

غرفة تحكّم في مبنى ليلاً. كل جدول زمني على هذه الشاشات يمكن أن يتفوّق عليه تجاوز واحد لم يمسحه أحد.

أكاديمية NLC · الحلقة 25

المبنى يطيع شخصاً آخر.

بروتوكولا BACnet مع Modbus وطبقة التكامل التي تذهب إليها ميزانية المشروع فعلاً. بدايةً من الآلية التي توقف المبنى بهدوء عن الاستجابة لجدوله الزمني.

اضبط الإصدار

استشهد بمراجعة البروتوكول لا بسنة الطبعة



1 بروتوكول BACnet هو **ANSI/ASHRAE 135**، وتعيد المواصفة ISO 16484-5 نشر النصّ نفسه متأخّرةً بطبعة تقريباً. أما الرقم المهمّ ميدانياً فهو مراجعة البروتوكول: فالطبعة 135-2020 كانت PR 22، والطبعة 135-2024 مع ملحقها المنشور هي PR 31. [1]

2 وكل ملحق مرتبط بمراجعة، والملاحق المعتمدة معاً تتشارك مراجعة واحدة: فالملاحق التسعة المعتمدة في 15 يونيو 2018 كلّها PR 20. والجهاز الذي يدّعي «BACnet 2020» يقول أقلّ بكثير من جهاز يدّعي PR 22. [1]

كما تغيّرت المفردات: استبدل الملحق 135-2020ce عبارة «سيّد وتابع مع تمرير الرمز» بعبارة **ناقل تسلسلي متعدّد النقاط مع تمرير الرمز**، واستبدل Max_Master بـ Max_Manager. فإن كان المستند ما زال يقول سيّد وتابع فقد كُتب على نصّ أقدم. [1]

ما لا يفعله BACnet

يوحّد السلك لا الكلمات



اسم الكائن مطلوب أن يكون فريداً داخل الجهاز الذي يحفظه فقط.
والاستثناء الوحيد اسم كائن الجهاز نفسه، إذ يجب أن يكون فريداً على
امتداد الشبكة كلّها. بلا اصطلاح تسمية، وبلا مفردات محكومة:
فبروتوكول BACnet يخبرك أن قيمة وصلت، ولا يخبرك أبداً بما تعنيه. [1]

وتلك الفجوة هي وجهة ميزانية التكامل، وهي ما تسدّه نماذج الوسوم: إذ تعطي Project Haystack مع Brick Schema الأسماءَ الثلاثة أعلاه معنى واحداً. أما المواصفة ASHRAE 223P وعنوانها الآن «نموذج بيانات دلالي لتطبيقات التحليلات والأتمتة في المباني» فهي **لم تُنشر بعد**: جرت مراجعتها العامة الرسمية الأولى في منتصف 2025، والثانية من أبريل إلى يونيو 2026. فلا تطبع لها سنة نشر. [2]

الأسطورة التي تحدّد حجم كل غرفة صعود

إنها 32 حِمل وحدة، لا 32 جهازاً



غيّر الملحق 135-2016bm في يونيو 2018 البند 9.2.2 من 32 عقدة إلى **32 حِمل وحدة** لكل مقطع، وأضاف إلى بيان PICS خانة لحِمل وحدة المرسل المستقبل. فعند تُمن حِمل وحدة تتيح الميزانية الكهربائية **ما يصل إلى 256 جهازاً**؛ وعند حِمل كامل 32. [1]

وأنت تقرأ بيان PICS ذاك: المطلوب في MS/TP هو **9600 مع 38400 باود فقط**. أما 19200 ثم 57600 ثم 76800 ثم 115200 فاختيارية، ومعدّل 115200 هو الوحيد الذي يهبط طول مقطعه الموصى به، من 1200 m إلى 1000 m. [1]

ثلاث وثائق وادّعاء واحد

بيان المطابقة وطريقة الاختبار والاعتماد ليست شيئاً واحداً

PICS	135.1	BTL
الادعاء	الاختبار	الشهادة
ملحق معياري	مواصفة منفصلة	برنامج خاص

ولا واحدة منها تعني قابلية التبادل

1. فـ **PICS** ادّعاء المصنّع، في الملحق المعياري A. والمواصفة **ANSI/ASHRAE 135.1** طريقة الاختبار المنفصلة، وطبعتها الحالية 2025. أما **BTL** فبرنامج اعتماد تديره BACnet International لا ASHRAE. [1][3]

2. واعتماد BTL لا يعني قابلية التبادل. فصفحة برنامج BTL نفسها تقول إن اختباراته «تتحقّق من أن المنتج ينفّذ **مجموعته المحدّدة** من خصائص BACnet تنفيذاً صحيحاً»: أي مطابقة لادّعاء المنتج نفسه. [3]

لذا اطلب بيان PICS، ثم اقرأه. فهو الوثيقة الوحيدة التي تقول ما سيفعله هذا الجهاز بعينه فعلاً.

لماذا تتوقّف المباني عن الطاعة

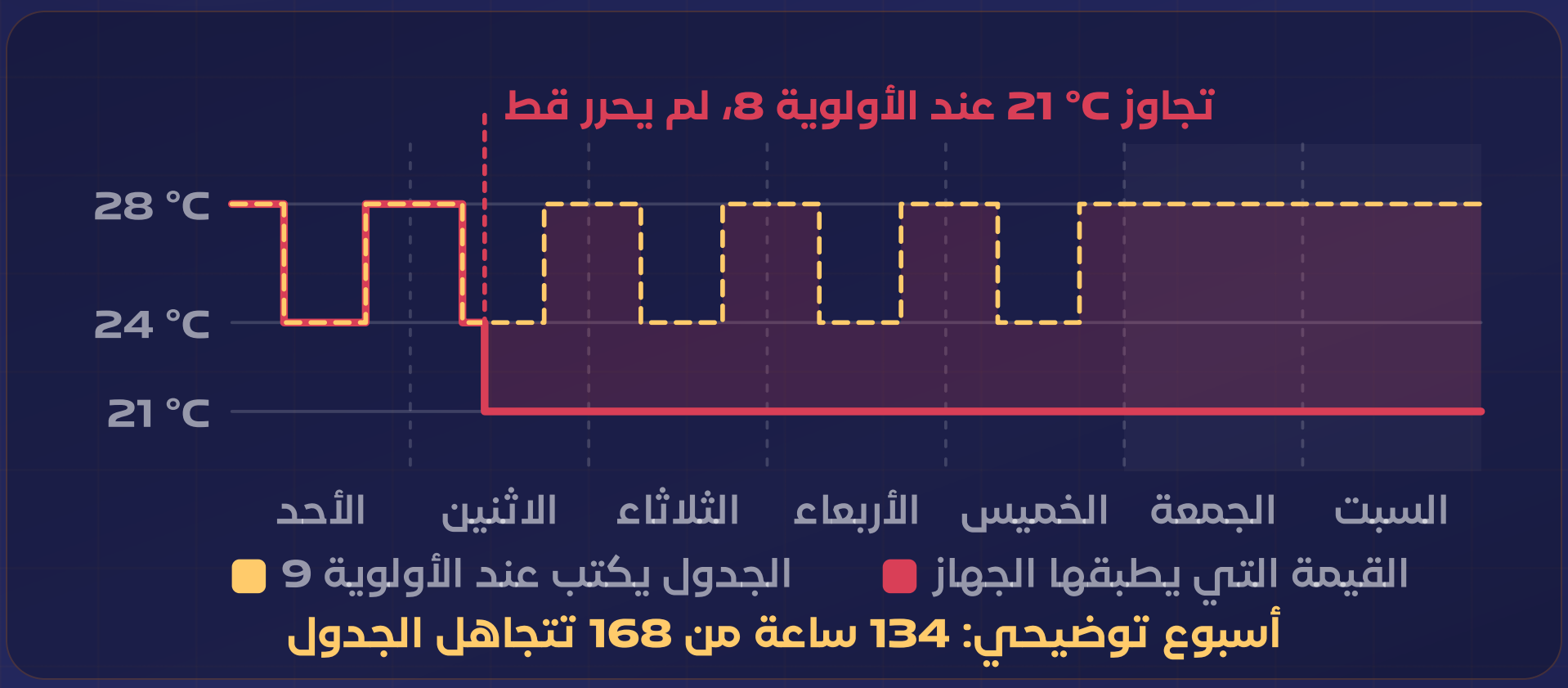
مصفوفة الأولوية، والتجاوز الذي لم يمسحه أحد

1	سلامة الأرواح، يدوي	NULL
2	سلامة الأرواح، آلي	NULL
3	متاح	NULL
4	متاح	NULL
5	تحكم المعدات الحرجة	NULL
6	أدنى زمن تشغيل وإيقاف	NULL
7	متاح	NULL
◄ 8	المشغل اليدوي	التجاوز يفوز: 21 °C
9	متاح	الجدول، مغلوب: 24 °C
10	متاح	NULL
11	متاح	NULL
12	متاح	NULL
13	متاح	NULL
14	متاح	NULL
15	متاح	NULL
16	متاح	NULL
	Relinquish_Default	26 °C
	يطبق الجهاز 21 °C من المستوى 8	نقاط ضبط توضيحية

للنقطة القابلة للأمر 16 خانة، ويطبّق الجهاز أول قيمة غير خالية من الأعلى؛ ولا تُطبَّق القيمة الافتراضية إلا حين تخلو الخانات كلّها. ومثال المواصفة نفسها يضع المجدول عند 9 والتجاوز اليدوي عند 8. **مستوى واحد بينهما، ويفوز المستوى 8 إلى أن يكتب أحد NULL مكانه.** [1]

كم يكلّف تجاوز عالق

الجدول يواصل الكتابة، ولا شيء يقرؤه.

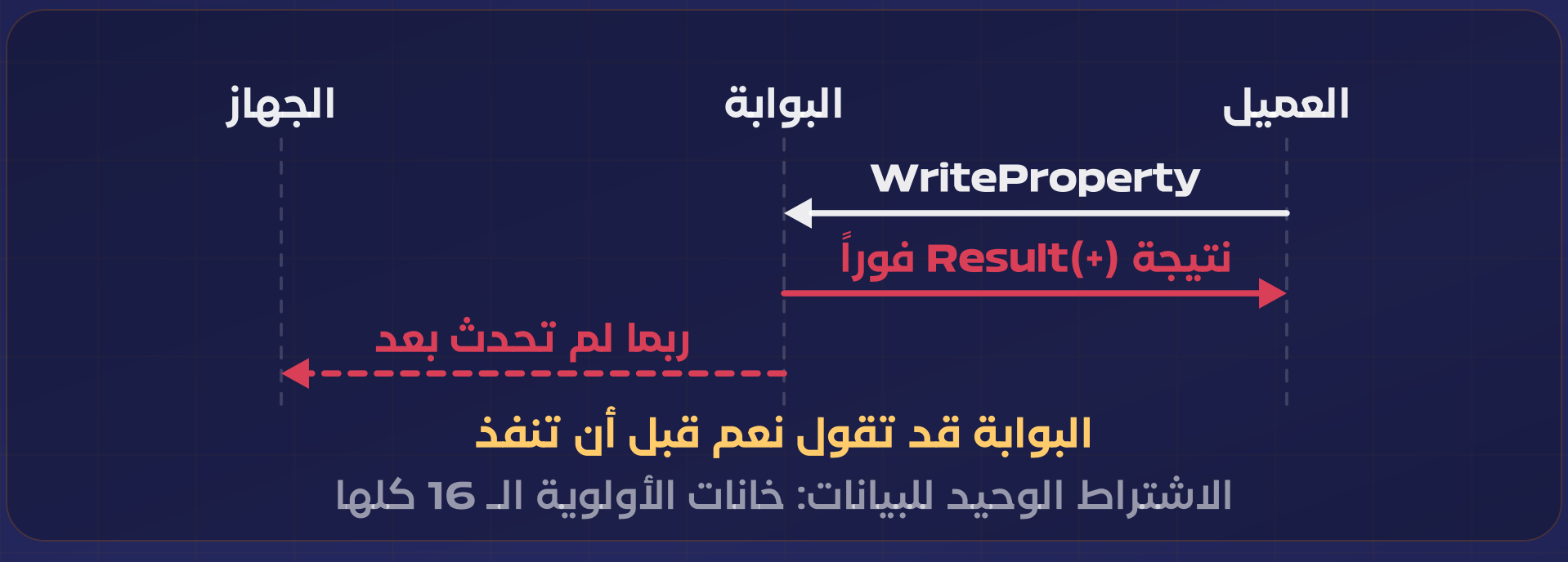


في هذا الأسبوع التوضيحي يصل التجاوز يوم الاثنين الساعة 10:00 ولا يُحرَّر أبداً. ومن بعده تطبّق **134 ساعة من ساعات الأسبوع الـ 168** قيمة لم يكتبها الجدول، منها 93 ساعة ليلاً وفي عطلة نهاية الأسبوع ثبتت فيها الغرفة على 21 °C بدل رفعها إلى 28 °C.

ولا يتغيّر شيء على شاشة الجدول: فكائن الجدول ما زال يكتب، ومنحنى نقطة الضبط خطّ ثابت يبدو تحكّماً جيداً. والعطل يظهر في مكان واحد فقط، هو مصفوفة أولوية النقطة نفسها، ولهذا فالمطلوب عند التسليم تقرير بكل خانة غير خالية.

البوّابات في المواصفة نفسها

الملحق H معياري، ومعظمه توصيات



1. اشتراطه الوحيد بشأن البيانات: «**يُشترط في البوّابات تنفيذ خصائص مصفوفة الأولوية تنفيذاً صحيحاً بكل خاناتها الستّ عشرة**». أما قواعده الملزمة الأخرى فتخصّ التوقيت والصمت. وما عدا ذلك من تصميم البوّابة هو، بنصّ المواصفة، مسألة محلّية. [1]

2. وفقدان المعلومات مكتوب أيضاً: فالبوّابة المطابقة قد تُرجع نتيجة نجاح لعملية كتابة **لم تنفّذها بعد**، وقد تُرجع لك القيمة التي كتبتها بدل القيمة الموجودة في الجهاز. [1]

وبند لا يكاد يشترطه أحد: منذ الملحق 135-2012al، يجب على البوّابة التي تُظهر أجهزة BACnet افتراضية أن توفّر **بيان PICS ثانياً منفصلاً** يغطّي تلك الأجهزة. سطر واحد في جدول المستندات. [1]

بروتوكول Modbus بصراحة

المواصفة تقول إن الربط يخصّ المورّد

سجلات الحفظ من واحد	40001	40002	40003	40004
على السلك	0	1	2	3
الممتدة من صفر	600000	600001	600002	600003

فارق الواحد في وثيقة PI-MBUS-300 نفسها، 1996



الوحدة المجمّعة على السطح تصل ومعها متحكّمها الخاص وخريطة سجلّاتها الخاصة. ولا تقول المواصفة أي سجلّ يحمل نقطة الضبط.

القسم 4.4 حرفياً: «**الربط المسبق بين نموذج بيانات MODBUS وتطبيق الجهاز يخصّ جهاز المورّد تماماً**». جملة واحدة من المواصفة تفسّر كل خلاف حول خرائط السجلّات مررت به. [4]

نموذج البيانات، وما يتركه

أربعة جداول، وكلمات 16 بت، ولا قاعدة للعدد العشري

الجدول الأساسي	نوع الكائن	الوصول	مرجع 1996
Discrete Inputs	بت واحد	قراءة فقط	1xxxx
Coils	بت واحد	قراءة وكتابة	0xxxx
Input Registers	كلمة 16 بت	قراءة فقط	3xxxx
Holding Registers	كلمة 16 بت	قراءة وكتابة	4xxxx

عدد عشري واحد بطول 32 بت، في سجلي حفظ

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

السلك نفسه وقراءتان: اطلب ترتيب الكلمات

يثبّت القسم 4.2 ترتيب big-endian لعنصر واحد من 16 بت ثم يتوقّف. **فكلمات «float» و«IEEE» و«32-bit» لا ترد في المواصفة إطلاقاً**، ولذلك يُقرأ سجلّا الحفظ نفسهما 21.5 بترتيب كلمات، وعدداً شبه صفري بالترتيب الآخر. [4]

ولا ترقّم المواصفة من 40001 أيضاً: فكل عنصر «يُعنوَن من 0 إلى 65535»، والعنصر «المرقّم X يُعنوَن في وحدة PDU بالرقم X-1». فخريطة السجلّات لا تصلح إلا إذا كُتبت عليها ثلاثة أشياء: أساس العنونة، ونوع البيانات، وترتيب الكلمات. [4]

الكلمة التي ترد صفر مرة

بروتوكول Modbus بلا أمن، لا بأمن ضعيف

في مواصفة Modbus ذات الـ 50 صفحة

الأمن	المصادقة	التشفير
0	0	0

لا أمن أصلاً، لا أمن ضعيف
النسخة الآمنة MODBUS/TCP Security على المنفذ 802

كلمات «الأمن» و«المصادقة» و«التشفير» ترد صفر مرة بالضبط في مواصفة بروتوكول تطبيق Modbus البالغة خمسين صفحة. [4]

وثمّة نسخة آمنة لا يكاد أحد يشترطها: MODBUS/TCP Security على المنفذ 802، بطبقة TLS 1.2 أو أحدث مع شهادات X.509v3 متبادلة ودور موصى به في امتداد الشهادة، نُشرت أول مرة عام 2018 وبلغت الإصدار v36. ومن المفيد أيضاً أن Modbus TCP هو الملفّ CP 15/1 في IEC 61784 بينما لا ملفّ IEC للخط التسلسلي، وأن صفحة الأجهزة المختبرة لدى منظمة Modbus تُدرج **شركتين**، فعبارة «معتمد Modbus» يجب أن تسمّي ما اختُبر. [4][8]

الأمن، بالأدلّة

كان لـ BACnet أمن فتخلّصت منه الصناعة

أقصى صلاحية للشهادة، القسم 5.2 من NCS-1:2020



ولا تضع ASHRAE أياً من هذه الحدود

1 **حذفت ASHRAE البند 24، أمن الشبكة، في نوفمبر 2019** بالملحق 135-2016by، ودوّنت السبب: «قبول محدود جداً في الصناعة». وبروتوكول BACnet/SC المعتمد في اليوم نفسه هو البديل. [1]

2 والجملة التي تبيع BACnet/SC هي الجملة التي تُفرقه: **«يجب أن يكون مرجع التوقيع تحت سيطرة الموقع»**. فاشتراطه يعني أن مالك المبنى صار يشغّل مرجع شهادات. [1]

وفي السعودية لذلك المرجع منظّم: فمعايير التشفير الوطنية لدى الهيئة الوطنية للأمن السيبراني، الملزمة بموجب الضابط 3-8-2 من الضوابط الأساسية، تضع حدوداً قصوى لصلاحية الشهادات لا تضعها مواصفة ASHRAE. مرجع الجذر 20 سنة، والوسيط 10 سنوات، والمستخدم النهائي 5 سنوات في المستوى MODERATE، أو 3 في المستوى ADVANCED. [5]

ما الذي يبنيه BACnet/SC فعلاً

كل جهاز يتّصل صادراً إلى محور



يستبدل BACnet/SC البثّ العام بالاتصالات. فلكل عقدة **اتصال حيّ واحد**، بالمحور الرئيسي أو بالمحور الاحتياطي، عبر WebSocket فوق **TLS 1.3**، ويقدّم الطرفان شهادتين موقّعتين مباشرةً من مرجع شهادات يضبطه الموقع. [1]

ولا تحدّد المواصفة منفذاً افتراضياً، ولا عمراً للشهادة، ولا فترة تجديد، وتشغيل مرجع الشهادات خارج نطاقها صراحةً. فكل ما يُبقي الشبكة حيّة في سنتها السادسة قرار يخصّ الموقع، ولذلك يجب أن يُكتب في المواصفة. [1]

استعمل الحادثة الصحيحة

هجومان حقيقيان على أتمتة المباني، وأسطورة واحدة

KNXlock	خاصية أمنية انقلبت على المالك	استشهد
FrostyGoop	الأصول لم تكن مجزأة تجزئة كافية	استشهد
Target	للفوترة، لا للتحكم في المبنى	أسطورة

استشهد بالحادثة لا بالحكاية

1. **هجوم KNXlock** هو الذي يجب أن تبدأ به: في 2021 أفرغ المهاجمون الأجهزة ثم ضبطوا مفتاح BCU حتى لا يستطيع المالك إعادة برمجتها. أما **FrostyGoop** فحالة Modbus، والجملة السببية هي جملة Dragos: أصول الشبكة «لم تكن مجزّأة تجزئة كافية». [6]

2. وصحّح حكاية Target بدل تكرارها. فتقرير مجلس الشيوخ يقول إن مقاول التكييف كان يملك وصولاً بعيداً «لأغراض الفوترة الإلكترونية وتقديم العقود وإدارة المشاريع»، لا للتحكّم في المبنى. [6]

والجملة التي تُقال لمن يزعم أن الشبكة معزولة: فرق التقييم لدى NSA مع CISA «كثيراً ما نفذت إلى شبكات التشغيل، رغم تأكيدات مسبقة بأنها معزولة تماماً». [6]

الموقف السعودي

أدلّة «مستدام» الأربعة التي راجعناها تحدّد البيانات لا البروتوكول

أدلة «مستدام»: 878 صفحة في 4 أدلة

مرات الورود: 0

تسمي BMS لا البروتوكول

Modbus BACnet
DALI KNX
MQTT LonWorks

اعتماد أساسي، دليل تجاري D+C

قياس الطاقة E-02
تشغيل الأنظمة PMM-01
قياس فرعي: 90% من الطلب فأكثر
الربط البعيد: إرشاد فقط

أربعة أدلة روجعت: قياس وتشغيل، بلا بروتوكول

في أدلّة «مستدام» الأربعة التي راجعناها 878 صفحة، ولا ورود واحد فيها لـ BACnet أو Modbus أو KNX أو DALI أو LonWorks أو MQTT. فهي تحدّد متطلّبات قياس الطاقة وتشغيل الأنظمة، وتسمّي أنظمة إدارة المباني، لكنها لا تسمّي لها بروتوكولاً أبداً. [7]

أما ما يجعله دليل المباني التجارية للتصميم والتنفيذ **اعتماداً أساسياً**، مطلوباً أياً كان التصنيف المستهدف، فهو قياس الطاقة E-02 وتشغيل الأنظمة PMM-01. ويجب أن تغطّي العدّادات الفرعية 90% على الأقل من الطلب على الطاقة، بما فيها أيّ حمل مقابس أو عمليات يبلغ 10 kW فأكثر. ولا يجعل الدليل السكني القياسَ اعتماداً أساسياً إلا من المستوى الفضّي. [7]

اكتب هذا في المواصفة

سبعة أسطر، كلٌّ منها قابل للتحقّق

مراجعة التشغيل في التصميم ← التسليم ← نهاية فترة الضمان

الوكيل معين ← تقرير مصفوفة الأولوية ← تقرير مصفوفة الأولوية

لكل وثيقة موعد، لا اسم فقط

تكامل أنظمة المباني، المستندات والتسليم

«أ. لكل جهاز BACnet: بيان PICS يذكر مراجعة البروتوكول رقماً، وحِمل وحدة المرسل المستقبل.

ب. لكل بوّابة تُظهر أجهزة افتراضية: بيان PICS ثانٍ لها.

ج. لكل مقطع MS/TP: مجموع أحمال وحدة لا يتجاوز 32.

د. لكل جهاز Modbus: خريطة سجلّات تذكر أساس العنونة ونوع البيانات وترتيب الكلمات.

هـ. عند التسليم ثم في نهاية فترة الضمان: كل خانة أولوية غير خالية، مع سببها.

و. عند اشتراط BACnet/SC: مرجع شهادات الموقع وإجراء تجديده، ضمن حدود NCS-1:2020، في دليل التشغيل والصيانة.

ز. وكيل تشغيل بخبرة خمس سنوات على الأقل، يرفع تقاريره إلى المالك، ويُعيَّن قبل مراجعة التشغيل في مرحلة التصميم، وفق PMM-01 في «مستدام».»

المصادر

من أين جاء كل رقم في هذا العرض

[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

مقالة الحلقة تسرد كل مصدر مع رابطه. وحساب المقاطع وحلّ الأولوية والأسبوع التوضيحي وترتيب كلمات العدد العشري كلّها محسوبة، لا مكتوبة باليد.

معرفة عملية في هندسة الإنارة

احفظها. وأرسلها إلى زميل.

اقرأ المقال الكامل للحلقة

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

الحلقة القادمة
أنواع PoE