmmeldungen, etc., Datenvermittlung)														
Brandmeldetechnik														
Videotechnik														
Zutrittskontrolle														
Intrusionsschutz														
Heizung														
Sanitärtechnik														
Person- und Inventarortung														
IT-Infrastruktur														
Beleuchtung														
Lüftungs- Kimaetechnik														
Entrauchung														
Aufzüge, Fahrtrappen, Transportanlagen														
Sichere Stromversorgung														

Darstellung von technischen Verknüpfungsmerkmalen in Gebäuden

liert werden sollte. Diese Schnittstellen wurden als „logische Verknüpfungspunkte“ abgebildet. Sie dienen dazu das Minimum an bereitgestellten Informationen zu definieren.

Diese „Logischen Verknüpfungspunkte“, bei denen es sich um Informationssignale handelt, die die einzelnen Anlagen an das Managementsystem übertragen, wurden in einer Beziehungsmatrix mit den anderen Einzelsystemen logisch verknüpft.

Die Definition neuer Verknüpfungen allein reicht aber nicht aus. Denn nicht jede Verknüpfung hat den gleichen Stellenwert im Gesamtgefüge der Verknüpfungsmatrix. Es wurde deshalb zusätzlich ein System geschaffen, das jede Verknüpfung gewichtet. Da jede zusätzliche Verknüpfung einen größeren Administrationsaufwand auf der Managementebene bedeutet, wurden nur solche Verknüpfungen mit anderen Systemen definiert, die die Gebäudesicherheit signifikant steigern. Trotz dieser Einschränkung ist aber in der dargestellten Verknüpfungsmatrix (Siehe Seite 3 unten) die Diskrepanz zwischen den derzeit realisierten, grau hinterlegten Verknüpfungen und den zusätzlichen neu definierten (weil sicherheitstechnisch erforderlichen), blau hinterlegten mehr als deutlich.

Beispielszenario Branddetektion

Anhand eines einfachen, aber sehr aussagekräftigen Beispielszenarios lässt sich die Notwendigkeit der ganzheitlichen sicherheitstechnischen Betrachtungsweise

eindrucksvoll verdeutlichen. Für ein besseres Verständnis wird das oben genannte Szenario (siehe Grafik unten) grafisch dargestellt und die Vorteile der neuen ganzheitlichen Betrachtungsweise gegenüber der bisherigen Praxis werden kurz aufgezeigt.

Derzeitige Maßnahmen

Bisher stellt die Brandmeldeanlage (BMA) die Schaltstelle zur Branddetektion und Alarmierung dar. Die an die BMA angeschlossenen Melder und Anlagen, Rauchmelder, Wärmemeldersprinkleranlagen, unter Umständen Sprinkleranlagen, signalisieren einen Brand an die BMA. Diese alarmiert die Feuerwehr, löst die Hausalarmanlage (externe Signalgeber) aus und leitet bestenfalls das Alarmierungssignal an eine übergeordnete Stelle (das Gebäudemanagementsystem – wenn vorhanden) bzw. an eine ständig besetzte Stelle (z. B. Wachschutz) weiter.

Zukünftige Erweiterungen

Über die heutigen Signalisierungsmöglichkeiten hinausgehend sind jedoch weitere Quellen zur Brandortbestimmung sinnvoll. Damit ließe sich der Brandort sicherer und genauer bestimmen.

Das Auslösesignal der Sprinkleranlage, das softwareseitige Erkennungssignal des Feuers durch die Videotechnik sowie das gestiegene Raumtemperatursignal des Einzelraumreglers oder Raumtemperatursensors, die alle an das Managementsystem angeschlossen

sind, können die Brandmeldung der BMA ergänzen und ermöglichen dann eine sichere Branddetektion. Aufgabe des Managementsystems ist es jetzt, diese Brandmeldung dem Personal anzuzeigen und die weitere Vorgehensweise vorzugeben. Mit Hilfe des Videoüberwachungssystems kann der Bereich, in dem das Feuer signalisiert wurde, kontrolliert und überwacht werden. So lässt sich schnell und leicht das Ausmaß des Brandes feststellen. Darüber hinaus ist mit der Personensorge schnell herauszufinden, wie viele Personen sich im Gefahrenbereich aufhalten. Über die elektroakustische Anlage werden Evakuierungsdurchsagen gemacht, die entweder von der BMA oder vom Managementsystem gezielt eingesetzt werden. Durch die intelligente Steuerung der Fördertechnik fahren Aufzüge im Brandfall eine sichere Etage an und ermöglichen so eine sichere Evakuierung.

Fluchtwege führen auf dem kürzesten Weg ins Freie. Das dynamische Fluchtwegeleitsystem wird automatisch aktiviert, kennzeichnet zusätzlich den Fluchtweg und kann diesen situationsabhängig verändern. Somit ist die größtmögliche Sicherheit gegeben.

Eine wichtige Schutzmaßnahme, die meist vergessen wird, ist das Sperren aller Zufahrtswege zum Gebäude – auch der (Tief-)Garage, die in vielen Fällen weiter zugänglich ist. Nur Rettungskräfte sollten aber im Brandfall den vollständigen Zugang zum Gebäude haben.

Die kombinatorische Auswertung aller System- und Anlagenmeldungen mit Hilfe der im Managementsystem umgesetzten Verknüpfungsmatrix stellt nicht nur die Gesamtfunktion des Gebäudes sicher, sie erhöht zudem aktiv die Sicherheit des darin arbeitenden Personals.

Die TEKO Ingenieurbüro GmbH hat den Ansatz der ganzheitlichen Betrachtungsweise bei der Planung der neuen Sicherheitszentrale eines großen deutschen Versicherers bereits umfassend umgesetzt.



■ Rudi Grimm, Paul Grys, Jochen Hanke
TEKO Ingenieurbüro GmbH
rgrimm@teko.de

Sicherheitspass für Gebäude

Im Jahre 2006 wurde erstmals ein Energiepass für Gebäude eingeführt. Er soll die Verbraucher und Mieter objektiv über den Energieverbrauch eines Gebäudes informieren, Einsparpotenziale aufzeigen und den Energiebedarf von Gebäuden bundesweit unkompliziert vergleichbar machen. Die Vorteile liegen auf der Hand. Mit Hilfe des Energiepasses ist es möglich, sich ein umfassendes Bild über die Energiebilanz eines Gebäudes zu verschaffen.

Was für den Energieverbrauch jetzt üblich geworden ist, ist jedoch für die Sicherheit noch lange nicht selbstverständlich. Die fehlende objektive Beurteilung des Sicherheitszustandes eines Gebäudes, das Bruchliegen von nicht genutztem Sicherheitspotenzial der installierten sicherheitstechnischen Anlagen und ein nicht objektiv vergleichbares Sicherheitsempfinden zeigen die Notwendigkeit eines Sicherheitspasses ähnlich dem Energiepass.

Analyse-Tool

Mit dem neuen Analyse-Tool SEM (Sicherheit, Energie, Management) wurde eine Softwarelösung entwickelt, die die Erfassung und Bewertung des Sicherheitszustandes von Gebäuden nach der von TEKO entwickelten Gebäudetechnik-Verknüpfungsmatrix unterstützt.



Gebäudetyp

Das Tool analysiert den Sicherheitszustand eines Gebäudes anhand mehrerer Parameter. Der erste Parameter ist der Gebäudetyp. Dabei werden die Bereiche Verkehr (Flughäfen, Bahnhöfe), Freizeit (Versammlungsstätten, große Sport- und Freizeitstätten), kommerziell (Bürogebäude, sensible Verwaltungsge-

bäude) und Wohnen (Hotels, große Wohngebäude) unterschieden. In jedem Bereich bzw. bei jedem Gebäudetyp werden spezifische sicherheitstechnische Merkmale vorausgesetzt und deren Gewichtung festgelegt. Durch die Unterteilung hinsichtlich der Gebäudetypen wird die Verknüpfungsmatrix effizient ausgewertet. Eine Erweiterung auf andere Gebäudetypen (z. B. Fabrikanlagen) ist grundsätzlich machbar.

Vorhandene Systeme und deren Verknüpfung

Die weiteren Parameter, nach denen der Sicherheitszustand eines Gebäudes analysiert wird, sind die installierten sicherheitstechnischen Anlagen und Systeme und die bei ihnen realisierten Kommunikationsverknüpfungen. Mit der Umsetzung der beschriebenen Verknüpfungsmatrix im Analyse-Tool SEM kann die aktuelle Gebäudesicherheit beurteilt und in einen Score-Wert des Sicherheitspasses eingestuft werden. Darüber hinaus zeigt SEM nicht genutztes Sicherheitspotenzial auf. Zusätzlich werden Vorschläge unterbreitet, die die Sicherheit des zu untersuchenden Gebäudes effizient steigern und zu einer Erhöhung des Score-Wertes führen. Dadurch kommt es zu einer besseren sicherheitstechnischen Einstufung des Gebäudes.

Weitere Funktionen von SEM seien hier nur in aller Kürze aufgeführt:

- Analyse des Sicherheitszustandes von Gebäuden anhand des Gebäudetyps, der installierten Systeme und der realisierten Verknüpfungen
- Berechnung eines daraus resultierenden Sicherheitsindex (Score-Wert)
- Möglichkeit der Untersuchung von Ausbaumaßnahmen
- Berichte über den aktuellen sicherheitstechnischen Gebäudezustand und Verbesserung bei der Ausnutzung bestehender Anlagen
- Analyse und Auswertung aus energetischer Sicht

Vorteile einer Zertifizierung mit Sicherheitspass

Die Berechnung des Sicherheitsindex dient als Grundlage für die Zertifizierung, die folgende Vorteile bietet:

- Die Zertifizierung der Gebäudetechnik in ihrer Gesamtfunktionalität ermöglicht ein effektiveres Management zur technischen Gesamtfunktions-sicherung des Objekts.
- Sicherheits-Prävention schafft Vertrauen bei Behörden, Versicherern und Kunden.
- Erprobte Vorsorgemaßnahmen und szenarienbasierte Handlungsabläufe verringern den Schaden bei dennoch eintretenden Störfällen.
- Die systematische Betrachtung des aktuellen Zustandes verringert den Aufwand bei der Nachrüstung/Er-tüchtigung der Gebäudetechnik.



Die Notwendigkeit einer Zertifizierung mit dem Sicherheitspass zeigen die Vorfälle der jüngsten Vergangenheit im In- und Ausland. Durch intelligente Sicherheits-Sensorik mit der Integration vorhandener Datenbestände können Gefährdungen rechtzeitig aufgezeigt werden.

- Rudi Grimm
TEKO Ingenieurbüro GmbH
rgrimm@teko.de

Personenortung im Gebäude

Kerntechnologie nicht nur für Sicherheit

Die Ortung von Personen in Gebäuden ist ein eigenes, wichtiges Gebiet im Rahmen des großen Themas Gebäudesicherheit. Wer hier nur an Überwachung denkt, übersieht wichtige Einsatzfelder. So kann die Ortung dazu dienen, die Sicherheit von Feuerwehrlern zu erhöhen oder bei einem Notfall in einem Krankenhaus den rettenden Arzt schneller zu finden – um nur zwei Beispiele unter vielen zu nennen.

Nicht alle heute genutzten Ortungstechnologien funktionieren auch innerhalb eines Gebäudes. Die Firma Telematica e. K. hat sich im Rahmen des „Verbundvorhabens sicheres Gebäude“ intensiv mit diesem Thema beschäftigt. Zunächst wurden verfügbare Ortungstechnologien sowie aktuelle Weiterentwicklungen und Ansätze ausführlich analysiert - insbesondere hinsichtlich ihrer Eignung für den Einsatz im Gebäude. Ziel war es, auf der Grundlage geeigneter Technologien Systemkonzepte für die Indoor-Ortung zu entwickeln. Zwei der entstandenen Systemkonzepte konnten im Projekt erfolgreich umgesetzt und getestet werden.

Ortungs-Infrastruktur

Die Wahl einer Ortungslösung hängt stark von der Art des Gebäudes und seiner Nutzung ab. In öffentlichen Einrichtungen ergeben sich andere Einsatzszenarien als in Wohngebäuden. In einem Krankenhaus beispielsweise unterstützt die Positionsermittlung von Sicherheits- oder Servicepersonal deren schnellen und gezielten Einsatz. Systeme wie eine RFID-Lösung, die eine im Gebäude angebrachte Ortungs-Infrastruktur haben, sind hier sinnvoll. Über am Körper getragene Transponder können so beispielsweise in der Notaufnahme dringend benötigte Ärzte schneller gefunden werden.

In Wohngebäuden dagegen beschränkt sich der Einsatz auf die Unterstützung von Rettungskräften, beispielsweise im Brandfall. Der Einsatzleiter kann die Bewegungen der Feuerwehrmänner im

Gebäude beobachten. Gerade in Hochhäusern ist es wichtig zu wissen, in welcher Etage sich die Einsatzkräfte befinden. Benötigte Verstärkung kann so direkt zu ihnen geleitet werden.

Mobile Ortungssysteme

Eine Ausstattung der Wohngebäude mit Ortungs-Infrastruktur ist nicht sinnvoll, da die Ortung im alltäglichen Betrieb des Gebäudes nicht nötig ist. Zudem kann eine installierte Infrastruktur ausfallen, wenn es brennt. Hier kommen daher Systeme ohne Infrastruktur im Gebäude zum Einsatz.

Das Sensorsystem „Multi-Sensor-Box“ (MSB) der Firma Telematica e.K. ist am Körper zu tragen. Es vereint mehrere mobile Sensoren. Ein Beschleunigungssensor und ein Magnetometer liefern einer Navigationssoftware die Daten, mit deren Hilfe die Schritt- und Richtungserkennung durchgeführt wird. Über zurückgelegte Distanz und Richtung und auf der Basis integrierter Gebäudepläne kann die Fortbewegung von einem Ausgangspunkt aus nachvollzogen werden. Die Funktionalität der MSB konnte im Testszenario „Brandfall im Gebäude“ erfolgreich demonstriert werden. Der Test startete außerhalb des Gebäudes mit dem simulierten Eintreffen der Feuerwehr. Die Anfangsposition wurde über GPS ermittelt. Die Positionsbestimmung im Gebäude erfolgte ausschließlich anhand der MSB-Sensoren. Ein derartiges Sensorsystem ist auch in der Lage ungewöhnliche Bewegungsabläufe zu detektieren, z. B. einen Sturz mit anschließender Bewegungslosigkeit.

Hybride Lösungen

In großen Einrichtungen wie Flughäfen wäre eine flächendeckende Infrastruktur, die eine kontinuierliche Ortung ermöglicht nicht rentabel. Für Anwender in sicherheitskritischen Bereichen wie Sicherheitspersonal, Polizei, Bundespolizei oder Feuerwehr muss jedoch



eine stetige Ortung möglich sein. Sensorsysteme alleine reichen für diese Fälle nicht aus, da die fortlaufende Positionsbestimmung mit der Zeit immer ungenauer wird. Für diese Einrichtungen bietet sich eine Kombination unterschiedlicher Ortungslösungen an. Ein solches hybrides System kann über eine Verbindung fester Infrastruktur, wie RFID-Transponder, mit mobilen Sensoren realisiert werden. Die Firma Telematica e.K. hat in einer zweiten Testanwendung – dem Einsatz von „Sicherheitspersonal bei der Gebäudeüberwachung“ – hier eine Lösung entwickelt. Neben der MSB kamen im Gebäude installierte Bluetooth-Transponder zum Einsatz, mit deren Hilfe Stützpositionen für die Positionsberechnung bereitgestellt wurden. Die Verbindung von mobilen Sensoren mit Ortungs-Infrastruktur (Transpondern) ist eine Neuerung im Bereich der Personenortung und steigert die Positionsgenauigkeit über längere Zeit.

Gerade bei Anwendern in sicherheitskritischen Bereichen wie Feuerwehr, Polizei oder Sicherheitsdiensten besteht Nachfrage nach handlichen Ortungsgeräten, die außer- und innerhalb von Gebäuden funktionieren. Daher wird Telematica e.K. nach den erfolgreichen Tests im „Verbundvorhaben sicheres Gebäude“ ihre Ortungslösungen weiterentwickeln.

■ Antje Günther
Telematica e.K.
aguenther@telematica.de

Gebäudeautomatisierung und Gebäudesicherheit

Hilfsmittel für Prävention, Gefahrenbekämpfung und Personenrettung

Mit computergestützten Systemen der Gebäudeautomatisierung, sogenannten Computer Aided Facility Management Systemen (CAFM), werden Flächen, Räume und technische Infra-Struktursysteme in Geländen und Gebäuden geplant, verwaltet und dokumentiert. Durch sie werden Gebäude und deren Ausrüstung rationell betrieben, geschäftliche Kernprozesse effektiv unterstützt und Betriebskosten gespart.

Die Gesellschaft zur Förderung angewandter Informatik (GFai) hat im Rahmen des Berliner „Verbundvorhabens sicheres Gebäude“ neue Techniken für die Prävention, Gefahrenbekämpfung und Personenrettung entwickelt, die auf anerkannten CAFM-Technologien basieren.

Wichtige CAFM-Basisfunktionalitäten, die für das neue Managementsystem angepasst und erweitert wurden, sind die Flächen- und Komponentenverwaltung.

Die Flächenverwaltung ermöglicht etwa die Visualisierung von Nutzungsplänen nach DIN 277 (u. a. auch Verkehrsflächen). Daneben sind auch sicherheitsrelevante Parameter wie Brandschutz- und Brandbekämpfungszonen, Flächen nach zugeordneten Sicherheitskategorien oder die Verteilung von Brandlasten darstellbar. Da ein maßstabsgerechtes Gebäudemodell zugrunde gelegt wird, können die zugehörigen Flächen- und Rauminhalte berechnet werden (siehe Bild 1).

Die Komponenten der Sicherheitstechnik werden ortsgenau abgebildet. Gerätebeschreibungen, Beschaltungsinformationen, Herstellerdaten und Wartungsparameter sind zentral in einer Datenbank abgelegt und per Mausclick verfügbar.

Durch Einbindung der Steuerungs- und Regelungsebene ist die Anzeige von aktuellen Messdaten im Gebäudeplan möglich (siehe Bild 2).

Darüber hinaus wurde ein Verfahren entwickelt, das potenzielle Fluchtwege aus der Gebäudestruktur ableitet und, bezogen auf konkrete Gefahrensituationen, optimale Fluchtrouten berechnet (siehe Bild 3). Dabei werden die Lokalisierung von Brandherden und zusätzli-

chen Gefahrenpotenzialen (z. B. Lagerorte gefährlicher Stoffe) berücksichtigt.

■ **Dipl.-Math. Silvia Nitz**
GFai Gesellschaft zur Förderung angewandter Informatik e.V.
 nitz@gfai.de

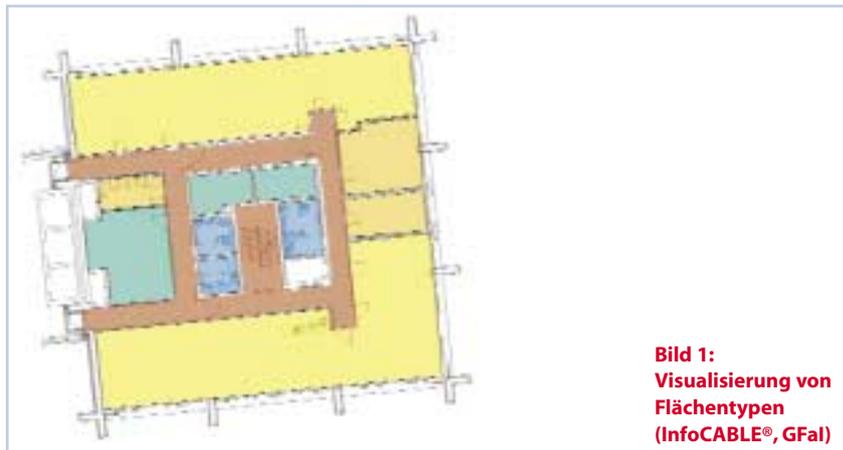


Bild 1:
Visualisierung von Flächentypen (InfoCABLE®, GFai)



Bild 2:
Anzeige aktueller Raumdaten (InfoCABLE®, GFai)



Bild 3:
Visualisierung von Fluchwegen (InfoCABLE®, GFai)

Steuerung der Gebäudesicherheit mit Embedded PC

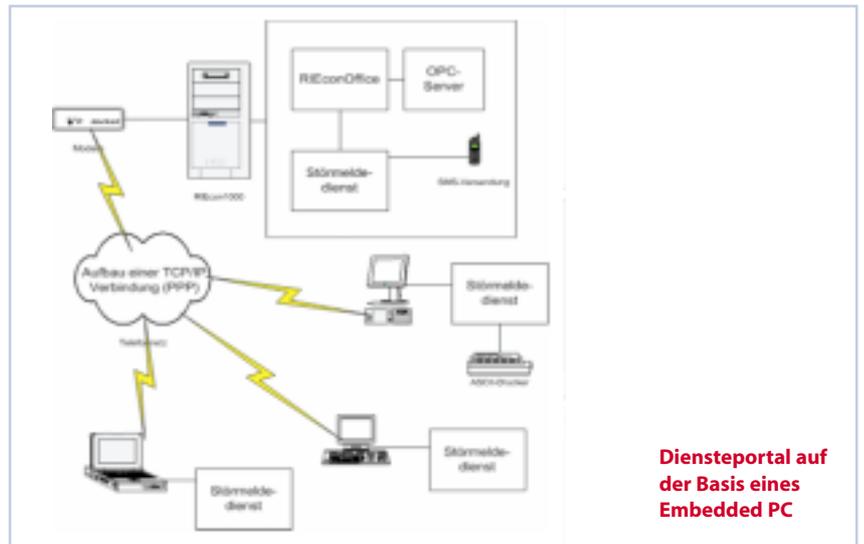
Vom Störmeldeserver zum Leittechnik-Dienstportal

„Lokaler Datenserver für haustechnische Anlagen“ heißt das Projekt, das von der Dr. Riedel Automatisierungstechnik GmbH im Rahmen des „Verbundvorhabens sicheres Gebäude“ konzipiert und erprobt wurde. Ziel war, eine übergeordnete Steuerung zur Gebäudesicherheit zu schaffen, die Daten unterschiedlicher Gewerke wie Gebäudeautomation, Fluchtwegesteuerung, Zugangskontrolle, Personenortung und Brandschutzanlagen nutzt. Bisher war eine derartige Steuerung nicht verfügbar, denn in den Systemen der Gewerkeanbieter fehlen lokale Datenserver mit offenen Kommunikationsstandards.

Charakteristisch für moderne Bauwerke ist, dass unterschiedlichste Aufgaben über vielfältige Zusammenhänge miteinander in Beziehung stehen. Dazu zählen beispielsweise:

- Klimatisierung (Heizung, Lüftung, Kühlung, Feuchtigkeitsregelung)
- Medienversorgung und -entsorgung (Elektrotechnik, Wasser/Abwasser, Gas, Kommunikationsmedien, Beleuchtung)
- Gebäudeschutz (Brand-, Einbruch- und Gefahrenmeldeanlagen, Löschanlagen, Entrauchungsanlagen, Zugangskontrollsystem, Videoüberwachung)
- Personenbeförderung (Rolltreppen, Aufzüge)

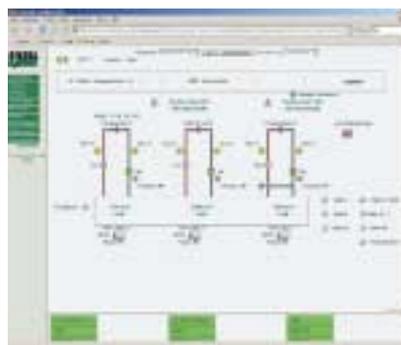
Die Dr. Riedel GmbH stand vor der Aufgabe, die Steuerung und Überwachung der verschiedenen Funktionseinheiten in ein Gebäudemanagementsystem zu integrieren. Die Lösung war ein Dienstportal (als Leittechnik- und Störmeldeserver) auf der Basis eines Embedded PC. Es übernimmt Aufgaben für die Gebäudeeigentümer, Serviceunternehmen und Sicherheitsdienstleister. Der Server lässt sich unter Zuweisung von Zugriffsrechten in Netzwerke einbinden und kommuniziert mit anderen Gewerke-Servern über eine standardisierte OPC-Softwareschnittstelle (OLE for Process Control).



Automatische Störmeldeerfassung

Die Bedienung erfolgt online über einen Standard-Internetbrowser. Die berechtigten Dienstleister können so von beliebiger Stelle aus auf die Daten zugreifen. Informationsbasis ist eine lokale Kommunikationsdatenbank, deren Prozessdaten auf HTML-Seiten visualisiert und zyklisch dynamisch eingeblendet werden. Damit wird die Fernüberwachung und -steuerung sowie die automatische Störmeldeerfassung (z. B. per E-Mail, SMS, Ticker/H-LT) aller angeschlossenen haustechnischen Prozesse ermöglicht. Die ausgewählten Prozessdaten werden archiviert und für die Auswertung aufbereitet.

Die Koppelung von Gefahreninformationen aus der Gebäudeautomation mit der Fluchtwegesteuerung und Perso-



BS-Plot: Dr. Riedel Automatisierungstechnik GmbH

nenortung wurde in enger Kooperation mit den Projektpartnern GFal und Telematica e.K. anhand eines Gebäudes der GSW in der Berliner Kochstraße durchgeführt. Die Beziehungsgeflechte in komplexen Systemen wurden anhand eines Brandszenarios beispielhaft dargestellt und gemeinsam mit den Projektpartnern getestet.

Im GSW-Haus wurde demonstriert, wie Informationen aus einem Gebäude aufgenommen, verarbeitet, weitergeleitet, visualisiert und umgesetzt werden und entsprechende Reaktionen auslösen. Im Katastrophenfall werden die Daten vom RIEcon Office System an das Infocable System der GFal übertragen. Es empfängt die Parameter der Melder und Temperatursensoren (Rauch- und Wärmemelder) aus der installierten Gebäudeleit- und sicherheitstechnik. Die Analyse der Informationen gibt Aufschluss über Position und Größe der Gefahrenquelle und darüber, welche Bereiche der Flucht- und Rettungswege beeinträchtigt sind. Das Dynamic Escape Routing (DER) übernimmt dabei eine intelligente, situationsbedingte Fluchtwegesteuerung. Es berechnet alternative Fluchtweg im Verkehrsweg des Gebäudes.

- Dr.-Ing. Manfred Riedel
Dr. Riedel Automatisierungstechnik GmbH
manfred.riedel@riedel-at.de

Terroristische Bedrohung und Gebäudesicherheit

Auch im Zeitalter der virtuellen Viren und trojanischen Pferde drohen Gefahren nicht primär aus dem Internet. Noch überwiegen eher die konventionellen Risiken. Sie weisen jedoch eine neue Qualität der Bedrohung auf. Erhöhte Gewaltbereitschaft, Sabotage und drohende Terrorakte sind hier die Stichworte.

Die Nutzung neuer Techniken in der Wirtschaftsspionage, bei Fälschungsdelikten und in allen Bereichen der Wirtschafts- und Betriebskriminalität durch Innetäter (oder zumindest unter deren Mithilfe) zwingen zu durchgängigen Verfahren und neuen Wegen in der Sicherheit. Besondere Bedeutung hat hier der Wissensschutz.

Gefährdungsanalyse

Die Gefährdungsanalyse dokumentiert den Grad und die Art des Gefährdungspotenzials eines Unternehmens, Gebäudes oder Areals. Kriterien wie Touristenmagnet, Symbolträchtigkeit, exponierte Lage, bauliche Beschaffenheit („Glaspalast“ oder „Betonblock“), „Public Viewing Area“, aber auch Kriegsteilnehmer im Irak zu sein, der Geschäftszweck oder die Art der hergestellten Produkte, schützenswerte Güter oder exponierte Personen zu beherbergen sind mögliche Gewichtungsfaktoren.

Sicherungskonzept

Das Sicherungskonzept legt den Schutz des Gebäudes nach Außen und der Werte der Unternehmung im Innern fest. Regelmäßige Penetrationstests der inneren und äußeren Absicherung testieren den Status quo der technischen, personellen und organisatorischen Schutzmaßnahmen eines Gebäudes. Schutz – besser „Security“ – sollte Teil eines integrierten und gelebten Managementsystems sein.

„Security-Management“ bedeutet die konkrete Umsetzung und Implementierung in das gesamt-unternehmerische Managementsystem. Es basiert auf kontinuierlicher Gefahren- und Risikoanalyse, Sicherstellung eines aktiven Grundschutzes, alltäglichem Monitoring und Reporting aller sicherheitsrelevanten Ereignisse und Ausführung angemessener prozessbegleitender Maßnahmen. Klare Verantwortungsbereiche und durchdachte Abläufe senken die Wahrscheinlichkeit von Schadensereignissen. Erprobte Vorsorgemaßnahmen verringern den Schaden bei dennoch eintretenden Schadensereignissen. Nachweisbare Abläufe und ausreichende Aufzeichnungen erleichtern die Abwehr unberechtigter Haftungsansprüche bis zur Exkulpation bei Strafverfahren. Diese Prävention schafft Vertrauen bei Behörden, Kunden und Nachbarn.

Die Gewährleistung der Unternehmenspflichten bildet die Basis für eine gerichtsfeste Organisation und damit die Grundlage eines proaktiven Risikomanagements. Auch Kreditgeber schauen vermehrt auf die Gesamtheit der Risiken.

Prophylaxe zählt

Nur ein integraler ganzheitlicher Ansatz führt zu Akzeptanz und erfolgreicher Prophylaxe mit Kostenersparnis. Aber alle Systeme sind immer nur so gut, wie die Mitarbeiter, die diese leben. Die QM-Schubladen der 20 Elemente sollten lange der Vergangenheit angehören. Sicherheit muss entlang existenziell relevanter Geschäftsprozesse geplant werden. Die stete Überprüfung der Notwendigkeit und Effektivität der implementierten Prozesse und Maßnahmen führt zu Nutzentransparenz (werteorientierte Messung). Wird diese optimal kommuniziert, trägt sie zu Sensibilisierung und damit kostenloser Prävention bei. Sicherheit ist 100 - X, ein stetiger Risikominderungsprozess.

■ Carsten Baeck
DRB Deutsche Risikoberatung GmbH
c.baeck@deutsche-risikoberatung.de

Das Gespenst der Haftung

Reduzierung von Haftungsrisiken im sicheren Gebäude

Sicherheit ist Chefsache. Seit Inkrafttreten des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) besteht ein Haftungsdurchgriff auf das Management – Geschäftsführer, Vorstand oder Aufsichtsrat sofern strategische, konzeptionelle oder operative Aufgaben verletzt werden. Die Versicherungswirtschaft hat dieses Risiko erkannt und bietet seitdem eine Vermögenshaftpflichtversicherung für die Unternehmensleitung, sogenannte „Directors & Officers Versicherungspolice“ an. Wie sehr ein solches Angebot nachgefragt wird, zeigt sich daran, dass die Versicherer nach Auftreten der ersten, nicht unerheblichen Haftungsfälle gezwungen waren, die Prämien beträchtlich zu erhöhen.

Rechtliche Verantwortlichkeit

Das KonTraG schafft bei Kapitalgesellschaften zusätzliche Risiken, führt jedoch zu größerer Kontrolle und Transparenz. Das Gesetz verpflichtet Aktiengesellschaften und GmbHs zur Einrichtung eines Überwachungssystems, das bestandsgefährdende Risiken frühzeitig erkennen und bewältigen hilft. Von Bedeutung ist die Möglichkeit, den Vorstand, die Geschäftsführung oder sogar den Aufsichtsrat unmittelbar haftbar zu machen.

Als Gegenmaßnahme kann der Vorstand bzw. die Geschäftsführung ein Risikomanagement-System einrichten. Da die Haftung an ein Verschulden und damit zumindest an eine wissentliche Pflichtverletzung anknüpft, wird damit ein Mittel zur Beherrschung und Minimierung potenzieller Haftungsrisiken geschaffen.

Haftungsmatrix

Um ein Risikomanagement-System einzurichten, ist es zwingend erforderlich zunächst die Haftungsrisiken zu systematisieren. Dafür wird eine unternehmensspezifische Matrix erstellt. Ein Risiko Management-System besteht aus fünf Stufen:

1. Risiko-Identifikation

Die Identifikation der Risiken dient der individuellen Erstellung des Risikoprofils des Unternehmens. Das Risikoprofil ergibt sich aus der systematischen Erfassung von Gefahrenquellen, Schadensursachen und Störpotenzialen sowie der Strukturierung in Risiko-Kategorien zur Festlegung von Frühwarnindikatoren.

2. Risiko-Bewertung

Nach der Identifikation der Risiken sind diese konkret zu bewerten. Die Bewertung umfasst die Ermittlung des Ausmaßes der einzelnen Risiken sowie die Wahrscheinlichkeit der Risikoverwirklichung. Das Risiko lässt sich mathematisch in folgender Formel ausdrücken: Schadenserwartungswert = Schadenshöhe x Schadenswahrscheinlichkeit.

3. Risiko-Steuerung

Auf der Grundlage der Identifikation und Bewertung sind aktive Reaktionsmöglichkeiten im Sinne einer Risiko-Steuerung festzulegen. Ziele sind die Vermeidung und Verminderung von Risiken durch die Etablierung von geeigneten Maßnahmen. Daneben sind Schritte der Risikoüberwälzung – z. B. Outsourcing – und der Risikokompensation – z. B. Versicherungsschutz – in Erwägung zu ziehen.

4. Risiko-Überwachung

Die ständige Veränderung in einem Unternehmen schafft die Notwendigkeit der Risikoüberwachung. Hierzu ist anhand der Beurteilung der aktuellen Risikosituation unter Berücksichtigung laufender Veränderungen ein permanenter Soll-/Ist-Abgleich vorzunehmen.

5. Risiko-Controlling

Das Risiko-Controlling als Kern des Risikomanagement-Systems ist Chefsache. Identifikation, Bewertung, Steuerung und Überwachung können fachspezifisch zugeordnet werden. Das Risiko-Controlling aber, d. h. die Überwachung des Risikomanagement-Kreislaufes, muss durch das Management erfolgen. Das Management hat zudem den Aufsichtsrat bzw. Beirat laufend zu informieren. Zur rechtswirksamen Abwehr

von Haftungsrisiken ist die permanente Dokumentation der einzelnen Elemente der Haftungsmatrix sowie die Erfüllung der Überwachungsfunktionen zu gewährleisten.

Risikomanagement und Gebäudesicherheit

In dem Umfang, in dem gebäudetechnische Systeme mit Raumautomation eingeführt und diese Systeme in einer Verknüpfungsmatrix komplex zueinander in Beziehung gesetzt werden, entsteht ein quasi-automatisches Risikomanagement-System.

Erst die Verknüpfung unterschiedlicher Systeme schafft die Voraussetzung einer Risiko-Bewertung (z. B. Temperaturerhöhung und Selbstentzündungsgefahr), die Möglichkeit der Risiko-Steuerung (z. B. automatisches Öffnen und Schließen von Bereichen) und die Möglichkeit der Risiko-Überwachung (z. B. optisch durch Kameras oder physikalisch durch Zutrittskontrolle). Die Erfassung und intelligente Nutzung aller Eigenschaften der installierten Gebäudetechnik über eine Schnittstelle stellt daneben eine grundlegende Lösung für ein Risiko-Controlling dar.

Das für die Gebäudewirtschaft entwickelte Konzept ermöglicht es, die Risiken auch rechtlich beherrschbar zu machen. Die damit einhergehende Dokumentation der Einzelschritte der Prävention und Steuerung dienen aktiv einer rechtlichen Haftungsabwehr. Das Management kann mit Verweis auf die Einführung des Konzepts den Vorwurf einer wissentlichen Pflichtverletzung widerlegen. Eine Zertifizierung des Konzepts bildet zudem den Vorteil eines argumentativen Ansatzes für die Neuverhandlung von Versicherungsprämien.

■ Dr. Frank A. Hammel
Knauthe Eggers, Rechtsanwälte Notare
hammel@knauthe-eggers.com

Selbstorganisierende Gebäudeautomationsysteme

Forschungsprojekt „SOGAS“

Die Idee für das neue Projekt „SOGAS“ setzt auf den Ergebnissen des „Verbundvorhabens sicheres Gebäude“ auf, will aber mit der Integration von kommunikationsfähigen Geräten und Sensorik noch einen Schritt weitergehen.

Dazu werden zwei Eigenschaften betrachtet, die bisher als unveränderliche Grundlage eines jeden Gebäudeautomationssystems galten:

- der statische Aufbau eines solchen Systems, das sich nur verändert, wenn Komponenten neu installiert oder demontiert werden und
- die Immobilität der Komponenten eines Gebäudeautomationssystems.

Beide Eigenschaften erscheinen zunächst sinnvoll, da Veränderungen des Systems selten und Sensoren und Aktoren ortsgebunden sind.

Immer mehr Kommunikationsgeräte

Verfolgt man aber den Gedanken der ganzheitlichen Sicht auf ein Gebäude über den Ansatz des „sicheren Gebäudes“ hinaus, ergibt sich ein verändertes Bild: Die Menge an kommunikationsfähigen, tragbaren Geräten sowie deren mögliche Netzzugänge haben sich in letzter Zeit enorm erhöht. Hatten wir vor einigen Jahren lediglich ein Handy, mit dem über das GSM-Netz telefoniert werden konnte, können heutige Geräte über verschiedene Weitverkehrs-Funknetze wie GPRS und UMTS kommunizieren und verfügen gleichzeitig über Schnittstellen zu lokalen Funknetzen wie z. B. Bluetooth. Auch die Anzahl weiterer tragbarer, kommunikationsfähiger Geräte, über die ein berufstätiger Mensch im Durchschnitt verfügt, ist gestiegen. Neben dem eben schon erwähnten multifunktionalen Handy gehören meist ein Bluetooth- und WLAN-fähiger Laptop und ein PDA, der ebenfalls mit diesen beiden Kommunikationsschnittstellen ausgerüstet ist, zur Arbeits- und zunehmend zur Freizeit-ausstattung vieler Menschen. Verfolgt man diesen Trend, ist zu erwarten, dass

in diese oder ähnliche Geräte zukünftig weitere Kommunikationsschnittstellen, wie beispielsweise RFID oder auch Sensoren zur Temperaturmessung oder Messung der Helligkeit, z. B. zur optimalen Regelung der Hintergrundbeleuchtung eingebaut werden.

Dynamische Einbindung

Dieser Entwicklung folgend, ist es das Ziel des Projekts „SOGAS“, in die ganzheitliche Sicht über die Sensoren und Aktoren in einem Gebäude auch die beweglichen, sich temporär in dem Gebäude befindlichen kommunikationsfähigen Geräte und Sensoren zu integrieren. Handys, PDAs, in Zukunft auch Wearables, also Kleidungsstücke, in denen Sensorik, Aktorik oder Kommunikation integriert sein können, werden beim Betreten des Gebäudes automatisch in das Gebäudeautomationssystem aufgenommen. Genau wie sich durch die ganzheitliche Sicht auf alle Gebäudeautomationssysteme in dem „Verbundvorhaben sicheres Gebäude“

eine Reihe von „hidden functions“ ergeben, ist auch durch die dynamische Einbindung mobiler Geräte eine weitere Zunahme der Funktionalität zu erwarten.

Breite Nutzung

Die Nutzungsmöglichkeiten erscheinen vielfältig. Mitarbeiter, aber auch Besucher einer Firma benötigen keine Chipkarte mehr für das Zutrittskontrollsystem, sondern können über ihr Handy identifiziert werden.

Vor dem Besuch einer gefährdeten Person wird ein Gebäude mit teuren, hochsensiblen, tragbaren Sprengstoffsensoren abgesucht. Sind die Sensoren in das Gebäudeautomationssystem integriert, kann im Alarmfall das System sofort mit dem entsprechend definierten Szenario reagieren, z. B. dem Abriegeln eines Bereichs.



Im Alarmzustand eines Gebäudes, z. B. bei Brand oder Gasalarm, unterstützt das Gebäudeautomationssystem das Auffinden und Öffnen von Rettungswegen für die im Gebäude befindlichen Personen. Auch Funktionen können dann gesperrt sein, wie z. B. das Anschalten elektrischer Geräte bei Gasalarm oder das Öffnen von Türen, die zum Brandherd hinführen. Ein Feuerwehrmann, der sich zum Haus bewegt, kann vom Gebäude über die Kennung eines in seiner Kleidung eingearbeiteten Chips als Feuerwehr erkannt werden. Über die temporäre Integration in das Gebäudeautomationssystem werden ihm an seinem jeweiligen Aufenthaltsort Rechte eingeräumt, die eine andere Person nicht hat. Nur er ist in der Lage jede Tür in jede Richtung zu öffnen, Geräte zu schalten oder Lüftungsklappen zu steuern.

Nicht in jedem Fall spielt die Mobilität eine Rolle. Manche Sensoren müssen nicht ständig Daten liefern, sondern werden dynamisch in das System aufgenommen. Dies geschieht, wenn eine Kombination bestimmter Umgebungsparameter gegeben ist, die eine potenzielle Gefahr signalisiert, welche ab diesem Zeitpunkt kontrolliert werden muss.

Sicherheit im Mittelpunkt

Besonderes Augenmerk wird im Projekt „SOGAS“ auf den Aspekt der Sicherheit gelegt werden. Zum einen ist es das Ziel, die Gebäude selbst durch den Einsatz von gebäudetechnischer Telematik sicherer zu machen. Zum zweiten muss genau untersucht werden, welche Abhängigkeiten zwischen Systemen, Sensoren, Aktoren und sämtlichen Parametern im Haus und in seiner Umgebung bestehen. Denn es gibt nicht nur die erwünschten „hidden functions“, sondern auch „hidden traps“, also versteckte Fallen. Als dritter Aspekt der Sicherheit müssen Ausfallsicherheit und Manipulationssicherheit untersucht werden.

Sprengstoff-Sensor

Handy-Identifizierung

etc.

SOGAS Middleware

Gebäudeautomationssystem

Fähigkeit zur Selbstorganisation

Neben der funktionalen Herausforderung stellt sich noch eine weitere, rein technische. Die Forderung nach Selbstorganisationsfähigkeit für das zukünftige Gebäudeautomationssystem legt nahe, die neusten Erkenntnisse aus sich selbst konfigurierenden Funknetzen einzubeziehen und damit ein gleiches technisches Niveau zwischen bisher ganz verschiedenen Systemansätzen zu erreichen.

Elektronische Systeme, die die Funktionssicherheit von Gebäuden unter den aktuellen Nutzungs- und Umweltbelastungen direkt messbar machen, sind bisher nicht bekannt. Grundlagenforschung auf diesem Gebiet fehlt generell. Die Forschungen des Projektes in Richtung der Kontextsensibilität von Gebäudeautomationslösungen sollen im Zusammenhang mit den Erkenntnissen aus dem „Verbundvorhaben sicheres Gebäude“ hier erstmals Wissen erschließen, um später zertifizierbare Sicherheits-Überwachungssysteme auf diesem Gebiet entwickeln zu können.

SOGAS Middleware

„SOGAS“ soll mit einer möglichst breiten Basis existierender Gebäudeautomationssysteme zusammenarbeiten, die untereinander nicht kompatibel sind. Außerdem müssen die statischen Strukturen der existierenden Gebäudeautomationssysteme um dynamische erweitert werden, ohne das jeweilige System selbst zu verändern. Eine mögliche Lösung für die beiden letztgenannten Punkte kann eine SOGAS-Middleware sein, die zwischen den Gebäude-

automationssystemen und den Applikationen der mobilen und dynamischen Komponenten eingesetzt wird und dort die jeweils andere Schicht simuliert. „SOGAS“ wird sich zusätzlich zu den Grundlagen für selbstorganisierende Gebäudeautomationssysteme auch mit deren Funktionsprinzipien, Infrastrukturen, der Koexistenz von mobilen Systemteilen mit festprogrammierten sowie den dafür notwendigen Sicherheitskonzepten beschäftigen. Es will ermitteln, welche neuen Methoden und Verfahren erforderlich sind, um die Gebäudeautomation „mobiler“ zu gestalten. Damit wird ein weiterer logischer Schritt in Richtung eines sicheren, automatisierten Gebäudes getan.

■ Prof. Birgit Wilkes
Technische Fachhochschule Wildau
bwilkes@igw.tfh-wildau.de

Gut und sicher wohnen

Zum Sicherheitsstandard in Berliner Wohngebäuden

Sicherheit ist Lebensqualität. Sich in der eigenen Wohnung und in deren Umfeld sicher zu fühlen, ist ein menschliches Grundbedürfnis. „Gut und sicher wohnen“ ist das Motto der Mitgliedsunternehmen des Verbandes Berlin-Brandenburgischer Wohnungsunternehmen e.V. (BBU) und des Bundesverbandes deutscher Wohnungs- und Immobilienunternehmen.

Der Sicherheitsstandard in Berliner Wohngebäuden ist generell hoch, in Einzelfällen aber muss etwas getan werden. Für Wohnungsunternehmen ist „Sicherheit“ ein zentrales Thema. Gehandelt werden muss, wenn in Kellern oder Sicherungskästen Brände gelegt werden oder Gruppen, beispielsweise von Jugendlichen, auf die Bewohner des Gebietes subjektiv bedrohlich wirken. Sicherheit, Sauberkeit und Service sind für die meisten Menschen die Voraussetzungen für ein angenehmes Wohnen. Für die Wohnungsunternehmen gibt es sechs wesentliche Gründe, die Sicherheit in Wohngebäuden und Wohnsiedlungen zu fördern:

- Verkehrssicherungspflicht
- Sicherheit im Alter
- Sicherheit von Alleinstehenden
- Brandschutz (Sicherheit vor Bränden)
- Havarieschutz (Sicherheit bei Material- oder Anlagenversagen)
- Schutz vor ungeplanten Kostensteigerungen – Kostensicherheit insbesondere bei den Verwaltungs-, Instandhaltungs- und Betriebskosten

Subjektives Sicherheitsgefühl fördern

Unsicherheit wird gekennzeichnet durch Schutzlosigkeit, Handlungsunsicherheit und Ungewissheit. Daher ist die Förderung des subjektiven Sicherheitsgefühls für die Wohnungswirtschaft unabdingbar. Dazu gehört auch eine positiv verstandene Nachbarschaftskontrolle. Denn Sicherheit bedeutet mehr als nur Abwesenheit von unmittelbarer Bedrohung durch Gewalt und Kriminalität.

Der Bundesverband deutsche Woh-

nungs- und Immobilienunternehmer nennt positive Beispiele und Strategien zur Erhöhung der Sicherheit:

- Sicherheit im Sinne der Verminderung oder Beseitigung von Schutzlosigkeit, z. B. durch technische Sicherheitsvorkehrungen oder einem Wachdienst
- Sicherheit im Sinne der Verminderung oder Beseitigung von Handlungsunsicherheit – z. B. durch die Vereinbarung von Regeln in einer Nachbarschaft oder die Lösung von Konflikten
- Sicherheit im Sinne der Verminderung oder Beseitigung von Ungewissheit – z. B. durch ein sicheres Wohnverhältnis oder ein Netzwerk aus Kontakten zu Nachbarn, die im Bedarfsfall Unterstützung bieten

Sicherheit kann also durch städtebauliche, architektonische und bautechnische Maßnahmen gestärkt werden. Wichtig sind aber auch Beratungs- und Betreuungsangebote für die Mieter und Maßnahmen zur Integration sowie die Verbesserung sozialer Infrastruktureinrichtungen. Die Erhöhung von Sicherheit ist auch durch die Förderung von Bürgerverantwortung, Nachbarschaftsnetzwerken sowie durch Unterstützung und Ermutigung von Bewohnern zu eigenem Handeln erreichbar.

Stärkung des Sicherheitsgefühls der Mieter

Für die Wohnungsunternehmen ergibt sich die Aufgabe, mit moderner Sicherheitstechnik den Schutz von Wohnungen und Gebäuden zu verbessern. Das Sicherheitsgefühl der Mieter lässt sich durch übersichtliche und freundliche Gestaltung der Außenbereiche, Eingänge und Treppenhäuser wirksam stärken. Dazu gehört auch die Beseitigung von Graffiti, Müll oder Vandalismusschäden. Darüber hinaus kann eine Sicherheitsberatung durch die Polizei und der Einsatz von Wachdiensten Sicherheit vermitteln. In Initiativen wie „Wachsamer Nachbarn“ engagieren sich Bewohner für mehr Sicherheit im Quartier. Auch Pfortnerlogen können dazu beitragen,

dass die Regeln des Zusammenlebens eingehalten werden. Moderation stärkt die Fähigkeit der Mieter, Nachbarschaftskonflikte konstruktiv zu lösen. Kommunikationsfördernde Raumstrukturen wie Gemeinschaftsräume schaffen Kontakte und ermöglichen soziale Kontrolle. Durch Sozialmanagement und zielgruppenorientierte Angebote wird Mietern geholfen, die sich in Problemlagen befinden, und das Zusammenleben in der Nachbarschaft erleichtert.

Handlungsbedarf

Die Entwicklung neuer Informations- und Kommunikationstechniken bietet hervorragende Möglichkeiten, den Komfort in den Wohnungen, aber auch das subjektive Sicherheitsgefühl weiter zu stärken. Beispielhaft sind das Bamberger Projekt SOPHIA (Soziale Personenbetreuung – Hilfen im Alltag) zur besseren Betreuung der in den angestammten Wohnungen alt werdenden Mieter. Es beruht auf der bewohnergestützten Kommunikation mit einer Sozialstation über den Fernseher mittels einer Telefon- oder Breitbandkabelinstallation. Im Projekt „Smarter Wohnen“ setzt die Wohnungsbaugenossenschaft HWG Hattingen eG technische Lösungen um, die das Wohnen sicher und komfortabel machen und veränderten Lebenssituationen gerecht werden. Diese umgesetzten Lösungen dienen nicht allein der Komfortverbesserung, sondern führen auch zur Reduzierung von Umweltbelastungen und Energiekosten.

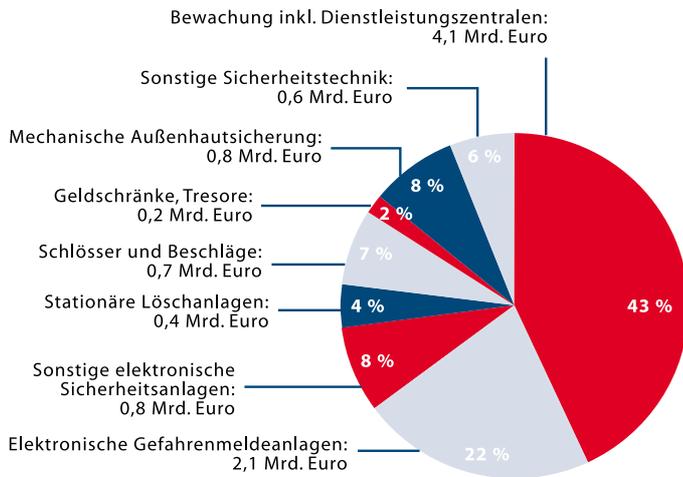
Letztlich tragen Lösungen im Zuge des vom Verband BBU unterstützten „Vernetzten Wohnens“ auch zur Sicherheit in den Beständen bei, wenn es beispielsweise darum geht, zur Brandvermeidung beizutragen, eventuell entstehende Brände frühzeitig zu erkennen und richtiges Verhalten im Brandfall zu vermitteln.

- **Siegfried Rehberg**
GdW Bundesverband deutscher Wohnungs- und Immobilienunternehmen e.V., Berlin
siegfried.rehberg@bbu.de

Sicherheitsmarkt in Zahlen

Sicherheitsmarkt in Deutschland 2003

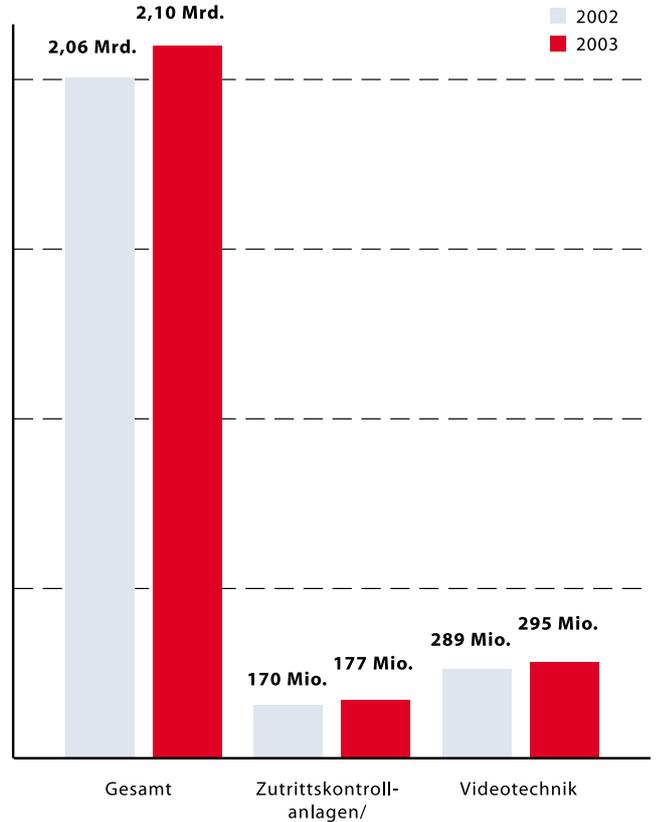
(Gesamtmarkt: 9,7 Mrd Euro)



Quelle: BDWS und SECURITY-Beirat, Messe Essen, Stand 25. Juni 2004

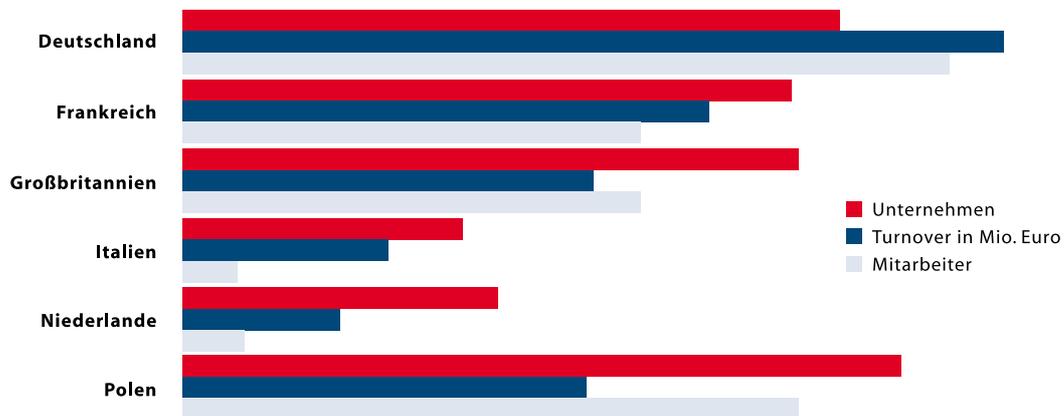
Markt für elektronische Sicherheit in Deutschland

(in Euro)



Quelle: Zentralverband Elektrotechnik und Elektronikindustrie e.V.

Die europäische Sicherheitsindustrie in Zahlen



Quelle: Confederation of European Services (Co ESS)

Berlin – eine Hauptstadt mit Sicherheit

Projekt Zukunft unterstützt „Sicherheit mit IT“

Die Notwendigkeit unserer Technologieinitiative „Sicherheit mit IT“ wird leider immer wieder durch tragische Ereignisse unterstrichen: Attentate terroristischer Gruppen, Erpressungsversuche der öffentlichen Hand mit Gift, Zusammenbruch der Energieversorgung oder der Einsturz von Gebäuden sind Beispiel dafür, dass es einen Bedarf an verbessertem Schutz wie an verbesserter Vorsorge und Überwachung gibt. Mancher Schadensfall wäre durch eine intelligente Überwachung zu verhindern, Menschenleben zu retten gewesen.

Gerade die Lösungen aus dem „Verbundvorhaben sicheres Gebäude“ zeigen Ansätze für neue, zukunftsfähige Konzepte, die mittelfristig auch kostendämpfend wirken werden. Allein durch die Datenintegration bisher unabhängiger Gebäudetechniksysteme lässt sich ein Mehr an Informationen über den Gebäudezustand gewinnen, ohne dass neue Systeme aufwändig nachinstalliert werden müssen.

Auch aus den anderen Arbeitsgruppen der Sicherheitsinitiative, der Produktionssicherheit, der Dokumentensicherheit, der Biometrie sowie dem Sicherheitsmanagement von Großveranstaltungen liegen interessante Lösungen vor, die sich nun am Markt etablieren müssen. Die Gesetzgebung (z. B. Videoüberwachung und Speicherung) ist in Bewegung, so dass Systemlösungen hier eine Chance bekommen.

Die Ergebnisse des Verbundvorhabens sprechen ganz eindeutig für ein Sicherheitszertifikat von Gebäuden. Jedes Spielzeug, jedes Flugzeug wird auf Herz und Nieren geprüft und technisch abgenommen. Warum nicht auch ein Gebäude?



■ **Dr. Wolfgang Both**
Landesinitiative Projekt Zukunft
wolfgang.both@senwaf.verwalt-berlin.de



Technologieinitiative „Sicherheit mit IT“

von Projekt Zukunft

Im Rahmen der Technologieinitiative „Sicherheit mit IT“ von Projekt Zukunft erarbeiten Forscher, Entwickler und Anwender vernetzte Systeme, die aus einem Nebeneinander einzelner Sicherheitslösungen eine integrierte und intelligente Sicherheitstechnik schaffen. Über die Kombination von Technologie- und Systemlösungen soll eine neue Qualität der Kommunikation, der Datenaufbereitung und ihrer Verwertung erzielt werden. In mehreren Anwendungsfeldern wie „Gebäudesicherheit“ oder „Produktionssicherheit“ entstehen bereits jetzt kommerzielle Lösungen. Die Technologieinitiative bietet hierfür eine hervorragende Plattform.

Zahlreiche Firmen und Forschungseinrichtungen in Berlin besitzen beim Thema „Sicherheit mit IT“ Kompetenz und Expertise. Sie sind Entwickler und Lieferanten für öffentliche und private Nachfrager für Bedarf an Sicherheitslösungen. Ihr Leistungsspektrum, aber auch die Vision von neuen Angeboten hat

die Technologieinitiative im folgenden für Berlin wichtigen Anwendungsfeldern aufbereitet:

- Kompetenzzentrum Biometrie
- sicheres Gebäude
- sicheres Dokument
- Sicherheit in der Produktion
- Sicherheitsmanagement für Großveranstaltungen

„Verbundvorhaben sicheres Gebäude“

Das „Verbundvorhaben sicheres Gebäude“ im Rahmen der Technologieinitiative „Sicherheit mit IT“ will eine der Öffentlichkeit zugängliche, wissenschaftlich gestützte Test- und Informationsplattform für gewerkeübergreifende Systemlösungen der Gebäudesicherheit schaffen. Die Plattform soll zu einem ständigen Arbeitsinstrument von Investoren und Planern moderner Gebäude werden.

Wichtige Links:

- www.projektzukunft.berlin.de
- www.probuilding.de
- www.sicherheit-mit-it.de
- www.akus.org
- www.its-pro.info
- www.identsys.de

■ Kontakt

Senatsverwaltung für Wirtschaft,
Arbeit und Frauen
Geschäftsstelle Projekt Zukunft
10820 Berlin

Dr. Wolfgang Both
Tel.: 030/9013-8257
Fax: 030/9013-7478
E-Mail: projektzukunft@senwaf.verwalt-berlin.de

www.projektzukunft.berlin.de

Öffentlichkeitsarbeit:
index
Tel.: 030/390 88 300
projekt-zukunft@index.de



Projekt Zukunft wird durch den Europäischen Fonds für regionale Entwicklung (EFRE) kofinanziert.