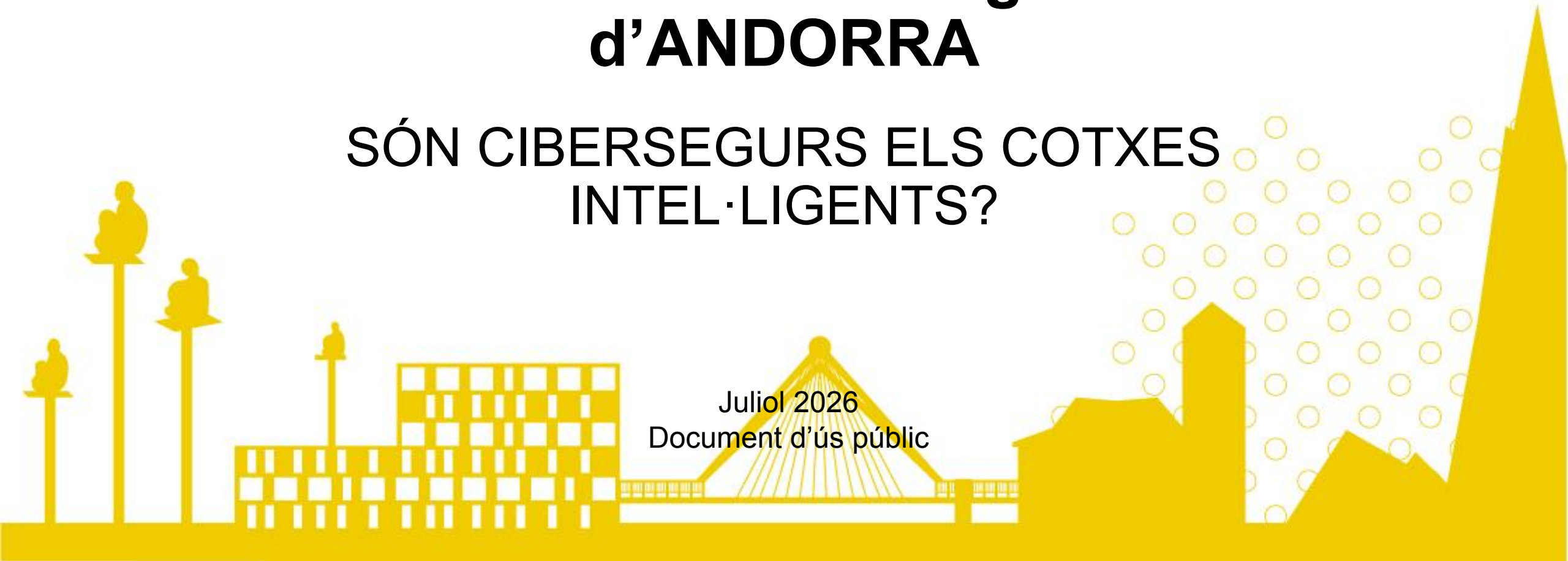
ANDORRA DIGITAL

ANDORRA DIGITAL CIBERSEGURETAT

Transformació Digital d'ANDORRA

SÓN CIBERSEGURS ELS COTXES INTEL·LIGENTS?



Juliol 2026
Document d'ús públic

Índex

1. Introducció

2. Què és un cotxe intel·ligent?

3. Per què la ciberseguretat és crítica?

4. Superfície d'atac del vehicle

5. Tipus d'atacs reals

6. Normativa i estàndards

Índex

7. Mesures de protecció de l'usuari

8. Conclusió

1. INTRODUCCIÓ

Els vehicles moderns integren programari, connectivitat, sensors i comunicació amb el núvol. Això fa que siguin sistemes ciberfísics exposats a riscos similars als de qualsevol dispositiu connectat.

UN COTXE INTEL·LIGENT ÉS UN ORDINADOR AMB RODES.
TOT ALLÒ QUE DEPÈN DE PROGRAMARI POT SER ATACAT.

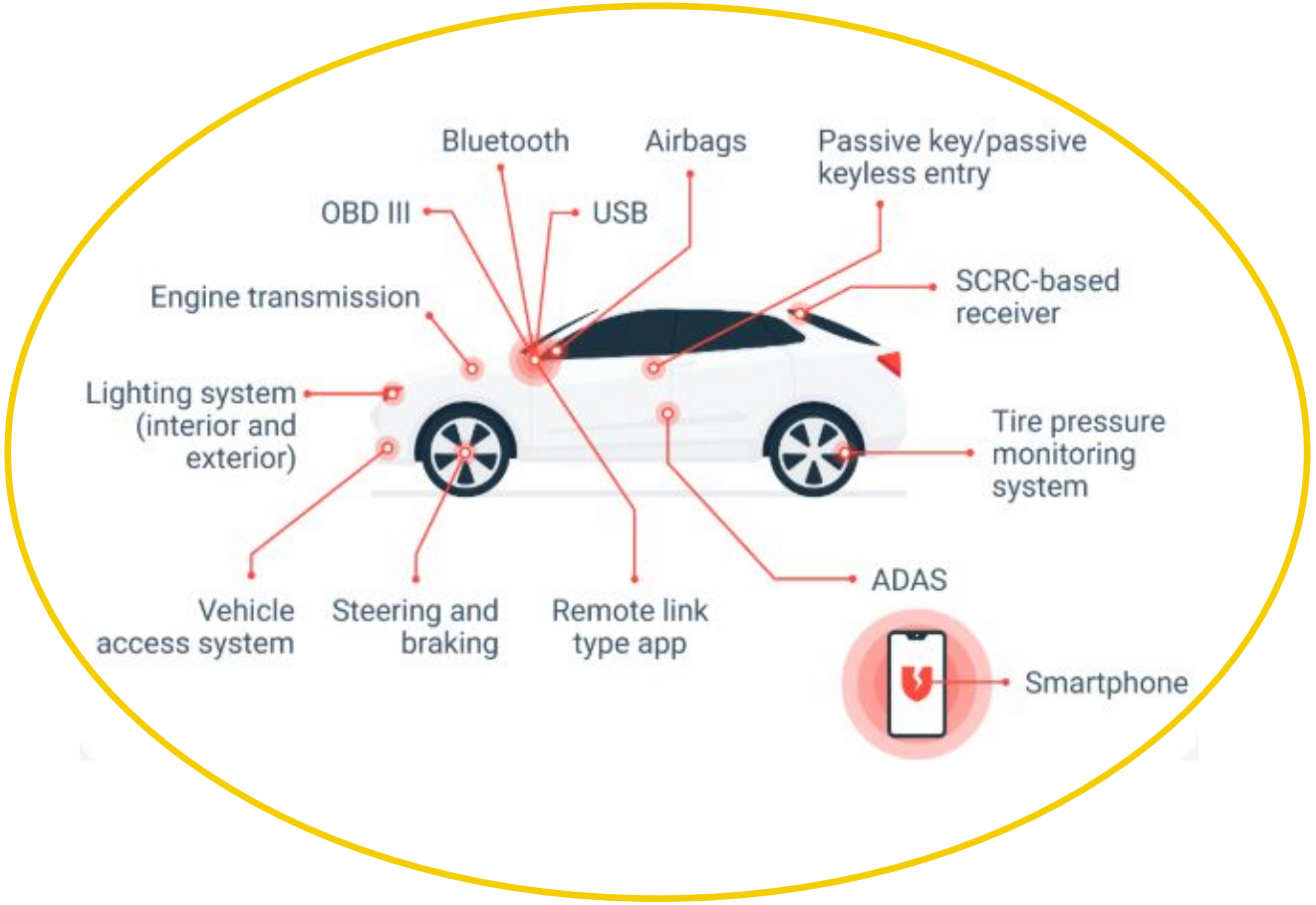
ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

2. QUÈ ÉS UN COTXE INTEL·LIGENT?

Un cotxe intel·ligent és un vehicle que incorpora:

- Múltiples **ECU** (unitats de control electrònic).
- **Sensors avançats** (càmeres, radar, LIDAR).
- **Connectivitat** (4G/5G, wifi, Bluetooth).
- **Sistemes d'assistència** (ADAS).
- **Actualitzacions OTA** (*over-the-air*).



És un **ordinador distribuït sobre rodes**, amb més de 100 milions de línies de codi.

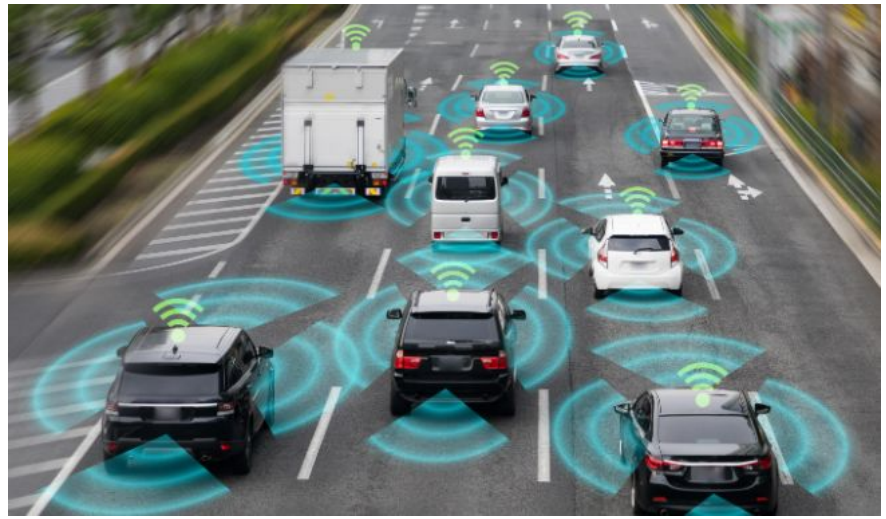
ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

3. PER QUÈ LA CIBERSEGURETAT ÉS CRÍTICA?

La digitalització del vehicle implica que:

- Un error de programari pot afectar la **seguretat física**.
- Un atac remot pot comprometre la **direcció,** la **frenada** o l'**acceleració**.
- El vehicle emmagatzema **dades personals i biomètriques**.
- La connectivitat obre portes a atacants externs.

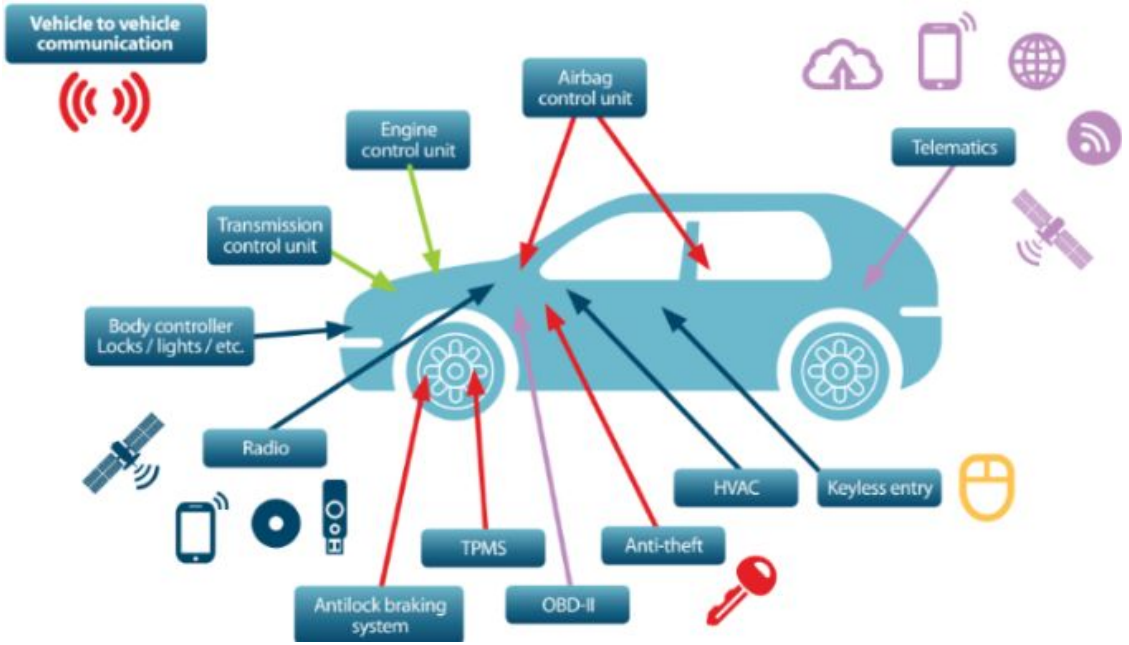


La **ciberseguretat** ja no és opcional: **és un requisit de seguretat viària.**

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

4. LA SUPERFÍCIE D'ATAC DEL VEHICLE



Principals punts vulnerables:

- **Sistema *keyless*** (*relay attacks* o atacs de retransmissió).
- **Bluetooth/wifi** del cotxe.
- **Ports OBD-II**.
- **Sistemes d'infoentreteniment**.
- **Comunicacions V2X** (de vehicle a infraestructura).
- **Sensors autònoms** (*spoofing* o suplantació, *jamming* o interferència de radar).
- **Bus CAN** (xarxa interna sense autenticació).

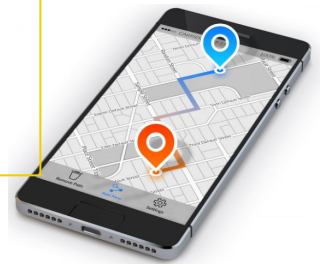
Cada component connectat és un possible vector d'atac.

Els ciberatacs més habituals tenen com a objectiu el sistema sense clau o ***keyless***.

*Aquesta tecnologia disposa d'una unitat de control. Per exemple, l**a centraleta del cotxe interpreta els senyals que envien els diferents dispositius del vehicle. Un atacant pot intentar **copiar el senyal del comandament** i enviar-lo a la centraleta per **obrir el cotxe** i accedir a l'interior o fins i tot **robar el vehicle complet**.*

El **GPS** que utilitza es pot enfrontar a dues amenaces molt importants i amb alt risc, com l'*spoofing* i el *jamming* que són capaces de manipular el senyal GPS, poden anul·lar l'autèntic i fins i tot substituir-lo.

Interrompre o saturar un senyal (ràdio, GPS, wifi, *keyless*...) per impedir que arribi al receptor.

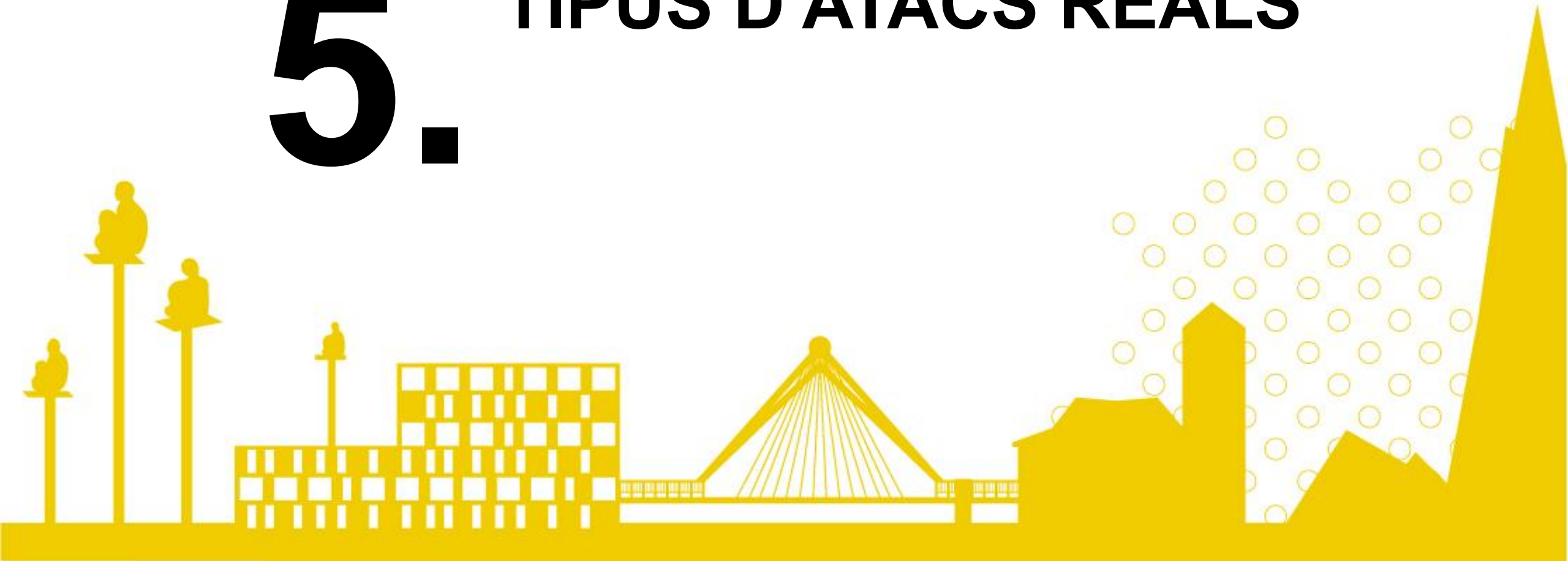


Suplantar una identitat o un senyal amb l'objectiu que un dispositiu, xarxa o usuari confiï en quelcom que en realitat és fals.

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

5. TIPUS D'ATACS REALS



Exemples documentats:

- **Pirateig del Jeep Cherokee (2015)**: control remot de frens i direcció.
- **Atacs de retransmissió a *keyless***: robatori en segons.
- **Suplantació GPS**: desviament de rutes o error de navegació.
- **Manipulació de sensors**: senyals falsos a càmeres o LIDAR.
- **Infecció via USB o apps mòbils**.

Aquests atacs demostren que l'amenaça és real, no teòrica.

6. NORMATIVA I ESTÀNDARDS

Normes clau que regulen la ciberseguretat del vehicle:

- **UNECE R155**: gestió de ciberseguretat obligatòria per a fabricants.
- **UNECE R156**: gestió d'actualitzacions de programari.
- **ISO/SAE 21434**: seguretat en enginyeria automotriu.
- **TISAX:** estàndard d'avaluació de la seguretat de la informació per a la indústria de l'automoció.

Des del 2024, cap cotxe nou es pot homologar a la UE sense complir aquestes normes.

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

7. MESURES DE PROTECCIÓ DE L'USUARI

Bones pràctiques per a propietaris:

- Desactiva ***keyless*** si no és necessari.
- No connectis dispositius USB desconeguts.
- Mantingues el cotxe **actualitzat**.
- Fes servir apps oficials i revisa permisos.
- Guarda la clau en **bosses Faraday**.
- No publiquis matrícules o VIN a xarxes socials

L'usuari és la part essencial de la seguretat.

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

8. CONCLUSIÓ

- Els cotxes intel·ligents **no són 100 % cibersegurs**, però sí que cada vegada estan més protegits.
- La ciberseguretat automotriu és un procés continu, no un estat final.
- La combinació de normativa, disseny segur i conscienciació de l'usuari és clau.
- El futur portarà més connectivitat…, i més reptes.

ANDORRA
DIGITAL