eliona
Smart Building
Platform

Kopplung unterschiedlicher BMS für AI-Integration, ESG-Reporting oder Betriebs-optimierung

Kopplung unterschiedlicher BMS für AI-Integration, ESG-Reporting oder Betriebsoptimierung

Dipl. Ing. Enrico Buoso

Zusammenfassung

Künstliche Intelligenz (Abk. KI) wandelt die Gebäudeautomation, insbesondere im Bereich der Energieoptimierung, um. Während AI einerseits neue Möglichkeiten eröffnet, treten andererseits Herausforderungen im Hinblick auf Datenschutz, Sicherheit und Integration mit verschiedenen Typen von BMS auf: Die Integration und gleichzeitige Verwaltung verschiedener BMS und deren Interaktionen mit externen Diensten ist kritisch. Diese Abhandlung zielt darauf ab, Klarheit und Einblick in diese Interaktionsaspekte zwischen "unterschiedlich" SMARTen Gebäuden und deren Verbesserung durch Dienste künstlicher Intelligenz zu geben, mit einem besonderen Augenmerk auf Sicherheit.

Schlüsselwörter

#Künstliche Intelligenz — #AI — #BMS-System — #Energieoptimierung — #Individueller Komfort — #Sicherheit und Überwachung

Inhaltsverzeichnis

Einführung

Die Einführung der künstlichen Intelligenz (Abk. KI) hat eine neue Ära im Bereich der Technologie markiert und Innovation in zahlreichen Sektoren gebracht, einschließlich der Gebäudeautomatisierung. Diese Transformation hat Türen zu Lösungen geöffnet, die zuvor als undenkbar galten und die Art und Weise, wie Gebäude funktionieren und wie sie mit den Bewohnern interagieren, revolutionieren könnten.

In der modernen Ära werden Gebäude nicht mehr als einfache unbelebte Strukturen angesehen; sie sind vielmehr zu "lebendigen" und vernetzten Entitäten geworden, ausgestattet mit Sensoren, Aktoren und intelligenten Systemen, die ihre Leistung kontinuierlich überwachen und optimieren.

Im Folgenden sind einige Anwendungen und mögliche Vorteile der Verwendung von KI in der Gebäudeautomatisierung aufgeführt:

1. **Energieoptimierung**
   Durch die Analyse historischer und Echtzeitdaten kann die KI Energiever brauchsmuster vorhersagen und automatisch HVAC-Systeme, Beleuchtung und andere Anlagen regulieren, um die Energieeffizienz zu maximieren.

2. **Prädiktive Wartung**
   Die KI kann den Zustand und die Leistung von Geräten überwachen und Anomalien oder Leistungsabfälle erkennen, was präventive Wartungseingriffe ermöglicht, bevor tatsächliche Ausfälle auftreten. Dadurch lassen sich gezielt Wartungsfenster optimal setzen.

3. **Personalisierter Komfort**
   Auf KI basierende Systeme können die Präferenzen einzelner Benutzer oder Bewohner lernen und die Innenraumumgebung entsprechend anpassen, was zu einem personalisierten Komfort führt.

4. **Sicherheit und Überwachung**
   Durch die Analyse von Videos und Bildverarbeitung kann die KI verdächtige Aktivitäten erkennen, Menschenansammlungen oder unerwartete Bewegungen identifizieren und Benachrichtigungen senden oder angemessene Sicherheitsmaßnahmen ergreifen.

5. **Sprachinteraktion und Chatbots**
   Die KI ermöglicht die Erstellung fortschrittlicher Benutzerschnittstellen, wie Sprachassistenten oder Chatbots, die den Bewohnern helfen können, auf natürlichere und intuitivere Weise mit dem Gebäudeautomatisierungssystem zu interagieren.

6. **Simulationen und Analysen:**
   Mit der KI ist es möglich, komplexe Simulationen über Nutzung und Energieeffizienz durchzuführen, die dazu beitragen, Entwurfs- und Betriebsentscheidungen zu leiten.

Die Liste ist nur beispielhaft und nicht erschöpfend, und es könnte eine Behandlung für jeden der oben genannten Punkte durchgeführt werden. Aus Gründen der Kürze wird sich im Folgenden ausschließlich auf die Integration von KI-Diensten zur Unterstützung der Energieoptimierung konzentriert, um Gebäude effizienter und umweltfreundlicher zu machen.

Die Einführung von KI in BMS ist nicht ohne Herausforderungen. Datenschutz, Daten Integrität, Datensicherheit, Integration mit bestehenden Systemen und der Bedarf an spezialisierten Kenntnissen sind alles Faktoren, die berücksichtigt werden müssen. Dennoch wird mit dem techno-logischen Fortschritt und der steigenden Nachfrage nach intelligenten und nachhaltigen Gebäuden die KI eine immer wichtigere Rolle in der Gebäudeautomatisierung spielen.

Die Komplexitäten bei der gleichzeitigen Verwaltung verschiedener BMS, insbesondere wenn sie von Grund auf unterschiedlich sind, sind bereits bekannt. Diese Herausforderung wird noch komplizierter, wenn die Interaktion mit externen KI-Diensten berücksichtigt wird. Daher ist es notwendig, Maßnahmen und Best Practices zu beleuchten, um sicherzustellen, dass die Integration verschiedener BMS, auch unterschiedlicher Typen, und externer KI-Dienste erfolgt, ohne die Sicherheit der Anlagen und der Bewohner zu gefährden.

Darüber hinaus wird die Tatsache berücksichtigt, dass die Realität von mehreren BMS immer verbreiteter wird und mit ihr neue Probleme und Chancen auftauchen. Daher ist eine detaillierte Analyse erforderlich, die eine klare Sicht darauf bietet, wie man sie effektiv handhabt und gleichzeitig Energieoptimierung und Sicherheit gewährleistet.

1. KI als externer Cloud-Servicedigkeit von Innovation im Gebäudemanagement

Die Energieeffizienz in Gebäuden war schon immer ein Thema von großer Bedeutung, und mit dem Aufkommen neuer Technologien erfahren traditionelle Ansätze eine signifikante Transfomation. Eine bedeutende Innovation in diesem Bereich ist die Implementierung von "digital twins" oder digitalen Zwillingen. Diese stellen in diesem speziellen Fall eine virtuelle Replik des Gebäudes und seiner Systeme dar, die eine Simulation und genaue Analyse der energetischen Dynamik ermöglichen.

Durch den Einsatz von KI, Big Data und die Integration entsprechender Wettervorhersagen ist es möglich, das Gebäudeautomationssystem proaktiv zu steuern. Dies garantiert nicht nur besseren Komfort und ein stabiles Innenklima, sondern führt vor allem zu einer Reduktion der Energiekosten und der CO_2 Emissionen.

Die Architektur solcher Systeme muss entworfen werden, um Hardware und Wartungskosten zu minimieren. Daher müssen alle notwendigen Simulationsberechnungen auf einem ëxternen Cloud-Service"(Abk. ECS) durchgeführt werden. Die erfassten Steuerdaten werden über einen sicheren Kommunikationsweg an das Gebäudeautomationssystem übermittelt. Während des Betriebs werden die Steuerdaten vom ECS zum BMS übertragen, das sie verarbeitet. Es sollte jedoch immer möglich sein, diesen Modus manuell zu deaktivieren.

Die Kommunikation mit dem BMS erfolgt über bestehende Kommunikationsprotokolle (zum Beispiel BACnet, ModBus, OPC UA, SBus) und wird über einen Gateway gesteuert. Dieses Gerät ist in der Regel physisch innerhalb des Gebäudes installiert und mit dem BMS-Netzwerk verbunden. Unter bestimmten Umständen kann es jedoch auch virtuell installiert werden. Das Gateway kommuniziert einerseits mit dem vorhandenen BMS und andererseits, über eine sichere Verbindung, mit dem Simulationsmodell des ECS, oder wie wir später sehen werden, in einer funktionaleren Konfiguration mit der Integrations- und Zentralisierungsplattform (siehe Abschnitt 3.2).

Mit anderen Worten, das System überwacht kontinuierlich die Anlage und die Umweltbedingungen durch regelmäßige Messungen und integriert Optimierungsalgorithmen, um die Steuerparameter des Gebäudes zu verwalten. Es ist immer möglich, zwischen traditioneller Steuerung und der Steuerung des ECS zu wechseln, was Flexibilität und operative Kontinuität auch während Wartungsarbeiten oder Fehlfunktionen gewährleistet. Der Wechsel wird logisch über Schalter gesteuert, um sicherzustellen, dass die korrekten eingestellten Werte auf Basis des aktiven oder inaktiven Zustands des ECS kontrolliert werden, während die Messkanäle unabhängig vom Zustand des Steuersystems bleiben.

2. Notwendigkeit von Innovation im Gebäudemanagement

Im Zeitalter der fortgeschrittenen Digitalisierung wird die Herausforderung einer effektiven Integration verschiedener Building Management Systeme immer dringender, besonders wenn es darum geht, sich mit externen "Künstlichen Intelligenz" -Diensten zu verbinden. Große Gebäude oder solche mit historischer Architektur müssen oft mehrere Generationen von BMS managen, die zu unterschiedlichen Zeiten installiert wurden oder von verschiedenen Herstellern stammen. Die Gründe für diese Vielfalt sind vielfältig, einschließlich der Übernahme anderer Unternehmen, teilweiser Infrastrukturmodernisierungen oder der Entscheidung, im Laufe der Zeit verschiedene Lieferanten zu nutzen.

Die getrennte Verwaltung und die Integration jedes einzelnen BMS mit externen KI-Diensten stoßen auf erhebliche Komplexität, wie zum Beispiel:

1. **Betriebliche Redundanz:**
   Die Überwachungs- und Wartungsprozesse können erforderlich sein, für jedes System dupliziert zu werden.
2. **Ineffiziente Datensammlung:**
   Die Aggregation und Analyse von Daten aus verschiedenen Systemen können Verzögerungen und Fehlermöglichkeiten verursachen.
3. **Kostspielige Wartung:**
   Jedes BMS kann exklusive Aktualisierungsund Wartungsprotokolle erfordern.

Als Alternative bietet ein zentralisierter Ansatz zur Verwaltung mehrerer BMS bedeutende Vorteile, wie:

1. **Energieoptimierung:**
   Eine einheitliche Plattform bietet eine vollständige Übersicht über den Energieverbrauch, fördert informierte Entscheidungen und verbesserte Energieeffizienz.

2. **Verwaltung vereinfachen:**
   Eine einzige Schnittstelle ermöglicht es den Betreibern, alle BMS zu überwachen und zu steuern, wodurch die operative Verwaltung vereinfacht wird.

3. **Fortgeschrittene Datenanalyse:**
   Die Vereinheitlichung der Daten auf einer Plattform ermöglicht es der KI, Informationen effektiver zu verarbeiten und zu analysieren, was präzisere und zeitnahe Einblicke bietet.

4. **Verbessertes Ansehen:**
   Intelligente und nachhaltige Gebäude können deren Reputation in den Augen von Eigentümern und Nutzern steigern.

Die KI-Dienste bieten das Potenzial, das Management von BMS zu transformieren, mit der Fähigkeit, große Datenmengen in Echtzeit zu verarbeiten, um:

- **Anomalien vorhersagen:**
  Schnelle Identifizierung von Problemen oder Ineffizienzen für proaktive Eingriffe und die Reduzierung von Betriebskosten.

- **Prozessautomatisierung:**
  Minimierung manueller Eingriffe und damit verbundener Fehler.

- **Fortgeschrittene Personalisierung:**
  Lernen aus den Präferenzen der Bewohner, um die Umgebungseinstellungen automatisch anzupassen. Zusammenfassend ist die Integration mehrerer BMS im Zeitalter der KI nicht nur eine Herausforderung, sondern auch eine Chance, um die Automatisierung von Gebäuden zu optimieren und die Gesamtleistung zu verbessern.

3. Integration zwischen mehreren BMS und KI

Nachfolgend wird der Aspekt der Integration von verschiedenen heterogenen BMS mit Diensten der künstlichen Intelligenz in Energiemanagementprozessen vertieft.

Die Datentypen, die wir in Betracht ziehen werden, sind:

1. **Heizungsdaten:**
   Diese umfassen Informationen über die Erzeugung, wie Betriebsstatus, Temperatureinstellungen, Verbrauchsmessungen und Fehlermeldungen.
2. **Lüftungsdaten:**
   Beziehen sich auf Daten zur Luftqualität, Lüftungsmodi und Informationen zum Energieverbrauch.
3. **Klimadaten:**
   Umfassen Daten zur Umgebungstemperatur, Feuchtigkeit, Klimaeinstellungen und Energieverbrauchsdaten im Zusammenhang mit Klimaanlagensystemen.
4. **Hydraulikdaten:**
   Beinhalten Informationen zu Wassersystemen, Wasserverbrauch, Druck- und Temperaturüberwachung und Leckdetektion.
5. **Elektrische Daten:**
   Beschäftigen sich mit dem Stromnetz, wie Energieverbrauch, Spannungsmessungen, Informationen zu Schaltkreisen und Meldungen von elektrischen Fehlern.
6. **Zählerablesungen:**
   Die regelmäßige Aufzeichnung und Übertragung von Daten von Strom-, Gas- und Wasserzählern ist für eine genaue Analyse des Verbrauchs und dessen Optimierung wesentlich.

Die Integration dieser Daten durch KI ermöglicht ein ganzheitliches Energiemanagement und optimiert die Effizienz und Nachhaltigkeit des Gebäudes, was zu einer Reduzierung der Betriebskosten und zu einer Verbesserung der Umweltleistung der Infrastruktur führt.

Ist es möglich, die KI ohne Unterbrechungen in bestehende BMS zu integrieren?

- **Anfängliche Bewertung:**
  Vor jedem Integrationsprozess ist es unerlässlich, eine gründliche Analyse des aktuellen BMS durchzuführen, um seine Fähigkeiten, Lücken und mögliche Verbesserungsbereiche zu verstehen. Die Wahl des Kommunikationsprotokolls ist entscheidend für eine stabile, aber auch kostenoptimierte Implementierung.
- **Planung und Testing:**
  Die Integration sollte in einer Testumgebung beginnen, die die bestehende Infrastruktur repliziert. Dies ermöglicht die Identifizierung und Lösung von Problemen, ohne den Betrieb des Gebäudes zu beeinträchtigen.
- **Schrittweise Implementierung:**
  Anstatt einer vollständigen und sofortigen Übernahme ist es sicherer, schrittweise vorzugehen, zunächst weniger kritische Funktionen zu integrieren.

Es gibt verschiedene Standards und Protokolle, die für die Interoperabilität von BMS und KI-Systemen entwickelt wurden. Protokolle wie BACnet, OPC UA und ModBus werden in der Industrie aufgrund ihrer Fähigkeit, die Kommunikation zwischen verschiedenen Geräten und Systemen zu erleichtern, weit verbreitet eingesetzt. Diese Protokolle können verwendet werden, um sicherzustellen, dass Daten konsistent und zuverlässig zwischen den BMS und den KI-Systemen ausgetauscht werden. Auch hier ist die Integrität der Daten zu berücksichtigen, da unterschiedliche Protokolle unterschiedliche Sicherheitsaspekte bieten.

3.1 Auswirkungen der Integration auf die bestehende IT Infrastruktur

- **Netzwerklast:**
  Die Einführung von KI könnte den Netzwerkverkehr erhöhen, da es zu einer erhöhten Datensammlung und Kommunikation zwischen Geräten kommen kann. Es ist unerlässlich, die bestehende Netzwerkinfrastruktur zu bewerten und, falls notwendig, zu verstärken.

– **Sicherheit:**
Die externe Verbindung kritischer Systeme, wie Brandschutzsysteme, könnte Risiken bergen. Daher ist es notwendig:

> **Netzwerksegmentierung:** Das Netzwerk in separate Segmente unterteilen, so dass kritische Systeme nicht direkt externen Angriffen ausgesetzt sind.
>
> **Firewalls und IDS:** Die Verwendung von fortschrittlichen Firewalls und Intrusion Detection Systemen kann helfen, verdächtige Aktivitäten zu überwachen und zu blockieren.
>
> **VPN:** Wenn von außen auf das BMS zugegriffen wird, muss ein VPN, Virtual Private Network, verwendet werden, um eine verschlüsselte und sichere Verbindung zu gewährleisten.
>
> **Updates und Patches:** Alle Systeme, einschließlich des BMS und der KI-Plattform, mussten mit den neuesten Sicherheitspatches aktualisiert gehalten werden.

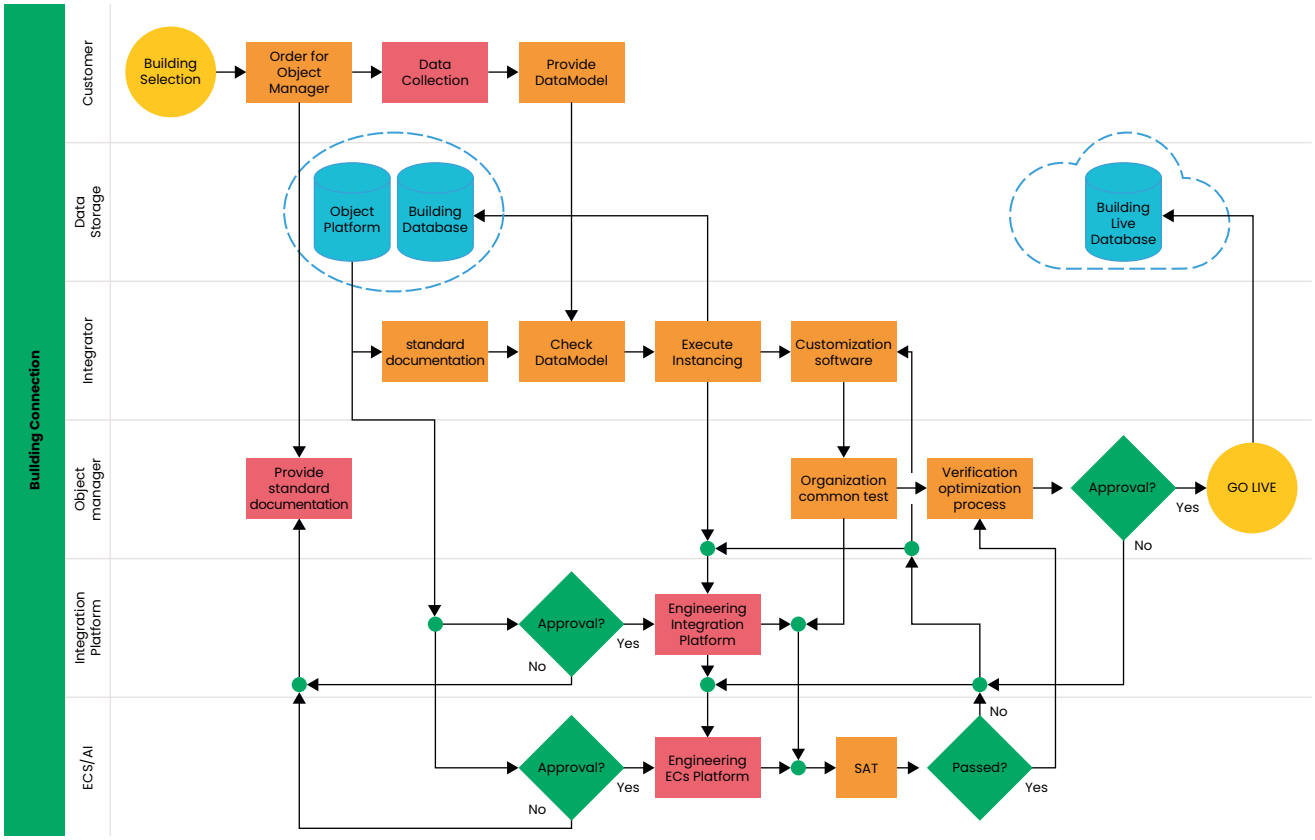

Abbildung 1. Prozess der Aktivierung eines Gebäudes

3.2 Integrationsplattformen

Die heterogene Natur der verschiedenen BMS und das Aufkommen von KI haben eine zunehmend fragmentierte Landschaft im Bau- und Infrastrukturmanagement geschaffen. Die Vielzahl an Lösungen, jede mit eigenen Standards und Protokollen, macht die Verwaltung komplex und verworren. Es ist daher unerlässlich, eine einheitliche Lösung, einen “zentralen Knotenpunkt”, zu identifizieren, der in der Lage ist, all diese verschiedenen Informationsquellen in einem kohärenten und optimierten Managementsystem zusammenzuführen.

In diesem Kontext führen wir einen **“Systemzentralisierer”** ein, eine Lösung, die in der Lage ist, verschiedene Systeme, Geräte und Kommunikationsprotokolle in einer zentralisierten Plattform zu vereinen, die in einem Gebäude oder mehreren Gebäuden vorhanden sind. Er dient als “Brücke” zwischen heterogenen Systemen und ermöglicht es ihnen, miteinander zu kommunizieren und zu interagieren. Später werden wir diese **“Zentralisierung”** als “Integrationsplattform”, abgekürzt PIZ , identifizieren. Diese Plattform ist nicht als Luxus zu betrachten, sondern als eine kritische Notwendigkeit.

Warum ist die PIZ essentiell als zentraler Punkt für Kontrolle und Überwachung?

- **Vereinheitlichung der Protokolle:**
  Verschiedene BMS können unterschiedliche Kommunikationsprotokolle verwenden. Ein Systemzentralisierer übersetzt und vereinheitlicht diese Protokolle und ermöglicht eine reibungslose Interaktion zwischen den Systemen.
- **Vereinheitlichung der semantischen Datenstruktur:**
  unterschiedliche BMS haben verschiedene Ausprägungen von Entitäten und verschiedene Entitäten.
- **Globale Sicht:**
  Bietet eine einheitliche Übersicht über alle Gebäude und Systeme unter seiner Verwaltung und vereinfacht so die Überwachung und Analyse.
- **Erleichterte Implementierung von KI:**
  Mit Daten, die von verschiedenen BMS über einen einzigen Punkt kanalisiert werden, wird die Implementierung und Nutzung von auf KI basierenden Lösungen handhabbarer und effektiver.

Direkte Vorteile der PIZ

- **Betriebliche Optimierung:**
  Durch die Fähigkeit, alle BMS über eine einzige Schnittstelle zu sehen und zu steuern, können Betreiber schnell auf Anforderungen reagieren und die Abläufe in Echtzeit optimieren.
- **Kostenreduzierung:**
  Durch Minimierung doppelter Anstrengungen und Optimierung der Energieeffizienz können signifikante Einsparungen bei den Betriebskosten erzielt werden.
- **Verbesserte Sicherheit:**
  Eine zentralisierte Verwaltung erleichtert die Implementierung einheitlicher Sicherheitsrichtlinien und das Monitoring potenzieller Bedrohungen oder Schwachstellen.

Perspektiven einer PIZ

- **Automatisches Lernen:**
  Die Plattform kann aus den Routinen der Gebäude lernen und Vorschläge zur Effizienzsteigerung machen.
- **Fortgeschrittene Prognosen:**
  Mit historischen und Echtzeitdaten kann sie präzise Vorhersagen treffen, wie zukünftiger Energieverbrauch oder Wartungsbedarf.
- **Intuitive Benutzeroberflächen:**
  Sie kann fortgeschrittene Benutzerschnittstellen bieten, die die Interaktion zwischen Betreibern und Systemen erleichtern.

Abschließend, in einer Welt, in der Gebäude immer "smarter" und vernetzter werden, treten PIZ als wesentliches Werkzeug hervor, um sicherzustellen, dass dieser Übergang reibungslos, effizient und sicher stattfindet. Mit der Hinzufügung von KI sind die Möglichkeiten für Optimierung und Innovation unbegrenzt.

3.3 Prozess

Der Prozess dient dazu, die Planung und Ausführung jedes Gebäudes systematisch und effektiv zu verwalten, um sicherzustellen, dass die Ergebnisse den Bedürfnissen, Qualitätsstandards und wirtschaftlichen Zielen entsprechen. Dies hilft auch bei der Integration von Anwendungsfällen und der Verbesserung der Datenqualität, was angesichts der wachsenden Bedeutung nachhaltiger Bauprojekte von großer Relevanz ist.

Im Flussdiagramm (Abb. 1) ist der vereinfachte Prozess der Aktivierung eines Gebäudes über eine PIZ dargestellt. Der Ausgangspunkt ist die Entscheidung, ein Gebäude auf der PIZ zu aktivieren, und der Endpunkt ist die Inbetriebnahme des Gebäudes.

3.4 Architektur der ‚'Go Live''

Das PIZ ist als ein Assistent zu betrachten, der es nicht nur den Nutzern digitaler Infrastrukturen ermöglicht, mit diesen zu interagieren und Bauprozesse und Geschäftsprozesse zu optimieren, sondern auch die Effizienz der Prozesse durch die Datenanalyse und ihre Anwendung in konkreten Anwendungsfällen zu steigern. Die Basis für die Vorhersagefunktionen eines modernen Gebäudes ist die intelligente Datenanalyse. Die dafür erforderlichen Daten werden in großer Menge von fast jedem Untersystem geliefert. Um im System gleichartig verarbeitet werden zu können, wird die Datenstruktur der Quelle normalisiert und in flexible Datengegenstände modelliert.

Im Folgenden wird die Architektur einer idealen Plattform beschrieben. Das PIZ muss skalierbar, modular und auf Mikroservices aufgebaut sein, die fortschrittliche Entwicklungs- und Bereitstellungspraktiken und eine fortschrittliche Messaging-Lösung für die Kommunikation zwischen Diensten nutzen.

Mikroservices sind ein architektonischer Ansatz, bei dem eine Anwendung als Sammlung kleiner, autonomer und modularer Dienste strukturiert ist. Jeder Dienst hat eine spezifische Funktion und führt eine bestimmte Aufgabe oder Aufgabengruppe aus.

Jeder Mikroservice sollte daher durch DevOps-Prozesse mithilfe der Continuous Integration und Continuous Delivery erstellt und als Container bereitgestellt werden. Es wird empfohlen, dass Mikroservices mit Apache Kafka kommunizieren.

Für die externe Kommunikation gibt es verschiedene Schnittstellen, zum Beispiel REST oder MQTT. In der PIZ müssen Daten in sogenannten Entitäten eingebunden werden. Diese Entitäten können dann strukturiert dargestellt werden, und es ist möglich, Datenpunkte schnell nach Gebäude, Etage, Anlage oder Raum zu filtern.

Als Beispiel siehe Abbildung 2, in der die Schnittstelle zwischen der PIZ und der Tridium Niagara-Plattform dargestellt ist, die auf TLS basiert und daher TCP als Vermittlungsebene verwendet.

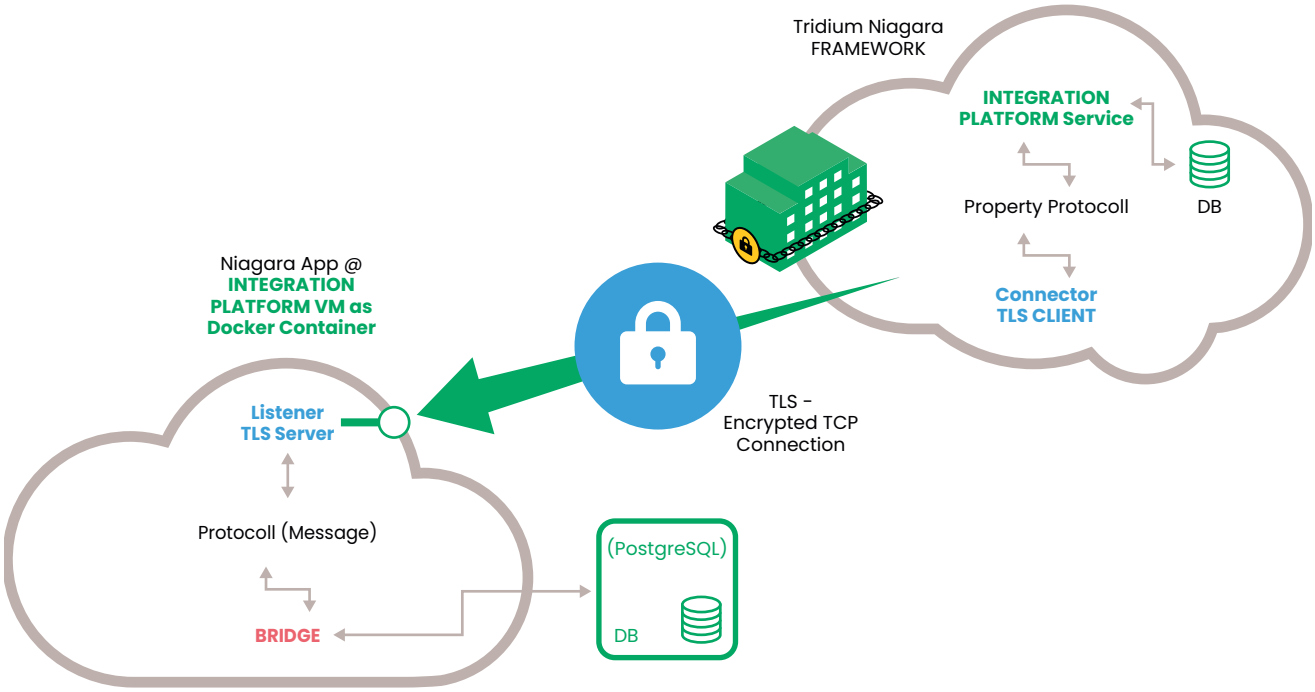

Abbildung 2. Beispiel für eine Schnittstelle zwischen Tridium Niagara und der Integrationsplattform

Als Authentifizierungsmethode wird ein Token verwendet, der von der PIZ mit einer Hash SHA256-Codierung gespeichert werden kann. Dies wird vom Niagara-System während der Verbindungsphase angefordert. Auf Anwendungsebene verwenden die Treiber ein proprietäres Protokoll, das für effizienten Datenaustausch optimiert ist.

Die Verbindung bleibt immer offen und ermöglicht einen bidirektionalen Datenaustausch. Über diese Schnittstelle ist es möglich, Datenpunkte von Tridium Niagara in die PIZ zu empfangen und umgekehrt auch Datenpunkte von der PIZ nach unten zu schreiben.

Auch Alarme können übertragen und bestätigt werden. Im Falle einer Verbindungsunterbrechung kann ein Indikator gesetzt werden, der anzeigt, dass die TCP-Verbindung mit der Niagara-Instanz unterbrochen wurde. Dieser Indikator kann als Alarm gesetzt werden. Darüber hinaus verwendet die Verbindung eine Ping-Methode, mit der ein fehlerhafter oder überlasteter Knoten erkannt werden kann, ohne dass dieser zuvor die TCP-Verbindung geschlossen hat. Auch das Fehlen des Ping-Signals kann als Alarm verwendet werden. Im Falle einer Verbindungsunterbrechung werden

1 First In, First Out, "Erstes Rein, Erstes Raus"

die Daten in Niagara auch in einem FIFO[1]-Puffer geschrieben. Seine Größe hängt von der durchschnittlichen Last und der Zeit ab, in der Daten möglicherweise im Puffer gespeichert werden müssen. Solange das System nicht an seiner Grenze ist, kann die Größe dieses Puffers frei gewählt werden. Nach einem Verbindungsverlust wird zum Beispiel alle 30 Sekunden versucht, eine Verbindung wiederherzustellen. Sobald die Verbindung mit der PIZ wiederhergestellt ist, wird dieser Puffer verarbeitet.

Eine gängige Methode zur Überwachung des Zustands einer Verbindung oder eines Geräts in Netzwerksystemen, einschließlich solcher, die TCP-Verbindungen verwenden, ist die Verwendung eines Lifebit. Ein Lifebit ist ein periodisches Signal, das von einem Gerät oder einer Anwendung gesendet wird, um dessen Betrieb und den aktiven Status der Verbindung anzuzeigen. Diese Überwachungsmethode ermöglicht es dem Empfänger, den Status des Senders zu überprüfen; wird das Lifebit innerhalb einer festgelegten Zeit nicht empfangen, geht man von einer Unterbrechung der Verbindung oder einem Ausfall des Senders aus. In Kontexten wie TCP-Verbindungen kann das Fehlen eines Lifebits als Alarm verwendet werden, um Unterbrechungen zu signalisieren. Der Einsatz des Lifebits bietet Vorteile in Bezug auf Einfachheit, Proaktivität bei der Erkennung von Verbindungsproblemen und Vielseitigkeit, was es zu einer effektiven Lösung macht, um die Gesundheit von Verbindungen in Systemen zu überwachen, in denen es wesentlich ist, mögliche Unterbrechungen zeitnah zu erkennen.

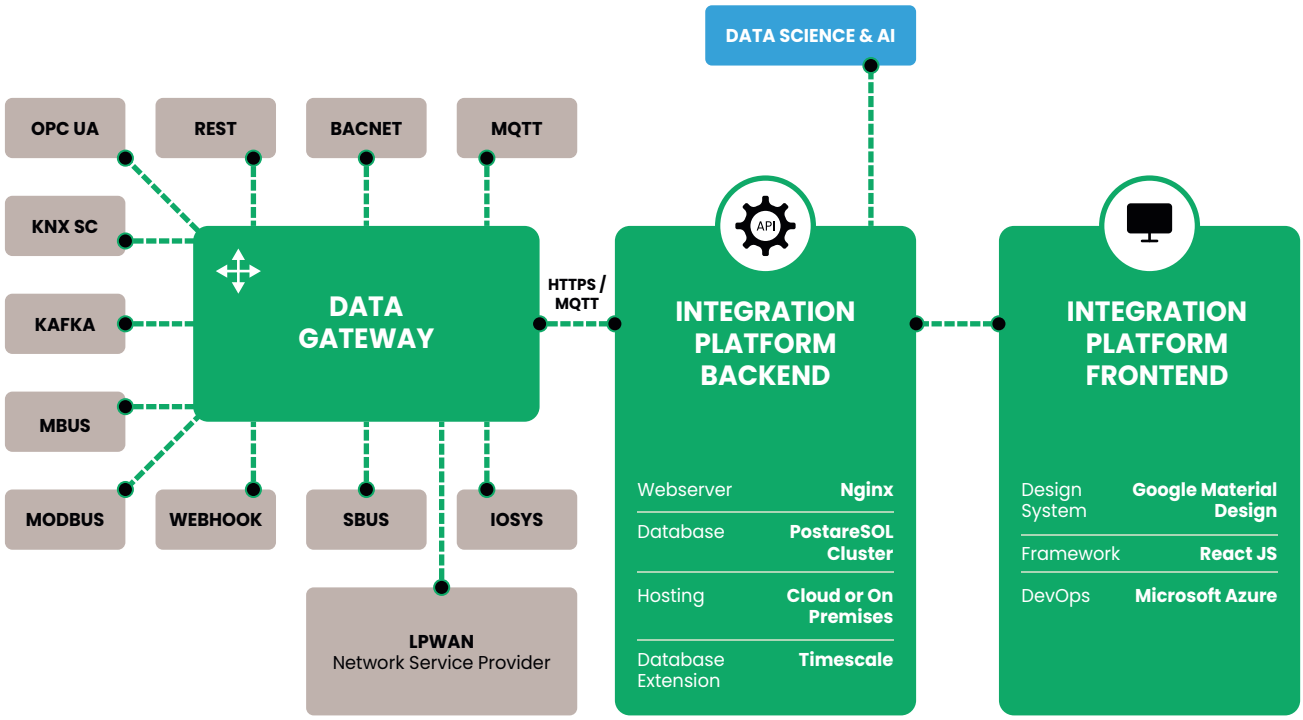

Abbildung 3. Architektur der Integrationsplattform

3.5 Dienstleistungen der PIZ

3.5.1 Kommunikationszertifikate

Die Public Key Infrastructure (PKI) spielt eine grundlegende Rolle im Kontext der Kommunikationssicherheit, insbesondere im Management von digitalen Zertifikaten, die als Werkzeuge für die Verschlüsselung und Identitätsprüfung in Kommunikationsverbindungen verwendet werden.
In der PKI ist der Einsatz von kryptografischen Schlüsselpaaren entscheidend, wobei der öffentliche Schlüssel über ein digitales Zertifikat verteilt und der private Schlüssel vom Benutzer sicher verwahrt wird. Es gibt zwei Hauptmethoden zum Erwerb dieser Zertifikate: Sie können über eine kostenlose Zertifizierungsstelle wie Let's Encrypt"[2] erworben werden, oder sie können von Individuen oder Organisationen generiert werden, wie zum Beispiel vom Verwalter des BMS.

3.5.2 Datenbank

Für die Speicherung, Verwaltung und Analyse von Daten sollte eine PostgreSQL-Datenbank verwendet werden. Diese kombiniert die Vorteile eines relationalen Datenmodells mit flexiblen JSON-Objekten, ideal für Analysen und den Einsatz in IoT-Anwendungen. Hohe Zuverlässigkeit und Leistung garantieren den Betrieb als zentrales Element einer Plattform
für intelligente Gebäude.

3.6 Visualisierung

Die Visualisierung der PIZ muss modern und konsistent sein sowie Technologien und Designprinzipien auf dem neuesten Stand verwenden, um eine optimale und an die spezifischen Bedürfnisse des Projekts angepasste User Experience zu gewährleisten.

Folgende Komponenten helfen dabei:

- **React-Framework:**
  ist eine von Facebook entwickelte Open-Source-JavaScript-Bibliothek zum Erstellen von Benutzeroberflächen. Sie basiert auf Komponenten, was bedeutet, dass die Benutzeroberfläche in wiederverwendbare und unabhängige Teile (Komponenten) unterteilt ist, die ihren eigenen Zustand verwalten.

- **Material UI:**
  ist eine Sammlung von React-Komponenten, die das Material Design[3] von Google implementieren.

2 letsencrypt.org

3 m3.material.io

— **Progressive Web App - PWA:**
ist eine Art von Webanwendung, die auf jeder Plattform funktionieren soll, die einen Standard-browser verwendet.

— **Integration von Visualisierungen des BMS -Frameworks:**
z.B. Tridium Niagara ist wahrscheinlich das Framework, das die PIZ integriert.

— **Entwicklung von benutzerdefinierten Widget:**
auch als Tiles bekannt, sind Interface-Elemente, die Informationen anzeigen oder spezifische Interaktionen anbieten.

Schnittstellen zu externen Systemen Verschiedene externe Systeme können verbunden werden, wie zum Beispiel IoT Central, ein verwalteter Dienst von Microsoft Azure[4], der über Webhook konfiguriert werden kann.

4 azure.microsoft.com

4. Die Struktur des Systems

Die Topografie in der Abbildung 4 wurde zu Darstellungszwecken vereinfachtet erstellt, sie ist flexibel und skalierbar.

4.1 Das Gateway

Das Gateway ist ein kritisches Gerät, das als Schnittstelle zwischen dem BMS und der PIZ dient, indem es das Kommunikationsprotokoll MQTT verwendet. Für seine korrekte Funktion benötigt das Gateway eine spezifische, von den Gebäudeadministratoren genehmigte IPAdresse.

Verbindungen und Konfigurationsdateien

Das Gateway verfügt über zwei wesentliche Verbindungen:

1. **Verbindung zum Internet** für die Kommunikation mit dem PIZ-System.
2. **Verbindung zum Gebäudenetzwerk** für allgemeinen Zugang.

Es gibt drei Hauptkonfigurationsdateien:

- **Eine Datei** definiert die Zugangspunkte zu den Daten des Steuerungssystems.
- **Eine zweite Datei** spezifiziert die Datenetikettierungsmethoden für das MQTT-System.
- **Eine dritte Datei**, genannt „Dispatch“, fungiert als Karte für die Datenzuordnung.

ZERTIFIKATE		
Typ	**Vorteile**	**Nachteile**
Kostenlose Zertifizierungsstelle: Let's Encrypt	Keine Kosten; Automatische Erneuerung der Zertifikate; Externes Vertrauen und Konformität: Zertifikate bieten Vertrauenswürdigkeit und Einhaltung von Sicherheitsstandards, indem sie die Domaininhaber validieren; Schnelle und unkomplizierte Installation;	Ermöglicht nicht das Hinzufügen spezifischer Details; Die URL muss öffentlich zugänglich sein; Öffentliche Exposition und Automatisierungsrisiken: Das Erfordernis einer öffentlichen Domäne kann für interne Systeme problematisch sein; Automatisierungsfehler könnten Sicherheitslücken öffnen;
Personalisierte Unternehmenszertifikate	Größere Flexibilität: alle Details des Zertifikats können angepasst werden; Einheitlichkeit: das Unternehmen kann eine einzige CA verwenden; Möglichkeit, selbstgenerierte Zertifikate zu verwenden; Vollständige Kontrolle und Datenschutz: Unternehmen haben die vollständige Kontrolle über die Zertifikatserstellung und -verwaltung, was die interne Sicherheit verbessert; es besteht keine Notwendigkeit, interne Dienste für eine externe CA offenzulegen, was die Vertraulichkeit schützt;	Müssen manuell erneuert werden; Es ist notwendig, die Ablaufdaten zu verfolgen; Erfordern aufmerksamere Wartung; Begrenztes Vertrauen und Sicherheitsmanagement: Selbstsignierte oder intern erstellte Zertifikate werden von externen Browsern möglicherweise nicht automatisch akzeptiert, was zusätzliche Konfigurationen erfordert; ohne die Infrastruktur einer dedizierten CA müssen Unternehmen ihre Sicherheitsmaßnahmen selbstständig auf dem neuesten Stand halten;

Tabelle 1. Vergleich zwischen Let's Encrypt und personalisierten Unternehmenszertifikaten

Installations- und Funktionalitätstests

Während der Installation werden kritische Tests durchgeführt, um sicherzustellen, dass das Gateway korrekt funktioniert, ohne vorhandene Daten zu überschreiben.

Test 1: Überprüfung der Anzeige und Schutz vor Überschreibung

- **Ziel:** Sicherstellen, dass das Gateway Werte korrekt anzeigt und dass schreibbare Datenpunkte beim Verbindungsaufbau nicht überschrieben werden.
- **Verfahren:** Es wird eine begrenzte Konfiguration geladen und überprüft, dass das Gateway nur die notwendigen Schreibrechte hat.
- **Erwartetes Ergebnis:** Die Werte der Datenpunkte werden korrekt angezeigt, ohne überschrieben zu werden.

Test 2: Bestätigung der Datenerfassung und Abwesenheit von Broadcast

- **Ziel:** Überprüfen, dass das Gateway alle Daten liest, ohne unerwünschte Broadcast-Übertragungen zu starten.
- **Verfahren:** Es wird eine Konfiguration angewandt, die dem Gateway nur Lesebetrieb erlaubt.
- **Erwartetes Ergebnis:** Alle Daten sind lesbar, ohne dass das Gateway Broadcast-Übertragungen startet, wie durch die Systemprotokolle verifiziert.

Positive Ergebnisse dieser Tests gewährleisten, dass das Gateway zuverlässig innerhalb der IT-Infrastruktur des Gebäudes arbeitet.

4.2 Dienst für Künstliche Intelligenz - ECS

Die ECS sind dafür ausgelegt, sich mit der vorhandenen Technologie zu integrieren, mit besonderem Schwerpunkt auf der Interaktion mit standardisierten IT-Protokollen und IP-basierten Verbindungen. Die Spezifikationen mussen entsprechend den Bedürfnissen und Eigenschaften jedes Gebäudes angepasst werden. Obwohl allgemein die KI Daten in einem zentralen HUB zur Optimierung der Latenzzeiten zentralisiert, kann sie den Zugriff über verschiedene globale Knoten verteilen und dabei den Datenschutz gewährleisten.

4.3 Topologie Grundlegende Elemente der ECS-Architektur

- **Datenbank:**
  Einsatz fortschrittlicher Datenbanken zur Verwaltung und Speicherung von Benutzerdaten, Gebäudeinformationen und historischen Daten über Energiemuster.

- **Backend & Schnittstelle:**
  Eine RESTful API dient als Kommunikationsbrücke zwischen verschiedenen Diensten und Anwendungen. Eine intuitive Benutzeroberfläche ermöglicht den Zugang und die Interaktion mit den Hauptfunktionen der ECS.

- **Lastausgleich:**
  Ein Load Balancer stellt sicher, dass Anfragen gleichmäßig auf die Server verteilt werden, um eine zeitnahe Antwort zu garantieren.

- **AI CORE:**
  Das Herzstück des Systems, zuständig für Analyse, Lernen und Optimierung. Ein Client-Modul der ECS interagiert mit anderen Diensten und unterstützt eine Vielzahl von Protokollen. Im Gegensatz zu traditionellen BCT , die feste Zeitpläne und einfache Messungen wie die Außentemperatur verwenden, implementiert das ECS fortgeschrittene Optimierungsfunktionen wie:

  > **Prädiktive Steuerung:**
  > Technologie, die Temperaturtrends vorwegnimmt und Operationen wie das Öffnen oder Schließen von Ventilen vor herkömmlichen Systemen regelt. Sie basiert in der Regel auf MPC, kann aber auch Steuerungen auf Basis von Fuzzy logic, Neuronalen Netzwerken und anderen Algorithmen beinhalten.
  >
  > **Optimale Temperaturwerte:**
  > Das ECS bestimmt die ideale Vorlauftemperatur für das Gebäude, basierend auf Daten wie den aktuellen und vorhergesagten Wetterbedingungen und der Gebäudenachfrage.
  >
  > **Anomalieerkennung und Betriebszeitanalyse:**
  > Kontinuierliche Überwachung der Geräte auf Anomalien und Ineffizienzen mit Intervention bei Problemen.

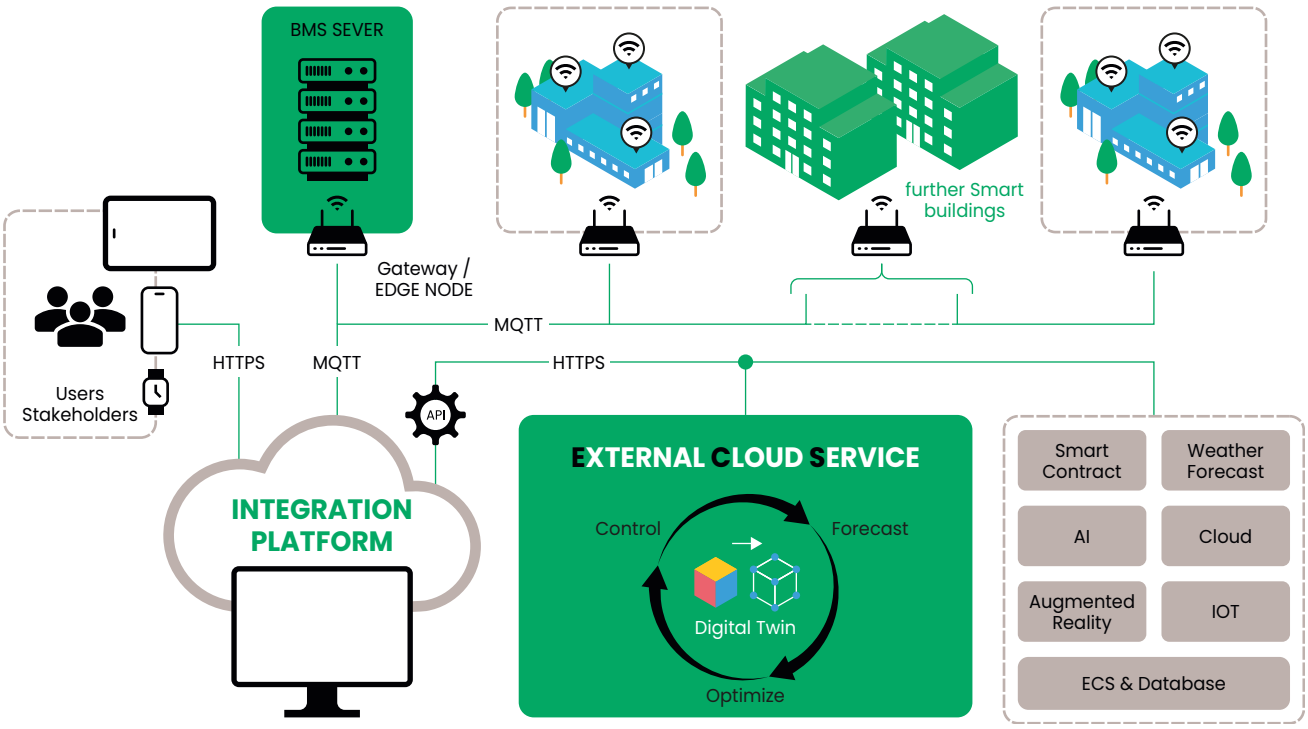

Abbildung 4. Systemstruktur

Sicherheit und Überwachung

Die Datenintegrität wird durch Firewalls und fortschrittliche Sicherheitssysteme gewährleistet. Spezialisierte Module überwachen ständig die Aktivität der KI und stellen sicher, dass sie ordnungsgemäß funktioniert und Anomalien meldet.

Künstliche Intelligenz bietet eine fortschrittliche und anpassbare Lösung zur Verbesserung der Energieeffizienz und Gebäudeverwaltung, indem sie die Kraft der Datenanalyse und des maschinellen Lernens nutzt.

AI CORE und Energieoptimierung

Der AI CORE konzentriert sich auf die Energieoptimierung und arbeitet in Synergie mit den bestehenden BCT . Er sammelt und analysiert Daten von den Gebäudegeräten, insbesondere vom HVAC-System, mit dem Ziel, die Energieeffizienz durch Folgendes zu verbessern:

- **Echtzeitüberwachung:**
  Stellt Details über die Gebäudeoperationen in Echtzeit zur Verfügung und speichert Daten für zukünftige Referenzen.

– **Adaptive Steuerung:**
Passt die Einstellungen der HVAC-Geräte basierend auf Benutzerverhaltensmodellen und -präferenzen sowie externen Umweltparametern an.

– **Automatisierung:**
Automatisiert Routineaufgaben wie das Ein- und Ausschalten von Geräten basierend auf prädiktiven Algorithmen und flexibler Programmierung.

Die Funktionalität des ECS basiert stark auf seiner Fähigkeit, reibungslos mit den Schlüsselkomponenten der BCT zu interagieren. Dies umfasst eine Reihe von Ressourcen wie Sensoren, Aktuatoren und spezifische Elemente wie Heiz- und Kühlsysteme, Lüftungseinheiten, Wasserwerke und zentrale Anlagen, um nur einige zu nennen. Die Kommunikation mit dem BCT wird durch die PIZ erleichtert, wie in Abbildung 5 dargestellt, unter Verwendung spezifischer APIs. Um die Sicherheit und Integrität der Daten zu gewährleisten, müssen alle Übertragungen mit TLS verschlüsselt werden, um die Informationen während der Übertragung zu schützen.

4.4 Schlüsselkonzepte des ECS

4.4.1 Datenabfrage über PIZ

Die API-Schnittstelle der PIZ liefert Gebäudeinformationen. Durch eine Anfrage an den spezifizierten Endpoint kann eine vollständige Liste der Daten jedes Gebäudes abgerufen werden. Diese Daten sind hierarchisch strukturiert, beginnend mit dem Gebäude, das Stockwerke enthält, die wiederum Räume mit spezifischen Daten enthalten. Es gibt eine Beziehung zwischen übergeordneten und untergeordneten assets, die über die ID parentLocationalAsset verwaltet wird.

4.4.2 Erstellung digitaler Gebäudemodelle

Mit den gesammelten Daten wird eine spezifische Datenstruktur für jedes Gebäude entwickelt. Diese Strukturen werden dann in Modelle im JSON-Format übersetzt. Die Modelle enthalten Details zum Gebäude, spezifische Konfigurationen, Betriebsdetails und externe Daten. Es gibt zwei Haupttypen von Daten: solche, die mit spezifischen Entitäten verbunden sind (z. B. Controller) und solche, die nicht verbunden sind. Beide Kategorien enthalten zwei Haupttypen von Daten: Sensoren (nur lesen) und Aktuatoren (änderbar). Nachdem diese Daten organisiert sind, wird erneut eine Schnittstelle zur PIZ hergestellt, um weitere Informationen und Trends abzurufen, die dann für detaillierte Analysen verwendet werden.

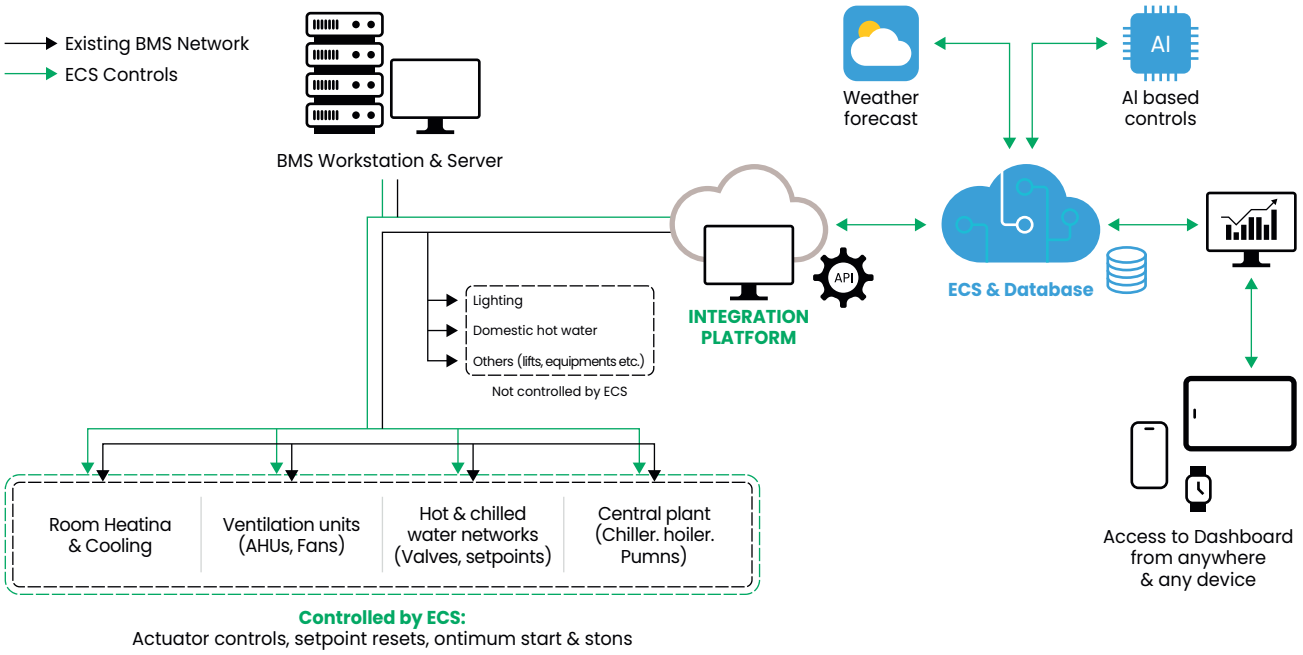

Abbildung 5. Topologie ECS

4.4.3 Benutzerverwaltung und Authentifizierung

Die Erstellung von Benutzerkonten sollte nur von autorisiertem Personal gehandhabt werden. Nach der Erstellung kann der Benutzer den Aktivierungsprozess und die Passworteinrichtung abschließen, z. B. per E-Mail, und einen Zugriffskontrolle durch ACLs durchführen.

4.4.4 Dashboard

Ein Dashboard ist unerlässlich, um eine Schnittstelle zum Überwachen des Dienstes und der Energieberichte bereitzustellen, jedoch ohne direkte Steuerung des Gebäudes zu ermöglichen. Die Funktionen sollten hauptsächlich mit der Überwachung des Dienststatus verbunden sein. Die Zugriffskontrolllisten bestimmen die Benutzerberechtigungen. Sobald die entsprechenden Berechtigungen erteilt wurden, kann der Benutzer verschiedene Optionen haben, wie Aktivierung, Deaktivierung oder Dry-run Modus. Das Dashboard dient als zentrale Benutzerschnittstelle und zeigt eine Übersicht über die Gebäudeleistung. Die Schlüsselfunktionen umfassen:

- Echtzeitüberwachung
- Anzeige des Gerätestatus
- Energieberichte
- Supportanfragen, Vorschläge und Empfehlungen

4.4.5 Datenarchivierung und -erhaltung

Zwei Hauptdatenbanken sind funktionaler:

1. **Die erste Datenbank** ist für unstrukturierte Daten wie Konfigurationen, Benutzerdaten, Berichte und Logs konzipiert. Diese Datenbank erfordert keinen häufigen Zugriff und wird über eine Langzeit-Speicherlösung verwaltet.
2. **Die zweite Datenbank** ist für die hochgeschwindigkeits Speicherung und Analyse von Echtzeit-Sensordaten optimiert, die häufigen Zugriff und hohe Lese-/Schreibgeschwindigkeiten erfordern.

Zusammenfassend ist die Architektur des ECS eine hervorragende Synergie zwischen der PIZ -Schnittstelle, dem digitalen Modell und dem Dashboard, unterstützt durch solide Datenarchivierungsstrategien. Jede Komponente ist so konzipiert, dass sie sich nahtlos integriert und eine optimale Endbenutzererfahrung und effiziente Energieverwaltung in Gebäuden gewährleistet.

5. Reengineering & Datenmanagement

5.1 Daten-Reengineering

Das Daten-Reengineering, durchgeführt vom PIZ , ist entscheidend bei der Implementierung von Softwarelösungen in bestehenden Systemen. Es umfasst die Analyse, Umgestaltung und Reintegration von Daten in das System, unter der Leitung des Integrators, um die Übereinstimmung mit den neuen Anforderungen und Funktionen der Software sicherzustellen.

5.2 Ziele:

- Durch den Integrator erfolgt die Optimierung der Datenqualität, um die Genauigkeit und Effizienz der Operationen zu steigern.
- Sicherstellung der Konsistenz und Homogenität der Daten über alle Systeme, inklusive des BMS und ECS.
- Identifizierung und Lösung von Dateninkonsistenzen, vorrangig durch den PIZ in Zusammenarbeit mit dem BMS.

5.3 Phasen des Reengineerings:

1. **Datenanalyse:**
   Der PIZ untersucht die aktuelle Datenarchitektur, identifiziert Quellen, Formate und Qualität.
2. **Datenbereinigung:**
   Korrektur inkonsistenter, doppelter oder fehlerhafter Daten, typischerweise durch das BMS unterstützt.
3. **Transformation:**
   Anpassung der Daten an neue Strukturen oder Formate, erforderlich für die Integration in die KI-basierten Systeme.
4. **Migration:**
   Übertragung der optimierten Daten in das ECS durch den PIZ .
5. **Überprüfung:**
   Sicherstellung der korrekten Migration durch Vergleich mit der Originalquelle, üblicherweise eine Aufgabe des Integrators.

5.4 Checkliste für das Rollout

Eine detaillierte Rollout-Checkliste, erstellt vom Integrator für jedes Gebäude, ist wesentlich, um alle kritischen Phasen effektiv zu überprüfen und abzuschließen. Dies umfasst die anfängliche Bewertung, Vorbereitung, Implementierung und das nachfolgende Monitoring, oft in Zusammenarbeit mit dem BMS und unter Verwendung des Gateways für Netzwerkkommunikation.

6. Liste der Datenpunkte / Objekte

Bei der Implementierung einer Automatisierungslösung ist es wesentlich, eine klare und strukturierte Sicht auf die im System verfügbaren Daten zu haben. Die Liste der Datenpunkte, oft in einem standardisierten Format wie dem Engineering Data Exchange - EDE bereitgestellt, bietet diese Klarheit.

6.1 Eigenschaften der Datenpunkte:

Typ:

- **Analog:** Stellt kontinuierliche Werte dar (z.B. Temperatur).
- **Digital:** Stellt ON/OFF Zustände oder diskrete Werte dar.
- **Ausgang:** Werte oder Befehle, die an Geräte gesendet werden.
- **Eingang:** Werte oder Signale, die von Geräten empfangen werden.
- **Wert:** Daten, die spezifische Messungen oder Konfigurationen darstellen.

Schreibfähigkeit:

- **Nur Lesen:** Diese Datenpunkte können nicht geändert werden und liefern statische Informationen oder Messungen.
- **Schreiben:** Diese Datenpunkte können geändert werden, um Befehle zu senden oder Konfigurationen zu ändern.

Namen:

- **Objektname:** Eine kurze Kennzeichnung, die den Datenpunkt identifiziert (z.B. Temperatur_Raum1”).
- **Beschreibung:** Eine detaillierte Beschreibung des Datenpunkts, oft mit weiteren Details zu seiner Rolle oder seinem Standort (z.B. Temperatursensor im Hauptkonferenzraum”).

Quelle:

- **IP-Adressen:** Gibt die Netzwerkadresse des Geräts an.
- **Physische Adresse:** Gibt den physischen Standort des Geräts innerhalb des Gebäudes an.
- **Register:** Objekt ID oder sostige Bus-Addresse

6.2 Strukturänderungen: Aktualisierungen

6.2.1 PIZ-Aktualisierungen

Aktualisierungen und neue Versionen können über SSH-Verbindungen implementiert werden. Jeder Mikroservice wird durch DevOps-Prozesse unter Verwendung von Continuous Integration und Continuous Delivery entwickelt und als Docker-Container bereitgestellt. Die Aktualisierung erfordert das Update aller Docker-Container.

Gründe für die Aktualisierung

- **Optimierung der API-Funktionalität:**
  Die API wird so optimiert, dass gelöschte Assets nicht mehr angezeigt werden.
- **Effiziente Log-Verwaltung:**
  Um zu verhindern, dass die Festplatte mit Logdateien überladen wird, werden geeignete Maßnahmen getroffen.
- **Aktualität und Leistung:**
  Mit der Aktualisierung wird die PIZ auf den neuesten Stand gebracht, um aktuelle Funktionen und optimierte Leistung zu gewährleisten. Risiken der Aktualisierung
- **Funktionsverlust eines Containers:**
  Es besteht das Risiko, dass ein oder mehrere Container nach der Aktualisierung nicht mehr vollständig funktionieren.
- **Inkompatibilitäten zwischen den Container:**
  Die Aktualisierung könnte zu Inkompatibilitäten zwischen den verschiedenen Containern führen. Maßnahmen zur Risikovermeidung
- **Server-Duplizierung:**
  Um die Risiken zu minimieren, wird der Server dupliziert und das Update in einer sicheren Testumgebung durchgeführt.
- **Umfangreiche Tests:**
  Alle Funktionen, einschließlich der MQTT-Schnittstellen, BMS-Apps, API-Zugänge usw., werden auf dem Testserver gründlich getestet und validiert.

– **Analyse und Problembehebung:**
  Im Falle von Problemen werden diese auf dem Testserver erkannt, analysiert und behoben, bevor das Live-System aktualisiert wird. Dies minimiert Ausfallzeiten und stellt sicher, dass die Plattform in ihrer neuesten Version optimal funktioniert.

6.2.2 Gateway-Aktualisierungen

Das Gateway ist ausschließlich für die Netzwerkverbindung vorgesehen, mit den in den technischen Spezifikationen des Geräts angegebenen Verbindungswerten. Weder Hardware noch Software stellen an sich eine direkte Gefahr dar. Allerdings können sie in ihrer Funktion zwischen den Netzen in der Infrastruktur signifikant die Interaktion der Netzwerkkomponenten „stören“, daher ist es angebracht, die Firmware auf dem neuesten Stand zu halten. Ein Firmware-Update kann mehrere Minuten dauern. Während des Updates kann das Gateway seine Funktion im Gesamtsystem nicht ausführen. Es sind entsprechende Vorkehrungen in der Anlage / Infrastruktur zu treffen. Wenn die Stromversorgung während des Update-Prozesses unterbrochen wird, könnte das Betriebssystem beschädigt werden. Vor dem Update wird empfohlen, eine Datensicherung durchzuführen. Dies ermöglicht es, jederzeit zu einer funktionierenden Konfiguration zurückzukehren.

7. SICHERHEIT

Der Begriff Sicherheit ist sicherlich sehr breit gefächert; im Folgenden wird er anhand von drei grundlegenden Aspekten analysiert:

1. **Datenschutz und Privatsphäre:**
   Dies bezieht sich auf den Schutz von Informationen innerhalb des Systems, um unbefugten Zugriff zu verhindern und die Vertraulichkeit der Daten zu gewährleisten. Dies betrifft hauptsächlich Sicherheitsmaßnahmen zum Schutz der Daten, Verschlüsselungsmechanismen, Authentifizierungsprotokolle, Datenschutzrichtlinien und die Einhaltung von Vorschriften.

2. **Integrität kritischer Funktionen:**
   Stellt sicher, dass durch Eingriffe in bestimmte Funktionen des BMS keine anderen als wesentlich betrachteten Funktionen beeinträchtigt oder gestört werden, oder dass die Sicherheit von Personen, wie z. B. Brandschutz, nicht gefährdet wird. Dies umfasst Verfahren und Protokolle, um Interferenzen zwischen Funktionen zu vermeiden, Funktionstests, Isolierung kritischer Funktionen und Echtzeit-Überwachung.

3. **Robustheit, Redundanz und System-Backup:**
   Betrifft die Fähigkeit des Systems, Ausfälle und Unterbrechungen zu widerstehen und einen ununterbrochenen und zuverlässigen Betrieb durch Redundanzund Backup-Mechanismen sicherzustellen. Dies umfasst Backup-Strategien, Redundanz der Architektur, Überwachung und Alarmierung bei Ausfällen, Wiederherstellungs- und Wiederanlaufpläne und regelmäßige Tests. Sicherheit muss in jedem Kontext spezifisch vertieft werden; im Folgenden werden nur die besten Praktiken bereitgestellt, die sicherlich nicht in jeder Situation erschöpfend sind.

7.1 Sicherheit und Datenschutz bei der Integration von BMS und ECS

In einer Ära zunehmender Konnektivität sind Sicherheit und Datenschutz zu grundlegenden Anliegen geworden. Während die ECS neue Möglichkeiten zur Optimierung und Verbesserung des Gebäudemanagements bieten, bringen sie auch neue Herausforderungen im Hinblick auf den Datenschutz und die Sicherheit der Infrastruktur mit sich. Die häufigsten aufkommenden Risiken sind:

- **Datenvulnerabilität:**
  Die KI hängt von großen Datenmengen ab, um effektiv zu funktionieren. Diese Daten können, wenn sie nicht angemessen geschützt sind, zu Zielen für Cyberangriffe werden.
- **Gezielte Angriffe:**
  Mit der zunehmenden Abhängigkeit von automatisierten Systemen könnten Gebäude Ziel von Angriffen werden, die darauf abzielen, Automatisierungssysteme zu stören oder zu manipulieren.
- **Integration veralteter Systeme:**
  Viele Gebäude nutzen immer noch ältere BMS, die möglicherweise nicht unter Berücksichtigung moderner Sicherheitsbedenken entwickelt wurden.

Die zu ergreifenden vorbeugenden Sicherheitsmaßnahmen sind im Allgemeinen:

- **Verschlüsselung:**
  Alle Daten, die zwischen den BMS, den PIZ und den ECS übertragen werden, müssen verschlüsselt sein, um sicherzustellen, dass sie während der Übertragung nicht abgefangen oder manipuliert werden können.
- **Zwei-Faktor-Authentifizierung:**
  Um sicherzustellen, dass nur autorisierte Personen Zugriff auf die Verwaltungssysteme haben, ist die Implementierung einer Zwei-Faktor-Authentifizierung unerlässlich.
- **Regelmäßige Updates:**
  Das gesamte System muss regelmäßig aktualisiert werden, um vor bekannten und potenziellen Schwachstellen zu schützen.

Das Management des Datenschutzes und die Einhaltung der Vorschriften sind eine Pflicht sowie eine Verpflichtung. Im Folgenden sind einige Best Practices aufgeführt, die angewendet werden sollten:

- **Information:**
  Es ist entscheidend, sich über die lokalen und internationalen Datenschutzgesetze und -vorschriften, wie die GDPR[5], General Data Protection Regulation, in Europa, zu informieren und diese einzuhalten.
- **Minimale Datensammlung:**
  Wo möglich, sollten Systeme nur die für ihren Betrieb notwendigen Daten sammeln, wodurch die Exposition gegenüber möglichen Verstößen begrenzt wird.
- **Datenschutzerklärung:**
  Benutzer und Bewohner von Gebäuden müssen darüber informiert werden, welche Daten gesammelt werden, wie sie verwendet werden und welche Sicherheitsmaßnahmen in Kraft sind.

In jedem Sicherheitskontext bleibt die goldene Regel der "Awareness", die sich in folgendem niederschlägt:

- **Schulung des Personals:**
  Das für die Verwaltung und Wartung der Systeme verantwortliche Personal muss eine angemessene Schulung in Cybersicherheit erhalten.
- **Aufklärung:**
  Die Bewohner und Benutzer der Gebäude sollten über die Risiken und die ergriffenen Maßnahmen zum Schutz ihrer Daten und ihrer Sicherheit informiert werden.

Während die Integration von ECS enorme Vorteile in Bezug auf Effizienz und Funktionalität bietet, ist es von entscheidender Bedeutung, die Herausforderungen im Zusammenhang mit Sicherheit und Datenschutz proaktiv anzugehen. Nur mit einem ganzheitlichen und informierten Ansatz kann sichergestellt werden, dass die Automatisierung von Gebäuden sicher und unter Wahrung der Privatsphäre der Nutzer voranschreitet.

5 eur-lex.europa.eu/eli/reg/2016/679/oj

7.2 Integrität kritischer Funktionen: Sicherheitsmaßnahmen

Sicherheit im Bereich des Gebäudemanagements und der Automatisierung ist eine unerlässliche Priorität, und neue Technologien müssen sicher und effizient implementiert werden.

Sicherheitsfunktionen und Ausfälle

Sicherheitsfunktionen der Automatisierungspyramide dürfen nicht durch Anschluss eines übergeordneten Systems umgangen werden. Dies beinhaltet Brandschutz, Einbruchschutz, Zutrittskontrolle, Notbeleuchtung, Videoüberwachung, Notstromversorgung, IT-Sicherheit, Frostschutz und manuelle Bedienbarkeit von Sicherheits- und Automatisierungskomponenten.

Die Implementierung von Sicherheitsfunktionen sollte vom entsprechenden Integrator durchgeführt werden. Also in diesem Bereich müssen im BMS generierte Werte im BMS aufgezeichnet werden und im Drittsystem generierte Werte sollten im Drittsystem gespeichert werden.

Nach einer Kommunikationsunterbrechung mit einem Gebäude muss das BMS seine übliche Regulierungs- und Steuerfunktion mit den voreingestellten Werten wieder aufnehmen.
Diese Werte müssen lokal gespeichert sein, damit sie im Falle einer Verbindungsunterbrechung sofortverfügbar sind.

Nach einem Stromausfall sollten sich die Verbindungen zwischen allen BMS, den PIZ und den ECS automatisch wiederherstellen.

7.3 Systemrobustheit

7.3.1 Steuerungsalgorithmen und Sicherheit

Das HVAC-System spielt eine entscheidende Rolle bei der Aufrechterhaltung eines komfortablen und sicheren Gebäudeinnenklimas. Wie jedes mechanische System birgt es jedoch Risiken, wenn es nicht richtig verwaltet wird. Das Steuerungssystem fungiert als Hauptregler für das HVAC-System, indem es dessen Funktionen überwacht und reguliert. Das ECS, das als zusätzliche Steuerungsebene über dem Gebäudesteuerungssystem fungiert, ergänzt dieses und stellt sicher, dass alle eingebauten Sicherheitsfunktionen, wie z.B. Brandschutz und Frostschutz, aktiv bleiben.

Wenn das ECS ein Problem oder eine Anomalie im HVAC-System feststellt, wie Überhitzung oder Stromausfall, wird vom BMS lokal die notwendigen Sicherheitsfunktionen gewährleistet.
Dieser Mechanismus stellt sicher, dass das HVAC-System immer die angemessenen Sicherheitsmaßnahmen bei Fehlfunktionen oder Ausfällen ergreifen kann.

Wenn ein Gebäudeoperator die Einstellungen des HVAC-Systems manuell ändern muss, während das ECS in Betrieb ist, kann dies über die Prioritätenliste des BMS erfolgen. Dies gewährleistet, dass die Gebäudebetreiber vollständige Flexibilität und Kontrolle über das System haben.

7.3.2 Verfahren bei Alarmen

Das ECS ist darauf ausgelegt, jede Anomalie oder Alarm, der in den Gebäudesystemen auftreten könnte, effektiv zu handhaben. Im Falle eines Alarmsignals:

- **Sofortige Benachrichtigung des Bedieners:**
  Jeder erkannte Alarm muss dem Bediener sofort über das Dashboard, E-Mail oder Push Benachrichtigungen, je nach voreingestellten Einstellungen, mitgeteilt werden.
- **Klassifizierung des Alarms:**
  Das ECS klassifiziert Alarme nach ihrer Schwere. Kritische Alarme, die sofortige Aufmerksamkeit erfordern, werden hervorgehoben und dem Bediener zur Kenntnis gebracht.
- **Automatische Rückkehr zum BMS:**
  Im Falle kritischer Alarme muss das ECS die Kontrolle automatisch an das BMS übertragen, um die Sicherheit des Gebäudes und seiner Bewohner zu gewährleisten.

7.3.3 Verfahren bei Ausfällen

Im Falle eines Systemausfalls, wie einer defekten Pumpe oder eines fehlerhaften Sensors:

- **Fehleridentifikation:**
  Das ECS identifiziert und lokalisiert den Fehler im System und stellt dem Bediener Details zur Verfügung.
- **Bypass-Strategie:**
  Wenn möglich, sollte das ECS eine vorübergehende Bypass-Strategie umsetzen, um die Betriebsfähigkeit des Gebäudes bis zur Behebung des Fehlers aufrechtzuerhalten.
- **Benachrichtigung und Aufzeichnungen:**
  Der Bediener muss über den Fehler informiert werden und das ECS muss ein Ereignisprotokoll führen, um die Diagnose und Problembehebung zu erleichtern. Um eine sichere und effiziente Verwaltung zu gewährleisten, ist es entscheidend, dass die Bediener angemessen geschult und auf dem neuesten Stand gehalten werden.

7.4 Backup und Wiederherstellung

7.4.1 Backup-Verfahren

Die Datensicherheit ist von größter Bedeutung, und es müssen robuste und regelmäßige Backup-Verfahren implementiert werden. Die Systeme müssen automatische Datenbackups auf sicheren und verschlüsselten Servern durchführen, um sicherzustellen, dass alle Informationen immer verfügbar sind, falls Unterbrechungen oder Verluste auftreten.

- **Gespeicherte Daten:**
  Neben den täglichen Vorgängen sollten die Backups Audit-Logs, benutzerdefinierte Konfigurationen, Benutzerprofile und andere kritische Daten umfassen.
- **Erfolgsbenachrichtigung:**
  Nach jedem Backup ist es gute Praxis, einen Bestätigungsbericht zu erstellen, um eventuelle Probleme im Prozess zu überprüfen.

Im Falle einer notwendigen Wiederherstellung aus einem Backup sollte eine detaillierte Datenüberprüfung durchgeführt werden, um deren Konsistenz und Richtigkeit sicherzustellen, und die Stakeholder sollten über die Wiederherstellung informiert werden, mit Details über den Grund und das Ergebnis des Prozesses.

7.4.2 Audit-Trail

Die Implementierung eines Audit-Trails, einer systematischen Aufzeichnung von Aktivitäten, Transaktionen oder Änderungen innerhalb eines Informationssystems, ist eine bewährte Praxis. Dieses Register hilft, eine vollständige und nachvollziehbare Chronologie aller relevanten Aktionen und Ereignisse, die innerhalb eines Systems auftreten, zu erstellen.

Funktionen eines Audit-Trails:

- **Nachverfolgbarkeit:**
  Ermöglicht es, Änderungen und Aktivitäten auf ihren Ursprung zurückzuführen, was für die Compliance und forensische Untersuchungen essenziell ist.

- **Analyse und Diagnose von Fehlern:**
  Stellt nützliche Informationen für die Diagnose und Behebung von technischen Problemen oder Fehlfunktionen bereit.

- **Compliance und rechtliche Anforderungen:**
  In vielen Branchen erforderlich, um regulatorische Anforderungen zu erfüllen und als Nachweis der Compliance zu dienen.

Inhalte eines Audit-Trails: Die aufgezeichneten Informationen umfassen typischerweise:

- Benutzeraktivitäten und -aktionen, wie Anmeldungen und Datenänderungen.
- Zeitstempel für jede Aktivität.
- IP-Adressen oder Identifikatoren der beteiligten Benutzer oder Systeme.
- Art der durchgeführten Aktion (zum Beispiel Änderung, Löschung, Zugriff).
- Zustand des Erfolgs oder Misserfolgs der Aktivitäten.

Sicherheitsaspekte:
Die Sicherheit des Audit-Trails ist von entscheidender Bedeutung. Um Manipulationen oder Löschungen zu vermeiden, wird er in sicheren Umgebungen aufbewahrt und ist nicht für reguläre Benutzer zugänglich.

Zusammenfassend ist ein Audit-Trail von grundlegender Bedeutung für die Sicherheit, Transparenz und Compliance in IT-Systemen und bietet die Fähigkeit, Aktivitäten nachvollziehbar zu machen und Unregelmäßigkeiten oder Sicherheitsverletzungen rechtzeitig zu erkennen.

8. Schlussfolgerungen

8.1 Die Zukunft der Künstlichen Intelligenz in der Gebäudeautomatisierung

Während die Künstliche Intelligenz weiterhin voranschreitet und als Technologie reift, ist es wesentlich, in die Zukunft zu blicken, um zu verstehen, wie diese Innovationen die Gebäudeautomatisierung und die Baubranche insgesamt weiter beeinflussen könnten.

8.2 Aufkommende Trends in der KI

- **Tiefes Lernen und neuronale Netze:**
  Während tiefes Lernen und neuronale Netze immer weiter fortgeschritten sind, könnten Gebäude von noch präziseren Datenanalysen und Vorhersagen über das Verhalten der Anlagen und der Bewohner profitieren.
- **Edge KI und verteiltes Rechnen:**
  Mit der Ausführung von KI direkt auf Edge-Geräten, wie Sensoren und Kameras, könnten Gebäude in Echtzeit reagieren, ohne Daten an ein zentrales Verarbeitungszentrum senden zu müssen, was die Effizienz steigert und die Reaktionszeiten verkürzt.

8.3 Integration mit anderen sich entwickelnden Technologien

- **IoT (Internet der Dinge):**
  Die weitere Verbreitung von vernetzten Geräten in Gebäuden wird eine noch detailliertere Datenerfassung ermöglichen, die der KI ein vollständigeres Bild für informierte Entscheidungen bietet.
- **Blockchain und Sicherheit:**
  Durch die Verwendung von Technologien wie Blockchain könnte es möglich sein, eine größere Sicherheit und Transparenz in der Gebäudedatenverwaltung zu gewährleisten. Die Verwendung von Smart Contracts könnte die Verwaltung von Diensten und Transaktionen automatisiere

8.4 Neue Interaktionsmodelle

- **Fortgeschrittene Benutzeroberflächen:**
  Mit dem Fortschritt der Technologie werden neue Schnittstellen, wie Augmented Reality, entstehen, die es den Bewohnern ermöglichen, auf bisher unvorstellbare Weise mit dem Gebäude und seinem Automatisierungssystem zu interagieren.

- **Integration mit virtuellen Assistenten:**
  Während virtuelle Assistenten immer raffinierter werden, könnten sie eine zentralere Rolle in der Gebäudeverwaltung übernehmen, indem sie bei Aufgaben wie der Temperaturregelung oder der prädiktiven Wartung helfen und Serviceinstallation erleichtern.

8.5 Herausforderungen und ethische Überlegungen für die Zukunft

- **Voreingenommenheit und Transparenz in der KI:**
  Es ist von grundlegender Bedeutung, dass Modelle künstlicher Intelligenz so gestaltet werden, dass sie jegliche Art von BIAS vermeiden, um sicherzustellen, dass ihre Entscheidungen gerecht und unvoreingenommen sind. Ebenso ist es unerlässlich, dass die Entscheidungsprozesse der KI transparent und nachvollziehbar sind, um das Vertrauen der Nutzer in die Anwendungen dieser Technologie zu erhalten."

- **Datenschutz der Bewohner:**
  Mit der weiteren Datenerfassung ist es wesentlich, die Privatsphäre der Bewohner zu gewährleisten und sicherzustellen, dass ihre Daten geschützt und ethisch genutzt werden.

In Zusammenfassung verspricht die Zukunft der KI in der Gebäudeautomation, bedeutende Innovationen und Verbesserungen zu bringen. Es wird jedoch wesentlich sein, proaktiv die Herausforderungen und ethischen Fragen anzugehen, die sich ergeben. Indem man sich über die neuesten Trends auf dem Laufenden hält und mit Branchenexperten zusammenarbeitet, wird es möglich sein, das Potenzial der KI voll auszuschöpfen und die Industrie in eine effizientere, nachhaltigere und benutzerzentriertere Zukunft zu führen.

Sie möchten erfahren, wie Eliona Ihren Infrastrukturbetrieb vereinfachen kann?

Vereinbaren Sie jetzt ein kostenloses Beratungsgespräch und erfahren Sie,

...wie Sie komplexe Systemlandschaften in einer Plattform integrieren.

...wie Sie Ihren CO_2-Abdruck um bis zu 35% verringern.

... wie Sie Betriebs-Prozesse auf Basis von Live KPIs optimieren.

eliona

Eliona by IoTEC AG
Harzachstrasse 5
8404 Winterthur

eliona.io
hello@eliona.io

Beratungs- und Demotermin
direkt online buchen >>>