

# Gefahrenmanagementsysteme Web-basierte Lösungen prägen den Markt

Von Ulrich Sobers, Duisburg

**G**eht nicht – gibt's nicht. Anders als noch vor einigen Jahren sollte es bei Anlagen, die auf dem aktuellen Stand der Technik sind, keine Hemmnisse mehr geben, unterschiedlichste Sicherheitskomponenten in ein funktionsfähiges Gefahrenmanagementsystem zu integrieren. BACnet und OPC haben sich als Protokolle durchgesetzt, die Nutzung wird durch Web-basierte Lösungen erleichtert, die eine Bedienung an beliebigen Arbeitsplätzen erlaubt.

Sicherheitstechnik ersetzt seit bald 20 Jahren immer mehr Überwachungs- und Schutzfunktionen, die einst von Menschen wahrgenommen wurden. Mit zunehmender Gefährdung und von außen auferlegten Sicherheitsanforderungen wuchs die Anzahl der Unternehmen und Liegenschaften, in denen sicherheitstechnische Komponenten verbaut werden, gleichzeitig aber auch die Zahl der verschiedenartigen Lösungen für immer neue Aufgaben. Angriffe auf Einrichtungen förderten die Verwendung von Einbruchmeldetechnik und Zugangskontrolle, Brandschutzanforderungen die Nutzung von Lösch- und Meldetechnik. Umweltschutz und Gefahrguthandling schufen Datenbank basierte Alarmierungseinrichtungen etc.. Alle diese Systeme wollen bedient sein und sollen im Bedarfsfall im Zusammenspiel auch Menschenleben retten. Die klassische Zentrale mit dem Sozialposten „Pfortner“ hat bei den heutigen Anforderungen an die notwendige Informationsverarbeitung ausgedient, weil sie diese nicht mehr bewältigen kann. Deshalb ist heutzutage jedes Unternehmen, das mehr als ein Gefahrenmeldesystem betreibt, potenzieller Kandidat für den Einbau eines Gefahrenmanagementsystems. Die Anforderungen an neue Leitsysteme sind heute daher vor allem die Dezentralisierung der Informationsverarbeitung, ergonomische Gestaltung der Bedienoberflächen und die freie Aufschaltmöglichkeit für beliebige Subsysteme.

## Ein Blick zurück

Was heute bei der Neueinführung von Gefahrenmanagementsystemen gefordert wird, war bis vor wenigen Jahren noch eine Herkulesarbeit für den zuständigen Planer oder Berater. Wer vor ca. 15 Jahren versucht hat, unterschiedliche Sicherheitseinrichtungen bzw. Sicherheitsanlagen miteinander zu verschalten, beispielsweise um Personen und Materialströme in Gebäuden zu leiten, der bekam nicht selten Probleme mit dem Kunden, weil es Vorschriften und Regelwerke gab, die dies verboten. In der Praxis konnten diese dazu führen, dass sich unterschiedliche Sicherheitseinrichtungen gegenseitig aushebelten und gravierende Sicherheitslücken in der Objektsicherheit entstanden. Ein Beispiel sind die unterschiedlichen Aufgaben von Einbruchschutz und Zugangskontrolle, die damals nicht in den Griff zu bekommen waren. Wurde versucht, die Einbruchmeldetechnik mit der Zustandskontrolle einer Tür zu verknüpfen, verstieß dies gegen VdS-Vorschriften. Wurde dagegen VdS-konform gearbeitet, musste die Einbruchmeldeanlage bei Publikumsverkehr in Gebäuden abgeschaltet werden. Das Resultat waren gravierende Sicherheitsmängel aufgrund fehlender Überwachung zu Tageszeiten, in denen diese dringend notwendig waren. Solche Probleme, insbesondere auch in der Bankensicherheit waren es, die die Fachgremien letztlich zum Umdenken und zur Neugestaltung der Vorschriftensammlungen bewegten und so den Weg für die ersten Gefahrenmanagementsysteme ebneten.

In der Anfangsphase, in der mit vielen Software-Macken und Schnittstellenproblemen zu kämpfen war, konzentrierte sich die Entwicklung auf so genannte Sicherheitsleitstände, die bis auf Ausnahmen bei wenigen Unternehmen in der Pfortnerzentrale installiert wurden, meist Mehrbildschirm Lösungen zur Darstellung von grafischen und inhaltlichen

Informationen. Daraus entstanden eine ganze Reihe von Problemen. An erster Stelle war dies oft die fehlende Qualifikation des Pfortnerpersonals, das nicht selten mit der Abarbeitung der eingehenden Meldungen und der Informationsflut auf den Bildschirmen überfordert war und die teuren Managementsysteme somit nicht richtig nutzen konnte. Die Problematik wurde meist dadurch verschärft, dass auf diese ständig besetzte Stelle gleichzeitig auch noch die Meldungen aus der Gebäudeleittechnik aufgeschaltet wurden. Ein weiteres großes Problem war, dass viel zu viele Meldungen immer nur zentral aufriefen und bearbeitet werden mussten, selbst wenn die eigentlich für die Abarbeitung zuständige Stelle ganz woanders im Unternehmen angesiedelt war. Anbindungen an weiterleitende Informationssysteme zur Entlastung des Pfortnerpersonals waren zunächst eher eine Ausnahme.

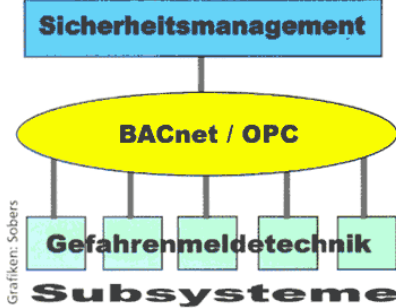
Auch die Schnittstellenprobleme zwischen den unterschiedlichen Sicherheitstechniken hatten Auswirkungen. Bei der Implementierung von Gefahrenmanagementsystemen in Unternehmen mussten deshalb Lösungen aus einer Hand bevorzugt werden, um die Realisierung eines Projektes nicht zu gefährden. Das Risiko, an 3rd Party Firmen zu geraten, die funktionierende Schnittstellen versprochen, diese aber nicht realisieren konnten, war insbesondere den externen Beratern zu hoch.

Das Vorbild für die Lösung der Probleme war aber schon Mitte der 90er Jahre in Sicht, die Disaster Management Systeme. Diese verteilen anhand von vorgegebenen Ablaufplänen in einem Schadens- oder Alarmfall Browserbasiert Informationen an Netzwerkadressen und überwachen die Rückmeldungen während der Abarbeitung der gespeicherten Szenarien. Diese Netzwerk-Lösung war nur noch auf die Sicherheitstechnik zu übertragen, um die ersten Gefahrenmanagementsysteme heutiger Prägung zu schaffen. Zunächst entwickelten die Hersteller vornehmlich proprietäre Lösungen, um sich Marktanteile zu sichern und ihre Preise durchsetzen zu können. Für die aus Kundensicht günstigere offene Lösung, die beliebige Fremdsysteme einbindet, fehlte zunächst ein gemeinsames „Protokoll“ über die die Komponenten ihre Systemzustände austauschen konnten, also eine Software, die die Maschinensprache des Subsystems in übergeordnete, für das Kontrollsystem verständliche Codes übersetzt.

## BACnet und OPC

Durchgesetzt haben sich im Markt nach derzeitigem Stand wohl die (Kommunikations-) Protokolle BACnet und OPC. Die meisten aktu-

## Systemeinbindung der Protokolle



ellen Subsysteme in der Sicherheit bieten einen Datenaustausch nach diesen Protokollen an, ihre Implementierung scheint inzwischen zu den notwendigen Produkt-Features zu gehören.

In der Praxis dürfte der Anwender kaum Unterschiede zwischen beiden Protokollen feststellen können, eine Gefahrenmeldeanlage reagiert bei Aufschaltung mittels OPC nicht anders als mittels BACnet.

BACnet kommt aus den USA ([www.bacnet.org](http://www.bacnet.org)) und beschreibt vornehmlich die Methode, Systeme der Heizungs-, Lüftungs- und Klimatechnik zusammen zu schalten und zu betreiben. Die Aufschaltung klassischer Sicherheitstechnik ist eher eine Zugabe. So wurden die Protokolle der Datenobjekte aus dem Bereich der Gefahrenmeldetechnik innerhalb von BACnet erst kürzlich vom zuständigen Komitee des ASHRAE (American Society of Heating Refrigeration and Air Conditioning Engineers) in dem so genannten „Addendum c“ der Öffentlichkeit vorgelegt. Wohl vor dem Hintergrund, dass BACnet von

der HKL-Schiene kommt, gab es in Deutschland für einige Zeit eine Diskussion zwischen Vertretern großer Firmen, ob nicht OPC das geeignetere Protokoll sein könnte. OPC steht für OLE Process Control und ist eine Standardisierung des Datenaustauschs aus der Prozess- und Automatisierungstechnik, bei der Daten Browser-basiert innerhalb einer Client-Server-Struktur gehandelt werden (siehe: [www.opc-foundation.org](http://www.opc-foundation.org)). OPC fungiert dabei als Server, der die Clients, also Subsysteme und das Managementsystem, mit Daten versorgt. Diese Konstellation liefert beim Aufbau von Netzwerkstrukturen erhebliche Freiheitsgrade, weshalb das Protokoll insbesondere von vielen Entwicklern präferiert wurde.

Zur Frage, ob nun BACnet oder OPC die bessere Lösung verspricht, gab es noch bis vor ca. drei Jahren ausführliche Diskussionen in der Fachwelt. Heute kann eher von einem akzeptierten Nebeneinander von BACnet und OPC gesprochen werden, insbesondere nachdem BACnet Promoter Siemens in seinem Portfolio für Gefahrenmanagementsysteme nun beide Protokolle führt. Heute werden von den meisten Anbietern auch beide Protokolle unterstützt, wobei im deutschen Markt ein leichtes Übergewicht für OPC-Anwendungen erkennbar ist. Ob sich ein einzelner Standard durchsetzen wird, kann aus heutiger Sicht noch nicht abgeschätzt werden.

Bis auf wenige Ausnahmen sind aktuelle Gefahrenmanagementsysteme heute eigentlich „nur noch“ Software, die von einem zentralen Server aus dezentrale Einrichtungen mit zugehörigen Informationen versorgt. Die überfrachtete Zentrale am Pfortnerarbeits-

platz hat ausgedient. Zu den Informations- und Meldesystemen, die heute aufgeschaltet werden können gehören:

- Einbruchmeldeanlage
  - Personenschutzanlage
  - Aufzugsnotruf
  - Videosysteme
  - Besuchermanagement
  - Zutrittskontrollanlagen
  - Fluchtwegsteuerungen
  - Rettungswegsteuerungen
  - Gebäudeautomatisierung
  - Brandmeldesysteme
  - Löschanlagensteuerung
  - PA Anlagen
  - Betriebsfunk
  - Wächterkontrollsysteme
- (Quelle: ZVEI)

Über den Einsatz von automatischen Wähl- und Ansagegeräten ist die Ankoppelung an Telefonsysteme möglich. Die weitere Meldungsgenerierung für E-Mail oder SMS als Alarmmedium wird in der Regel vom Internet Server bereitgestellt.

Um zu ermitteln, was gängige Gefahrenmanagementsysteme heute leisten, werden im Folgenden die Features von drei im Markt wichtigen Produktlösungen: GMA Manager Web von Siemens, Building Integration System (BIS) von Bosch, GEMOS Software von ela-soft. Auf weitere Anbieter wird in der Tabelle (S. 75) verwiesen.

Der wichtigste Fortschritt ist wohl, dass sich die eingangs beschriebenen Schwachstellen, wie unergonomischer Aufbau des Gesamtsystems und Überfrachtung der Arbeitsplätze

## Mehrplatzfähige Gefahrenmanagementsysteme

Anbieter	Produkt	vorh. Standardprotokolle (u.a.) / (Anzahl) gerätespezif. Schnittstellen	Internet-Adresse
<b>Advancis Software &amp; Services GmbH</b>	WinGuard	OPC, > 150 gerätespezif.	<a href="http://www.advancis.de">www.advancis.de</a>
<b>Andover Controls GmbH</b>	Continuum Cyberstation	BACnet, ca. 300 gerätespezif.	<a href="http://www.andovercontrols.de">www.andovercontrols.de</a>
<b>b+m Informatik AG</b>	GEBANIS Vers. 5	OPC, EIB, BACnet, > 40 gerätespezif.	<a href="http://www.gebanis.de">www.gebanis.de</a>
<b>Bosch Sicherheitssysteme GmbH</b>	BIS Building Integr. System	OPC	<a href="http://www.bosch.de">www.bosch.de</a>
<b>Comm-Tec GmbH</b>	AMX iBuilding	OPC, LON, EIB, serielle Standards, >300 gerätespezif.	<a href="http://www.comm-tec.de">www.comm-tec.de</a>
<b>Ela-soft GmbH &amp; Co. KG</b>	Gemos	OPC, BACnet, LON, >300 gerätespezif.	<a href="http://www.ela-soft.com">www.ela-soft.com</a>
<b>GICO Software GmbH</b>	Software f. Gefahrenmanagement	3 gerätespezif.	<a href="http://www.gico.de">www.gico.de</a>
<b>Honeywell Building Solutions</b>	Enterprise Buildings Integrator	OPC, BACnet, LON, >100 gerätespezif.	<a href="http://www.honeywell.de/hbs">www.honeywell.de/hbs</a>
<b>Interflex Datensysteme GmbH &amp; Co KG</b>		k.A.	<a href="http://www.interflex.de/de/">www.interflex.de/de/</a>
<b>Lenel Systems International</b>	OnGuard ET SE	OPC	<a href="http://www.lenel.com">www.lenel.com</a>
<b>Metall- und Stahlbau Wagner GmbH - Geschäftsbereich GDM</b>	NADINE	LON, BACnet, Profibus, OPC, Modbus, EIB, >150 gerätespezif.	<a href="http://www.gdms.de">www.gdms.de</a>
<b>Novar GmbH</b>	Winmag	OPC, ca. 60 gerätespezif.	<a href="http://www.novar.de">www.novar.de</a>
<b>Schille Informationssysteme GmbH</b>	PVIs Enterprise Security	OPC, LON, BACnet, SNMP, EIB, >200 gerätespezif.	<a href="http://www.schille.com">www.schille.com</a>
<b>Securiton GmbH</b>	SLS-Pro	OPC, BACnet, ca. 80 gerätespezif.	<a href="http://www.securiton.de">www.securiton.de</a>
<b>Siemens Building Technol. GmbH &amp; Co. KG</b>	GMA-Manager WEB	BACnet, OPC, OpenInterface, gerätespezif.	<a href="http://www.de.sbt.siemens.com">www.de.sbt.siemens.com</a>
<b>Total Walther GmbH</b>	AV 300	OPC, BACnet, LON, ca. 300 gerätespezif.	<a href="http://www.tycosafetyproducts.com">www.tycosafetyproducts.com</a>

mit auflaufenden Alarmen durch Netzwerk-basierte Lösungen vermeiden lassen.

### GMA Manager Web

Die Siemens-Software wird nicht in modularer Form angeboten, sondern als Komplettpaket kundenspezifisch programmiert. Als Betriebssystem kommt LINUX zum Einsatz, das den Vorteil einer höheren Betriebsstabilität gegenüber Windows aufweist. Erkauft wird dies allerdings damit, dass bei Problemen, etwa Anpassungen an veränderte Bedingungen, auch ein LINUX-Fachmann zur Verfügung stehen muss. Der GMA Manager nutzt von der Programmierseite her JAVA-Technologien, um möglichst viele Plattformen ansprechen zu können. Die Serverseite kann beim GMA Manager redundant ausgelegt werden, so dass Systemausfälle nicht zu einer Beeinträchtigung des Betriebs führen. Im einfachsten Fall werden mit der Software die Sicherheitsgewerke

- Zeiterfassung und Zutrittskontrolle
- Einbruchmeldetechnik
- Brandmeldetechnik
- Videoüberwachung

auf einer Managementebene zusammengefasst. Diese Managementebene wird üblicherweise dann parallel zu Telefonsystemen betrieben, die die notwendige Drucker/Fax/E-Mail/SMS-Funktionalität beisteuern. Nach oben hin besitzt der GMA Manager außerdem eine Schnittstelle zu E-Business-Systemen wie SAP, so dass eine Informationsweitergabe auch auf dieser Ebene möglich ist. Innerhalb des Sicherheitsnetzwerks verteilt die Software in einem Alarmfall mittels des TCP/IP-Protokolls Informationen an beliebige angeschlossene Netzwerkteilnehmer, also auch an Windows-Systeme. Bei der Generierung von Informationen kann auf Datenbanken zurückgegriffen werden, so dass beispielsweise bei einem Umweltaalarm Gefahrstoffdaten an angeschlossene Teilnehmer, etwa an die Feuerwehr, übertragen werden. Die Software verfügt über eine intuitive Oberfläche, deren Informationsdarstellung bei Bedarf auf einen grafischen und einen Textbildschirm aufgeteilt werden kann. Aus ergonomischen Überlegungen ist aber die Alternativlösung mit einem großen Monitor, bei dem der Maßnahmentext in die vom System generierten Alarmgrafiken integriert wird, vorzuziehen. Zur grafischen Aufbereitung von Vorgaben zur Alarmbearbeitung können Objektpläne in das System eingespielt werden, in die man hinein zoomen kann. Unterstützt wird das Zeichnungsformat DXF, so dass bereits bei der Gebäudeplanung entsprechendes Vorlagenmaterial generiert werden kann. Zu berücksichtigen

ist allerdings, dass das ursprünglich von AUTOCAD stammende DXF Zeichnungsformat nicht grundsätzlich genormt ist, sondern dass es Dialekte gibt, die ein direktes Portieren von Zeichnungen unmöglich machen können. Entweder bei der Systembeschaffung des GMA Manager oder bei der Vergabe von Planungsaufträgen ist deshalb auf Kompatibilität zu achten.

Beim GMA Manager Web hat sich Siemens im Interesse der Kunden von einer alten Direktive gelöst, nach der bei Siemens-Anlagen nur weitere Siemens-Komponenten angeschlossen werden konnten. Die aktuelle GMS-Software verfügt deshalb über beide Protokoll-Schnittstellen, OPC und BACnet, und ist so auch für die Aufschaltung von Subsystemen anderer Hersteller geeignet.

### Building Integration System (BIS)

Das System von Bosch Sicherheitsysteme zielt insbesondere auf die Bedürfnisse von Großanwendern, wie Kraftwerke, Flughäfen, Industrieanlagen, Banken, Kliniken und JVA. Ein Unterschied zu anderen Lösungen ist, dass es lediglich das Protokoll OPC versteht. BIS ist schon in der Grundkonfiguration modular aufgebaut, so dass bereits bei der Beschaffung Auswahlmöglichkeiten bestehen. Basis ist die „Automation Engine“ (Sicherheitsmanagement), die um die „Access Engine“ (Steuerungsmodul für Zutrittskontrolle) und die „Video Engine“ (Einbindung von Video- und Bildsystemen) sowie weitere Module, zum Beispiel für HKL Anlagen, Gebäudeleitsysteme, Systeme zur biometrischen und videotechnischen Personenidentifikation oder digitale Bildspeichersysteme, erweitert werden kann.

Die BIS Software läuft mit verschlüsselter Kommunikation nach dem Client-Server-Prinzip auf handelsüblicher Hardware (nach Bosch Spezifikation) unter Windows 2000 oder Windows XP. Da Microsoft den Support für Windows 2000 in absehbarer Zeit einstellen will, sollte bei Neuerwerbung gleich die notwendige Anzahl von XP-Lizenzen beschafft werden. Auch BIS verteilt im Alarmfall im Netzwerk Bearbeitungsanweisungen an die angeschlossenen Netzwerkteilnehmer und steuert automatisch dazu erforderliche externe Hardwarekomponenten, etwa digitale Videorecorder, an. Die visuelle Aufarbeitung von Alarmanweisungen erfolgt auf der Basis von im System hinterlegten Szenarien unter Einbindung von Objektplänen im AutoCad Format, in die sich das BIS automatisch hinein zoomt, um dem Bediener einen Lageüberblick zu verschaffen. In den Plänen können alle Melder grafisch erfasst werden,

## Typisch Schweiz:



## Präzise!

So genau wie eine Schweizer Uhr mit der Zeit, nimmt es auch Securiton mit anspruchsvoller Sicherheit.

Unser Arbeitsgebiet umfasst die gesamte Sicherheitstechnik – von Brand-, Einbruch-, Video- und Zutrittskontrollanlagen bis zu übergreifenden Sicherheitsmanagement-Systemen.

Natürlich mit bewährter Schweizer Qualität und dem Know-how eines Marktführers.

Sie suchen die perfekte Sicherheitslösung? Wir sind der richtige Partner.



Securiton GmbH  
Von-Drais-Straße 33  
D-77855 Achern  
Tel.: 0 78 41 62 23-0  
Fax: 0 78 41 62 23-10  
info@Securiton.de  
www.securiton.de

Ein Unternehmen der  
Securitas Gruppe Schweiz

so dass dem Bediener auch gleich Informationen zukommen, welche Art Alarmgeber ausgelöst hat. Durch die Integration der Leitplanerstellung in den Architektenprozess lassen sich daher Gesteuerungskosten bei Objekten einsparen. Das BIS ist von der Bediener- und Anlagenseite für 99 gleichzeitige Benutzer, 500.000 Melderpunkte und den Anschluss von 128 Subsystemen ausgelegt. Die Anbindung von 3rd Party Produkten der Sicherheitstechnik ist über OPC möglich. Kundenfreundlich sind die für jeden Anwendungsfall gesondert als HTML-Seiten erstellten Bedienoberflächen und Aktionspläne, bei denen Änderungen oder Aktualisierungen leicht vom Betreiber selber eingepflegt werden können. Dies reduziert Serviceaufwand und somit laufende Kosten.

**GEMOS**

Sehr flexibel hinsichtlich der Einsatzmöglichkeiten ist die systemunabhängige Software GEMOS von ela-soft. Sie ist in drei Variationen erhältlich, die sich bei ansonsten gleicher Funktionalität vor allem in der Zahl der Bedienplätze oder der anschließbaren Subsysteme unterscheiden, um Lösungen für kleine, mittlere beziehungsweise große Unternehmen zu bieten. Die Light-Version ist eine Einzelplatzlösung für Kleinbetriebe. Die Standard- und Professional Versionen sind für größere Anwender gedacht, wobei die Professional-Version unbegrenzte Ausbaumöglichkeiten bei der Zahl der aufschaltbaren Melder, der Anzahl speicherbarer Szenarien und der Anschlussmöglichkeit für Subsysteme bietet.

Kern des GEMOS Systems ist ein zentraler Server, der redundant ausgelegt werden kann und auf dem die einzelnen Module der Software laufen. Der Server verarbeitet alle Meldungen angeschlossener Clients und verwaltet die korrekte Kommunikation zwischen den Systemteilnehmern auf der Basis des TCP/IP-Protokolls. Dabei besteht die Software aus folgenden Modulen:

- Kernmodule (Visualisierung, Meldungsbearbeitung, Stammdaten)
- Zusatzmodule (Videomanager, Kommunikationsmanager, GLT-Manager, Kalendersteuerung, Dokumentenmanagement, Adressverwaltung, usw.)
- Schnittstellenmodule (Sicherheits-, Gebäude-, Kommunikationstechnik)

Hieraus lässt sich quasi nach dem Baukastenprinzip für jeden Anwendungsfall die geeignete Lösung zusammenstellen.

Die folgende Grafik zeigt, dass GEMOS hierarchisch nach einer Baumstruktur arbeitet. Vom System werden in einem Alarmfall so genannte Alarmstapel generiert, die an die zuständigen Nutzer zur Abarbeitung verteilt werden. Im Rahmen dieser Baumstruktur ist GEMOS leicht für die verschiedenen Einsatzzwecke konfigurierbar. Als mögliche Betriebssysteme für die Software nennt der Hersteller LINUX, Windows 2000 und Windows XP. Die visuelle Darstellung von Alarmszenarien erfolgt Browser-basiert entweder mit Mozilla oder Internet Explorer. Die angezeigten Seiten werden in HTML generiert, was Kostenvorteile bei der Pflege bringt. Zusätzlich zu HTML sind im System

Scripte der Programmiersprachen PHP, Perl und CGI lauffähig. Durch die Implementierung von PHP werden die aufrufbaren Seiten interaktiv gestaltbar, das heißt, es können vom Bediener direkte Eingaben gemacht werden, was in der Praxis ergonomische Vorteile durch vereinfachte Bedienbarkeit und somit auch eine höhere Handhabungssicherheit mit sich bringt. Zur Darstellung von Alarmen kommen elektronisch aufbereitete Planunterlagen mit integrierten, aktiven Meldersymbolen zum Einsatz. Ela-soft gibt an, alle gängigen Zeichnungsformate mit Mel-

**VfS-Planungshandbuch Gebäudemanagementsysteme**

Zwei Jahre sind in IT-orientierten Technologien eine Zeit, in der sich manches ändert. Beim Verband für Sicherheitstechnik e.V. steht daher eine Überarbeitung des 2003 erschienenen Handbuchs „Gebäudemanagementsysteme“ auf der Agenda, mit der bereits begonnen wurde. Dennoch ist auch das vorliegende Planerhandbuch eine lohnenswerte Lektüre. Insbesondere die enthaltenen Vorgaben und Empfehlungen sind nicht für den Planer, sondern auch für den Endkunden eine nützliche Hilfe bei Entscheidungsfindungen in den Bereichen Gebäudeüberwachung und Gebäudemanagement. Eingesetzt wird es unter anderem in der Kundenbetreuung von den Anwendern Bosch, Siemens, ela-soft und ADVANCIS. Aber auch ein Direktbezug des 82-seitigen (A4) Werks (50 €) ist möglich (<http://www.vfs-hh.de/verkauf.html>)

dersymbolen einlesen zu können, also nicht nur AutoCad und DXF. Dies spart den Projektstress, etwa mit dem Gewinner eines Architektenwettbewerbs, der nicht Auto-Cad, sondern ein Architekten-CAD-System besitzt. Aus der Umsetzung und Erfahrung von mehreren hundert Projekten kann bei GEMOS auf dreihundert gelöste Schnittstellenmodule zum Anschluss marktgängiger Gefahrenmeldetechnik zurückgegriffen werden. Dies macht die Software abwärtskompatibel, das heißt, sie ist auch für die Betreiber bestehender Objekte mit älteren verbauten Techniken einsetzbar. Neben diesen herstellereigenen Lösungen stehen folgende weitere Anbindungsmöglichkeiten zur Verfügung:

- Physikalische Anbindungen: RS232, RS485, Ethernet, ATM
- IT-Schnittstellen: seriell, parallel, paketorientiert
- Protokolle: BACnet, OPC, LON, Bitbus, VdS2465

Über das Videomodul, das mit einer integrierten, virtuellen Kreuzschiene ausgestattet werden kann, ist auch die Ansteuerung von Schwenk-Neige-Kameras mit Zoom möglich. Interessant ist auch das Zusatzmodul „Wächterrundgang“. Über diese Funktion lassen sich alle Melder, die im System verzeichnet sind, mittels Zeitfenster als „Stechstelle“ programmieren. Kontrollgänge sind somit effizient planbar und nachvollziehbar, Schummeln ist ausgeschlossen und die Rundgänge lassen sich leicht an veränderte Situationen anpassen. Daneben verfügt die Software noch über eine Rechteverwaltung für die Benutzer und die Möglichkeit Protokolle über erfolgte Aktionen zu generieren.

Kontakt: [www.sobers.de](http://www.sobers.de)

**Baumstruktur bei GEMOS, dem Gefahrenmanagementsystem von ela-soft**

