Haus mit Hirn: Auf die Architektur kommt es an

Was man bei der Vernetzung von Gebäudetechnik und IT beachten muss

Sigurd Schobert

Moderne Gebäude – ganz gleich ob es sich um Büro- oder Industriegebäude handelt oder zeitgemäße Wohngebäude – zeichnen sich heute durch eine zukunftsgerechte, flexible und aktuelle Elektroinstallation aus. Dazu gehört nicht nur eine Infrastruktur für die Kommunikationstechnik (Telekommunikation, Datentechnik, Multimedia), sondern auch eine zeitgerechte Gebäudetechnik für Sicherheit, Steuerung der technischen Anlagen sowie deren Administration.

Der Begriff der »intelligenten Gebäude« hat sich in den letzten dreißig Jahren stark gewandelt: Während er sich ursprünglich auf die architektonische/konstruktive Planung von Häusern bezog, verstand man hierunter ab den 1980er Jahren die Automation und das Management von Energie-, Alarm- und Zutrittsystemen. In den letzten Jahren wandelte sich im Zusammenhang mit dem Konvergenzansatz erneut der Fokus: Nunmehr können und sollen sämtliche Systeme – von der Eingangskontrolle (**Bild 1**) bis zum Brandmelder – zusammenpassen (interoperabel), und das zentral gesteuert. Das erfordert eine Vernetzung aller Sensoren, Aktoren, Bedienelemente, Verbraucher und anderer technischer Einheiten miteinander. Somit ergibt sich eine dezentrale Anordnung der Steuerungseinheiten (Direct Digital Control – DDC), welche durchgängig mittels eines Bussystems (basierend auf Protokollen wie etwa Ethernet oder TCP/IP) vernetzt sein müssen.

In diesem Zusammenhang bezieht sich das Thema Sicherheit – anders als im reinen Office-Umfeld – in erster Linie nicht auf Datensicherheit, sondern vielmehr auf Verfügbarkeit und Ausfallsicherheit der bestehenden Systeme. Dies ist umso mehr von Bedeutung, als es im schlimmsten Fall tatsächlich um Menschenleben geht, man denke dabei an den Betrieb von Aufzugsystemen und Ähnlichem. Das Problem einer ganzheitlichen Gebäudeautomatisierung besteht darin, dass sich einheitliche Standards noch nicht hinreichend durchgesetzt haben und die Hersteller der Komponenten vielfach auf proprietäre Lösungen setzen. Damit muss das Netzwerk, das die Subsysteme verbindet und steuern soll, umgehen können.

Alle Fäden laufen in der Zentrale zusammen: Gebäudetechnik, Sicherheitstechnik, Administration von Servern oder Steuerung von Licht und Klima

Quelle: Mabotix

Bild 1: Überwachungskameras sorgen für Sicherheit: Montage an einem Lampenmast, daher fällt sie nicht besonders auf

Quelle: Sigurd Schobert

Bild 2: Auch Rolltreppen gehören zur Haustechnik (One World Financial Center, New York)

Quelle: Sigurd Schobert

Bild 3: IP-Phone: die moderne Form der Sprachkommunikation

Viele Systeme, ein Netz

Es handelt sich hierbei um äußerst verschiedenartige Teilsysteme, wie etwa Licht, Heizung und Klimaanlage, Energieverbrauch, Transportsysteme (Aufzüge, Rolltreppen, **Bild 2**), physische Sicherheitssysteme sowie das IT-Netz, d. h. integrierte Sprach- und Datenübertragung. Die Vorteile und die Funktionalität eines intelligenten Gebäudes steigen dabei mit der Anzahl der angebundenen Systeme und insbesondere deren Vereinbarkeit.

Dem zentralen Management kommt hier die Schlüsselrolle zu. Um das Gebäude effektiv zu überwachen und die einzelnen Bereiche zu steuern, müssen alle Systeme in einer einzigen Plattform und auf dem gleichen Netzwerk nebeneinander bestehen können.

Die Final Information Points (FIPs), also die Elemente mit einer spezifischen Funktion des Subsystems wie z. B. IP-Phones (VoIP-Endgeräte, **Bild 3**) und

Sigurd Schobert, Redaktion »de«, nach Unterlagen von Architecture bei Enterasys Networks

Netzwerkdrucker, müssen dabei erkannt werden (ihre Funktion und Aufgabe innerhalb des Gebäudes und des Subsystems, zu dem es gehört) und auf für sie funktionswichtige Informationen Zugriff haben. Zudem muss ihr Status (Sicherheit, Art der gesendeten Information, Verhalten) fortwährend unter Kontrolle stehen (Analysen), um so sicherzustellen, dass sie nicht die Informationen anderer FIPs gefährden bzw. verfälschen.

Zur höchsten Priorität gehört dazu die Ausfallsicherheit, da Störungen des Netzwerks fatale Folgen haben können. Zudem weisen die Steuerungssysteme oft eine so große Empfindlichkeit auf, dass diese vor dem eigenen Netz geschützt werden müssen und nicht umgekehrt: Eine hohe Anfälligkeit für einen Angriff auf einen Server (Denial of Service-Attacken) besteht hier oft schon alleine durch die reine Broadcast-Last im Netz (gestreute, adresslose Übertragung von Nachrichten über ein Kommunikationsnetz). Jedoch auch Attacken von außen, wie Hackings oder Viren gefährden das System und müssen wirkungsvoll verhindert werden.

Eine Frage der Architektur

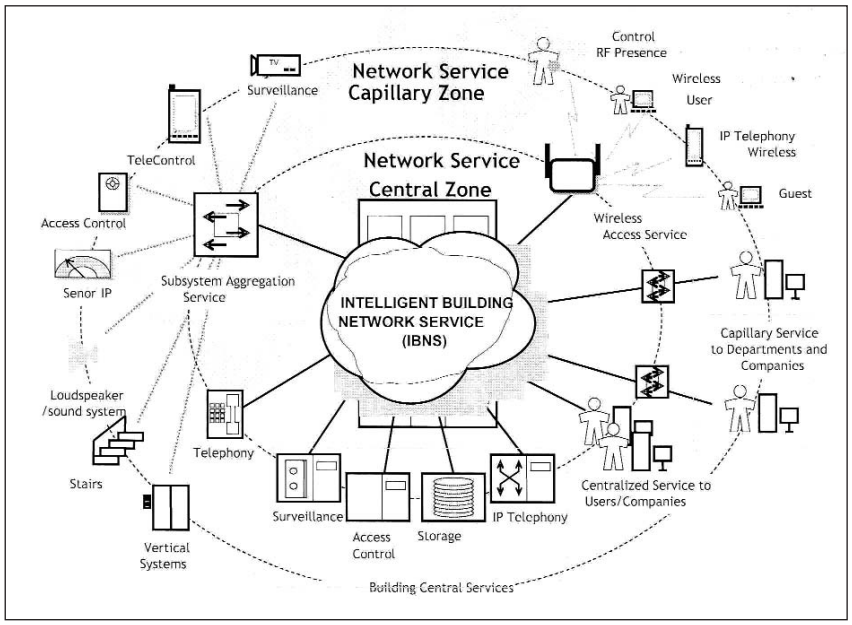
Eine umfassende Anbindung aller Komponenten stellt eine hohe Herausforderung dar. Die verschiedenen Kontrollsysteme unterschiedlicher Hersteller – die zumeist ihre eigenen, proprietären Systeme verwenden – erfordern eine Anbindung an ein einheitliches Kommunikationsnetz. Ein zentralisiertes Identitäts-Management-System (Identity Management) fasst die Zugangskontrolle und physische Anwesenheitsdetektoren in einem einzigen Netz zusammen. Dazu benötigt man auch eine Bereitstellung einer ausreichenden Netzabdeckung für schon vorhandene und noch zukünftige Anwendungen im Wireless-Bereich (Funknetz).

Sinnvoll erscheint, die Vielzahl der Anwendungen in zwei verschiedene Arbeitszonen aufzuteilen:

- Zum einen in eine innere Zone (Network Services Central Zone – Z_{CEN}),
- zum anderen eine äußere Zone (Network Services Capilarry Zone – Z_{CAP}) (**Bild 4**).

Als »innerer Kreis« enthält Z_{CEN} alle Komponenten, die die entsprechenden Services für die Integration aller Systeme bereitstellen, hierzu zählen insbesondere die »klassischen« IT-Bereiche wie Access Control, Storage (Datenspeicherung) und dergleichen, jedoch auch die Telefonie.

In der äußeren Zone (Z_{CAP}) fasst man sämtliche Haussteuerungselemente zusammen. Diese sind in der Regel nicht für die Anbindung über Ethernet/IP ausgerichtet, können jedoch über Aggregatoren (Schnittstellensammler, Schnittstellenkonverter) FIBs anschließen. Das bedeutet, die vorhandene Technologie des Subsystems muss erst in der IP-Technologie erfasst werden.



Quelle: Weissenbach-PR

Bild 4: Die Vielzahl der Anwendungen in den zwei verschiedenen Arbeitszonen innerer und äußerer Bereich in der Gebäudetechnik. Die meisten Systeme sind untereinander vernetzt

Ein Netz für alle Fälle

Um den gegenwärtigen, vor allem aber auch den zukünftigen Anforderungen gerecht zu werden, muss das Netzwerk folgende Bedingungen erfüllen:

Kommunikationsarchitektur

- Neue Verbindungspunkte wie VoIP-Telefone müssen sich problemlos hinzufügen lassen.
- Die Bandbreite des Netzwerks muss erhöht werden können.
- Automatische Fehlerbehandlung: Das System muss in der Lage sein, Störungen selbstständig zu beheben.
- Hohe Netzleistung in sicheren Umgebungen (**Bild 5**).

Integration der Zugangskontrolle

- Gebäudezutrittssysteme, gesicherter Zugang zur Workstation sowie dynamische Zugriffsrechte müssen in einem einzigen Identitäts-Management (Identity Management)-System zusammengefasst werden können.

- Informationen von verschiedenen Quellen, zum Beispiel aus Datenbanken, Logistik, Personal müssen zusammenpassen. Das erfordert auch einen entsprechenden Zugang gemäß der Richtlinien (Policies).
- Schnelle Integration neuer biometrischer Nutzeridentifikation (**Bild 6**).

Integration der Sicherheitssysteme
- Integration von Gebäude- (physisch) und Computer-Sicherheitssystemen (logisch),
- Rückgriff auf den Sicherheitsstatus sämtlicher Kontroll- und Kommunikationssubsysteme, egal ob in Z_{GEN} oder Z_{CAP},
- Integration automatisierter Problemlösungen und automatischer Maßnahmen, um Sicherheitsprobleme zu erkennen und lösen, die durch physischen oder logischen Zugang erfolgen.

Zentrales Management

Das zentrale Management muss dabei eine Reihe verschiedener Eigenschaften aufweisen:

FIPs einrichten und löschen können, unter Berücksichtigung:
- ihres Verhaltens im entsprechenden Subsystem, z. B. VoIP-Netz,
- ihres Verhaltens entsprechend ihres Standorts,
- ihrer Umgebung unter anomalen Bedingungen (Fehler, Sicherheitsprobleme),
- zudem Eliminierung unautorisierter Verbindungen und

Quelle: Weissenbach-PR

Bild 5: Videokonferenzen erfordern eine höhere Bandbreite als reine Sprachkommunikation

Quelle: PCS

Bild 6: Sicherheit durch biometrische Identifikation

- Speicherung und Abfrage von Daten (Relationale Inventur) der FIPs.

Security Domains errichten können, insbesondere:
- Work Zones und Interaktion zwischen den Subsystemen,
- eine zentralisierte Reserve an Ressourcen für jedes Subsystem,
- die Anpassung in Echtzeit des Verhaltens der Subsysteme.

Über automatische Fehlerbeseitigung (Automatic Response) verfügen:
Um die Funktionen der Teilsysteme aufrechterhalten zu können, muss das Netzwerk auf Bedrohungen automatisiert reagieren und die Anomalie unmittelbar lösen. Dafür
- muss das normale Verhalten (durchschnittliches Datenvolumen und Zugriffe) definiert werden (**Bild 7**),
- müssen Quarantänemaßnahmen wie z. B. des Abschalten eines einzelnen Arbeitsplatzes definiert werden aufgrund der Art des FIP, des Status des FIP, des Standortes des FIP und dessen Service-Levels wie zugesicherte Verfügbarkeit, sowie der Zeit und
- die durchgeführten Aktionen an das Steuerungsmodul (Control Panel) gemeldet werden.

Zukunftssichere Architekturen

Gefragt sind also Architekturen, die sich leicht erweitern lassen. Entsprechend neuer Entwicklungen erfordert dieses eine Anpassung auf den neusten Stand, vor allem zusammen mit Geräten und Lösungen von Drittanbietern. Zudem sollten sie jegliche Sicherheitsfunktionen (wie Access Control, Richtlinienverwaltung oder automatisierte Störungsbeseitigung) direkt an jedem Access Port zur Verfügung stellen. Neueste, Switch-basierte Sicherheitsarchitekturen wie etwa Secure Network tragen dieser Tatsache Rechnung. Dabei bedarf es keines Unterschieds, ob es sich um einen Switch für den Einsatz im Bürobereich handelt oder um einen Switch im Bereich der Gebäudeautomatisierung, unter Umständen mit ganz anderen Umweltvorgaben (Temperatur, Schock, Luftfeuchtigkeit). Für den Einsatz mit DDCs (Steuerungseinheiten) müssen auf dem Switch die gleichen Funktionen und das gleiche Management wie bei Büroswitches bereitgestellt werden.

Um ein Netzwerk – und damit auch das gesamte Gebäude – effektiv zu schützen (und Ersteres auch automa-

GLOSSAR

VLAN:
In einem Virtual Local Area Network ist die physikalische Netzwerkstruktur unabhängig von der logischen Struktur.

Rate-Limiting-Regeln:
Sind Teil einer Policy und begrenzen die Bandbreite einer Applikation.

Radius Server:
Ist der Remote-Authentication-Dial-in-User-Service-Server (Radius). Der Radius-Server übernimmt Passwortprüfung.

802.1x:
Standard für die Authentifizierung in LANs

MAC-Adresse:
Ist die Hardwareadresse, in einem Gerät.

Default:
Ist die vorgegebene Softwareeinstellung.

Identity-Management-System:
Identity-Management umfasst alle Maßnahmen für den sicheren Zugang

Access Control:
Das ist eine Zugangskontrolle.

Storage:
Ist die Speichereinheit im Netzwerk

Broadcast Last:
Gestreute Daten innerhalb des Netzwerks.

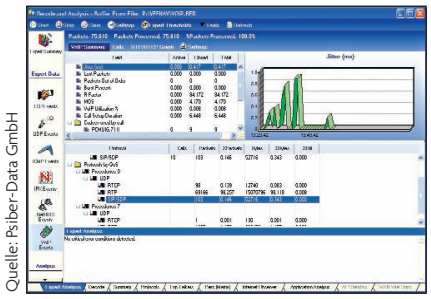
Denial of Service (DoS):
Ist ein Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz

Final Information Points (FIPs):
Sind Endpunkte des Netzwerks z. B. IP-Phones.

Policies:
Policies sind Statuten, Richtlinien oder Verhaltensregeln.

tisch zu konfigurieren), muss zunächst eine Berechtigung (Authentisierung) am Access-Port mit nachfolgender Regelzuweisung erfolgen. Hiermit stellt man sicher, dass nur autorisierte Nutzer und Geräte das am Netz machen können, was sie sollen: So können beispielsweise Servicetechniker nur auf die Anlagen mit dem Administrationsprotokoll zugreifen, für die sie auch zuständig sind.

Ein Switch muss dabei optimalerweise alle entsprechenden Verfahren (wie 802.1x, MAC-Adresse, Webportal oder Default) gleichzeitig pro Port unterstützen, so dass sich der Administrationsaufwand nicht unnötig erhöht. Ansonsten müsste der Elektroinstallateur bei jedem Umzug den Authentisierungsvorgang neu anpassen. Bei der Authentisierung verschiedener Benutzer bzw. Geräte gleichzeitig an einem Port müssen dort dann auch unterschiedliche Gruppen-Regeln je nach Benutzer und Gerät gleichzeitig vorhanden sein. Der PC bekommt beispielsweise andere Regeln als eine Überwachungskamera am selben Port, für einen Gast sollen



Quelle: Psiber-Data GmbH

Bild 7: Ermitteln des Datendurchsatzes eines Sprachnetzes über Voice over IP. Hier erfasst man die Auslastung des Netzes

andere Regeln gelten als für den eigenen Mitarbeiter etc.

Eine Frage der Policy

Hierbei sollten die dann vom Radius-Server (Client-Server-Protokoll zur Authentifizierung, Autorisierung und zum Accounting) zugewiesenen Policies schon auf dem Switch vorgehalten werden. Damit vermeidet man Verzögerungen bei der Anmeldung und Skalierungs- sowie Redundanzprobleme beim Policy Manager des jeweiligen Herstellers. Eine Policy beinhaltet optimalerweise VLAN, Access Control, Priority- und Rate Limiting-Regeln (Bandbegrenzung), die auch noch für spezifischen Verkehr des authentisierten Nutzers/Geräts gelten. Das Policy-Management sollte für alle (Sub-)Systeme identisch und skalierbar sein. Dabei kommt gerade der Funktion Rate-Limiting, zum Schutz der Gebäudetechnik, eine außerordentliche Bedeutung zu.

Durch eine dynamische automatisierte Störungs-/Fehlerbeseitigung (Intrusion Response) lassen sich nicht nur IT-, sondern auch die jeweiligen Subsysteme vor Angriffen und Ausfällen schützen. Wichtig ist, dass die entsprechende Sicherheitslösung im gesamten Gebäude direkt an jedem Access-Port zur Verfügung steht und universell einsetzbar ist. Unabhängig von der Art der Endsysteme, ob Computer oder Aufzüge, der Nutzerkategorie, egal ob Gast oder Sicherheitspersonal – die Systeme verschiedener Hersteller müssen zusammenarbeiten können.