CASE STUDY

Strengthening Cybersecurity of Airport Building Management Systems

How an airport gained continuous BMS visibility, vulnerability prioritisation, and protocol-aware threat detection—turning OT telemetry into business-impact decisions without touching a single controller.

SECTOR: Airport Operations - Building Management Systems

GRAMAX SERVICES: OT Security Assessment | Asset Discovery & Vulnerability Management | Risk Mitigation Advisory

TECHNOLOGY PARTNER: Velos Shield

THE CONTEXT

This case study demonstrates Velos Shield's core proposition: OT security should not stop at asset visibility or alert generation. In a cyber-physical environment such as airport BMS, the real value is the ability to connect passive discovery, vulnerability intelligence, abnormal behaviour detection, and business-impact prioritisation into one continuous operating view.

Behind every terminal is a large, interconnected Building Management System (BMS) - HVAC, chilled-water plants, electrical distribution, lighting, elevators, access control, and fire and life-safety monitoring, increasingly linked together over the same IP network. It is easy to think of this as ordinary facilities equipment. In practice, it behaves like any other operational technology environment: it runs physical processes, it runs continuously, and it was never designed with today's cyber threats in mind.

The risk is magnified at an airport because the BMS network rarely stays isolated. It typically connects outward to corporate IT, airport operations systems, outside contractors, remote maintenance platforms, and cloud services. A single weak link in that chain doesn't just risk an HVAC outage - it can ripple into passenger comfort, equipment availability, operational continuity, and physical security.

> **THE GAP**
> *The airport's facilities and security teams knew their building systems well. What they lacked was a continuous, trustworthy view of the network carrying all of that activity - and a structured, tool-based way to discover assets, surface vulnerabilities, and know what deserved attention.*

THE CHALLENGE

Familiar building systems, an unfamiliar attack surface

A closer look at the BMS environment surfaced the same kinds of gaps that recur across facilities networks that have grown organically over time.

Unclear Asset Ownership
Controllers and devices had been added over the years without a complete, current inventory of what existed or how critical each one was.

Flat, Under-Segmented Networks
Building systems shared network space with limited separation, making it easier for an issue in one area to reach another.

Loose Credentials & Access
Shared or default logins and broad vendor privileges made it hard to know exactly who could reach which systems.

Ageing, Unpatched Systems
Some servers and workstations ran outdated software with no formal, ongoing process for keeping them current.

Always-On Remote Access
Vendor and maintenance connections stayed open long after the work was done, with little record of what happened during the session.

No Eyes on the Network Itself
There was no tool-based way to see what normal BMS traffic looked like, let alone notice the moment something drifted from it.

WHY IT MATTERS

The building systems don't need to be attacked directly to be a way in

An intruder doesn't need to touch any flight-critical system to cause disruption. A realistic path runs from the internet or a compromised IT account, into the general network, across to the BMS, through an engineering workstation, and finally to a controller managing a real, physical process.

From there, the possibilities are uncomfortably practical: adjusting HVAC setpoints or stopping equipment outright, triggering false alarms or silencing real ones, changing operating schedules, or quietly disabling the very monitoring meant to catch this kind of activity. None of it requires anything exotic - it uses the same protocols and access paths that engineers rely on every day.

OT SECURITY TOOL-BASED ASSESSMENT

Asset discovery and vulnerability management, grounded in evidence - not assumptions

Gramax structured the engagement as a tool-based OT security assessment rather than a checklist-only review. The objective was to replace the airport's incomplete asset records with a verified, living inventory, and to convert that inventory into a prioritized, risk-ranked view of exposure - the foundation every later mitigation decision would rest on.

Asset Discovery

Velos Shield, a passive OT security and intelligence platform, was connected to the BMS network via SPAN ports with no agents installed and no active probing of controllers. Over the discovery window, it built a verified inventory of engineering workstations, BMS servers, controllers, sensors, actuators, and the protocols each one used. It also revealed communication relationships, unmanaged devices, forgotten remote-access endpoints, and shadow connections into adjacent systems—turning network traffic into an evidence-based operating baseline.

Vulnerability Management

Each discovered asset was fingerprinted—make, model, firmware, and version where the protocol exposed it—and correlated against known vulnerability and exposure data for that class of device. Findings were not left as a raw vulnerability list: Gramax's assessment team layered in operational context—what the asset controls, how exposed it is on the network, and what a credible attack path to it looks like—to separate theoretical exposure from risk that could genuinely affect airport operations.

> **OUTCOME**
> *A verified BMS asset inventory, a prioritised vulnerability register, and a continuously monitored behavioural baseline—each tied to business impact and available as an operating view the airport team could use beyond the initial assessment.*

THE APPROACH

Unlike conventional IT monitoring or one-time OT assessments, Velos Shield is positioned as a continuous OT intelligence layer. It passively learns the environment, identifies assets and communication patterns, correlates vulnerabilities with operational context, and helps teams distinguish routine engineering activity from behaviour that could affect safety, uptime, or service continuity.

A two-part approach: establish the baseline, then watch it continuously

Gramax paired its OT security assessment methodology with Velos Shield's passive OT security and intelligence platform—first to establish where the BMS environment stood, and then to keep it continuously monitored as the asset base, traffic patterns, vulnerabilities, and remote-access behaviour changed over time.

Baseline	Discover	Correlate	Monitor
Gramax-led assessment of assets, architecture, configurations and process.	Passive network visibility surfaces every asset and conversation.	Findings mapped to vulnerabilities and business-impact risk.	Velos Shield NIDS watches continuously against the baseline.

Phase 1 - Establishing the Baseline

A structured Gramax review of assets, network architecture, configurations, and working processes gave the team a clear, point-in-time picture of where the BMS stood against recognized OT security practices - the foundation everything else builds on.

Phase 2 - Watching Continuously

A snapshot goes stale the day after it's taken. The Velos Shield NIDS platform closes that gap by passively listening to network traffic - through mirrored ports, with no agents installed on sensitive controllers - and building a living picture of every asset and every conversation between them: who talks to whom, over which protocol, how often, and why.

> **HOW THE BASELINE IS USED**
>
> *A day-to-day pattern like the BMS server reading data from an air-handling unit controller is ordinary and expected. An engineering workstation suddenly writing commands to multiple controllers, or an unfamiliar device repeatedly querying equipment across the building, looks very different once that baseline exists - and is exactly the kind of activity conventional IT monitoring was never built to notice.*

HOW IT WORKED

Asset & Network Awareness
New or unknown devices, unexpected addresses, and changes to the network layout are surfaced as soon as they appear.

Protocol-Level Detection
Unauthorized commands and unusual command frequency stand out against the everyday rhythm of the building's own systems.

Cyber-Attack Indicators
Reconnaissance, lateral movement between systems, and repeated login attempts are recognized as patterns, not isolated events.

BMS-Specific Anomalies
Unexpected setpoint changes, abnormal controller restarts, and unusual access to critical equipment are flagged in context.

FROM RISK IDENTIFICATION TO MITIGATION

Turning telemetry into a decision the airport could act on

Discovery and detection tools generate signals. They do not, by themselves, tell an organisation what to fix first or how to act. That was Gramax's role throughout the engagement: translating asset inventory, vulnerability data, and NIDS telemetry into contextualised risk, clear priorities, and a practical remediation path for the airport's leadership and engineering teams.

Identifying Risk

- Consolidated the asset inventory and vulnerability findings into a single risk register, scored by likelihood and by the operational or safety consequence if the asset were compromised.
- Mapped realistic attack paths - from the internet or a compromised IT account, through the BMS, to a controller - so findings were understood in the context of how an intrusion would actually unfold, not in isolation.
- Reviewed access and remote-connectivity patterns surfaced by the platform to identify where vendor privileges and always-on sessions created unmanaged exposure.

Mitigating Risk

- Prioritized a remediation roadmap ordered by business impact, so the airport's engineering team addressed the highest-consequence gaps first rather than working through findings in discovery order.
- Defined a network segmentation plan separating the BMS from enterprise IT and from lower-trust zones such as the vendor jump server, reducing the paths an issue in one area could take to reach another.
- Set governance controls for vendor and remote-maintenance access - time-bound, reviewed, and logged - replacing always-on, shared-credential connections.
- Tuned Velos Shield NIDS detection policies against the agreed baseline and connected its alerting into the airport's SOC and incident-response process, so new risk is caught continuously rather than only at the next assessment cycle.

> **GRAMAX'S ROLE**
> *Velos Shield gave the airport the eyes on the network. Gramax gave the airport the judgment to act on what those eyes saw - from a prioritized risk register through to a segmentation and governance plan the engineering team could execute.*

SECURITY ARCHITECTURE

A layered design, built around how the building actually operates

Rather than a single perimeter, the recommended architecture layers defenses from the enterprise network down to the field devices themselves - so that a problem in one layer doesn't have a clear path to the next.

Enterprise IT	Airport SOC	OT Monitoring	OT DMZ	BMS Zone	Field Zone
The corporate network and its users.	Central monitoring and response.	Velos Shield NIDS, watching continuously.	Jump server and remote-access gateway.	BMS servers and engineering workstations.	Controllers, sensors, and actuators.

WHAT CHANGED

From scattered visibility to a shared, dependable picture

AREA	BEFORE	AFTER
Asset Visibility	Incomplete records of what controllers existed on the network	**Critical BMS assets identified and classified by business impact**

AREA	BEFORE	AFTER
Vulnerability Data	No structured, tool-based vulnerability view of BMS devices	**Correlated, risk-scored vulnerability register tied to real assets**
Network Design	Flat segments and legacy protocols with little separation	**A documented architecture with a clear segmentation roadmap**
Access Control	Shared credentials and loosely managed vendor access	**Vendor access controlled, time-bound, and reviewed**
Monitoring	No protocol-level insight into everyday BMS traffic	**Continuous, protocol-aware monitoring in place**
Detection & Response	Limited anomaly detection and incomplete vulnerability data	**Prioritized vulnerabilities with SOC-integrated detection**

BUSINESS & OPERATIONAL IMPACT

What continuous visibility means beyond the network diagram

Representative outcomes included improved visibility of BMS-connected assets, a prioritised risk register for remediation planning, reduced uncertainty around vendor access, and a continuous baseline for detecting changes in OT behaviour. Where customer-approved metrics are available, this section should quantify asset count, number of high-risk findings prioritised, reduction in unmanaged remote-access paths, and time taken to establish the baseline.

For airport leadership, the value was not only technical visibility. The engagement created a common view for facilities, engineering, cybersecurity, SOC, and executive teams: what assets exist, which systems matter most to operations, where vulnerabilities create real exposure, and which actions reduce the likelihood of service disruption.

- Reduced operational risk - fewer opportunities for unauthorized manipulation of building systems.
- Improved resilience—critical environmental and facility services had a clearer monitoring and response path during a cyber incident.
- Faster detection - moving from investigating after something goes wrong to spotting unusual behavior as it happens.
- Stronger vendor governance - full visibility into third-party remote access and contractor activity.
- Clearer executive visibility—technical findings translated into business-impact language, showing which BMS risks could affect comfort, equipment availability, service continuity, contractor governance, or incident response readiness.

CONCLUSION

The building systems are infrastructure now - not just facilities

An airport's Building Management System has quietly become a cyber-physical layer of critical infrastructure, not simply a facilities convenience. Connecting it to IP networks, enterprise IT, remote maintenance, and cloud services opened doors that traditional facilities practices were never built to defend.

Pairing a Gramax-led, tool-based OT security assessment with Velos Shield's continuous NIDS monitoring gave the airport something more durable than a snapshot: a verified asset inventory, a prioritized vulnerability and risk register, and an ongoing, shared understanding of what's on the network, how it normally behaves, and what deserves a closer look - the foundation for keeping terminal operations resilient as the environment keeps changing.

ABOUT

The partnership behind this engagement

GRAMAX CYBERTECH LIMITED

GRAMAX Cybertech Limited is a specialized cybersecurity company focused on safeguarding critical infrastructure and cyber-physical environments against modern cyber threats. Gramax brings together expertise across IT, OT, IoT, physical and edge environments to protect the systems that power essential operations across aviation, energy & utilities, maritime, manufacturing and urban infrastructure.

VELOS SHIELD

Velos Shield, a product of Rathon.AI, is an OT security and intelligence platform that delivers continuous, passive visibility across industrial and cyber-physical environments. It turns operational telemetry into asset intelligence, risk prioritisation, threat detection, and decision-ready security insights. Built for zero-downtime operations, it helps security, engineering, and business leaders see what matters, act with confidence, and protect critical operations.