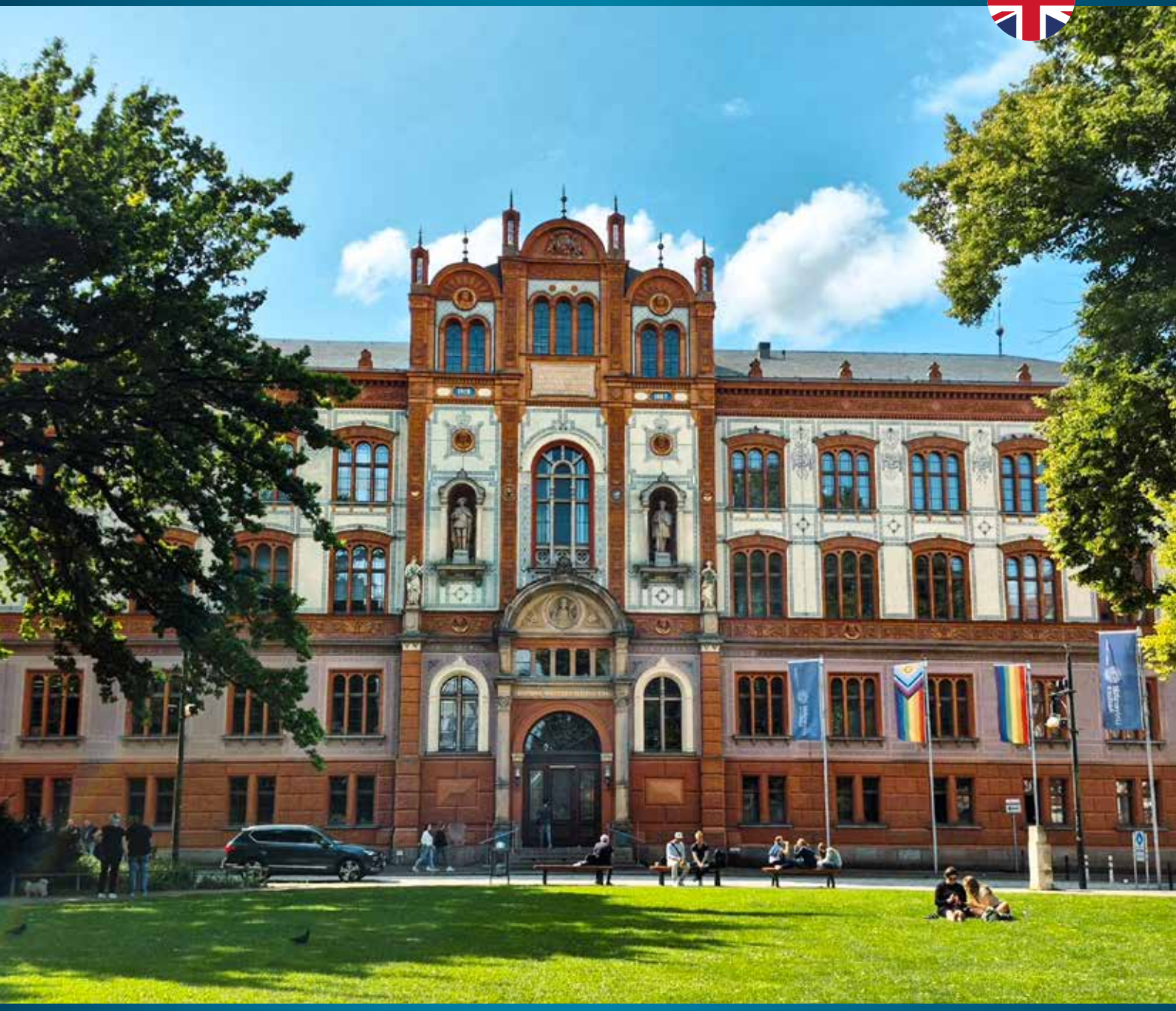
www.big-eu.org

ISSN 1614-9572

BACnet Europe Journal

Issue / Ausgabe 43

September/ September 2025



Managementplattform für Digitalisierung und Energieeffizienz

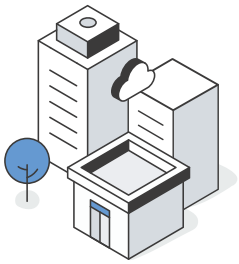
Smarter operations. Lower energy. Higher efficiency

B-CON
Smart Building Hub

Die Standardschnittstelle zu Ihrer Gebäudetechnik / you standard-interface at all buildings services

MBE und Energie-Management / BMS and energy managment

- Visualisierung / visalization
- Alarm & Event
- Zeitplan / schedule
- Trend
- Report
- Energie- / energy Management
- Energie- / energy Monitoring
- Energie-Controlling



Building-, Facility- and Asset-Management

- Wartungsmanagement / maintenance
- Technisches Monitoring / technical monitoring
- Instandhaltung / repair
- BIM-Server
- Raumbuchung / desk booking
- Business-Intelligence
- CO2-Bilanz / ESG
- CAFM
- Waste-Management
- ERP (SAP, ...)
- Datacenter Infrastructure Managements (DCIM)
- u.v.m / and much more

BACnet · Modbus · KNX · OPC · M-Bus · LoRa · MQTT · SNMP

- Anlagen-automation / system automation
- Raum-automation / room automation
- Energiedaten-erfassung / metering
- Sicherheits-technik / security systems
- Förder-technik / elevator and escaltor
- IT und Netz-werktechnik / IT- and network-systems
- IoT Systeme / IoT-systems

The BACnet BMS with energy management and open API

Die BACnet Management- und Bedieneinrichtung mit Energiemanagement und offenen Digitalisierungsschnittstellen

ICONAG
make buildings smarter

Zukunftssichere MBE/GLT und Energiemanagement-Systeme im Kontext des Gebäudeenergiegesetzes – herstellerneutrales Gebäudeautomationsmanagement mit BACnet, ModBus, KNX, LoRa und Co – Praxisseminar

Mit Gutscheincode „BIG-EU“ 300 Euro sparen

Anmeldung unter www.iconag.com/schulung

ICONAG-Leittechnik GmbH
D-55743 Idar-Oberstein
+49-6781-56234-0
info@iconag.com

www.iconag.com

Beyond Technology
Mehr als Technik

The Value of Open Systems for Sustainable Digitalization
Die Bedeutung offener Systeme für nachhaltige Digitalisierung

Dear Readers,

Openness and interoperability are the foundation of sustainable and future-proof building automation. In a world that increasingly depends on connected systems and real-time data, open communication protocols like BACnet are more relevant than ever – especially in mission-critical environments such as data centers.

Data centers are the backbone of the digital economy. They demand uncompromising availability, highest operational efficiency, and stringent compliance with energy and sustainability goals. In this context, the role of intelligent building automation – enabled by vendor-independent systems – is gaining strategic importance. BACnet not only ensures smooth interoperability across systems, but also enables transparency and efficiency through integrated energy monitoring, optimized control strategies, and open interfaces.

Modern data centers are no longer isolated technical islands – they are dynamic environments that must respond to changing demands in real-time. Open communication is the key to unlocking this flexibility. From cooling and power management to access control and fault detection, BACnet allows for a holistic and responsive infrastructure management that is both secure and scalable.

We at BIG-EU continue to promote the standardization and evolution of BACnet. Our goal is to support operators, integrators, and manufacturers in creating solutions that are sustainable, secure, and open. Because open systems are not just a technological choice – they are a strategic one.

I hope you enjoy reading this new edition of the BACnet Europe Journal, which once again brings together valuable insights, innovations, and success stories from across the BACnet community.

Stefan Pfützer
Treasurer, Executive Board
BACnet Interest Group Europe e. V.

Sehr geehrte Damen und Herren,

Offenheit und Interoperabilität sind die Grundlage nachhaltiger und zukunftssicherer Gebäudeautomation. In einer Welt, die zunehmend auf vernetzte Systeme und Echtzeitdaten angewiesen ist, sind offene Kommunikationsprotokolle wie BACnet wichtiger denn je – insbesondere in geschäftskritischen Bereichen wie Rechenzentren.

Rechenzentren bilden das Rückgrat der digitalen Wirtschaft. Sie verlangen kompromisslose Verfügbarkeit, höchste Betriebseffizienz und gleichzeitig die Einhaltung anspruchsvoller Energie- und Nachhaltigkeitsziele. In diesem Kontext gewinnt die Rolle intelligenter Gebäudeautomation, die auf herstellerunabhängigen Systemen basiert, strategisch an Bedeutung. BACnet ermöglicht nicht nur die reibungslose Interoperabilität zwischen Systemen, sondern schafft durch integrierte Energiemonitoring-Funktionen, optimierte Regelstrategien und offene Schnittstellen Transparenz und Effizienz.

Moderne Rechenzentren sind längst keine isolierten technischen Inseln mehr – sie sind dynamische Umgebungen, die sich in Echtzeit an veränderte Anforderungen anpassen müssen. Offene Kommunikation ist der Schlüssel zu dieser Flexibilität. Von der Kühlung und Energieversorgung über Zugangskontrolle bis hin zur Störungsanalyse erlaubt BACnet ein ganzheitliches und responsives Infrastrukturmanagement – sicher und skalierbar zugleich.

Wir in der BIG-EU setzen uns weiterhin für die Standardisierung und Weiterentwicklung von BACnet ein. Unser Ziel ist es, Betreiber, Integratoren und Hersteller dabei zu unterstützen, Lösungen zu schaffen, die nachhaltig, sicher und offen sind. Denn offene Systeme sind nicht nur eine technologische Entscheidung – sie sind eine strategische.

Ich wünsche Ihnen eine inspirierende Lektüre der aktuellen Ausgabe des BACnet Europe Journals, das wieder zahlreiche Impulse, Innovationen und Erfolgsgeschichten aus der Welt von BACnet vereint.

Stefan Pfützer
Schatzmeister im Vorstand
BACnet Interest Group Europe e. V.

NEW COURSE ***NOW AVAILABLE!***

Sign-up for a FREE account

THE BACnet INSTITUTE

Courses • Resources • Community

Stay ahead of the curve with our FREE BACnet Cybersecurity course!

As buildings become more and more interoperable, so should cybersecurity.

The BACnet Cybersecurity course provides an overview of BACnet Secure Connect (BACnet/SC), focusing on its significance in enhancing the security of interoperable building automation systems. Participants will gain an understanding of how BACnet/SC differs from existing security measures, its technical aspects and its interaction with other BACnet devices. This course also addresses the cybersecurity challenges and future strategies for improving BACnet security. This course also places BACnet/SC in the context of the larger building automation cybersecurity landscape.

Start learning with FREE courses, resources, and our expert forum at ***thebacnetinstitute.org****! Additional free, online, and self-paced courses include* ***BACnet Basics****,* ***BACnet Device Profiles****, and the* ***Facility Manager's Guide to Building Automation Systems****.*

Contents Inhalt

Editorial – Vorwort

Solutions – Anwendungen

BACnet Insight

Technology – Technik

Young Talent for Building Automation – Nachwuchs für die Gebäudeautomation

Products – Produkte

BACnet Interest Group Europe News

Cover Photo | Titelbild
University of Rostock, Main Building (p. 12) © Peter Wickboldt

Energy Management and Building Automation at the University of Rostock with Qanteon

Energiemanagement und Gebäudeautomation an der Universität Rostock mit Qanteon

The University of Rostock covers all areas of a comprehensive university with its range of subjects and, with over 160 buildings and building complexes, has numerous special features, particularly in teaching and research. The University of Rostock relies consistently on comprehensive building automation to ensure the safe operation of its buildings and associated infrastructure.

Die Universität Rostock deckt mit ihrem Fächerspektrum alle Bereiche einer Volluniversität ab und verfügt mit über 160 Gebäuden und Gebäudekomplexen über zahlreiche Besonderheiten insbesondere in der Lehre und Forschung. Für den sicheren Betrieb der Gebäude und der zugehörigen Infrastruktur setzt die Universität Rostock konsequent auf eine umfassende Gebäudeautomation.

In addition to modern measurement, control, and regulation technology at the field level, this includes DDC controllers at the automation level and a powerful management level. Among other things, with the BACnet Advanced Operator Workstation Qanteon from Kieback&Peter. Qanteon is an innovative software solution that enables classic building automation with integrated energy management to operate all properties efficiently, reliably, and above all safely and transparently.

Building Automation for a Wide Range of Requirements

The requirements for building technology at the University of Rostock are very diverse:

- Event rooms must be prepared quickly and flexibly for conferences, presentations, and receptions.
- Lecture halls and seminar rooms require reliable and quiet air conditioning that adapts to changing occupancy. The focus here is not only on temperatures, but also on CO_2 levels in the auditorium.
- Laboratories require precise temperature, humidity, and air quality control to ensure safe and stable working conditions. The University of Rostock has a complex variety of S3 laboratories with airlocks and clean rooms for animal experiments, as well as a vibration-free laser testing laboratory.
- Administrative areas with continuous assurance and documentation of workplace guidelines.

The university's own data center poses a particular challenge. As a communications hub, high-performance computing cluster, and service provider for all areas of the university, 100% availability is essential. This requires not only highly trained personnel, but also special expertise in building automation, among other things, to ensure safety-related conditions and automated processes in emergency operation.

Thanks to networked building automation, all these scenarios can be monitored and controlled centrally. The system reacts automatically to utilization, time of day, or outside temperature, ensuring that only as much energy is consumed as is actually necessary and that supply security is guaranteed at all times.

Qanteon as a Central Hub for Operations and Energy Management

Qanteon combines energy management and building automation in a single system. It automatically collects consumption and generation data for electricity, heating, cooling, and water via the BACnet protocol and visualizes it in a clearly structured interface.

The integrated analysis functions reveal potential savings and enable targeted optimizations. This has already resulted in noticeable energy savings in individual parts of the building – while maintaining a consistently high level of comfort.

In addition to the numerous analysis options, a special feature is the automatic creation of reports, e.g., in the form of invoices, and their automatic dispatch. The University of Rostock uses this tool for the fully automated billing of co-supplied institutions, enabling immediate and transparent billing of material and media requirements.

Dashboard and benchmark views allow property users to be directly involved in the transparent and immediate analysis of "their" property's requirements. A friendly competition between users regarding the energy requirements of their buildings can be a positive side effect of the benchmarking process.

Support in Everyday Life – Stationary and Mobile

A particular advantage is the combination of stationary operation and the mobile Qanteon Readme app.

There are still meter reading areas that, even with modern infrastructure, can only be recorded manually due to low consumption values, unfavorable locations, or high investment costs. With the Readme app, we use house and building technicians to record meter readings directly on site, which are then automatically synchronized with the system. This saves time, reduces walking distances, and minimizes sources of error in manual (handwritten) recording.

Reliable Alarms and Compliance with Standards

Qanteon automatically reports deviations, peak loads, or critical values so that measures can be taken immediately. In addition, the system supports compliance with energy management standards such as ISO 50001 and provides all necessary evidence and key figures.

Conclusion

The long-standing collaboration between the University of Rostock and Kieback&Peter shows how classic building automation and modern energy management complement each other perfectly, how weak points are analyzed jointly, and how solutions are created that both serve the University of Rostock and advance Kieback&Peter's software development. A current example of this is the joint development of the integration of LoRaWAN components and the security strategy developed for this purpose.

Laboratory at the University of Rostock
Labor an der Universität Rostock

In the future, the University of Rostock will continue to do everything in its power to ensure intelligent control systems for teaching and research, to guarantee high security standards in data communication and processing, and at the same time to present energy costs transparently and reduce energy consumption wherever possible.

Building management technology is at the heart of property management and is subject to constant change and external influences. As the University of Rostock, it is therefore a constant challenge for us to help shape and develop these systems. ■

Neben moderner Mess-, Steuer- und Regeltechnik in der Feldebene gehören dazu die DDC-Controller in der Automationsebene sowie eine leistungsfähige Managementebene. U.a. mit der BACnet Advanced Operator Workstation Qanteon von Kieback&Peter. Qanteon bietet als innovative Softwarelösung die Möglichkeit klassische Gebäudeautomation, mit dem integriertem Energiemanagement alle Liegenschaften effizient, zuverlässig und vor allem sicher und transparent zu betreiben.

Gebäudeautomation für unterschiedlichste Anforderungen

Die Anforderungen an die Gebäudetechnik sind an der Universität Rostock sehr vielfältig:

- Veranstaltungsräume müssen für Tagungen, Präsentationen und Empfänge schnell und flexibel vorbereitet werden.
- Hörsäle und Seminarräume benötigen eine zuverlässige und leise Klimatisierung, die sich an die wechselnde Belegung anpasst. Im Fokus stehen hier nicht nur die Temperaturen, sondern auch die CO_2-Belastungen für das Auditorium.
- Labore erfordern präzise Temperatur-, Feuchte- und Luftqualitätsregelungen, um sichere und stabile Arbeitsbedingungen zu gewährleisten. Dabei verfügt die Universität Rostock über eine komplexe Vielfalt von S3 Laboren mit Schleusen und Reinstbereichen für Tierversuche bis zum erschütterungsfreien Laserversuchslabor
- Administrative Bereiche mit der kontinuierlichen Sicherstellung und Dokumentation der Arbeitsstättenrichtlinie

Eine besondere Herausforderung stellt das universitätseigene Rechenzentrum dar. Als Kommunikationszentrale, Hochleistungsrechencluster und Dienstleister für alle Bereiche der Universität ist eine 100-prozentige Verfügbarkeit unerlässlich. Dies erfordert nicht nur sehr gut geschultes Personal, sondern besonders Know How in der Gebäudeautomation u.a. zur Gewährleistung sicherheitsrelevanter Rahmenbedingungen und automatisierter Prozesse im Notbetrieb.

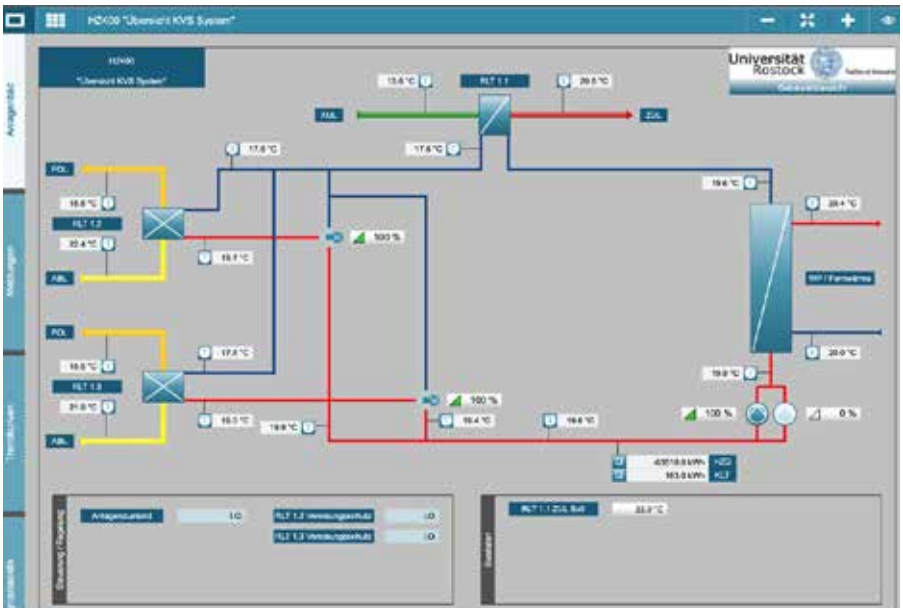
Durch die vernetzte Gebäudeautomation können alle diese Szenarien zentral überwacht und gesteuert werden. Das System reagiert automatisch auf Auslastung, Tageszeit oder Außentemperatur und stellt so sicher, dass nur so viel Energie verbraucht wird, wie tatsächlich nötig ist und die Versorgungssicherheit jederzeit gewährleistet ist.

Qanteon als zentrale Schaltstelle für den Betrieb und dem Energiemanagement

Qanteon verbindet Energiemanagement und Gebäudeautomation in einem System. Es erfasst Verbrauchs- und Erzeugerdaten für Strom, Wärme, Kälte und Wasser automatisch über das BACnet-Protokoll und visualisiert sie in einer klar strukturierten Oberfläche.

Die integrierten Analysefunktionen machen Einsparpotenziale sichtbar und ermöglichen gezielte Optimierungen. So konnten in einzelnen Gebäudeteilen bereits spürbare Energieeinsparungen erzielt werden – bei gleichbleibend hohem Komfort.

Ein besonderes Merkmal stellt neben den zahlreichen Analyseoptionen die automatische Erstellung von Berichten z.B. in Form von Rechnungen und die automatische Versendung dar. Die Universität Rostock nutzt dieses Tool



u.a. für die vollautomatische Abrechnung von mitversorgten Institutionen und ermöglicht somit eine sofortige und transparente Abrechnung der Stoff- und Medienbedarfe.

Dashboard- und Benchmarkansichten ermöglichen die direkte Einbeziehung der Liegenschaftsnutzer zur transparenten und sofortigen Bedarfsanalyse „ihrer" Liegenschaft. Ein kollegialer Konkurrenz-kampf über den nutzerabhängigen Energiebedarf der Gebäude kann dabei ein positiver Nebeneffekt im Benchmarkverfahren sein.

Unterstützung im Alltag – stationär und mobil

Ein besonderer Vorteil ist die Kombination aus stationärer Bedienung und der mobilen Qanteon Readme App.

Es gibt immer noch Zählwerterfassungsbereiche, die auch bei einer modernen Infrastruktur infolge von geringen Verbrauchswerten, ungünstigen Lagen oder zu hohen Investitionskosten nur händisch erfasst werden können. Mit der Readme App erfassen wir durch die Haus- und Gebäudetechniker Zählerstände direkt vor Ort, die dann automatisch mit dem System synchronisiert werden. Das spart Zeit, reduziert Laufwege und minimiert Fehlerquellen bei der manuellen (handschriftlichen) Erfassung.

Zuverlässige Alarmierung und Normkonformität

Qanteon meldet Abweichungen, Lastspitzen oder kritische Werte automatisch, so dass sofort Maßnahmen eingeleitet werden können. Zudem unterstützt das System die Einhaltung von Energiemanagementnormen wie ISO 50001 und liefert alle erforderlichen Nachweise und Kennzahlen.

Fazit

Die langjährige Zusammenarbeit der Universität Rostock mit Kieback&Peter zeigt, wie klassische Gebäudeautomation und modernes Energiemanagement sich optimal ergänzen, Schwachpunkte gemeinsam analysiert und Lösungen geschaffen werden, die sowohl der Universität Rostock dienen, wie auch Kieback&Peter in ihrer Softwareentwicklung vorantreiben. Ein aktuelles Beispiel stellt hierbei die gemeinsame Entwicklung der Integration von LoRaWAN- Komponenten und die hierzu entwickelte Sicherheitsstrategie dar.

Auch in Zukunft wird die Universität Rostock alles daran setzten, intelligente Steuerungssysteme zur Gewährleistung des Lehr- und Forschungsbetriebes sicherzustellen, den hohen Sicherheitsstandard in der Datenkommunikation und -verarbeitung zu gewährleisten, gleichzeitig die Energiekosten transparent darzustellen und w,o es möglich ist, den Energiebedarf zu senken.

Die Gebäudeleittechnik ist für den Liegenschaftsbetrieb das Herzstück und unterliegt ständigem Wandel und den äußeren Einflüssen. Es ist für uns als Universität Rostock somit eine ständige Herausforderung, diese Systeme mitzugestalten und zu entwickeln. ■

Exterior view of Rostock University – new and old main buildings
Außenansicht Universität Rostock – Hauptgebäude Neu und Altbau

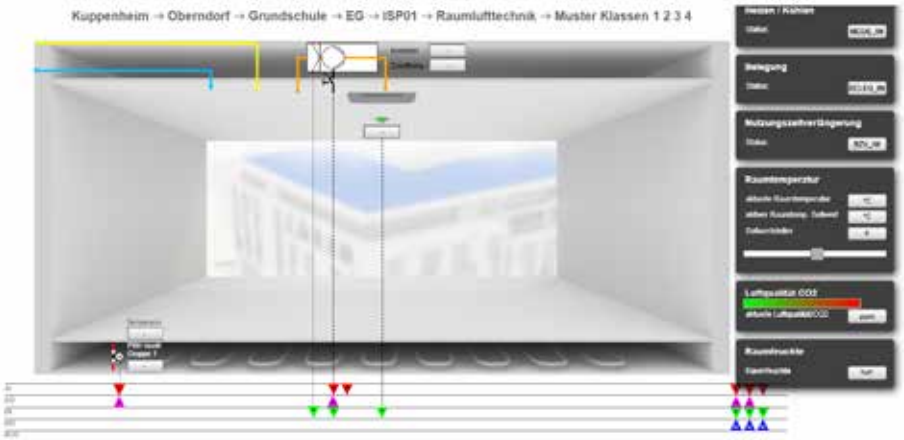
Peter Wickboldt
Referatsleiter Betriebstechnik und Logistik | Universität Rostock
peter.wickboldt@uni-rostock.de | www.uni-rostock.de

OASstudio: Web-Based Design Platform for the Effective Digitization of Building Technology

OASstudio: Webbasierte Designplattform für die effektive Digitalisierung der Gebäudetechnik

OAS Open Automation Systems presents OASstudio, a pioneering, web-based desig and configuration platform that redefines the entire building automation workflow. From system diagrams and graphical visualization to the automatic generation of documentation in accordance with VDI 3814 and DIN EN ISO 16484 for planning purposes, this holistic concept brings together all the individual steps in a single digital process. This makes it easy to configure and plan complex systems, and if necessary, to expand them in a user-friendly manner without redrawing them.

Mit OASstudio präsentiert OAS Open AutomationSystems eine zukunftsweisende, webbasierte Design- und Konfigurationsplattform, die den gesamten Workflow der Gebäudeautomation neu definiert. Vom Anlagenschema über die grafische Visualisierung bis zur automatischen Generierung aller Unterlagen gemäß VDI 3814 und DIN-EN-ISO 16484 für die Planung: Das ganzheitliche Konzept führt alle Einzelschritte in einem einzigen digitalen Prozess zusammen. So lassen sich auch komplexe Anlagen einfach konfigurieren, planen und bei Bedarf bedienerfreundlich und ohne Neuzeichnung erweitern.



Configurator: Example room automation, primary school, classrooms on the ground floor
Konfigurator: Beispiel Raumautomation, Grundschule, Klassen im EG

Traditionally, the planning of technical building equipment takes place in several consecutive steps, which are often separate from one another. It begins with creating a graphical representation of the system diagram in CAD systems and continues with coordinating with specialist planners. It also involves manually transferring information to function lists in accordance with VDI 3814. Then, the visualization for the building management system is created. The BA system diagram, which depicts all components of a heating system – from heat generation to boilers, heat pumps, and combined heat and power plants – plays a central role as a common basis for all subsequent steps.

However, it is precisely at this stage that communication breakdowns, unnecessary coordination and avoidable sources of error frequently occur. With OASstudio, OAS is setting a new standard: this web-based design and configuration platform brings together all the relevant steps in a continuous, cloud-based process for the first time. It offers the benefits of an intuitive configurator alongside many years of practical expertise, and incorporates tools such as CAD and Excel, as well as enabling the creation of system diagrams, graphical visualizations and complete planning documents in accordance with DIN EN ISO 16484.

Based on this, even complex and customized systems can be configured with just a few clicks. For instance, users can design a double boiler system with return flow elevation and flexibly expand it as required, such as by adding a third boiler, without the need for redrawing or time-consuming coordination.

Systematic Digitization

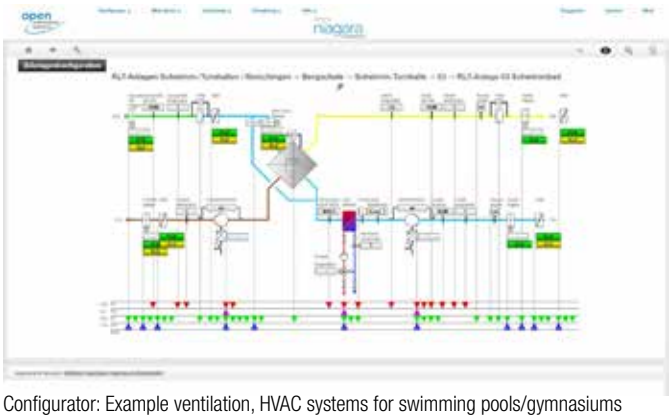
The OAS configuration tool provides all project participants with the complete system diagram from the planning phase onwards, as well as a full description and an overview of all physical data points, inputs, and outputs. Other advantages include functional texts and Excel-based I/O lists. Service specifications are currently being developed and will be available with the next update, including an automatically generated GAEB interface. Additionally, the graphical representation is semi-automatically linked to the control software. Thus, the cloud-based visualization enables intuitive navigation from the campus view to the individual components. Last but not least, the OAS Graphic Library provides planners and system partners with access to an extensive collection of symbols and elements covering all areas of heating, air conditioning, ventilation and room automation when configuring building technology.

This is supplemented by function macros specially developed for the Niagara framework. These contain all the necessary control modules, such as those for temperature requirements or heating curve control, and can be integrated directly into the automation software. This includes automatic data point linking via 'tagging'. As a result, even the programming of

Configurator: Example ventilation, HVAC systems for swimming pools/gymnasiums
Konfigurator: Beispiel Lüftung, RLT-Anlagen Schwimm-/Turnhallen

Configurator: Example heating, boiler. Heating circuits, WWB, fresh water cascade
Konfigurator: Beispiel Heizung, Kessel. Heizkreise, WWB, Frischwasserkaskade

Configurator: Example heating, trade fair, heating circuits
Konfigurator: Beispiel Heizung, Messe, Heizkreise



Configurator: Example ventilation, HVAC systems for swimming pools/gymnasiums
Konfigurator: Beispiel Lüftung, RLT-Anlagen Schwimm-/Turnhallen

entire systems can be completed in just a few minutes. Data points, graphics and structures created in OASstudio can also be transferred directly to the Niagara Workbench.

Standard, Open and Fully Automated

As a specialist in open building automation systems, OAS relies on neutral data exchange throughout the configuration process with OASstudio. Managing Director Ralf Rostock emphasizes: “The system remains open, flexible and independent, regardless of whether BACnet, Modbus, a proprietary bus or boilers from different manufacturers are used.”

The platform is optimized for Niagara technology, on which all OAS solutions are based. The advantage: All Niagara framework-based automation systems are supported directly, regardless of the manufacturer. This means that all project participants, from investors to planners to integrators, can be provided with an attractive visualization interface at an early stage. ■

More at: www.openautomationsystems.store/produkte/oas-studio

Die Planung der technischen Gebäudeausrüstung erfolgt traditionell in mehreren aufeinanderfolgenden Schritten, die häufig voneinander getrennt sind. Dies beginnt mit der grafischen Darstellung des Anlagenschemas in CAD-Systemen, erstreckt sich über die Abstimmung mit Fachplanern und umfasst die manuelle Übertragung in Funktionslisten gemäß VDI 3814. Anschließend wird die Visualisierung für die Gebäudeleittechnik erstellt. Besonders das GA-Anlagenschema, das alle Komponenten einer Heizungsanlage – von der Wärmeerzeugung über Kessel und Wärmepumpen bis hin zu Blockheizkraftwerken – abbildet, spielt dabei eine zentrale Rolle als gemeinsame Grundlage für alle weiteren Schritte.

Doch genau an dieser Stelle entstehen immer wieder Medienbrüche, redundante Abstimmungen und vermeidbare Fehlerquellen. Mit OASstudio setzt OAS einen neuen Standard: Die webbasierte Design- und Konfigurationsplattform vereint erstmals alle relevanten Schritte in einem durchgängigen, cloudbasierten Prozess. Sie kombiniert die Vorteile eines intuitiven Konfigurators mit langjährigem Praxis-Know-how und integriert Werkzeuge wie CAD und Excel ebenso wie die normgerechte Erstellung von Anlagenschemata, grafischen Visualisierungen und vollständigen Planungsunterlagen gemäß DIN EN ISO 16484.

Auf dieser Basis lassen sich selbst komplexe und individuelle Anlagen mit wenigen Klicks konfigurieren. So können Nutzer beispielsweise eine doppelte Kesselanlage mit Rücklaufanhebung planen und diese bei Bedarf ohne Neuzeichnung oder aufwändige Abstimmung flexibel erweitern – etwa um einen dritten Kessel.

Digitalisierung mit System

Mit dem Konfigurations-Tool von OAS erhalten alle Projektbeteiligten bereits ab der Planungsphase nicht nur das vollständige Anlagenschema, sondern auch eine vollständige Beschreibung sowie eine Übersicht aller physikalischen Datenpunkte und Ein- und Ausgänge. Weitere Vorteile umfassen unter anderem Funktionstexte und Excel-basierte IO-Listen. Automatisch generierte Leistungsverzeichnisse inklusive GAEB-Schnittstelle sind derzeit in Entwicklung und mit dem nächsten Update verfügbar. Dazu kommt die halbautomatische Verknüpfung der

grafischen Darstellung mit der Steuerungssoftware. Die cloudbasierte Visualisierung ermöglicht so eine intuitive Navigation von der Campus-Ansicht bis hin zur einzelnen Komponente.

Nicht zuletzt steht Planern und Systempartnern bei der Konfiguration der Gebäudetechnik mit der OAS Graphic Library eine umfangreiche Symbol- und Elemente-Sammlung zur Verfügung, die alle Bereiche von Heizung, Klima, Lüftung und Raumautomation abdeckt.

Ergänzt wird sie durch Funktionsmakros, die speziell für das Niagara-Framework entwickelt wurden. Diese enthalten alle relevanten Regelmodule, etwa für Temperaturanforderungen oder die Heizkurvensteuerung, und können – inklusive automatischer Datenpunktverknüpfung via „Tagging" – direkt in die Automationssoftware eingebunden werden. Selbst die Programmierung ganzer Anlagen lässt sich so in nur wenigen Minuten realisieren. In OASstudio erstellte Datenpunkte, Grafiken und Strukturen lassen sich zudem direkt in die Niagara Workbench übernehmen.

Standardoffen und durchgängig automatisiert

Als Spezialist für offene Gebäudeautomationssysteme setzt OAS bei der Konfiguration mit OASstudio durchgängig auf einen standardmäßig neutralen Datenaustausch: Geschäftsführer Ralf Rostock betont: „Das System bleibt offen, flexibel und unabhängig, ganz egal ob BACnet, Modbus, proprietärer Bus oder Kessel unterschiedlicher Hersteller zum Einsatz kommen."

Optimiert ist die Plattform dabei für die Niagara-Technologie, auf deren Grundlage alle OAS-Lösungen aufbauen. Der Vorteil: Herstellerunabhängig werden alle Niagara-Framework-basierten Automatisierungssysteme direkt unterstützt, sodass alle Projektbeteiligten vom Investor über den Planer bis zum Integrator frühzeitig mit einer ansprechenden Visualisierungsoberfläche versorgt werden können.

Weitere Produktinformationen unter:
www.openautomationsystems.store/produkte/oas-studio

Ralf Rostock
Geschäftsführender Gesellschafter | OAS Open AutomationSystems GmbH
sales@oa-systems.de | www.openautomationsystems.store

Buildings in Digital Dialogue: Why GEZE Relies on BACnet

Gebäude im digitalen Dialog: Warum GEZE auf BACnet setzt

In modern smart buildings, simply automating systems is no longer enough – what matters is their seamless communication across all technical trades. Especially in the area of door, window, and safety technology, integration into the building management system is often incomplete or entirely lacking. GEZE bridges this gap with myGEZE Control: an open solution that connects door, window, and safety systems – regardless of manufacturer – using the established BACnet protocol or OPC UA, and integrates them into the building management system.

In modernen Smart Buildings reicht es nicht aus, Systeme zu automatisieren – entscheidend ist ihre nahtlose Kommunikation über alle Gewerke hinweg. Gerade im Bereich Tür-, Fenster- und Sicherheitstechnik bleibt die Integration in die Gebäudeleittechnik oft lückenhaft oder fehlt ganz. GEZE schließt diese Lücke mit myGEZE Control: einer offenen Lösung, die Tür-, Fenster- und Sicherheitstechnik herstellerunabhängig über das etablierte BACnet-Protokoll oder OPC UA vernetzt und in die Gebäudeleittechnik integriert.

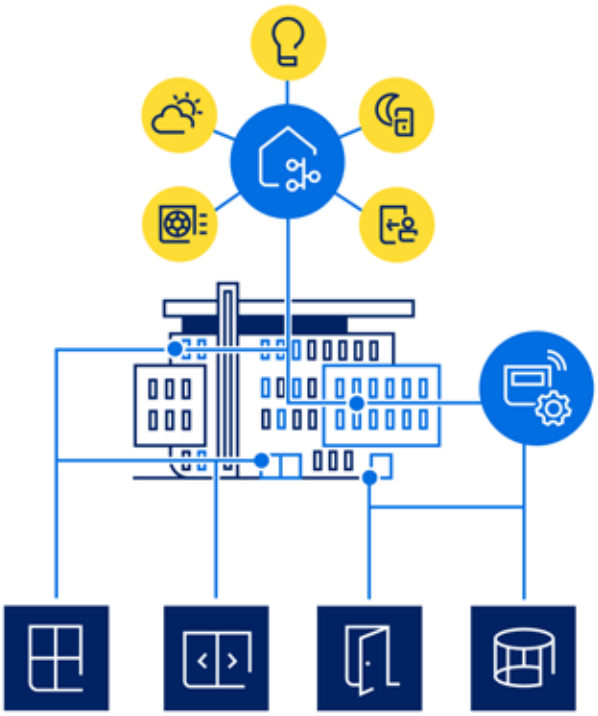
With myGEZE Control, building functions are intelligently linked across systems. Escape and rescue routes can be centrally monitored and controlled, ventilation scenarios automated, and maintenance strategically planned in advance.

Enhanced Safety, Comfort, and Transparency

Networked doors and windows provide real-time information about the building envelope. The entire system can be managed via a single device: doors can be centrally locked, escape routes released, or smoke and heat extraction triggered. Maintenance and operations are also simplified, as malfunctions are reported immediately – before they become a problem.

By integrating into a centralized building management system, cross-discipline communication becomes possible – for instance, between windows, heating, and shading. If a window is opened, the heating output can automatically decrease, or if CO_2 levels are high, the ventilation system can start as needed. This not only improves user comfort, but also significantly enhances energy efficiency.

Sensors further enable the intelligent control of windows – for natural night cooling, automated shading, or fresh air supply in response to elevated CO_2 levels. The result is a noticeably better indoor climate and reduced energy



consumption. Over a 20-year period, this can lead to savings of up to 50% in ventilation costs.

The myGEZE Connectivity Payback Calculator shows how economically this pays off. It evaluates individual usage scenarios and clearly indicates when the investment in automated door and window systems and their networking will amortize. This payback is achieved through specific savings – such as lower energy consumption, reduced maintenance effort, or improved indoor air quality that boosts productivity. This makes smart building planning fact-based and future-ready.

Thinking of doors and windows as integral components of building automation pays off – by optimizing comfort, maximizing safety, and sustainably increasing property value.

Learn more about GEZE's solutions:
www.connectivity.geze.com/de/vernetzung-tuer-fenster

Mit myGEZE Control werden Gebäudefunktionen gewerkübergreifend intelligent verknüpft. So lassen sich Flucht- und Rettungswege zentral überwachen und steuern, Lüftungsszenarien automatisieren und Wartungen vorausschauend planen.

Ein Plus an Sicherheit, Komfort und Transparenz

Vernetzte Türen und Fenster liefern in Echtzeit Informationen über den Zustand der Gebäudehülle. Über ein Endgerät lässt sich das komplette System steuern: Türen können zentral verriegelt, Fluchtwege freigegeben oder Rauch- und Wärmeabzüge ausgelöst werden. Auch Wartung und Betrieb werden einfacher, denn Störungen werden direkt gemeldet, bevor sie zum Problem werden.

Durch die Integration in ein übergeordnetes Leitsystem ist auch die gewerkeübergreifende Kommunikation möglich – etwa zwischen Fenster, Heizung und Verschattung. So kann sich bei geöffnetem Fenster die Heizleistung automatisch reduzieren oder bei hoher CO_2-Konzentration die Lüftung bedarfsgerecht starten. Das steigert nicht nur den Nutzerkomfort, sondern verbessert auch die Energieeffizienz spürbar.

Sensoren ermöglichen zudem die intelligente Steuerung von Fenstern: etwa für natürliche Nachtauskühlung, automatische Verschattung oder frische Luft bei hoher CO_2-Konzentration. Das verbessert das Raumklima spürbar und senkt den Energieverbrauch. So lassen sich – auf einen Zeitraum von 20 Jahren gerechnet – bis zu 50 Prozent der Lüftungskosten einsparen.

Wie wirtschaftlich sich das rechnet, zeigt der myGEZE Connectivity Amortisationsrechner. Er bewertet individuelle Nutzungsszenarien und macht sichtbar, ab wann sich der Invest in automatische Tür- und Fenstersysteme und ihre Vernetzung amortisiert. Die Amortisation ergibt sich durch konkrete Einsparpotenziale – etwa durch reduzierten Energieverbrauch, geringerer Wartungsaufwand oder bessere Raumluftqualität, die die Produktivität verbessert. Damit wird die Planung von Smart Buildings faktenbasiert und zukunftssicher.

Türen und Fenster als integraler Bestandteil der Gebäudeautomation zu denken, zahlt sich aus – für optimierten Komfort, höchste Sicherheit und eine nachhaltige Steigerung des Immobilienwerts.

Erfahren Sie mehr über die Lösungen von GEZE: www.connectivity.geze.com/de/vernetzung-tuer-fenster

GEZE GmbH
presse@geze.com
www.geze.de

Smarter Airports with Battery-Free Wireless Sensors

Intelligentere Flughäfen mit batterielosen Funksensoren

© Getty Images/iStockphoto

Bridging BACnet and Wireless EnOcean Technology

Airports are complex infrastructures where facility managers face significant challenges in maintaining high levels of passenger comfort while keeping energy use in check. Varying occupancy patterns across terminal zones – gates, lounges, baggage claim – require flexible, real-time environmental data to support optimal HVAC and lighting. Battery-free wireless sensors, integrated with BACnet-based building automation systems, provide an efficient, scalable solution for these challenges.

Scalable Sensing for Smart Terminals

Continuous monitoring of indoor environmental quality demands extensive sensor deployment – particularly across high-traffic public buildings like airport terminals. A conventional approach using wired or battery-powered sensors becomes cost-prohibitive due to installation labor and maintenance needs.

For example, Heathrow's four main terminals span over 540,000 m². Ensuring comfort and air quality in such a space requires dense sensor coverage – typically one CO_2 sensor per 2500 m², plus temperature, humidity, illumination, and motion detection. Roughly 400 multi-sensor devices would be necessary, each traditionally involving either extensive wiring or periodic battery replacement.

To address this challenge, multi-functional, battery-free wireless sensors powered by ambient energy sources offer a compelling alternative. With a pair of devices providing integrated temperature, humidity, CO_2, light, and occupancy detection, each pair minimizes the number of units needed while maximizing data coverage.

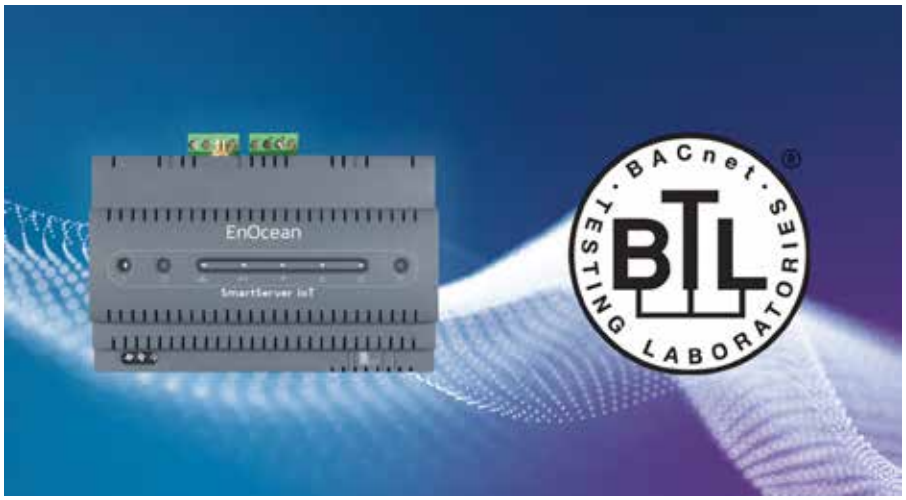
Energy Harvesting: No Wires, No Batteries

These sensors use indoor solar cells to harvest energy from ambient light enabling permanent operation without external power or batteries. Data transmission is wireless and can be easily integrated with BACnet-based systems, ensuring seamless integration into existing building management frameworks.

Installation becomes dramatically simplified: sensors can be adhered directly to walls or ceilings, eliminating the need for wires or battery maintenance. The result is a future-proof sensor infrastructure that is highly adaptable to spatial reconfigurations or operational shifts – ideal for dynamic environments like airports.

Integrating with the BACnet Network

The EnOcean SmartServer IoT integrates battery-free sensor data into the existing BACnet building management system. Each sensor appears as a digital twin with location and key values like CO_2, temperature, and humidity. These BACnet objects behave just like those from wired devices, making integration seamless. The SmartServer also supports semantic tagging with standards like Project Haystack or Brick Schema to simplify use in analytics and optimization tools.



SmartServer IoT © EnOcean

Conclusion

Battery-free wireless sensors represent a transformative technology for large-scale facilities. By harnessing energy harvesting and BACnet integration, airports can significantly improve passenger comfort while achieving demonstrable energy savings. These next-generation sensing technologies will play a critical role in making airports smarter and greener spaces. BACnet und drahtlose Enocean-Technologie ■

BACnet und drahtlose Enocean-Technologie

Flughäfen sind komplexe Infrastrukturen, in denen Facility Manager ein hohes Maß an Komfort für die Passagiere gewährleisten sollen und gleichzeitig den Energieverbrauch unter Kontrolle halten müssen. Unterschiedliche Auslastungsmuster in den verschiedenen Bereichen des Terminals – Gates, Lounges, Gepäckausgabe – erfordern flexible Echtzeitdaten für eine optimale Klimatisierung und Beleuchtung. Batterielose Funksensoren, die in BACnet-basierte Gebäudeautomationssysteme integriert sind, bieten eine effiziente und skalierbare Lösung für diese Herausforderungen.

Skalierbare Sensorik für intelligente Terminals

Die kontinuierliche Überwachung der Raumluftqualität erfordert den Einsatz einer Vielzahl von Sensoren. Ein herkömmlicher Ansatz mit kabelgebundenen oder batteriebetriebenen Sensoren ist aufgrund des Installationsaufwands und der Wartungsanforderungen kostspielig.

Beispielsweise erstrecken sich die vier Hauptterminals des Flughafens Heathrow über mehr als 540.000 m². Um Komfort und Luftqualität in solchen Gebäuden zu gewährleisten, ist eine dichte Sensorabdeckung erforderlich – in der Regel ein CO_2-Sensor pro 2500 m² sowie Sensoren für Temperatur, Luftfeuchtigkeit, Beleuchtung und Bewegung. Dazu wären etwa 400 Multisensoren erforderlich, entweder mit umfangreicher Verkabelung oder regelmäßigem Batteriewechsel.

Für diese Herausforderung bieten multifunktionale, batterielose Funksensoren, die mit Umgebungsenergie betrieben werden, eine überzeugende Alternative. Mit einem Gerätepaar, das integrierte Temperatur-, Feuchtigkeits-, CO_2- und Lichtmessungen sowie eine Anwesenheitserkennung bietet, minimiert jedes Paar die Anzahl der benötigten Einheiten und maximiert die Datenabdeckung.

Energy Harvesting: Keine Kabel, keine Batterien

Diese Sensoren nutzen Solarzellen, um Energie aus Licht zu gewinnen, wodurch ein dauerhafter Betrieb ohne externe Stromversorgung oder Batterien möglich ist. Dadurch wird die Installation vereinfacht. Die Datenübertragung erfolgt drahtlos und lässt sich problemlos in BACnet-basierte Systeme integrieren. Das Ergebnis ist eine zukunftssichere Sensorinfrastruktur, die sich leicht an Veränderungen anpassen lässt – ideal für dynamische Umgebungen wie Flughäfen.

BACnet-Integration

Der EnOcean SmartServer IoT integriert batterielose Sensordaten in das BACnet-Gebäudemanagementsystem. Jeder Sensor erscheint als digitaler Zwilling mit Standort und Schlüsselwerten wie CO_2, Temperatur und Luftfeuchtigkeit. Diese BACnet-Objekte verhalten sich genau wie die von kabelgebundenen Geräten, wodurch eine nahtlose Integration gewährleistet ist. Der SmartServer unterstützt auch das Semantic Tagging mit Standards (Project Haystack, Brick Schema) für die einfache Verwendung in Analyse-/ Optimierungstools.

Fazit

Batterielose Funksensoren stellen eine transformative Technologie für große Gebäude dar. Durch die Nutzung von Energy Harvesting und BACnet-Integration können Flughäfen den Komfort für Passagiere deutlich verbessern und Energieeinsparungen erzielen. Diese Sensortechnologien werden eine entscheidende Rolle dabei spielen, Flughäfen zu intelligenteren und umweltfreundlicheren Orten zu machen. ■

EnOcean
Sustainable IoT

Rich Blomseth
Director of Product Management at EnOcean
www.enocean.com

Technical Monitoring – The Key to Digital Energy Efficiency

Technisches Monitoring als Schlüssel zur digitalen Energieeffizienz

From regulatory requirement to intelligent building optimization

Von der gesetzlichen Vorgabe zur intelligenten Gebäudeoptimierung

In today's world, energy efficiency is no longer just a cost factor – it has become a core component of sustainable corporate strategy. As a result, building owners and planners are increasingly turning their attention to comprehensive monitoring solutions. evon is currently developing a powerful, standards-compliant, and fully integrated solution for technical monitoring of building systems – designed to seamlessly integrate with its established building management system and meet current regulatory requirements. The solution is in the final stages of development and testing and will soon become part of evon's product portfolio.

Legislation as a Driver of Innovation

Across Europe, regulatory requirements for buildings and technical systems are becoming increasingly stringent. Leading the charge is the European Union's Energy Performance of Buildings Directive (EPBD 2024), which must be implemented by all member states by May 2026. Its goal: a digitally enabled, energy-efficient building operation through mandatory monitoring and control systems. On the national level, the pressure is also growing. Germany's new Energy Efficiency Act, the VDI Guideline 6041 on technical monitoring in facility management, and the AMEV Recommendation No. 178 all set clear expectations for quality assurance and performance tracking throughout the building lifecycle – from planning and construction to ongoing operation. The result: building owners, planners, and integrators are actively seeking solutions that not only meet regulatory requirements but also deliver tangible added value.

Monitoring with Substance and Purpose

evon pursues a consistently integrated approach with its Technical Monitoring solution, which can be seamlessly embedded into existing Building Management Systems (BMS). Visualization, alarm management, dashboarding, automated trend analyses, and legally compliant documentation are comprehensively covered by a standardized library.

evon does not view Technical Monitoring as a bureaucratic obligation, but rather as an intelligent tool to increase operational transparency, sustainably optimize energy consumption, and reduce operating costs in the long term. Continuous data analysis enables early detection of inefficiencies and faulty system behavior. Energy and operational data can be evaluated automatically, with a standardized interface structure ensuring a consistent and comparable data basis.

Unlike conventional solutions that implement technical monitoring as a separate solution and only access data from the building automation system via external interfaces, evon's monitoring is fully integrated into the central building management system. This eliminates media discontinuities, providing unrestricted access to all relevant data and functions. As a result, data acquisition, analysis, and visualization are consolidated within a single platform, ensuring maximum transparency, high efficiency, and intuitive operation.

BACnet & BACnet Secure – Communication Standards Built for the Future

evon's technical monitoring offers full support for the BACnet protocol and complies with all specifications of the BACnet/SC Secure Connect standard. By integrating BACnet/SC, the system enables secure, encrypted, and reliable communication – a critical requirement for use in safety-sensitive and highly connected infrastructures. This ensures the solution is fully aligned with both current and future needs in smart building automation.

As a certified BACnet Advanced Operator Workstation (B-AWS), the solution meets all normative requirements, ensuring cross-vendor interoperability, standards compliance, and long-term investment security.

From Obligation to Opportunity: Monitoring as a Strategic Investment

evon's technical monitoring solution clearly demonstrates that what begins as a regulatory obligation can evolve into a valuable strategic asset – for operators, investors, and planners

Screenshot from evon's technical monitoring
Screenshot aus dem technischen Monitoring von evon
© evon GmbH

alike. With high-quality, continuously analyzed operational data, new opportunities emerge for predictive maintenance, resource-efficient operation, and the achievement of ambitious sustainability goals.

Learn more about the upcoming features and wide-ranging applications of evon's technical monitoring system. ■

Von der gesetzlichen Vorgabe zur intelligenten Gebäudeoptimierung

In einer Zeit, in der Energieeffizienz längst nicht mehr bloß ein Kostenfaktor, sondern ein zentrales Element nachhaltiger Unternehmensstrategien ist, rücken ganzheitliche Monitoringlösungen zunehmend in den Fokus der Gebäudebetreiber und Planer. evon arbeitet derzeit intensiv an einer leistungsfähigen, normkonformen und vollständig integrierten Lösung für das Technische Monitoring gebäudetechnischer Anlagen – nahtlos kombinierbar mit dem etablierten Gebäudemanagementsystem und perfekt abgestimmt auf aktuelle gesetzliche Anforderungen. Die Lösung befindet sich aktuell in der Entwicklungs- und Erprobungsphase und wird zukünftig das Produktportfolio von evon erweitern.

Gesetzgebung als Innovationstreiber

Die regulatorischen Rahmenbedingungen für Gebäude und technische Anlagen verschärfen sich europaweit. Allen voran die Energy Performance of Buildings Directive (EPBD 2024) der EU, die bis Mai 2026 in allen Mitgliedsstaaten umzusetzen ist. Ziel: ein digital gestützter, energieeffizienter Gebäudebetrieb durch verpflichtende Monitoring- und Steuerungssysteme. Auch auf nationaler Ebene wächst der Druck: Das neue Energieeffizienzgesetz, die VDI-Richtlinie 6041 zum Technischen Monitoring im Facility Management sowie die AMEV-Empfehlung Nr. 178 stellen klare Anforderungen an Qualitätssicherung und Effizienzkontrolle im Lebenszyklus von Gebäuden – von der Planung über die Errichtung bis zum Betrieb. Die Konsequenz: Gebäudebetreiber, Planer und Integratoren suchen nach Lösungen, die regulatorische Vorgaben nicht nur erfüllen, sondern echten Mehrwert schaffen.

Monitoring mit System und Substanz

evon verfolgt mit seinem Technischen Monitoring einen konsequent integrierten Ansatz, der sich vollständig in bestehende Building Management Systems (BMS) integrieren lässt. Visualisierung, Alarmmanagement, Dashboarding, automatische Trendanalysen und eine gesetzeskonforme Dokumentation werden dabei durch eine standardisierte Bibliothek vollständig abgedeckt.

Dabei versteht evon Technisches Monitoring nicht als bürokratische Pflicht, sondern als intelligentes Instrument zur Erhöhung der Betriebstransparenz, zur nachhaltigen Optimierung von Energieverbräuchen und zur langfristigen Senkung der Betriebskosten. Ineffizienzen und fehlerhaftes Anlagenverhalten sollen frühzeitig durch kontinuierliche Datenanalyse erkannt werden. Energie- und Betriebsdaten lassen sich automatisiert auswerten, wobei eine standardisierte Schnittstellenstruktur eine konsistente und vergleichbare Datenbasis schafft.

Im Unterschied zu herkömmlichen Lösungen, die das Technische Monitoring als separate Lösung implementieren und nur über externe Schnittstellen auf Daten aus der Gebäudeautomation zugreifen, ist das Monitoring von evon vollständig in das zentrale Gebäudemanagementsystem integriert. Medienbrüche entfallen, sämtliche relevanten Daten und Funktionen stehen uneingeschränkt zur Verfügung. Dadurch werden Erfassung, Analyse und Visualisierung innerhalb einer Plattform gebündelt, was maximale Transparenz, hohe Effizienz und eine intuitive Bedienung ermöglicht.

BACnet & BACnet Secure – Standardisierte Kommunikation mit Zukunft

Das Technische Monitoring von evon unterstützt das BACnet-Protokoll in vollem Umfang und erfüllt sämtliche Spezifikationen des BACnet/SC Secure Connect Standards. Die Integration von BACnet/SC gewährleistet eine sichere, verschlüsselte und ausfallsichere Kommunikation – ein wesentliches Merkmal für den zuverlässigen Betrieb sicherheitskritischer sowie stark vernetzter Infrastrukturen. Damit ist die Lösung optimal auf die aktuellen wie auch zukünftigen Anforderungen der intelligenten Gebäudeautomation vorbereitet.

Als zertifizierte BACnet Advanced Operator Workstation (B-AWS) erfüllt die Lösung alle vorgeschriebenen Anforderungen vollständig. Sie gewährleistet eine herstellerübergreifende Interoperabilität, Normkonformität und langfristige Investitionssicherheit.

Pflicht wird zur Chance: Monitoring als Zukunftsinvestition

Das Technische Monitoring von evon macht deutlich: Was als gesetzliche Verpflichtung beginnt, kann zur echten strategischen Ressource werden – für Betreiber, Investoren und Planer gleichermaßen. Auf Basis hochwertiger, kontinuierlich analysierter Betriebsdaten eröffnen sich neue Wege zur vorausschauenden Instandhaltung, zum ressourcenschonenden Betrieb und zur Erfüllung anspruchsvoller Nachhaltigkeitsziele.

Erfahren Sie mehr über die kommenden Funktionen und vielfältigen Einsatzmöglichkeiten des Technischen Monitorings von evon. ■

About evon GmbH

evon is an Austrian software company based in St. Ruprecht an der Raab. For over 15 years, evon has been developing manufacturer-independent, hardware-neutral, and user-friendly automation software for building automation, industry, and traffic management. As part of the SPIE group of companies, evon combines local innovation with global expertise and long-term stability. True to its motto: "We increase your success – because we live and breathe digitalisation."

Über die evon GmbH

evon ist ein österreichisches Softwareunternehmen mit Sitz in St. Ruprecht an der Raab. Seit über 15 Jahren entwickelt evon herstellerunabhängige, hardwareneutrale und benutzerfreundliche Automatisierungssoftware für die Bereiche Gebäudeautomation, Industrie und Verkehrsmanagement. Als Teil der Unternehmensgruppe SPIE kombiniert evon lokale Innovationskraft mit globaler Kompetenz und nachhaltiger Stabilität. Ganz nach dem Motto: „Wir steigern Ihren Erfolg – weil wir für Digitalisierung brennen."

Hartmut Henzler
Senior Sales Manager Germany | evon GmbH
hartmut.henzler.ext@evon-automation.com | www.evon-automation.com

KMG Clinics: Centralization and Modernization of Building Automation Based on BACnet/SC – A Project with Vision

KMG Kliniken: Zentralisierung und Modernisierung der Gebäudeautomation auf BACnet/SC Basis – Ein Projekt mit Weitblick

With the goal of establishing future-proof, centrally controlled building automation, KMG Clinics launched an extensive digitization and modernization project in 2020, which is expected to be completed by 2026.

Mit dem Ziel, eine zukunftssichere und zentral gesteuerte Gebäudeautomation zu etablieren, starteten die KMG Kliniken im Jahr 2020 ein umfangreiches Digitalisierungs- und Modernisierungsprojekt, das voraussichtlich bis 2026 abgeschlossen sein wird.

The hospital group operates six hospitals and several rehabilitation facilities in Germany, including locations in Güstrow, Sonderhausen, Plau am See, Luckenwalde, and Wittstock (Dosse), which have already been successfully modernized.

Focus on Security of Supply and Integration

A particular challenge was to modernize the existing systems while the clinics remained in operation – without compromising the essential functionality of critical infrastructure such as fire alarm systems or safety-related building management technology. Thanks to our BACnet-based building management software enteliWEB, we were able to seamlessly integrate a wide variety of existing systems.

Our manufacturer-independent solution enables central monitoring and control of all systems, regardless of their origin. With our comprehensive platform and integrative software functions, we were able to offer decisive advantages. The user-friendly interface and integrated energy management functions were particularly appreciated.

Support from Top Management

From the outset, the project was actively supported by the management of KMG Clinics – not least in order to achieve the ambitious company-wide climate targets. The consistent implementation of the central strategy, together with reliable project partners such as SI-Building Automation GmbH and EliteBuildingArchiTec Germany GmbH, enabled a rapid return on investment and led to significant savings in energy consumption and a measurable reduction in CO_2 emissions.

Holistic Approach for Maximum Efficiency

The project focused on a holistic system approach: Building automation was consistently networked with IT structures to achieve maximum efficiency and transparency. In the course of this, outdated systems – some of which were over 30 years old – were replaced, central functions were standardized, and new components were implemented to enable predictive maintenance. Our modular product family proved to be a key tool for sustainable modernization, as it offers maximum compatibility and scalability for both retrofit projects and new installations. This enables the clinics to respond flexibly to future requirements in the areas of energy efficiency and regulatory compliance.

Inventory as the Key to Success

One of the biggest challenges was the detailed recording and analysis of the existing systems. Due to missing or outdated documentation, it was essential to accurately record the actual conditions. Under the direction of the hospital management and in close coordination with the engineering firm EliteBuildingArchiTec Germany GmbH and the construction department, a comprehensive concept was developed and translated into a structured service specification – the basis for sustainable and trouble-free implementation.

Securely Networked with BACnet/SC

From the outset, particular attention was paid to IT security. The new communication structure is based on the BACnet/SC standard (BACnet Secure Connect), which enables secure data transfer between the locations and the central data center through TLS-based encrypted communication.

Our BACnet/SC-enabled controllers played a central role in this, ensuring both the highest security requirements and maximum performance. The system was supplemented by proven BACnet/SC routers from Krefeld-based MBS GmbH – with the result that Güstrow is now considered the largest BACnet/SC-based property in Germany.

Digital Access for Maximum Responsiveness

Thanks to the early integration of the IT department and technical facility management, daily operations were also taken to a new level. Technical support is now more efficient than ever: tablets with access to a secure WLAN technology network allow location-independent access to the building management system – and thus significantly faster response times in the event of a malfunction.

System openness as a success factor

With our system partner, SI Building Automation GmbH, KMG Clinics had an experienced partner at its side who can look back on a wide range of projects with a wide variety of manufacturers. As an independent system integrator, SI-Building

Aerial view of KMG Clinic Güstrow © KMG Clinics
Luftaufnahme KMG Klinik Güstrow © KMG Kliniken

Automation GmbH selects the optimal components for each project, ensuring maximum flexibility and high investment security.

Future-Oriented Perspective

Based on the project experience, the first training courses in BACnet/SC are already being held to prepare additional specialists for secure network communication in the building automation environment.

Quote from Frank Niemann, Managing Director of Service Companies Technology at KMG Clinics:

"Our energy efficiency reports show significant energy savings for the modernized automation areas. This in turn has led to reduced operating costs, which are important for all clinics today."

Der Klinikverbund betreibt sechs Krankenhäuser sowie mehrere Reha-Einrichtungen in den neuen Bundesländern – darunter Standorte in Güstrow, Sonderhausen, Plau am See, Luckenwalde und Wittstock (Dosse), die bereits erfolgreich modernisiert wurden.

Fokus auf Versorgungssicherheit und Integration

Eine besondere Herausforderung bestand darin, die bestehenden Systeme bei laufendem Klinikbetrieb zu modernisieren – ohne die essenzielle Funktionalität kritischer Infrastrukturen wie Brandmeldeanlagen oder sicherheitsrelevanter Gebäudeleittechnik zu beeinträchtigen. Dank unserer auf BACnet basierenden Gebäudemanagement-Software enteliWEB gelang die nahtlose Integration unterschiedlichster Bestandsanlagen.

Unsere herstellerübergreifende Lösung ermöglicht eine zentrale Überwachung und Steuerung aller Systeme – unabhängig von deren Herkunft. Mit unserer umfassenden Plattform und den integrativen Softwarefunktionen konnten wir entscheidende Vorteile bieten. Besonders geschätzt wurden dabei die benutzerfreundliche Oberfläche sowie die integrierten Funktionen für Energiemanagement.

Unterstützung durch das Top-Management

Von Beginn an wurde das Projekt durch die Geschäftsführung der KMG Kliniken aktiv gefördert – nicht zuletzt, um die ambitionierten unternehmensweiten Klimaziele zu erreichen. Die konsequente Umsetzung der zentralen Strategie, gemeinsam mit verlässlichen Projektpartnern wie der SI-Building Automation GmbH und der EliteBuildingArchiTec Germany GmbH, ermöglichte eine schnelle Amortisation der Investitionen und führte zu signifikanten Einsparungen beim Energieverbrauch sowie einer messbaren Reduktion des CO_2-Ausstoßes.

Ganzheitlicher Ansatz für maximale Effizienz

Im Zentrum des Projekts stand ein ganzheitlicher Systemansatz: Die Gebäudeautomation wurde konsequent mit IT-Strukturen vernetzt, um eine maximale Effizienz und Transparenz zu erreichen. Im Zuge dessen wurden veraltete Systeme – teils über 30 Jahre alt – abgelöst, zentrale Funktionen standardisiert und neue Komponenten implementiert, die prädiktive Wartung ermöglichen.

Unsere modulare Produktfamilie erwies sich dabei als zentrales Werkzeug für die nachhaltige Modernisierung, da sie sowohl für Retrofit-Projekte als auch für Neuanlagen höchste Kompatibilität und Skalierbarkeit bietet. Dadurch können

die Kliniken auch auf künftige Anforderungen im Bereich Energieeffizienz und regulatorische Vorgaben flexibel reagieren.

Bestandsaufnahme als Schlüssel zum Erfolg

Eine der größten Herausforderungen bestand in der detaillierten Erfassung und Analyse der Bestandsanlagen. Aufgrund fehlender oder veralteter Dokumentation war eine präzise Aufnahme der realen Gegebenheiten unerlässlich. Unter Leitung der Klinikführung und in enger Abstimmung mit dem beauftragten Ingenieurbüro, der EliteBuildingArchiTec Germany GmbH, sowie der Bauabteilung wurde ein umfassendes Konzept entwickelt und in ein strukturiertes Leistungsverzeichnis überführt – die Grundlage für eine nachhaltige und störungsfreie Umsetzung.

Sicher vernetzt mit BACnet/SC

Von Beginn an wurde besonderes Augenmerk auf IT-Sicherheit gelegt. So basiert die neue Kommunikationsstruktur auf dem BACnet/SC Standard (BACnet Secure Connect), der durch verschlüsselte Kommunikation auf TLS-Basis einen sicheren Datentransfer zwischen den Standorten und dem zentralen Rechenzentrum ermöglicht.

Eine zentrale Rolle übernahmen dabei unsere BACnet/SC fähigen Controller, die sowohl höchste Sicherheitsanforderungen als auch maximale Performance gewährleisten. Ergänzt wurde das System durch bewährte BACnet/SC Router der Krefelder MBS GmbH – mit dem Ergebnis, dass Güstrow heute als größte BACnet/SC basierte Liegenschaft Deutschlands gilt.

Digitaler Zugriff für maximale Reaktionsfähigkeit

Dank der frühzeitigen Integration der IT-Abteilung und des technischen Facility Managements konnte auch der tägliche Betrieb auf ein neues Niveau gehoben werden. Die technische Betreuung erfolgt heute effizienter denn je: Tablets mit Zugriff auf ein sicheres WLAN-Technik-

Control cabinet in Germany's largest BACnet/SC-based property © Tino Erler, SI-Building Automation
Schaltschrank in Deutschlands größter BACnet/SC basierten Liegenschaft © Tino Erler, SI-Building Automation

netz erlauben den ortsunabhängigen Zugang zur Gebäudeleittechnik – und damit deutlich schnellere Reaktionszeiten im Störungsfall.

Erfolgsfaktor Systemoffenheit

Mit unserem Systempartner, der SI Building Automation GmbH, stand den KMG Kliniken ein erfahrener Partner zur Seite, der auf eine große Bandbreite an Projekten mit unterschiedlichsten Fabrikaten zurückblicken kann. Als unabhängiger Systemintegrator setzt die SI-Building Automation GmbH projektbezogen die jeweils optimalen Komponenten und sichert damit maximale Flexibilität bei gleichzeitig hoher Investitionssicherheit.

Zukunftsorientierte Perspektive

Auf Basis der Projekterfahrungen werden heute bereits erste Schulungen im Bereich BACnet/SC durchgeführt, um weitere Fachkräfte auf die sichere Netzwerkkommunikation im Gebäudeautomationsumfeld vorzubereiten.

Zitat Frank Niemann, Geschäftsführer Servicegesellschaften Technik bei den KMG Kliniken:

„Unsere Energieeffizienzberichte weisen eine signifikante Energieeinsparung für die modernisierten Automatisierungsschwerpunkte auf. Diese führte wiederum zu reduzierten Betriebskosten, die in der heutigen Zeit wichtig für alle Kliniken sind."

Marco Weyer
Sales Manager | Delta Controls Germany GmbH
sales@deltacontrols.de | www.deltacontrols.de

Delta CONTROLS
Delta Controls Germany

Cybersecurity in Building Operations: A Methodical Approach for Future-Proof and Scalable IT/OT Security in Building Automation

Cybersicherheit im Gebäudebetrieb: Ein methodischer Ansatz für zukunftssichere und skalierbare IT/OT-Sicherheit in der Gebäudeautomation

Advances in digitalization enable data-based control and monitoring of buildings and have revolutionized building operations.
Die fortschreitende Digitalisierung ermöglicht eine datenbasierte Steuerung und Überwachung von Gebäuden und hat den Gebäudebetrieb revolutioniert.

In the relevant technical literature – especially in older editions – buildings were often still regarded as isolated structures. This paradigm has changed fundamentally. Today, there is no question that modern buildings are no longer isolated structures, but highly networked systems in which operational technology (OT) and information technology (IT) are seamlessly integrated.

However, this development, fueled by market trends and legal and regulatory requirements, not only brings efficiency gains, but also new challenges – especially in the area of cybersecurity. The threat of cyberattacks on building infrastructures is real and growing steadily.

Comprehensive Requirements

Until now, IT security has primarily been anchored as a central task of classic corporate IT. However, this security approach is now increasingly extending to operational technology (OT) as IT/OT security and thus also holistically to building digitization.

Cyber security must therefore be established as an integral part of building operations. It is crucial that the principle of "security by design" is taken into account right from the requirements analysis stage. Only then can all those involved – from planners and building owners to operators – act on a sound basis.

The key: a methodical and risk-oriented approach.

IT/OT Security in Building Operations

The basis for sustainable IT/OT security in building operations is a methodical and risk-oriented approach based on proven standards such as BSI basic protection. This approach makes it possible to systematically identify and evaluate cybersecurity risks and minimize them through appropriate measures.

Risk analysis is a central component of this process. It creates the necessary risk transparency to enable informed decisions to be made. This involves not only identifying vulnerabilities, but also assessing the potential impact of threats on building operations.

Cybersecurity as a Special Service Already Included in Planning in Accordance with HOAI

The importance of cybersecurity, especially risk management, is also reflected in the fee schedule for architects and engineers (HOAI), where it is listed as a special service. This emphasizes that IT/OT security cannot be considered a by-product, but rather an independent and essential task in the planning, construction, and operation process.

A methodical approach to IT/OT security integrates the relevant components of risk analysis into the service phases of the HOAI. This includes:

- Clarification of responsibilities and roles: Clear responsibilities for construction, operation, and IT/OT security must be defined early on in the planning phases.
- Identification of the objects to be examined: Which systems and components are critical for building operation?
- Determination of protection requirements: What availability, confidentiality, and integrity requirements exist for the identified systems?

- Identification of relevant threats: What potential attacks or disruptions could jeopardize operations?
- Determination of IT/OT security objectives: What security objectives must be achieved to meet the protection requirements?
- Derivation of tailored protective measures: What technical and organizational measures are necessary to achieve the security objectives?

A key aspect of risk management is its iterative and revolving nature. Cyber security is not a one-time event, but a continuous process. Even after a building has been handed over to the operator, the IT/OT security level must be regularly reviewed and adjusted. New threats, technological developments, and changing operational requirements require the continuous development of security measures.

Guide to Cyber Security in Building Automation

The guide "Cybersecurity in Building Automation" developed by WG-FM is based on the construction and service phases of the HOAI established in Germany. We believe that combining planning and construction with modern IT methods will create clear benefits for the entire life cycle of a building and allow the individual phases along the HOAI to be broken down accordingly.

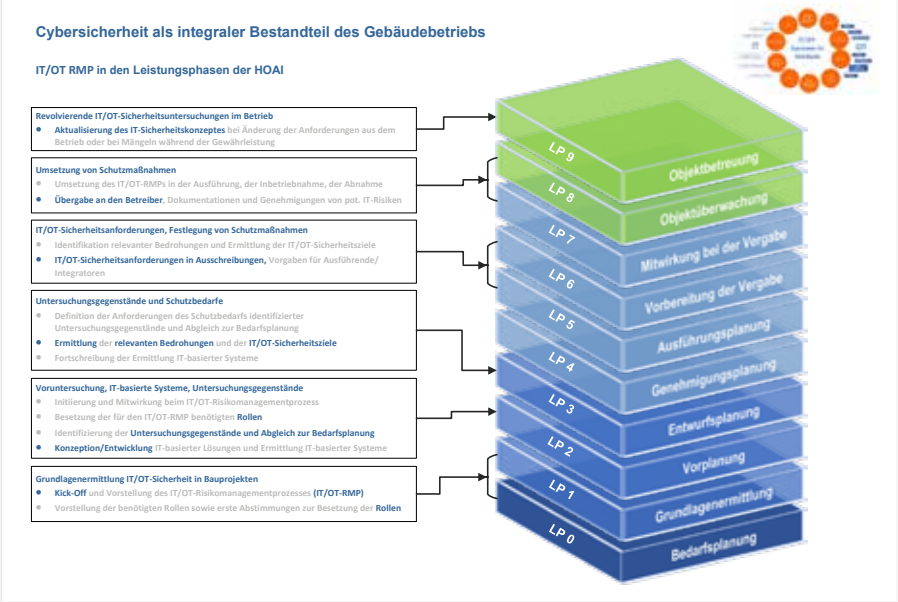
With the help of this guide and taking into account the requirements of the BSI basic protection, all parties involved can be guided and supported through the individual phases in a targeted manner.

Conclusion: Cybersecurity as an Integral Part of Building Operations

Cybersecurity in IT/OT and especially in building operations is not an option, but a necessity. The methodical and risk-oriented approach, which is based on standards such as the BSI basic protection, provides a solid and scalable foundation for systematically addressing security risks. Our guide addresses this need and clearly shows how cybersecurity requirements can be integrated into the HOAI service phases and along the life cycle phases of a property in accordance with GEFMA-100.

This not only clarifies responsibilities and roles, but also enables targeted planning and implementation of protective measures. It is crucial to understand the iterative nature of risk management in conjunction with HOIA and GEFMA: Cybersecurity is an ongoing process that must be continuously maintained even after a building has been commissioned.

The work cards, which have proven their worth since the initial publication of the "Cybersecurity in Building Automation" guide in 2024 (see also issue 41 of the BACnet Europe Journal, page 29), have been updated and are also systematically classified in the iterative process.



Gebäude wurden in der einschlägigen Fachliteratur – insbesondere in älteren Ausgaben – häufig noch als isolierte Strukturen betrachtet. Dieses Paradigma hat sich grundlegend gewandelt. Heute steht außer Frage, dass moderne Gebäude längst keine isolierten Strukturen mehr sind, sondern hochvernetzte Systeme, in denen Operational Technology (OT) und Information Technology (IT) nahtlos ineinandergreifen.

Diese Entwicklung, befeuert durch Markttrends und durch gesetzliche Vorgaben und regulatorische Anforderungen, bringt jedoch nicht nur Effizienzgewinne, sondern auch neue Herausforderungen mit sich – insbesondere im Bereich der Cybersicherheit. Die Bedrohung durch Cyberangriffe auf Gebäudeinfrastrukturen ist real und wächst stetig.

Umfassende Anforderungen

Bisher war IT-Sicherheit vor allem als zentrale Aufgabe der klassischen Unternehmens-IT verankert. Inzwischen erstreckt sich dieser Sicherheitsansatz jedoch zunehmend als IT/OT-Sicherheit auch auf die Betriebstechnologie (OT) und damit auch ganzheitlich auf die Gebäudedigitalisierung.

Cybersicherheit ist somit als integraler Bestandteil des Gebäudebetriebs zu etablieren. Dabei ist es entscheidend, dass die Maßgabe „Security by Design" bereits in der Bedarfsermittlung berücksichtigt wird. Nur so können alle Beteiligten – von Planern über Bauherren bis hin zu Betreibern – auf einer fundierten Grundlage agieren.

Der Schlüssel: Ein methodischer und risikoorientierter Ansatz.

IT/OT-Sicherheit im Gebäudebetrieb

Die Grundlage für eine nachhaltige IT/OT-Sicherheit im Gebäudebetrieb ist ein methodischer und risikoorientierter Ansatz, der sich an bewährten Standards wie bspw. dem BSI-Grundschutz orientiert. Dieser Ansatz ermöglicht es, Cybersicherheitsrisiken systematisch zu identifizieren, zu bewerten und durch geeignete Maßnahmen zu minimieren.

Ein zentraler Bestandteil dieses Prozesses ist die Risikoanalyse. Sie schafft die notwendige Risikotransparenz, um fundierte Entscheidungen treffen zu können. Dabei geht es nicht nur um die Identifikation von Schwachstellen, sondern auch um die Bewertung der potenziellen Auswirkungen von Bedrohungen auf den Gebäudebetrieb.

Cybersicherheit als besondere Leistung schon bei der Planung gemäß HOAI.

Die Bedeutung der Cybersicherheit, insbesondere des Risikomanagements spiegelt sich auch in der Honorarordnung für Architekten und Ingenieure (HOAI) wider, wo es als besondere Leistung ausgewiesen ist. Dies unterstreicht, dass IT/OT-Sicherheit nicht als Nebenprodukt betrachtet werden kann, sondern als eigenständige und essenzielle Aufgabe im Planungs-, Errichtungs- und Betriebsprozess.

Ein methodischer Ansatz zur IT/OT-Sicherheit integriert die relevanten Bestandteile der Risikoanalyse in die Leistungsphasen der HOAI. Dies umfasst:

- Klärung von Verantwortlichkeiten und Rollen: Bereits in den frühen Planungsphasen müssen klare Zuständigkeiten für Bau, Betrieb und IT/OT-Sicherheit definiert werden.
- Identifikation der Untersuchungsgegenstände: Welche Systeme und Komponenten sind kritisch für den Gebäudebetrieb?
- Festlegung von Schutzbedarfen: Welche Verfügbarkeits-, Vertraulichkeits- und Integritätsanforderungen bestehen für die identifizierten Systeme?
- Identifikation relevanter Bedrohungen: Welche potenziellen Angriffe oder Störungen könnten den Betrieb gefährden?
- Ermittlung der IT/OT-Sicherheitsziele: Welche Sicherheitsziele müssen erreicht werden, um die Schutzbedarfe zu erfüllen?

- Ableitung passgenauer Schutzmaßnahmen: Welche technischen und organisatorischen Maßnahmen sind erforderlich, um die Sicherheitsziele zu erreichen?

Ein entscheidender Aspekt des Risikomanagements ist sein iterativer und revolvierender Charakter. Cybersicherheit ist kein einmaliger Akt, sondern ein kontinuierlicher Prozess. Auch nach der Übergabe eines Gebäudes an den Betreiber muss das IT/OT-Sicherheitsniveau regelmäßig überprüft und angepasst werden. Neue Bedrohungen, technologische Entwicklungen und veränderte Betriebsanforderungen erfordern eine ständige Weiterentwicklung der Sicherheitsmaßnahmen.

Leitfaden Cybersicherheit in der Gebäudeautomation

Der von der WG-FM entwickelte Leitfaden „Cybersicherheit in der Gebäudeautomation“ lehnt sich an die Bau- bzw. Leistungsphasen der in Deutschland etablierten HOAI an Wir versprechen uns durch die Hochzeit von Planung und Bau mit modernen IT-Methoden einen klaren Gewinn für den gesamten Lebenszyklus eines Gebäudes zu schaffen, und die einzelnen Phasen entlang der HOAI entsprechend aufzufächern.

Mithilfe dieses Leitfadens und unter Berücksichtigung der Anforderungen des BSI-Grundschutzes können alle Beteiligten gezielt durch die einzelnen Phasen geführt und unterstützt werden.

Fazit: Cybersicherheit als integraler Bestandteil des Gebäudebetriebs

Cybersicherheit in der IT/OT und speziell im Gebäudebetrieb ist keine Option, sondern eine Notwendigkeit. Der methodische und risikoorientierte Ansatz, der sich an Standards wie bspw. dem BSI-Grundschutz orientiert, bietet eine solide und skalierbare Grundlage, um Sicherheitsrisiken systematisch zu adressieren. Unser Leitfaden adressiert diese Notwendigkeit und zeigt anschaulich die Integration von Cybersicherheitsanforderungen in die Leistungsphasen der HOAI und entlang der Lebenszyklusphasen einer Immobilie nach GEFMA-100.

Dies schafft nicht nur Klarheit über Verantwortlichkeiten und Rollen, sondern ermöglicht auch eine zielgerichtete Planung und Umsetzung von Schutzmaßnahmen. Dabei ist es entscheidend, den iterativen Charakter des Risikomanagements gleichsam mit der HOIA und der GEFMA zu verstehen: Cybersicherheit ist ein fortlaufender Prozess, der auch nach der Inbetriebnahme eines Gebäudes kontinuierlich gepflegt werden muss.

Die seit Erstveröffentlichung des Leitfadens „Cybersicherheit in der Gebäudeautomation“ 2024 (S. auch Ausgabe 41 des BACnet Europe Journals, Seite 29) bewährten Arbeitskarten wurden fortgeschrieben und sind ebenso systematisch im iterativen Prozess eingeordnet. ■

Marco Favaro
IT-Sicherheitsmanager / IT-Risikomanagement in Bauprojekten, Deutschen Bundesbank

Jochem Gombert
Bauliche Standards Betriebstechnik im Baumanagement, Deutschen Bundesbank

EU Building Security Requirements: NIS-2, CER, CRA, and RED

EU-Vorgaben zur Gebäudesicherheit: NIS-2, CER, CRA und RED

Cybersecurity, physical resilience, and product security are no longer optional extras, but legal requirements. Cybersicherheit, physische Resilienz und Produktsicherheit sind keine Kür mehr, sondern gesetzliche Pflicht.

With the ongoing digitalization of technical infrastructures, automated building systems are increasingly becoming the focus of legislation. The European Union has created a comprehensive set of regulations that fundamentally changes the security architecture in building automation. This article highlights the four key regulations – NIS-2, CER, CRA, and RED – and shows what they mean in concrete terms for operators, integrators, and manufacturers.

NIS-2: Legal Obligation for Cyber Resilience

The revised Network and Information Security Directive (NIS-2) has been in force at European level since January 2023. It aims to strengthen the digital resilience of critical and important facilities, including numerous players in building automation.

Key requirements for operators:

- Conduct systematic risk analyses
- Establishment of standardized processes for dealing with security incidents
- Securing the supply chain through contractual and organizational measures
- Introduction of a reporting procedure for cyber incidents
- Designation of a permanent point of contact at the national supervisory authority, e.g., in Germany, the Federal Office for Information Security (BSI)

Operators of large properties, data centers, or utilities in particular should assess how they are affected at an early stage. The directive requires technical and organizational measures, including documented internal processes.

The NIS 2 Directive had to be transposed into national law in all member states of the European Union by October 17, 2024, at the latest. While some countries have already completed the implementation process or are in the final stages, national legislation is still being drafted in other countries, including Germany.

In Germany, implementation is currently being carried out through the "Act on the Implementation of the NIS 2 Directive and on the Regulation of Essential Features of Information Security Management in the Federal Administration" (NIS2UmsuCG). This involves both adapting existing laws, such as the BSI Act, and introducing new obligations for operators of critical and important facilities.

Until the respective national implementation is complete, the provisions of the original NIS 1 Directive will continue to apply in many countries. This will remain legally binding until it is formally replaced by national NIS 2 law . Companies and operators should therefore familiarize themselves with the extended requirements of NIS 2 at an early stage. Regardless of the current state of implementation, significantly more comprehensive documentation, reporting, and security requirements are expected to become mandatory in the future. →1

CER: Physical Resilience for Critical Infrastructures

The Critical Entities Resilience Directive (CER), valid since January 2023, adds a physical dimension to NIS-2. It addresses risks from sabotage, natural disasters, or technical failures.

Sectors affected:

- Energy supply (electricity, gas, and oil)
- Transport and traffic (rail, air, road, and sea)
- Digital infrastructure
- Water management (drinking water supply and wastewater disposal)
- Public administration
- Health
- Food supply
- Space
- Banking
- Financial market infrastructure

Obligations for operators:

- Conducting physical risk analyses
- Technical protective measures such as access controls and fire protection
- Concepts to ensure operations even in the event of a crisis
- Compliance with reporting obligations

Regulatory framework	Adoption at EU level	Transposition into national law	Who is affected?	Implementation deadlines
NIS-2 (Directive (EU) 2022/2555)	December 2022	Required (implementation in Germany via NIS2UmsuCG in progress)	Operators of critical and important facilities, including large building operators	By October 17, 2024
CER (Directive (EU) 2022/2557)	December 2022	Required (national implementation in progress)	Operators of critical physical infrastructure (including in the energy, transport, and public administration sectors)	By October 17, 2024
CRA (Cyber Resilience Act)	March 2024	Not required (regulation – applies directly in all member states)	Manufacturers and suppliers of products with digital elements, including GA components	Mandatory requirements apply from Q4 2027 (36-month transition period)
RED (amendment to the Radio Equipment Directive by delegated act)	Amendments adopted on January 7, 2022	Not required (automatically valid)	Manufacturers of radio equipment, including IoT and GA components	New requirements apply from August 1, 2025

For smart buildings, this means that fire protection, access security, redundancies, and monitoring are now required by law – no longer just best practice.

The CER Directive will also be specified in a separate legislative procedure. It is becoming apparent that operators with physically vulnerable infrastructure – such as data centers, utility facilities, or security-critical buildings – will have to implement new organizational and technical measures.

- By January 17, 2026, national strategies for the resilience of critical facilities must be in place and comprehensive risk analyses must be carried out.
- Critical facilities must be identified by July 17, 2026, after which strict requirements will apply to affected organizations for implementation within a maximum of 10 months.

Some EU member states have already completed national implementation or are at an advanced stage.

CRA: Security Obligations for Manufacturers of Digital Products

The Cyber Resilience Act (CRA) was adopted in December 2024 and will become binding in December 2027. The regulation defines basic security requirements for products with digital components. Manufacturers must demonstrate that IT security has been taken into account not only during development but throughout the entire life cycle of their products.

Key requirements are:

- Secure development and production ("security by design")
- Standardized vulnerability handling
- Transparent and binding reporting processes for security vulnerabilities
- Regular updates and clear communication about security risks

For components in building automation such as BACnet gateways, control devices, or KNX routers, this means Security "by design" and "by default" becomes mandatory – including transparent vulnerability communication and mandatory reporting channels in the event of security breaches . →2

The BSI has published Technical Guideline TR-03183 for the implementation of the CRA. This is divided into three parts:

1. General Requirements – Overview of security-related product requirements
2. Software Bill of Materials (SBOM) – Transparency regarding the software components used
3. Vulnerability Reports and Notifications – Rules for handling incoming vulnerability reports

→3

RED: Cybersecurity of Wireless Components

The revised Radio Equipment Directive (RED) came into force Together with the CRA, it creates a dual obligation.

- Devices must be radio and electromagnetically safe
- IT protection mechanisms (e.g., encryption, access control) are also mandatory

This affects WLAN-enabled controllers, LoRa gateways, and GSM modules, among other things. →4

National Additions: TRBS 1115-1 & IT-Grundschutz++

In addition to the EU requirements, national regulations such as TRBS 1115-1 and the new IT-Grundschutz++ specify the security requirements in Germany.

TRBS 1115-1

The Technical Rule for Industrial Safety TRBS 1115-1 specifies the requirements of the Industrial Safety Regulation (BetrSichV) with regard to work equipment consisting of a combination of hardware and software – so-called "digital work equipment." Building automation systems also fall into this category if they perform safety-related functions or can be maintained via the internet. TRBS 1115-1 emphasizes the operator's responsibility for assessing the risks of such systems, taking cyber risks into account. This includes, for example, evaluating update mechanisms, remote access paths, and security functions. The rule makes it clear that cybersecurity is no longer an isolated IT issue, but an integral part of occupational safety – with direct implications for maintenance, servicing, and protective measures on site. →5

Modernization of "IT-Grundschutz"

The "IT-Grundschutz" of the BSI is currently undergoing a fundamental revision. The new "Grundschutz++" is to be introduced in stages from January 1, 2026. A key innovation is the provision of a machine-readable set of rules that covers all requirements in a structured JSON file. This facilitates automated integration into ISMS tools and supports companies in their ongoing security assessments.

The new structure follows an object-based approach, reduces redundancies, and increases transparency. To further facilitate applicability, the security levels "basic", "standard", and "increased protection requirement" are being replaced by flexible performance figures in conjunction with dynamic thresholds. For small and medium-sized organizations, the BSI will provide practical entry-level assistance via the "Path to Basic Security" (WiBA) concept.

IT-Grundschutz modules INF.13 and INF.14

Two new modules have been introduced in the IT-Grundschutz Compendium 2022 that are aimed directly at operators of building automation systems.

- INF.13 Technical Building Management (TBM) covers the planning and operation of building services such as heating, ventilation, air conditioning, and energy supply, including security requirements and risk analyses. It addresses risks arising from unsecured remote maintenance access, missing rights concepts, or outdated protocols. →6

- INF.14 Building Automation (BACS) focuses on automation and control systems in buildings, in particular interfaces to IT networks as well as data security, availability, and integrity, and concentrates on the technical infrastructure of buildings, especially power supply, air conditioning, access security, and fire protection. →7

Both modules provide practical requirements for network segmentation, protocol hardening, and physical asset protection. For operators, this means that both the digital and physical architecture of buildings must be actively protected and regularly checked. Manufacturers benefit if they develop and document their products directly with these modules in mind.

Event / Deadline	Date	Description
Publication in the EU Official Journal	November 20, 2024	Publication of the legal text in the European Official Journal
Entry into force of the regulation	December 11, 2024	CRA is formally in force and directly applicable in all Member States.
Start of the transition period	December 11, 2024	Manufacturers, importers, and distributors have time to implement the regulation.
Obligation to report active vulnerabilities and security incidents	September 11, 2026	Manufacturers must report security vulnerabilities and incidents to ENISA within 24 hours.
Mandatory application requirements	December 11, 2027	All requirements apply in full: security requirements, CE marking, market surveillance, conformity assessment.

Vulnerability Management for Hardware and Software Components

Components in building automation today often consist of complex combinations of software and hardware, such as embedded Linux, web interfaces, network protocols, and physical interfaces. Vulnerabilities in such systems can manifest themselves at many levels.

Receiving reports on vulnerabilities

To make it easier for security researchers and others to find the right contact person in organizations, organizations should provide a security.txt file on their website in accordance with RFC 9116. The security.txt is a file that provides relevant contact information in a human- and machine-readable form. It is located at a defined location on the organization's website, which simplifies contact and allows it to be found using automatic tools (e.g., web crawlers). Those who find the file must be able to trust that the information will reach the right person at the organization and via the appropriate channels. Since this may be sensitive information, it makes sense not only to standardize the transfer of information, but also to confirm the authenticity of the contact details provided, ideally using cryptographic means in . →8

Provision of vulnerability information

Effective vulnerability management is therefore essential for manufacturers, integrators, and operators. The Common Security Advisory Framework (CSAF) provides a structured, machine-readable way to publish vulnerability information and share it automatically. Manufacturers can clearly identify which products are affected, which firmware versions are vulnerable, and what countermeasures are available. CSAF significantly reduces the manual effort involved in searching for security information and determining whether or not a product is affected. It allows manufacturers, users, operators, and administrators to automatically retrieve information about individual vulnerabilities and determine whether they are affected. Non-affected items can also be communicated in a scalable manner (Vulnerability Exploitability eXchange (VEX) as a profile in CSAF).

In an increasingly networked and complex world, the number of security-related vulnerabilities will grow significantly, and modern vulnerability management using CSAF documents will become indispensable. The BSI provides support with platforms and tools related to CSAF, including validation tools and templates for structured advisories, and provides reports on vulnerabilities and security gaps via the CERT-Bund warning and information service. In addition, there is a CSAF lister listing public bodies that publish CSAF documents.

Vulnerability management and Security.txt

Effective vulnerability management is essential.

Organizations should:

- Provide a security.txt file in accordance with RFC 9116 to facilitate contact for security notifications
- Use the Common Security Advisory Framework (CSAF) to publish structured, machine-readable advisories

The CSAF format allows both affected and unaffected parties to communicate (via VEX profiles).

The BSI provides tools, templates, and a central platform for distribution. →9

Cyber Security in Building Automation

Asset management in building automation with Malcolm

In networked buildings, asset management forms the basis for secure and stable operation. Only those who know which devices are connected where and how can respond specifically to security incidents, vulnerability reports, or failures. However, many operators still work with fragmented lists or incomplete documentation. This is where the open-source project Malcolm comes in. Developed by the Idaho National Laboratory (INL), it enables the passive recording and analysis of communication behavior in industrial and building technology networks. Malcolm automatically detects assets in the network, classifies them, and visualizes their communication relationships. Tools such as Zeek, Suricata, and Kibana are used for this purpose. This not only gives operators a complete overview of their technical infrastructure, but also provides an early warning system for unusual activities. Malcolm provides a valuable foundation for compliance, incident management, and auditability, especially in heterogeneous networks with BACnet/IP, KNX, MQTT, and proprietary protocols. →10

Network security in building automation

Network security is the backbone of building security. With the increasing networking and external connection of automation components, the risks are growing – for example, through unprotected VPN gateways, directly accessible controllers, or uncontrolled remote access. Exposed systems must be consistently isolated. They should never be directly accessible from the internet, but secured via secure VPN connections, two-factor authentication, and firewalls. Protocols such as BACnet/IP or Modbus/TCP may also only be used via clearly defined communication paths. The transition between IT and OT networks is particularly critical. This interface must be protected by dedicated zones or demilitarized zones (DMZ). Only clearly authorized data flows should take place here – ideally monitored by DPI (Deep Packet Inspection) and logging systems such as Malcolm.

The international standard IEC 62443 defines a zoning model for this purpose that is ideal for use in building automation. Networks are divided into security zones, for example for management systems, automation networks, field devices, and external service providers. The connections between these zones – known as conduits – are controlled and secured in a graded manner. Each zone is assigned a defined security level depending on its risk. This prevents, for example, an infected IT client from gaining uncontrolled access to the building management system. The defense-in-depth model is therefore also the optimal method for securing networks in building automation.

From standard to implementation: VDMA and BIG-EU provide guidance

The topics of cybersecurity and resilience are also becoming increasingly important in building automation. Two current documents provide important guidance on this subject: VDMA Standard 24774 and the "Security in Building Automation" guideline from the BACnet Interest Group Europe (BIG-EU) Working Group WG-FM.

VDMA Standard Sheet 24774 is aimed at all parties involved in the life cycle of technical building equipment – from planners and installers to manufacturers and operators. The aim of the document is to transfer the information security requirements from standards such as IEC 62443 to the context of building automation in a practical manner. The standard introduces basic role and concept models, assigns specific responsibilities, and describes measures for risk analysis and risk minimization. Typical risk situations such as unauthorized access, manipulation, or system failure are outlined, and security measures are presented, including network segmentation, access control, remote access protection, and vulnerability and patch management. A central

element is the introduction of a zoning model (zones and conduits) for structured security architecture analogous to IEC 62443. The standard also emphasizes that cybersecurity is not a one-time event, but a continuous process in operations – including regular testing, documentation, and training. It thus provides a valuable bridge between international standards and practical implementation – especially for operators and system integrators. →11

In addition to this, the WG-FM guideline "Security in Building Automation" was published by BIG-EU. This makes it clear that security begins in the planning phase. The guideline recommends developing a comprehensive security concept at an early stage that involves all parties involved – from planning and commissioning to ongoing operation. Technical recommendations include network segmentation, avoiding direct Internet exposure of automation systems, secure remote maintenance solutions, and structured vulnerability management.

Operator obligations are also a focus: they should create the organizational conditions necessary to respond to security-related events. The guide is closely based on established standards such as IEC 62443 and ISO 27001, but remains deliberately application-oriented – especially for small and medium-sized enterprises. With supplementary checklists and practical tips, the guide offers pragmatic assistance for the secure implementation of GA projects in the area of conflict between technical complexity and regulatory responsibility.

Both documents – VDMA Standard Sheet 24774 and the WG-FM guide – make an important contribution to making cybersecurity in building automation tangible, plannable, and sustainable. →12

Conclusion

The legal framework for cybersecurity is changing, with new obligations for operators and manufacturers arising from European regulations such as NIS-2, CER, CRA, and RED. But regardless of deadlines and regulations, one thing is certain: anyone who wants to operate their buildings and systems securely in the long term should act proactively now. Cybersecurity requirements cannot be reduced to individual measures, but require a well-thought-out combination of technical solutions, organizational processes, and clear responsibilities. This is the only way for building automation operators and manufacturers to effectively control the increasing risks while responsibly exploiting the opportunities offered by digitalization. ■

Mit der fortschreitenden Digitalisierung technischer Infrastrukturen geraten automatisierte Gebäudeanlagen zunehmend in den Fokus der Gesetzgebung. Die Europäische Union hat ein umfassendes Regelwerk geschaffen, das die Sicherheitsarchitektur in der Gebäudeautomation grundlegend verändert. Dieser Beitrag beleuchtet die vier zentralen Regulierungen – NIS-2, CER, CRA und RED – und zeigt auf, was sie für Betreiber, Integratoren und Hersteller konkret bedeuten.

NIS-2: Gesetzliche Pflicht zur Cyberresilienz

Seit Januar 2023 ist die überarbeitete Richtlinie über Netz- und Informationssicherheit (NIS-2) auf europäischer Ebene in Kraft. Sie zielt darauf ab, die digitale Widerstandsfähigkeit kritischer und wichtiger Einrichtungen zu stärken – darunter auch zahlreiche Akteure der Gebäudeautomation.

Zentrale Anforderungen für Betreiber:

- Durchführung systematischer Risikoanalysen
- Etablierung standardisierter Prozesse für den Umgang mit Sicherheitsvorfällen
- Absicherung der Lieferkette durch vertragliche und organisatorische Maßnahmen
- Einführung eines Meldeverfahrens bei Cybervorfällen
- Benennung einer festen Kontaktstelle bei der nationalen Aufsichtsbehörde, z.B. in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Insbesondere Betreiber großer Liegenschaften, Rechenzentren oder Versorgungseinrichtungen sollten sich frühzeitig mit der eigenen Betroffenheit auseinandersetzen. Die Richtlinie verlangt technische und organisatorische Maßnahmen – einschließlich dokumentierter interner Prozesse.

Die NIS-2-Richtlinie musste in allen Mitgliedstaaten der Europäischen Union bis spätestens zum 17. Oktober 2024 in nationales Recht überführt werden. Während einige Länder den Umsetzungsprozess bereits abgeschlossen haben oder sich in der finalen Phase befinden, ist in anderen Staaten – darunter auch Deutschland – die nationale Gesetzgebung noch in Bearbeitung.

In Deutschland erfolgt die Umsetzung derzeit durch das sogenannte „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" (NIS2UmsuCG). Dabei werden sowohl bestehende Gesetze – etwa das BSI-Gesetz – angepasst als auch neue Verpflichtungen für Betreiber kritischer und wichtiger Einrichtungen eingeführt.

Solange die jeweilige nationale Umsetzung noch nicht abgeschlossen ist, gelten in vielen Ländern weiterhin die Bestimmungen der ursprünglichen NIS-1-Richtlinie. Diese bleibt bis zur formellen Ablösung durch nationales NIS-2-Recht rechtsverbindlich. Unternehmen und Betreiber sollten sich daher frühzeitig mit den erweiterten Anforderungen der NIS-2 vertraut machen. Denn unabhängig vom aktuellen Umsetzungsstand ist mit deutlich umfassenderen Dokumentations-, Melde- und Sicherheitsanforderungen zu rechnen, die in Zukunft verbindlich werden. →1

CER: Physische Resilienz für kritische Infrastrukturen

Die Critical Entities Resilience Directive (CER), gültig seit Januar 2023, ergänzt die NIS-2 um die physische Dimension. Sie adressiert Risiken durch Sabotage, Naturkatastrophen oder technische Ausfälle.

Betroffene Sektoren:

- Energieversorgung (Strom, Gas und Öl)
- Transport und Verkehr (Schiene, Luft, Straße und See)
- Digitale Infrastruktur
- Wasserwirtschaft (Trinkwasserversorgung und Abwasserentsorgung)
- Öffentliche Verwaltung
- Gesundheitswesen
- Lebensmittelversorgung
- Weltraum
- Bankwesen
- Finanzmarkt-Infrastruktur

Pflichten für Betreiber:

- Durchführung physischer Risikoanalysen
- Technische Schutzmaßnahmen wie Zutrittskontrollen und Brandschutz
- Konzepte zur Sicherstellung des Betriebs auch im Krisenfall
- Meldepflichten einhalten

Für smarte Gebäude bedeutet das: Brandschutz, Zugangssicherheit, Redundanzen und Monitoring sind regulatorisch vorgeschrieben – nicht mehr nur Best Practice.

Auch die CER-Richtlinie wird im Rahmen eines eigenen Gesetzgebungsverfahrens konkretisiert werden. Hier zeichnet sich ab, dass insbesondere Betreiber mit physisch schutzbedürftiger Infrastruktur – etwa Rechenzentren, Versorgungseinrichtungen oder sicherheitskritische Gebäude – neue organisatorische und technische Maßnahmen umsetzen müssen.

- Bis 17. Januar 2026 müssen nationale Strategien zur Resilienz kritischer Einrichtungen sowie umfassende Risikoanalysen durchgeführt werden.
- Bis 17. Juli 2026 sind kritische Einrichtungen zu identifizieren – danach gelten für betroffene Organisationen strenge Vorgaben zur Umsetzung innerhalb von höchstens 10 Monaten.

Einige EU-Mitgliedstaaten haben die nationale Umsetzung bereits abgeschlossen oder befinden sich in fortgeschrittenen Phasen.

CRA: Sicherheitspflicht für Hersteller digitaler Produkte

Der Cyber Resilience Act (CRA) wurde im Dezember 2024 verabschiedet und wird ab Dezember 2027 verbindlich. Die Verordnung definiert grundlegende Sicherheitsanforderungen für Produkte mit digitalen Komponenten. Hersteller müssen nicht nur während der Entwicklung, son-

dern über den gesamten Lebenszyklus ihrer Produkte hinweg nachweisen, dass IT-Sicherheit berücksichtigt wurde.

Zentrale Anforderungen sind:

- sichere Entwicklung und Produktion („Security by Design"),
- standardisierte Schwachstellenbehandlung,
- transparente und verbindliche Meldeprozesse bei Sicherheitslücken,
- regelmäßige Updates und klare Kommunikation über Sicherheitsrisiken.

Für Komponenten in der Gebäudeautomation wie BACnet-Gateways, Steuergeräte oder KNX-Router bedeutet dies Sicherheit „by design", und „by default" wird zum Pflichtprogramm – samt transparenter Schwachstellenkommunikation und verpflichtender Meldewege im Fall von Sicherheitslücken. →2

Das BSI hat zur Umsetzung des CRA die Technische Richtlinie TR-03183 veröffentlicht. Diese gliedert sich in drei Teile:

- 1.General Requirements – Übersicht zu sicherheitsrelevanten Produktanforderungen
- 2.Software Bill of Materials (SBOM) – Transparenz über verwendete Softwarekomponenten
- 3.Vulnerability Reports and Notifications – Regeln zum Umgang mit eingehenden Schwachstellenmeldungen

→3

RED: Cybersicherheit drahtloser Komponenten

Ab dem 1. August 2025 ist die überarbeitete Radio Equipment Directive (RED) in Kraft. Gemeinsam mit dem CRA schafft sie eine doppelte Verpflichtung:

- Geräte müssen funktechnisch und elektromagnetisch sicher sein.
- Zusätzlich sind IT-Schutzmechanismen (z. B. Verschlüsselung, Zugriffskontrolle) verpflichtend.

Betroffen sind u. a. WLAN-fähige Steuerungen, LoRa-Gateways und GSM-Module. →4

Nationale Ergänzungen: TRBS 1115-1 & IT-Grundschutz++

Neben den EU-Vorgaben konkretisieren in Deutschland nationale Regelungen wie TRBS 1115-1 und der neue IT-Grundschutz++ die Sicherheitsanforderungen.

TRBS 1115-1

Die Technische Regel für Betriebssicherheit TRBS 1115-1 konkretisiert die Anforderungen der Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf Arbeitsmittel, die aus einer Kombination von Hard- und Software bestehen – sogenannte „digitale Arbeitsmittel". Auch Gebäudeautomationssysteme fallen unter diese Kategorie, wenn sie sicherheitsrelevante Funktionen erfüllen oder über das Internet wartbar sind. Die TRBS 1115-1 betont die Verantwortung des Betreibers für die Gefährdungsbeurteilung solcher Systeme unter Berücksichtigung von Cyberrisiken. Dies beinhaltet beispielsweise die Bewertung von Update-Mechanismen, Fernzugriffswegen oder Sicherheitsfunktionen. Die Regel verdeutlicht: Cybersicherheit ist kein isoliertes IT-Thema mehr, sondern integraler Bestandteil der Arbeitssicherheit – mit direkten Auswirkungen auf Wartung, Instandhaltung und Schutzmaßnahmen vor Ort. →5

Modernisierung des IT-Grundschutzes

Der IT-Grundschutz des BSI wird derzeit grundlegend überarbeitet. Ab dem 1. Januar 2026 soll der neue „Grundschutz++" stufenweise eingeführt werden. Wesentliche Neuerung ist die Bereitstellung eines maschinenlesbaren Regelwerks, das als JSON-Datei strukturiert alle Anforderungen umfasst. Dies erleichtert die automatisierte Integration in ISMS-Tools und unterstützt Unternehmen bei der kontinuierlichen Sicherheitsbewertung.

Die neue Struktur verfolgt einen objektbasierten Ansatz, reduziert Redundanzen und erhöht die Transparenz. Um die Anwendbarkeit weiter zu erleichtern, werden die Absicherungsstufen Basis, Standard und erhöhter Schutzbedarf durch flexible Leistungszahlen in Verbindung mit dynamischen Schwellwerten ersetzt. Für kleine und mittlere Organisationen wird das BSI praxisnahe Einstiegshilfen über das Konzept „Weg in die Basis-Absicherung" (WiBA) bereitstellen.

IT-Grundschutzbausteine INF.13 und INF.14

Im IT-Grundschutz-Kompendium 2022 wurden zwei neue Bausteine eingeführt, die sich direkt an Betreiber von Gebäudeautomationssystemen richten.

- INF.13 Technisches Gebäudemanagement (TBM) deckt Planung und Betrieb gebäudetechnischer Anlagen ab – etwa Heizung, Lüftung, Klima, Energieversorgung – mit Sicherheitsanforderungen und Gefährdungsanalysen. Dabei werden Risiken adressiert, die etwa durch ungesicherte Fernwartungszugänge, fehlende Rechtekonzepte oder veraltete Protokolle entstehen. →6

- INF.14 Gebäudeautomation (BACS) konzentriert sich auf Automations- und Regelungssysteme im Gebäude, insbesondere Schnittstellen zu IT-Netzen sowie Datensicherheit, Verfügbarkeit und Integrität und fokussiert auf die technische Infrastruktur von Gebäuden, insbesondere Stromversorgung, Klimatisierung, Zugangssicherheit oder Brandschutz. →7

Beide Bausteine liefern praxisnahe Anforderungen zur Segmentierung von Netzwerken, zur Protokollhärtung und zum Schutz der physischen Anlagen. Für Betreiber bedeutet dies: Sowohl die digitale als auch die physische Architektur von Gebäuden muss aktiv geschützt und regelmäßig überprüft werden. Hersteller profitieren, wenn sie ihre Produkte direkt mit Blick auf diese Bausteine entwickeln und dokumentieren.

Schwachstellenmanagement bei Hard- und Softwarekomponenten

Komponenten in der Gebäudeautomation bestehen heute oft aus komplexen Kombinationen aus Software und Hardware – etwa Embedded Linux, Webschnittstellen, Netzwerkprotokollen und physischen Schnittstellen. Schwachstellen in solchen Systemen können sich auf vielen Ebenen manifestieren.

Regelwerk	Verabschiedung auf EU-Ebenel	Umsetzung in nationales Recht	Wer ist betroffen?	Umsetzungsfristen
NIS-2 (Richtlinie (EU) 2022/2555	Dezember 2022	Erforderlich (Umsetzung in DE über NIS2UmsuCG in Arbeit)	Betreiber kritischer und wichtiger Einrichtungen, darunter auch größere Betreiber von Gebäuden	Spätestens 17. Oktober 2024
CER (Richtlinie (EU) 2022/2557)	Dezember 2022	Erforderlich (nationale Umsetzung in Arbeit)	Betreiber kritischer physischer Infrastrukturen (u. a. im Bereich Energie, Transport, öffentliche Verwaltung)	Spätestens 17. Oktober 2024
CRA (Cyber Resilience Act)	März 2024	Nicht erforderlich (Verordnung – gilt direkt in allen Mitgliedstaaten)	Hersteller und Anbieter von Produkten mit digitalen Elementen, inkl. GA-Komponenten	Verpflichtende Anforderungen gelten ab Q4 2027 (36 Monate Übergangsfrist)
RED (Änderung der Funkanlagenrichtlinie durch delegierten Rechtsakt)	Änderungen beschlossen am 7. Januar 2022	Nicht erforderlich (automatisch gültig)	Hersteller funktechnischer Geräte, inkl. IoT- und GA-Komponenten	Neue Anforderungen gelten ab 1. August 2025

Meldungen zu Schwachstellen empfangen

Um Sicherheitsforschenden und anderen das Auffinden des passenden Kontakts in Organisationen zu erleichtern, sollten die Organisationen eine security.txt gemäß RFC 9116 auf ihrer Webseite bereitstellen. Die security.txt ist eine Datei, die relevante Kontaktinformationen in menschen- und maschinenlesbarer Form bereitstellt. Sie befindet sich an einem definierten Ort auf der Internetseite der Organisation, wodurch die Kontaktaufnahme vereinfacht wird und sie mittels automatischer Werkzeuge (z. B. per Web-Crawler) gefunden werden kann. Die Findenden sind darauf angewiesen, dass die Informationen bei der Organisation an der richtigen Stelle und über geeignete Kanäle ankommen. Da es sich um sensible Informationen handeln kann, ist es sinnvoll, dass nicht nur die Informationsweitergabe standardisiert erfolgt, sondern auch die Echtheit des angegebenen Kontakts, im Optimalfall kryptografisch gesichert, bestätigt wird. →8

Bereitstellung von Schwachstelleninformationen

Ein effektives Schwachstellenmanagement ist deshalb für Hersteller, Integratoren wie Betreiber essenziell. Das Common Security Advisory Framework (CSAF) bietet eine strukturierte, maschinenlesbare Möglichkeit, Schwachstelleninformationen zu veröffentlichen und automatisiert weiterzugeben. Hersteller können so klar benennen, welche Produkte betroffen sind, welche Firmware-Versionen angreifbar sind und wie Gegenmaßnahmen aussehen. CSAF reduziert den manuellen Aufwand bei der Suche nach Sicherheitsinformationen und bei der Feststellung von Betroffenheit oder eben Nicht-Betroffenheit erheblich. Es erlaubt Herstellern, Anwendern, Betreibern und der Verwaltung die Informationen zu einzelnen Schwachstellen automatisiert abzurufen und eine Betroffenheit festzustellen. Auch Nicht-Betroffenheiten können so skalierbar kommuniziert werden (Vulnerability Exploitability eXchange (VEX) als Profil in CSAF).

Im Zuge einer immer stärker vernetzten und komplexeren Welt wird die Anzahl an sicherheitsrelevanten Schwachstellen signifikant wachsen und zeitgemäßes Schwachstellenmanagement mittels CSAF-Dokumenten nicht mehr wegzudenken sein. Das BSI unterstützt mit Plattformen und Tools rund um CSAF, darunter Validierungstools und Templates für strukturierte Advisories und stellt über den Warn- und Informationsdienst von CERT-Bund Meldungen zu Schwachstellen und Sicherheitslücken bereit. Zusätzlich findet sich dort noch ein CSAF-Lister. Dort sind öffentliche Stellen, die CSAF-Dokumente veröffentlichen, aufgelistet.

Schwachstellenmanagement und security.txt

Ein effektives Schwachstellenmanagement ist essenziell.

Organisationen sollten:

- eine security.txt-Datei gemäß RFC 9116 bereitstellen, um Kontaktaufnahme für Sicherheitsmeldungen zu erleichtern,
- das Common Security Advisory Framework (CSAF) nutzen, um strukturierte, maschinenlesbare Advisories zu veröffentlichen.

Das CSAF-Format erlaubt sowohl die Kommunikation von Betroffenheit als auch von Nicht-Betroffenheit (via VEX-Profile).

Das BSI stellt Tools, Templates und eine zentrale Plattform für die Verteilung bereit. →9

Cybersicherheit in der Gebäudeautomation

Asset-Management in der Gebäudeautomation mit Malcolm

In vernetzten Gebäuden bildet das Asset-Management die Grundlage für einen sicheren und stabilen Betrieb. Nur wer weiß, welche Geräte wo und wie eingebunden sind, kann gezielt auf Sicherheitsvorfälle, Schwachstellenmeldungen oder Ausfälle reagieren. Doch viele Betreiber arbeiten noch mit fragmentierten Listen oder unvollständigen Dokumentationen.

Hier setzt das Open-Source-Projekt Malcolm an. Entwickelt vom Idaho National Laboratory (INL), ermöglicht es die passive Erfassung und Analyse von Kommunikationsverhalten in industriellen und gebäudetechnischen Netzwerken. Malcolm erkennt automatisch Assets im Netzwerk, klassifiziert sie und visualisiert ihre Kommunikationsbeziehungen. Dabei kommen Werkzeuge wie Zeek, Suricata und Kibana zum Einsatz. Betreiber erhalten so nicht nur einen vollständigen Überblick über ihre technische Infrastruktur, sondern auch ein Frühwarnsystem bei ungewöhnlichen Aktivitäten. Gerade in heterogenen Netzen mit BACnet/IP, KNX, MQTT und proprietären Protokollen bietet Malcolm eine wertvolle Grundlage für Compliance, Vorfallmanagement und Auditierbarkeit. →10

Netzwerksicherheit in der Gebäudeautomation

Die Netzwerksicherheit bildet das Rückgrat der Gebäudesicherheit. Mit der zunehmenden Vernetzung und externen Anbindung von Automationskomponenten steigen die Risiken – etwa durch ungeschützte VPN-Gateways, direkt erreichbare Steuerungen oder unkontrollierten Fernzugriff. Exponierte Systeme müssen konsequent abgeschottet werden. Sie sollten nie direkt aus dem Internet erreichbar sein, sondern über sichere VPN-Verbindungen, Zwei-Faktor-Authentifizierung und Firewalls abgesichert werden. Auch Protokolle wie BACnet/IP oder Modbus/TCP dürfen nur über klar definierte Kommunikationspfade genutzt werden. Besonders kritisch ist der Übergang zwischen IT- und OT-Netzen. Diese Schnittstelle muss über dedizierte Zonen oder Demilitarisierte Zonen (DMZ) geschützt werden. Nur klar autorisierte Datenflüsse dürfen hier stattfinden – idealerweise überwacht durch DPI (Deep Packet Inspection) und Logging-Systeme wie z. B. Malcolm.

Die internationale Norm IEC 62443 definiert hierfür ein Zonierungsmodell, das sich in der Gebäudeautomation hervorragend anwenden lässt. Netzwerke werden in Sicherheitszonen unterteilt, etwa für Managementsysteme, Automationsnetzwerke, Feldgeräte und externe Dienstleister. Die Verbindungen zwischen diesen Zonen – sogenannte Conduits – werden kontrolliert und abgestuft abgesichert. Jede Zone erhält ein definiertes Schutzniveau (Security Level), abhängig von ihrem Risiko. So wird verhindert, dass etwa ein infizierter IT-Client unkontrolliert Zugriff auf die Gebäudeleittechnik erlangt. Das Modell der tiefgestaffelten Verteidigung („Defense in Depth“) ist damit auch in der Gebäudeautomation die optimale Methode zur Absicherung der Netzwerke.

Von der Norm zur Umsetzung: VDMA und BIG-EU liefern Orientierung

Die Themen Cybersicherheit und Resilienz rücken auch in der Gebäudeautomation zunehmend in den Vordergrund. Zwei aktuelle Dokumente liefern dazu wichtige Orientierungshilfen: das VDMA-Einheitsblatt 24774 sowie der Leitfaden „Sicherheit in der Gebäudeautomation“ der BIG-EU-Arbeitsgruppe WG-FM.

Das VDMA-Einheitsblatt 24774, richtet sich an alle am Lebenszyklus technischer Gebäudeausrüstung beteiligten Akteure – von Planern und Errichtern über Hersteller bis hin zu Betreibern. Ziel des Dokuments ist es, die Anforde-

Ereignis / Frist	Datum	Beschreibung
Veröffentlichung im EU-Amtsblatt	20. November 2024	Veröffentlichung des Gesetzestextes im Europäischen Amtsblatt
Inkrafttreten der Verordnung	11. Dezember 2024	CRA ist formal in Kraft, gilt direkt in allen Mitgliedstaaten.
Beginn der Übergangsfrist	11. Dezember 2024	Hersteller, Importeure und Händler haben Zeit zur Umsetzung.
Pflicht zur Meldung aktiver Schwachstellen und Sicherheitsvorfälle	11. September 2026	Hersteller müssen Sicherheitslücken und Vorfälle binnen 24 Stunden an ENISA melden.
Verbindliche Anwendungspflichten	11. Dezember 2027	Alle Anforderungen gelten vollumfänglich: Sicherheitsanforderungen, CE-Kennzeichnung, Marktüberwachung, Konformitätsbewertung.

rungen an die Informationssicherheit aus Normen wie IEC 62443 praxisgerecht auf den Kontext der Gebäudeautomation zu übertragen. Dabei führt das Einheitsblatt grundlegende Rollen- und Begriffsmodelle ein, weist konkrete Verantwortlichkeiten zu und beschreibt Maßnahmen zur Risikoanalyse und Risikominimierung. Es werden typische Gefährdungslagen wie unautorisierter Zugriff, Manipulation oder Systemausfall skizziert, und es werden Sicherheitsmaßnahmen vorgestellt – unter anderem zur Netzwerksegmentierung, Zugriffskontrolle, Absicherung von Fernzugängen sowie zum Schwachstellen- und Patchmanagement. Zentrales Element ist die Einführung eines Zonierungsmodells (Zonen und Conduits) zur strukturierten Sicherheitsarchitektur analog zur IEC 62443. Das Einheitsblatt betont zudem, dass Cybersicherheit kein einmaliger Akt, sondern ein kontinuierlicher Prozess im Betrieb ist – inklusive regelmäßiger Prüfung, Dokumentation und Schulung. Damit bietet es eine wertvolle Brücke zwischen internationalen Normen und der Umsetzung in der Praxis – insbesondere für Betreiber und Systemintegratoren. →11

Ergänzend dazu wurde der WG-FM-Leitfaden „Sicherheit in der Gebäudeautomation“ durch die BIG-EU veröffentlicht. Dabei wird deutlich: Sicherheit beginnt bereits in der Planungsphase. Der Leitfaden empfiehlt, frühzeitig ein übergreifendes Sicherheitskonzept zu erstellen, das alle Beteiligten – von der Planung über die Inbetriebnahme bis zum laufenden Betrieb – einbezieht. Technische Empfehlungen beinhalten u. a. die Segmentierung von Netzwerken, die Vermeidung direkter Internetexponierung von Automationssystemen, sichere Fernwartungslösungen sowie ein strukturiertes Schwachstellenmanagement.

Auch Betreiberpflichten stehen im Fokus: Sie sollen die organisatorischen Voraussetzungen schaffen, um auf sicherheitsrelevante Ereignisse reagieren zu können. Dabei orientiert sich der Leitfaden eng an etablierten Normen wie IEC 62443 und ISO 27001, bleibt aber bewusst anwendungsnah – insbesondere für kleine und mittlere Unternehmen. Durch ergänzende Checklisten und praxisbezogene Hinweise bietet der Leitfaden eine pragmatische Hilfestellung für die sichere Umsetzung von GA-Projekten im Spannungsfeld zwischen technischer Komplexität und regulatorischer Verantwortung.

Beide Dokumente – das VDMA-Einheitsblatt 24774 und der WG-FM-Leitfaden – leisten einen wichtigen Beitrag dazu, Cybersicherheit in der Gebäudeautomation greifbar, planbar und nachhaltig umsetzbar zu machen. →12

Fazit

Die gesetzlichen Rahmenbedingungen im Bereich Cybersicherheit befinden sich im Wandel – mit neuen Pflichten für Betreiber und Hersteller durch europäische Regelwerke wie NIS-2, CER, CRA und RED. Doch unabhängig von Fristen und Vorschriften gilt: Wer seine Gebäude und Systeme langfristig sicher betreiben will, sollte jetzt proaktiv handeln. Die Anforderungen an Cybersicherheit lassen sich nicht auf einzelne Maßnahmen reduzieren, sondern verlangen ein durchdachtes Zusammenspiel aus technischen Lösungen, organisatorischen Prozessen und klaren Zuständigkeiten. Nur so können Betreiber und Hersteller der Gebäudeautomation die zunehmenden Risiken wirksam kontrollieren – und gleichzeitig die Chancen der Digitalisierung verantwortungsvoll nutzen. ■

1 IEU directive
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555

Richtlinien der EU
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX%3A32022L2555

Informationsportal des BSI zu NIS-2
https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/regulierte-wirtschaft_node.html

2 BSI information portal on CRA:
www.bsi.bund.de/dok/cra-en

Informationsportal BSI zu CRA:
www.bsi.bund.de/dok/cra

3 BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

BSI TR-03183 Cyber-Resilienz-Anforderungen
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

4 EU – Webseite RED
https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

BSI Pressemeldung RED
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250130_RED_Cybersicherheit.html

5 English not available
TRBS 1115 Teil 1
https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1

6 English not available
INF.13 Technisches Gebäudemanagement
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_13_Technisches_Gebaeudemanagement_Edition_2023.pdf

7 English Version of the IT-Grundschutz-Compendium Edition 2022
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf

INF.14 Gebäudeautomation (Edition 2023)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.pdf

8 security.txt: A Simple File with Big Value
https://www.cisa.gov/news-events/news/securitytxt-simple-file-big-value

security.txt: Standardised contact information for IT security disclosures
https://www.dguv.de/ifa/fachinfos/industrial-security/kontaktstandard-security-txt/index-2.jsp

BSI CS-149 Sicherheitskontakte mit Hilfe einer security.txt nach RFC 9116 angeben
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_149.html

9 Common Security Advisory Framework (CSAF)
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-

Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

Common Security Advisory Framework (CSAF)
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

10 Project page on GITHub
https://github.com/idaholab/Malcolm
German not available

11 English not available
VDMA-Einheitsblatt 24774
Überträgt IEC 62443 auf den GA-Lebenszyklus, inkl. Rollenmodell, Risikobewertung, Zonierung
https://www.vdma.eu/documents/d/group-34568/vdma-24774_2023-03

12 WG-FM Guide Security in Building Automation (BIG-EU) – Focus on implementation in small and medium-sized BA projects:
https://www.big-eu.org/wp-content/uploads/sites/6/2025/02/BIG-EU-WG-FM-100-Version-01-Stand-09-24_English.pdf

WG-FM-Leitfaden: Sicherheit in der Gebäudeautomation (BIG-EU) – Fokus auf Umsetzung in kleinen und mittleren GA-Projekten:
https://www.big-eu.org/wp-content/uploads/sites/6/2024/09/BIG-EU-WG-FM-100-Version-01-Stand-09-24.pdf

Jens Kluge
Referat C 25 – Industrielle Steuerungs- und Automatisierungssysteme Bundesamt für Sicherheit in der Informationstechnik
ics-sec@bsi.bund.de | www.bsi.bund.de

Secure HTTPS Provides Enhanced Security in a Building Management System

Sicheres HTTPS bietet erhöhte Sicherheit in einem Gebäudemanagementsystem

Network Security is more critical than ever in today's building management system (BMS) networks to ensure authentication, integrity, and confidentiality of data transferred over the Internet. This article describes how BACnet-complaint devices that incorporate HTTPS deliver encrypted communication and protect the integrity of client data. This article also describes the HTTPS authentication and encryption method which utilizes keys and digital certificates. It compares certificates generated by a Certificate Authority (CA) vs. self-signed certificates and provides a resource to create your own self-signed certificate.

Netzwerksicherheit ist in den heutigen Gebäudemanagementsystemen (BMS) wichtiger denn je, um die Authentifizierung, Integrität und Vertraulichkeit der über das Internet übertragenen Daten zu gewährleisten. In diesem Artikel wird beschrieben, wie BACnet-konforme Geräte mit HTTPS eine verschlüsselte Kommunikation ermöglichen und die Integrität der Kundendaten schützen. Außerdem werden die HTTPS-Authentifizierungs- und Verschlüsselungsmethode beschrieben, die Schlüssel und digitale Zertifikate verwendet. Es werden von einer Zertifizierungsstelle (CA) generierte Zertifikate mit selbstsignierten Zertifikaten verglichen und eine Ressource zum Erstellen eigener selbstsignierter Zertifikate bereitgestellt.

BACnet-complaint devices that incorporate HTTPS provide encrypted webpage communication and protect the integrity of client data.
BACnet-konforme Geräte mit HTTPS bieten verschlüsselte Webseitenkommunikation und schützen die Integrität der Kundendaten. © Contemporary Controls

BACnet remains the most popular protocol utilized in HVACR control systems and there is a robust ecosystem of devices that comprise these systems, including Gateways to integrate other protocols, such as Modbus and EnOcean, to BACnet. As more and more devices are utilized to meet the demands of today's building management system (BMS) and smart building infrastructures, network security is more critical than ever to ensure authentication, integrity, and confidentiality of data transferred over the Internet.

BACnet-complaint devices that incorporate HTTPS (Secure HTTP) deliver encrypted communication and protect the integrity of client data. Resident HTTPS webservers allow commissioning, status reporting, and troubleshooting in a secure manner using any standard web browser, thereby improving access control to the devices.

HTTPS (Secure HTTP) uses encryption for secure communication over an IP network. HTTPS traffic is encrypted using Transport Layer Security (TLS), formerly Secure Sockets Layer (SSL). The protocol is still referred to as HTTP over SSL, commonly shown as https:// in the browser address bar.

Digital Certificates

SSL/TLS relies on the use of keys and digital certificates for data encryption, device authentication, and data integrity. Keys occur in pairs (public/private) and are used for encryption/decryption. A public key is used for encryption, while the private key is used for decryption.

Digital certificates are used for authentication and encryption, verifying ownership and authenticity to ensure that only authorized devices communicate with each other. The public key is part of the certificate, while the private key is secret to the device.

Mechanisms exist to generate certificates and keys for a device and to scale the architecture to multiple devices.

Digital Certificates – Certificate Authority

Certificates are typically issued and managed by a trusted third-party company, called a Certificate Authority (CA). Getting an SSL certificate installed for a website by a well-known CA that is trusted by all devices and browsers, such as DigiCert, Comodo, GoDaddy, Lets Encrypt, can provide access to the website seamlessly over the public Internet. The device can get the certificate directly from the CA or send a Certificate Signing Request (CSR) to the CA to get the corresponding certificate. These trusted CAs only provide certificates to websites or devices which have a public IP address. They won't provide certificates for devices on an internal network with private IP addresses.

Digital Certificates – Public Key Infrastructure

For an internal BMS network, getting a certificate from a public CA is not necessary and can be expensive given the considerable number of devices in a building. The

IT department can implement their own infrastructure to generate these keys and certificates. The term PKI (Public Key Infrastructure) is used to define this setup. The building automation product vendors may also have specific software tools to implement the PKI, but the certificates and keys for all devices at a site, irrespective of their brand, must be generated from the same tool to ensure interoperability. The certificates on devices also expire and need to be renewed.

Devices used on internal networks can also employ a self-signed digital certificate to make a web browser trust your internal devices. A self-signed certificate is a type of SSL/TLS credential you sign yourself rather than having it signed by a trusted third-party CA. If you don't have an IT department, you can generate the self-signed certificate yourself. In addition, generating a self-signed certificate for internal network devices eliminates the associated cost of getting a certificate from a trusted third-party CA.

Digital Certificates – Self-Signed

Self-signed digital certificates are created by signing the certificate with the owner's private key. They are created, issued, and signed by the company or developer who is responsible for the website/software being signed. Unlike certificates issued by a trusted CA, no external party verifies a self-signed certificate. Self-signed certificates are fast, free, and easy to issue. They are appropriate for local development, testing, or staging environments, internal network websites and providing secure webpages for devices. However, you must be aware of their limitations, such as despite the strong encryption they provide, they lack the backing of recognized authority, so browsers on different PCs will display security warnings for them.

Digital Certificates – OpenSSL

You can generate and install a self-signed certificate using OpenSSL, a commonly used command-line utility for generating keys, creating certificate signing requests (CSRs), and managing certificates.

According to OpenSSL documentation at https://docs.openssl.org/master/man7/ossl-guide-introduction: "OpenSSL is a robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication. Its features are made available via a command line application that enables users to perform various cryptography related functions such as generating keys and certificates. Additionally, it supplies two libraries that application developers can use to implement cryptography-based capabilities and to securely communicate across a network. Finally, it also has a set of providers that supply implementations of a broad set of cryptographic algorithms. OpenSSL is fully open source. Version 3.0 and above are distributed under the Apache v2 license."

Digital certificates verify ownership and authenticity to ensure that communication occurs with authorized devices.
Digitale Zertifikate überprüfen die Eigentümerschaft und Authentizität, um sicherzustellen, dass die Kommunikation mit autorisierten Geräten erfolgt.
© Creative Commons

If you don't have OpenSSL on your Windows's PC, you can install an OpenSSL package. If you are accessing the HTTPS device from a different PC, a security warning message will appear. You must download the self-signed certificate and install it to your local machine's trusted certificate store.

For more information, Contemporary Controls has created an Application Note: How to Create and Use Self-Signed SSL Certificates that explains how to add OpenSSL and create a self-signed certificate for Windows using Windows Package Manager, WinGet. WinGet is a free and open-source package manager designed by Microsoft that allows users to discover, install, upgrade, remove, and configure applications on Windows 10, Windows 11, and Windows Server 2025 computers. The application note also explains how to install this self-signed certificate on the device, and how to download and install the self-signed certificate on different Windows machines to eliminate the security warning. Instructions are provided for commonly used browsers – Google Chrome, Microsoft Edge, and Mozilla Firefox – and how to overcome the Security Warning message.

Conclusion

HTTPS encrypts the transport of data to ensure data integrity and prevents information from being modified, corrupted, or stolen during transmission. SSL/TLS protocols authenticate users to secure information and ensure it won't be revealed to unauthorized users. HTTPS requires digital certificates to validate the domain ownership and integrity. For external networks, you should obtain this credential from a trusted third-party CA.

Self-signed certificates are valuable for creating secure communication channels for internal networks when you control the environment. They offer quick deployment and cost savings and are ideal for testing, local development, or internal applications. Understanding these concepts is critical to implementing security for IP devices in general. For the Building Automation world based on BACnet, they provide the foundational knowledge for successful and robust implementation of BACnet/SC. ■

BACnet ist nach wie vor das beliebteste Protokoll für HVACR-Steuerungssysteme. Es gibt ein robustes Ökosystem von Geräten, aus denen diese Systeme bestehen, darunter Gateways zur Integration anderer Protokolle wie Modbus und EnOcean in BACnet. Da immer mehr Geräte eingesetzt werden, um die Anforderungen der heutigen Gebäudemanagementsysteme (BMS) und intelligenten Gebäudeinfrastrukturen zu erfüllen, ist die Netzwerksicherheit wichtiger denn je, um die Authentifizierung, Integrität und Vertraulichkeit der über das Internet übertragenen Daten zu gewährleisten.

BACnet-konforme Geräte mit HTTPS (Secure HTTP) bieten verschlüsselte Kommunikation und schützen die Integrität der Kundendaten. Integrierte HTTPS-Webserver ermöglichen die Inbetriebnahme, Statusberichterstattung und Fehlerbehebung auf sichere Weise über jeden Standard-Webbrowser und verbessern so die Zugriffskontrolle auf die Geräte.

HTTPS (Secure HTTP) verwendet Verschlüsselung für die sichere Kommunikation über ein IP-Netzwerk. Der HTTPS-Datenverkehr wird mit Transport Layer Security (TLS), früher Secure Sockets Layer (SSL), verschlüsselt. Das Protokoll wird weiterhin als HTTP über SSL bezeichnet und in der Adressleiste des Browsers üblicherweise als https:// angezeigt.

Digitale Zertifikate

SSL/TLS basiert auf der Verwendung von Schlüsseln und digitalen Zertifikaten für die Datenverschlüsselung, Geräteauthentifizierung und Datenintegrität. Schlüssel kommen paarweise vor (öffentlich/privat) und werden zur Ver- und Entschlüsselung verwendet. Ein öffentlicher Schlüssel wird zur Verschlüsselung verwendet, während der private Schlüssel zur Entschlüsselung dient.

Digitale Zertifikate werden zur Authentifizierung und Verschlüsselung verwendet, um die Eigentümerschaft und Authentizität zu überprüfen und sicherzustellen, dass nur autorisierte Geräte miteinander kommunizieren. Der öffentliche Schlüssel ist Teil des Zertifikats, während der private Schlüssel für das Gerät geheim ist.

Es gibt Mechanismen, um Zertifikate und Schlüssel für ein Gerät zu generieren und die Architektur auf mehrere Geräte zu skalieren.

Digitale Zertifikate – Zertifizierungsstelle

Zertifikate werden in der Regel von einem vertrauenswürdigen Drittunternehmen, einer sogenannten Zertifizierungsstelle (CA), ausgestellt und verwaltet. Die Installation eines SSL-Zertifikats für eine Website durch eine bekannte CA, welcher von allen Geräten und Browsern vertraut wird, wie z. B. DigiCert, Comodo, GoDaddy oder Lets Encrypt, kann einen nahtlosen Zugriff auf die Website über das öffentliche Internet ermöglichen. Das Gerät kann

das Zertifikat direkt von der CA beziehen oder eine Zertifikatssignierungsanforderung (CSR) an die CA senden, um das entsprechende Zertifikat zu erhalten. Diese vertrauenswürdigen CAs stellen Zertifikate nur für Websites oder Geräte mit einer öffentlichen IP-Adresse aus. Sie stellen keine Zertifikate für Geräte in einem internen Netzwerk mit privaten IP-Adressen aus.

Digitale Zertifikate – Public-Key-Infrastruktur

Für ein internes BMS-Netzwerk ist es nicht erforderlich, ein Zertifikat von einer öffentlichen Zertifizierungsstelle zu beziehen. Dies kann angesichts der beträchtlichen Anzahl von Geräten in einem Gebäude kostspielig sein. Die IT-Abteilung kann eine eigene Infrastruktur zur Generierung dieser Schlüssel und Zertifikate implementieren. Der Begriff PKI (Public Key Infrastructure) wird verwendet, um diese Konfiguration zu definieren. Die Anbieter von Gebäudeautomationsprodukten verfügen möglicherweise auch über spezielle Softwaretools zur Implementierung der PKI, aber die Zertifikate und Schlüssel für alle Geräte an einem Standort, unabhängig von ihrer Marke, müssen mit demselben Tool generiert werden, um die Interoperabilität zu gewährleisten. Die Zertifikate auf den Geräten laufen ebenfalls ab und müssen erneuert werden.

Geräte, die in internen Netzwerken verwendet werden, können auch ein selbstsigniertes digitales Zertifikat verwenden, damit ein Webbrowser Ihren internen Geräten vertraut. Ein selbstsigniertes Zertifikat ist eine Art SSL/TLS-Berechtigungsnachweis, den Sie selbst signieren, anstatt ihn von einer vertrauenswürdigen Drittanbieter-Zertifizierungsstelle signieren zu lassen. Wenn Sie keine IT-Abteilung haben, können Sie das selbstsignierte Zertifikat selbst erstellen. Darüber hinaus entfallen durch die Erstellung eines selbstsignierten Zertifikats für interne Netzwerkgeräte die Kosten für die Beschaffung eines Zertifikats von einer vertrauenswürdigen Drittanbieter-Zertifizierungsstelle.

About the Author

Harpartap Parmar is a Director of Product Management at Contemporary Controls, which designs and manufactures BACnet building controls and IP networking equipment. Parmar focuses on network security, IP routers and their application to Building Automation. He has over 25 years of experience at Contemporary Controls with a range of networking, control, and communication products.

Über den Autor

Harpartap Parmar ist Leiter des Produktmanagement bei Contemporary Controls, einem Hersteller und Entwickler für BACnet- und Netzwerkgeräte. Sein Spezielgebiet konzentriert sich vor allem auf Netzwerksicherheit und deren Anwendung in der Gebäudeautomation. Er verfügt über mehr als 25 Jahre Erfahrung bei Contemporary Controls mit einer Reihe von Netzwerk-, Steuerungs- und Kommunikationsprodukten.

Digitale Zertifikate – Selbstsigniert

Selbstsignierte digitale Zertifikate werden erstellt, indem das Zertifikat mit dem privaten Schlüssel des Eigentümers signiert wird. Sie werden von dem Unternehmen oder Entwickler erstellt, ausgestellt und signiert, das bzw. der für die zu signierende Website/Software verantwortlich ist. Im Gegensatz zu Zertifikaten, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden, werden selbstsignierte Zertifikate nicht von einer externen Stelle überprüft. Selbstsignierte Zertifikate sind schnell, kostenlos und einfach auszustellen. Sie eignen sich für lokale Entwicklungs-, Test- oder Staging-Umgebungen, interne Netzwerk-Websites und die Bereitstellung sicherer Webseiten für Geräte. Sie müssen sich jedoch ihrer Einschränkungen bewusst sein, z. B. dass sie trotz ihrer starken Verschlüsselung nicht von einer anerkannten Behörde unterstützt werden, sodass Browser auf anderen PCs Sicherheitswarnungen für sie anzeigen.

Digitale Zertifikate – OpenSSL

Sie können ein selbstsigniertes Zertifikat mit OpenSSL erstellen und installieren, einem häufig verwendeten Befehlszeilenprogramm zum Generieren von Schlüsseln, Erstellen von Zertifikatssignierungsanforderungen (CSRs) und Verwalten von Zertifikaten.

Laut der OpenSSL-Dokumentation unter https://docs.openssl.org/master/man7/ossl-guide-introduction „ist OpenSSL ein robustes, kommerzielles Toolkit mit vollem Funktionsumfang für allgemeine Kryptografie und sichere Kommunikation. Seine Funktionen werden über eine Befehlszeilenanwendung bereitgestellt, mit der Benutzer verschiedene kryptografische Funktionen wie die Generierung von Schlüsseln und Zertifikaten ausführen können. Darüber hinaus enthält es zwei Bibliotheken, mit denen Anwendungsentwickler kryptografische Funktionen implementieren und sicher über ein Netzwerk kommunizieren können. Schließlich verfügt es auch über eine Reihe von Anbietern, die Implementierungen einer breiten Palette von kryptografischen Algorithmen bereitstellen. OpenSSL ist vollständig Open Source. Version 3.0 und höher werden unter der Apache v2-Lizenz vertrieben."

Wenn Sie OpenSSL nicht auf Ihrem Windows-PC installiert haben, können Sie ein OpenSSL-Paket installieren. Wenn Sie von einem anderen PC aus auf das HTTPS-Gerät zugreifen, wird eine Sicherheitswarnung angezeigt. Sie müssen das selbstsignierte Zertifikat herunterladen und in den vertrauenswürdigen Zertifikatsspeicher Ihres lokalen Computers installieren.

Weitere Informationen finden Sie unter: Application Note: How to Create and Use Self-Signed SSL Certificates von Contemporary Controls, in dem erklärt wird, wie Sie OpenSSL hinzufügen und verwenden, um mit dem Windows Package Manager WinGet ein selbstsigniertes Zertifikat für Windows zu erstellen. WinGet ist ein kostenloser open-source Paketmanager von Microsoft, mit dem Benutzer Anwendungen auf Computern mit Windows 10, Windows 11 und Windows Server 2025 suchen, installieren, aktualisieren, entfernen und konfigurieren können. Der Anwendungshinweis erklärt auch, wie dieses selbstsignierte Zertifikat auf dem Gerät installiert wird und wie das es auf verschiedenen Windows-Rechnern heruntergeladen und installiert wird, um die Sicherheitswarnung zu beseitigen. Es werden Anweisungen für häufig verwendete Browser – Google Chrome, Microsoft Edge und Mozilla Firefox – sowie zur Umgehung der Sicherheitswarnung bereitgestellt.

Fazit

HTTPS verschlüsselt die Datenübertragung, um die Datenintegrität zu gewährleisten und zu verhindern, dass Informationen während der Übertragung verändert, beschädigt oder gestohlen werden. SSL/TLS-Protokolle authentifizieren Benutzer, um Informationen zu schützen und sicherzustellen, dass sie nicht an unbefugte Benutzer weitergegeben werden. HTTPS erfordert digitale Zertifikate, um die Eigentümerschaft und Integrität der Domain zu überprüfen. Für externe Netzwerke sollten Sie diese Berechtigungsnachweise von einer vertrauenswürdigen Drittanbieter-Zertifizierungsstelle beziehen.

Selbstsignierte Zertifikate sind wertvoll für die Einrichtung sicherer Kommunikationskanäle für interne Netzwerke, wenn Sie die Umgebung kontrollieren. Sie bieten eine schnelle Bereitstellung und Kosteneinsparungen und eignen sich ideal für Tests, lokale Entwicklung oder interne Anwendungen. Das Verständnis dieser Konzepte ist für die Implementierung von Sicherheit für IP-Geräte im Allgemeinen von entscheidender Bedeutung. Für die auf BACnet basierende Gebäudeautomation liefern sie das grundlegende Wissen für eine erfolgreiche und robuste Implementierung von BACnet/SC.

CONTEMPORARY CONTROLS

Harpartap Parmar
Leiter Produktmanagement | Contemporary Controls
hparmar@ccontrols.com | www.ccontrols.com

Minimum Standards for IT Security in Building Automation

Mindeststandards für IT-Sicherheit in der Gebäudeautomation

The basic rules for IT security in building automation in Germany are the standards and the Basic Protection Compendium of the Federal Office for Information Security (BSI). The basic protection modules for building management (INF.13) and building automation (INF.14) are mandatory for federal authorities and operators of critical infrastructures (information available at www.bsi.de).

Grundlegende Regelwerke für IT-Sicherheit in der Gebäudeautomation in Deutschland sind die Standards und das Grundschutzkompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Grundschutzbausteine Infrastruktur für Gebäudemanagement (INF.13) und Gebäudeautomation (INF.14) sind verpflichtend für Bundesbehörden und Betreiber kritischer Infrastrukturen (Informationen unter www.bsi.de).

In addition, the VDMA 24774 (2023-03) standard supports BA planning, implementation, and operation with specific requirements for BA systems.

Nevertheless, there is no such thing as 100% IT security for building automation. The specific IT security standards to be met in building automation must be derived from a risk analysis for the respective use of the building.

The current BSI Standards and Basic Protection Compendium in the IT Basic Protection Module INF14 Building Automation from 2022 lists the following risk situations as relevant for building automation:

- Inadequate planning of building automation, for example due to a lack of redundancy or high complexity in the interaction of different trades.
- Faulty integration of TGA systems into building automation or faulty configuration of building automation.
- Use of insecure systems and protocols in building automation, such as the "old" BACnet protocol, as well as KNX or ModBus.
- Manipulation of the interfaces of independent TGA systems for building automation (e.g., via a manipulated fire alarm that opens all doors).

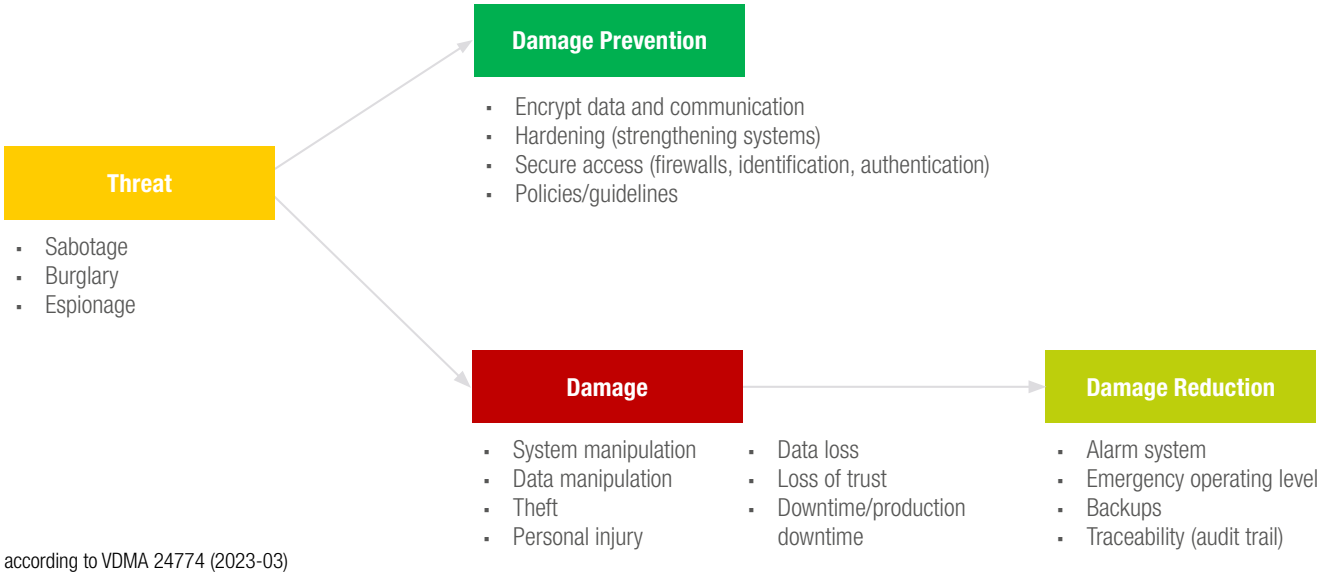
Added to this are the long-life cycles of building services systems, which require a high degree of forward planning for BA systems and a strategic approach.

Based on this, the following specifications should be taken into account when planning BA systems.

Specifications for the Planning of GA Systems

- Specifications for encrypted data transmission/communication (BACnet/SC, KNX-Secure, or similar).
- Deactivation of all unnecessary services and accesses ex works ("hardened" devices and software) including documentation of the ports used.
- Management software with functions for recording user activities (audit trail).
- Acceptance of the GA system only with the latest firmware (automation stations) or software version (BBE, MBE), at least all security-relevant updates, in particular the latest Windows patches and the latest versions of the software systems used.

IT SECURITY STRATEGY FOR BUILDING AUTOMATION



according to VDMA 24774 (2023-03)
vergleichbar mit VDMA 24774 (2023-03)

Requirements for the Implementation and Execution of Building Automation Systems

- Set up physically or virtually separate IP networks for building automation, including protection of particularly vulnerable network segments by firewalls.
- Secure access for remote maintenance.
- Define a backup concept for automation stations and the management level, including instructions for recovery.
- Physically secure switch cabinets, technical rooms, etc., including deactivation of USB or Ethernet access.
- Malware protection and the latest security patches for engineering tools.
- Project-specific adjustment of access authorizations and change of passwords (especially on automation stations, BBE, MBE), activation of auto-logoff functions.
- Hardening of systems by deactivating or deleting all unused services, physical access points, user accounts, processes, and programs (especially on automation stations, BBE, MBE), activation of auto-logoff functions.
- Creation of work regulations and behavioral instructions for the permanent maintenance of IT security by the installer (SOP = Standard Operating Procedure).
- Creation and handover of GA network documentation with model designations of the components, MAC addresses, installation location, and firmware versions.
- IT security training for operators.

Requirements for the Operation of GA Systems

- Individual usernames and passwords.
- Regular security-related updates/upgrades (especially for PCs, servers, and routers), ensuring that updates are downloaded exclusively in unaltered form from certified sources.
- Regular backups of system programming, configuration, configuration changes to the MBE software, and stored operating data.
- Ensuring compliance with work regulations and behavioral guidelines, including regular updates to the IT security concept as part of GA system maintenance.
- Regular IT security training.

Summary

Even in building automation, there is no 100% guarantee of data availability, integrity, authenticity, and confidentiality. However, a good level of security can be achieved by specifying and observing simple technical and organizational measures. The consistent use of BACnet/SC is only one, albeit important, component for greater future security. In summary, here are five tips:

1. Determine the protection requirements for each building based on a risk analysis and use this to derive the IT security concept for the building automation system. This must be done jointly by specialist planners, building owners, and operators.
2. Be aware that HVAC systems are particularly vulnerable in terms of IT security, with the greatest risks currently still arising from the connection of building automation to the Internet, e.g., through cloud computing or gateways.
3. Based on a security concept, define specific IT security requirements for planning, implementation, and operation. Use the specifications from VDMA 24774 for this purpose. Against the backdrop of increasing cloud computing, encrypted protocols such as BACnet/SC should also be required for new BA systems and when renovating existing BA systems.
4. Issue work regulations and behavioral guidelines (policies) for damage prevention and mitigation. Agree on software maintenance and system maintenance to regularly close known security gaps.
5. During regular maintenance, check not only compliance with policies, but also that the IT security concept for the building automation system is up to date. ■

Darüber hinaus unterstützt das Einheitsblatt VDMA 24774 (2023-03) die GA-Planung und Umsetzung und Betrieb mit konkreten Vorgaben für GA-Systeme.

Dennoch gibt es auch für die Gebäudeautomation keine 100-prozentige IT-Sicherheit. Welche IT-Sicherheitsstandards im Gewerk Gebäudeautomation konkret zu treffen sind, müssen aus einer Risikoanalyse für die jeweilige Nutzung des Gebäudes abgeleitet werden.

Im noch aktuellen BSI-Standards- und Grundschutzkompendium im IT-Grundschutzbaustein INF14 Gebäudeautomation von 2022 werden u.a. folgende Gefährdungslagen für die Gebäudeautomation als relevant genannt:

- Unzureichende Planung der Gebäudeautomation, zum Beispiel durch fehlende Redundanzen oder hohe Komplexität der Zusammenarbeit unterschiedlicher Gewerke.
- Fehlerhafte Integration von TGA-Anlagen in die Gebäudeautomation bzw. fehlerhafte Konfiguration der Gebäudeautomation.
- Nutzung unsicherer Systeme und Protokolle in der Gebäudeautomation, wie es z. B. das „alte“ BACnet-Protokoll, ebenso wie KNX oder ModBus sind.
- Manipulation der Schnittstellen von eigenständigen TGA-Anlagen zur Gebäudeautomation (zum Beispiel über eine manipulierte Brandmeldung, die alle Türen öffnet).

Hinzu kommen noch die langen Lebenszyklen gebäudetechnischer Anlagen, die ein besonderes Maß an vorausschauender Planung von GA-Systemen und ein strategisches Vorgehen erfordern.

Daraus abgeleitet sollten folgende Vorgaben sollten bei der Planung von GA-Systemen Berücksichtigung finden.

Vorgaben an die Planung von GA-Systemen

- Vorgaben für eine verschlüsselte Datenübertragung / Kommunikation (BACnet/SC, KNX-Secure o.ä.).
- Deaktivierung aller nicht benötigten Dienste und Zugänge ab Werk („gehärtete“ Geräte und Software) samt Dokumentation der verwendeten Ports.
- Managementsoftware mit Funktionen zur Aufzeichnung der Benutzeraktivitäten (Audit Trial).
- Abnahme des GA-Systems nur mit der aktuellsten Firmware (Automationsstationen)

beziehungsweise Softwareversion (BBE, MBE), zumindest alle Security-relevante Updates, insbesondere die aktuellen Patches von Windows sowie die aktuellen Versionen der eingesetzten Softwaresysteme.

Vorgaben an die Umsetzung und Ausführung der Gebäudeautomationssysteme

- Einrichtung physikalisch oder virtuell getrennte IP-Netzwerke für die Gebäudeautomation samt Absicherung besonders gefährdeter Netzwerksegmente durch Firewalls.
- Gesicherter Zugriff für Fernwartung.
- Festlegung eines Back-up Konzeptes für Automationsstationen und Managementebene samt Anweisungen für ein Recovery.
- Physische Sicherung von Schaltschränken, Technikräumen etc. samt Deaktivierung von USB- oder Ethernet-Zugängen.
- Malwareschutz und aktuellste Sicherheitspatches für Engineering-Werkzeuge.
- Projektspezifische Anpassung der Zugriffsberechtigungen und Änderung der Passwörter (insbesondere auf Automationsstationen, BBE, MBE), Aktivierung von Auto-Logoff-Funktionen.
- Nachhärtung der Systeme durch Deaktivierung beziehungsweise Löschung aller ungenutzter Dienste, physikalische Zugänge, Benutzerkonten, Prozesse und Programme (insbesondere auf Automationsstationen, BBE, MBE), Aktivierung von Auto-Logoff-Funktionen.
- Erstellung der Arbeitsvorschriften und Verhaltensanweisungen zum dauerhaften Erhalt der IT-Sicherheit durch den Errichter (SOP = Standard Operating Procedure).
- Erstellung und Übergabe einer GA-Netzwerk-Dokumentation mit Modellbezeichnungen der Komponenten, MAC-Adressen, Einbauort und Firmware Versionsständen.
- IT-Sicherheitsschulung für die Bediener.

Vorgaben an den Betrieb der GA-Systeme

- Individuelle Benutzernamen und Passwörter.
- Regelmäßige security-relevante Updates/Upgrades (insbesondere von PCs, Servern und Routern), dabei Sicherstellung, dass Updates ausschließlich unverfälscht, von Quellen mit Zertifikat heruntergeladen werden.
- Regelmäßige Back-ups von Anlagenprogrammierung, Konfiguration, Konfigurationsänderungen der MBE-Software sowie der gespeicherten Betriebsdaten.
- Sicherstellung der Einhaltung der Arbeitsvorschriften und Verhaltensanweisungen samt regelmäßiger Aktualisierung des IT-Sicherheitskonzeptes im Rahmen der Wartung des GA-Systems.
- Regelmäßige IT-Sicherheitsschulungen.

Zusammenfassung

Auch in der Gebäudeautomation gibt es keine 100-prozentige Sicherheit für Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Daten. Durch Vorgabe und Beachtung einfacher technischer und organisatorischer Maßnahmen kann jedoch ein gutes Sicherheitsniveau erreicht werden. Der konsequente Einsatz von BACnet/SC ist dabei nur ein, wenn auch wichtiger Baustein für mehr Zukunftssicherheit. Zusammenfassend folgende 5 Tipps:

1. Stellen Sie für jedes Gebäude den Schutzbedarf auf Basis einer Risikoanalyse fest und leiten Sie daraus das IT-Sicherheitskonzept für die GA ab. Dies müssen Fachplaner, Bauherr und Betreiber gemeinsam tun.
2. Machen Sie sich bewusst, dass GA-Systeme besonders verwundbar in Bezug auf die IT-Sicherheit sind, wobei sich die größten Risiken aktuell noch aus der Anbindung der Gebäudeautomation an das Internet ergeben, z. B. durch Cloud-Computing oder Gateways.
3. Machen Sie auf Basis eines Sicherheitskonzeptes konkrete IT-Sicherheits-Vorgaben für Planung, Umsetzung und Betrieb. Nutzen Sie dafür die Vorgaben aus VDMA 24774. Auch vor dem Hintergrund des zunehmenden Cloud-Computing sollten für neu zu errichtende GA-Systeme und bei Sanierung vorhandener GA-Systeme verschlüsselte Protokolle wie BACnet/SC gefordert werden.
4. Erlassen Sie Arbeitsvorschriften und Verhaltensanweisungen (Policies) zur Schadensvermeidung und Schadensminderung. Vereinbaren Sie Softwarepflege und Systemwartung zum regelmäßigen Schließen bekannter Sicherheitslücken.
5. Prüfen Sie im Zuge regelmäßiger Wartung nicht nur die Einhaltung der Policies, sondern auch die Aktualität des IT-Sicherheitskonzeptes für die GA. ■

About Christian Wild

Christian Wild is the managing director of Iconag Leittechnik in Idar-Oberstein, a software company for manufacturer-independent building control technology, energy management, and digitization in technical building management. For more than 25 years, he and his team have been working to make technical building management efficient and secure through the use of open technologies such as BACnet, KNX, OPC, and ModBus.

Über Christian Wild

Christian Wild ist Geschäftsführer der Iconag Leittechnik in Idar-Oberstein, ein Softwareunternehmen für herstellerneutrale Gebäudeleittechnik, Energiemanagement und Digitalisierung im technischen Gebäudemanagement. Er arbeitet seit mehr als 25 Jahren mit seinem Team daran, durch Einsatz offener Technologien wie BACnet, KNX, OPC oder ModBus das Technische Gebäudemanagement effizient und sicher zu gestalten.

Christian Wild
Geschäftsführer | ICONAG Leittechnik GmbH Idar-Oberstein
christian.wild@iconag.com | www.iconag.com

Artificial Intelligence in the field of Building Automation

Künstliche Intelligenz in der Gebäude-automation

The term "AI – Artificial Intelligence" is increasingly associated with buildings and building automation. The question is: what is it, where do its tangible benefits lie in this field, and how does the building infrastructure need to be adapted to realize those benefits?

Der Begriff „KI – Künstliche Intelligenz" wird in zunehmendem Maße mit Gebäuden und Gebäudeautomation in Verbindung gebracht. Die Frage ist: Was ist künstliche Intelligenz, wo liegen ihre konkreten Vorteile für die Gebäudeautomation, und wie muss die Gebäudeinfrastruktur angepasst werden, um diese Vorteile zu nutzen?

Today's building automation systems in the main operate 'statically' in response to fixed time programs or simple control parameters. Room temperature control is based on a preset temperature that is the same throughout the day. Lighting is operated manually, with switches, or on the basis of simple presence switches. None of this is truly 'intelligent'. The new dimension that AI can add into the building automation environment is to use autonomous analysis of the data as a basis for optimized operation. Thus, the heating and cooling dynamic of rooms, weather forecasts, predicted room occupancy during the course of the day can all be factored into the operation of the heating.

Similarly, cleaning schedules can be based not only on the current actual values in terms of the intensity of use of kitchens, canteens and toilets and other areas, but can be based on predictions drawn from an analysis of usage patterns in the previous days and weeks. This kind of forward-looking building management can be applied in almost every area of building services, leading to increased energy efficiency, reduced operating costs, improved space utilization and other advantages.

All this – and much more – is possible when data on building system status and conditions is intelligently evaluated. This requires intensive processing of large amounts of data, with many variables to be considered. Artificial Intelligence (AI) offers many new, tailor-made solutions which are eminently suited to efficient building management.

"Building Automation", "Smart Building" and "Cognitive Building"

Initially, "Building Automation" was comparatively "unintelligent". Systems were programmed to follow a set of simple rules, allowing for quick system start-up and subsequent ease of maintenance.

The "Smart Building" typically builds on this classic building automation with flexible IT-based management systems. These offer unrestricted programming using modern IT languages and tools, easy integration with other IT systems such as workspace/room reservation systems or data banks, and data visualization for facility managers and for "ordinary" users.

The growing assimilation of sensor-generated data into the IT-based management level opens the way for more advanced data processing solutions to come into play – such as AI tools. This is the pre-condition for the implementation of any prognosis-based form of building management. The sophisticated processing of sensor-generated data makes the Smart Building into a "Cognitive Building". (Fig. 1)

AI-Learning Process

The first step in any Artificial Intelligence process is system learning. This can take three forms.

- Unsupervised Learning
- Supervised Learning
- Reinforcement Learning

"Unsupervised Learning" is used when large quantities of data must be processed and categorized. This grouping enables the recognition of deviations from norms and interdependencies. For example, sensor data from identical circulation pumps can be grouped. If data from one pump or group of pumps deviates from the norm, there may be a defect, and a human engineer can be sent to investigate.

"Supervised Learning" often makes use of neural networks. They consist of entry and exit nodes as well as further nodes in the intermediate layers. Mathematically weighted relationships exist between the diverse nodes (neurons). In order to optimize these relationships, the neural network is subjected to a training phase with known input and output patterns. In the field of building automation, for example, a neural network can "learn" the current consumption profiles of different appliances and which appliances are active when. This information

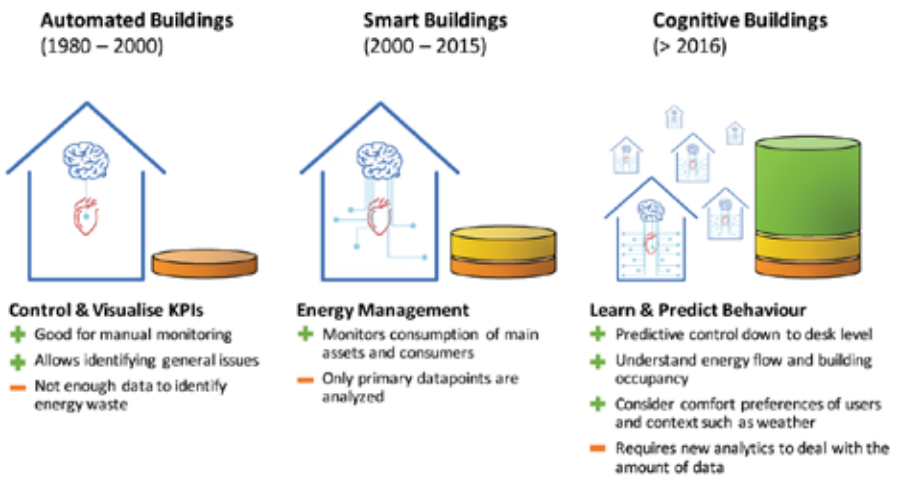


Fig. 1: Building Automation – Smart Building – Cognitive Building (source: IBM)
Abb. 1: Gebäudeautomation – Smart Building – Cognitive Building (Quelle: IBM)

can be used to avoid "spikes" in building energy consumption, by shutting down some appliances and extending the operation time of others.

Another form of Artificial Intelligence is represented by processes that autonomously determine which actions are appropriate in a given situation. They emulate human behavior whereby different solutions are tried in order to determine the best way forwards in a hitherto unknown situation, and conclusions drawn retrospectively. The learning task becomes more challenging when feedback is given much later and hinges upon events in the relatively distant past. This is true in a human context, and equally true in computer environments.

The best-known example in this category is "Reinforcement Learning". Consider the issue of determining the optimal start and stop times of heating to achieve a comfortable temperature when the building opens. At the simplest level, the learning algorithm receives the value from the room temperature sensor and can act on the actuator on the radiator. By a process of trial and error, the algorithm can determine the necessary lead time. However, this simple example ignores the fact that, for instance, the speed of heating also depends on the outside temperature, so the reading from an exterior temperature sensor needs to be considered. Instead of providing a pre-set target temperature, the algorithm may be given evaluations (good / OK / cold) during the day and must learn in response to this feedback.

In addition, the algorithm can be provided with an additional rating every month based on the overall energy cost: encouraging efficient behavior and discouraging inefficient responses. A "stable" response that balances comfort and efficiency can be established, but exploration should continue to accommodate changes in behavior and the environment.

It can be seen that these three approaches are complementary. The learning method should be chosen depending on the task in hand – each has its merits.

Concrete Applications

Many diverse AI-based applications are available in the field of building automation. They can be broadly categorized as follows:

- Optimized facility management: needs-based control of heating plants, circulating pumps, lighting etc. (as opposed to control on the basis of simple parameters or by timer).
- Optimized utilization of spaces and infrastructure: capacity analysis and forecasting, e.g. for meeting rooms, canteens, pantries, transit areas, toilets and parking spaces as well as the provision of information in the short term (for building occupants) and in the long term (for facility managers, e.g. in form of advice on building restructuring).
- Load management: forward-looking operation of electrical systems in order to avoid (costly) peak loads.
- Precautionary maintenance and optimized servicing: analysis of failure probability, timely maintenance and consequential avoidance of technical failures.
- Employee-oriented value-added services: mobile devices can – for instance – be used to generate space utilization forecasts, view canteen usage intensity, request parking space availability and preferred workspace location or select individual meals.
- Compensation of skilled-staff shortages: making effective use of facility maintenance staff in managing the building's technical systems.
- Focus on meaningful sensor data: generate as much data as possible from as few sensors as possible – reducing redundancy, cutting investment and operating costs.

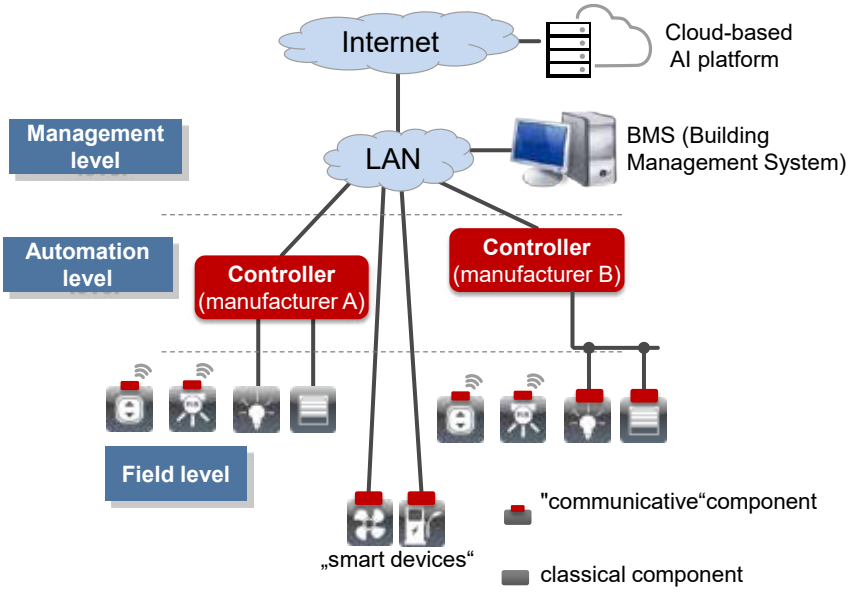


Fig. 2: linking building automation with a (cloud-based) AI platform
Abb. 2: Verbindung von Gebäudeautomation mit (cloud-basierter) AI-Plattform

Demands upon System Architecture

An AI platform is indispensable for the introduction of intelligent learning processes such as those described above. This can be either cloud-based or server-based. Cloud-based server farms offer more processing power, and cloud-based AI frameworks offer a broader range of features, so this currently represents common practice.

The AI platform is built on a Smart Building infrastructure, and all technical systems should ideally be connected to a BMS (Building Management System). The BMS must be able to govern the building facility and room automation systems.

Requirements for Building Infrastructure

AI-based processes require high computing power and are therefore best run on a dedicated AI platform. This can be cloud-based or run on a server in the company's own data center. Due to the higher computing power of cloud-based server farms and the currently greater scope of services offered by cloud-based AI frameworks, this option is shown in Fig. 2.

This figure also shows that a smart building must be in place as a basis for the use of AI-based processes. It is important that all building services in this smart building are connected to a building management system (BMS) for communication purposes. In many cases, building automation is still implemented in such a way that room-side and system-side automation are operated separately from each other as respective island systems. This must be converted into a holistically networked installation.

It must also be ensured that a BMS can also control room and system automation. In many cases, the specific behavior of, for example, room-side bus systems and system-

side controllers is hard-coded and cannot be influenced by the BMS. This ability to influence must be guaranteed, which means that all controllers and systems must be connected to each other for communication purposes. This requires a powerful and standardized TCP/IP-based protocol, with BACnet/IP and BACnet/SC being particularly suitable options.

In addition, it must be taken into account that the AI platform requires as much data as possible from a wide variety of sensors for effective operation. Wiring the required number of sensors would be very complex and expensive, especially in an existing building. Radio-based sensors are a good solution here, ideally battery-free and maintenance-free energy harvesting sensors such as those with EnOcean technology.

All of this information can then be used to create cloud-based digital twins and further improve the monitoring of activities, the working environment, augmented reality, productivity, and the health and safety of building users.

Conclusions

AI-based processes enable a broad range of applications in the field of building automation. The concrete benefits anticipated from AI-based solutions should be clearly defined before implementation, since this plays a determining role in the choice of learning process and its modelling, as well as in the choice of AI platform and the type, number and location of the energy harvesting sensors needed to supply the data inputs. ■

Moderne Gebäudeautomationssysteme arbeiten in der Regel „statisch“ – als Antwort auf feste Zeitprogramme oder einfache Steuerungsparameter. So basiert die Raumtemperaturregelung auf einer vorgegebenen Temperatur, die den ganzen Tag über konstant bleibt. Die Beleuchtung wird manuell, mit Schaltern oder auf Basis einfacher Präsenztaster betrieben. All das ist nicht wirklich „intelligent“. Die neue Perspektive, die die KI der Gebäudeautomation eröffnen kann, ist die autonome Analyse der Daten als Grundlage für einen optimierten Betrieb. So lassen sich etwa die Heiz- und Kühldynamik von Räumen, Wettervorhersagen oder erwartete Raumbelegung im Tagesverlauf in den Heizungsbetrieb miteinbeziehen.

Ebenso können sich Reinigungspläne nicht nur auf die aktuellen Ist-Werte bezüglich Nutzungsintensität von Küchen, Kantinen und Toiletten und anderen Bereichen beziehen, sondern auch auf Vorhersagen, die sich aus einer Analyse der Nutzungsmuster der vergangenen Tage und Wochen ableiten lassen. Dieses zukunftsorientierte Gebäudemanagement lässt sich in fast allen Bereichen der Gebäudetechnik anwenden. Es verbessert die Energieeffizienz sowie Raumnutzung und senkt Betriebskosten.

All dies – und noch viel mehr – ist möglich, wenn Daten über Zustand und Beschaffenheit des Gebäudesystems intelligent ausgewertet werden. Dies erfordert eine umfangreiche Verarbeitung großer Datenmengen, wobei viele Variablen berücksichtigt werden müssen. Künstliche Intelligenz (KI) schafft die Grundlage für innovative, maßgeschneiderte Lösungen, die sich hervor- ragend für ein effizientes Gebäudemanagement eignen.

„Gebäudeautomation“, „Smart Building“ und „Cognitive Building”

Anfänglich war „Gebäudeautomation“ vergleichsweise „unintelligent“. Die Systeme waren so programmiert, dass sie einfachen Regeln folgten, die eine schnelle Inbetriebnahme und später eine einfache Wartung ermöglichten.

Das „Intelligente Gebäude“ („Smart Building“) baut typischerweise auf dieser klassischen Gebäudeautomation mit IT-basierten Managementsystemen auf. Diese bieten eine flexible Programmierung unter Verwendung moderner IT-Sprachen und -Werkzeuge, eine einfache Integration in andere IT-Systeme wie Arbeitsplatz- bzw. Raumreservierungssysteme oder Datenbanken sowie eine Datenvisualisierung für Facility-Manager und „normale“ Benutzer.

Die zunehmende Einbindung sensorgenerierter Daten in die IT-basierte Steuerungsebene öffnet den Weg für fortschrittlichere Datenverarbeitungslösungen – wie z.B. KI-Tools. Dies wiederum schafft die Voraussetzung für die Implementierung jeder prognosegestützten Form von Gebäudemanagement. Die ausgeklügelte Verarbeitung sensorgenerierter Daten macht das intelligente zu einem „kognitiven Gebäude“. (Abb. 1)

KI-Lernprozess

Der erste Schritt in jedem KI-Prozess ist das Systemlernen. Dies kann drei Formen annehmen.

- Unbeaufsichtigtes Lernen
- Beaufsichtigtes Lernen
- Verstärkendes Lernen

„Unbeaufsichtigtes Lernen“ kommt zum Einsatz, wenn große Datenmengen verarbeitet und gruppiert werden müssen. Diese Gruppierung ermöglicht es, Abweichungen von Normen und Abhängigkeiten zu erkennen. Beispielsweise lassen sich Sensordaten identischer Umwälzpumpen zusammenfassen. Weichen die Daten einer bestimmten Pumpe oder Pumpengruppe von der Norm ab, kann ein Defekt vorliegen. In diesem Falle muss ein Techniker zur Überprüfung herangezogen werden.

Beim „Beaufsichtigten Lernen“ kommen häufig neuronale Netze zum Einsatz. Sie bestehen aus Eingangs- und Ausgangsknoten sowie weiteren Knoten in den Zwischenschichten. Zwischen den verschiedenen Knoten (Neuronen) bestehen mathematisch gewichtete Beziehungen. Um diese Beziehungen zu optimieren, wird das neuronale Netz einer Trainingsphase mit bekannten Ein- und Ausgangsmustern unterzogen. Im Bereich der Gebäudeautomation kann ein neuronales Netz z.B. „lernen“, welche Stromverbrauchsprofile verschiedene Geräte haben und welche Geräte wann aktiv sind. Diese Informationen lassen sich zum Vermeiden von „Spitzen“ im Energieverbrauch von Gebäuden nutzen, indem einige Geräte abgeschaltet und die Betriebszeit an- derer verlängert wird.

Eine weitere Form künstlicher Intelligenz stellen Prozesse dar, die selbstständig bestimmen, welche Handlungen in einer gegebenen Situation angemessen sind. Sie ahmen menschliches Verhalten nach, wobei verschiedene Lösungen ausprobiert werden, um in einer bisher unbekannten Situation den besten Lösungsansatz zu ermitteln und im Nachhinein Schlussfolgerun- gen zu ziehen. Die Lernaufgabe wird umso herausfordernder, je später das Feedback erfolgt und je weiter die Referenzereignisse zurückliegen. Dies gilt für den Menschen ebenso wie für den Computer.

Das bekannteste Beispiel in dieser Kategorie ist „Verstärkungslernen“. Man denke zum Beispiel an die Bestimmung der optimalen Start- und Stoppzeiten der Heizung, um bei der Öffnung des Gebäudes eine möglichst angenehme Temperatur zu gewährleisten. Auf der einfachsten Ebene erhält der Lernalgorithmus den Wert vom Raumtemperatursensor und kann auf den Heizkörperregler zugreifen. Durch einen Trial and Error-Prozess kann der Algorithmus die notwendige Vorlaufzeit ermitteln. Dieses einfache Beispiel blendet jedoch die Tatsache aus, dass z.B. die Aufheizgeschwindigkeit auch von der Außentemperatur abhängt. Deshalb muss der Messwert eines Außentemperatursensors ebenfalls Berücksichtigung finden. Anstatt eine voreingestellte Zieltemperatur zu erzeugen, kann der Algorithmus im Tagesverlauf Auswertungen erhalten (gut / OK / kalt). Das Lernen erfolgt dann als Rückmeldung daraus.

Darüber hinaus kann der Algorithmus eine zusätzliche Monatsauswertung auf Grundlage der Gesamtenergiekosten erhalten: Förderung effizienten Verhaltens und Vermeidung ineffizienter Rückkopplung. So lässt sich eine „stabile" Reaktion ermitteln, die Komfort und Effizienz ausgleicht. Zugleich sollte die Exploration weitergehen, um Änderungen im Verhalten und in der Umwelt zu berücksichtigen.

Fazit: Die drei Ansätze ergänzen sich. Welche Lernmethode am besten passt, hängt von der jeweiligen Aufgabe ab. Jede hat ihre Vorzüge.

Konkrete Anwendungsfelder

Für die Gebäudeautomatisierung sind viele verschiedene KI-basierte Anwendungen verfügbar. Sie lassen sich grob wie folgt unterteilen:

- Optimiertes Gebäudemanagement: bedarfsgerechte Steuerung von Heizungsanlagen, Um- wälzpumpen, Beleuchtung usw. (im Gegensatz zur Steuerung auf Basis einfacher Parameter oder durch Zeitschaltuhr).
- Optimierte Nutzung von Räumen und Infrastruktur: Kapazitätsanalyse und -prognose, z.B. für Besprechungsräume, Kantinen, Durchgangsbereiche, Toiletten und Parkplätze sowie die kurzfristige (für Gebäudenutzer) und langfristige (für Facility Manager, z.B. in Form von Beratung bei Gebäudesanierungen) Bereitstellung von Informationen.
- Lastmanagement: Vorausschauender Betrieb der elektrischen Anlagen zur Vermeidung von (kostspieligen) Lastspitzen.
- Vorbeugende Instandhaltung und optimierte Wartung: Analyse der Ausfallwahrscheinlichkeit, rechtzeitige Wartung und konsequente Vermeidung technischer Ausfälle.
- Mitarbeiterorientierte Mehrwertdienste: Mit mobilen Geräten können z.B. Raumnutzungsprognosen erstellt, die Nutzungsintensität von Kantinen eingesehen oder die Parkplatzverfügbarkeit abgefragt werden.
- Kompensation von Fachkräftemangel: Effektiver Einsatz von Wartungspersonal bei der Verwaltung der technischen Gebäude-Systeme.
- Konzentration auf aussagekräftige Sensordaten: Möglichst große Datenmengen werden mit möglichst wenigen Sensoren gesammelt. Das reduziert Redundanzen, senkt Investitions- und Betriebskosten.

Anforderungen an die Systemarchitektur

Zur Einführung intelligenter Lernprozesse wie oben beschrieben ist eine KI-Plattform unverzichtbar. Diese kann cloud- oder serverbasiert sein. Cloud-basierte Serverfarmen bieten mehr Rechenleistung, während Cloud-basierte KI-Frameworks ein breiteres Spektrum an Funktionen aufweisen, so dass dies derzeit gängige Praxis ist.

Die KI-Plattform baut auf einer Smart Building Infrastruktur auf. Die technischen Systeme sollten idealerweise mit einem BMS (Building Management System) verbunden sein. Das BMS muss die Gebäude- und Raumautomationssysteme steuern können.

Anforderungen an Gebäudeinfrastruktur

KI-basierte Verfahren benötigen eine hohe Rechenleistung und somit werden diese sinnvollerweise auf einer eigenen KI-Plattform betrieben. Diese kann sowohl cloud-basiert als auch auf einem Server im eigenen Rechenzentrum zur Ausführung kommen. Aufgrund der höheren Rechenleistung cloud-basierter Serverfarmen und des derzeit größeren Leistungsumfangs von cloud-basierten KI-Frameworks, ist diese Variante in der Abbildung 2 dargestellt.

Aus dieser Abbildung geht ebenso hervor, dass zur Nutzung von KI-basierten Verfahren ein Smart Building als Grundlage vorhanden sein muss. Wichtig ist dabei, dass bei diesem Smart Building möglichst alle Gewerke kommunikativ an ein BMS (Building Management System) angeschlossen sind. In vielen Fällen wird die Gebäudeautomation noch so ausgeführt, dass die raumseitige und die anlagenseitige Automation separat voneinander als jeweiliges Inselsystem betrieben wird. Dies ist in eine ganzheitlich vernetzte Installation zu überführen.

Ebenso muss gewährleistet werden, dass ein BMS auch steuernd auf die raum- und anlagenseitige Automation einwirken kann. In vielen Fällen wird das konkrete Verhalten von z.B. raumseitigen Bus-Systemen und anlagenseitigen Controllern fest programmiert und ist vom BMS nicht beeinflussbar. Diese Einflussmöglichkeit muss gewährleistet sein und somit müssen alle Controller und Gewerke kommunikativ miteinander verbunden sein. Dies erfordert zum einen ein leistungsfähiges und standardisiertes TCP/IP-basiertes Protokoll; wobei sich hier BACnet/IP und BACnet/SC in besonderem Maß anbieten.

Ergänzend muss berücksichtigt werden, dass die KI-Plattform für ihren effektiven Betrieb möglichst viele Datenmengen verschiedenster Sensoren benötigt. Die Verkabelung dieser benötigten Anzahl von Sensoren wäre sehr aufwendig und teuer – insbesondere in einem bestehenden Gebäude. Hier bieten sich funkbasierte Sensoren an und idealerweise batterie- und wartungsfreie Energy-Harvesting-Sensoren wie z.B. solche mit EnOcean-Technologie.

In Summe lassen sich diese Informationen dann verwenden, um cloud-basierte digitale Zwillinge („Digital Twins") zu erstellen und das Monitoring von Aktivitäten, Arbeitsumgebung, Augmented Reality, Produktivität sowie Gesundheit und Sicherheit der Gebäudenutzer weiter zu verbessern.

Fazit

KI-basierte Prozesse ermöglichen ein breites Spektrum von Anwendungen im Bereich der Gebäudeautomation. Die konkreten Vorteile, die von KI-basierten Lösungen erwartet werden, sollten vor der Implementierung klar definiert werden. Dies nämlich spielt eine entscheidende Rolle bei der Wahl des Lernprozesses und seiner Modellierung sowie der Wahl der KI-Plattform bzw. Art, Anzahl und Lage der zur Datensammlung benötigten Energy-Harvesting-Sensoren.

Prof. Dr. Michael Krödel
Professor für Gebäudeautomation und -technologie
bei der Technischen Hochschule Rosenheim
michael.kroedel@th-rosenheim.de | www.th-rosenheim.de

Graham Martin
Chairman & CEO | EnOcean Alliance
graham.martin@enocean.com | www.enocean-alliance.org

Study Building Automation with BACnet Expertise: Mainz University of Applied Sciences is a Pioneer in Networked Building Technology

Gebäudeautomation mit BACnet-Kompetenz studieren: Hochschule Mainz als Vorreiter für vernetzte Gebäudetechnik

What does it take to shape the future of building automation? A solid engineering education, a strong practical focus, and a deep understanding of standards such as BACnet. Mainz University of Applied Sciences combines all of this in its range of courses. The focus is not only on technology, but also on its implementation in digital and sustainable building operations.

Was braucht es, um die Zukunft der Gebäudeautomation erfolgreich zu gestalten? Eine fundierte ingenieurwissenschaftliche Ausbildung, ein ausgeprägter Praxisbezug – und ein tiefes Verständnis für Standards wie BACnet. All das vereint die Hochschule Mainz – University of Applied Sciences – in ihrem Studienangebot. Im Fokus steht dabei nicht nur die Technik, sondern auch deren Umsetzung im digitalen und nachhaltigen Gebäudebetrieb.

A Training Center with Vision: Mainz University of Applied Sciences

Mainz University of Applied Sciences, located in Rhineland-Palatinate, is one of Germany's renowned technical universities when it comes to practice-oriented education in the fields of construction, environmental technology, and real estate management. The Technology department, located at Holzstraße 36 in the heart of Mainz, offers degree programs that focus intensively on building automation, technical building equipment (TGA), energy efficiency, and digital building management.

Specifically, the focus is on the following study programs:

- Construction and Real Estate Management / Facilities Management (B.Eng.)
- Technical Real Estate Management (B.Eng., dual)
- Construction and Real Estate Management / Facilities Management (M.Eng./M.Sc.)
- Technical Real Estate Management (M.Eng.)

These degree programs combine classic engineering disciplines with business content and place a clear emphasis on digitalization, sustainability, and smart technologies.

Building Automation at the Heart of the Curriculum

In the programs mentioned above, building automation is not just one module among many, but an integral part of the curriculum. In the modules "Technical Building Equipment," "Measurement, Control, and Regulation Technology," and "Building Automation," students acquire in-depth knowledge about the planning, implementation, and optimization of technical systems in buildings. This content is supplemented by aspects such as digital building management (BIM, IoT), energy and sustainability concepts, and legal and economic fundamentals.

Special attention is paid to practical application: in laboratories, practical projects, and a specially equipped real-world laboratory – the Smart Building Real-World Laboratory – students work directly with real systems and BACnet-based systems. This enables a deep understanding of the interfaces between sensor technology, actuator technology, and communication technologies – a skill that is increasingly in demand in the modern TGA industry.

Practice-Integrated and Future-Oriented –Dual and Part-Time Options

The dual degree program in Technical Real Estate Management stands out thanks to its close ties between the university and companies. Every year, around 20 to 30 students enroll in this practice-integrated program. The full-time Construction and Real Estate Management program has around 60 to 80 new enrollments per year. Both study formats provide targeted preparation for careers at the interface between technology, management, and digitalization.

The university also offers part-time master's programs that enable students to gain further qualifications after their initial degree, for example in the areas of sustainability, digital facility management, or energy management.

BACnet as a Key Competence in the Real-World Laboratory

BACnet plays a central role in the program. The international communication standard is not only taught in theory, but also actively used in the real-world laboratory. Students analyze BACnet communication processes, parameterize devices, interpret data points, and implement small automation solutions. The university works together with partners who themselves use BACnet-based systems, including public institutions, service providers, and manufacturers of building automation solutions.

This practical approach makes it possible to combine theory and reality – an aspect that is very well received by both students and industry. Many theses and practical projects are developed directly in cooperation with companies from the industry.

HOCHSCHULE MAINZ

Mainz University of Applied Sciences campus
Campus Hochschule Mainz

Requirements and Target Group: Who should apply?

The university's programs are aimed at young people who are enthusiastic about technology, digitalization, energy efficiency, and real estate management. Applicants are expected to have a good basic understanding of natural sciences – especially mathematics, physics, and computer science – as well as a willingness to think in an interdisciplinary manner and work in a practice-oriented way. Creative, logical thinking is expressly encouraged, as the solutions of the future require the combination of a wide variety of perspectives.

Expert forums at Mainz University of Applied Sciences – Platforms for Interdisciplinary Exchange

Mainz University of Applied Sciences regularly organizes specialist forums that promote exchange between research, teaching, and practice. In collaboration with partners from industry, professional associations, and other universities, current topics from areas such as digitalization, sustainability, design, and technological innovation are addressed. Workshops, lectures, and practical formats such as live demonstrations provide lively access to complex issues.

One example of this is the BACtwin Forum 2025, which will take place on October 28, 2025, in the LUX Pavilion at Mainz University of Applied Sciences. In the field of architecture, technology, and interdisciplinarity (ATI), this forum is dedicated to the tangible "digital twin" in the context of buildings. Here, interested parties from research, planning, and operations meet with manufacturers, experts, and representatives of associations such as AMEV and GEFMA to exchange ideas on current developments relating to BACnet, digital twins, and BACtwin – an ideal example of a successful networking event with technical depth and practical inspiration.

International Perspectives and Career Opportunities

Graduates of Mainz University of Applied Sciences are in high demand internationally – whether in planning offices, operating companies, public building authorities, or technical consulting. Around 30–40% of alumni from the Technical Real Estate Management program work directly in building automation, energy management, or smart building.

The university is particularly attractive to students with international interests: the International Office offers a choice of more than 150 partner universities worldwide, from Europe to North America and Asia. Internships, exchange programs, and joint research projects promote international networking and provide optimal preparation for globalized job markets.

Commitment to Young Talent – Cooperation with BIG-EU

Mainz University of Applied Sciences is actively committed to promoting young talent in the industry. In cooperation with associations such as the BACnet Interest Group Europe (BIG-EU), it sees great opportunities to bring young people into contact with real-world applications and networks at an early stage. Formats such as guest lectures, excursions, specialist workshops, and joint exchanges at events such as the BACtwin Forum are expressly encouraged and supported by the university.

Conclusion: Learn About the Future of Building Automation in Mainz

With its interdisciplinary approach, clear practical relevance, and anchoring of modern automation

standards such as BACnet, Mainz University of Applied Sciences offers a strong foundation for a career in intelligent building technology. Anyone who wants to design technology, operate buildings sustainably, and experience digitalization in a practical way will find the ideal starting point here – with real projects, reliable partners, and internationally transferable skills.

Eine Ausbildungsstätte mit Weitblick: Hochschule Mainz

Die Hochschule Mainz mit Sitz in Rheinland-Pfalz gehört zu den renommierten technischen Hochschulen Deutschlands, wenn es um die praxisorientierte Ausbildung in den Bereichen Bauwesen, Umwelttechnik und Immobilienmanagement geht. Im Fachbereich Technik, angesiedelt an der Holzstraße 36 im Herzen von Mainz, werden Studiengänge angeboten, die sich intensiv mit Gebäudeautomation, technischer Gebäudeausrüstung (TGA), Energieeffizienz und digitalem Gebäudemanagement befassen.

Konkret stehen folgende Studienprogramme im Fokus:

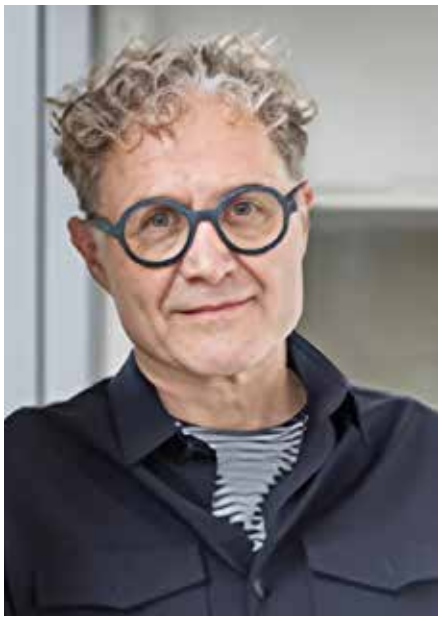
- Bau- und Immobilienmanagement / Facilities Management (B.Eng.)
- Technisches Immobilienmanagement (B.Eng., dual)
- Bau- und Immobilienmanagement / Facilities Management (M.Eng. / M.Sc.)
- Technisches Immobilienmanagement (M.Sc. /M.Eng.)

Diese Studiengänge verknüpfen klassische Ingenieurdisziplinen mit betriebswirtschaftlichen Inhalten und legen gleichzeitig einen klaren Schwerpunkt auf Digitalisierung, Nachhaltigkeit und smarte Technologien.

Gebäudeautomation im Fokus des Curriculums

In den genannten Programmen ist die Gebäudeautomation nicht nur ein Modul unter vielen, sondern ein integraler Bestandteil. In den Modulen „Technische Gebäudeausrüstung“, „Mess-, Steuer- und Regelungstechnik“ und „Gebäudeautomation“ erwerben die Studierenden fundiertes Wissen über die Planung, Umsetzung und Optimierung technischer Systeme im Gebäude. Ergänzt werden diese Inhalte durch Aspekte wie digitales Gebäudemanagement (BIM, IoT), Energie- und Nachhaltigkeitskonzepte sowie rechtliche und wirtschaftliche Grundlagen.

Ein besonderes Augenmerk gilt der praktischen Anwendung: In Laboren, Praxisprojekten und



Prof. Thomas Giel
Head of the degree program, Department of Technology, Construction and Environment, Professor of Sustainable Building Energy Systems. © Melanie Billian
Studiengangsleitung, Fachbereich Technik, Fachrichtung Bau und Umwelt, Professor für Professur für nachhaltige Gebäudeenergiesysteme. © Melanie Billian

einem eigens eingerichteten Reallabor – dem Smart Building Reallabor – arbeiten die Studierenden direkt mit realen Anlagen und BACnet-basierten Systemen. Das ermöglicht ein tiefes Verständnis der Schnittstellen zwischen Sensorik, Aktorik und Kommunikationstechnologien – eine Fähigkeit, die in der modernen TGA-Branche zunehmend gefragt ist.

Praxisintegriert und zukunftsorientiert – duale und berufsbegleitende Optionen

Der duale Studiengang Technisches Immobilienmanagement hebt sich durch die enge Verzahnung von Hochschule und Unternehmen hervor. Jährlich schreiben sich etwa 20 bis 30 Studierende in diesen praxisintegrierten Studiengang ein. Der Vollzeit-Studiengang Bau- und Immobilienmanagement verzeichnet rund 60 bis 80 Neueinschreibungen pro Jahr. Beide Studienformate bereiten gezielt auf Tätigkeiten an der Schnittstelle zwischen Technik, Management und Digitalisierung vor.

Die Hochschule bietet darüber hinaus berufsbegleitende Master-Programme an, die es ermöglichen, sich nach einem ersten Abschluss gezielt weiter zu qualifizieren – etwa in den Bereichen Nachhaltigkeit, digitales Facility Management oder Energiemanagement.

BACnet als eine Schlüsselkompetenz im Reallabor

BACnet spielt in der Ausbildung eine wichtige Rolle. Der internationale Kommunikationsstandard wird nicht nur theoretisch vermittelt, sondern auch aktiv im Reallabor eingesetzt. Die Studierenden analysieren zukünftig BACnet-Kommunikationsverläufe, parametrieren Geräte, interpretieren Datenpunkte und setzen kleine Automationslösungen um. Die Hochschule arbeitet hierbei mit Partnern zusammen, die selbst BACnet-basierte Systeme nutzen – darunter öffentliche Einrichtungen, Dienstleister und Hersteller von Gebäudeautomationslösungen

Dieser praxisorientierte Ansatz ermöglicht es, Theorie und Praxis miteinander zu verbinden – ein Aspekt, der sowohl bei Studierenden als auch in der Industrie sehr gut ankommt. Viele Abschlussarbeiten und Praxisprojekte werden direkt in Zusammenarbeit mit Unternehmen aus der Industrie entwickelt.

Anforderungen und Zielgruppe: Wer sollte sich bewerben?

Die Hochschule richtet sich mit ihrem Angebot an junge Menschen, die sich für Technik, Digitalisierung, Energieeffizienz und Immobilienbetrieb begeistern. Erwartet werden ein gutes naturwissenschaftliches Grundverständnis – insbesondere in Mathematik, Physik und Informatik – sowie die Bereitschaft, interdisziplinär zu denken und praxisorientiert zu arbeiten. Kreatives, logisches Denken wird ausdrücklich gefördert, denn die Lösungen der Zukunft erfordern das Zusammenführen unterschiedlichster Perspektiven.

Fachforen an der Hochschule Mainz – Plattformen für interdisziplinären Austausch

Die Hochschule Mainz richtet regelmäßig Fachforen aus, die den Austausch zwischen Forschung, Lehre und Praxis fördern. In Zusammenarbeit mit Partnern aus Industrie, Fachverbänden und anderen Hochschulen werden aktuelle Themen aus Bereichen wie Digitalisierung, Nachhaltigkeit, Gestaltung und technologischer Innovation aufgegriffen. Workshops, Vorträge und praxisnahe Formate wie Live-Demonstrationen ermöglichen einen lebendigen Zugang zu komplexen Fragestellungen.

Ein Beispiel hierfür ist das BACtwin Forum 2025, das am 28. Oktober 2025 im LUX-Pavillon der Hochschule Mainz stattfindet. Im Bereich Architektur, Technik und Interdisziplinarität (ATI) widmet sich dieses Forum dem erlebbaren „Digi-

talen Zwilling“ im Gebäudekontext. Hier treffen sich Interessierte aus Forschung, Planung und Betrieb mit Herstellern, Fachleuten und Vertretern von Verbänden wie AMEV und GEFMA, um sich zu aktuellen Entwicklungen rund um BACnet, digitale Zwillinge und BACtwin auszutauschen – ein ideales Beispiel für ein gelungenes Networking-Event mit fachlicher Tiefe und praxisnahen Impulsen.

Internationale Perspektiven und Karrierechancen

Absolvent:innen der Hochschule Mainz sind international gefragt – sei es in Planungsbüros, bei Betreibergesellschaften, öffentlichen Bauverwaltungen oder im technischen Consulting. Rund 30–40 % der Alumni des Studiengangs Technisches Immobilienmanagement arbeiten direkt in der Gebäudeautomation, im Energiemanagement oder im Bereich Smart Building.

Besonders attraktiv ist die Hochschule für Studierende mit internationalem Interesse: Über das International Office stehen mehr als 150 Partnerhochschulen weltweit zur Auswahl – von Europa über Nordamerika bis Asien. Praktika, Austauschprogramme und gemeinsame Forschungsprojekte fördern die internationale Vernetzung und bereiten optimal auf globalisierte Berufsmärkte vor.

Engagement für den Nachwuchs – Zusammenarbeit mit der BIG-EU

Die Hochschule Mainz engagiert sich aktiv für den Branchennachwuchs. In der Zusammenarbeit mit Verbänden wie der BACnet Interest Group Europe (BIG-EU) sieht sie große Chancen, junge Menschen frühzeitig mit realen Anwendungen und Netzwerken in Berührung zu bringen. Formate wie Gastvorträge, Exkursionen, Fachworkshops oder der gemeinsame Austausch im Rahmen von Events wie dem BACtwin Forum sind ausdrücklich erwünscht und werden seitens der Hochschule unterstützt.

Fazit: In Mainz die Zukunft der Gebäudeautomation erlernen

Mit ihrer interdisziplinären Ausrichtung, dem klaren Praxisbezug und der Verankerung moderner Automationsstandards wie BACnet bietet die Hochschule Mainz ein starkes Fundament für eine Karriere in der intelligenten Gebäudetechnik. Wer Technik gestalten, Gebäude nachhaltig betreiben und Digitalisierung praxisnah erleben will, findet hier den idealen Einstieg – mit realen Projekten, verlässlichen Partnern und international anschlussfähigen Kompetenzen. ■

Energy-Efficient Room Automation with Artificial Intelligence

Energieeffiziente Raumautomation mit Künstlicher Intelligenz planen

The AI assistant AUTERAS saves time, prevents human errors, and facilitates compliance with regulatory requirements.
Der KI-Assistent AUTERAS spart Arbeitszeit, vermeidet menschliche Fehler und erleichtert die Einhaltung gesetzlicher Vorgaben.

Since the German Building Energy Act (GEG) and the European Energy Performance of Buildings Directive (EPBD) set minimum requirements for building automation, these cannot be delegated to the later appointed specialist planner. At least their principles must be defined very early on (Phase 1 of the HOAI). The AI assistant www.AUTERAS.de provides a simple tool that also includes architects and homeowners.

The starting point can be existing room books or BIM models from architects, which can be uploaded to the tool.

Then, the assistant conducts an interview (Figure 1), in which the users primarily communicate their functional wishes for each room for all trades. During the interview, the assistant already develops suitable automation concepts in the background, which are based on standard functions of ISO 16484-4 (or EN 17609) and are therefore still neutral with regard to technology or manufacturer. They allow, however, the assignment to an energy efficiency class according to ISO 52120 (or EN 15232) and thus, via DIN V 18599, to the regulatory requirements of GEG and EPBD. Although these standard functions are only processed within the assistant and the user does not necessarily need them for his design, they can be downloaded on request, for example, to document them according to the new German BIM room book guideline VDI 6070. They can also be used as a basis for functional descriptions in later tender texts.

To better explain these intermediate results, the assistant provides explanatory videos for all functions, which can also be understood by homeowners.

In the course of the detailed design, the programming of the automation software could follow, which is increasingly taken over worldwide by generative AI. AUTERAS also takes a similar path with the software components, which are encapsulated in devices of room automation (KNX) or BACnet room controllers. The AI selects for each room combinations of components from a library (catalog) that together meet all customer wishes and are interoperable at their interfaces (Figure 2). Due to the requirement for compatibility, partial solutions must be frequently rejected during the search, which leads to numerous iterations and makes the solution of a puzzle similar. Humans are quickly overwhelmed, while the AI finds good results.

Figure 1: Part of an interview: AUTERAS asks about wishes regarding heating and cooling. At the same time, the energy efficiency class is calculated (here C, marked in red).
Bild 1: Teil eines Interviews: AUTERAS fragt nach den Wünschen bezüglich Heizen und Kühlen. Gleichzeitig wird die Energieeffizienzklasse berechnet (hier C, rot markiert).

Since the KNX technology has a uniform tool (ETS), the BIM building structure (floors, rooms), all device combinations, as well as their software configuration and networking can be uploaded to this ETS. They are then ready for commissioning on the construction site.

The tool is available in a free version and was awarded the “Electrifying Ideas Award” 2025

Figure 2: One of several design proposals by the AI (hardware and software) for export to subsequent tools
Bild 2: Einer von mehreren Entwurfsvorschlägen der KI (Hardware und Software) zum Export in nachfolgende Tools

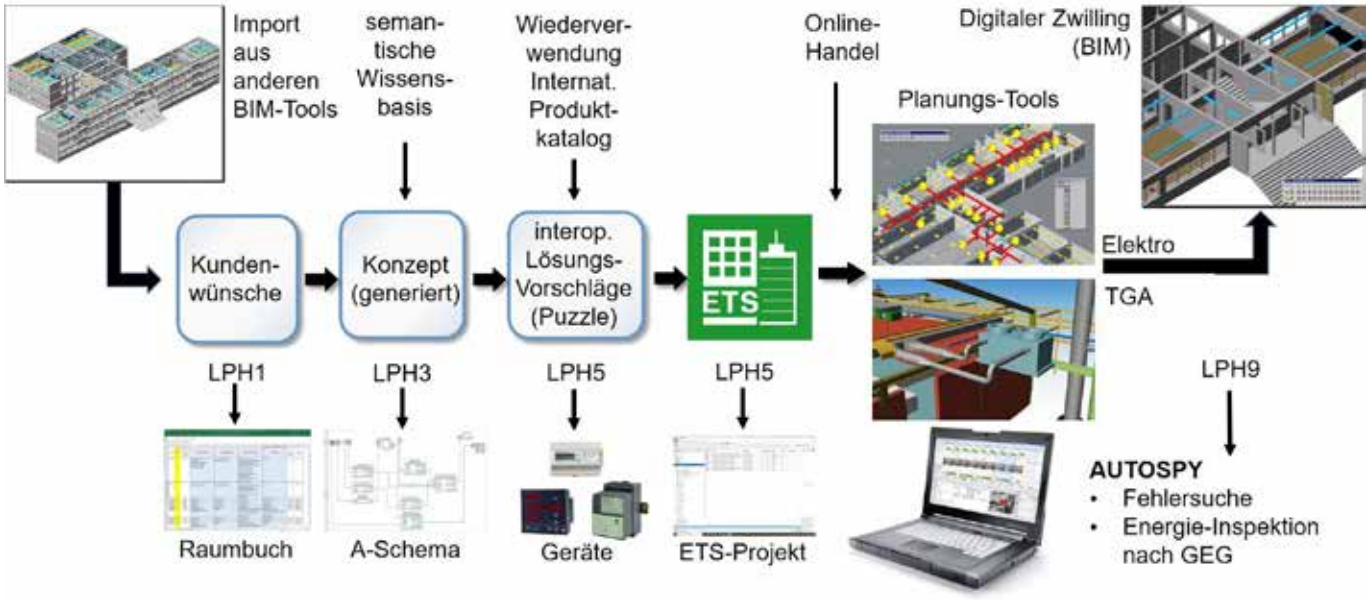


Figure 3: Tool workflow from BIM (left) to the construction site (right). The three blue boxes in the middle belong to AUTERAS.
Bild 3: Tool-Workflow vom BIM (links) bis zur Baustelle (rechts). Zu AUTERAS gehören die drei blauen Boxen in der Mitte.

by the German Association of the Electrical and Digital Industry (ZVEI) as well as "best project" by the "Smart Home Initiative Germany". Technical details and videos can also be found under https://serviceflow.ga-entwurf.de/ ■

Seit das Gebäudeenergiegesetz GEG (deutsch) bzw. die Energy Performance of Buildings Directive EPBD (europäisch) Mindestanforderungen an die Gebäudeautomation stellen, kann man sie nicht mehr an den später beauftragten Fachplaner delegieren. Zumindest deren Grundsätze müssen bereits sehr früh (Leistungsphase 1 nach HOAI) definiert werden. Der KI-Assistent www.AUTERAS.de bietet dazu einfache Hilfsmittel, die auch Architekten und Bauherren einbeziehen.

Ausgangspunkt können bereits vorhandene Raumbücher oder BIM-Modelle der Architekten sein, die in das Tool hochgeladen werden.

Dann führt der Assistent ein Interview (Bild 1), in dessen Dialog die Nutzer ihm vor allem ihre funktionalen Wünsche an jeden Raum für alle Gewerke mitteilen. Während des Dialogs entwickelt der Assistent im Hintergrund bereits passende Automatisierungskonzepte. Sie beruhen auf Standardfunktionen der ISO 16484-4 (bzw. EN 17609), sind also noch neutral bezüglich Technologie oder Fabrikat. Sie erlauben aber schon die Zuordnung zu einer Energieeffizienzklasse nach ISO 52120 (bzw. EN 15232) und damit über den Umweg DIN V 18599 auch zu den gesetzlichen Forderungen nach GEG bzw. EPBD. Obwohl diese Standardfunktionen nur innerhalb des Assistenten verarbeitet werden und der Nutzer sie für seinen Entwurf nicht unbedingt braucht, werden sie auf Wunsch als Download ausgegeben, wenn er sie z. B. nach der neuen BIM-Raumbuch-Richtlinie VDI 6070 dokumentieren möchte. Sie können auch als Basis für Funktionsbeschreibungen in späteren Ausschreibungstexten genutzt werden.

Zur besseren Erläuterung dieser Zwischenergebnisse bietet der Assistent für alle Funktionen Erklärvideos an, die auch Bauherren verstehen können.

Im Zuge der Ausführungsplanung könnte nun die Programmiereng der Automatisierungssoftware folgen, die weltweit zunehmend durch generative KI übernommen wird. Einen ähnlichen Weg geht auch AUTERAS mit den Softwarebausteinen, die z. B. in Geräten der Raumautomation (KNX) oder BACnet-Raumcontrollern gekapselt sind. Die KI wählt für jeden Raum aus einer Bibliothek (Katalog) Kombinationen von Komponenten aus, die gemeinsam alle geforderten Kundenwünsche erfüllen und an ihren Schnittstellen interoperabel zusammenpassen (Bild 2). Durch diese Forderung nach Passfähigkeit müssen bei der Suche ständig Teillösungen verworfen werden, was zu zahlreichen Iterationen führt ist und der Lösung eines Puzzles ähnelt. Menschen sind dadurch schnell überfordert, während die KI gute Ergebnisse findet.

Da die KNX-Technologie über ein einheitliches Tool (ETS) verfügt, können die BIM-Gebäudestruktur (Etagen, Räume), alle Gerätekombinationen sowie ihre Softwarekonfiguration und Vernetzung in diese ETS hochgeladen werden. Sie stehen danach zur Inbetriebnahme auf der Baustelle bereit.

Das Tool ist in einer kostenlosen Version nutzbar und wurde mit dem „Electrifying Ideas Award" 2025 des deutschen Verbandes der Elektro- und Digitalindustrie (ZVEI) sowie als „bestes Projekt" von der „Smart Home Initiative Deutschland" ausgezeichnet. Technische Details und Videos findet man auch unter https://serviceflow.ga-entwurf.de ■

TECHNISCHE UNIVERSITÄT DRESDEN
Fakultät Informatik

Prof. Dr.-Ing. habil. Klaus Kabitzsch
(TIS), Institut für Angewandte Informatik (IAI)
der Fakultät Informatik, TU Dresden
klaus.kabitzsch@tu-dresden.de
www.auteras.de

Digital Efficiency with BACtwin – from Concept to Operation

Digitale Effizienz mit dem BACtwin – von der Idee bis zum Betrieb

The AMEV BACtwin templates provide a standardized digital twin for building automation in the Eplan Platform 2026. BACtwin is based on a structured BACnet data model and forms a consistent information framework – from planning and execution to technical operation.
Mit den AMEV-BACtwin-Vorlagen steht in der Eplan Plattform 2026 ein standardisierter, digitaler Zwilling für die Gebäudeautomation zur Verfügung. Der BACtwin basiert auf einem strukturierten BACnet-Datenmodell und bildet ein durchgängiges Informationsgerüst – von der Planung über die Ausführung bis hin zum technischen Betrieb.

The Eplan platform enables a model-based planning process based on BACtwin, taking into account the planning guidelines and standards in accordance with VDI 3814 and DIN EN ISO 16484.

BACtwin Implementation

With the release of the Eplan platform 2026 (Sept. 2025) and the industry-specific Industry Package Building Automation, new building automation templates – known as segment templates and macros – have been made available. This means that the current AMEV BACtwin 2025 (libraries 1–3) is implemented and can be used directly in engineering.

Segment templates contain all the necessary technical information on sensors, actuators, devices, units, systems, or system components – including the associated objects and functions. They support standardized, automated planning, documentation, and evaluation

The segment templates are structured according to the BACtwin model and form so-called structure segments, which are used for project structuring (e.g., building, system, subsystem, assembly) and their structure identification. Special segment templates for units, functions, and planning objects are available for detailed system planning. To ensure clear classification of these versatile segment templates, objects are structured and classified in accordance with IEC 62424 and DIN EN 81346. See Figure 1.

Pre-designed segment templates at the PLT station level (templates for measuring and consumer stations) already contain the finished BACtwin unit templates. See Figure 2.

At the functional level, segment templates of the PLT station functions contain the AMEV BACtwin object templates.

Ready-Made Planning Data – Pre-Assigned Value Sets for Property Sets

All properties for evaluating the BA functions and for documentation are pre-assigned with predefined value sets from AMEV BACtwin and in accordance with VDI 3814 / DIN EN ISO 16484. These can be used directly by the BA specialist planner or adapted to operator requirements if necessary. See Figure 3.

The Engineering Workflow Macro Planning

Macros for aggregates from the areas of sensor technology, actuator technology, and devices are available in the macro project. These can be used to configure assemblies and complete systems. The preconfigured segment templates are stored in the background of these macros or can be selected during placement in the diagram using value set queries. See Figure 4.

Data for All Participants

Another advantage in the engineering process is the provision and use of consistent data for downstream processes such as switchgear planning and the transfer of function data and PLC information for hardware configuration and software programming. All relevant planning

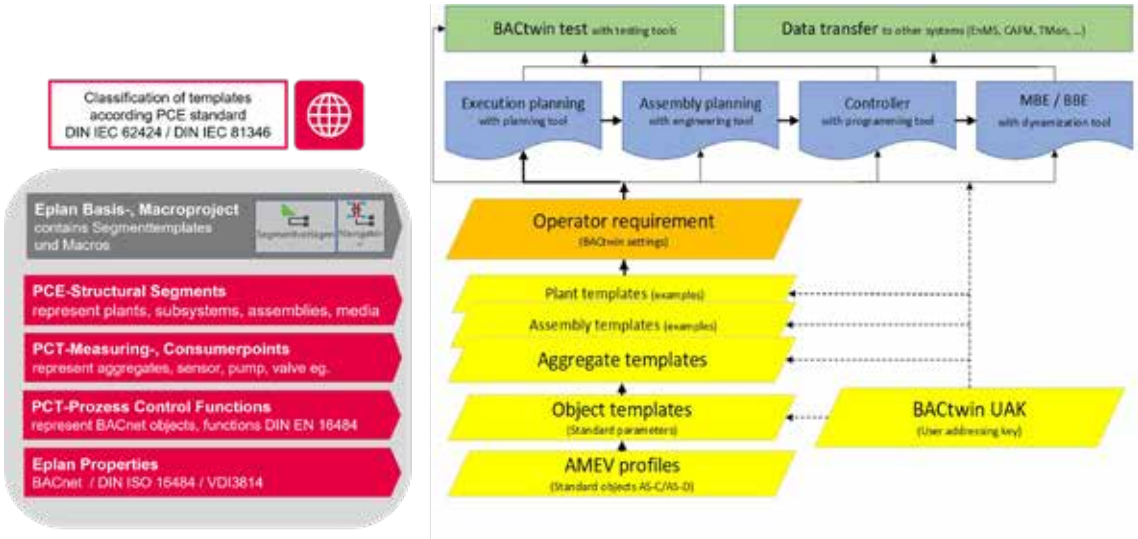


Fig. 1: Structural design of the BACtwin concept Eplan (Source: AMEV / Eplan)
Abb. 1: Struktureller Aufbau des BACtwin Konzepts Eplan (Quelle: AMEV / Eplan)

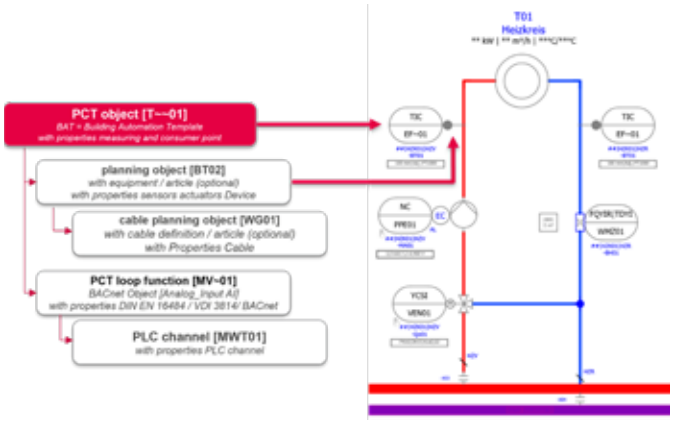


Fig. 2: PLT location using the example of a temperature measuring point (source: Eplan)
Abb.2: PLT-Stelle am Beispiel einer Temperaturmessstelle (Quelle: Eplan)

Fig 3: Predefined BACtwin value sets in segment templates in Eplan (source: Eplan)
Abb.3: Vorbelegte BACtwin-Wertesätze in Segmentvorlagen bei Eplan (Quelle: Eplan

data – from sensors, actuators, cables, and devices to functions – is managed centrally in the project database in the preliminary planning navigator across all disciplines (basic evaluation, planning, circuit diagram creation, automatic production).

Evaluation

Pre-designed standard sheets for creating BA function diagrams and forms for evaluating operating resources, objects, and functions enable complete documentation in accordance with VDI 3814 and DIN ISO 16484 standards.

Data

Import and export functions in formats such as Excel, CSV, or XML ensure easy external processing and exchange with other authoring systems. See Figure 5.

Planning and Execution: Potential for Partial or Full Automation with Eplan Solutions

The structured macro library based on the BA spectrum forms the basis for the partially automated creation of control schemes or circuit diagrams by configurators. The degree of automation depends on the depth of the macro library, thus creating considerable efficiency potential in planning and execution.

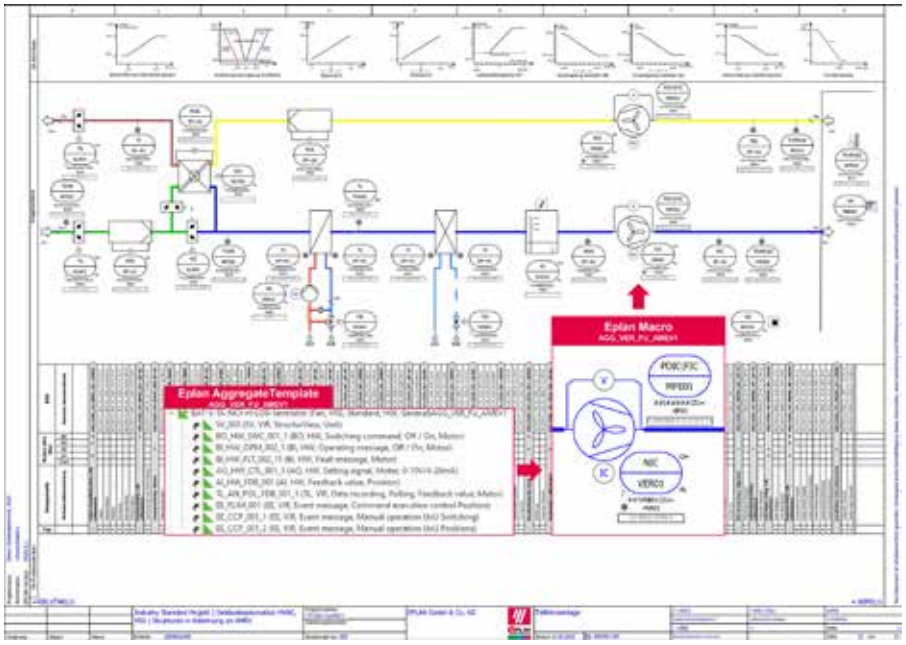


Fig. 4: Example of a simplified engineering process (source: Eplan)
Abb 4: Beispiel eines vereinfachten Engineering-Prozesses (Quelle: Eplan))

In Technical Operation: Digital Twin with Real Added Value

During operation, Eplan's BACtwin enables seamless digital documentation of all BA components, communication objects, and control functions – right down to the digital control cabinet in Eplan eView. This simplifies maintenance, fault analysis, and optimization, and provides a valuable database for energy management and future modernization.

- Planners benefit from clear specifications that promote clarity and accuracy.
- Installers use standardized interfaces to simplify configuration, programming, and commissioning.
- Operators receive transparent digital documentation with a high degree of traceability – a benefit for operational safety, maintenance, and operating processes.
- Collaboration: International projects can be worked on across teams using a multi-language feature and made available via the cloud.

Conclusion

The integration of BACtwin into the professional planning environment of the Eplan platform creates a robust foundation for a consistent BA project. With the BACtwin model in the Eplan platform, building automation becomes plannable, traceable, and future-proof. This results in greater efficiency from planning to technical operation in building automation.

Die Eplan Plattform ermöglicht einen modellbasierten Planungsprozess auf Grundlage des BACtwin, unter Berücksichtigung der Planungsrichtlinien und Standards gemäß VDI 3814 und DIN EN ISO 16484.

BACtwin Implementierung

Mit dem Release der Eplan Plattform 2026 (Sept. 2025) und dem branchenspezifischen Industry Package Building Automation wurden neue Building Automation Vorlagen – sogenannte Segmentvorlagen und Makros – bereitgestellt. Damit ist der aktuelle AMEV BACtwin 2025 (Bibliotheken 1–3) implementiert und direkt im Engineering einsetzbar.

Segmentvorlagen beinhalten alle notwendigen technischen Informationen zu Sensoren, Aktoren, Geräten, Aggregaten, Anlagen oder Anlagenteilen – einschließlich der zugehörigen Objekte und Funktionen. Sie unterstützen die standardisierte, automatisierte Planung, Dokumentation und Auswertung.

Die Segmentvorlagen sind entsprechend dem BACtwin-Modell gegliedert und bilden sogenannte Strukturegmente, die der Projektstrukturierung (z. B. Gebäude, Anlage, Teilanlage, Baugruppe) und deren Strukturkennzeichnung dienen. Für die detaillierte Anlagenplanung stehen spezielle Segmentvorlagen für Aggregate, Funktionen und Planungsobjekte zur Verfügung. Zur übersichtlichen Einordnung dieser vielseitigen Segmentvorlagen erfolgt die Strukturierung und Klassifizierung von Objekten nach IEC 62424 sowie DIN EN 81346. Siehe Abb. 1.

Vorgefertigte Segmentvorlagen auf PLT-Stellenebene (Vorlagen für Mess- und Verbraucherstellen) beinhalten bereits die fertigen BACtwin Aggregate Templates. Siehe Abb. 2.

Auf der funktionalen Ebene beinhalten Segmentvorlagen der PLT-Stellenfunktionen die AMEV BACtwin Objekt Templates.

Fertige Planungsdaten – vorbelegte Wertesätze der Propertysets

Sämtliche Eigenschaften zur Auswertung der GA-Funktionen und zur Dokumentation sind mit vordefinierten Wertesätzen des AMEV BACtwin sowie gemäß VDI 3814/DIN EN ISO 16484 vorbelegt. Diese können vom GA-Fachplaner direkt verwendet oder bei Bedarf an Betreiberanforderungen angepasst werden. Siehe App. 3.

Der Engineering Workflow Makroplanung

Im Makroprojekt stehen Makros für Aggregate aus den Bereichen Sensorik, Aktorik und Geräte zur Verfügung. Daraus lassen sich Baugruppen und komplette Anlagen konfigurieren. Im Hintergrund dieser Makros sind die vorkonfigurierten Segmentvorlagen hinterlegt oder können bei der Platzierung im Schema über Wertesatzabfragen ausgewählt werden. Siehe Abb. 4.

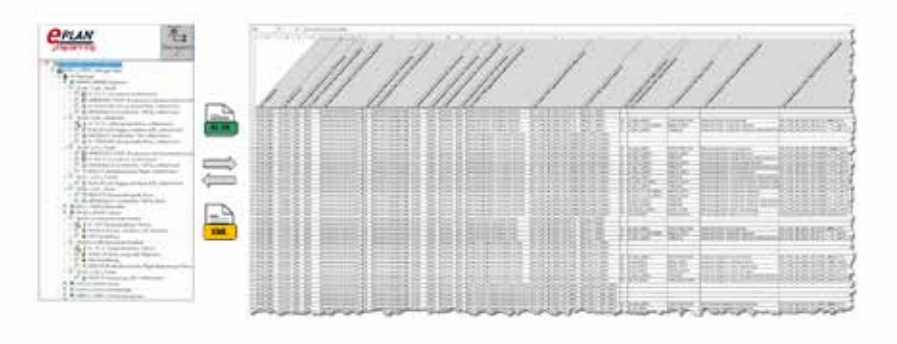


Fig. 5: Import and export interfaces in the Eplan platform
Abb 5: Im- und Export-Schnittstellen in der Eplan Plattform

Daten für alle Beteiligten

Ein weiterer Vorteil im Engineering-Prozess ist die Bereitstellung und Nutzung konsistenter Daten für nachgelagerte Prozesse wie die Schaltanlagenplanung sowie die Übergabe von Funktionsdaten und SPS-Informationen für Hardwarekonfiguration und Softwareprogrammierung. Alle relevanten Planungsdaten – von Sensoren, Aktoren, Kabeln und Geräten bis hin zu Funktionen – werden zentral in der Projektdatenbank im Vorplanungsnavigator über alle Disziplinen hinweg (Grundlagenermittlung, Planung, Schaltplanerstellung, automatische Fertigung) verwaltet.

Auswertung

Bereits vorgefertigte Normblätter zur Erstellung der GA-Funktionsschemas sowie Formulare für Auswertungen von Betriebsmitteln, Objekten und Funktionen ermöglichen eine lückenlose Dokumentation endsprechend der Standards VDI 3814 und DIN ISO 16484.

Datenaustausch

Durch Im- und Exportfunktionen in Formate wie Excel, CSV oder XML ist eine einfache externe Bearbeitung sowie der Austausch mit anderen Autorensystemen gewährleistet. Siehe Abb. 5.

Planung und Ausführung: Potenzial zur Teil- oder Vollautomatisierung durch Eplan Lösungen

Die strukturierte Makrobibliothek auf Basis des GA-Spektrums bildet die Basis für eine teilautomatisierte Erstellung von Regelschemen oder Stromlaufplänen durch Konfiguratoren. Der Automatisierungsgrad hängt von der Tiefe der Makrobibliothek ab – und schafft so erhebliches Effizienzpotenzial in Planung und Ausführung.

Im technischen Betrieb: Digitaler Zwilling mit echtem Mehrwert

Im Betrieb ermöglicht Eplan mit dem BACtwin eine lückenlose digitale Dokumentation aller GA-Komponenten, Kommunikationsobjekte und Regelungsfunktionen – bis hin zum digitalen Schaltschrank in Eplan eView. Das erleichtert Wartung, Störfallanalyse und Optimierung und liefert eine wertvolle Datenbasis für Energiemanagement und zukünftige Modernisierungen.

- Planer profitieren von klaren Vorgaben, die Übersicht und Fehlerfreiheit fördern.
- Errichter nutzen standardisierte Schnittstellen zur Vereinfachung von Konfiguration, Programmierung und Inbetriebnahme.
- Betreiber erhalten eine transparente digitale Dokumentation mit hoher Nachvollziehbarkeit – ein Gewinn für Betriebssicherheit, Wartungs- und Betriebsprozesse.
- Kollaboration: Internationale Projekte können per Multi Language teamübergreifend bearbeitet und per Cloud bereitgestellt werden.

Fazit

Die Einbindung des BACtwin in die professionelle Planungsumgebung der Eplan Plattform schafft eine belastbare Grundlage für ein durchgängiges GA-Projekt. Mit dem BACtwin Modell in der Eplan Plattform wird die Gebäudeautomation planbar, nachvollziehbar und zukunftssicher. Das gibt mehr Effizienz von der Planung bis zum technischen Betrieb in der Gebäudeautomation. ■

Eplan GmbH & Co. KG
schulte.r@eplan.de
www.eplan.de

What Remains when Standards Change?
Was bleibt, wenn sich Standards verändern?

Certifications aren't sexy. They sound like audit trails, footnotes, spreadsheets. Like precision, patience – and too many Teams calls. But it's exactly here, in this technocratic niche, where something vital beats: A heart for quality. And for the future.

Zertifizierungen sind nicht sexy. Sie klingen nach Prüfprotokollen, Fußnoten, Tabellen. Nach Genauigkeit, Geduld – und vielen Teams-Calls. Aber genau hier, in dieser technokratischen Nische, schlägt ein Herz für Qualität. Und für Zukunft.

I'm part of the BTL Working Group at BACnet International – a team that meets every two weeks, virtually, across time zones and disciplines. Together, we turn protocol revisions into real-world reliability. At the centre: the test package. And one clear, powerful belief – that interoperability should never be left to chance.

As of 1 January 2025, only devices with protocol revision 18 or higher are eligible for certification. A small change in wording – a big step for the industry.

Test Package 26.0 is more than a technical update. It's living proof that an open, global communication standard can evolve without losing its integrity. Addenda, errata, interim documents – what may seem dry from the outside is, in fact, a finely tuned mechanism. One that allows new features, new devices, and new ideas to be tested – even before the full package is complete.

That's not bureaucracy. That's agility by design.

And it doesn't stop there. The next change is already on the horizon: Test Package 26.1 arrives at the end of 2025. With new naming conventions. New concepts for derivative certification. And a clear commitment: not just to make things better, but to make them clearer – as seen in the new alignment between EPICS files and the Test InfoSheet.

In parallel, interim documents are constantly in development. They allow us to test cutting-edge devices already supporting BACnet Revision 30 – even when the official test plan isn't ready. Certification stays flexible. And manufacturers stay connected.

So, what remains when standards evolve? Perhaps exactly what makes them strong: The willingness to question. The drive for quality. And the shared goal of turning complexity into reliability – for manufacturers, planners, and users alike.

I'm proud to help shape that path as an active member of the BTL Working Group at BACnet International. ■

Ich bin Teil der BTL Working Group der BACnet International (BI), die sich alle zwei Wochen virtuell trifft. Gemeinsam mit anderen engagierten Mitgliedern arbeiten wir daran, aus Protokollrevisionen verlässliche Realitäten zu machen. Im Zentrum: das Testpaket. Und eine einfache, aber starke Idee – dass Interoperabilität nicht dem Zufall überlassen werden darf.

Seit dem 1. Januar 2025 gilt: Nur Geräte mit einer Protokollrevision ab 18 dürfen zertifiziert werden. Der Standard definiert, was morgen zählt – und bringt die Branche in Bewegung.

Auch Testpaket 26.0 ist mehr als nur ein technisches Update – es ist ein Beweis für die lebendige Weiterentwicklung eines offenen, weltweiten Kommunikationsstandards. Addenda, Errata, Interimsdokumente: Was für Außenstehende trocken klingt, ist in Wahrheit ein feines Räderwerk. Es sorgt dafür, dass neue Funktionen, neue Geräte, neue Ideen getestet werden können – selbst wenn das eigentliche Paket noch in Arbeit ist.

Das ist nicht bürokratisch. Das ist beweglich gedacht.

Und es geht weiter: Die nächste Veränderung steht schon vor der Tür. Testpaket 26.1 kommt Ende 2025. Mit neuen Namenskonventionen. Mit neuen Ideen zur Derivat-Zertifizierung. Und mit dem Anspruch, Dinge nicht nur besser, sondern klarer zu machen – wie die neue Abstimmung zwischen EPICS-Datei und Test-InfoSheet zeigt.

Gleichzeitig arbeiten wir laufend an Interimsdokumenten. Sie ermöglichen es, auch die neuesten Geräte mit BACnet Revision 30 zu testen – selbst wenn der offizielle Testplan noch nicht so weit ist. So bleibt die Zertifizierung flexibel – und Hersteller bleiben anschlussfähig.

Was bleibt also, wenn sich Standards verändern? Vielleicht genau das, was sie stark macht: die Bereitschaft, sich zu hinterfragen. Die Lust auf Qualität. Und das gemeinsame Ziel, aus Komplexität Verlässlichkeit zu machen – für Hersteller, Planer und Anwender.

Ich freue mich, diesen Weg in der BTL Working Group von BACnet International aktiv mitgestalten zu dürfen. ■

Alexandra Henczka
Leiterin BACnet-Testlabor der MBS GmbH
Head of BACnet Test Lab at MBS GmbH
Member of BTL-Working Group

BIG-EU at ISH 2025: Visibility, Exchange, and a Strong Presence in Frankfurt

BIG-EU auf der ISH 2025: Sichtbarkeit, Austausch und starke Präsenz in Frankfurt

Once again, the BACnet Interest Group Europe (BIG-EU) took part in ISH – the leading international trade fair for building automation and sanitary solutions – with a dedicated exhibition stand.
Auch in diesem Jahr war die BACnet Interest Group Europe (BIG-EU) auf der ISH – der internationalen Leitmesse für Gebäudeautomation, Sanitär-, Heiz- und Klimatechnik – mit einem eigenen Gemeinschaftsstand vertreten.

From March 10 to 14, 2025, BIG-EU was joined by its co-exhibitors Kieback&Peter, Evon, Johnson Controls, Tridium, and TÜV Süd for five highly successful days in Frankfurt.

Five Days of Intensive Engagement

The BIG-EU stand attracted steady interest throughout the entire week. Visitors took the opportunity to engage directly with representatives from member companies and learn about the latest in BACnet technology. Discussions frequently revolved around the future of interoperable solutions, BACnet Secure Connect (BACnet/SC), and the evolving role of BACnet in smart, networked buildings.

This year, digital communication was also a major focus: live coverage via BIG-EU's LinkedIn and Instagram channels gave followers real-time impressions from the trade fair floor. Interviews with co-exhibitors, spontaneous visitor comments, and member highlights were published continuously during the event – creating high engagement and boosting awareness far beyond the exhibition hall. The positive response has already sparked early interest in upcoming events, such as Light + Building in March 2026.

Young Talent Honored, Community Connected

A highlight on Tuesday evening was the presentation of the BIG-EU Young Talent Award. This year, a single outstanding academic thesis

BIG-EU joint stand at the ISH 2025
BIG-EU Gemeinschaftsstand auf der ISH 2025

Oussama Kalai-Ezzar (m), a graduate of Cologne University of Applied Sciences, was honoured with the BIG-EU Award 2025. The prize was presented by Tobias Plath (r) and Johan Schakenraad (l).
Oussama Kalai-Ezzar (m), ein Absolvent der Fachhochschule Köln, wurde mit dem BIG-EU Award 2025 ausgezeichnet. Der Preis wurde überreicht von Tobias Platz (r) und Johan Schakenraad (l).

related to BACnet was recognized – an important tradition to support the next generation of innovators in building automation.

Following the award, BIG-EU hosted its traditional networking event at the stand. Known throughout the industry as a go-to spot for informal exchange, the gathering was once again very well attended. The relaxed setting encouraged cross-company conversations and reinforced the strong sense of community within the BACnet ecosystem.

Conclusion

With strong attendance, active digital outreach, and a vibrant exchange of ideas, ISH 2025 proved a resounding success for the BACnet Interest Group Europe. The next events are already on the horizon – and anticipation is building.

Vom 10. bis 14. März 2025 präsentierte sich die BIG-EU gemeinsam mit den Mitausstellern Kieback & Peter, Evon, Johnson Controls, Tridium und TÜV Süd – und das mit großem Erfolg.

Fünf Messetage mit intensivem Austausch

Der BIG-EU-Stand war über alle Tage hinweg sehr gut besucht. Zahlreiche Besucherinnen und Besucher informierten sich über den aktuellen Stand der BACnet-Technologie und nutzten die Gelegenheit zum fachlichen Austausch mit Vertreterinnen und Vertretern der Mitgliedsunternehmen. Das wachsende Interesse an interoperablen, standardisierten Lösungen zeigte sich besonders in den Gesprächen zu aktuellen Entwicklungen wie BACnet/SC und zur Rolle von BACnet in smarten, vernetzten Gebäuden.

Ein besonderer Fokus lag dieses Jahr auf der digitalen Kommunikation: Über die Social-Media-Kanäle der BIG-EU – insbesondere LinkedIn und Instagram – wurden laufend Eindrücke von der Messe veröffentlicht. Interviews mit Mitausstellern, Kurzstatements von Mitgliedern und spontane Besuchermeinungen machten das Messegeschehen auch digital erlebbar. Die hohe Reichweite der Beiträge sorgte für zusätzliche Sichtbarkeit – und weckt schon jetzt das Interesse an der nächsten großen Branchenmesse: der Light + Building im März 2026.

Nachwuchsauszeichnung und Networking-Event

Ein besonderes Highlight war erneut die Verleihung der BIG-EU Nachwuchsauszeichnung am Dienstagabend. Prämiert wurde eine herausragende Abschlussarbeit mit direktem Bezug zu BACnet – ein starkes Zeichen für die Förderung junger Talente in der Branche.

Im Anschluss fand das traditionelle Networking-Event am Stand der BIG-EU statt. In der Branche längst bekannt als einer der zentralen Treffpunkte für persönliche Gespräche in entspannter Atmosphäre, war die Veranstaltung auch in diesem Jahr sehr gut besucht. Die Gelegenheit zum informellen Austausch wurde rege genutzt – über Unternehmensgrenzen hinweg.

Fazit

Mit einer starken Präsenz, aktiver digitaler Kommunikation und gelebter Netzwerkkultur war die ISH 2025 für die BACnet Interest Group Europe ein voller Erfolg. Die nächsten Veranstaltungen sind bereits in Planung – und die Vorfreude ist groß.

Spring Meeting 2025 in Lisbon: Exchange, Insights, and New Impulses

Frühjahrsmeeting 2025 in Lissabon: Austausch, Einblicke und neue Impulse

Participants at the Spring Meeting 2025 in Lisbon
Teilnehmende des Spring Meetings 2025 in Lissabon

On May 12 and 13, 2025, members of the BACnet Interest Group Europe (BIG-EU) gathered in the Portuguese capital for the traditional Spring Meeting to discuss current topics and future developments.
Am 12. und 13. Mai 2025 kamen die Mitglieder der BACnet Interest Group Europe (BIG-EU) in der portugiesischen Hauptstadt zusammen, um im Rahmen des traditionellen Frühjahrsmeetings über aktuelle Themen und künftige Entwicklungen zu beraten.

The host city of Lisbon provided not only a Mediterranean flair but also a fitting setting for two days of content-rich and personally engaging events.

Committee Meetings and Executive-Level Exchange

The opening day on May 12 was dedicated entirely to internal committee work: the Advisory Board and Executive Board convened for a joint meeting. Strategic issues related to the further development of BACnet, international cooperation, and the orientation of future formats were discussed in depth.

Later that evening, BIG-EU invited participants to a joint networking dinner – not only for board members, but also for early arrivals attending the member meeting the following day. In a relaxed atmosphere and over Portuguese cuisine, informal conversations took place and new contacts were made. Many topics were revisited from new personal perspectives during these exchanges.

General Assembly with a Forward-Looking Agenda

On May 13, the official BIG-EU Spring Meeting took place. The general assembly provided updates on the association's current developments – including financial matters, activities from the past year, and the admission of new members. The spotlight was on upcoming BIG-EU initiatives such as planned events, working group projects, and strategic partnerships.

A Successful Gathering

The Spring Meeting 2025 in Lisbon was characterized by productive dialogue, a spirit of partnership, and shared goals. It once again highlighted the importance of personal contact within the BACnet community – as a foundation for technological collaboration and the continued advancement of the BACnet standard in Europe and beyond. ■

Die Gastgeberstadt Lissabon bot dabei nicht nur mediterranes Flair, sondern auch einen passenden Rahmen für zwei inhaltlich dichte und gleichzeitig persönlich geprägte Veranstaltungstage.

Gremiensitzungen und Austausch auf Leitungsebene

Der Auftakt am 12. Mai stand ganz im Zeichen der internen Gremienarbeit: Advisory Board und Executive Board tagten in einer gemeinsamen Sitzung. Strategische Fragen rund um die Weiterentwicklung von BACnet, internationale Kooperationen sowie die Ausrichtung zukünftiger Formate wurden hier intensiv diskutiert.

Im Anschluss lud die BIG-EU am Abend zu einem gemeinsamen Networking Dinner ein – nicht nur für die Gremienmitglieder, sondern auch für bereits angereiste Teilnehmerinnen und Teilnehmer des Mitgliedertreffens am Folgetag. In entspannter Atmosphäre wurden bei portugiesischer Küche auch informelle Gespräche geführt und neue Kontakte geknüpft. Zahlreiche Themen fanden dabei im persönlichen Austausch noch einmal eine neue Perspektive.

This year's BACnet Plugfest also brought the global community of BACnet developers to Lisbon
Das diesjährige BACnet Plugfest brachte auch die weltweite Gemeinschaft der BACnet-Entwickler nach Lissabon

Preparatory meeting at the Spring Meeting 2025 in Lisbon
Vorbereitungstreffen auf dem Spring Meeting 2025 in Lissabon

Mitgliederversammlung mit Blick nach vorn

Am 13. Mai fand dann das offizielle Frühjahrsmeeting der BIG-EU statt. Die Mitgliederversammlung informierte über aktuelle Entwicklungen im Verein – darunter die Finanzsituation, Aktivitäten des vergangenen Jahres und die Aufnahme neuer Mitglieder. Besonders im Fokus standen die kommenden Initiativen der BACnet Interest Group, etwa geplante Veranstaltungen, Arbeitsgruppenprojekte und strategische Partnerschaften.

Ein erfolgreiches Zusammenkommen

Das Frühjahrsmeeting 2025 in Lissabon war geprägt von produktivem Austausch, partnerschaftlichem Dialog und gemeinsamer Zielsetzung. Es unterstrich erneut, wie wichtig der persönliche Kontakt innerhalb der BACnet-Community ist – als Grundlage für technologische Zusammenarbeit und den weiteren Ausbau des BACnet-Standards in Europa und darüber hinaus.

New: Building Automation Tech Talks – Technical Know-How, Made Understandable

Neu: Building Automation Tech Talks – Technik verständlich gemacht

On July 4, 2025, the BACnet Interest Group Europe (BIG-EU) launched a fresh new format: the Building Automation Tech Talks. What began as an idea within the BIG-EU Technical Working Group was discussed in detail during recent meetings – including the final round in Lisbon – and has now come to life.

Mit einem neuen Format bringt die BACnet Interest Group Europe (BIG-EU) frischen Wind in den technischen Dialog: Am 4. Juli 2025 feierten die Building Automation Tech Talks ihre Premiere. Was in der Arbeitsgruppe Technik zunächst als Idee reifte, wurde zuletzt in Lissabon konkret diskutiert und einstimmig verabschiedet – nun ist der erste Schritt gemacht.

The concept is as straightforward as it is impactful: break down technical BACnet topics in a way that's easy to grasp – by engineers, for engineers. The focus lies on the latest developments and the real-world challenges encountered in BACnet-based projects. Less theory, more practice. And above all, knowledge sharing at eye level.

A Strong Start: Cybersecurity Takes Center Stage

The inaugural session tackled a topic that's both timely and crucial: "Basics of Cybersecurity in Building Automation." Frank Schubert from Beckhoff presented key insights, covering everything from legal frameworks like CRA and NIS2 to core concepts such as TLS encryption and the evolving convergence of IT and OT. The session was expertly moderated by Salvatore Gattaldi, head of the BIG-EU Technical Working Group.

With nearly 100 registrations and more than 60 live attendees, the first Tech Talk proved to be a resounding success – a clear indication that the format hits a nerve in the BACnet community.

A Webinar – But Different

Each Tech Talk is a one-hour webinar, combining a focused 30-minute presentation with a live Q&A session. No overloaded slides or overly technical jargon – just clear, practical input with room for discussion. The sessions are held in English and are free of charge. Only a brief registration is required.

More to Come

The enthusiastic response confirms it: the demand is high. The BACnet community can look forward to many more Tech Talks to come. Upcoming topics and dates will be announced soon via the BIG-EU platform.

A promising start – and the beginning of a new chapter in BACnet's technical dialogue. ■

Die Idee hinter dem Format ist ebenso einfach wie wirkungsvoll: Technische Themen aus der BACnet-Welt sollen künftig kompakt, praxisnah und verständlich vermittelt werden – von Praktikern für Praktiker. Der Fokus liegt auf aktuellen Entwicklungen und Herausforderungen, wie sie in realen Projekten auftreten. Und das nicht theoretisch, sondern mit einem klaren Ziel: Wissen teilen, Fragen klären, den Austausch fördern.

Premiere mit Cybersecurity – ein Thema, das bewegt

Den Auftakt bildete das Thema „Basics of Cybersecurity in Building Automation“. Frank Schubert von Beckhoff gab in seinem Vortrag einen strukturierten Überblick über den Status quo der IT-Sicherheit – von regulatorischen Anforderungen wie CRA und NIS2 über technische Grundlagen wie TLS bis hin zur immer wichtigeren IT/OT-Konvergenz. Die anschließende Diskussion, souverän moderiert von Salvatore Gattaldi, dem Leiter der technischen Arbeitsgruppe, zeigte: Das Thema trifft einen Nerv.

Mit knapp 100 Anmeldungen und mehr als 60 Teilnehmenden war das erste Tech Talk-Webinar ein voller Erfolg – und zugleich ein klares Signal für die Relevanz des Formats.

Webinar – aber anders

Das gewählte Format – einstündige Webinare mit halbstündiger Präsentation und anschließender Fragerunde – überzeugte durch seine Effizienz und Nähe zur Praxis. Keine überladenen Folien, kein Fachjargon um des Fachjargons willen, sondern ein klarer Fokus auf Verständlichkeit und Austausch. Die Tech Talks finden auf Englisch statt und sind kostenfrei. Eine einfache Registrierung genügt.

Agenda des ersten Tech Talks

- Warum Cybersecurity in der Gebäudeautomation (heute mehr denn je) relevant ist
- Normen und gesetzliche Anforderungen (CRA, NIS2 u. a.)
- Grundlagen der TLS-Verschlüsselung
- Verantwortlichkeiten der verschiedenen Akteure
- IT/OT-Konvergenz – Chance und Herausforderung zugleich

Fortsetzung folgt

Die große Resonanz auf das erste Webinar zeigt: Der Bedarf ist da. Die BACnet-Gemeinschaft darf sich also auf weitere spannende Ausgaben der Tech Talks freuen. Themen und Termine werden über die BIG-EU-Plattform bekannt gegeben.

Ein gelungener Auftakt – und ein neues Kapitel für den technischen Austausch in der Welt von BACnet.

Scott Ziegenfus Named Chairman of ASHRAE SSPC 135

Scott Ziegenfus übernimmt Vorsitz von ASHRAE SSPC 135

Scott Ziegenfus, a seasoned leader in building automation and lighting controls, has been named Chairman of ASHRAE SSPC 135, the committee responsible for the BACnet standard. With over three decades of experience and a deep commitment to interoperability and innovation, Ziegenfus brings a unique perspective rooted in real-world applications and a vision to modernize the standard for the next generation.

Scott Ziegenfus, ein erfahrener Experte für Gebäudeautomation und Lichtsteuerung, wurde zum Vorsitzenden des ASHRAE SSPC 135 ernannt – dem Komitee hinter dem BACnet-Standard. Mit über drei Jahrzehnten Branchenerfahrung verfolgt er ein klares Ziel: die Modernisierung des Standards unter Berücksichtigung praktischer Herausforderungen und zukünftiger Anforderungen.

A Career Built on Integration

Ziegenfus's journey spans leadership roles at Lutron Electronics, Hubbell Lighting, and currently Current Lighting, where he serves as Vice President of Customer Experience, Technical Services and Customer Facing Software. His work has consistently focused on bridging systems – lighting, HVAC, access control – through open protocols and seamless integration.

His involvement with BACnet began over 15 years ago, culminating in roles as Vice Chairman, Secretary and Convener of both the Protocol Services Working Group and the Data Modeling Working Group. These positions have given him a front-row seat to the evolution of BACnet and the challenges faced by engineers implementing it.

BACnet: A Living Standard

Since its first publication in 1995, BACnet has undergone continuous, transformative upgrades. Far from being a legacy protocol, BACnet is a living, adaptive standard that rivals any modern communication protocol in flexibility, scalability, and relevance.

"BACnet has evolved from a pioneering protocol into a modern, adaptive standard that meets today's complex integration and cybersecurity demands," says Ziegenfus.

Timeline of Key Milestones

- 1995 – First publication of ANSI/ASHRAE Standard 135
- 2003 – BACnet becomes ISO 16484-5
- 2004–2015 – Expansion to BACnet/IP, BACnet/WS, and wireless protocols
- 2012 – Introduction of 54 standard objects for modeling diverse building systems
- 2015–Present – Focus on cybersecurity, semantic tagging, and application profiles

These milestones reflect BACnet's ability to adapt to emerging technologies and integration needs, making it a cornerstone of smart building infrastructure.

A Vision for the Future

Today, the BACnet standard spans 1,527 pages – a testament to its depth, but also a barrier for new engineers. Ziegenfus's vision as Chairman is to:

- Optimize and organize the standard for clarity and usability
- Modernize its structure to reflect current system design practices
- Create pathways for new engineers to adopt and implement BACnet more easily

"My goal is to make BACnet more accessible, more intuitive, and more powerful – for everyone," Ziegenfus explains. "We need to ensure that the next generation of engineers can engage with the standard without being overwhelmed by its complexity."

Lighting Industry Leadership

Ziegenfus is the first Chair from the lighting industry, a milestone that reflects the growing importance of lighting systems in building automation. He credits Current Lighting for their continued support as he takes on this leadership role.

Conclusion

With a career rooted in practical applications and a passion for open standards, Scott Ziegenfus is poised to lead BACnet into its next chapter. His vision promises a more streamlined, modernized standard – one that empowers engineers and integrators to build smarter, more connected environments. ■

Integration als roter Faden

Ziegenfus war in leitenden Positionen bei Lutron Electronics, Hubbell Lighting und aktuell bei Current Lighting tätig, wo er als Vice President für Customer Experience, Technische Services und kundenzentrierte Softwarelösungen verantwortlich ist. Seine berufliche Laufbahn ist geprägt vom Streben nach nahtloser Integration – sei es zwischen Licht, HLK oder Zutrittskontrolle – stets auf Basis offener Protokolle.

Sein Engagement für BACnet begann vor über 15 Jahren. Er bekleidete seither Schlüsselpositionen wie stellvertretender Vorsitzender, Sekretär und Leiter der Arbeitsgruppen für Protokolldienste und Datenmodellierung.

BACnet – ein lebendiger Standard

Seit seiner ersten Veröffentlichung im Jahr 1995 hat sich der BACnet-Standard kontinuierlich weiterentwickelt. Er gilt heute als dynamischer, skalierbarer Standard, der moderne Anforderungen an Integration und Cybersicherheit erfüllt.

„BACnet ist heute ein flexibler, adaptiver Standard, der den aktuellen Herausforderungen in der Gebäudeautomation gewachsen ist", so Ziegenfus.

Meilensteine in der Entwicklung

- 1995 – Erstveröffentlichung des ANSI/ASHRAE Standard 135
- 2003 – BACnet wird ISO 16484-5
- 2004–2015 – Erweiterung um BACnet/IP, BACnet/WS und drahtlose Protokolle
- 2012 – Einführung von 54 Standardobjekten zur Modellierung verschiedenster Gebäudesysteme
- 2015–heute – Fokus auf Cybersicherheit, semantisches Tagging und Applikationsprofile

Diese Meilensteine spiegeln die Fähigkeit von BACnet wider, sich an neue Technologien und Integrationsanforderungen anzupassen, wodurch es zu einem Eckpfeiler der intelligenten Gebäudeinfrastruktur wird.

Eine Vision für die Zukunft

Der BACnet-Standard umfasst heute über 1.500 Seiten – ein Zeichen seiner Komplexität, aber auch ein Hindernis für neue Ingenieure. Ziegenfus verfolgt daher eine klare Mission:

- Struktur und Verständlichkeit verbessern
- Den Standard modernisieren – analog zu heutigen Systemarchitekturen
- Einstieg für junge Fachkräfte erleichtern

Scott Ziegenfus, Chairman of ASHRAE SSPC 135
Scott Ziegenfus, SSPC135 Vorsitzender

„Mein Ziel ist es, BACnet zugänglicher, intuitiver und leistungsfähiger zu machen – für alle“, erklärt Ziegenfus.

Lichtindustrie erstmals an der Spitze

Ziegenfus ist der erste Vorsitzende mit Hintergrund in der Lichtindustrie – ein Indikator für die zunehmende Bedeutung von Lichtsystemen in der Gebäudeautomation. Er betont die Unterstützung seines aktuellen Arbeitgebers Current Lighting bei der Übernahme dieser Führungsrolle.

Fazit

Mit seiner praxisnahen Denkweise und der Leidenschaft für offene Standards führt Scott Ziegenfus den BACnet-Standard in ein neues Kapitel – mit Fokus auf Klarheit, Modernität und Zukunftsfähigkeit. ■

How BIG-EU's Social Media Strategy Boosts Reach, Knowledge, and Community

Die BACnet-Community verbinden – ein Posting nach dem anderen

BACnet stands for communication – and that's precisely what BIG-EU is all about.
Wie die Social-Media-Strategie der BIG-EU Reichweite, Wissen und Gemeinschaft fördert

As the European voice for BACnet, our goal is to promote interoperability, knowledge sharing, and innovation in the field of building automation. But technological excellence alone does not create a community – it is created through visibility, interaction, and a shared understanding.

Since 2024, BIG-EU has significantly increased its online reach. In May 2025, we surpassed the 3,000 follower mark on LinkedIn – representing a 42.9% increase within a year. Impressions also rose by over 50%, and the engagement rate grew by 48.7%. These figures show that our content is reaching the community – and creating real added value.

But it's not just about numbers. It's about fostering a vibrant, informed, and connected community. We strive to do this not only at trade shows and our own events such as Plugfest or the BACnet Forum, but also throughout the year on our social media channels.

From Technical Protocol to Human History

Our goal is to make the people behind BACnet visible – the developers, engineers, project managers, and visionaries who bring the open protocol to life. With formats such as "Who's Who," we regularly introduce experts who shape the working groups and direction of BIG-EU. These posts regularly generate high levels of interaction – a clear sign of the community's interest in personal stories and professional motivation.

We also report on key events such as ISH, Light + Building, Plugfest, and our meetings, as well as our own events. Reels and stories provide exclusive behind-the-scenes insights – from award ceremonies and expert panels to the energy of the discussions at the heart of the action.

Sharing Knowledge – with Style

More and more of our posts are focused on building knowledge. From new publications like the BACnet Cybersecurity Guide or the GEG White Paper 2024 to explaining interoperability testing at Plugfest, every post has one goal: to educate, empower, and connect!

We don't replace standards – we explain them. We don't duplicate documents – we make them accessible. And we promote the dialogue that distinguishes BACnet as a community project.

Community – the Foundation of BACnet

The success of BACnet depends not only on technical stability, but also on the network behind it. Manufacturers, system integrators, facility managers, and students – everyone benefits from an active community. Our posts make this connection visible and strengthen it. Comments, reposts, and mentions show that our followers are not silent consumers, but active contributors.

As one member once said, "BACnet is not just a protocol – it's the people who make it possible." This sentence reflects our communication. We post, we explain, we celebrate – and above all, we listen.

What's next?

BIG-EU will continue to invest in its social media presence in the future. We are planning new technical content in collaboration with the working groups, an expansion of our strategies, and lots more insights. We also want to showcase more voices from our membership – and thus further highlight the diversity and expertise of our community.

BACnet communicates not only with devices, but also with you. If you're not following us yet, LinkedIn and Instagram are not far away.

Because communication is not just what BACnet makes possible – it is our common foundation.

Als europäische Stimme für BACnet ist es unser Ziel, Interoperabilität, Wissensaustausch und Innovation im Bereich der Gebäudeautomation voranzutreiben. Doch technologische Exzellenz allein schafft keine Gemeinschaft – sie entsteht durch Sichtbarkeit, Interaktion und ein gemeinsames Verständnis.

Seit dem Jahr 2024 hat die BIG-EU ihre Online-Reichweite deutlich gesteigert. Im Mai 2025 haben wir auf LinkedIn die Marke von 3.000 Followern überschritten – das entspricht einem Zuwachs von 42,9 % innerhalb eines Jahres. Auch die Impressionen stiegen um über 50 %, die Engagement-Rate wuchs um 48,7 %. Diese Kennzahlen zeigen: Unsere Inhalte erreichen die Community – und schaffen echten Mehrwert.

Doch es geht nicht nur um Zahlen. Es geht darum, eine lebendige, informierte und vernetzte Community zu fördern. Das versuchen wir nicht nur auf Messen und eigenen Veranstaltungen wie dem Plugfest oder dem BACnet Forum – sondern das ganze Jahr über auf unseren Social-Media-Kanälen.

Vom technischen Protokoll zur menschlichen Geschichte

Unser Ziel ist es, die Menschen hinter BACnet sichtbar zu machen – die Entwickler:innen, Ingenieur:innen, Projektmanager:innen und Visionär:innen, die das offene Protokoll mit Leben füllen. Mit Formaten wie „Who is Who“ stellen wir regelmäßig Expert:innen vor, die die Arbeitsgruppen und Ausrichtung der BIG-EU prägen. Diese Beiträge generieren regelmäßig hohe Interaktionen – ein deutliches Zeichen für das Interesse der Community an persönlichen Geschichten und fachlicher Motivation. Ebenso berichten wir über zentrale Events wie die ISH, Light + Building, das Plugfest und unseren Meetings, aber auch über eigene Veranstaltungen. Reels und Storys geben exklusive Einblicke hinter die Kulissen – von Preisverleihungen und Fachpanels bis hin zur Energie der Gespräche mitten im Geschehen.

Wissen vermitteln – mit Format

Immer mehr unserer Beiträge widmen sich dem Wissensaufbau. Von neuen Publikationen wie dem BACnet-Leitfaden zur Cybersicherheit oder dem GEG-Whitepaper 2024 bis hin zur Erklärung von Interoperabilitätstests auf dem Plugfest – jeder Post verfolgt ein Ziel: Aufklären, befähigen und verbinden!

Wir ersetzen keine Standards – wir erklären sie. Wir duplizieren keine Dokumente – wir machen sie zugänglich. Und wir fördern den Dialog, der BACnet als Community-Projekt auszeichnet.

Community – das Fundament von BACnet

Der Erfolg von BACnet hängt nicht nur von technischer Stabilität ab, sondern vom Netzwerk, das dahintersteht. Hersteller, Systemintegratoren, Facility Manager und Studierende – alle profitieren von einer aktiven Gemeinschaft. Unsere Posts machen diese Verbindung sichtbar und stärken sie. Kommentare, Reposts und Erwähnungen zeigen: Unsere Follower sind keine stillen Konsument:innen, sondern aktive Mitgestalter:innen.

Wie ein Mitglied einmal sagte: „BACnet ist nicht nur ein Protokoll – es sind die Menschen, die es möglich machen.“ Dieser Satz spiegelt unsere Kommunikation wider. Wir posten, wir erklären, wir feiern – und vor allem: Wir hören zu.

Wie geht es weiter?

Auch in Zukunft wird die BIG-EU gezielt in ihre Social-Media-Präsenz investieren. Geplant sind neue technische Inhalte in Zusammenarbeit mit den Arbeitsgruppen, ein Ausbau der Strategien und ganz viel mehr Insights. Außerdem möchten wir mehr Stimmen aus unserer Mitgliedschaft zeigen – und damit die Vielfalt und das Know-how unserer Community weiter sichtbar machen.

BACnet kommuniziert nicht nur mit Geräten, sondern auch mit euch. Wer uns noch nicht folgt: LinkedIn und Instagram sind nicht weit entfernt.

Denn Kommunikation ist nicht nur das, was BACnet möglich macht – sie ist unser gemeinsames Fundament. ■

Antonia Stahlberg
TEMA Technologie Marketing AG

News from SSPC 135: New Leadership, Standards Progress, and Global Alignment

Neuigkeiten von SSPC 135: Neue Führung, Fortschritte bei den Standards und globale Ausrichtung

The ASHRAE Standing Standard Project Committee 135 (SSPC135), which governs the BACnet protocol, continues its mission to develop and maintain interoperable and future-proof solutions for building automation systems.

Das ASHRAE Standing Standard Project Committee 135 (SSPC135), zuständig für das BACnet-Protokoll, führt seine Aufgabe fort, interoperable und zukunftssichere Lösungen für Gebäudeautomationssysteme zu entwickeln und zu pflegen.

At the most recent plenary meeting on May 2nd, 2025, in Fort Lauderdale, Florida, the committee elected a new leadership team:

- Chair: Scott Ziegenfus (Hubbell Lighting)
- Vice Chair: Salvatore Cataldi (BELIMO Automation AG)
- Secretary: Nathaniel Benes (University of Nebraska)

This leadership transition follows the successful tenure of Coleman Brumley, whose contributions were formally recognized by the committee.

Key milestones since the last report include the publication of ASHRAE 135.1-2025, which introduces several critical updates and test corrections.

The public review of Addendum 135-ct is complete. It defines a way to convert BACnet data into RDF (Resource Description Framework), a W3C standard that works like a universal dictionary for machines. This makes BACnet information usable by semantic systems such as digital twins and analytics

A particularly significant development is the approval of ASHRAE 223P for its first public review. This proposed standard adds a semantic interoperability layer for describing equipment interconnections – a move that has been warmly received by both ISO TC205 and CEN TC 247 as an essential complement to existing communication standards. ■

Auf der jüngsten Plenarsitzung am 2. Mai 2025 in Fort Lauderdale, Florida, wählte das Komitee ein neues Führungsteam:

- Vorsitz: Scott Ziegenfus (Hubbell Lighting)
- Stellvertretender Vorsitzender: Salvatore Cataldi (BELIMO Automation AG)
- Sekretär: Nathaniel Benes (University of Nebraska)

Dieser Führungswechsel folgt auf die erfolgreiche Amtszeit von Coleman Brumley, dessen Beiträge vom Ausschuss offiziell gewürdigt wurden.

Zu den wichtigsten Meilensteinen seit dem letzten Bericht gehört die Veröffentlichung von ASHRAE 135.1-2025.Diese enthält mehrere wichtige Aktualisierungen und Test-Korrekturen.

Die öffentliche Überprüfung (Public Review) des Addendums 135-ct ist abgeschlossen. Es definiert eine Methode zur Konvertierung von BACnet-Daten in RDF (Resource Description Framework), einen W3C-Standard, der wie ein universelles Wörterbuch für Maschinen funktioniert. Dadurch können BACnet-Informationen von semantischen Systemen wie digitalen Zwillingen und Analysen genutzt werden.

Eine besonders wichtige Entwicklung ist die Freigabe von ASHRAE 223P für den erste öffentlichen Review. Diese vorgeschlagene Norm fügt eine semantische Interoperabilitätsebene zur Beschreibung von Geräteverbindungen hinzu – ein Schritt, der sowohl vom ISO TC205 als auch vom CEN TC 247 als wesentliche Ergänzung zu bestehenden Kommunikationsstandards begrüßt wurde. ■

Scott Ziegenfus (Hubbell Lighting)

Salvatore Cataldi (BELIMO Automation AG)

Nathaniel Benes (University of Nebraska)

Calendar of BACnet Events – BACnet-Kalender

Date | Datum	Location | Ort	Event | Veranstaltung	Information | Kontakt
2025			
17.–19.09.2025	Rostock, Germany	GLT-Anwendertagung 2025	BIG-EU Office, info@big-eu.org
06.–07.10.2025	Madrid	BIG-EU Autumn Meeting 2025	BIG-EU Office, info@big-eu.org
06.10.2025	Madrid	BIG-EU Open House (optional)	BIG-EU Office, info@big-eu.org
15.10.2025	London, UK	UK BACnet Forum 2025	BIG-EU Office, info@big-eu.org
15.–16.10.2025	London, UK	BIG-EU at Smart Buildings Show 2025	BIG-EU Office, info@big-eu.org
9.–11.12.2025	Berlin, Germany	BACnet Certificate Exchange Summit – Hands-on BACnet/SC Developer Workshop	BIG-EU Office, info@big-eu.org
08.–13.03.2026	Frankfurt/M, Germany	Light + Building 2026	BIG-EU Office, info@big-eu.org

BACnet Europe Journal

BACnet INTEREST GROUP EUROPE

Preview Issue 44 – March 2026 | Vorschau Ausgabe 44 – März 2026

30 Years of BACnet – Starting Smart, Getting Smarter.
Current developments and trends in building automation with BACnet, Light + Building 2026
Aktuelle Entwicklungen und Trends der Gebäudeautomation mit BACnet, Light + Building 2026

Editorial and advertisement deadline: Januar 16, 2026
Redaktions- und Anzeigenschluss: 6. Januar 2026

We are looking forward to receiving your order and contributions to bacnetjournal@tema.de.

Date of publication: March 2, 2026
Erscheinungstermin: 2. März 2026

Wir freuen uns auf die Anmeldung Ihrer Beiträge an bacnetjournal@tema.de.

Editorial Notes
Impressum

BACnet Europe Journal | ISSN 1614-9572

The BACnet Europe Journal is the European magazine for building automation based on BACnet technology. Experts, practitioners and professionals lead the way in applying and developing the BACnet standard – from building automation trends to devices and application projects; from qualification and training to testing and certification; from who's who in the BACnet community to useful information on events and publications. Special attention is given to members and activities of the BACnet Interest Group Europe (BIG-EU).

Distribution
This bi-annual and bi-lingual Journal (English/German) can be ordered free of charge by partners, members, media representatives and friends of the BACnet Interest Group Europe (BIG-EU) – registered society. Order the BACnet Europe Journal by email from bacnetjournal@tema.de

Online Distribution
Order your digital copy by email: bacnetjournal@tema.de
Or download it from this website: bacnetjournal.org/bacnet-journale/bacnet-europe-journal

Editor
TEMA Technologie Marketing AG, Burtscheider Markt 24
52066 Aachen, Germany

Executive Board
Thomas Kurowski, Siemens (President)
Stefan Pfützer, SBC Saia-Burgess Controls (Treasurer)
Johan Schakenraad, Johnson Controls (Secretary)
Tobias Plath, MBS GmbH (Board Member)

Editorial Office
TEMA Technologie Marketing AG
Hans Symanczik (Editor in Chief)
Phone: +49 241 88970-124
email: symanczik@tema.de
Hermann Josef Pilgram (Editor)
email: pilgram@tema.de

Media Services
TEMA Technologie Marketing AG
Hans Symanczik
Phone: +49 241 88970-124
email: symanczik@tema.de

Picture Credits
BIG-EU, TEMA AG and specified companies

light+building

Frankfurt am Main
08.–13.03.2026

Networking the BACnet Standard in Europe

JOIN THE ASHRAE BACnet INTEREST GROUP EUROPE

Visit us at
light+building
in hall 9.0

Roger Braun Honorary Member · Karl Heinz Belser Honorary Member · Peter Fischer Honorary Member · Brad Hill Honorary Member · Bernhard Isler Honorary Member · Tobias Kleine Honorary Member · Hans Kranz Honorary Member · Nils Meinert Honorary Member · René Quirighetti Honorary Member · Volker Röhl Honorary Member · Klaus Wächter Honorary Member

BACnet is ISO 16484-5. The most successful communication standard in building automation has a global market coverage of 64%. Source: BSRIA 2021

www.big-eu.org
+49 241 88970-124