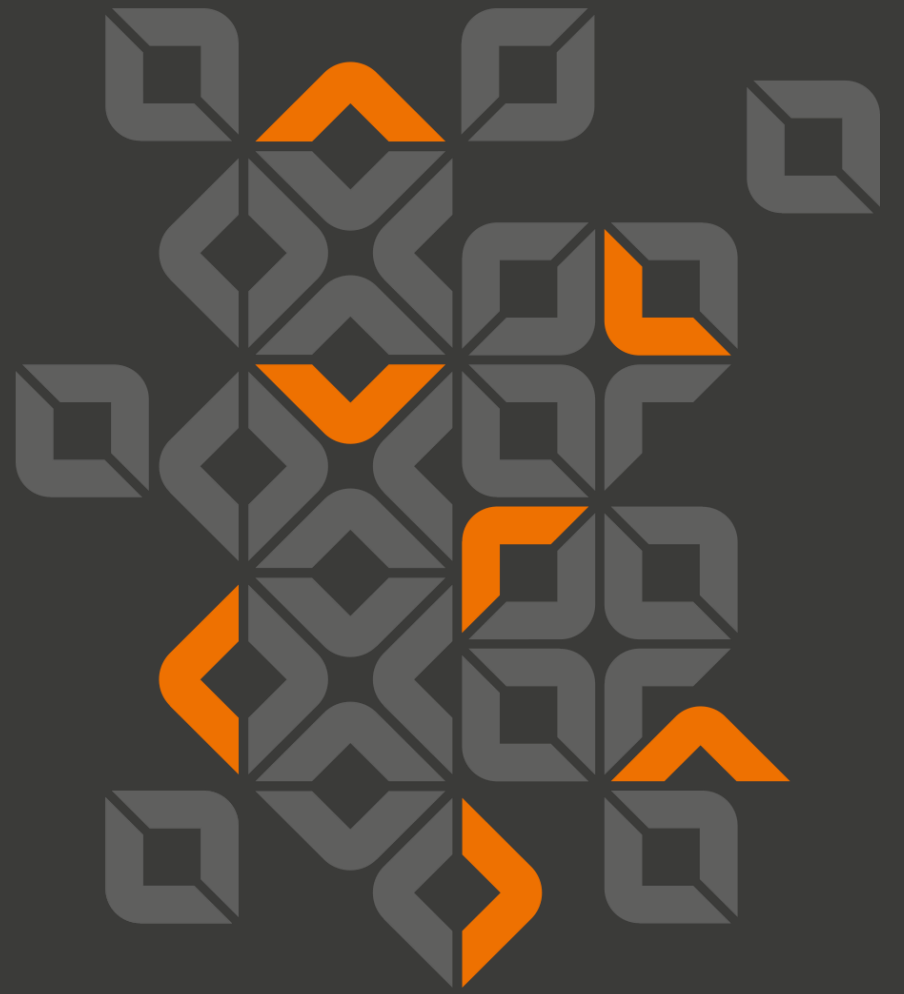
Network Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában



ALVERAD
TECHNOLOGY FOCUS

Répás József – Nemzeti Közszolgálati Egyetem - KMDI

Alverad Technology Focus Kft.

- Független, integrált, szakmai partner
- Akkreditált kiberbiztonsági vizsgálólaboratórium
- Ipari rendszerek, informatikai rendszerek, szoftverek biztonsági vizsgálata

NAH-1-1829/2022
Vizsgálólaboratórium

Bevezető

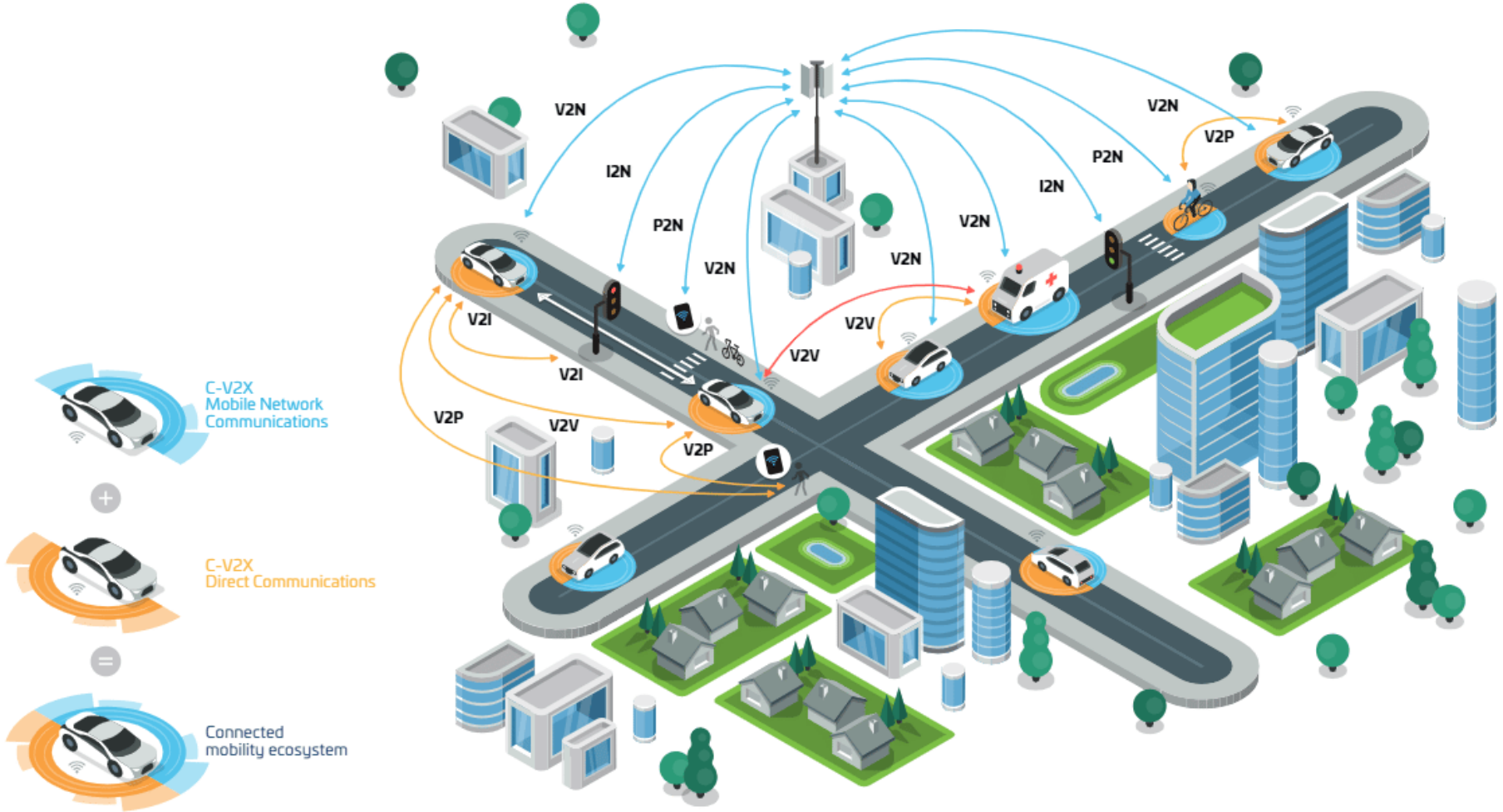
- A járműipar fejlődése
- Modern közúti közlekedési járművek megjelenése
- Hálózatba kapcsolt járművek
- Önvezető - emberi beavatkozás nélkül működő- járművek

- Közúti közlekedés balesetmentesítése
- Hatékony forgalomszervezés
- Károsanyag kibocsátás csökkentés
- Életmód változás

Aktualitás

- Új információs és kommunikációs technológiák
- Exponenciálisan növekszik a hálózatokban átvitt információk mennyisége
- Új szabályozási és vizsgálati környezet
- Járműgyártók elleni kibertámadások
- e-Call Segélyhívó Rendszer

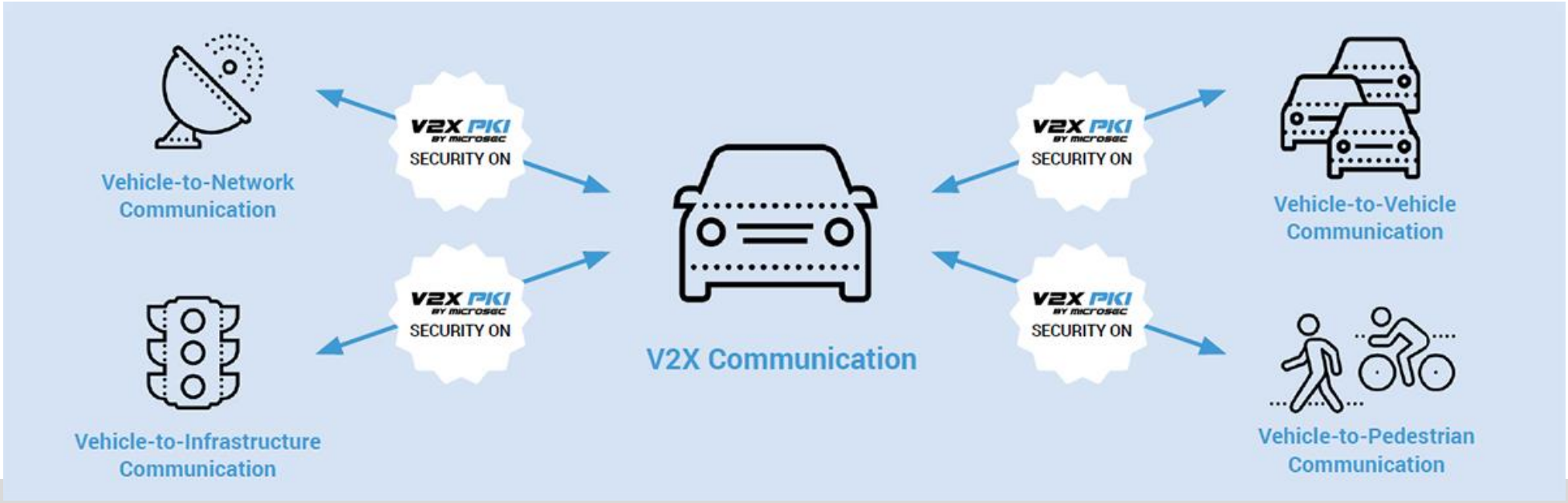
C-ITS


C-V2X
Mobile Network
Communications
C-V2X
Direct Communications
Connected
mobility ecosystem
V2N
I2N
P2N
V2N
V2N
V2N
I2N
P2N
V2P
V2I
V2I
V2V
V2V
V2P
V2V
V2P

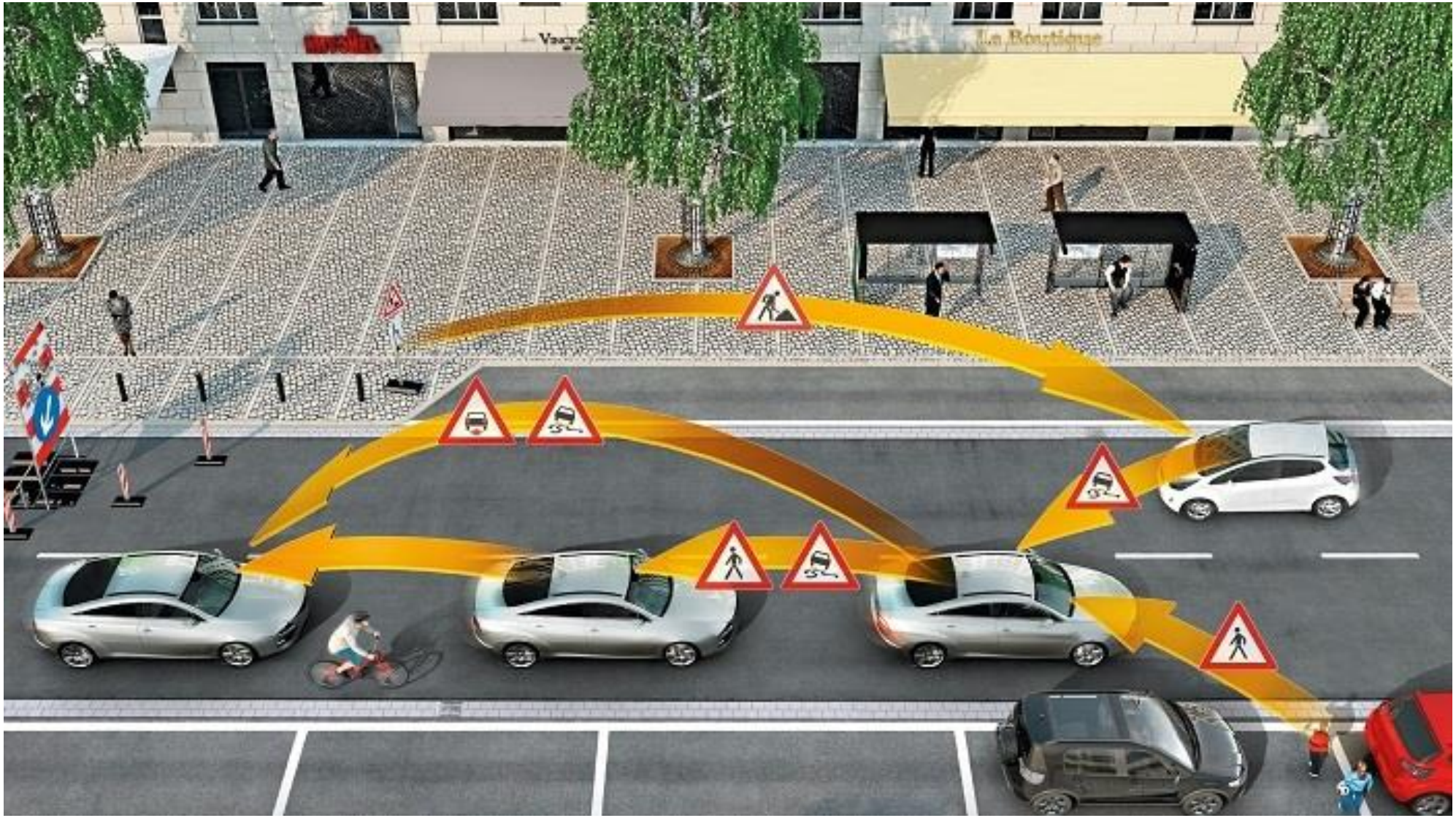
V2X

A jármű- és minden lehetséges dolog közötti együttműködés, kommunikáció lehetővé teszi, hogy összekapcsolja az összes járműtípust és a különféle infrastrukturális rendszereket.

Ez a kapcsolat magában foglalja az autókat, az autópályákat, a hajókat, a vonatokat, a repülőgépeket, valamint a gyalogosokat stb. is, ezáltal megvalósítva a teljes körű kooperativitást a közlekedésben



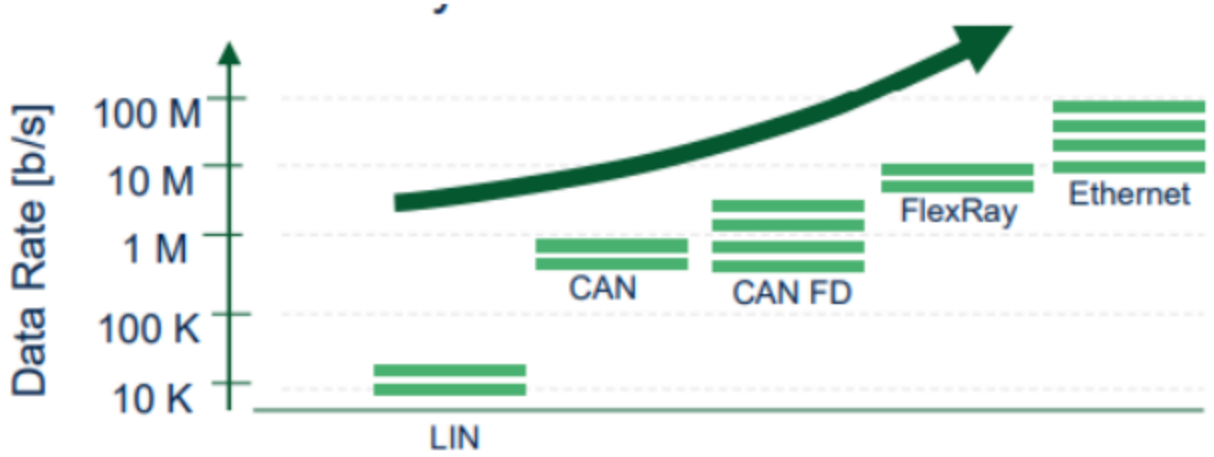
DSRC - Dedicated short-range communication



Jármű belső kommunikáció

Az autóipar általánosan elfogadott kommunikációs szabványa:

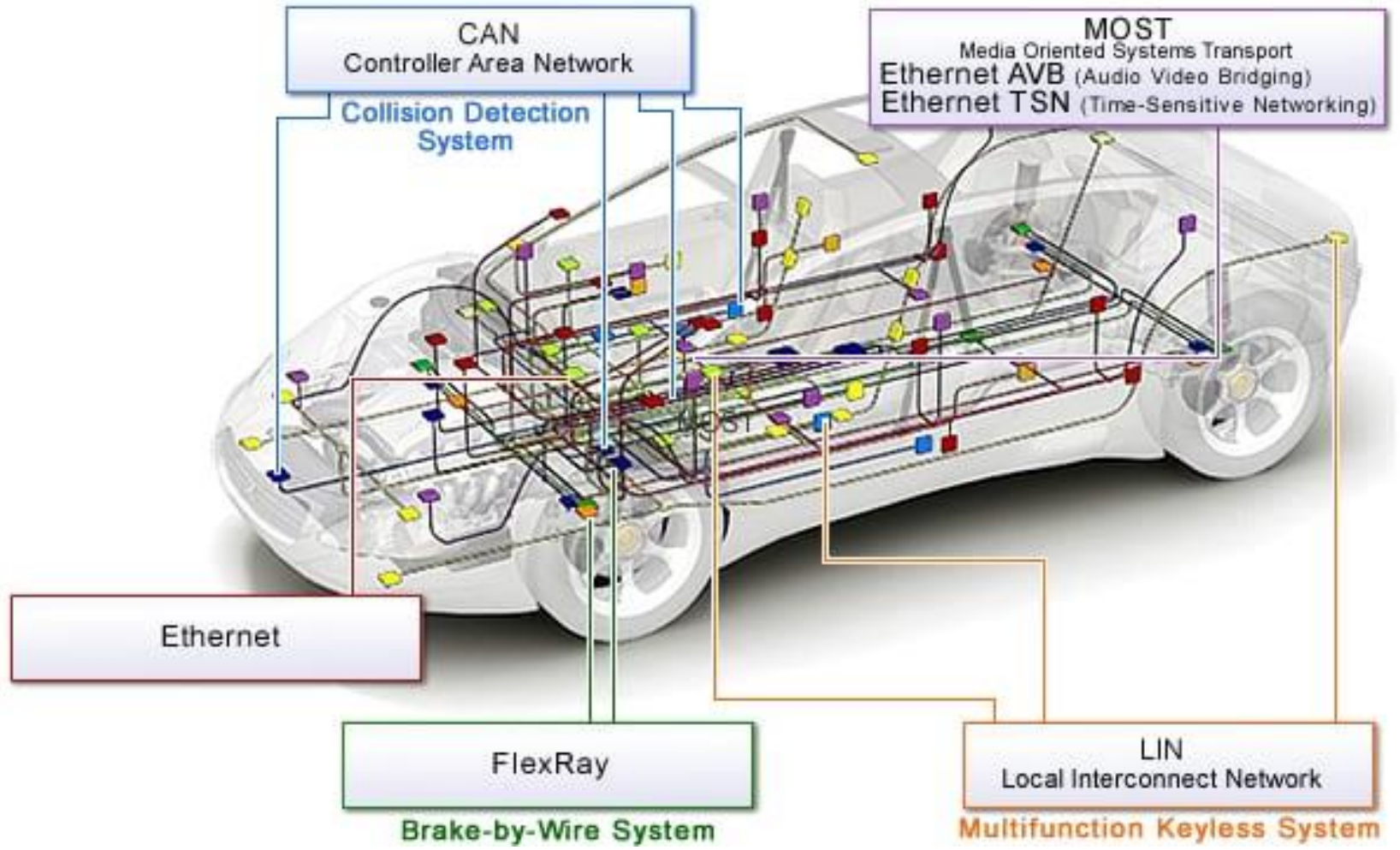
- a CAN (Controller Area Network) protokoll,
- LIN (Local Interconnect Network),
- Flaxray,
- Automotive Ethernet.



Melyek szegmentált kialakítással, egyre gyorsabb és biztonságosabb kommunikációt hivatottak megvalósítani. Gateway-eken keresztül.

Jármű belső kommunikáció

A2B – Analog Devices‘ Automotive Audio Bus
MOST – Media Oriented System Transport



Jármű és nyomok

- Jármű a támadás célpontja,
- A jármű eszköz a bűncselekmény elvégzéséhez,
- Jármű tartalmazza az bizonyítékot.

- Európa Tanács Ajánlása a „Számítógépes-környezetben elkövetett bűncselekményekről”
  - Csalás, hamisítás, szabotázs,
  - Adatokban és programokban történő károkozás, ezek megváltoztatása,
  - Jogellenes behatolást
  - Jogellenes titokszerzést, kémkedés.

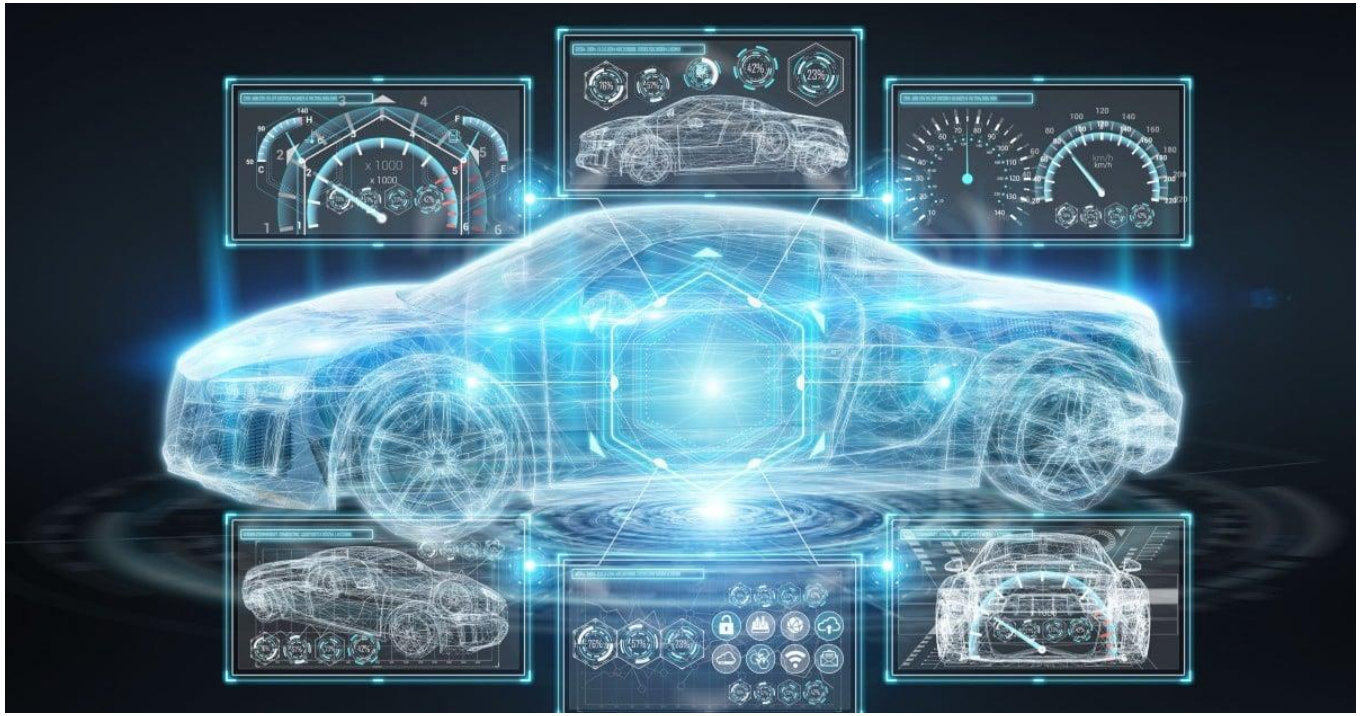
Forenzikus szakértői vizsgálat

- A vizsgálatok célja, a járművekben, járműrendszerekben bekövetkezett események hiteles, rekonstrukciója, felderítése. A releváns eseményekről bizonyítékok szolgáltatása, a későbbi, akár nyomozati és igazságszolgáltatási tevékenységekhez való felhasználáshoz.

Járművekhez kapcsolódó hálózati szakértői vizsgálatok célja

Járművekben található bizonyítékok

- Fellelése,
- Feltárása,
- Kinyerése,
- Vizsgálata,
- Megőrzése.



- Nyilvánvalóvá kell tenni, hogy mi történt, olyan esetekben is ami nem megismételhető.
- Live forensics kapcsolat + naplózás.

Vizsgálatok szükségessége

- Feltételezett visszaélés,
  - Jogosult vagy jogosulatlan hozzáférés,
  - Manipuláció,
  - Visszaélés vizsgálata.
- Megtörtént esemény vizsgálata,
- Root case elemzés
- Kártékony kód,
- Terrorcselekmény,
- Titkos információgyűjtés.

Network Forensics

A Network Forensics a Computer Forensics egyik ága, amely kommunikációs hálózatok mozgásban lévő adatainak (data in motion) azonosításához, vizsgálatához, értékeléséhez és elemzéséhez, illékony és dinamikus információkkal foglalkozik.

Célja annak biztosítása, hogy megértsük a hálózaton keresztül átvitt adatokat, valamint a végpontok felé irányuló, vagy közötti interakciók és tevékenységek feltárása.

A hálózatokban megjelenő potenciális digitális bizonyítékokat a network forensics eszközrendszerével kell azonosítani és értékelni.

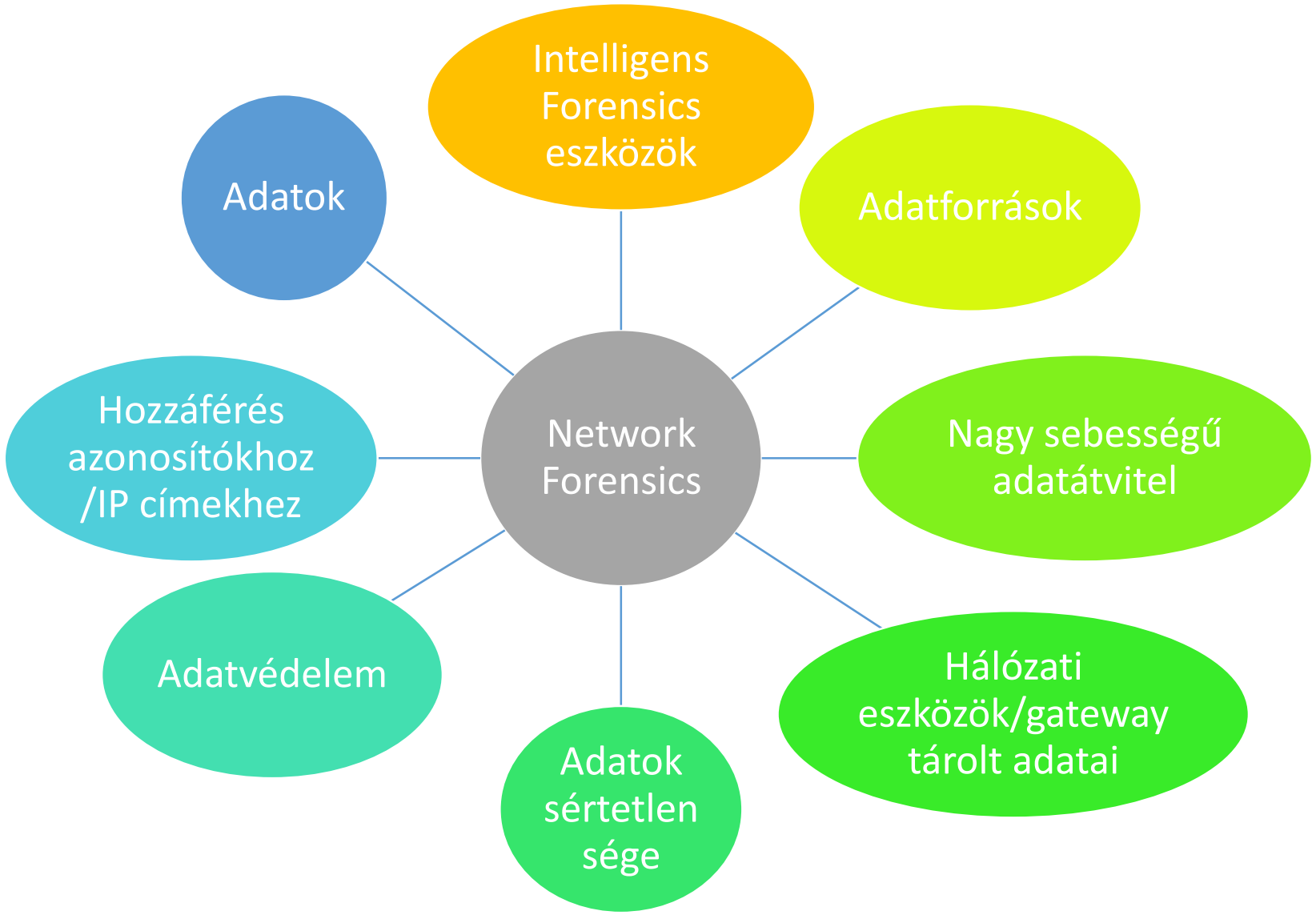
Network Forensics

- Hatóság,
- Katonai és állami szervezetek,
- Vállalatok,
- Egyetemek és kutató szervezetek,
- Kiberbiztonsági szervezetek.

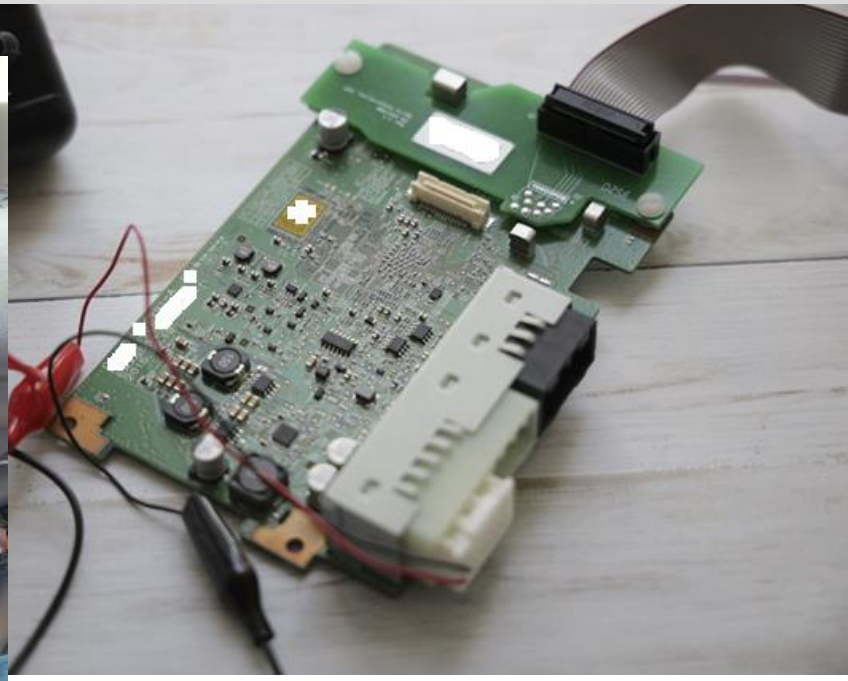
- Kiberműveletek,
- Incidenskezelés,
- Igazságszolgáltatás,
- Csalásmegelőzés,
- Hálózati teljesítmény optimalizálás,
- Kutatás és fejlesztés.

Csatornák és kihívások

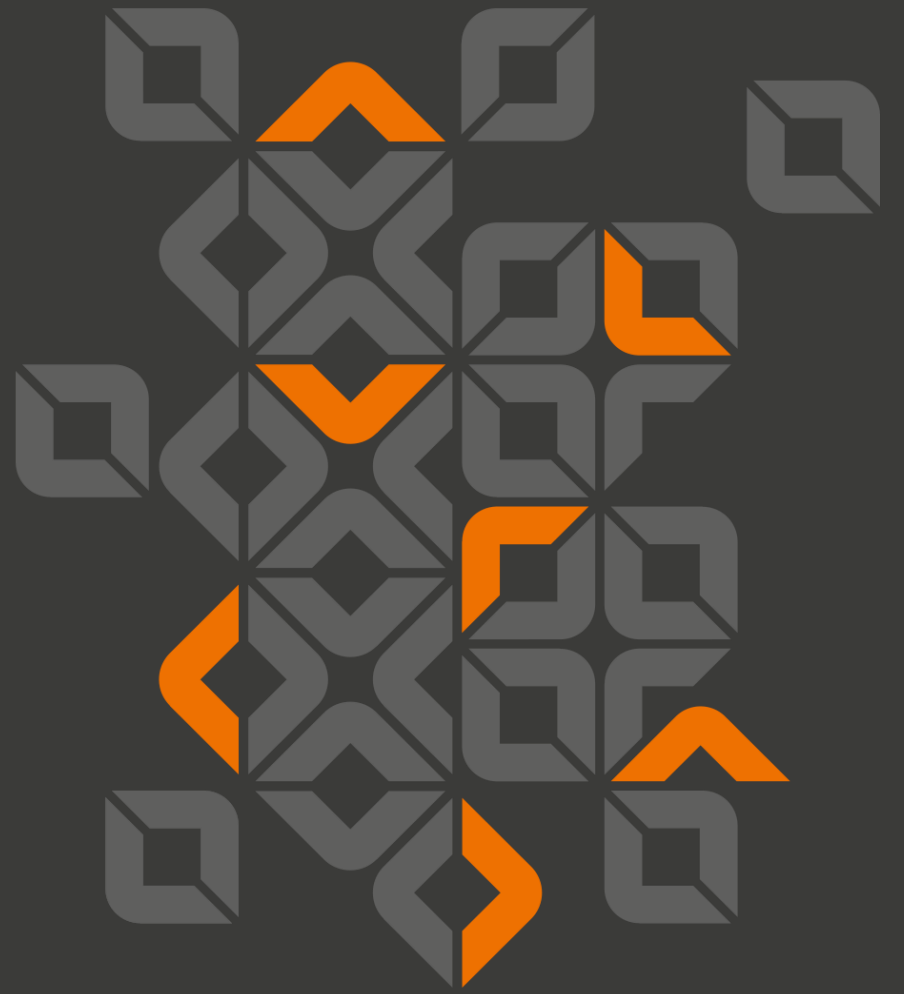
- Vezetékes
  - OBD-II
  - USB
- Vezeték nélküli
  - Wifi
  - Bluetooth
  - RFID



Jármű szakértői vizsgálat



Köszönöm a figyelmet!



ALVERAD
TECHNOLOGY FOCUS