

## Rückblick ZVEI-Kolloquium Gebäudeautomation 2023

# Vernetzt, interoperabel, sicher?

Aktuelle Trends rund um intelligente Gebäude und die digitale Transformation von und mit Gebäudeautomation standen Ende 2023 beim ZVEI-Kolloquium Gebäudeautomation im Fokus. Die rund 200 Teilnehmer bekamen nicht nur einen Ausblick auf kommende Veränderungen, die mit der Digitalisierung einhergehen, sondern sie erfuhren auch, was eine Vernetzung für die Sicherheit der Gebäudeautomation bedeutet, welche Bedeutung Speichersysteme haben und wieso die Cloud nicht immer die beste Lösung ist.



Bild: Kalscheuer (alle Bilder)

**Bild 1:** Gespannt schauten die Talkrunden-Referenten auf die eingeblendeten Ergebnisse der Live-Umfrage unter den Teilnehmern des ZVEI-Kolloquiums Gebäudeautomation

Zum »Standards Evening« begrüßte **Adalbert Neumann** (Vorsitzender ZVEI-Fachabteilung Gebäudeautomation und CEO Busch-Jaeger Elektro) die Teilnehmer im alten Schachthof Offenbach und übergab die Bühne für die kurzen Breaking News der Standards rund um KNX, wibutler, Matter und EeBus. Was die verschiedenen Standards für die Gebäudeautomation bedeuten, wurde anschließend in der von **Johannes Hauck** (Hager Electro) moderierten Diskussion deutlich (**Bild 1**).

Zwar verbessere Wettbewerb Lösungen, so der Konsens der Talkrunde, aber die Zahl der im Markt verfügbaren Standards müsse endlich sein. Ansonsten seien Updates in der Praxis nicht mehr handhabbar. Zwar würden sich kaum alle Wettbewerber zusammenschließen, aber die Interoperabilität von Produkten, der problemlose Austausch von Geräten und Rückwärtskompatibilität zum Investitionsschutz seien die Basis für eine funktionierende Gebäudeautomation.

Dabei stand für alle Referenten fest, dass der Endkunde nicht zum Systemintegrator werden soll. Endkunden wollen nicht pro-

grammieren, sondern die vom Fachhandwerker eingerichteten Funktionen und konfigurierten Szenen nutzen, fasste **Hans-Joachim Langels** (Vorstand KNX Deutschland) zusammen. Wichtig sei dabei, den Markt nicht den US-Konzernen zu überlassen, die beispielsweise mit Alexa und Siri bereits das Segment der proaktiven Sprachassistenten besetzt haben.

### Wachsender Energiehandel zwischen den Prosumern

Der zweite Tag wurde von **Hajo Deul** (Referent Fachverband Elektroinstallationssysteme im ZVEI) und **Adalbert Neumann** eröffnet. Sie stellten fest, dass Künstliche Intelligenz und vorbeugende Instandhaltung in der Gebäudeautomation angekommen sind, wobei man außerhalb Deutschlands bereits einige Schritte voraus sei. Dr. **Torsten Hager** (Hager Electro) identifizierte u. a. den Peer-to-Peer-Leistungshandel in Wohnquartieren als einen Treiber für die Gebäudeautomation (**Bild 2**). Viel noch zu hebendes Potenzial sah Dr. **Hager** rund um Klima-, Lüftungsanlagen, Wärmepumpen, mobile Speichersysteme

(E-Autos) und verteilte PV-Speicher, die das Energiemanagement orchestrieren muss.

Dr. **Hager** prophezeite, dass sich ein wachsender Handel von Energie zwischen Prosumern etablieren werde – entweder direkt oder über Zwischenhändler. Bei zunehmendem Peer-to-Peer-Leistungshandel müsse allerdings der Überlastungsgrenze der Stromnetze durch intelligente Infrastruktur und selbstregulierende Systeme begegnet werden, um weiterhin die notwendige Netzstabilität zu gewährleisten.

### Wandel vom Produktgeschäft zum Servicegeschäft

Prof. Dr.-Ing. **Martin Höttecke** (Fachbereich Energie, Gebäude, Umwelt der FH Münster) warf einen näheren Blick auf das »ZVEI-Leitbild Gebäudeautomation 2030« (**Bild 3**). Er bezeichnete die Automation von Gebäuden, auf die rund 35 % des Energieverbrauchs entfallen, als einen wichtigen Ansatz für die Problemlösung beim Klimawandel. Nicht zuletzt der digitale Lebensstil, KI und regulatorische Trends (wie das Gebäudeenergiegesetz und Cybersicherheit) sorgen dafür, dass Gebäude nachhaltig betrieben und Prozesse und Produkte zu 100 % vernetzt werden müssen.

Er fasste zusammen, dass die Gebäudeautomation in den kommenden Jahren mit immer größeren Stückzahlen zum Massenmarkt werde, bis sich ein Wandel vom Produkt- zum Lösungs- und Servicegeschäft vollziehe. Schon heute seien einfache Installation und automatische Datenauswertung in Zeiten des Fachkräftemangels und des intelligenten Gebäudes unverzichtbar, so Prof. Dr.-Ing. **Martin Höttecke**, der auch die anschließende Talkrunde (**Bild 4**) rund um den Markt der Gebäudeautomation der Zukunft moderierte.

Mit den Vorteilen und Risiken von IoT in der Gebäudetechnik befasste sich der Vortrag von **Christian Kiefel**, CEO von ProKNX.



**Bild 2:** Dr. Torsten Hager sah den Leistungshandel in Wohnquartieren als einen Treiber für die Gebäudeautomation



**Bild 3:** Auf das »ZVEI Leitbild Gebäudeautomation 2030« warf Prof. Dr.-Ing. Martin Höttecke einen näheren Blick



**Bild 4:** Die Talkrunde am zweiten Veranstaltungstag befasste sich mit dem zukünftigen Markt der Gebäudeautomation

Er erläuterte, wie die rund 35 Milliarden Produkte, die aktuell im Internet der Dinge miteinander vernetzt sind, ihren Beitrag zu Komfort, Energiesparen, Fernüberwachung und vorausschauender Wartung leisten. Der übliche Kommunikationsweg verläuft dabei beispielsweise bei Sprachbefehlen von einem Online-Sprachassistenten über einen Internetrouter, einen Clouddienst wie Amazon hin zu einem auswertenden Skill Server und ein Third-Party-Gateway bis zum eingeschalteten Licht. Dabei muss die Tür zwischen Skill Server und Gateway permanent offen sein, was sicherheitstechnisch ein enormes Risiko darstellt.

Mit jedem aktivierten Skill im Internet of Things wird das lokale Netz über dieses Gerät zugänglich und bietet potenzielle Angriffspunkte für Unbefugte. Zwar gebe es Lösungen wie »Aragon« (ProKNX-Produktlinie, die eine Offline-Sprachsteuerung lokal auf dem Gerät statt Cloud-Services nutzt), bei der Daten geschützt im Haus bleiben, aber Kiefel regte an, generell darüber nachzudenken, ob Automation nicht öfter lokal »on the edge« erfolgen könne, zumal bisher genutzte Clouddienste jederzeit plötzlich kostenpflichtig oder abgeschaltet werden können.

### Mobile Speicher aus dem Elektrofahrzeug stationär verwenden

Das Thema Speichersysteme und Energieflussmanagement in Gebäuden wurde von Mark Junker (RWTH Aachen) beleuchtet. Er stellte dar, dass die Energiewende auf Speichersystemen aufbaut – vom Batterieheimspeicher über Industriespeicher bis hin zu Großspeichern. Beim Thema Batterieheimspeicher lenkte er die Aufmerksamkeit auf das Potenzial der Elektrofahrzeug-Speicherung, die gemessen an der Kilowattstunde

günstiger sei als Heimspeicher. Er riet dazu, mobile Speicher aus Elektrofahrzeugen, die eine Großteil an der Gesamtspeicherkapazität in Privathäusern ausmachen, aber zu 97 % der Zeit nicht genutzt werden, bewusst als Stromspeicher für den eigenen Haushalt zu integrieren (Vehicle to Grid, gesteuertes bidirektionales Laden).

Darüber hinaus sei auch ein »Second Use« von Fahrzeugbatterien in Betracht zu ziehen, also die Nutzung der Speicher nach ihrem Einsatz im Fahrzeug. Denn immerhin bleibe am »Lebensende« der Fahrzeugbatterien noch eine Ladekapazität von rund 70 % erhalten, die weiterhin stationär genutzt werden könnte.

### Löcher in der Vertrauensgrenze und Risiko-Multiplikatoren

Dezentrale Speichersysteme und erneuerbare Energien bezeichnete auch Raimund Thiel als das Rückgrat der zukünftigen Energieversorgung. Er widmete sich zusammen mit Dr. Ingo Hanke (beide SMA Solar Technology) dem Thema Cloud-basierte Geschäfts- und Servicelösungen. Wichtig sei, dass bei der notwendigen digitalen Vernetzung Cybersecurity von Anfang an mitbetrachtet werde. Vor allem, wenn bisher isolierte Systeme wie z. B. Wechselrichter nun einen Internet- und Remote-Zugriff erhielten. Die Anbindung an das Internet schaffe Löcher in der Vertrauensgrenze und die Cloud-Anwendung werde zum Multiplikator von Risiken: Der Angreifer muss nur das Cloud-System angreifen, um Schaden anzurichten. Dies sei insbesondere für nationalstaatliche Angreifer attraktiv, die cloudbasierte kritische Infrastrukturen im Visier haben.

Für cloudbasierte Systeme sind zusätzliche Schutzmaßnahmen nötig, die technologisch

unabhängig voneinander sein müssen – vom Perimeter (Firewalls) über Authentifizierung und Ende-zu-Ende-Verschlüsselung der Kommunikation und Monitoring (Anomalie-Detektion) bis hin zur Endpoint-Security auf dem Endgerät. Die Referenten stellten als Lösung exemplarisch die sichere IoT-Plattform mit AES-256-Verschlüsselung »SMA Webconnect« und das Endkunden-Produkt »SMA Smart Connect« vor.

### Regelmäßige Wartung der Infrastruktur schützt vor Schadsoftware

In seiner Keynote zum Thema Cyber-Sicherheitskonzepte von Gebäudeautomation erinnerte Ernst Graßmann (Geschäftsführer Braintop) ebenfalls an die Risiken vernetzter Technik. So bemängelte er, dass Gebäude-IT und IoT-Geräte im Zweckbau oft eine Lebenszeit von bis zu 20 Jahren haben, allerdings keine regelmäßige, gesteuerte Kontrolle oder Wartung der Infrastruktur stattfindet, was dem Einbringen von Schadsoftware Vorschub leiste. Auch sollte man sich die Frage stellen, wo die genutzte Cloud geografisch verortet sei und wer diese eigentlich betreut.

Das Fazit von Ernst Graßmann nach dem Motto »Vertraue nie, prüfe immer«: Switche müssen administrierbar sein, Netzwerke müssen geplant und dokumentiert sein, das WLAN muss segmentiert sein, die Passwortrichtlinien müssen umgesetzt werden und das Patchmanagement benötigt festgelegte Zuständigkeiten. So ist man für die digitale Transformation der Gebäudeautomation deutlich besser gewappnet. ●



**Autorin:**  
Britta Kalscheuer,  
Redaktion »de«