

Gépjármű fedélzeti integráció a biztonság szemszögéből

Lente Csaba

MISZK Informatikai
és Hírközlési
Szakmai Tagozat



Alapfogalmak

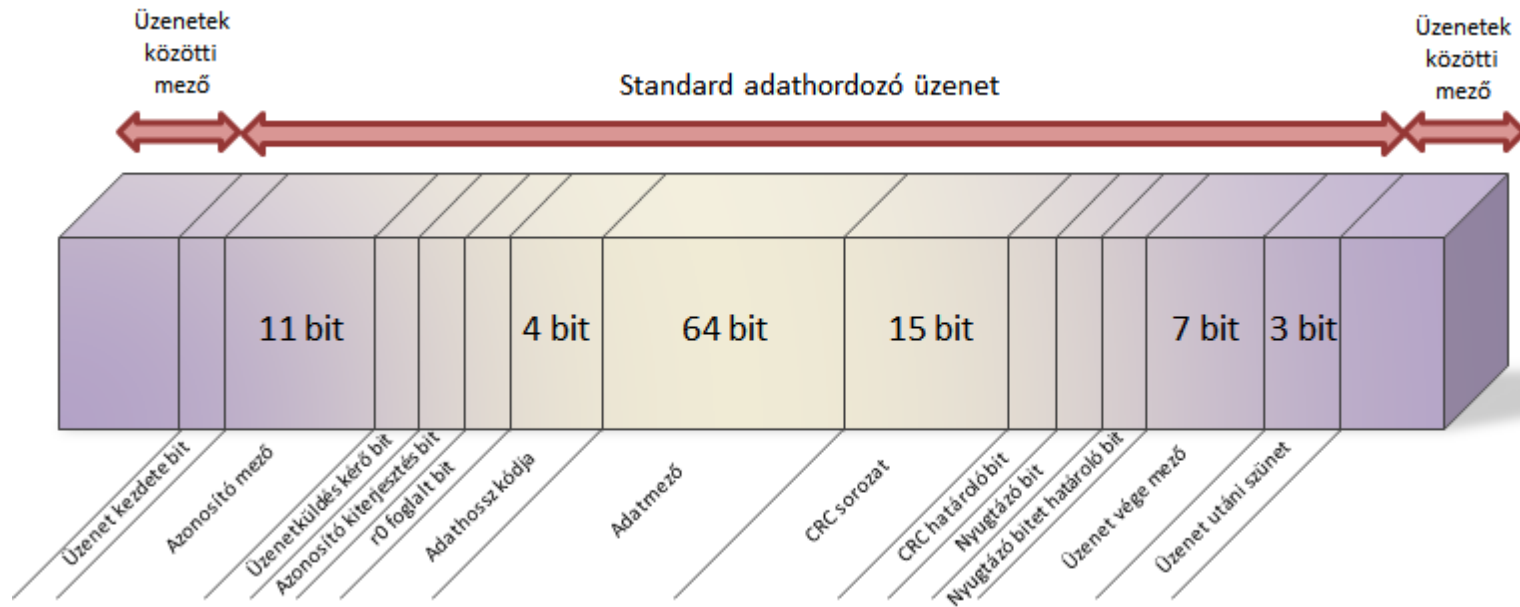
- Járműfedélzeti rendszerek fejlődése
- Digitalizáció, multiplex sínrendszer, OSI szabvány
- CAN fedélzeti kommunikáció
- Elosztott hálózat csomópontjai a mai járművekben
- Kommunikáció a fedélzeten
- Állapot és hibakódok kezelése
- Védelmi intézkedések
- Rendkívüli helyzetek, vész üzemmódok

Az OSI szabvány rétegendje

- Alkalmazási réteg
- Megjelenítési réteg
- Viszony réteg
- Szállítási réteg
- Hálózati réteg
- Adatkapcsolati réteg
- Fizikai réteg

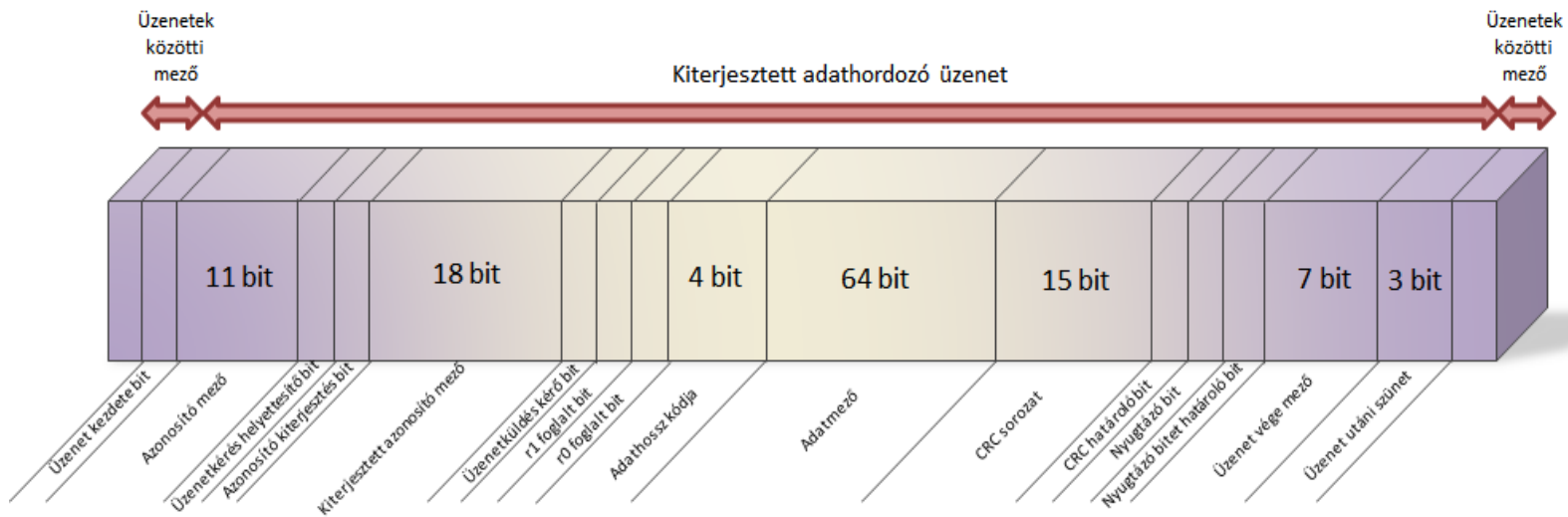
Alapfogalmak

CAN kommunikáció (2.0A)

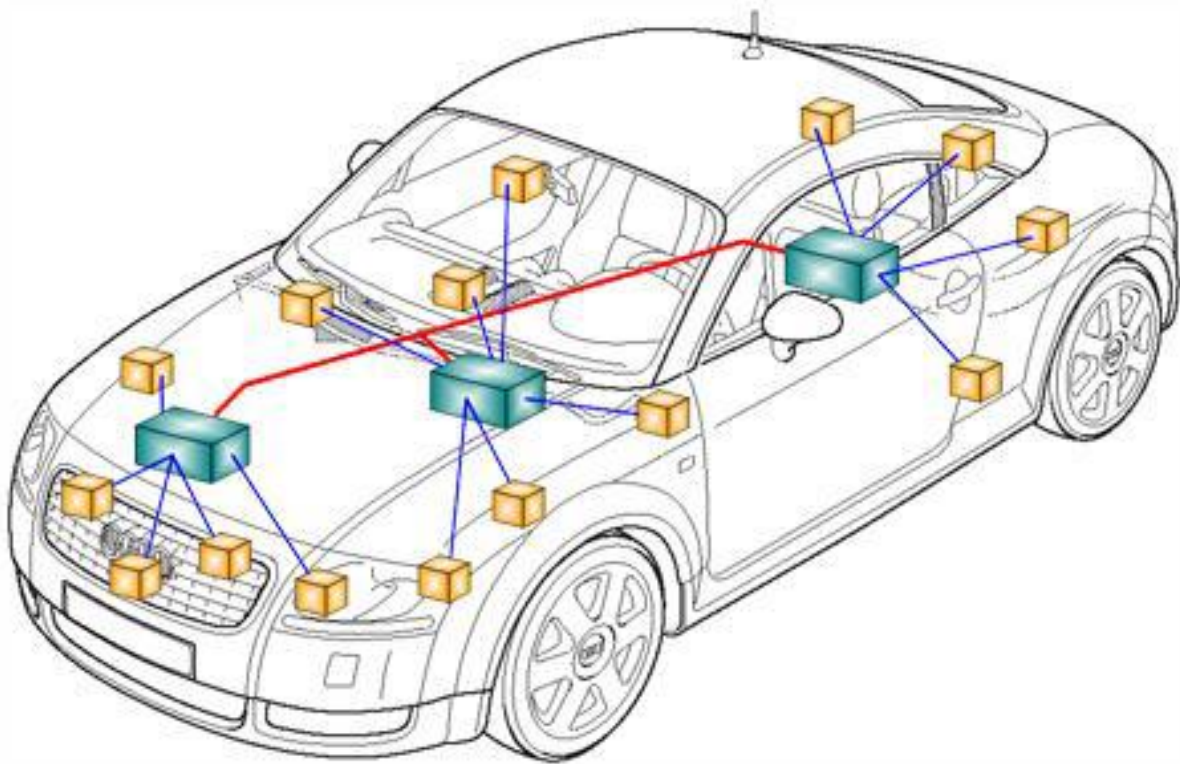


Alapfogalmak

CAN kommunikáció (2.0B)



Elosztott hálózat



Kommunikáció a fedélzeten

Jellemzők:

- Multimaster csomópontok
- Üzenetközpontúság
- Broadcast üzenetküldés
- Eseményvezérelt
- Flexibilitás, gyorsaság
- Hibatűrés, javítás, nyugtázás
- Hiba és vész állapotok kezelése

Biztonsági kérdések

- Üzemviteli biztonság
- Műszaki biztonság
- Adatbiztonság
- Közlekedési biztonság
- Vagyonbiztonság
- Környezeti biztonság
- Rendszerszintű biztonság

Illegális behatolás a fedélzetre

Jellemző elkövetési módok:

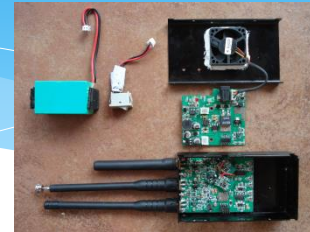
- Központi zár vezérlés blokkolás
- Távirányító lehallgatás
- Keyless-go periodikus jel lopás
- CARB csatlakozóhoz férés aktív és standby periódusban
- Bluetooth biztonsági rés használata
- Fedélzeti hotspot feltörés
- Applikáción keresztüli behatolás

Elterjedt behatolási eszközök

- ✓ Központi zár blokkoló adóvevőből:



- ✓ Profi zár blokkoló három hullámsávon:



- ✓ 8 ch GSM, Wifi, GPS multi Jammer:



- ✓ ASK 315 Keyless Go Repeater:



- ✓ OBD-II fedélzeti kiolvasó:



- ✓ Aktív RFID kulcs klónozó:



Nyomozati lehetőségek

Tárgykörözés alatt

- GPS / mobilszolgáltató nyilatkoztatása / online keresés
- Járműkövetési rendszerek lekérdezése
- Hagyományos nyomkutatás, kamerás felvételek

Fellelt jármű esetén

- Egyedi azonosítók ellenőrzése (digitálisak is)
- Fedélzeti szakértői vizsgálat elrendelése
- Informatikai alapú közvetlen nyomrögzítés

Árulkodó digitális nyomok

- Behatolás CAN bus megsértésével
- Központi zár vevő megzavarása
- Plusz kulcs azonosító a fedélzeti naplóban
- Illegális checksum generálása
- Fejegységben tárolt GPS/POE adatok
- Digitális „ikresítés”
- ECU tiltásainak feloldása
- Bluetooth/Wifi eseménynapló

Hozzáférés a digitális nyomokhoz

- Rendszerbeszállítói kódok ismeretében
- Teljes körű hozzáférési jog és eszköz birtokában a márka központi szervizpontján (Admin mód)
- Járműspecifikus kód és állapot analízátorral
- Célszoftverek és hardverek használatával

Reális elvárások a szakértővel szemben

- A zárt fedélzeti informatikai rendszerbe behatolás tényének és körülményeinek megállapítása
- A behatolás módszerének feltárása
- Digitális nyomok rögzítése
- Eseménynaplók adatainak hiteles mentése és elemző vizsgálata
- A célhardverek állapotának felmérése
- Műszaki vagy szoftveres jogellenes beavatkozás adatainak kinyerése és átadása

További veszélyek

- Behatolás a szórakoztató központ és a fedélzeti telemetria biztonsági réseinek kihasználásával
- Kulcsnélküli rendszerek sikeres támadása, a védelem kiiktatása (belsőégésű motor: immobilizer, hibrid/elektromos hajtáslánc: inverter)
- Fedélzeti irányítás (motor, sávelhagyás figyelő, követés érzékelő) átvétele
- Önvezető járművek távoli befolyásolása

Hogyan védekezzünk?

- Gondos típus/modell választás
- Egyedi mechanikai/elektronikai védelem szakszerű kialakítása
- Távirányító gomb használatának mellőzése a kulcson
- Néma riasztás alkalmazása
- Validált fedélzeti mobil applikációk alkalmazása
- A fedélzeti interkommunikáció zárttá tétele

Járművek, melyekhez specifikus hacktool eszközök beszerezhetők

Gyakorlatilag minden távirányítással nyitható és kulcsnélküli indítórendszerrel szerelt jármű veszélyeztetett, de az *elkövetési statisztikák szerint* különösen:

- Prémium kategóriában: BMW SD-XD sorozat 2012-től, Audi Q és R sorozat, Mercedes C, E osztály, Land Rover 2010-től, Volvo XC, Mini és Smart, Lexus NX-RX
- Klasszikus típusok közül: Toyota RAV4, Prius 3-4, VW Tiguan, Touran, Nissan Quashqai 2013-tól, Mazda CX

Mit ígér a közeljövő?

- Továbbfejlesztett energiasejt, hibrid és tiszta elektromos hajtást, elfogadható valós hatótávval (-> 1000km)
- „Fekete doboz” digitális eseményrögzítővel
- Széria tartozék vészívó fedélzeti egységet baleseti riasztásra
- Automata áramtalanítót ütközés esetére
- Biztonsági kiegészítő fékrendszert másodlagos ütközések kivédésére
- Még több felhasználói kényelmet, látványos megoldást, kommunikációt

Köszönöm a figyelmet!

