dbr

COMPANY PROFILE

Making the complex simple

CONTACT

mail@dbr.co.uk
+44 7713 157086

ADDRESS

135 Cannon Workshops
3 Cannon Drive
London
E14 4AS

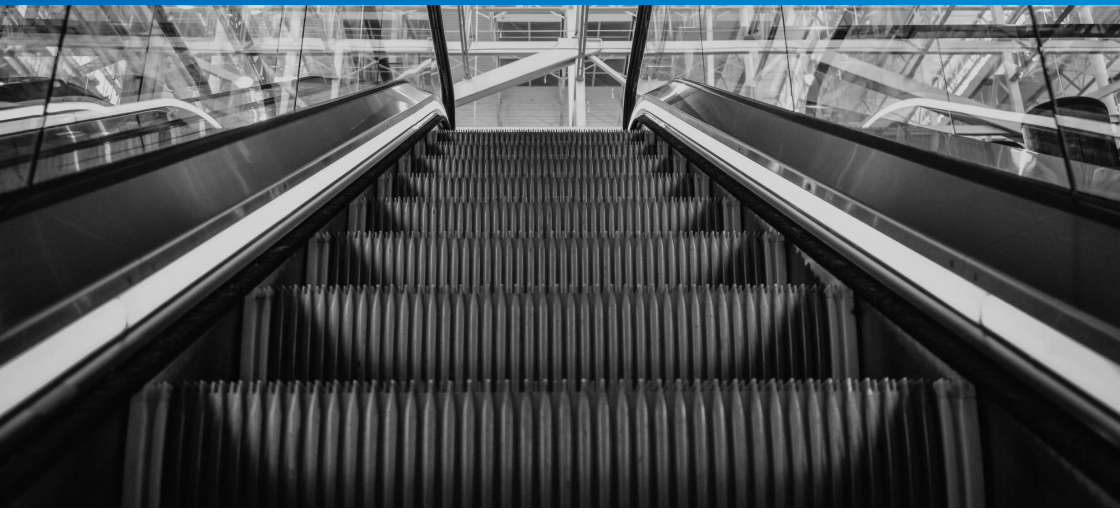
OUR SERVICES

dbr bespoke data solutions has been created to suit your needs, giving you access to your data, displayed and analysed to suit your needs.

Data from all existing monitoring systems can be collected and coupled with advanced security protocols and analytics, providing clients with real time visibility of their business-critical assets. Working with you, our technology can take existing data feeds from asset controllers, particularly pre IoT systems, coupled with additional sensor technologies if required.

The dbr data platform provides a unique data feed focused on sustainability, business efficiency and wellbeing. Our data analytics will focus on ensuring your infrastructure runs efficiently, reducing energy consumption and carbon emissions to nett zero?

Can maintenance costs be reduced, moving from fix it when it breaks, to being able to accurately predict system faults and react prior to failure. With our analytical platform we can predict when assets will fail, saving time and money, and improve staff wellbeing.



Whatever you need to monitor, the dbr data platform can be tailored to meet your individual requirements, with infographics available on any web enabled device with username and password protection.

BENEFITS

REDUCED DOWNTIME

PREDICTIVE MAINTENANCE:
Sensors can detect early signs of wear or failure, allowing for maintenance before breakdowns occur.

FASTER RESPONSE:
Alerts and diagnostics enable quicker interventions, minimizing disruptions.

LOWER OPERATING COSTS

FEWER SITE VISITS:
Remote monitoring reduces the need for frequent on-site inspections.

EFFICIENT RESOURCE ALLOCATION:
Teams can focus efforts on assets that truly need attention.

INCREASED ASSET LIFESPAN

TIMELY MAINTENANCE:
Well-maintained equipment lasts longer.

CONDITION-BASED USAGE:
Adjust usage patterns based on real-time data to avoid overstressing assets.

IMPROVED SAFETY

HAZARD DETECTION:
Monitor for dangerous conditions (e.g., pressure, temperature, gas leaks) remotely.

REDUCED HUMAN EXPOSURE:
Less need to send personnel into potentially hazardous or remote environments.

REAL-TIME INSIGHTS & DECISION-MAKING

LIVE DATA FEEDS:
Managers can make informed decisions using current operational data.

DASHBOARDS & ANALYTICS:
Visual tools help track performance trends and identify anomalies.

SCALABILITY

EASIER TO EXPAND:
Adding new assets or locations is more straightforward with centralized monitoring.

GLOBAL REACH:
Organizations can monitor assets across multiple geographies from a single platform.

REGULATORY COMPLIANCE

AUTOMATED REPORTING:
Easily generate logs and reports for audits and compliance requirements.

CONSISENT MONITORING:
Ensure adherence to operational and environmental standards.

ENHANCED SECURITY

ACCESS CONTROL:
Track and restrict asset access remotely.

TAMPER DETECTION:
Instant alerts for unauthorized activity or breaches.

COMPANY PROFILE

dbr is an innovative remote asset monitoring company that leverages advanced technology to help organisations optimise the performance and reliability of their assets.

The dbr team has over 50 years of combined experience in hardware design, data analytics and industrial applications, capable of fully understanding and delivering our clients needs.

Building long term relationships with our clients challenges us to constantly develop innovation that drives their businesses forward.

WE LOOK FORWARD TO WORKING WITH YOU AND MAKING THE COMPLEX SIMPLE

CONTACT

mail@dbr.co.uk
+44 7713 157086

ADDRESS

135 Cannon Workshops
3 Cannon Drive
London
E14 4AS

OLYMPUS

DATA COLLECTION UNIT

USE

Olympus collects data from various sources like:

TCP/IP connected systems
USB based readers
radio using 868/922MHz
digital/analog sensors

Protocols we support are for example, Modbus, BACnet, CAN bus, MQTT, HTTP(S), SNMP, ...

The unit can be expanded using built in slot to add RS-232, RS-422, RS-485, CAN bus, direct connection to connect to various analog or digital sensors.

Multiple units could be connected using built in radio with reach of approx. 20-50m indoors and 300-500m outdors. The radio is protected by AES 128 encryption.

SPECIFICATION

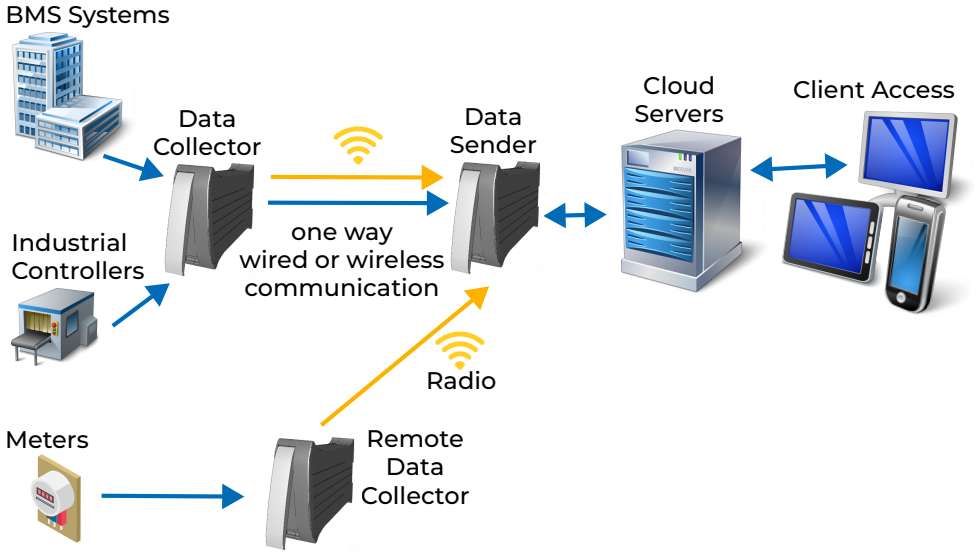
size:
100 x 120 x 35mm
DIN rail mountable

power supply:
9-36VDC / 9-36VAC
(2pin 5mm terminal block)

I/O:
1x LAN 10/100/1000 Mbps
1x USB 2.0
1x internal sub 1GHz radio
1x configurable connector
(up to 10pin terminal block)
1x expansion slot
optional Wi-Fi

CPU:
AMR Cortex-A72 on module

SOLUTION EXAMPLE



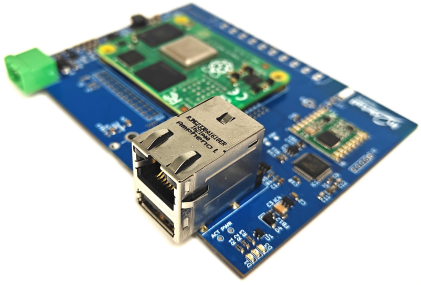
DETAILS

We collect data from existing systems securely and push pre IoT systems providing IoT connectivity.

The data collection unit is running locked down Debian Linux on ecrypted storage so your data are protected end to end.

All communication between data collectors and our servers is TLS/SSL encrypted and uses JWT authentication.

Radio communication is AES 128 encrypted.



CONTACT

mail@dbr.co.uk
+44 7713 157086

BUSBYTE

UNHACKABLE DATA TRANSFER

PROBLEM

Do you face challenges in retrieving data from on-site or remote, hard-to-reach locations without compromising asset security or exposing systems to potential cyber threats?

Is ensuring end-to-end data security a critical requirement for your operations?

Our solution provides a secure, reliable method for retrieving data from remote systems without increasing the attack surface.

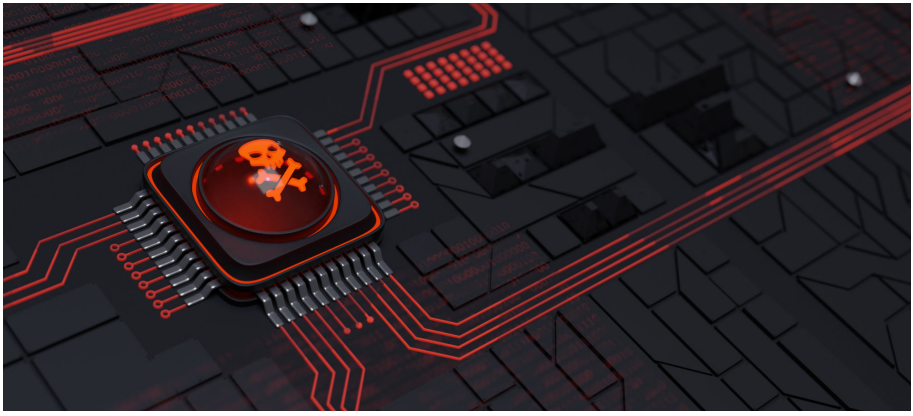
SOLUTION

We utilize a combination of air-gapped architecture and a strict read-only methodology to securely retrieve data from a wide range of industrial systems.

BusByte technology operates across two distinct security layers:

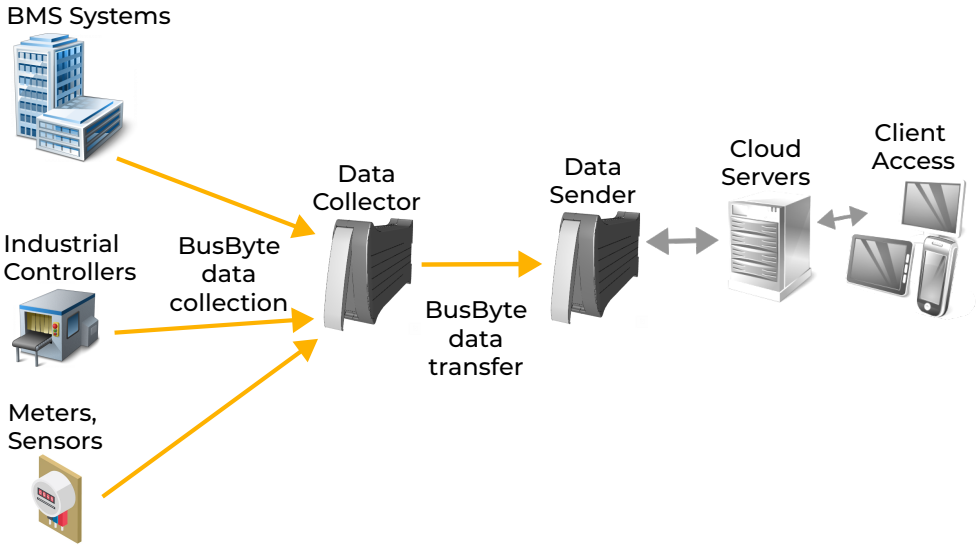
First layer applies to data collection and enforces a strict read-only policy, including support for serial communication protocols such as Modbus.

Second layer enhances data transfer security when TCP/IP-based collection is used, ensuring the system remains fully isolated and virtually impervious to external attacks.



dbr

COMMUNICATION EXAMPLE



DETAILS

We collect data from existing systems securely and push pre IoT systems providing IoT connectivity.

Data transfer can be carried out over wireless or wired connections, depending on the deployment requirements.

The data collector and data sender unit is locked down OS on ecrypted storage so your data are protected end to end.

All communication between data collectors and our servers is TLS/SSL encrypted.

CONTACT

mail@dbr.co.uk
+44 7713 157086

LIFT
MONITORING

PROBLEM

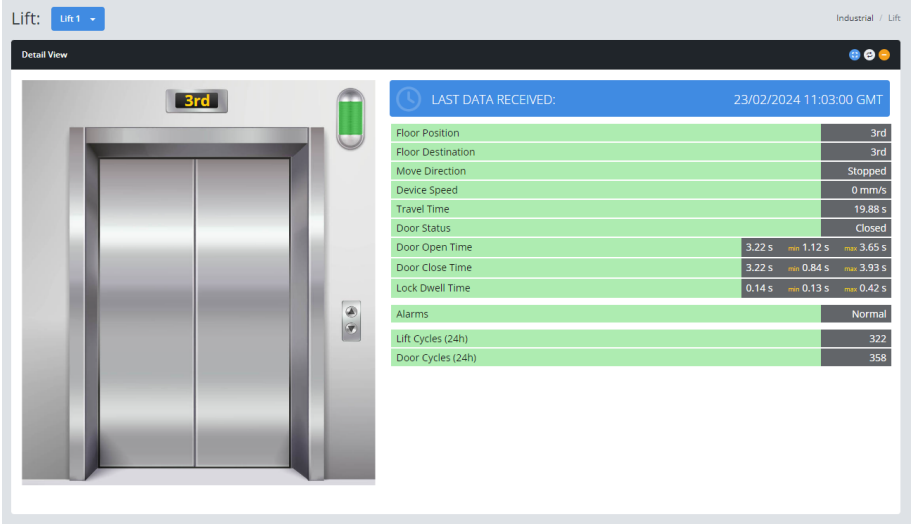
The Civil Aviation Authority requires airport management companies to meet availability levels for passenger lifts. If airports fail to meet the required availability levels, the CAA imposes fines. There is a similar system used by Transport for London to measure lift service partner performance.

The ability to monitor failure points and improve lift reliability is virtually impossible given that range and age of lifts installed across the transport network in the UK.

CHALLENGE

The challenge was to create a communication system that could collect data direct from lifts in real time, with an analytical platform to detect variation in the lift normal running signature and raise pre-set alarms prior to lift failure.

As the communication system would take direct feed from the lift controller, the solution must protect the lifts from cyber threats an unauthorised access.



dbr

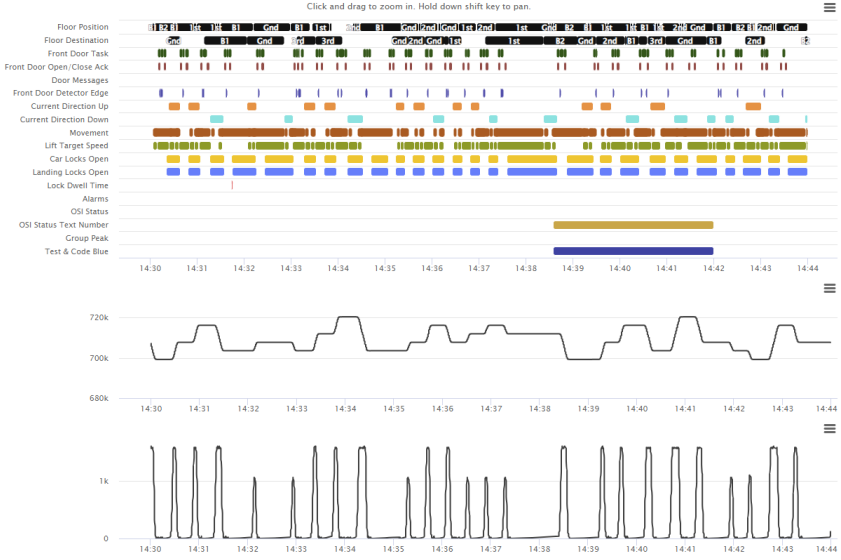
SOLUTION

Our data harvester connects into the lift controller, taking constant lift movement element values, alarm status and health condition, which is fed to our secure cloud-based servers. After the data is processed, the lift display, together with real-time current status and graphs showing historic trends is available on any web enabled device, with username and password protection.

Data is transferred through a tightly controlled, one way communication channel that prevents any access back to the lift unit being monitored.

BENEFITS

- Allows pre-emptive maintenance actions prior to lifts failing in service.
- Reduces unplanned maintenance actions.
- Eliminate business disruption costs.
- Eliminates CAA/TfL fines.



CONTACT

mail@dbr.co.uk
+44 7713 157086

ESCALATOR
MONITORING

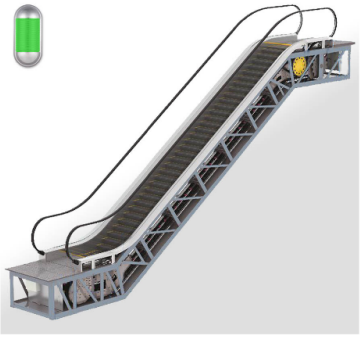
PROBLEM

A number of London Underground stations are designated ‘gold’ status during significant public events and requires maintenance actions to be implemented that would mitigate any potential escalator failure points.

The ability to currently monitor failure points and maintain escalator reliability is virtually impossible given that range and age of escalators installed across the transport network in the UK.

CHALLENGE

The challenge was to create a communication system that could collect data direct from escalators in real time, with an analytical platform to detect variation in the escalator normal running signature and raise pre-set alarms prior to escalator failure.
As the communication system would take direct feed from the escalator controller, the solution must protect the escalators from cyber threats an unauthorised access.



LAST DATA RECEIVED:	19/06/2025 13:04:02 BST
Software Version	V01.32
Job Number	E0344
5V I/O Healthy	☑
5V Comms Healthy	☑
24V Healthy	☑
Brake Mon Fail	☐
Safety Chain Latch	☐
Speed Mon Fault	☐
Handrail Fault	☐
Missing Step Fault	☐
Drive Fault	☐
Broken Chain Switch	☐
Trap Door Switch	☐
Direction	Stationary
Speed	1140 RPM
Speed Monitoring Timer	2.98 s
Left Handrail Timer	2.98 s
Right Handrail Timer	2.94 s
Top Missing Step Timer	1.38 s
Bottom Missing Step Timer	1.38 s

SOLUTION

Our data harvester connects into the escalator controller, taking constant inputs/outputs, alarm status and health condition, which is fed to our secure cloud-based servers. After the data is processed, the escalator display, together with real-time current status and graphs showing historic trends is available on any web enabled device, with username and password protection.

Data is transferred through a tightly controlled, one way communication channel that prevents any access back to the escalator unit being monitored.

BENEFITS

- Allows pre-emptive maintenance actions prior to lifts failing in service.
- Reduces unplanned maintenance actions.
- Eliminate business disruption costs.
- Reduces potential health & safety issues with high levels of passenger traffic.

CONTACT

mail@dbr.co.uk
+44 7713 157086

ENVIRONMENT
SWITCHROOM MONITORING

PROBLEM

All switch rooms on the London train network located underground or in tunnels are subject to overheating due to no ventilation and inadequate remote air conditioning systems.

If the temperature rises above safe operating levels the equipment in the switch room shutdown, having a significant negative impact on train movements.

CHALLENGE

The challenge was to create a communication system that could monitor the temperature and humidity in switch rooms and raise alarms to request maintenance actions before the systems shutdown.

We also needed to address the communication of data from the switch room to our cloud-based servers with no Wi-Fi signal costs to hard wire CAT5/6 cable would be prohibitive.

SOLUTION

Our data harvester constantly collects data from sensors measuring room temperature and humidity, which is fed to our secure cloud-based servers.

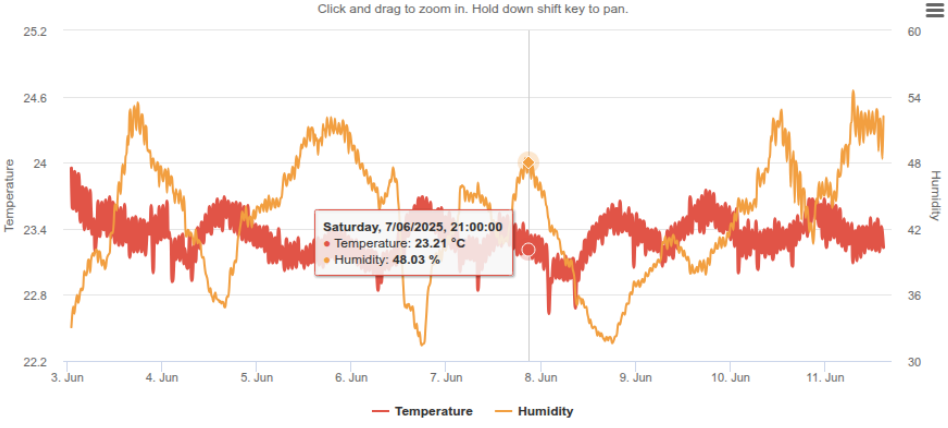
After the data is processed, we display the current real-time values together with graphs showing historic trends available on any web enabled device, with username and password protection.

To resolve the communication issue, we use long range radio from underground or tunnel locations until we have 4G/5G Wi-Fi access.

We can also connect directly with remote air condition units to monitor performance and asset health.

BENEFITS

- Allows pre-emptive maintenance actions prior to exceeding safe temperature operating levels.
- Reduces labour costs for continual manual checking of temperatures.
- Eliminate business disruption costs.



CONTACT

mail@dbr.co.uk
+44 7713 157086

REMOTE ACCESS

DIRECT PORTS, WWW, ...

PROBLEM

Organizations increasingly need time limited remote access to network-enabled industrial devices or computer systems to facilitate efficient management, and control from virtually any location.

However, directly exposing these systems to the public internet introduces substantial security risks, making them susceptible to unauthorized access, cyberattacks, and data breaches.

Many of these systems were not originally designed with modern cybersecurity standards in mind and may lack support for secure protocols such as HTTPS. As a result, allowing unencrypted HTTP traffic significantly heightens the risk of interception and exploitation, compromising both operational integrity and sensitive data.

Addressing these challenges requires a secure, reliable, and easy-to-deploy solution that enables remote access without undermining the security posture of the organization.

CHALLENGE

How can an organization establish highly secure, temporary connections to remote industrial devices or computer systems in a way that ensures data integrity and protection against cyber threats, while also avoiding the need for permanent exposure to the public internet?

Additionally, how can this be achieved in a cost-effective manner that reduces ongoing maintenance efforts and minimizes the complexity of managing remote access infrastructure?

dbr

SOLUTION

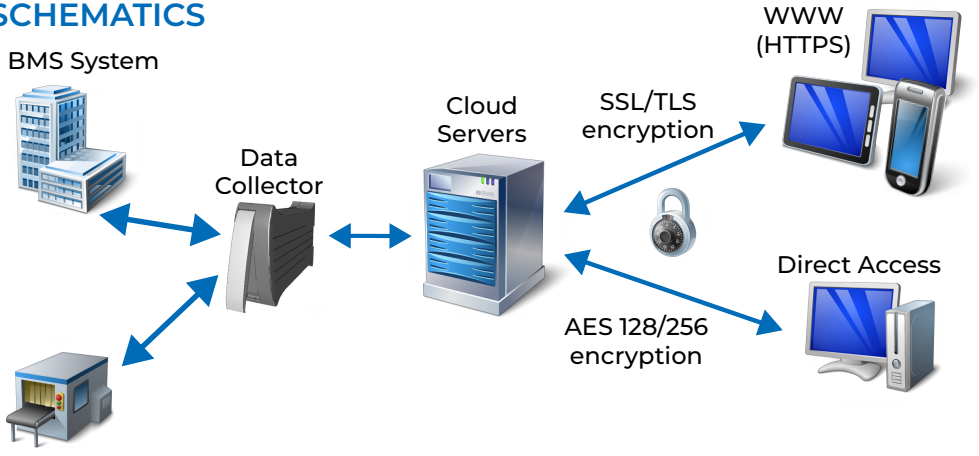
Our system serves the purpose of establishing a secure connection to a specific device's IP address and port. It accomplishes this by creating time limited encrypted tunnel that facilitates the transmission of traffic between the desired device and our public server.

We also offer the capability to monitor devices through direct port connections, such as service access. This functionality allows for service level access, enabling users to efficiently monitor and manage devices directly through their respective ports.

For HTTP connections, we go a step further by adding an SSL layer encryption on our server. This SSL encryption provides an additional layer of security, assuring the confidentiality and integrity of the communication.

Furthermore, to enhance security even more, we provide access via randomized URLs, adding an extra level of obscurity and reducing the risk of unauthorized access.

SCHEMATICS



CONTACT

mail@dbr.co.uk
+44 7713 157086

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

CHALLENGE

How can data from the Building Management System (BMS) be securely transmitted to the cloud to enable remote management and centralized 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 authorized personnel to gain real-time visibility across multiple facilities, analyze 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, unauthorized access, and system tampering.

dbr

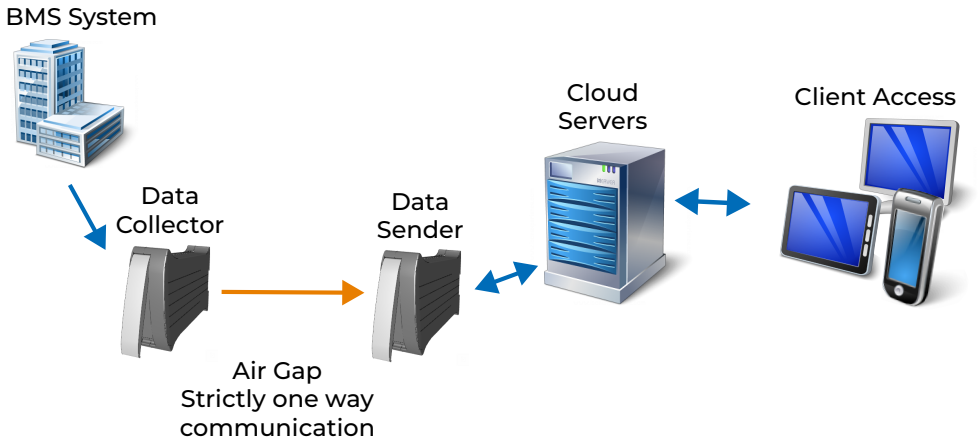
SOLUTION

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 centralized 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



CONTACT

mail@dbr.co.uk
+44 7713 157086

CROWCON
GAS MONITORS

PROBLEM

Several Crowcon gas monitors are installed across a London train network, used to monitor methane and hydrogen sulphide levels from water drainage systems.

Each monitoring unit is connected to SCADA which relays when alarm limits have been exceeded, there is no real time monitoring to show current gas levels.

To obtain current values requires a site visit to manually record gas levels shown on the Crowcon display, but the gas monitoring locations are often in remote areas with limited restricted access.

CHALLENGE

The challenge was to create a communication system that could collect data direct from the Crowcon gas monitoring units in real time, with an analytical platform to detect variation in gas levels and raise pre-set alarms prior to exceeding the safe gas level limits.

As the communication system would take direct feed from the controller, the solution must protect the gas monitors from cyber threats an unauthorised access.

LAST DATA RECEIVED:	11/06/2025 13:18:22 BST
System Uptime	128 days 13:36:15
System Status	OK
System Fault 1	OK
System Fault 2	OK
System Warning 1	OK
System Warning 2	OK
Channel 1 Name	FLA - Flammable Methane Detector
Channel 1 Status	OK
Channel 1 Level	0.000 %LEL
Channel 1 Alarm Limits	warning 20 alarm 40
Channel 2 Name	ESU - Environmental Sampling Unit
Channel 2 Status	OK
Channel 2 Level	7.380
Channel 2 Alarm Limits	warning below 5.0 warning above 15.0
Channel 3 Name	H2S - Hydrogen Sulfide Pit
Channel 3 Status	OK
Channel 3 Level	0.400 PPM
Channel 3 Alarm Limits	warning 100 alarm 200
Channel 4 Name	H2S - Hydrogen Sulfide Atmosphere
Channel 4 Status	OK
Channel 4 Level	0.510 PPM
Channel 4 Alarm Limits	warning 100 alarm 200

SOLUTION

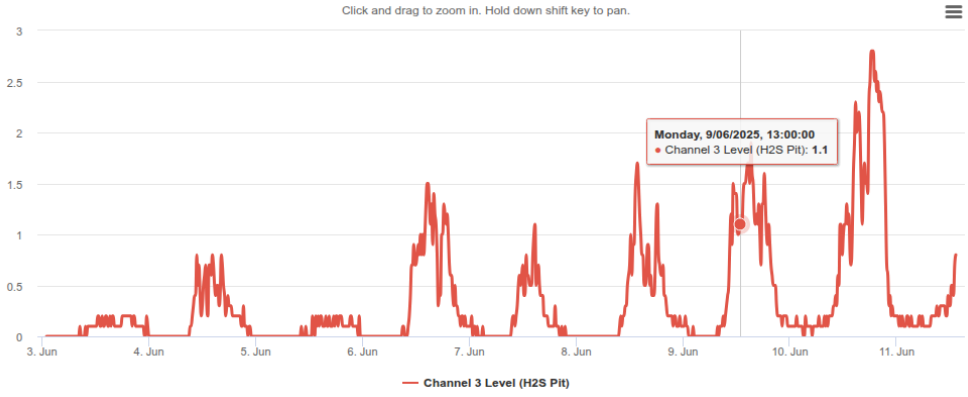
Our data harvester connects into the Crowcon control unit, taking constant gas values, alarm status and health condition, which is fed to our secure cloud-based servers.

After the data is processed, the Crowcon display, together with real-time current status and graphs showing historic trends is available on any web enabled device, with username and password protection.

Data is transferred through a tightly controlled, one way communication channel that prevents any access back to the Crowcon units being monitored.

BENEFITS

- Allows pre-emptive maintenance actions prior to exceeding safe gas levels.
- Reduces labour costs for continual manual checking gas values.
- Eliminate business disruption costs.
- Eliminates health risks from gas exposure



CONTACT

mail@dbr.co.uk
+44 7713 157086