

A building management head end at night. Every schedule on these screens can be outranked by one override nobody cleared.

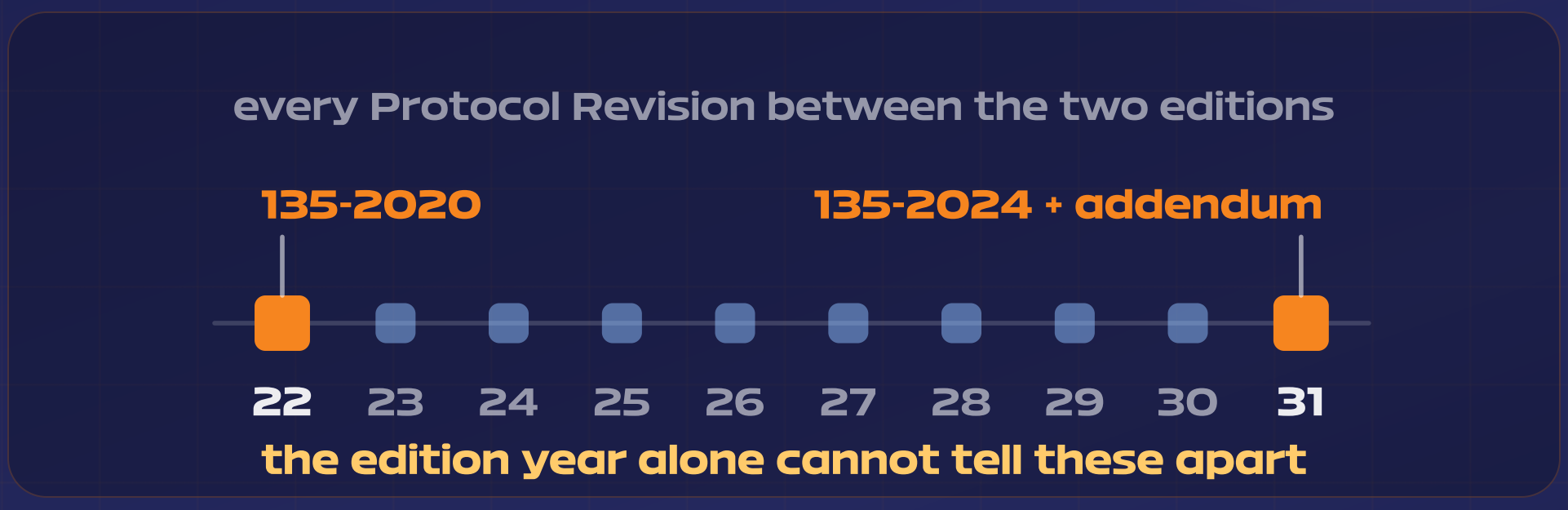
NLC ACADEMY · EPISODE 25

The building is obeying someone else.

BACnet, Modbus and the integration layer where the project money actually goes. Starting with the mechanism that quietly stops a building responding to its own schedule.

GET THE VERSION RIGHT

Cite the Protocol Revision, not the edition year



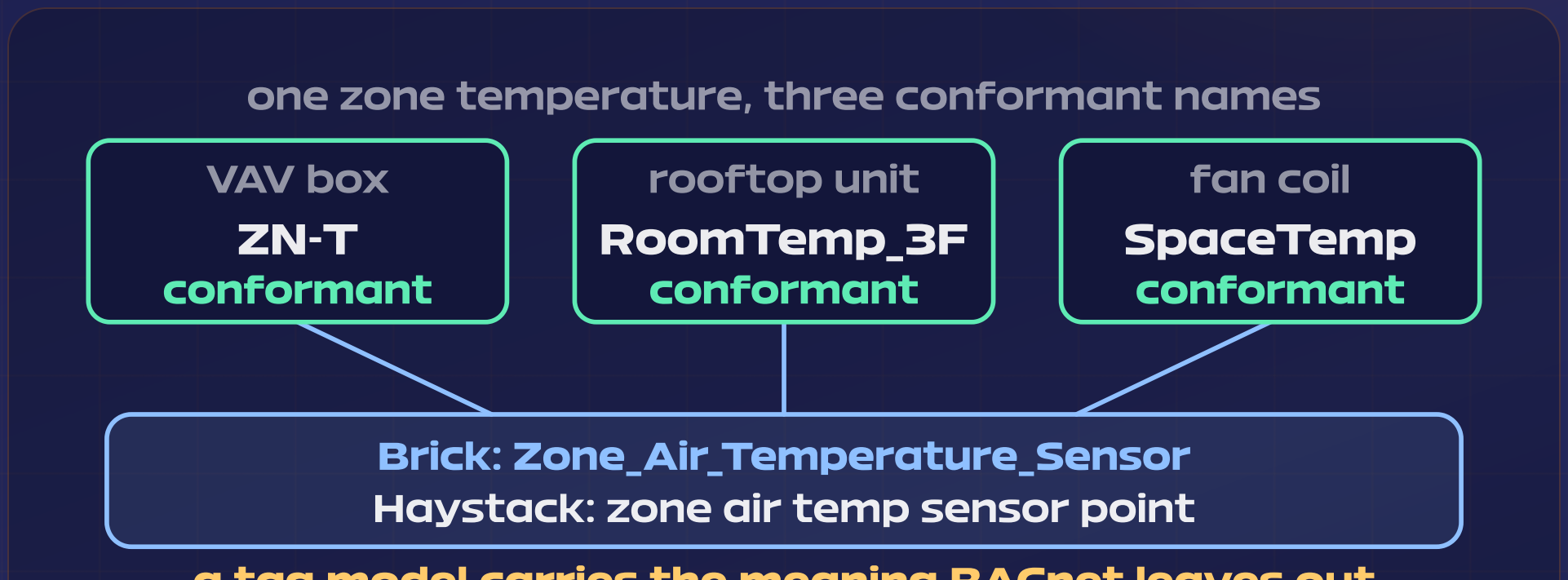
1. BACnet is **ANSI/ASHRAE 135**, and ISO 16484-5 republishes the same text about an edition behind. The number that matters on site is the Protocol Revision: 135-2020 was PR 22, and 135-2024 plus its published addendum is PR 31. [1]

2. Every addendum is tied to a PR, and addenda approved together share one: the nine approved on 15 June 2018 are all PR 20. A device claiming "BACnet 2020" tells you far less than one claiming PR 22. [1]

And the vocabulary moved: addendum 135-2020ce replaced "master-slave/token-passing" with multidrop serial bus/token passing, and Max_Master with Max_Manager. A submittal that still says master-slave was written against an older text. [1]

WHAT BACNET DOES NOT DO

It standardises the wire, not the words



Object_Name only has to be unique inside the device that holds it. The one exception is the Device object's own name, which must be unique across the internetwork. No naming convention, no controlled vocabulary: BACnet tells you a value arrived, never what it means. [1]

That gap is where the integration budget goes, and it is what tag models close: Project Haystack and the Brick Schema give the three names above one meaning. ASHRAE 223P, now titled "Semantic Data Model for Analytics and Automation Applications in Buildings", is **still not published**: its first formal public review ran in mid-2025 and a second from April to June 2026. Do not print a publication year for it. [2]

THE MYTH THAT SIZES EVERY RISER

It is 32 unit loads, not 32 devices



Addendum 135-2016bm (June 2018) changed clause 9.2.2 from 32 nodes to **32 unit loads** per segment, and added a PICS field for the transceiver's unit loading. At an eighth of a unit load the electrical budget allows **up to 256 devices**; at a full one, 32. [1]

While you are reading that PICS: only **9600 and 38400 baud are required** in MS/TP. 19200, 57600, 76800 and 115200 are optional, and 115200 is the only rate whose recommended segment length drops, from 1200 m to 1000 m. [1]

THREE DOCUMENTS, ONE CLAIM

PICS, test method and certification are not the same thing

PICS	135.1	BTL
the claim	the test	the certificate
normative annex	separate standard	private programme

none of the three means interchangeable

1. The **PICS** is the manufacturer's claim, in normative Annex A. **ANSI/ASHRAE 135.1** is the separate test method, now in its 2025 edition. **BTL** is a certification programme administered by BACnet International, not by ASHRAE. [1][3]

2. And BTL certification does not mean interchangeable. BTL's own programme page says its tests "validate that the product correctly implements **its specified set** of BACnet features": conformance to the product's own claim. [3]

So demand the PICS, and read it. It is the only document that says what this particular device will actually do.

WHY BUILDINGS STOP OBEYING

The priority array, and the override nobody cleared

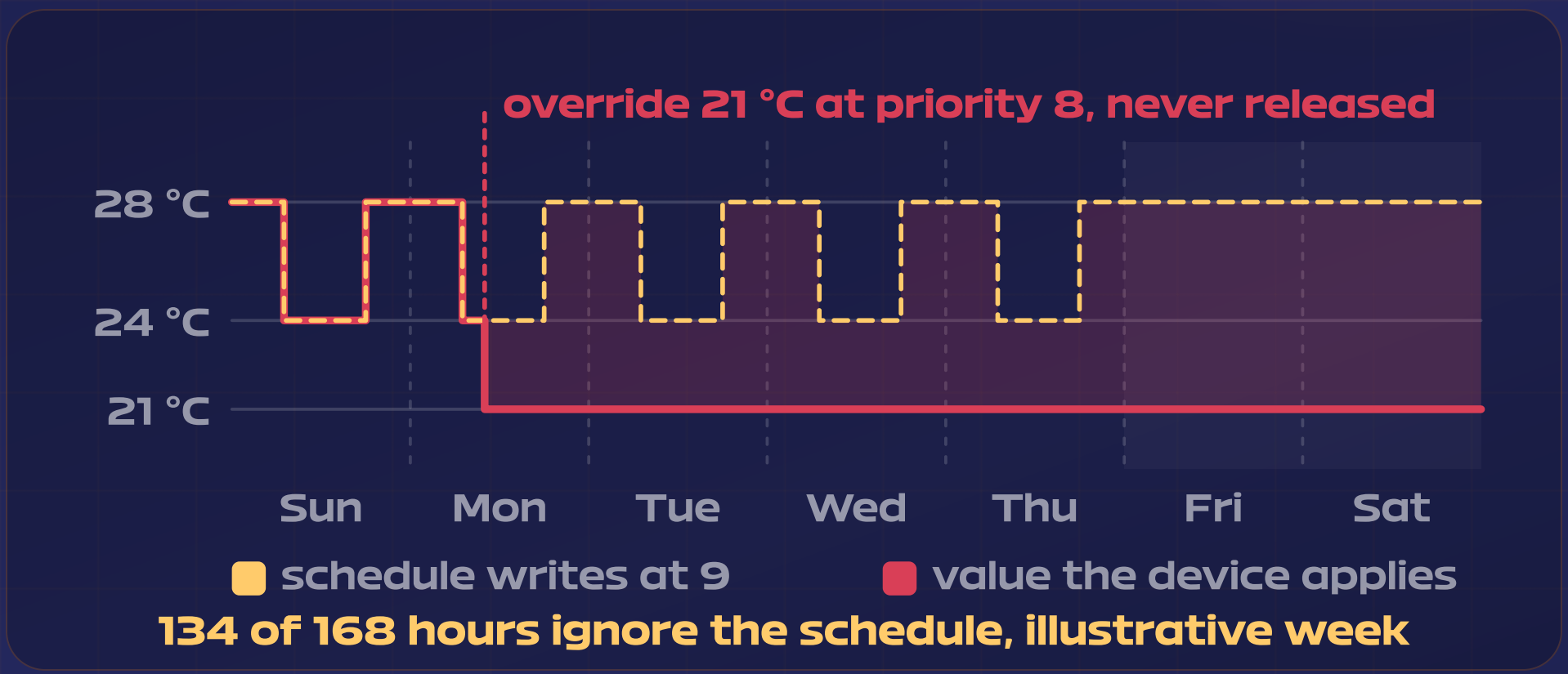
1	Manual Life Safety	NULL
2	Automatic Life Safety	NULL
3	Available	NULL
4	Available	NULL
5	Critical Equipment Control	NULL
6	Minimum On/Off	NULL
7	Available	NULL
▶ 8	Manual Operator	21 °C override wins
9	Available	24 °C schedule, outranked
10	Available	NULL
11	Available	NULL
12	Available	NULL
13	Available	NULL
14	Available	NULL
15	Available	NULL
16	Available	NULL
	Relinquish_Default	26 °C

Present_Value = 21 °C, from level 8 — illustrative setpoints

A commandable point holds 16 slots and applies the first non-NULL one from the top; Relinquish_Default applies only when all 16 are NULL. The standard's own example puts the scheduler at 9 and a manual override at 8. **One level apart, and 8 wins until someone writes NULL back.** [1]

WHAT A STUCK OVERRIDE COSTS

The schedule keeps writing. Nothing reads it.



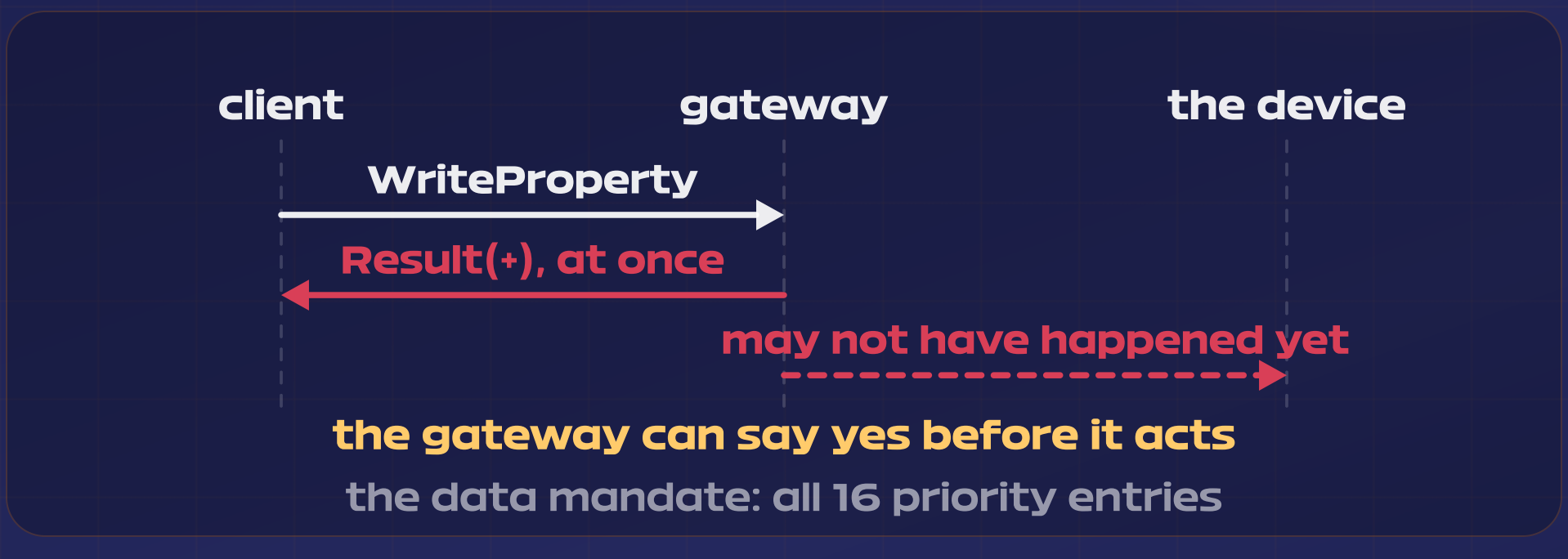
134 of 168 hours ignore the schedule, illustrative week

In this illustrative week the override arrives on Monday at 10:00 and is never released. From then on **134 of the week's 168 hours** apply a value the schedule did not write, and 93 of them are nights and the weekend held at 21 °C instead of set back to 28 °C.

Nothing on the schedule screen changes: the schedule object is still writing, and a trend of the setpoint is a steady line that looks like good control. The fault shows in one place only, the priority array of the point itself, which is why the handover ask is a report of every non-NULL slot.

GATEWAYS ARE IN THE STANDARD

Annex H is normative, and most of it says should



1. Its one mandate about data: **"Gateways are required to implement Priority_Array properties correctly with all 16 entries."** Its other hard rules are about timing and silence. The rest of gateway design is, in the standard's words, a local matter. [1]

2. And the information loss is written down: a conforming gateway may return Result(+) to a write **it has not yet performed**, and may read back the value you wrote instead of the value in the device. [1]

One clause almost nobody specifies: since addendum 135-2012al, a gateway presenting virtual BACnet devices must supply a second, separate PICS covering those virtual devices. One line in a submittal schedule. [1]

MODBUS, HONESTLY

The standard says the mapping is vendor specific

holding one-based	40001	40002	40003	40004
on the wire	0	1	2	3
extended zero-based	600000	600001	600002	600003

the off-by-one is in PI-MBUS-300 (1996)



The packaged unit on the roof arrives with its own controller and its own register map. Nothing in the specification says which register holds the setpoint.

Section 4.4, verbatim: **"The pre-mapping between the MODBUS data model and the device application is totally vendor device specific."** One sentence from the specification explains every register-map argument you have ever had. [4]

THE DATA MODEL, AND WHAT IT LEAVES OUT

Four tables, 16-bit words, and no rule for a float

primary table	object type	access	1996 ref
Discrete Inputs	Single bit	Read-Only	1xxxx
Coils	Single bit	Read-Write	0xxxx
Input Registers	16-bit word	Read-Only	3xxxx
Holding Registers	16-bit word	Read-Write	4xxxx

one 32-bit float, two holding registers

ABCD	0x41AC	0x0000	→	= 21.5
CDAB	0x0000	0x41AC	→	= 2.4e-41

same wire, two readings: ask for the word order

Section 4.2 fixes big-endian for one 16-bit item and stops there. **"Float", "IEEE" and "32-bit" appear nowhere in the specification**, so the same two holding registers read 21.5 in one word order and 2.4e-41 in the other. [4]

It does not number from 40001 either: every item is "addressed from 0 to 65535", and an item "numbered X is addressed in the MODBUS PDU X-1". A register map is only usable with three things written on it: the address base, the data type and the word order. [4]

THE WORD THAT APPEARS ZERO TIMES

Modbus has no security, not weak security

in the 50-page Modbus specification

0	0	0
security	authentication	encryption

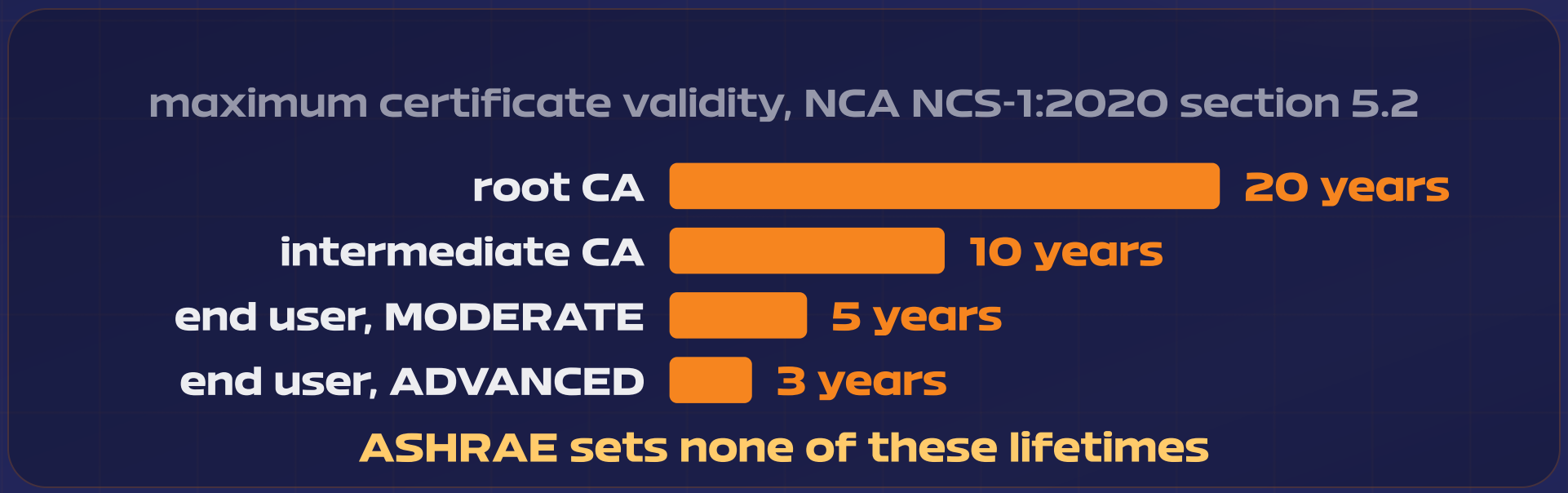
no security, not weak security
MODBUS/TCP Security: TLS on port 802

"Security", "authentication" and "encryption" appear exactly zero times in the 50-page Modbus Application Protocol Specification. [4]

There is a secure version almost nobody specifies: MODBUS/TCP Security on port 802, TLS 1.2 or better with mutual X.509v3 certificates and a recommended role in a certificate extension, first published in 2018 and now at v36. Worth knowing too that Modbus TCP is profile CP 15/1 in IEC 61784, while the serial line has no IEC profile, and that the Modbus Organization's tested-devices page lists **two companies**, so a "Modbus certified" claim should name what was tested. [4][8]

SECURITY, WITH THE RECEIPTS

BACnet had security and the industry threw it away



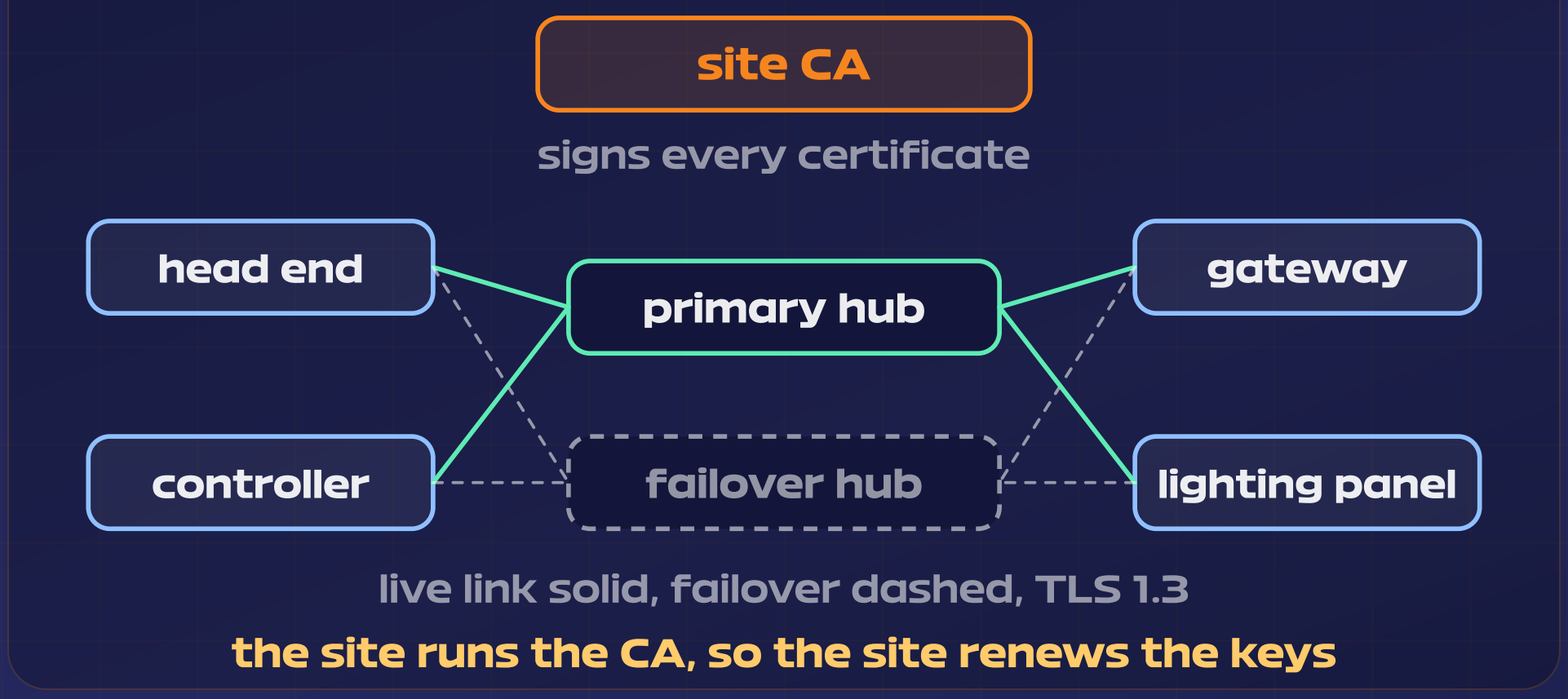
1. ASHRAE **deleted Clause 24, Network Security, in November 2019** with addendum 135-2016by, and wrote the reason down: "very limited industry acceptance". BACnet/SC, approved the same day, is the replacement. [1]

2. The line that sells BACnet/SC and the line that sinks it are the same one: **"The signing CA shall be controlled by the site."** Specifying it means the building owner now operates a certificate authority. [1]

In Saudi Arabia that authority has a regulator. The NCA's National Cryptographic Standards, made binding by ECC control 2-8-3, set validity limits the ASHRAE standard does not: root CA at most 20 years, intermediate at most 10, end-user at most 5 at the MODERATE level and 3 at ADVANCED. [5]

WHAT BACNET/SC ACTUALLY BUILDS

Every device dials out to a hub



BACnet/SC replaces broadcast with connections. Each node holds **one live connection**, to the primary hub or the failover hub, as a WebSocket over **TLS 1.3**, and both ends present certificates signed directly by a CA the site configured. [1]

The standard sets no default port and no certificate lifetime or renewal interval, and running the CA is explicitly outside its scope. Everything that keeps the network alive in year six is a site decision, so it has to be written into the specification. [1]

USE THE RIGHT INCIDENT

Two real building-automation attacks, and one myth

KNXlock	a security feature turned against the owner	cite
FrostyGoop	the assets were not adequately segmented	cite
Target	for billing, not building control	myth

cite the incident, not the anecdote

1. **KNXlock** is the one to lead with: in 2021 attackers unloaded the devices and then set the BCU key, so the owner could not reprogram them. **FrostyGoop** is the Modbus case, and the causal sentence is Dragos's: the network assets "were not adequately segmented". [6]

2. Correct the Target story rather than repeating it. The Senate report says the HVAC contractor had remote access "for electronic billing, contract submission, and project management purposes", not for building control. [6]

And the sentence to quote at anyone who says the network is isolated: NSA and CISA assessment teams "have often gained access to OT networks, despite prior assurance that the networks were fully air gapped". [6]

THE SAUDI POSITION

The four Mostadam manuals reviewed specify data, not a protocol

Mostadam, 878 pages across 4 manuals

0 occurrences

BMS yes, protocol no

BACnet
Modbus
KNX
DALI
LonWorks
MQTT

Keystone, Commercial D+C

E-02 Energy Metering
PMM-01 Commissioning
sub-meters ≥ 90% of demand

remote link: guidance only

4 manuals reviewed: metering, commissioning, no protocol

878 pages across the four Mostadam manuals reviewed, and not one occurrence of BACnet, Modbus, KNX, DALI, LonWorks or MQTT. They specify metering and commissioning requirements and name building management systems, but never a BAS protocol. [7]

What the commercial Design + Construction manual does make a **Keystone credit**, required whatever rating is targeted, is E-02 Energy Metering and PMM-01 Systems Commissioning. Sub-meters must cover at least 90% of energy demand, including any receptacle or process load of 10 kW and above. The residential manual makes metering a keystone only from Silver. [7]

WRITE THIS INTO THE SPECIFICATION

Seven lines, each one checkable



each artefact has a date, not just a name

BAS INTEGRATION, SUBMITTALS AND HANDOVER

"a. Each BACnet device: a PICS stating its Protocol Revision as a number and its transceiver unit loading.
b. Each gateway presenting virtual devices: a second PICS for them.
c. Each MS/TP segment: unit loads summing to 32 or fewer.
d. Each Modbus device: a register map giving address base, data type and word order.
e. At handover and at the end of the defects period: every non-NULL priority slot, with its reason.
f. If BACnet/SC: the site CA and its renewal procedure, within NCA NCS-1:2020 limits, in the O&M manual.
g. A Commissioning Agent with at least five years' experience, reporting to the owner, appointed before the design-phase commissioning review (Mostadam PMM-01)."

SOURCES

Where every number in this deck comes from

[1] ANSI/ASHRAE 135; ISO 16484-5; addenda bm, ce, al, by, bj, cu
[2] Project Haystack; Brick Schema; ASHRAE 223P (unpublished)
[3] BTL Certification Program, btl.org; ANSI/ASHRAE 135.1-2025
[4] Modbus spec V1.1b3; MODBUS/TCP Security v36; PI-MBUS-300 (1996)
[5] NCA National Cryptographic Standards NCS-1:2020; ECC 2-8-3
[6] Limes KNXlock; Dragos FrostyGoop; US Senate; CISA AA23-278A
[7] Mostadam Commercial and Residential D+C; SBC 1001 s. 603
[8] IEC 61784-5-15:2010; Modbus Organization, tested devices

The episode article lists every source with a link. The segment arithmetic, the priority resolution, the illustrative week and the float word order are computed, not typed.

PRACTICAL LIGHTING ENGINEERING

Save this. Send it to a colleague.

Read the full episode article

https://nlc.com.sa/academy/bas-backbone.html

Next episode
PoE Types