

BMS

BUILDING MANAGEMENT SYSTEM

PROBLEM

The Building Management System (BMS) cannot be exposed to the public internet due to the company's strong cybersecurity policy. There is a significant risk that exposing the system could lead to hacking attempts, which in turn could result in system shutdowns or damage to critical infrastructure

However, this security measure introduces several operational challenges:

Constant On-Site Supervision:

Requires permanent staff presence, leading to high operational costs.

Limited Remote Monitoring:

Restricted visibility hinders the ability to detect and respond to issues promptly.

Lack of Centralised Oversight:

No unified view across multiple buildings makes it extremely difficult to balance usage or redistribute personnel and departments to underutilised areas.

CHALLENGE

How can data from the Building Management System (BMS) be securely transmitted to the cloud to enable remote management and centralised oversight of building operations, without compromising the integrity or safety of the underlying infrastructure?

The challenge lies in finding a secure, reliable method of transmitting operational data from isolated, on-premises BMS networks to cloud-based platforms. This would allow authorised personnel to gain real-time visibility across multiple facilities, analyse performance trends, proactively address maintenance issues, and make informed decisions about space and energy usage. At the same time, the solution must protect the BMS from cyber threats, unauthorised access, and system tampering.





SOLUTION

To ensure secure data transmission from the Building Management System (BMS) to a cloud-accessible environment, we employ an **air-gapped architecture**. This method physically and logically separates the secure internal BMS network from any system connected to the public internet.

Data is transferred through a tightly controlled, one-way communication channel that prevents any external access to the core BMS infrastructure. This architecture eliminates the risk of direct cyberattacks on the BMS while still

allowing for selective data sharing needed for remote monitoring, analytics, and centralised oversight.

This approach has been **thoroughly tested and validated by major blue-chip companies** across critical infrastructure sectors. It is regarded as a highly secure, resilient solution that meets stringent cybersecurity standards while enabling essential operational visibility and control.



SCHEMATICS

BMS System



Data Collector



Data Sender



Air Gap
Strictly one way
communication



Cloud
Servers



Client Access



CONTACT

mail@dbr.co.uk
+44 1268 442888

