Smart Cluster im intelligenten Gebäude und Smart Home

Gebäudesteuerungen zukunftsoffen und investitionssicher gestalten

Bei der klassischen Form der Smart Home Steuerung wird alles auf eine Karte gesetzt: eine einzige Steuerzentrale mit möglichst vielen Schnittstellen.

Das schafft extreme Abhängigkeiten: vom Hersteller, von dessen Architektur und der jeweiligen Programmiersprache. Insgesamt kann nur ein Teil der am Markt verfügbaren Geräte und deren Kontext abgebildet werden. Für alle anderen Devices heißt es: kein Anschluss unter dieser Nummer.

Entdecken Sie eine neue Dimension der Gebäudesteuerung: die Smart Cluster Technologie.

Die Zukunft der smarten Steuerung von Gebäuden

Man stelle sich eine Gebäudesteuerung vor, die nicht nur **modular aufgebaut** ist, sondern auch als **massiv verteiltes Grid organisiert** ist. Und schon wird vieles besser: fehlertolerant, unabhängig und vor allem zukunftsoffen.

Wie genau dieses Kunststück gelingen kann? Ganz einfach – mit deutschem **Ingenieur Know-how**, breit aufgestellter IT und **Infrastruktur-Expertiese** und industriellem Anspruch an die **Qualität**.

So löst man die typischen Beschränkungen einer klassischen zentralen Steuerzentrale auf und gründet **einen smarten Verbund von intelligenten Geräten**:

✔ 1. gelöstes Problem: Vielzahl von Schnittstellen & Standards

Schnittstellen gibt es im Smart Home Umfeld mehr als genug. Einige wenige Schnittstellen basieren auf allgemein verfügbaren und normierten Standards wie z. B. KNX, Zigbee oder CEC. Doch scheinen viele Hersteller ihren eigenen und damit hausinternen Standard etablieren zu wollen. Man denke nur an die

Vielzahl von Smart TV Anwendungsschnittstellen (API), einzig um die Funktion einer Fernbedienung zu simulieren.

Durch eine aufwändige manuelle Konfiguration innerhalb der jeweiligen Steuerung lässt sich schon einiges an Logik umsetzen. Doch das ist weder effizient noch nachhaltig, sondern in allen Belangen höchst proprietär und damit nicht auf andere Systeme übertragbar.

In einem stark begrenzten Rahmen mag das noch funktionieren. Wenn jedoch die Ansprüche steigen und stetig neue semi-smarte Geräte hinzukommen, wird es schwierig und zunehmend teurer. Erst recht, wenn ein bestimmtes Gerät mit dessen Schnittstelle nicht direkt unterstützt werden. Denn dann muss speziell entwickelte Hard- und Software der Steuerzentrale vorgeschaltet werden.

Die Lösung: lose Kopplung

Kein System der Welt kann **alle Schnittstellen** in **maximaler Qualität** zur Verfügung stellen. Deshalb ist es besser, wenn man alles **frei kombinieren** kann: einfach das beste Modul von beliebigen Herstellern bzw. Entwicklern nehmen.

Das erreicht man am besten durch einen gemeinsamen Event-Bus. Hier hat sich **MQTT als Standard** etabliert. Mit diesem lassen sich **beliebige Adapter und Konverter** flexibel zu einem großen Ganzen verknüpfen.

Doch MQTT leistet noch mehr. Module für **Künstliche Intelligenz und Machine Learning** einbinden, damit das intelligente Gebäude noch intelligenter wird? Kein Problem mit MQTT. Auch der **Benutzerkomfort** lässt sich optimieren: mit unterschiedlichen User-Interfaces und Dashboards, die problemlos parallel genutzt werden können.

Technisch spricht man dann von "lose Kopplung": neue bzw. veränderte Module können jederzeit in die Kommunikation eingeklinkt werden.

Der große **Vorteil** und besondere Charme des Smart Cluster Ansatzes liegt darin, dass diese Module in **jeder beliebigen Programmiersprache** und somit unabhängig von plattformspezifischen Besonderheiten genutzt werden können.

Ermöglich wird dies durch den Einsatz von **virtuellen Umgebungen**, den sogenannten Containern.

Mit dem Smart Cluster Ansatz und „losen Kopplungen“ erzielt man völlige Freiheit bezüglich der Modulauswahl und gewinnt einiges an Sicherheit hinzu.

✔ 2. gelöstes Problem: Ausfallsicherheit & Verfügbarkeit

Klassische Ansätze basieren auf einer zentralen Steuerzentrale: ein komplexes Gerät, eine Hardware, ein Betriebssystem, eine Software-Plattform. Aber es gibt kein Fallback bzw. keine Ausfallsicherheit, falls etwas vorübergehed hängt oder ganz ausfällt.
Insbesondere nach Software-Aktualisierungen und Firmware-Updates kommt es öfter zu Problemen, die sich nicht durch einen Reboot beheben lassen.

Niemand würde in einen Flieger steigen, der nur einfach abgesichert ist und dann auf einen sicheren und entspannten "Fly by Wire" Flug vertrauen.

Die Lösung: Redundanz

In der Industrie setzt man deshalb auf **massiv redundante Systeme**, sogenannte Cluster, die im Fehlerfall **automatisch einspringen**.

Wenn ein Modul nicht wie gewünscht arbeitet, wird automatisch auf ein anderes gleichwertiges Modul (idealerweise mit einem anderen Software-Stand) zurückgegriffen.
Damit lassen sich **Totalausfälle vermeiden** und Hardware-Probleme sowie Software-Fehler **sicher umschiffen**.

So ist Verlass auf stets verfügbare und dezent im Hintergrund arbeitende Heinzelmännchen.

✔ 3. gelöstes Problem: Vergessene Infrastruktur & IoT-Wildwuchs

Klassische Ansätze der Gebäudeautomation beziehen nicht die IT bzw. OT Infrastruktur mit ein, auf der sie basieren. Um die maximale Vernetzung zu erreichen, werden alle Geräte über eine allgemein zugängliche interne Infrastruktur miteinander verknüpft.

Gegen Angriffe von außen versucht man, sich mittels Firewall und VPN zu schützen. Das interne Netz wird hierbei als vermeintlich sicher angesehen.
Wer überwacht denn heute, mit wem der Smart TV kommuniziert? Wohin die Daten des Stromzählers fließen? Oder ob die Gebäude-Kamera überhaupt Bilder ins Internet senden darf?
Nicht so schlimm? Doch Achtung, alleine auf der Basis von smarten Daten lässt sich das ganze Geschehen nahezu vollständig ausspionieren. Smarte Fernseher senden Kanalwechsel. Aus der Verlaufskurve des Smart Meter lassen sich die Geräte und deren Nutzung ableiten (ja, sogar der aktuell gestreamte Film, da weißer Hintergrund mehr Strom verbraucht). Und sämtliche Mikrofone sind gerne genutzte Informationsquellen.

Das ist fast so, als ob man ein Gebäude ohne Türen bauen würde. Und nur einen Bodyguard vor das Gartentor stellt.

Die Lösung: Alle Geräte in einem Repository verwalten

Um **bestmögliche Sicherheit** zu realisieren, ist es unverzichtbar, dass man neben den IoT-Devices auch **sämtliche Komponenten** der Netzwerk- und Kommunikationsschicht gemeinsam in einem **Repository** hinterlegt.
Neben den IoT Geräten und anderen Assets werden dort auch alle Kommunikationspfade und -Typen verwaltet. Die Geräte können hier auch allgemeingültig und somit einheitlich **konfiguriert** werden. Und während des Betriebs lässt sich ihr **Status überwachen**.
Was aufwändig und kompliziert klingt, ist mit dem richtigen Ansatz ganz einfach. Da man das Thema **ganzheitlich** löst, definiert man **jedes Gerät nur einmal**. Basierend auf den Daten dieses Infrastruktur Repository werden dann **automatisiert die gerätespezifischen Konfigurationen** erstellt und die Devices entsprechend befüllt.

Auf diese Weise lässt sich der **Gerätezoo sicher einzäunen**. Man gewinnt wieder die Oberhand und kann dediziert **entscheiden, wer wann und wo welche Daten** zu sehen bekommt oder auf welche **Geräte-Funktionen zugreifen** darf.

So lebt man nicht gut und komfortabel, sondern weiß auch seine Privatsphäre und Persönlichkeitsrechte gewahrt und sämtliche Technik sicher geschützt.

✔

4. gelöstes Problem: Externe Abhängigkeiten & fehlende Internet-Verbindung

Viele vermeintlich smarte Steuerungen benötigen eine aktive Internet-Verbindung, um vollständig arbeiten zu können. Wer für Komfort Funktionen wie die Sprachsteuerung auf Public Cloud Services wie Amazon Alexa oder den Google Assistant setzt, macht sich zwingend von einer stabilen Internet Verbindung abhängig.

Doch wenn diese einmal nicht verfügbar ist, fängt man zu rotieren an, da man sich nach alternativen Möglichkeiten zur Steuerung umsehen muss.

Richtig schlimm, wird es, wenn sogar Basis-Funktionen (wie Heizen, Lüften, Strom und Licht) auf Cloud-Software basieren. Dann ist es schnell zappenduster.

Die Lösung: Unabhängig & Eigenständig

Um sich gegen solche Probleme zu schützen, hilft nur eins: sich **unabhängig machen** – **auf allen Ebenen**. Das bedeutet, Verbindungen nach außen weitgehend zu kappen und möglichst alles **dezentral zu organisieren**.

Das fängt bei einer **lokal verfügbaren Sprachsteuerung** an und hört bei lokal ermittelten **Wetterdaten** noch lange nicht auf.

Alles dezentral organisieren: So sorgt man für Unabhängigkeit und gewinnt persönliche Freiheit.

Smart Cluster – Komplexität in den Griff bekommen und Kosten reduzieren

Ein einziger Hersteller kann nicht alle Probleme lösen? Korrekt. Doch wer sagt denn, dass man sich auf einen Hersteller beschränken muss? Warum nicht jeweils **die besten Module** für einen bestimmten Zweck wählen und **gesamtheitlich verknüpfen**?

Das ist genau das, was ein **Smart Cluster** zusätzlich zu einer klassischen Steuerzentrale ermöglicht:

- smart, modular, funktional und individuell anpassbar
- sicher, hochverfügbar, ausbaufähig und transparent

Zukunftsoffen & flexibel: einfach beginnen und groß durchstarten

Klingt, als ob ein Smart Cluster ziemlich teuer sei? Denn es scheint zwar technologisch ausgefeilt, aber vielleicht etwas oversized. Ganz sicher nicht, denn bereits mit **günstiger Technik** (wie mehreren Raspberry PI 4) lässt sich bereits ein **hochverfügbares Smart Cluster aufbauen**.

Zukunftsoffenheit ist immer inklusive: Da das Cluster ausschließlich auf **Standard-Komponenten** basiert, kann das Cluster **jederzeit flexibel für neue Anforderungen** adaptiert werden.
Bezüglich der Software-Module spielt es keine Rolle, welcher Hersteller mit welcher Programmiersprache dieses erstellt hat.

Es ist einzig darauf zu achten, dass jedes beteiligte Modul **über eine MQTT Verbindung** verfügt und **unter Linux lauffähig** ist.

Das Ganze ist mehr als die Summe seiner Teile.

Smart Cluster: ganzheitliches Denken in der Gebäudeautomatisierung

bintellix ® denkt, konzeptioniert und handelt von A bis Z ganzheitlich.

Wir integrieren unterschiedliche Technologien zu einem gemeinsamen, leistungsfähigen Verbund.

Die einzelnen IoT-Devices werden dabei automatisiert gemanagt. Für die Nutzer bedeutet das maximale Transparenz auf allen Ebenen, wie es ohne ein Smart Cluster nicht zu erreichen ist.
Um die technischen Details braucht Sie sich keine Gedanken machen. Da sind wir zu Hause.

Unsere Gewährleistung: Es läuft. Diskret und sicher.

Smart gelöst: Auf diese Basis bauen wir

Unser Smart Cluster Ansatz basiert auf zwei Säulen: Connected Intelligence und Open Connectivity.

Unknown Tag (taglib-pdf): <object>

Auf einen Blick: Smart Cluster Vorteile fürs Smart Home

1. Unknown Tag (taglib-pdf): <details>
2. Unknown Tag (taglib-pdf): <details>
3. Unknown Tag (taglib-pdf): <details>
4. Unknown Tag (taglib-pdf): <details>
5. Unknown Tag (taglib-pdf): <details>
6. Unknown Tag (taglib-pdf): <details>
7. Unknown Tag (taglib-pdf): <details>
8. Unknown Tag (taglib-pdf): <details>

Unternehmen
bintellix GmbH & Co. KG
Geigenbergerstr. 7a
81477 München
Deutschland

Comunity
facebook.com/bintellix
twitter.com/bintellix
github.com/twitter

Kontakt
+49 89-7507504-0
+49 89-7507504-99
info@bintellix.com
Kontaktformular

Unternehmensgruppe
INTERSECURITY