

القارئ المثبّت على هذا العمود هو أحد طرفي سلك نُشرت مواصفة واجهته عام 1996.

أكاديمية NLC · الحلقة 28

حوالي 952 بت/ثانية. في 2026.

مثال توقيت نموذجي لواجهة Wiegand، وهي واجهة قارئ نُشرت عام 1996 ولم تُراجَع قط. استبدلها، وافحص البطاقة أيضاً: فالوصلة والبطاقة خطران منفصلان.

ليست ملغاة بل متروكة

ثلاثون سنة، ولا مراجعة حتى الآن.

AC-01: 30 سنة بلا أي مراجعة



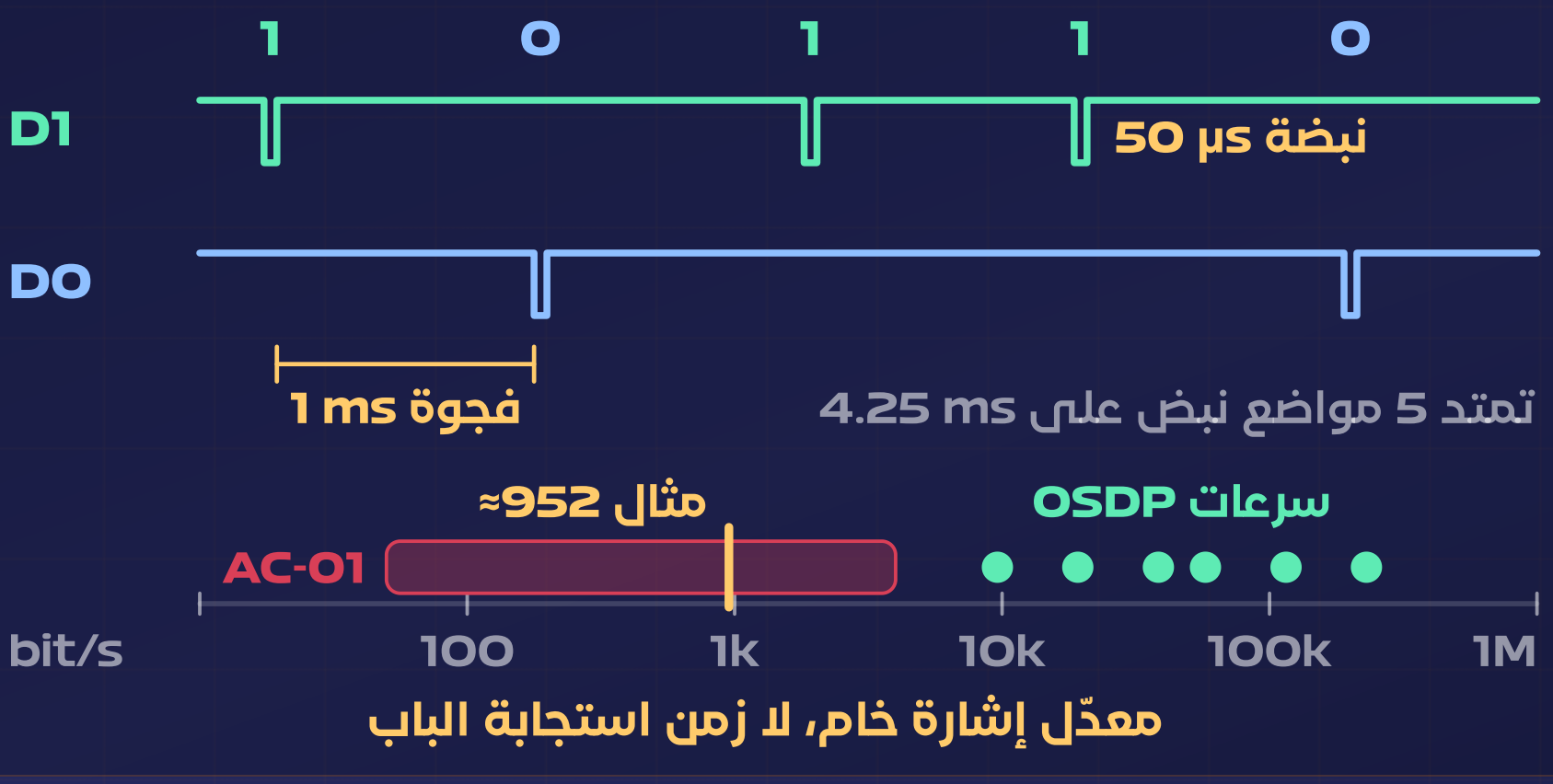
1	1996	نشر AC-01	
2	2008	عرض أداة تنصّت	
3	2011	فريق عمل OSDP	
4	2015	تنصّت عبر BLE	
5	2020	IEC 60839-11-5	
6	2023	نشر 5 ثغرات	
7	2024	v2.2.2 تصحيح فقط	
8	2026	لم يصدر v2.3	

يسجّل كتالوج SIA (نسخة مؤرشفة في يونيو 2026) أن **AC-01-1996.10** نُشرت سنة **1996**، وأنها ليست مواصفة **ANSI**، وأن لجنتها الراعية **مُنحلّة**. ولم تصدر لها أي مراجعة. [2]

أما OSDP فمسار مستقل ونشط: أصدرت SIA الإصدار 2.1.7 سنة 2015، ثم 2.2 سنة 2020، ثم 2.2.2 في أكتوبر 2024، إلى جانب IEC 60839-11-5:2020. وحتى 4 أكتوبر 2026 لم نجد إصداراً أحدث، وقد أُحيلت نتائج 2023 الأمنية إلى إصدار v2.3 قادم. [1][4]

لنقِس «البطء»

حوالي 952 بت/ثانية مثال توقيت، لا سرعة لـ Wiegand



تحدّد AC-01 نافذة: نبضات بعرض 20 إلى 100 µs، وفاصلاً بين النبضات من 200 µs إلى 20 ms يعرّفه مصنّعو القارئات بأنه زمن التوقّف بين نبضتين. والمثال النموذجي، نبضة **50 µs** مع فجوة **1 ms**، يعطي حوالي **1.05 ms** لكل بتّ، أي حوالي **952 بت/ثانية**. [2][5]

وهذا معدّل إشارة خام، لا معدّل نقل ولا زمن استجابة الباب: فإطار الـ 26 بت بهذا التوقيت يستغرق حوالي 26 ms، بينما يذكر أحد قارئات HID أنه يحتاج 175 ms لقراءة البطاقة والإبلاغ عنها. فـ OSDP لا يجعل الأبواب أسرع بعشرة أضعاف. [5]

التقسيم غير الموجود في المواصفة

تعرّف AC-01 الإطار، لا معناه



رمز طلب لدى مصنّع، لا جزء من AC-01

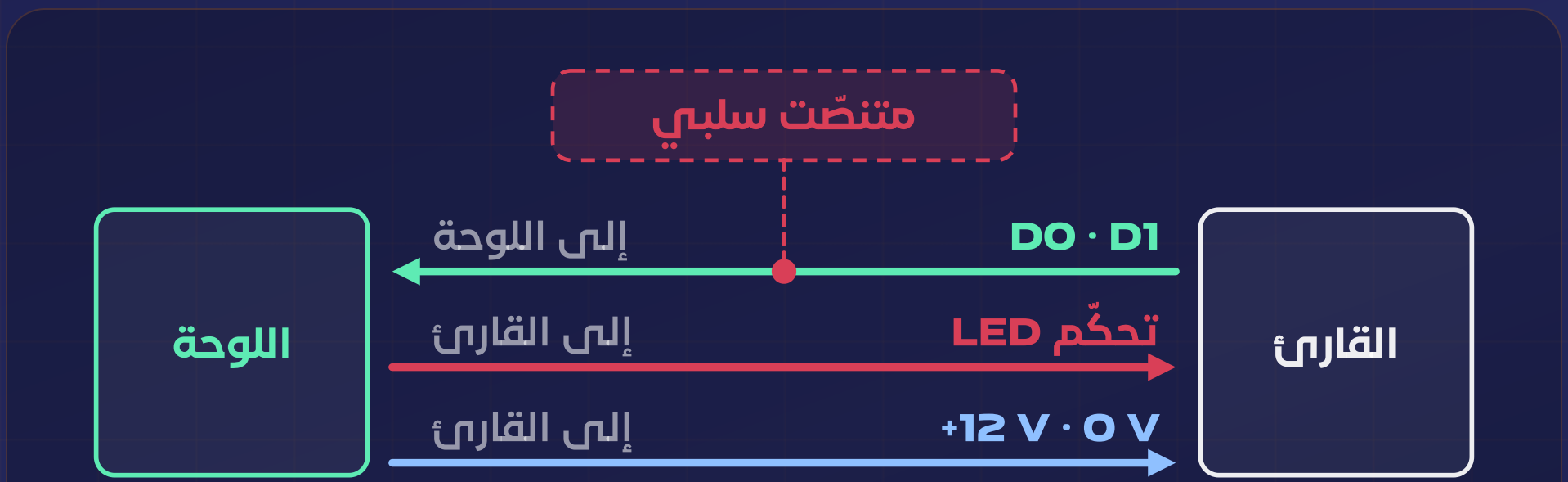
تتوقّف AC-01 عند 24 بت ترميز

يعرّف البند 5 في AC-01 إطار الـ 26 بت بأنه بتّا تكافؤ مع **24 بت ترميز**، ويترك تقسيمها للمصنّعين. أما **رمز المنشأة ذو الـ 8 بت مع رقم البطاقة ذي الـ 16 بت** فصيغة لدى أحد المصنّعين اسمها H10301، وليست جزءاً من AC-01. [2]

فعبارة «Wiegand 26» لا تعني دائماً 8 مع 16، وتوجد صيغ أطول. ولا تحمل الواجهة حقلاً للطول، ولا أي تدقيق للسلامة سوى بتّي التكافؤ. [2][5]

السلك الخامس

بيانات Wiegand أحادية الاتجاه، لكن الكابل ليس كذلك.



لا آلية مدمجة في AC-01 لكشف التنصّت السلبي

تسير بيانات البطاقة على DO/D1 من القارئ إلى المتحكّم، بينما يسير موصّل التحكّم بمؤشّر LED (البند 3.2.5) وزوج التغذية في الاتجاه المعاكس. **ولا توفّر AC-01 آلية مدمجة لكشف التنصّت السلبي على DO/D1.** [2]



الطرف الآخر من السلك نفسه، داخل غرفة التمديدات. أبقِها مقفلة، ومراقَبة ضد العبث، وبعيدة عن متناول العامة.

أسلاك، لا تشفير

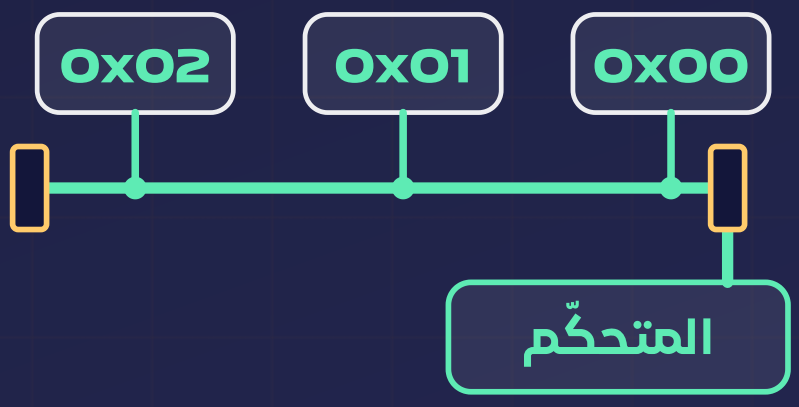
توصيل نجمي مقابل ناقل مشترك

Wiegand، توصيل نجمي



كابل مستقل لكل قارئ
8 أطراف عملياً
61-153 m حسب المقطع

OSDP، ناقل مشترك



زوج واحد مع التغذية
سلسلة مُنهاة الطرفين
200 m بتغذية من المتحكم

الطوبولوجيا ليست أماناً، فالأمان مصدره القناة الآمنة. يمدّ Wiegand كابلاً لكل قارئ، أما OSDP فيتشارك زوج RS-485 واحداً في سلسلة متتالية مُنهاة الطرفين، ويطلب دليل HID Signo مقاومة إنهاء 120 Ω لمسارات OSDP التي تتجاوز 61 m. ويستعلم المتحكّم كل عنوان، فيظهر القارئ الصامت متوقّفاً. [7]

سعة العناوين ليست سعة المنفذ: عناوين OSDP من 0x00 إلى 0x7E، أي 127 جهازاً، بينما يقبل HID Mercury MP1501 جهازَي OSDP لكل منفذ قارئ. فتحقّق من حدّ كل متحكّم. [7]

المقارنة التي يبالغ فيها الجميع

مسافة الطبقة الفيزيائية ليست مسافة الباب المُغذّى

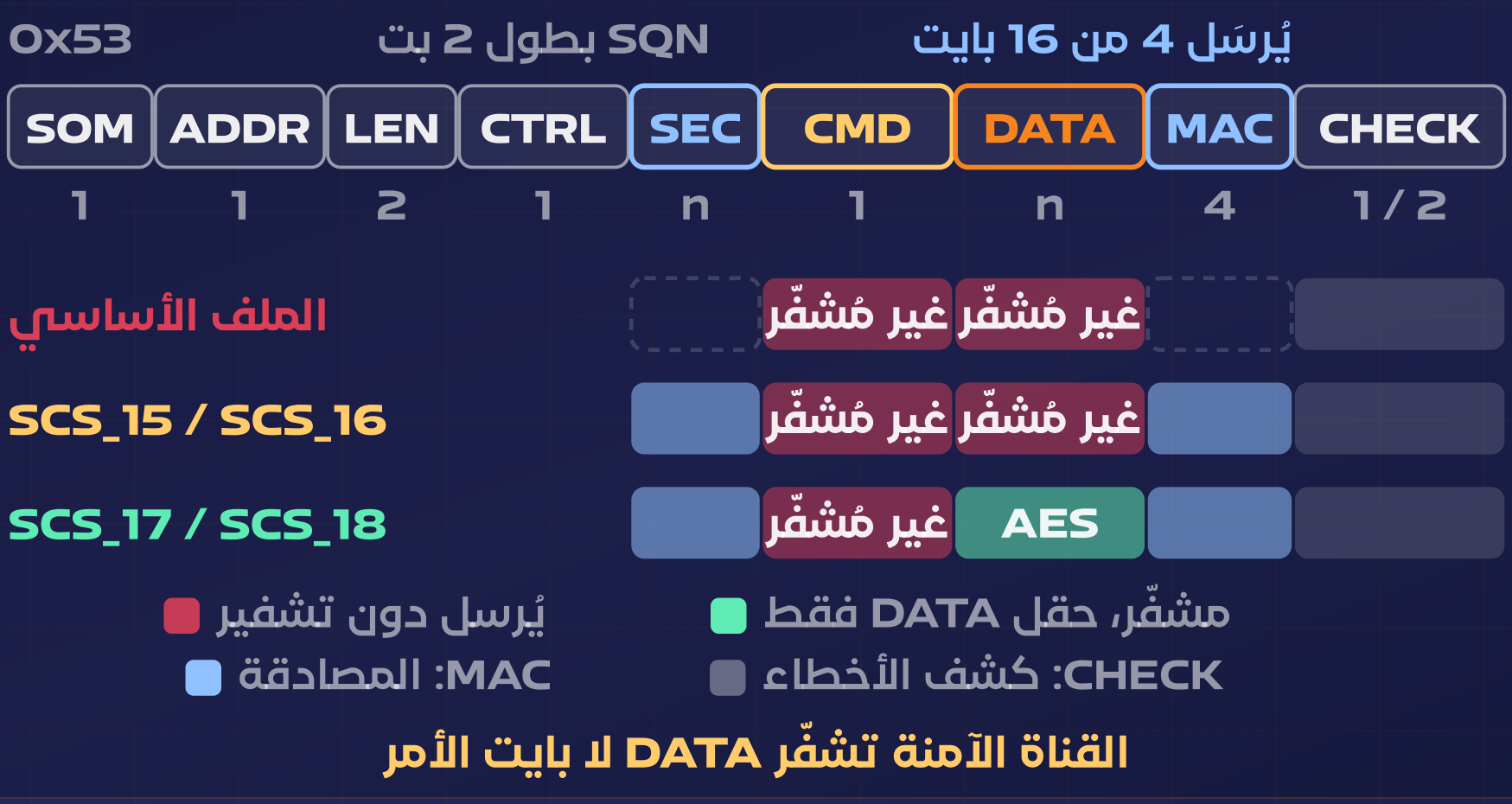


إرشاد AC-01 لـ Wiegand: **61 m عند 22 AWG، ثم 91 m عند 20 AWG، ثم 153 m عند 18 AWG**. وإرشاد Axis لوحدة A1610 في OSDP: **200 m لقارئ مُغذّى من المتحكم**، وحتى 1,000 m للبيانات مع قارئ بتغذية محلية. أما حوالي 1,200 m فإرشاد الطبقة الفيزيائية لـ RS-485، لا حدّ لـ OSDP. وهذه أمثلة منتجات. [2][7]

مقارنةً بـ Wiegand بمقطع 18 AWG: حوالي 7.8 مرة على الورق، ثم حوالي 1.3 مرة فقط عند باب قارئه مُغذّى من المتحكم.

الجملة التي تبيع طمأنينة زائفة

وجود OSDP لا يعني تلقائيًا أن الاتصال مشفّر. اقرأ الحزمة.

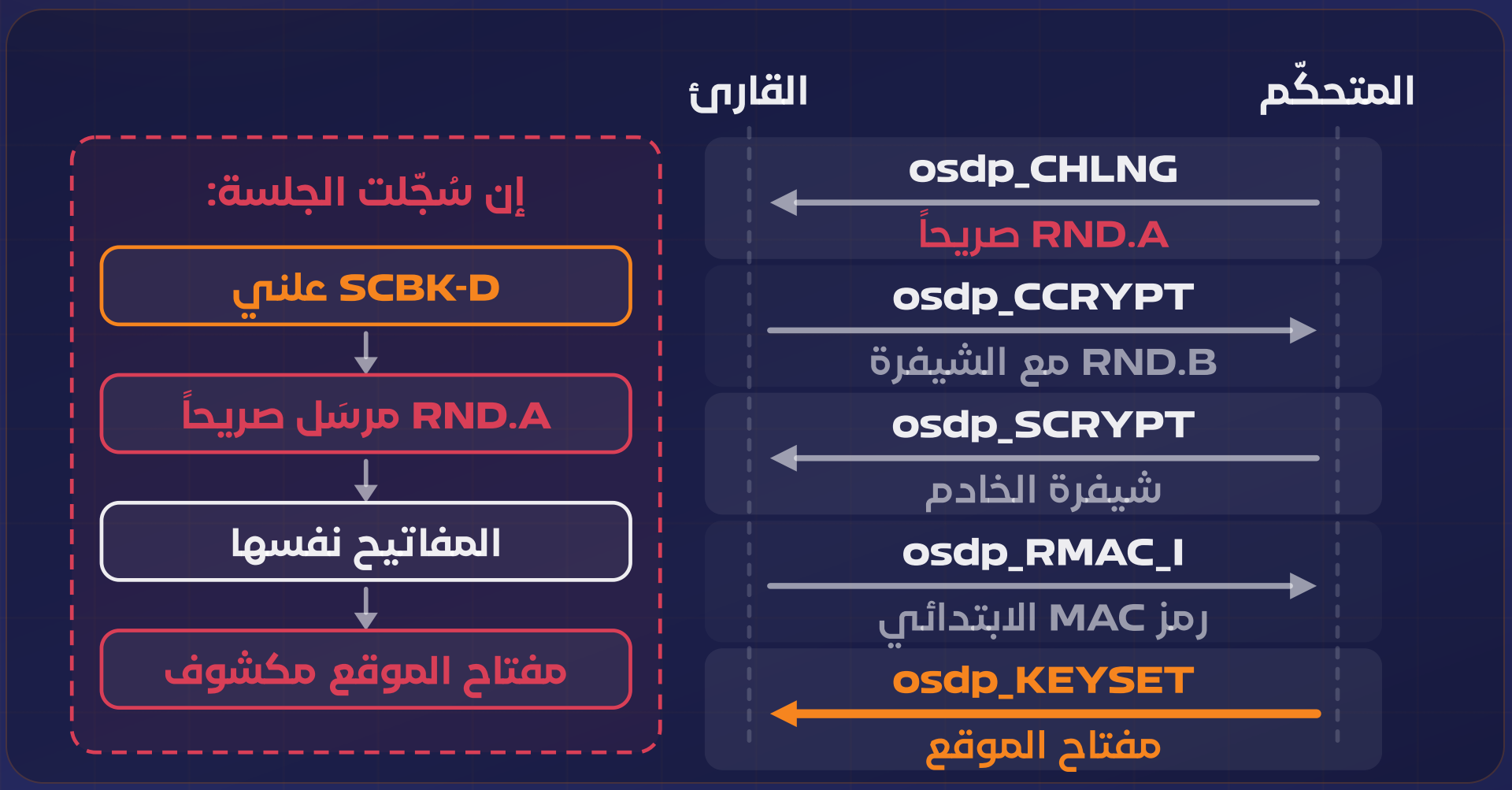


ثلاث حمايات لثلاث وظائف: checksum أو CRC في كل حزمة لكشف الأخطاء، ثم رمز MAC على الحزمة في القناة الآمنة للمصادقة، ثم تشفير حقل DATA وحده بخوارزمية AES-128 في النوعين SCS_17/18، مع بقاء الترويسة والأمر مرئيين. ولا يوجد في OSDP الأساسي إلا الأولى. [4][7]

ويصادق SCS_15/16 برمز MAC على بيانات غير مُشفّرة، وهما لرسالتَي POLL مع ACK. فاشترط القناة الآمنة **مفروضةً**: يرفض المتحكّم أي قارئ بدونها. [7]

أسهل شيء يمكن فحصه في جولة التسليم

قد يسافر مفتاح الموقع تحت مفتاح منشور



ثلاثة مفاتيح: **SCBK-D**، المفتاح الافتراضي المنشور لوضع التركيب، ثم **SCBK**، المفتاح الأساس الدائم لكل قارئ، ثم مفاتيح جلسة تُشتق منه في كل جلسة. فإن اقترن القارئ في وضع التركيب عبر أسلاك غير موثوقة، قد يكشف التسجيل مفتاحه **SCBK**، ولا يُلغي رفضُ **SCBK-D** لاحقاً هذا الانكشاف. [4][7]

اقرن القارئ على أسلاك موثوقة مادياً أو بالطريقة البديلة التي يوفّرها المصنّع، ثم تحقّق من رفض SCBK-D. [7]

بتّات السرّية لا بتّات المفتاح

مفتاح بطول 128 بت قد تساوي سرّيته 0 بت

0 بت	المفتاح الافتراضي، SCBK-D
	لمن يملك نصّ المواصفة
0 بت	وضع التركيب متروك مفتوحاً
	لجهاز على السلك يطلبه
9.6 بت	أنماط Bishop Fox الثلاثة المختبَرة
	768 احتمالاً، لهذه المجموعة فقط
128 بت	مفتاح عشوائي منتظم بطول 128 بت
	بشرط عشوائيته الحقيقية وحفظ سرّيته

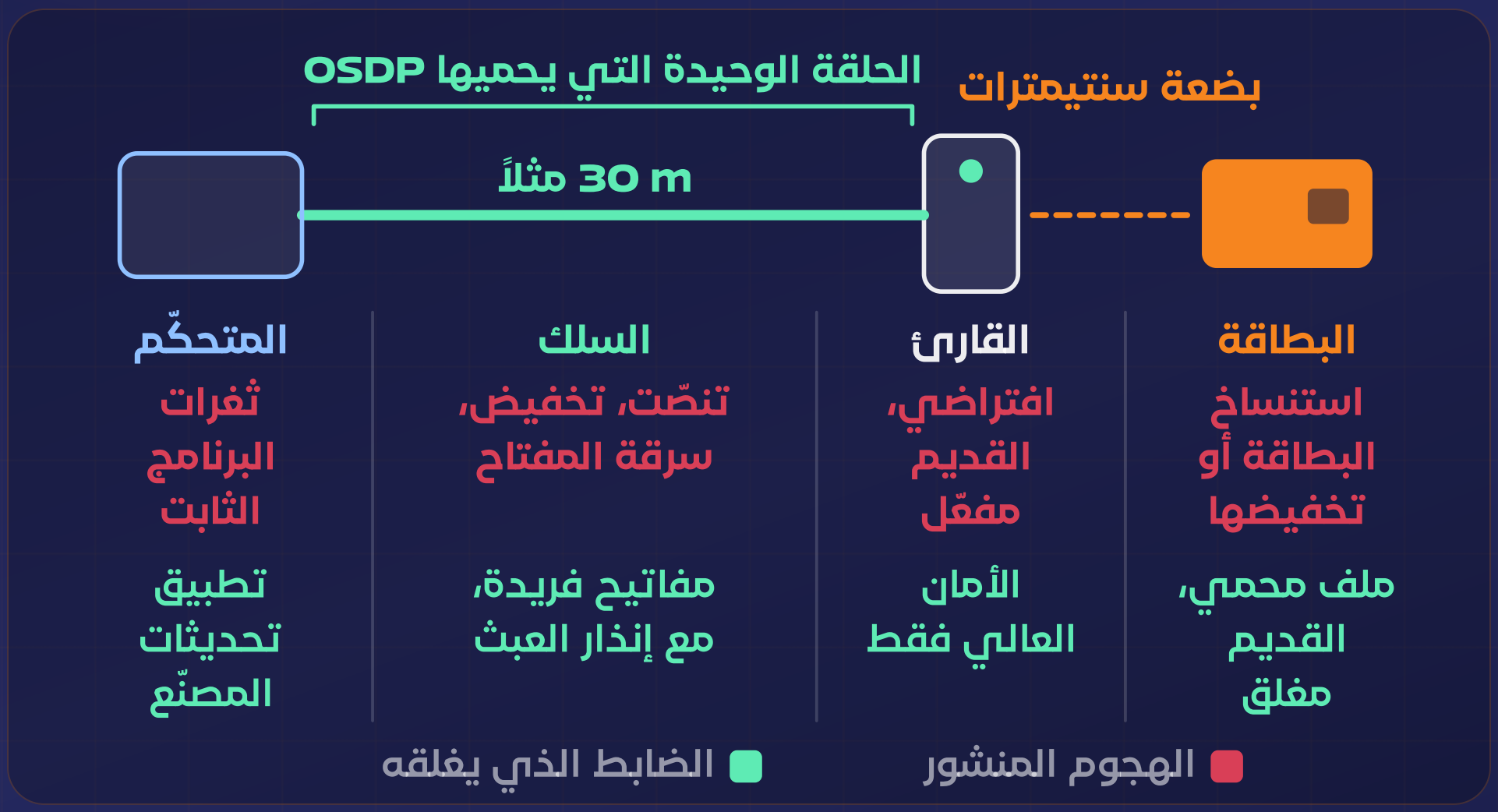
قيمة المفتاح في كلفة البحث عنه، لا في طوله

خوارزمية AES-128 ليست مكسورة، والضعف في إدارة المفاتيح. فالمفتاح الافتراضي المنشور قيمته 0 بت لمن يملك نصّ المواصفة، ووضع التركيب المتروك قد يسلّم المفتاح لجهاز على السلك. وأنماط Bishop Fox الثلاثة المختبَرة تعطي 768 احتمالاً، أي $\log_2(768) \approx 9.6$ بت لهذه المجموعة وحدها. [4]

ولا يساوي المفتاح 128 بت إلا إذا اختير عشوائياً بانتظام من كل القيم الممكنة وحُفظت سرّيته، ووصف «مولّد في الموقع» لا يثبت ذلك.

إعادة الترتيب التي وُجدت هذه الحلقة لأجلها

يحمي OSDP الوصلة بين القارئ والمتحكم، أما استنساخ البطاقة فهو خطر منفصل.



تحمي القناة الآمنة الوصلة بين القارئ والمتحكّم، لكنها لا تؤمّن البطاقة ولا بطاقات 125 kHz القديمة ولا الصيغ المفتوحة ولا ضبط القارئ ولا البرنامج الثابت للمتحكّم. **فعالج الوصلة والبطاقة معاً، فلا يغني أحدهما عن الآخر.** [1][6]

والبرنامج الثابت جزء من السلسلة: ثغرة CVE-2023-21406 في معالج OSDP بجهاز AXIS A1001 (الإصدار 1.65.4 وما قبله) أصلحها تحديث من Axis. [9]

التشفير ليس هو الهدف

هجوم خفض مستوى الأمان لا يحتاج إلى كسر AES-128



شريحة AES-128 لا تُهاجَم

تصف HID مهاجمين يعجزون عن نسخ بطاقة Seos أو DESFire، فـ«يستخدمون وضع الترحيل بالعكس»: تُقرأ بيانات البطاقة ثم تُرمَّز على بطاقة من جيل قديم. ولا ينجح ذلك إلا حيث تبقى التقنية القديمة مفعّلة ويقبلها القارئ. [6]

فالتعرّض يتوقّف على الضبط. والحلّ لدى HID تعطيل البطاقات القديمة في القارئ بعد انتهاء الترحيل، أو طلب قارئات **بملف عالي الأمان حصراً** لا يمكن تفعيل وضع الترحيل فيها. [6]

الجزء الذي لا يصلحه التشفير

رقم البطاقة وحده ليس دليلاً على أصالتها

مفتوحة
H10301
يمكن لأي أحد طلب الرقم
التكرار ممكن

متتبَّعة
H10302
تضبط HID الإصدار
التكرار ممنوع

مقيّدة
Corporate 1000
للمشترين المعتمَدين فقط
التكرار ممنوع

ضبط الإصدار ليس إثباتاً للأصالة
فذلك يتطلّب مصادقة البطاقة

رقم البطاقة يعرّف المستخدم، لكنه لا يثبت أن البطاقة أصلية. فذلك يتطلّب مصادقة البطاقة، وحماية بياناتها، وضبط إصدارها، وتفويضاً صحيحاً في المتحكّم. ومع ذلك تطلب HID حماية أرقام البطاقات كما تُحمى كلمات المرور. [6]

فالصيغ المفتوحة مثل H10301 «يمكن لأي فرد طلبها»، لذا قد تتكرّر الأرقام. أما الصيغ المتتبَّعة والمقيّدة فتضبط الإصدار، لكنها لا تصادق على البطاقة. [6]

سُلّمان، ولا واحد منهما يفتح الباب.

الدرجة ليست هي المستوى، والمواصفة تستثني القفل.

IEC 60839-11-1

1 2 3 4

يحدّدها تقييم المخاطر، لكل نقطة دخول

UL 294

I II III IV

يحدّدها الاختبار النمطي، لكل منتج

سُلّمان، على أساسين مختلفين

1. درجات **IEC 60839-11-1** من 1 إلى 4 تُحدَّد لكل نقطة دخول بتقييم المخاطر، أما مستويات **UL 294** من I إلى IV فتأتي من اختبار المنتج. فهما نظاما تصنيف منفصلان، فلا تقرأ الدرجة 4 على أنها المستوى IV. [3]

2. تحيل IEC 60839-11-1 الأقفال والفتّاحات والبوّابات الدوّارة والحواجز إلى مواصفات أخرى. أما سلوك القفل عند انقطاع التغذية، أي أن يتحرّر (fail-safe) أو يبقى مقفلاً (fail-secure)، فمعرّف في 11-2 لكنه غير مشترط فيها. [3]

تخضع أبواب الهروب للقسم 1010 في **SBC 201-CR-2024** مع **SBC 801-CR-2024**، ولقواعد الدفاع المدني لسبل الهروب: فتح بلا مفتاح ولا معرفة خاصة، ووسيلة يدوية عند تعطّل الوسيلة الآلية. فراجع كل باب على حدة. [8]

الجواب السعودي، بصراحة

لم نحدّد اشتراطاً صريحاً لـ OSDP في المراجع السعودية التي راجعناها (4 أكتوبر 2026)

الدخول، سجلّات CCTV	NCA ECC-2:2024, 2-14
مواصفات خليجية ظهرت	11-1:2014, 11-2:2016
جزء OSDP، أي 11-5	لم يظهر في البحث
OSDP على السلك	لم نجد اشتراطاً صريحاً

قد تشترطه مواصفات المشروع أو العميل

مراجع رُوجعت في 4 أكتوبر 2026

تنطبق ضوابط **NCA ECC-2:2024** على الجهات الحكومية، وعلى جهات القطاع الخاص التي تملك أو تشغّل بنى تحتية وطنية حساسة. ويشترط البند 2-14 الدخول المصرّح به إلى المناطق الحرجة، وسجلّات الدخول والمراقبة (CCTV) وحمايتها، ولا يسمّي بروتوكول قارئ. [8]

وفي بحث في متجر هيئة التقييس الخليجية بتاريخ 4 أكتوبر 2026 ظهر الجزآن 11-1 مع 11-2 مواصفتين خليجيتين، ولم يظهر 11-5. والمواصفة الخليجية لا تصبح وحدها إلزاماً سعودياً، وقد يشترط المشروع أو العميل [8] .OSDP

اكتب هذا بدلاً من ذلك

ستة فحوص قبل التسليم

1. **البطاقة:** حدّد تقنية آمنة، وعطّل البطاقات القديمة ما لم يوجد مبرر موثّق.
2. **الإصدار:** اضبط إصدار البطاقات، واحمِ أرقامها بوصفها بيانات حساسة.
3. **الوصلة:** فعّل القناة الآمنة في OSDP، وارفض اتصال القارئ دونها.
4. **المفاتيح:** استخدم مفتاحاً عشوائياً فريداً لكل قارئ؛ اضبطه بأمان وارفض SCBK-D أثناء التشغيل المعتاد.
5. **الإشراف:** اختبر إنذارات العبث وانقطاع الاتصال، وطبّق تحديثات البرنامج الثابت من المصنّع.
6. **الباب:** حدّد الدرجة وسلوك القفل عند انقطاع التغذية وفق متطلبات الحريق وسلامة الأرواح وكود البناء.

التسليم: نتائج الاختبارات وسجلات توليد المفاتيح، دون المفاتيح نفسها.

علامة OSDP Verified تثبت المطابقة، لا أمان التركيب. [1]

المصادر

من أين جاء كل ادعاء

[1] SIA OSDP v2.2.2 (Oct 2024); IEC 60839-11-5:2020, Ed. 1.0 SIA statements 10 Aug 2023, 18 Mar 2026; OSDP Verified list, Jun and Jul 2026

[2] SIA AC-01-1996.10, 26-Bit Wiegand Reader Interface cl. 3.2, 3.3, 4.3, 5; SIA catalogue entry, archived Jun 2026

[3] IEC 60839-11-1:2013, cl. 1; IEC 60839-11-2:2014, cl. 7.3.1 UL 294:2023, 8th edition

[4] Bishop Fox, Badge of Shame: Breaking into Secure Facilities with OSDP DEF CON 31, 9 Aug 2023

[5] US 8,358,783 B2, Table 1A; BALTECH, Wiegand specification HID ThinLine II manual 5395-901, p.5; Gecko (2008); BLEKey (2015)

[6] HID Global, Safeguarding Against Legacy Downgrade Attacks (2024) pp.1 to 4

[7] ICT AN-321 (Nov 2024), pp.9 to 27; HID Mercury MP1501 Axis A1610, TA1101-B; HID Signo installation guide; TIA-485-A

[8] NCA ECC-2:2024, 2-14; SBC 201-CR-2024 and 801-CR-2024, Section 1010 Civil Defence escape-route rules, ch. 3; GSO store search, 4 Oct 2026

[9] Axis security advisory and NVD record, CVE-2023-21406 AXIS A1001, firmware 1.65.4 or earlier

الروابط في قسم المصادر بالمقال (رمز QR في الشريحة التالية).

معرفة عملية في هندسة أنظمة التحكم بالدخول

احفظها، وشاركها مع زميل.

اقرأ المقال الكامل للحلقة

https://nlc.com.sa/ar/academy/access-control-osdp.html

الحلقة القادمة

النداء العام ومؤشّر STI