

SOLUTION BRIEF

Your building is an industrial control system.
Almost nobody treats it like one.

Heating and cooling, power distribution, access control, cameras, lifts, lighting and fire systems are all controllers on a network, speaking industrial protocols, making decisions with physical consequences. In a plant, equipment like that sits inside a security programme. In a building, it is usually procured by facilities, installed by a contractor, connected to the corporate network and owned by nobody in security at all.

That gap is why facility systems keep appearing in incident write-ups as the way in, and why the people responsible for the building are frequently the last to hear about it.

WHY THIS ESTATE IS DIFFERENT FROM BOTH IT AND PLANT OT

Nobody owns it

Facilities owns the equipment, IT owns the network, security owns the risk, and the integrator who installed it left years ago. Every inventory question crosses at least two departments and usually stalls there.

It arrived through procurement, not IT

Building systems are bought as part of a construction or fit-out project. They rarely pass through an architecture review, and the as-built documentation is a commissioning document nobody has revisited.

The consequences are physical

Access control decides who gets through a door. Cooling decides whether a data hall stays up. These are not information risks, and treating them as low priority because they are not servers misreads the impact.

Contractor access is permanent and undocumented

Maintenance contracts routinely include remote access for the vendor. That path outlives the project, is rarely reviewed, and is often the most privileged route into the building estate.

WHAT WIRETRACE DOES HERE

WireTrace connects to a SPAN port or TAP and observes. Nothing is installed on any controller and nothing is transmitted onto the monitored network, which matters as much here as in a plant: a building controller mid-sequence is not something anyone wants a scanner interrogating.

QUESTION	ANSWERED FROM OBSERVED TRAFFIC
What building systems are actually connected?	Controllers, gateways, panels, cameras, readers and the equipment added by three different contractors, identified by vendor, model and firmware.
Are they where we think they are?	Whether the building network is genuinely separated from the corporate one, or joined by a shared gateway, a workstation or a rule that was meant to be temporary.
Who is reaching them?	Which systems and which external destinations the building estate communicates with, including manufacturer and maintenance connections nobody recorded.
Where is it exposed?	Unauthenticated management interfaces, credentials in the clear and default configurations, observed rather than assumed.
What changed after the last fit-out?	New devices and new relationships that appeared during works and were never removed afterwards.

PROTOCOL DEPTH ACROSS THE BUILDING ESTATE

Building protocols are read for the commands and values they carry rather than counted as sessions. Coverage includes **BACnet**, **Modbus**, **KNX**, **SNMP** for infrastructure and power management, **OPC** and **EtherNet/IP**, alongside the enterprise protocols the same systems use for management, identity and updates, within a set of more than 250 protocols across the whole estate.

WHERE IT APPLIES

ENVIRONMENT

Airports and transport hubs

Baggage handling, boarding systems, access control and building services on shared infrastructure, in an environment where an outage is a public event and the estate spans many contractors.

ENVIRONMENT

Data centres

Power distribution, UPS, cooling and environmental monitoring are the availability chain. They are operational technology by any reasonable definition, and they are frequently monitored only for faults rather than for security.

ENVIRONMENT

Hospitals as buildings

Separate from the clinical device estate, a hospital runs pressure regimes, cooling and access control that are patient-safety relevant in their own right.

ENVIRONMENT

Commercial and mixed-use estates

Offices, retail and stadiums where one building management platform spans many sites and one compromised gateway reaches all of them.

ENVIRONMENT

Campuses and universities

Decades of accumulated building systems from different eras and vendors, on a network that also carries research and student traffic.

ENVIRONMENT

Industrial sites, the other half

The plant gets attention and the building around it does not, despite sharing infrastructure and often sharing a route into the process network.

WHAT ORGANISATIONS TYPICALLY FIND

These recur across facility assessments. None is exotic, and that is the point: they persist because nothing was looking at the building estate at all.

- ✓ Building controllers reachable from **general user networks**
- ✓ Management interfaces running **default or shared credentials**
- ✓ Equipment communicating with **manufacturer services** nobody approved
- ✓ A gateway **bridging the building and corporate** networks
- ✓ Devices from a fit-out that **completed years ago**, still connected
- ✓ Contractor remote access **still live** after the contract ended

The organisational problem is usually harder than the technical one. Once you can show facilities, IT and security the same observed list of what is connected and what it talks to, the ownership conversation becomes possible. Before that, each team is describing a different estate from a different document and the discussion goes nowhere. An observed inventory is the thing all three can agree is true.

REGULATORY CONTEXT

Building systems fall inside the same asset management, network security and access control expectations as the rest of the estate, and are frequently the part that fails an assessment because nobody counted them. Evidence maps to **ISO 27001**, **NIST CSF 2.0** and, where the facility supports an industrial or critical process, **IEC 62443-3-3**, alongside the national frameworks that apply in your market.

Start with one building

A scoped assessment needs a mirror port where the building network aggregates, and a short observation window. It returns what is genuinely connected, how it is communicating and where it is exposed. Facilities teams are usually surprised by the count, and security teams by what the building can reach.

Book a demo at wiretrace.io/request-demo · or email sales@wiretrace.io