apis® Building Performance

APIS GUIDE 09 · BUILDINGS

The smart building *readiness checklist.*

A smart building is not a building with more sensors. It is a building whose data somebody acts on — and that is the layer nobody budgets for.

APIS · ENGINEERING & ADVISORY

25 pages · PDF · English
Issue v1.0 · 20 August 2026
apisgroup.net/guides-ebooks

ABOUT THIS GUIDE

Sensors are not *the answer.*

Most smart building projects deliver a working system that nobody uses. The devices are installed, the network is live, the dashboard exists, and eighteen months later the alarms are unread, the schedules have drifted back to the defaults, and the building consumes what it consumed before.

This is not a technology failure. The equipment usually works exactly as specified. It is a readiness failure: the building was not equipped to receive the system, the data was not structured so anyone could use it, and — the decisive one — nobody's job description changed when the system was switched on.

This guide covers what is actually being bought when someone says "smart building", the four layers a system is made of and why spend and failure sit at opposite ends of them, what metering and sensing you need before any of it is worth doing, the network and cybersecurity boundary, how data naming and ownership decide whether you are locked in, the people layer, how to specify and procure it, and how to prove afterwards that it worked. It ends with a forty-point checklist you can attach to a tender.

> WHAT THIS GUIDE DOES NOT CONTAIN, AND WHY
>
> **No product names, no platform recommendations, no prices, no payback figures and no percentage savings claims.** The smart building market has a shorter product half-life than any other subject in this series, and a named platform printed here would be superseded or acquired before the project it was quoted for finished.
>
> What it gives instead is the structure that does not change: the four layers, the questions that determine whether you own your own data, and the readiness conditions that decide whether any of it produces a result. Those are the same in 2026 as they were in 2016, and they will be the same in 2036.

Who this is written for

- Building owners and asset managers considering a smart building or BMS investment
- Facilities and technical managers who will inherit whatever is installed
- Public bodies and municipalities procuring building automation on their own estate
- Developers specifying controls for a new building, where most of this is cheaper to get right
- Boards, lenders and investment committees evaluating a proposal somebody else prepared

What this guide is not

It is not a design document and does not replace a controls engineer, a network architect or a security specialist. It covers **the readiness of a building and an organisation** to make use of building automation and analytics — not the design of the control system itself, not the design of the IT network, and not the underlying mechanical and electrical systems, which are the subject of other guides in this series.

How to use it

If you are considering an investment: work through Sections 01 to 03 before anyone is asked to quote — most of what determines success is settled there. If you have a proposal in front of you: Sections 04 to 07 are how to interrogate it. Section 09 is the checklist.

Contents

SECTIONS

APIS Ltd. (APIS sh.p.k.) · Rruga Prishtinë–Lipjan km 10, Livagjë, 10500 Graçanica, Republic of Kosovo · +383 49 787 233 · apisgroup.net
Document APS-GD-09, issue v1.0 of 20 August 2026. Prepared by APIS Engineering & Advisory.

SECTION 01

What is *actually being bought.*

"Smart building" describes at least five different purchases with different costs, different benefits and different failure modes. Establishing which one you want is the whole of the feasibility stage.

The term covers everything from a replacement heating controller to a portfolio analytics platform, and a proposal will happily use it for all of them. Before any budget is discussed, establish which of the following is the actual objective — because they are not stages of the same project and buying them in the wrong order wastes most of the money.

FIVE DIFFERENT PURCHASES

What is bought	What it does	What it depends on
Control	Plant runs when it should, at the right set point, in the right sequence. Weather compensation, optimum start, setback, zoning, interlocks	Nothing but itself. **This is where almost all the achievable saving is**, it is the cheapest layer, and it is routinely skipped in favour of the ones above it
Visibility	Somebody can see what the building is doing — consumption, temperatures, plant status, alarms	Metering and sensing that actually exists. Section 03. Visibility of nothing is a dashboard of nothing
Analytics	Software identifies faults, drift and waste from the data, rather than a person noticing	Both of the above, plus data that is named and structured so software can interpret it. Section 05
Occupant experience	Booking, access, wayfinding, environmental control by app, space utilisation	A different problem from the others, with different stakeholders and different privacy obligations. Frequently bundled in and rarely costed honestly
Reporting and compliance	Evidence for energy reporting, sustainability disclosure, certification or a lender's condition	Metering at the right boundaries, and data you can export. The requirement should be established before design — Section 07

THE ORDER THAT MATTERS

Control first. Then visibility. Then analytics.

Analytics applied to a building whose controls were never commissioned will identify, at considerable expense, the faults that commissioning would have fixed. Visibility installed on a building with no sub-metering will display a single incoming figure that the utility bill already told you.

The most common failure in this field is buying layer three to solve a layer one problem — and it is the most expensive, because analytics carries a subscription and commissioning does not.

Four claims to test in any proposal

1. **"It will save energy."** Ask through what mechanism. Better control saves energy. A dashboard does not save energy; a person acting on a dashboard does. If the saving depends on somebody changing behaviour, ask who that person is and whether they have been told — Section 06.

2. **“It is open.”** Ask which protocol, which version, and which functions are implemented. Section 05 sets out the difference between speaking a protocol and being open.
3. **“It is future-proof.”** Nothing is. Ask instead what happens when the platform is replaced in eight years: does the field wiring survive, do the devices survive, does the data come with you?
4. **“It integrates everything.”** Ask what the integration is for. Systems integrated because they can be, rather than because a decision depends on the combination, add cost, add attack surface and add failure modes without adding value.

> EXISTING BUILDINGS: FIND OUT WHAT IS ALREADY THERE FIRST
>
> Most commercial buildings already contain a building management system, often more than one, frequently unsupported and usually unused. Before specifying anything, establish: what is installed, what still functions, who holds the software and the passwords, whether the manufacturer still supports it, and what it is actually controlling today.
>
> This survey routinely finds that a substantial part of the proposed scope already exists and needs recommissioning rather than replacement — which is a much cheaper project with a faster result, and one no supplier will propose unprompted.

SECTION 02

The four layers, and where spend *and failure diverge.*

Money concentrates at the bottom. Failure concentrates at the top. Almost every disappointing project is explained by that single inversion.

A smart building system is four layers stacked on each other. Each depends entirely on the one below. The budget conversation is almost always about the bottom two, and the outcome is almost always decided by the top two.

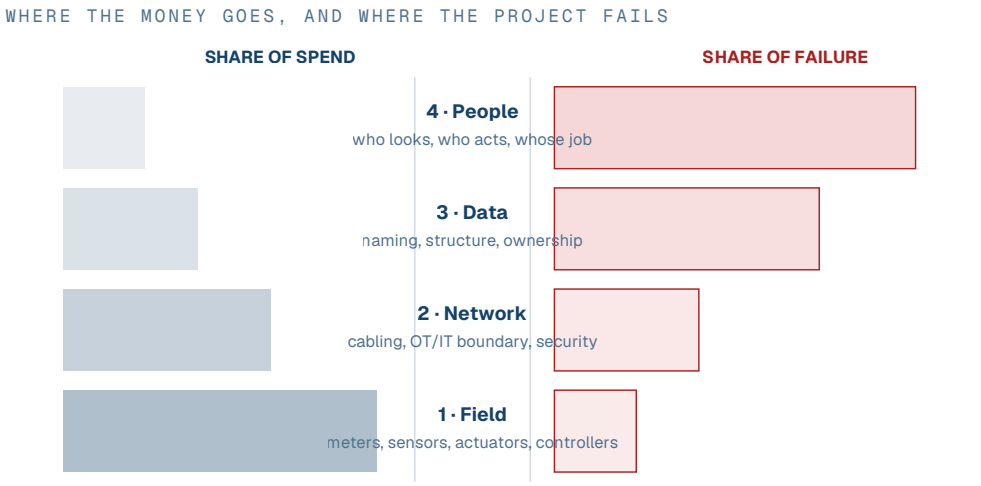

Figure 2.1 — The inversion. Spend is concentrated in the field layer; failure is concentrated in the people layer. Bar widths illustrate the relationship only and are not derived from any dataset.

What each layer is, and what it costs to get wrong

Layer	Contains	Consequence of getting it wrong
1 · Field	Meters, sensors, valves, dampers, actuators, variable speed drives, field controllers and the wiring between them	Expensive and disruptive to correct, because it is physical and distributed through an occupied building. Get this right first time or accept a second installation
2 · Network	The cabling and communications carrying data from field devices to wherever it is processed, and the boundary between operational technology and corporate IT	Moderately expensive to correct, and the layer where a security exposure is created that nobody notices until it is exploited. Section 04
3 · Data	How points are named, how they are structured, where they are stored, who owns them and whether you can export them	**Cheap to get right at design stage and effectively impossible to correct later.** This is where lock-in is created. Section 05
4 · People	Who reads the output, who is authorised to act on it, whose objectives it belongs to and how much of their week it occupies	Costs almost nothing and is almost always omitted. A system nobody is responsible for produces no result at all, however well the other three layers are built. Section 06

THE QUESTION THAT PREDICTS THE OUTCOME

“After this is installed, whose job is it to look at it, how often, and what are they expected to do about what they see?”

Ask it at proposal stage. If the answer is a name, a frequency and a defined action, the project has a reasonable chance. If the answer is “the FM team will monitor it” or “the system is self-optimising”, layer four does not exist and the investment will be assessed in two years as having underdelivered.

This is not a criticism of suppliers. Layer four is not theirs to provide, and no supplier can sell you an owner. It is the buyer’s to build, and it is the cheapest part of the project.

What to do about the inversion

1. **Budget layer four explicitly**, as time rather than capital. A defined fraction of a named person’s week, written into their objectives — see Section 06.
2. **Spend on layer three at design stage**, when a naming convention costs a conversation. After commissioning it costs a re-tagging exercise across every point in the building.
3. **Phase layer one**, because it is the expensive one and because a smaller field layer that is actually used beats a comprehensive one that is not. Section 03 sets out where to start.
4. **Do not let layer four be someone’s fifth priority.** If nobody’s objectives change, nothing changes.

SECTION 03

Layer one — *metering and sensing.*

You cannot manage what you do not measure, and you cannot measure what nobody installed. Where to start, and where to stop.

Metering is the foundation of every layer above it. A building with a single incoming meter can be controlled but not analysed: the data tells you the total and nothing about where it went. The question is not whether to sub-meter but where the boundaries should fall.

Where to put the boundaries

Meter where a decision could be made, or where a cost must be allocated. Metering anywhere else produces data that is collected, stored and never used.

METERING BOUNDARIES, IN PRIORITY ORDER

Boundary	Why it earns its place
Incoming supply, every fuel	The baseline for everything. Interval data, not monthly totals — see Guide 05 in this series
Major plant — heating, cooling, ventilation	The largest consumers, and the ones a control change affects. Without this, no control improvement can be demonstrated
Lighting, where separately distributed	Straightforward to meter and straightforward to act on
Tenant or cost-centre boundaries	Where energy is recharged, or where a department's consumption is its own responsibility
Any single large process or IT load	Where one load is big enough that its behaviour matters on its own
On-site generation and storage	Generation, export and self-consumption cannot be evidenced otherwise. See Guides 03 and 06
Water, and any other billed utility	Frequently omitted, and leaks are invisible without it

> METERING FOR BILLING IS A DIFFERENT REQUIREMENT
>
> Where a meter's reading will be the basis of a charge to a third party — a tenant, a concession, a shared-service partner — it must generally be of a type approved for that purpose in your jurisdiction. That approval cannot be added afterwards. Establish the requirement before procurement, because discovering it later means replacing meters or not billing.

Sensing — and the discipline of not over-sensing

Sensors have become cheap enough that specifying too many is now easier than specifying too few, and a large sensor count is frequently presented as evidence of sophistication. Every sensor is a device to be installed, powered, addressed, named, maintained, calibrated and eventually replaced.

- **Space conditions** — temperature, and humidity where the building needs it controlled. The basis of both comfort control and complaint resolution
- **Indoor air quality**, where ventilation is to be demand-controlled. This is one of the clearest cases: the sensor pays for itself by not ventilating an empty room
- **Occupancy or presence**, where lighting, ventilation or heating are to respond to it. Note the privacy dimension — Section 05
- **Plant condition** — flow and return temperatures, pressures, differential pressure across filters, run hours, status and fault contacts. Unglamorous and the most useful data in the building for maintenance
- **External conditions** — a local weather sensor, without which weather compensation is running on an assumption
- **Water and leak detection**, in plant rooms and above sensitive spaces. Low cost, occasionally decisive

> THE TEST FOR EVERY PROPOSED SENSOR
>
> **“What decision or automatic action changes as a result of this reading, and who or what makes it?”**
>
> If the answer is that it will appear on a dashboard, it is not a sensor — it is a future maintenance item and a line in a subscription. Ask the question of every point in the schedule, and expect the schedule to get shorter.

Calibration, drift and the credibility of everything above

Sensors drift. A temperature sensor reading two degrees high will cause the control system to do exactly the wrong thing, indefinitely, with complete confidence — and an analytics platform built on it will generate confident, wrong conclusions.

Specify, at procurement: the calibration requirement and interval for each sensor type, who performs it, how a drifting or failed sensor is detected and flagged, and what the control strategy does when a sensor fails. **A control system that fails safe on sensor loss is a specification item, not an assumption.**

> IF THE BUILDING ALREADY HAS SOME OF THIS
>
> Existing meters and sensors are frequently present, unconnected and forgotten — installed for a previous project, a previous tenant or a previous certification. Survey them before specifying new ones: their location, whether they still work, whether they can be read, and whether they are on a protocol anything can talk to.
>
> Connecting an existing meter is a fraction of the cost of installing a new one, and this survey routinely reduces the field layer scope more than any other single action.

SECTION 04

Layer two — the network *and the OT/IT boundary.*

The layer where a building becomes connected to the outside world, and where that connection becomes somebody's responsibility — or nobody's.

Building automation was for decades a closed world: proprietary cabling, no external connection, and a security model that consisted of a locked plant room door. Every trend in the field — remote access, cloud analytics, integration with corporate systems — has dismantled that model, and most existing buildings have made the transition without anyone deciding to.

Operational technology is not information technology

The distinction matters because the two are governed by different priorities, and applying the wrong set is how both security incidents and operational failures occur.

Concern	Corporate IT	Building operational technology
First priority	Confidentiality of data	**Availability and safety.** A heating system that stops is an operational event; in some buildings it is a safety event
Patching	Frequent, often automatic	Infrequent, requires testing, and a controller may not be patchable at all
Equipment life	Three to five years	Ten to twenty years, sometimes longer than the manufacturer
Downtime for maintenance	Scheduled and accepted	Constrained by occupancy, weather and process
Who administers it	An IT function with defined ownership	Frequently the installing contractor, remotely, under an arrangement nobody has reviewed

THE THREE QUESTIONS THAT EXPOSE MOST OF THE RISK

One. Who can reach this system from outside the building today? Name them. The answer usually includes at least one contractor, and occasionally a contractor who no longer works for you.

Two. What would happen if that access were misused? Not stolen data — consider what an attacker could do by changing set points, disabling alarms or stopping plant. In a hospital, a cold store or a data centre, that is a serious question.

Three. Who is accountable for this system's security — by name? If the answer is that IT assumes the controls contractor handles it and the controls contractor assumes IT handles it, which is the common case, then nobody does.

What to require, at procurement

IEC 62443 is the international series addressing security for industrial automation and control systems, and it is the right framework to name in a specification. ISO/IEC 27001 governs the organisational information security management system within which it sits. Neither is a substitute for the specific requirements below.

- **Network segregation.** The building control network separated from the corporate network and from any guest network, with the boundary defined and controlled. This is the single most effective measure and it is a design decision, not a product
- **No shared or default credentials.** Individual accounts, and a documented process for removing access when a person or a contractor leaves. Default passwords on field controllers are endemic and are the most common finding in any assessment
- **Remote access under your control** — through your own mechanism, logged, with access granted for a defined purpose and revoked afterwards. Not a permanent connection installed by the contractor for their convenience
- **An asset inventory** of every connected device, its firmware version and its support status. You cannot secure what you have not listed
- **A patching and support position**, stated per device: what is patchable, by whom, how often, and what happens when the manufacturer ends support before you end use
- **Logging** of who connected, when, and what they changed. This is also how a drifted set point is traced back to a cause
- **Defined failure behaviour.** What the building does if the network fails, if the cloud connection fails, or if the platform provider ceases to operate. **Local control must survive the loss of everything above it** — this is a specification requirement and should be demonstrated at commissioning

> CLOUD DEPENDENCY IS A DESIGN DECISION, NOT A DETAIL
>
> Where a control function depends on a connection to an external platform, an internet outage becomes a building services outage. For scheduling and analytics that is usually acceptable. For anything affecting safety, statutory function or a critical process it is not.
>
> Require the proposal to state, function by function, what continues to work when the connection is lost — and require it to be demonstrated during commissioning by disconnecting the link and observing the building, rather than by accepting the answer in writing.

Cabling and physical infrastructure

The cabling is the part with the longest life and the least attention. It will outlast the controllers, probably the platform, and possibly the building's current use.

- **Structured, documented and labelled**, with as-built records that reflect what was actually installed rather than what was drawn
- **Spare capacity and spare containment**, since adding a cable later in an occupied building costs a multiple of adding it during installation
- **Segregation from power** and appropriate protection in plant rooms and risers
- **Where wireless devices are proposed**: establish battery life and the replacement programme, the coverage survey that supports the design, what interference the building environment presents, and how a failed device is detected. Wireless removes cable cost and introduces a maintenance population

SECTION 05

Layer three — data, naming *and who owns it.*

The cheapest layer to get right, the most expensive to correct, and the one where lock-in is created without anybody noticing.

Every point in a building automation system has a name. In a system installed without a convention, those names are whatever the commissioning engineer typed — abbreviations, panel references, a previous project's conventions, and occasionally the room number of a room that has since been subdivided.

For a person reading one screen, this is a nuisance. For any software attempting to interpret the building — analytics, reporting, a future platform migration — it is fatal, because the software cannot tell what a point represents. This is the single most common reason an analytics investment fails to deliver: the data arrives and nothing can be inferred from it.

> SPECIFY THE NAMING CONVENTION BEFORE COMMISSIONING, NOT AFTER
>
> A point naming and tagging convention costs a conversation at design stage. Applied retrospectively across a whole building it is a re-tagging project — every point identified, interpreted, renamed and re-verified — and it is charged as one.
>
> **Require the convention to be agreed and issued before commissioning begins, and require the as-built point schedule to be delivered in it.** It is one paragraph in a specification and it protects everything above layer three.

What a workable convention contains

The specific scheme matters far less than having one and applying it consistently. Any convention should let a reader — human or software — determine, from the name alone:

- **What the point is** — a temperature, a status, a set point, a command, a meter reading
- **What equipment it belongs to**, identified consistently with the asset register and the as-built drawings
- **Where that equipment is** — building, floor, zone or room, in an identifier that survives a change of tenant
- **What it serves**, where that is not obvious from the equipment
- **Its units and its expected range**, so that an implausible value can be detected automatically

Industry tagging schemas exist for exactly this purpose and are worth adopting rather than inventing a scheme. **Establish which your adviser proposes, whether the platform supports it natively, and whether the tags travel with an export** — a schema applied only inside one platform does not solve the migration problem it was adopted to solve.

Protocols — and what "open" actually has to mean

Openness is claimed universally and delivered variably. Naming a protocol in a specification is necessary and not sufficient.

THE PROTOCOLS YOU WILL ENCOUNTER

Protocol	What it is
BACnet	The principal open protocol for building automation, standardised internationally as ISO 16484-5. The usual answer for plant-level integration
Modbus	A long-established industrial protocol, widely implemented in meters, drives and plant. Simple, ubiquitous, and carries no semantic information — a Modbus register is a number with no indication of what it means, which is why naming matters
KNX	An open standard for building electronic systems, standardised within the ISO/IEC 14543-3 series. Common in lighting, blinds and room control
MQTT	A lightweight messaging protocol widely used to carry device data to a platform. A transport, not a data model — it moves values without defining what they mean
Proprietary protocols	Still present, particularly in older installations and in some manufacturers' field-level networks. Not disqualifying at field level, provided the boundary above them is open

FOUR QUESTIONS THAT SEPARATE OPEN FROM "SUPPORTS OPEN"

One. Which protocol, which version, and which objects or functions are implemented? Partial implementations are common and are sufficient to read values while remaining insufficient to configure, command or migrate.

Two. Can a third party — not the installer — connect to this system, read every point, and change configuration, using standard tools? Ask for the mechanism, not the assurance.

Three. Name a project where this equipment has been migrated to a different front end or platform. A supplier who can is telling you something; a supplier who cannot is telling you something else.

Four. What is proprietary above the open layer? Frequently the field devices speak an open protocol and the configuration tool, the engineering software or the licence model does not — which is enough to lock in every purpose that matters.

Ownership — the questions to settle before contract

The data itself	Who owns the point data and the historical record? Can you export all of it, in a documented format, at any time and at the end of the contract? Establish this in the contract, not in a conversation
Historical data on exit	What happens to years of history when you change provider? Data that cannot leave is data that cannot inform the next system, and it is the thing you will most want
Engineering software and licences	Do you hold them, or does the installer? A building whose control strategy can only be modified by one company is a building with one supplier for twenty years
Credentials at every level	Including engineering-level access to field controllers. Obtain them at handover and verify they work — this is a handover test, not a paperwork item
Source of the control strategy	The programmed logic, documented, in a form somebody else could read and modify
Subscription terms	Cost per point or per building, term, price protection, and what the system does if the subscription lapses. Over ten years this frequently exceeds the installation cost

WHERE OCCUPANCY DATA BECOMES PERSONAL DATA

Presence detection, desk utilisation, access control records, camera-derived counting and app-based booking can identify individuals and their movements, whether or not that was the intention. Where they do, personal data protection obligations apply.

Establish before specifying: what is collected, at what granularity, what the lawful basis is, how long it is retained, who the processor is and where it is held, and what employees and visitors are told. In Kosovo and the surrounding region this is governed by the applicable personal data protection law, and it is a question for counsel rather than for the systems integrator. Aggregating or anonymising at the point of collection is frequently sufficient for the purpose and removes the obligation — but it must be designed in, not retrofitted.

SECTION 06

Layer four — *the people layer.*

Costs almost nothing, is almost always omitted, and determines whether any of the other three produce a result.

A building automation system generates findings. Somebody has to read them, judge which matter, act on them, and verify that the action worked. Where that person does not exist, the system produces an accurate and continuous record of a building performing exactly as badly as it did before.

This is not a training problem, and it is not solved by a better dashboard. It is an organisational problem: the work is real, recurring and unallocated.

WHAT LAYER FOUR ACTUALLY REQUIRES

1. **A named person.** Not a team, not a function — a name, with a deputy.
2. **Defined time.** A stated fraction of their week. Half a day a month with a consumption chart finds more than most retrospective audits, but only if it is protected time rather than time that exists in principle.
3. **Authority to act.** Permission to change a schedule or a set point without raising a request that takes three weeks. Where the authority is missing, findings accumulate unaddressed and the person stops looking.
4. **An escalation route** for anything beyond their authority or competence, with somebody obliged to respond.
5. **It in their objectives.** If building performance is not something they are measured on, it is their fifth priority, and their first four will always win.

What the routine looks like

Frequency	Activity
Daily, briefly	Critical alarms only. The list must be short enough to read — see below
Weekly	Consumption against expectation; anything running outside its schedule; complaints logged against what the system shows
Monthly	Consumption normalised against weather and occupancy — the method in Guide 05 of this series; open findings reviewed and closed; set points verified against the commissioned schedule
Seasonally	Heating and cooling changeover behaviour; verification that the strategy responds as intended at the edges of the year
Annually	A structured review — has performance drifted, which findings were never closed, what should change, and is the system still doing what it was bought to do

Alarm discipline — the reason most systems stop being read

A system that raises hundreds of alarms trains its operator to ignore all of them, and after a few weeks the alarm list is a permanent scrolling background nobody reads. Once that happens, the genuine fault is invisible and the system has ceased to function regardless of its technical state.

Alarm rationalisation is therefore not housekeeping; it is what keeps layer four alive:

- **Every alarm has a defined response.** If nobody would do anything about it, it is not an alarm — it is a log entry
- **Priority levels that mean something**, with a small critical set that is genuinely critical and warrants a call
- **Standing alarms are resolved or removed.** An alarm that has been active for three months is not conveying information
- **Review the alarm list itself** at defined intervals, and treat a growing list as a fault in the system rather than a fault in the building

Require alarm rationalisation as a deliverable in the specification, with the list reviewed and agreed at handover — not as a page of defaults inherited from the manufacturer.

> THE HANDOVER THAT ACTUALLY TRANSFERS CAPABILITY
>
> Training delivered on the last day of a project, to whoever is available, is attendance rather than transfer. Specify instead:
>
> - Training for **named individuals**, at their competence level, with the operational routine above as its subject rather than a tour of the software
> - A **second session after the first season**, when the building has done something the operator did not expect and the questions are real
> - **Documentation written for an operator** — what each strategy does, why each set point is what it is, and what to do when a specific thing happens
> - A **defined support route** for the first year, with response times, so the operator has somewhere to go before they give up
>
> And plan for the person leaving. A building that depends on one individual's undocumented knowledge reverts to defaults within a year of their departure.

SECTION 07

Specifying *and procuring it.*

What has to be in the tender documents, because none of it can be added afterwards without paying twice.

A generic controls specification produces a system that works, is closed, is named inconsistently and is understood only by the company that installed it. Every one of those outcomes is avoided by a paragraph in the specification, and each is expensive to reverse.

What the specification must state

THE CLAUSES THAT DECIDE THE OUTCOME

Clause	What to require
Objective	Which of the five purchases in Section 01 this is, and what it must achieve. Without it the tender is priced on equipment
Points schedule	Every point required, by system, with type and units — issued by you, not proposed by the tenderer. This is the document that makes offers comparable
Naming and tagging convention	Stated, and required to be applied before commissioning. Section 05
Protocols	Named, with version and the functions required to be implemented. Section 05
Control strategies	Described in words: what each system does, under what conditions, with what interlocks and what fail-safe behaviour. Not left to the tenderer's standard library
Set points and schedules	Required to be documented with the reason for each value, and issued at handover as a schedule
Network and security	Segregation, credential management, remote access mechanism, logging, asset inventory, patching position. Section 04
Failure behaviour	What the building does on loss of network, loss of cloud connection, loss of a sensor, and loss of the platform provider. To be demonstrated, not asserted
Alarm rationalisation	Required as a deliverable, with the list reviewed and agreed at handover. Section 06
Data ownership and export	Ownership, export format, export at any time and at end of contract, and retention of history on exit
Software, licences and credentials	Held by the client, delivered at handover, and verified to work before the final payment
Training	Named individuals, defined content, and a second session after the first season
Documentation	As-built points schedule in the agreed convention, strategy descriptions, set point schedule with reasons, network diagram, asset inventory
Support and subscription	Cost per year, term, price protection, behaviour on lapse, and response times

ISSUE THE POINTS SCHEDULE YOURSELF

The single highest-return action available in a controls tender. When each tenderer proposes their own points list, the offers are not comparable — the cheapest is cheapest because it has fewer points, and nobody notices until commissioning.

A points schedule issued with the tender makes every offer price the same system, exposes what each has excluded, and becomes the checklist against which commissioning is verified. It takes a day to produce and it is the document a controls tender most often lacks.

Commissioning — the part that is cut when the programme slips

Controls commissioning is the last activity before handover and the first to be compressed. It is also where the entire benefit is realised: an uncommissioned control system is a set of devices running on factory defaults.

- **Point-to-point verification** — every point proved to read the right value from the right device, in the right units, with the right sign. Sensors reading the wrong sign are common and produce confidently wrong control
- **Strategy verification** — each control sequence exercised and observed doing what the specification says, including at the edges: startup, shutdown, changeover, fault
- **Failure mode testing** — sensor disconnected, network disconnected, cloud connection removed, and the building observed. Section 04
- **Set point and schedule documentation** as commissioned, with reasons
- **Alarm list rationalised** and agreed
- **Seasonal verification** — a return visit in the opposite season, written into the contract and priced within it. A system commissioned in summer has not been proved in heating, and without the clause the visit becomes a variation and does not happen

MAKE THE LAST PAYMENT DEPEND ON THE HANDOVER PACK

The as-built points schedule, the strategy documentation, the set point schedule, the credentials and the licences are all easy to obtain before final payment and very difficult afterwards. Tie a defined retention to their delivery and verification, and verify by using them — log in with the credentials, open the engineering software, export the data — rather than by receiving a folder.

Existing buildings — sequence the work

1. **Survey what exists** and establish what still works, what is supported and who holds the keys. Section 01
2. **Recommission what is there** before replacing it. On many buildings this delivers most of the available benefit at a fraction of the cost, and it establishes whether the building responds as expected
3. **Fill the metering gaps** at the boundaries that matter. Section 03
4. **Then extend or replace**, with the naming convention, the protocols and the ownership terms settled first

A supplier will rarely propose step two, because it is the smallest project available. It is also frequently the right one, and doing it first makes the case for steps three and four evidenced rather than assumed.

SECTION 08

What it costs to own, *and proving it worked.*

No figures here — only the structure of the cost, and the method for demonstrating a result that a finance director will accept.

The cost structure

Field devices and installation	Meters, sensors, actuators, controllers, panels, and the labour to install them in an occupied building
Cabling and containment	The longest-lived element. Spare capacity here is cheap now and expensive later
Network and security	Segregation, hardware, and the design work behind the OT/IT boundary
Software, platform and licences	Initial licences and any per-point or per-building charge
Engineering and commissioning	Strategy design, configuration, point-to-point verification, seasonal return visit. The item that is compressed when the programme slips
Documentation and training	Small, and the difference between a system that is operated and one that is not
Recurring — subscription	Per year, per point or per building. **Over ten years this frequently exceeds the installation cost** and it is rarely shown alongside it
Recurring — maintenance and calibration	Sensor calibration, device replacement, battery replacement on wireless devices
Recurring — the people layer	Time, not capital. Budget it explicitly. Section 06
Replacement within life	The platform and the controllers will be replaced at least once within the life of the cabling and the field devices. This belongs in the case from the start

> COMPARE ON LIFETIME COST, NOT ON THE INSTALLATION PRICE
>
> Two proposals with similar installation prices can differ substantially over ten years once the subscription, the licence model and the eventual platform replacement are included — and the cheaper installation is frequently the one tied to the more expensive platform, because that is where the supplier's return sits.
>
> Guide 07 in this series sets out how to build that comparison and how to write it into a tender so that bidders compete on it. Building controls is a case where it changes the answer more often than not.

Proving it worked

The benefit of a controls investment is a reduction in consumption, a reduction in reactive maintenance, or a reduction in complaints. All three are measurable, and none is measurable without a baseline established before the work.

1. **Establish the baseline before anything is installed.** Twelve months of interval data, normalised for weather and occupancy — the method is set out in Guide 05 of this series. This is the step that cannot be recovered afterwards: once the system is in, the pre-installation building no longer exists to be measured.

2. **Record the reactive call rate and the complaint rate** for the same period. Both are frequently the more persuasive number, and both are free to collect.
3. **Agree the verification method before contract** — what will be measured, over what period, adjusted for what, and by whom. Where a supplier offers a performance guarantee, this is the mechanism that makes it enforceable rather than decorative.
4. **Report against it at defined intervals**, and treat a divergence as a fault to investigate rather than a number to explain.

> SAVINGS DRIFT, AND DRIFT IS INVISIBLE WITHOUT MONITORING
>
> Control improvements decay. Set points are overridden in response to a complaint and never restored; a schedule is extended for an event and stays extended; a device fails and its function is bypassed; a strategy is disabled during a fault and never re-enabled. Each is a small, locally reasonable decision, and together they return the building to where it started within a few years.
>
> The counter-measure is the monthly routine in Section 06, and specifically the comparison of the current set point schedule against the one commissioned. That single check catches most of it, and it takes minutes.

On savings claims generally. Any percentage saving quoted for a building controls investment depends on how the building is controlled today, its condition, its occupancy, its climate and whether anybody will operate the system afterwards. A figure quoted before someone has read your interval data and examined your current control strategy is marketing, not engineering. Establish the baseline first; everything after it can be assessed honestly.

SECTION 09

The forty-point *readiness checklist.*

Attach it to the tender. If every box can be ticked before contract, the system will still be in use in three years.

A · BEFORE ANYTHING IS SPECIFIED

- ☐ Which of the five purchases this is, stated in one sentence
- ☐ Control, visibility and analytics sequenced in that order, not bought together
- ☐ Existing systems surveyed — what is installed, what works, who holds the keys
- ☐ Recommissioning of existing systems considered and priced before replacement
- ☐ Twelve months of interval data secured as the baseline, before any work begins
- ☐ Reactive call rate and complaint rate recorded for the same period
- ☐ Any reporting, certification or lender requirement established before design
- ☐ Whether energy will be billed to third parties established, for metering approval

B · FIELD LAYER

- ☐ Metering boundaries set where a decision is made or a cost allocated
- ☐ Existing meters and sensors surveyed and reused where possible
- ☐ Every proposed sensor justified by a decision or automatic action it changes
- ☐ Billing-approved metering specified where energy is recharged
- ☐ Calibration requirement and interval stated per sensor type
- ☐ Sensor failure detection and fail-safe control behaviour specified
- ☐ Wireless devices: battery life, replacement programme and coverage survey established

C · NETWORK AND SECURITY

- ☐ Building control network segregated from corporate and guest networks
- ☐ Everyone with external access to the system named, and stale access removed
- ☐ A named individual accountable for the system's security
- ☐ Individual credentials required; no shared or default passwords accepted
- ☐ Remote access under client control, logged, granted and revoked by purpose
- ☐ Asset inventory of every connected device with firmware and support status
- ☐ Patching position stated per device, including end-of-support handling
- ☐ Failure behaviour specified for loss of network, cloud and platform provider
- ☐ Local control proved to survive loss of the connection, by demonstration
- ☐ Cabling documented, labelled, segregated, with spare capacity and containment

D · DATA AND OWNERSHIP

- ☐ Naming and tagging convention agreed and issued before commissioning
- ☐ As-built points schedule required to be delivered in that convention
- ☐ Protocols named with version and required functions implemented
- ☐ A migration reference obtained — a project where this equipment moved platform
- ☐ Data ownership, export format and export at any time agreed in contract
- ☐ Retention of historical data on exit agreed
- ☐ Engineering software, licences and credentials held by the client and verified at handover
- ☐ Control strategy source documented in a form another party could modify
- ☐ Occupancy and personal data: lawful basis, retention and processor established with counsel

E · PEOPLE, COMMISSIONING AND PROOF

- ☐ A named person, with a deputy, defined time, authority to act and it in their objectives
- ☐ Alarm rationalisation required as a deliverable and agreed at handover
- ☐ Point-to-point verification, strategy verification and failure mode testing all specified
- ☐ Seasonal return visit written into the contract and priced within it
- ☐ Training for named individuals, plus a second session after the first season
- ☐ Verification method for the claimed benefit agreed before contract, against the baseline

Readiness sign-off

Complete and retain with the tender documents.

SMART BUILDING READINESS SIGN-OFF

Item	Name and role	Date and signature
Building and objective		
Baseline period and data source		
Existing systems survey by		
Named operator (layer four)		
Security accountability held by		
Checklist points 1–40 confirmed		
Released for tender by		

IF YOU CAN ONLY DO THREE THINGS

One. Name the person whose job it is to look at the output, give them the time and the authority, and put it in their objectives. Layer four costs nothing and decides everything.

Two. Agree the naming convention and the data ownership terms before commissioning. Both are free at design stage and effectively unrecoverable afterwards.

Three. Establish the baseline before anything is installed. Once the system is in, the building you were trying to measure no longer exists.

REFERENCE

Standards referred to *in this guide.*

Listed by number and subject so that you can obtain and read them. Confirm the current edition and the applicable national adoption before citing any of them.

STANDARDS REGISTER

Reference	Subject
ISO 16484 series	Building automation and control systems — including project specification and implementation, hardware, functions, and the data communication protocol
ISO 16484-5	Building automation and control systems — data communication protocol, the international standardisation of BACnet
EN ISO 52120-1	Energy performance of buildings — contribution of building automation, controls and building management, superseding the former EN 15232
ISO/IEC 14543-3 series	Home and building electronic systems — the standardisation within which KNX sits
IEC 62443 series	Security for industrial automation and control systems — the framework to name for operational technology security
ISO/IEC 27001	Information security management systems — the organisational framework within which the above sits
ISO 50001	Energy management systems
ISO 50006	Measuring energy performance using energy baselines and energy performance indicators
EN 16247 series	Energy audits — general requirements and the building-specific part
ISO 41001	Facility management — management systems
ISO 19650 series	Organization and digitization of information about buildings — information management using building information modelling, relevant to asset data handover
EN 15232	Superseded by EN ISO 52120-1. Listed because it is still cited in older specifications and literature

PROTOCOLS AND SCHEMAS REFERRED TO

BACnet	Building automation data communication protocol, standardised as ISO 16484-5
Modbus	An industrial communication protocol in general use. Carries values without semantic information
KNX	Building electronic systems, standardised within ISO/IEC 14543-3
MQTT	A lightweight publish-subscribe messaging transport in wide use for device data. A transport, not a data model
Tagging schemas	Industry data-tagging conventions for building points exist and are worth adopting rather than inventing a scheme. **Establish which your adviser proposes and whether the platform supports it natively** — these are industry conventions rather than international standards, and support varies

HOW TO USE THIS REGISTER — AND WHAT GOVERNS ABOVE IT

Standards are revised, withdrawn and superseded. Verify the current edition with the national standards body applicable to your project, and confirm that the clause you intend to rely on still says what you think it says. Nothing in this guide should be relied upon as a statement of the content of any standard, protocol or schema.

Two matters govern above all of the above. Where a smart readiness, energy performance or sustainability reporting requirement applies to your building, that requirement governs the evidence the system must produce — and those frameworks are national, developing and must be established for your jurisdiction at the time of the project. And where occupancy or access data identifies individuals, the applicable personal data protection law governs above any technical consideration in this guide.

About APIS

APIS is an integrated engineering group founded in Kosovo, operating across the Western Balkans and into the European Union. The Group delivers mechanical, electrical, energy and infrastructure works through twenty-one delivery divisions across two strategic business units — Building Systems & Technologies, and Energy, Industry & Infrastructure — supported by four engineering excellence centres. APIS operates management systems certified to ISO 9001, ISO 14001, ISO 45001 and ISO 50001.

The **Engineering Excellence Centres** provide cross-disciplinary technical advisory work, including building automation strategy, metering and monitoring design, controls specification and commissioning, and the operational routines that keep a system in use after handover. Because APIS also designs, installs, commissions and maintains the systems it specifies, its recommendations come from operating buildings rather than from a product catalogue — which matters most at the layer-four questions in Section 06.

Prepared by APIS Engineering & Advisory · **Document** APS-GD-09 issue v1.0 of 20 August 2026 · **Contact** apisgroup.net/contact

Have a building management system *that nobody reads?*

Most buildings do. Our engineers will survey what is already installed, establish what still works and who holds the keys, recommission what is there before anything is replaced, and build the operational routine that keeps it in use — because a system nobody owns produces no result, however well it was installed.

SPEAK TO APIS ENGINEERING & ADVISORY

Existing system survey and recommissioning · metering and monitoring design · controls specification and points schedules · OT/IT boundary and security review · data ownership and migration · commissioning and seasonal verification · operational routines and training

apisgroup.net/contact · +383 49 787 233

More free guides, playbooks and checklists from APIS engineers:
apisgroup.net/guides-ebooks

APIS Ltd. · APIS sh.p.k.
Rruga Prishtinë-Lipjan km 10, Livagjë
10500 Graçanica, Republic of Kosovo
APS-GD-09 v1.0 · 20.08.2026

apis® Building Performance