Smart cluster in the intelligent building and smart home

Designing building control systems that are open to the future and investment-proof

In the classic form of smart home control, everything is put on one card: a single control center with as many interfaces as possible.

This creates extreme dependencies: on the manufacturer, its architecture and the respective programming language. Overall, only some of the devices available on the market and their context can be mapped. For all other devices it means: no connection under this number.

Discover a new dimension of building control: smart cluster technology.

The future of smart building control

Imagine a building control system that is not only modular, but also organized as a massively distributed grid. And already many things will be better: fault-tolerant, independent and, above all, open to the future.

How exactly can this feat be achieved? Quite simply - with German engineering know-how, broad-based IT and infrastructure expertise and industrial quality standards.

This is how you dissolve the typical limitations of a classic central control center and establish a smart network of intelligent devices:

✔

1. Problem solved: multitude of interfaces & standards

Interfaces are more than enough in the smart home environment. A few interfaces are based on generally available and standardized standards such as KNX, Zigbee or CEC. But many manufacturers seem to

want to establish their own and thus in-house standard. Just think of the multitude of Smart TV application interfaces (API), solely to simulate the function of a remote control.

A lot of logic can be implemented by a complex manual configuration within the respective control. However, this is neither efficient nor sustainable, but highly proprietary in all respects and thus not transferable to other systems.

Within a very limited framework, this may still work. However, when the demands increase and new semi-smart devices are constantly added, it becomes difficult and increasingly expensive. Especially if a specific device and its interface are not directly supported. This is because specially developed hardware and software must then be connected upstream of the control center.

The solution: loose coupling

No system in the world can provide all interfaces in maximum quality. That is why it is better to be able to combine everything freely: simply take the best module from any manufacturer or developer.

This is best achieved by a common event bus. Here MQTT has established itself as a standard. With this, any adapters and converters can be flexibly linked to form a large whole.

But MQTT can do even more. Integrating modules for artificial intelligence and machine learning to make the smart building even smarter? No problem with MQTT. User convenience can also be optimized: with different user interfaces and dashboards that can easily be used in parallel.

Technically, this is called "loose coupling": new or modified modules can be linked into the communication at any time.

The great advantage and special charm of the Smart Cluster approach is that these modules can be used in any programming language and thus independently of platform-specific features.

This is made possible by the use of virtual environments, the so-called containers.

With the smart cluster approach and "loose couplings" one achieves complete freedom with regard to module selection and gains some additional security.

✔ 2. Solved problem: resilience & availability

Classical approaches are based on a central control center: a complex device, a hardware, an operating system, a software platform. But there is no fallback or failover in case something hangs vorübergehed or fails completely.
Especially after software updates and firmware updates, there are more often problems that can't be fixed by a reboot.

No one would get into a plane that is just backed up and then trust in a safe and relaxed "fly by wire" flight.

The solution: redundancy

In the industry, therefore, people rely on massively redundant systems, so-called clusters, which automatically step in in the event of a fault.

If a module does not work as desired, another equivalent module (ideally with a different software version) is automatically used. This avoids total failures and allows hardware problems and software errors to be safely bypassed.
This avoids total failures and allows hardware problems and software errors to be safely bypassed.

You can rely on brownies, who are always available and work discreetly in the background.

✔ 3. Problem solved: Forgotten infrastructure & IoT proliferation

Classical approaches to building automation do not involve the IT or OT infrastructure on which they are based. To achieve maximum interconnectivity, all devices are linked via a generally accessible internal infrastructure.

Attempts are made to protect against external attacks by means of firewalls and VPNs. The internal network is seen as supposedly secure.
Who monitors who the smart TV communicates with today? Where the data from the electricity meter is going? Or whether the building's camera is even allowed to send images to the Internet?
Not so bad? But beware, based on smart data alone, the entire event can be almost completely spied out. Smart TVs send channel changes. The devices and their usage can be deduced from the smart meter's history curve (yes, even the currently streamed movie, since white backgrounds consume more power). And all microphones are readily used sources of information.

It's almost like building a building without doors. And only put a bodyguard in front of the garden gate.

The solution: Manage all devices in a repository

In order to realize the best possible security, it is indispensable to store not only the IoT devices but also all components of the network and communication layer together in a repository.
In addition to the IoT devices and other assets, all communication paths and types are also managed there. The devices can also be configured here in a generally valid and thus uniform manner. And their status can be monitored during operation.
What sounds complex and complicated is actually quite simple with the right approach. Since you solve the issue holistically, you define each device only once. Based on the data in this infrastructure repository, the device-specific configurations are then created automatically and the devices are filled accordingly.

In this way, the device zoo can be securely fenced off. You regain the upper hand and can make dedicated decisions about who gets to see what data, when and where, or which device functions can be accessed.

This way, you not only live well and comfortably, but also know that your privacy and personal rights are protected and that all technology is securely protected.

✔ 4. Problem solved: External dependencies & lack of internet connection

But once this is unavailable, you start to rotate as you have to look for alternative ways to control it. Relying on public cloud services like Amazon Alexa or Google Assistant for convenience features like voice control makes you compellingly dependent on a stable internet connection.

But once this is unavailable, you start to rotate as you have to look for alternative ways to control it.

It gets really bad when even basic functions (like heating, ventilation, electricity and light) are based on cloud software. Then it's quickly all over.

The solution: independent & self-sufficient

To protect against such problems, only one thing helps: make yourself independent - at all levels. This means cutting off connections to the outside world as far as possible and organizing everything in a decentralized manner.

This starts with locally available voice control and doesn't stop with locally determined weather data.

Organize everything decentrally: This is how you ensure independence and gain personal freedom.

Smart Cluster - Getting a grip on complexity and reducing costs.

A single manufacturer can't solve all the problems? Correct. But who says you have to limit yourself to one manufacturer? Why not choose the best modules for a particular purpose and link them together as a whole?

This is exactly what a smart cluster enables in addition to a classic control center:

- smart, modular, functional and individually adaptable
- secure, highly available, expandable and transparent

Open to the future & flexible: start simple and go big

Sounds like a smart cluster is pretty expensive? Because it seems technologically sophisticated, but perhaps a bit oversized. Certainly not, because even with inexpensive technology (such as several Raspberry PI 4), a highly available Smart Cluster can already be set up.

Future openness is always included: Since the cluster is based exclusively on standard components, it can be flexibly adapted to new requirements at any time.
With regard to the software modules, it does not matter which manufacturer created them with which programming language.

It is only important to ensure that each module involved has an MQTT connection and can run under Linux.

The whole is more than the sum of its parts.

Smart Cluster: holistic thinking in building automation

bintellix ® thinks, designs and acts holistically from A to Z.

We integrate different technologies into a common, powerful network.

The individual IoT devices are managed automatically. For users, this means maximum transparency at all levels, which cannot be achieved without a smart cluster.
You don't need to worry about the technical details. That's where we are at home.

Our guarantee: It runs. Discreetly and securely.

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

Community
facebook.com/bintellix
twitter.com/bintellix
github.com/twitter

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

Unternehmensgruppe
INTERSECURITY