

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

Az autonóm közúti járművek kiberbiztonsági kihívásai és társadalmi megítélésük

Jelige: knight rider

Pályamunka lezárásának időpontja:
2022. május

2023.

Tartalomjegyzék

Bevezetés.....	1
Téma aktualitása.....	1
Tudományos probléma	1
Módszertan	2
Kutatási hipotézisek	2
Kutatási célkitűzések.....	2
1 Autonóm közúti közlekedési eszközök felépítése.....	4
1.1 Autonóm vezetés definiálása	4
1.2 Gépjárművezérlő rendszerek	6
1.3 Autonóm vezetési rendszerelemek	8
1.3.1 Autonóm irányítást segítő szenzorok	9
1.3.2 Operációs rendszerréteg	11
1.3.3 Feldolgozó algoritmusok.....	12
1.4 Külső kommunikációt támogató rendszerelemek.....	12
1.5 Következtetések.....	15
2 Önvezető közúti járművek kiberbiztonsági kihívásai és megoldásai.....	16
2.1 Gépjárművezérlő rendszerek kiberbiztonsági fenyegetései.....	16
2.2 Gépjárművezérlő rendszerek védelmi eljárásai	17
2.3 Autonóm vezetési rendszerelemek kiberbiztonsági fenyegetései	19
2.4 Autonóm vezetési rendszerelemek védelmi eljárásai	21
2.5 Külső kommunikációt támogató rendszerelemek kiberbiztonsági fenyegetései	25
2.6 Külső kommunikációt támogató rendszerelemek védelmi eljárásai	27
2.7 Következtetések.....	30
3 Az autonóm járművek jogszabályi és szabványi kereteinek vizsgálata	31
3.1 Jogszabályok.....	31
3.1.1 Egyesült Államok szabályozása	31

3.1.2	Európai Unió szabályozása	35
3.2	Az automatizált közúti járművekkel kapcsolatos szabványok	37
3.2.1	Megoldások bemutatása	38
3.3	Következtetések.....	57
4	Az autonóm közlekedés társadalmi megítélése.....	59
4.1	Online tartalom analízis.....	59
4.1.1	Elemzés részletei	60
4.2	Hazai helyzet felmérése.....	61
4.2.1	Kérdőív bemutatás.....	61
4.2.2	Eredmények.....	63
4.3	Következtetések.....	70
5	Összegzés	71
6	Irodalomjegyzék.....	73
	Mellékletek.....	78
1.	számú melléklet (ábrajegyzék).....	78
2.	számú melléklet (táblázat jegyzék)	78
3.	számú melléklet (rövidítések jegyzéke)	80
4.	számú melléklet (kérdőív).....	81
5.	számú melléklet (kérdőív kiértékelés)	85

Bevezetés¹

A beépített technológiai megoldások és a vezeték nélküli képességek elterjedésével a mai járművek már nem elszigetelt mechanikus gépek. Egy összekapcsolt rendszer részévé válnak, amelyben folyamatosan kommunikálnak a járművek az egyes rendszerelemei egy belső hálózatban, továbbá a járművek egymással és a forgalom irányítási központtal egyaránt. Ezen összekapcsolt adatok halmazát nevezzük önvezető közlekedési eszközök irányítási rendszerének. Ez a rendszer képes támogatni az autonóm közlekedés jövőbeli bevezetését és a mesterséges intelligencia használatával jelentősen javítani lehet a közlekedés biztonságát, hatékonyságát és fenntarthatóságát. Az autonóm közlekedési eszközök megjelenése azonban új biztonsági kérdéseket vet fel, amelyek az egész rendszert potenciális célponttá teszik a kiberbiztonsági támadásoknak, ezek pedig mind a közlekedés biztonságát, mind pedig az emberi életet veszélyeztethetik.

Téma aktualitása

A globális autonóm járművek piacát 2021-ben 94,43 milliárd USD-ra becsülték, és az előrejelzések szerint 2030-ra eléri a 1808,44 milliárd USD-t, amely 2021 és 2030 között 38,8%-os összetett éves növekedési ütemet mutat. Ezt a fejlődést támogatják a kormányzati finanszírozások, a szabályozási keretek és a digitális infrastruktúrába való befektetések. Emellett fokozott önálló mozgást biztosít a fogyatékkal élők és a nem járművezetők számára is. Nagyfokú rugalmasságot és kényelmet kínálnak a pihenéshez, olvasáshoz vagy akár munkavégzéshez utazás közben, ami javítja a személyek hatékonyságát. ²

Tudományos probléma

Azonban ezt a fokú növekedést le kell követnie a biztonsági fejlesztéseknek és szabályozásoknak is egyaránt. Egy önvezető közúti jármű számos olyan technológiából áll, amely képesek kommunikálni egymással egy belső hálózaton, illetve képesek egy külső hálózat esetében adatokat továbbítani, illetve fogadni. Ezen felül a járművek különböző megoldásokkal térképezik fel a környezetet és más-más döntési mechanizmust alkalmaznak. Mind a kommunikáció, mind az egyes rendszerelmek rendelkeznek gyengeségekkel, sérülékenységekkel amelyek kihasználása súlyos következményekkel járnak. Az elterjedésében, fontos a jogi környezet megteremtése is, amely biztosítja ezen járművek

¹ A dolgozatot az Innovációs és Technológiai Minisztérium ÚNKP-21-2-I-NKE-111 kódszámú Új Nemzeti Kiválóság Programjának szakami támogatásával készült

² „Autonomous Vehicle Market Size, Share, Trends, Report 2022-2030”, elérés 2022. április 4., <https://www.precedenceresearch.com/autonomous-vehicle-market>.

tesztelésének és használatának részletszabályait. Továbbá vizsgálandó terület a társadalmi elfogadottsága is ezen technológiáknak, illetve fontos felmérni azokat a félelmeket, amelyek megjelennek a társadalomban az önvezető járművek témakörében.

Módszertan

Kutatásom során megvizsgálom egy state-of-art analízissel, hogy milyen technológiai megoldásokra van szükség az önvezető közúti járművek kialakításához, illetve ezen eszközök és megoldások milyen fenyegetésekkel néznek szembe kiberbiztonsági megközelítésből. Ezen felül jogszabály vizsgálattal térképezem fel azokat a szabályozásokat, amelyekkel az egyes államok biztosítják az önvezető közúti járművek tesztelését és használatát. Illetve a feltérképezem és csoportosítom azokat a szabványokat, amelyeket figyelembe kell venni az autógyártóknak, ha megfelelő minőségű és biztonságos járművet szeretnének gyártani.

Szentiment analízist végezek, melyben megvizsgálom, hogy az interneten a önvezető járművekkel kapcsolatos szavak hol és milyen formában jelennek meg. Kérdőíves felmérést végeztem hazai viszonylatban, amelynek egy részét klaszter elemzéssel vizsgáltam, másik részét pedig Kruskal-Wallis-próba alá vetem, illetve egyváltozós elemzéssel értékeltem ki, hogy megvizsgáljam a társadalmi véleményt az önvezető járművekkel kapcsolatban.

Kutatási hipotézisek

Kutatásom kezdetén az alábbi hipotéziseket fogalmaztam meg:

H1: Az Egyesült államokban magasabb érettséggel rendelkeznek stratégia alkotási és szabályozási területen az autonóm közlekedéssel kapcsolatban mint az Európai Unióban.

H2: Az önvezetés témája az online térben szakmai és hír -oldalakra korlátozódik, nem épült be a közbeszédbe.

H3: Azok a személyek, akik kevésbé tartják élvezetesnek az autonóm vezetést, nagyobb mértékben tartanak a kontroll elvesztésének veszélyétől.

H4: A kitöltők körében az önvezető járművek használat iránti attitűdöt befolyásolják az egyes kiberbiztonsági és adatvédelmi kockázatoktól való félelem.

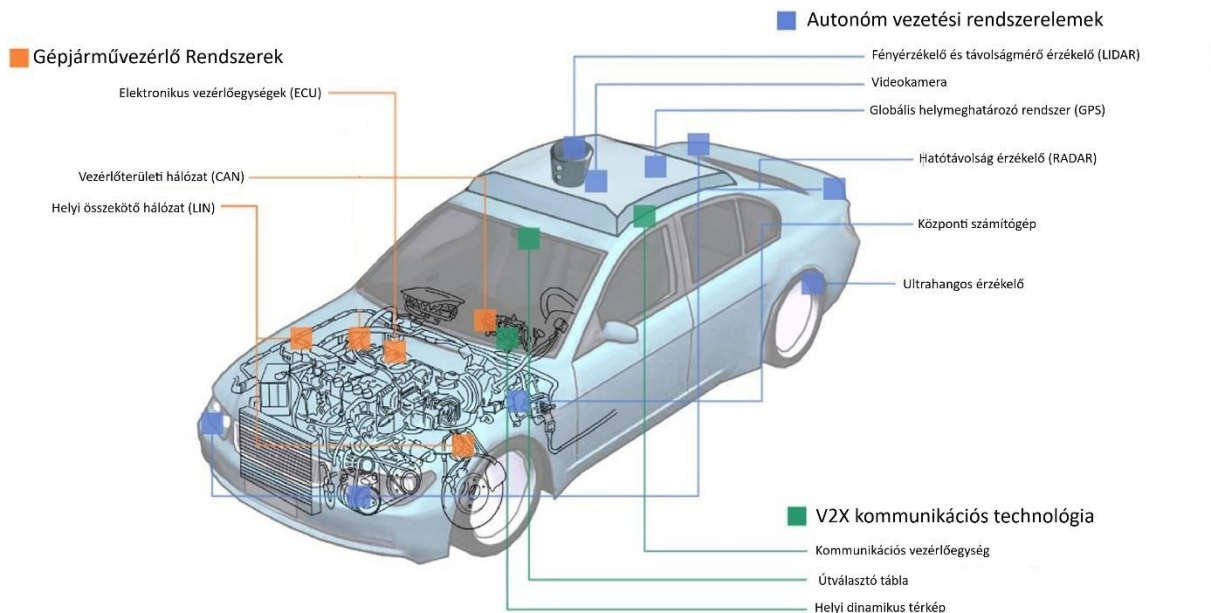
Kutatási célkitűzések

Kutatásom célja egy képet adni az önvezető közúti járművek rendszer felépítéséről, illetve ennek technológiai háttéréről, és kiberbiztonsági kihívásairól. További elemzés során egy képet alakítok ki azon meglévő szabványokról, amelyek biztosíthatják az önvezető járművek egyes területének biztonságát, illetve hatékonyságát. További célom képet adni ezen terület jelenlegi szabályozásáról az Egyesült Államok és Európai Unió tekintetében. Ezen felül az

autonóm vezetéssel kapcsolatos társadalmi elfogadást is vizsgálom hazai tekintetben, illetve azt hogy az adott kitöltők mennyire tartanak az egyes kiberbiztonsági kihívásoktól ezen technológiával kapcsolatban. A szakirodalom feldolgozás közben azt az észrevételt tettem, hogy tudományos cikkek nem nagyon foglalkoznak ilyen átfogóan a témával, aminek a fő oka a terjedelmi korlát lehet. Jelen kutatásom terjedelmi korlátja megfelelő méretűnek bizonyosult arra, hogy egy átfogó képet biztosítson az önvezető közúti járművek vizsgálatához.

1 Autonóm közúti közlekedési eszközök felépítése

Ez a rendszer leírás fontos részét képezi dolgozatomnak, mivel egy átfogó keretet biztosít azon kutatásokról és megoldásokról, amelyek alapján ki lehet indulni egy biztonságos önvezető rendszer kialakítása felé. Azonban ezen pályamunka terjedelmi korlátai miatt az egyes rendszerelemek igen részletes bemutatását nem tudom véghez vinni. Ma már számos kutatás különböző mélységekben, különböző struktúrában vizsgálja ezt a téma területet, jelen kutatásban 1. számú ábrán látható felosztás került alkalmazásra, amely alapján elindultam a kutatásomban. Azonban látható lesz az a későbbi felosztásokban, hogy ezek a rendszerek nem szeparálhatóak el egymástól teljesen, hiszen például egy GNSS technológia elősegíti az önvezetést mint képességet, illetve a kommunikációt is, hiszen képes a helyzetét kommunikálni a környezetével.



1. ábra Az önvezető közúti jármű rendszerelemei (saját szerkesztés, forrás: Kyounggon Kim és mtsai.)

1.1 Autonóm vezetés definiálása

Ahhoz, hogy megvizsgáljuk az autonóm közlekedési eszközök egyes aspektusait, fontos tisztázni, hogy mit is értünk autonóm jármű alatt. Fontos hangsúlyozni, hogy az önvezetés fogalma jelen kutatásban műszaki kontextusban kerül felhasználásra.

Ehhez számos definíciót találunk a legáltalánosabbtól kezdve a komplexebb terminológiai rendszerig ebben a témában. Kichun Jo és szerzőtársai például a következő meghatározással éltek: „Az autonóm jármű olyan közlekedési eszköz, amely emberi beavatkozás nélkül képes

vezetni magát.”³ Tehát az autonóm rendszer olyan műszaki egység, amely bizonyos feladatokat ellát anélkül, hogy bármilyen emberi parancsoktól függene. Azonban, hogy mind műszaki, mind jogi értelemben részletesen tudjuk vizsgálni az önvezető járműveket, pontosabb definícióra lesz szükség. Ehhez szükséges lesz egy olyan definíciós rendszerre, amely kategorikus különbségeket tesz az automatizálás különböző módjai (szintjei) között. Ehhez az autóiipari mérnökök globális szövetsége, a SAE International jelentését használtam fel, amely címe „A közúti gépjárművek vezetési automatizálási rendszereivel kapcsolatos kifejezések taxonómiája és meghatározása” (J3016™ szabványként is ismert).⁴

A jelentés a vezetési automatizálás hat szintjét határozza meg az automatizálás nélkülítől a teljes automatizálásig. A 1. számú táblázat mutatja be a szabvány által használt egyes szinteket. A vastagított fekete vonal jelöli az önvezető képességek mértéket az egyes szinteken.

1. táblázat Automatizálás szintjének meghatározása (saját szerkesztés, forrás: „J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, <https://www.sae.org>)

SAE szint	Megnevezés	Meghatározás	A kormányzás és a gyorsítás/lassítás végrehajtása	A vezetési környezet monitorozása	Dinamikus vezetési feladatok esetén beavatkozási kérelem kezelője	Rendszerképesség (érintett vezetési módok)
0	Nincs automatizálás	Teljesen a sofőr kontrollálja a vezetés összes aspektusát.	Vezető	Vezető	Vezető	n/a
1	Vezetői segítség	A vezetőtámogató rendszer megvalósítás vezetői üzemmód-specifikusan a kormányzás és a gyorsítás/lassítás vezetési környezetre vonatkozó információk alapján azzal a kitéttel, hogy a vezető elvégzi az összes dinamikus vezetéshez fűződő feladatot.	Vezető és rendszer	Vezető	Vezető	Néhány vezetési mód
2	Részleges automatizálás	A vezetőtámogató rendszer megvalósítás egy vagy több vezetőtámogató rendszer által, amely végrehajtja mind a kormányzást mind a gyorsítást/lassítást vezetési környezetre vonatkozó információk alapján azzal a kitéttel, hogy a vezető elvégzi az összes dinamikus vezetéshez fűződő fennmaradt feladatot.	Rendszer	Vezető	Vezető	Néhány vezetési mód
3	Feltételes automatizálás	Az automatizált vezetési rendszer vezetői üzemmód-specifikus megvalósítása a	Rendszer	Rendszer	Vezető	Néhány vezetési mód

³ Kichun Jo, Chansoo Kim, és Myoung-ho Sunwoo, „Simultaneous Localization and Map Change Update for the High Definition Map-Based Autonomous Driving Car”, *Sensors* 18, sz. 9 (2018. szeptember): 3145, <https://doi.org/10.3390/s18093145>.

⁴ „J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International” (SAE International, 2021. április), 3, https://www.sae.org/standards/content/j3016_202104.

SAE szint	Megnevezés	Meghatározás	A kormányzás és a gyorsítás/lassítás végrehajtása	A vezetési környezet monitorozása	Dinamikus vezetési feladatok esetén beavatkozási kérelem kezelője	Rendszerképesség (érintett vezetési módok)
		dinamikus vezetési feladatok minden aspektusában, azzal a kitéttel, hogy a vezető megfelelően reagál a beavatkozási kérésre.				
4	Magas automatizálás	Az automatizált vezetési rendszer vezetői üzemmód-specifikus megvalósítása a dinamikus vezetési feladatok minden aspektusában, még akkor is, ha a vezető nem reagál megfelelően egy beavatkozási kérésre.	Rendszer	Rendszer	Rendszer	Néhány vezetési mód
5	Teljes automatizálás	Az automatizált vezetési rendszer vezetői üzemmód-specifikus megvalósítása a dinamikus vezetési feladatok minden aspektusában, minden út- és környezeti körülmény között, amelyet a vezető kezelhetne.	Rendszer	Rendszer	Rendszer	Összes vezetési mód

A kulcsfontosságú különbség a 2. szint és a 3. szint között az, hogy míg a 2. szinten a vezető hajtja végre a dinamikus vezetési feladat egy részét, addig 3. szinten az automatizált vezetési rendszer látja el a teljes dinamikus vezetési feladatot. Azonban fontos definiálnunk a „dinamikus vezetési feladat” fogalmát, amely magában foglalja a vezetési feladat operatív részét (például: kormányzás, fékezés, gyorsítás, jármű és úttest figyelése) és taktikai részét (például: eseményekre való reagálás, sávváltás, kanyarodás, jelzések használata stb.), de nem tartozik bele a vezetési feladat stratégiai aspektusa (például utazás tervezés).⁵

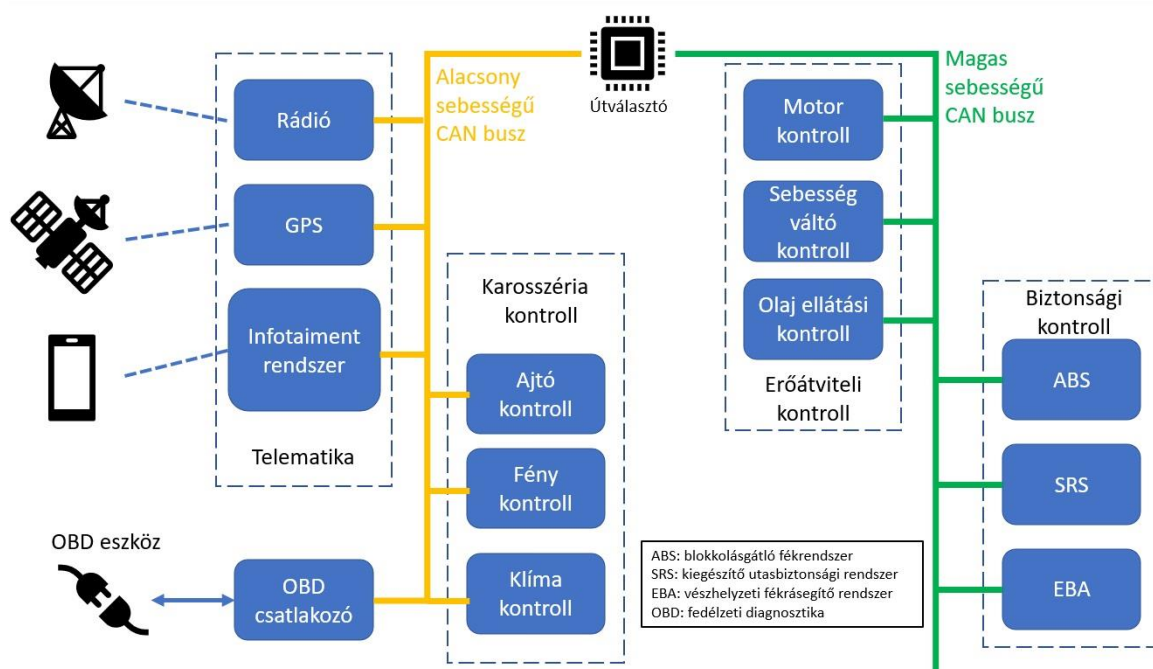
Kijelenthetjük tehát, hogy az autonómia szintjének meghatározása igen is fontos elem, amikor az önvezető járműveket vizsgáljuk. Az egyes rendszerelemek megvizsgálásakor törekedtem a teljesen automatizált járműkategória feltérképezésére, mivel ezen vizsgálat tartalmazza az alacsonyabb szintek tulajdonságait is egyaránt.

1.2 Gépjárművezérlő rendszerek

Az egyik legfontosabb egység ebben a kategóriában az elektronikus vezérlőegység (Electronic Control Units, továbbiakban ECU). A ECU vezérli például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zár, a légzsák, a légkondicionáló rendszer és a fényvezérlés moduljait. Jellemzően a kis- és közepes méretű járművek körülbelül 50 ECU-t tartalmaznak és legalább 70-et foglalnak magukban a luxusautók. Egyes csúcskategóriás

⁵ „J3016C”, 3.

járművek akár 80 ECU-val is rendelkeznek. A járműben lévő hálózat összeköti az ECU-kat és továbbítja az adatokat közöttük. Ez a hálózat magában foglalja többek között a vezérlőterületi hálózatot (Controller Area Network, továbbiakban CAN), helyi összekötő hálózatot (Local Interconnect Network, LIN), ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárahhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak. A FlexRay egy új generációs busz-technológia, amely nagy sebességű és hibatűrő kommunikációt biztosít.⁶ Jelen vizsgálatban a CAN hálózat felépítésére és sebezhetőségeire fókuszál, mivel ez a hálózat a legelterjedtebb az autóiparban. Az 2. számú ábra mutatja be egy autó belső hálózatát, amely CAN busz hálózatot használ. Jól látható, hogy ezen busz rendszernek kettő típusa van. Az alacsony sebességű CAN hálózat főleg telematikai és karosszéria kontroll egységeiért felel, míg a magas sebességű rendszer főleg a jármű konkrét vezérlésért felel. Itt található meg az erőátvitelért felelős ECU-k mint például a sebességváltó kontrollja, vagy a motor kontrollja.⁷



2. ábra A CAN hálózat felépítése (saját szerkesztés, forrás: Jiajia Liu és mtsai.)

Ebbe a CAN hálózatba kapcsolt ECU-k az üzeneteket CAN keretbe küldik meg egymásnak. A CAN keret felépítése az 2. számú táblázatban látható.

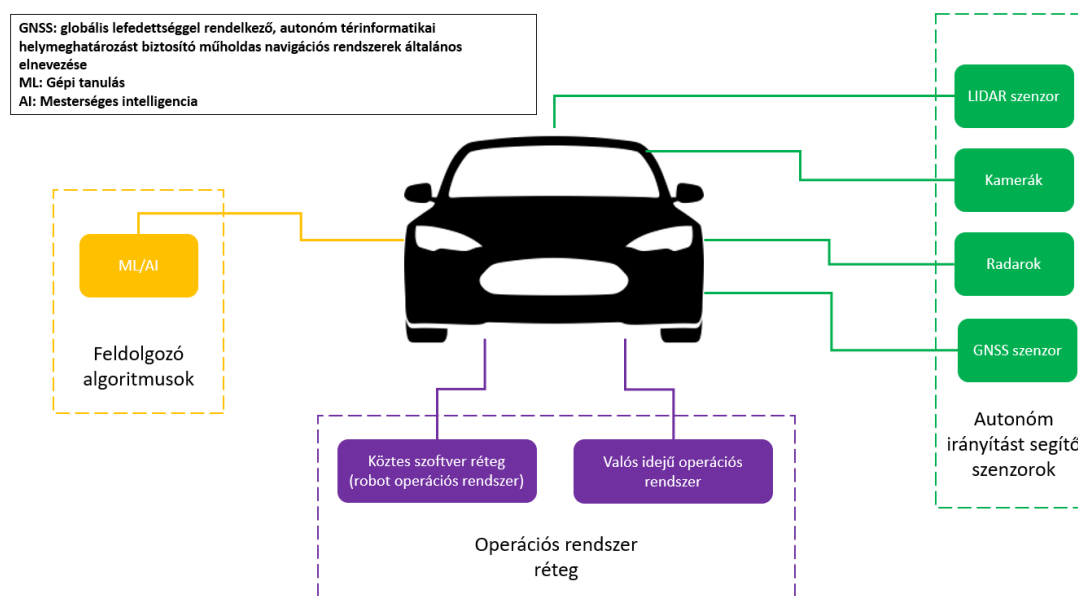
⁶ Kyounggon Kim és mtsai., „Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense”, *Computers & Security* 103 (2021. április 1.): 102150, <https://doi.org/10.1016/j.cose.2020.102150>.

⁷ Jiajia Liu és mtsai., „In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions”, *IEEE Network* 31, sz. 5 (2017): 50–58, <https://doi.org/10.1109/MNET.2017.1600257>.

2. táblázat A CAN keret felépítése (saját szerkesztés, forrás: <https://www.kvaser.com/can-protocol-tutorial/##canMessages>)

CAN keret részének megnevezése	Funkciója
Start of Frame	A keret kezdetét jelzi
Identifier Field	Azonosító mező többnyire az adatmező tartalmát azonosítja. Az RTR bittel együtt meghatározza a keret prioritását is.
RTR (Remote Transmit Request)	Távoli átviteli kérelem
Control Field	Az adatmező hosszát adja meg
Data field	A tartalma tetszőleges
CRC (cyclic redundancy check) field	A ciklikus redundancia-ellenőrzés az üzenet hibamentes célba juttatását segíti.
ACK (Acknowledge)	Az elfogadó bit a CRC mező végéig van és ezt a bit-et a vevő felülírja ezzel tudatja a küldővel, hogy a küldés sikeres.
End of Frame	Ez a szakasz jelenti az üzenet végét.

1.3 Autonóm vezetési rendszerelemek



3. ábra Az önvezetést biztosító rendszerelemek (saját szerkesztés)

1.3.1 Autonóm irányítást segítő szenzorok

Az önvezető járművek különböző érzékelőkre támaszkodnak a valós idejű helymeghatározás és a környezet érzékelése érdekében. A LiDAR, a kamera, a radar és a GNSS a legfontosabb érzékelők, amelyeket a különböző autonóm vezetési rendszerek használnak. Az ezekből az érzékelőkből gyűjtött adatokat a rendszer legtöbbször a gépi tanulás technológiáját alkalmazva átalakítja és feldolgozza. Ezen érzékelőknek különböző feladata van távolság érzékelés szerint:

- 1. Közeli érzékelés (0-5 m): az ultrahangos érzékelők olyan közelségérzékelők, amelyek célja az akadályok érzékelése a karosszériától néhány méteren belül. Elsősorban alacsony sebességű forgatókönyvekhez, pl. parkolássegítéshez tervezték őket.
- 2. Kis hatótávolságú érzékelés (5-30 m): az előre néző kamerákat a sávelhagyásra figyelmeztető, a jelzőtáblák felismerésére, a hátrafelé néző kamerákat pedig a parkolássegítésre használják.
- 3. Közepes hatótávolságú érzékelés (80-160 m): a LiDAR és a közepes hatótávolságú radarok (Mediumrange radars MRR) az ütközésselkerülést és a gyalogosok felismerését biztosítja.
- 4. Nagy hatótávolságú érzékelő (160-250 m): A nagy hatótávolságú radarok (Long-range radars LRR) adaptív sebességtartó automatika számára tervezték nagy sebességnél.⁸

Ezeket az az autonóm vezetést elősegítő érzékelőket a következő módon definiálhatjuk:

- A globális navigációs műholdrendszer (Global Navigation Satellite System továbbiakban GNSS) egy műholdalapú helymeghatározó, navigációs és időmérő (Navigation and Timing továbbiakban PNT) rendszer. Jelenleg számos GNSS van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által vezetett globális helymeghatározó rendszer (Global Positioning System továbbiakban: GPS) vitathatatlanul a legismertebb. Mindazonáltal az európai vezetésű GALILEO, az orosz vezetésű GLONASS, a

⁸ Chen Yan, Wenyuan Xu, és Jianhao Liu, „Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle”, *Def Con* 24, sz. 8 (2016): 109.

kínai BeiDou, az India által vezetett IRSS és a japán QZSS mellett áll.⁹ Kollektív keretrendszerként a GNSS globálisan meghatározó és költséghatékony kültéri PNT technológiává vált. Az egyes GNSS technológiák alkalmazása elengedhetetlen egy önvezető jármű esetében, a pontos helymeghatározás érdekében. Illetve az intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges ezen szenzorok alkalmazása.

- Több érzékelő, például a fényérzékelő és távolságmérő szenzor (Light Detection and Ranging továbbiakban LiDAR), a kamerák és a RADAR, ultrahang csatlakozik a döntéshozó mikrokontrollerhez különféle interfészekon, például Etherneten, CAN hálózaton keresztül. A LiDAR szenzor nyers bemenetét 3D pontfelhőnek nevezzük, amelynek dimenziója $n \times 4$, ahol n az adatpontok számát jelöli, és minden adatpont 4 dimenziós amely áll egy 3D vektorból, w_x , w_y és w_z , kordinátákkal valamint a pont intenzitásából. Ezen adatokat dolgozza fel a rendszer és detektálja az akadályokat.¹⁰
- A kamerákat széles körben alkalmazzák az önvezető járművekben. Az autonóm és félautonóm járművek (SAE 2-es és magasabb szint) több pozícióban elhelyezett kamerákra támaszkodnak, hogy 360 fokos képet kapjanak a jármű körül. A kamerák olyan fontos autonóm feladatokhoz nyújtanak információkat, mint például a közlekedési táblák felismerése és a sávfelismerés.¹¹ A kamerák a LiDAR helyettesítésére is használhatók tárgyészlelési feladatokhoz és alacsonyabb költségű távolságmérésekhez, de bizonyos helyzetekben, például esőben, ködben vagy hóban gyenge teljesítményt nyújtanak. A LiDAR-ral és a radarokkal együtt a kamerák bőséges és változatos adatokat szolgáltatnak az autonóm vezetéshez.
- Radar olyan érzékelő, amely elektromágneses hullámokat bocsájt ki a rádió vagy mikrohullámú tartományban, hogy észleljék a tárgyakat, és mérjék távolságukat és sebességüket a visszavert jelek érzékelésével. Az önvezető járművek esetében a radarok számos alkalmazásban hasznosak. Például a kis hatótávolságú radarok lehetővé teszik a parkolás elősegítését. A nagy

⁹ Atanu Santra és mtsai., „Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region”, *Advances in Space Research* 63, sz. 9 (2019): 2995–3008.

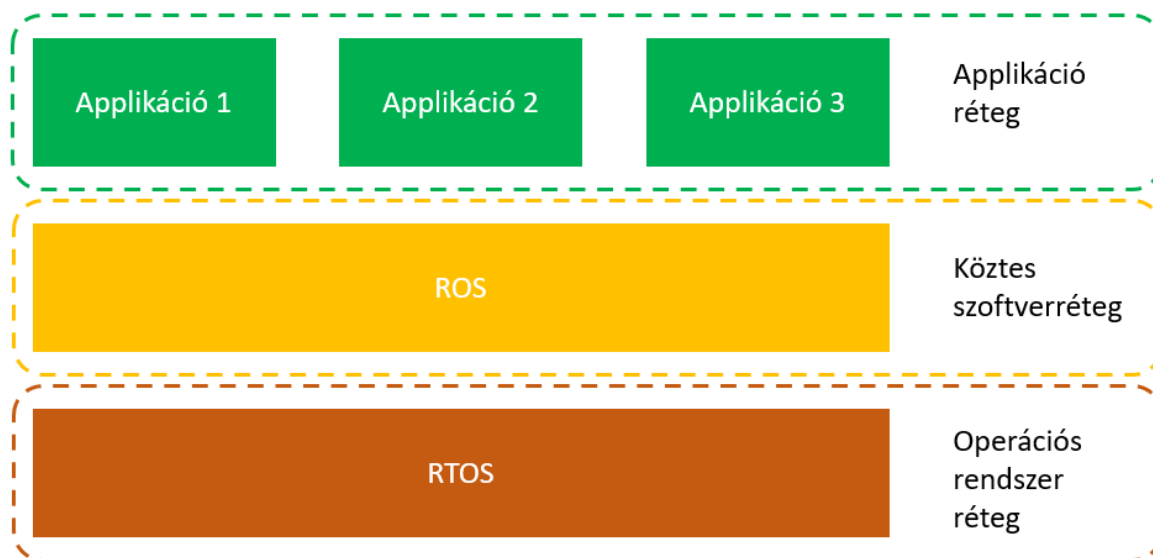
¹⁰ Yulong Cao és mtsai., „Adversarial sensor attack on lidar-based perception in autonomous driving”, in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, 2267–81.

¹¹ Aharon Bar Hillel és mtsai., „Recent Progress in Road and Lane Detection: A Survey”, *Machine Vision and Applications* 25, sz. 3 (2014. április 1.): 727–45, <https://doi.org/10.1007/s00138-011-0404-2>.

hatótávolságú radarok segítik az automatikus távolságszabályozást és fékrásegítést.¹²

1.3.2 Operációs rendszerréteg

Itt két fő típusról beszélhetünk az autonóm járművek esetében. Az egyik amely az önvezető funkciók összehangolásáért és működéséért felel, ebben megtalálható a valós idejű operációs



4. ábra Az operációs rendszerréteg bemutatása (saját szerkesztés, forrás: Takuya Azumi, Yuya Maruyama, és Shinpei Kato)

rendszer (Real-Time Operating System továbbiakban RTOS), illetve a másik amire szükségünk van az RTOS mellett egy köztes szoftverréteg, amely összekapcsolja a különböző autonóm vezetési szolgáltatásokat. Ezt a legtöbb létező autonóm vezetési megoldás a robot operációs rendszer (Robot Operating System továbbiakban ROS) segítségével éri el.

Az RTOS operációs rendszerben van egy ütemező nevű modul, amely ütemezi a különböző feladatokat, és meghatározza, hogy egy folyamat mikor fusson le a processzoron, és így érhető el, hogy az egyes feladatok akár egyszerre is lefussanak. Két típusa van a kemény és a puha RTOS. A kettő közötti különbség, hogy a kemény rendszer esetében határidők meghatározásra kerülnek, és azt az adott időkereten belül kell végrehajtani, különben a késlekedés katasztrofális következményekkel járhat például légzsákrendszer esetében. A puha esetben a rendszer válaszüzeje elsődleges, de nem kritikus a rendszer működése szempontjából, tehát a határidő fontos, de a rendszer elfogadja a határidők esetenkénti elmulasztását is.

A ROS egy kommunikációért felelős köztes szoftver, amely megkönnyíti az autonóm járműrendszer különböző részei közötti kommunikációt. Például a képrögzítő szolgáltatás

¹² Yan, Xu, és Liu, „Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle”.

üzeneteket tesz közzé a ROS-on keresztül, és mind a lokalizációs szolgáltatás, mind az akadályérzékelő szolgáltatás lekéri a közzétett képeket, hogy helyzet- és akadályfrissítéseket generáljon.¹³

1.3.3 Feldolgozó algoritmusok

Az automatizált vezetési rendszerek gyors fejlődésével a biztonságos vezetési környezethez elengedhetetlen a stabil és megbízható környezetelemzés. A feldolgozó algoritmusok olyan megoldások, amely az egyes autonóm közlekedést segítő szenzorok adatait dolgozzák fel, és például kameraalapú útszegmentálásnak mára már számos megoldás létezik. Ez a feldolgozás a 4. számú ábrán az applikáció rétegen megy végbe. Ezen feldolgozást elősegíti a járművekbe implementált gépi tanulás is. A mélytanuláson alapuló képszemantikai szegmentálás az egyik legjobb megoldás, mivel kellően nagy kiterjedésű és bonyolult környezeteket képes kielemezni. A rögzített képet több régióra tagolja, és minden egyes pixel osztályát (objektumát) felismeri, így pixelszintű osztályozásnak tekinthető. A képosztályozástól eltérően a képszemantikai szegmentálás azonosítja a képeken található objektumosztályokat, és megtalálja a képeken található objektumok helyét is. Ezenkívül pontos objektumhatár-információkat szolgáltat.¹⁴ Az egyik ilyen technológiai megoldás a konvolúciós neurális hálózat (Convolutional Neural Networks továbbiakban CNN), amelyet már alkalmaznak számos jármű modellnél.

1.4 Külső kommunikációt támogató rendszerelemek

A külső kommunikációt részlegesen érintettem a szenzorok esetében, amikor például a GNSS szenzort vizsgáltam, illetve a CAN rendszernél a további műholdas kommunikáció is érintve volt. Azonban ezt a részt azért terveztem külön fejezetben tárgyalni, mert igen fontos annak a vizsgálata, hogy egy ilyen önvezető jármű, pontosan mivel kapcsolódik még, és ezt milyen céllal teszi. Itt egy új rendszer fogalmát is tisztázni kell, ami nem más mint az Intelligens Közlekedési Rendszer (Intelligent Transport System továbbiakban ITS), amely az összekapcsolt járművek rendszere. Ahol a járművekbe épített érzékelők és egy központi közlekedés irányítási rendszer adatai alapján a jármű képes az intelligens döntés hozatalra.¹⁵

¹³ Takuya Azumi, Yuya Maruyama, és Shinpei Kato, „ROS-lite: ROS Framework for NoC-Based Embedded Many-Core Platform”, in *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2020, 4375–82, <https://doi.org/10.1109/IROS45743.2020.9340977>.

¹⁴ Ping-Rong Chen és mtsai., „DSNet: An Efficient CNN for Road Scene Segmentation”, *APSIPA Transactions on Signal and Information Processing* 9 (2020. ed), <https://doi.org/10.1017/ATSIP.2020.25>.

¹⁵ Meiyuan Zhao, Jesse Walker, és Chieh-Chih Wang, „Security challenges for the intelligent transportation system”, 2012. 0 17., 107–15, <https://doi.org/10.1145/2490428.2490444>.

Ez a rendszer azért is hangsúlyos mert ezáltal a járműveknek nem csak a saját adataikra kell támaszkodniuk, hanem egy központi rendszer tud adatot szolgáltatni, olyan információkról, amelyeket a szenzorok a távolsági vagy akadályi korlátok miatt nem képesek érzékelni.

Az ITS keretében a kritikus vezetési információk megosztása a jármű ad hoc hálózatán (vehicular ad hoc network továbbiakban VANET) megy végbe. Ez a VANET 3 fő kommunikációs típust különböztet meg:

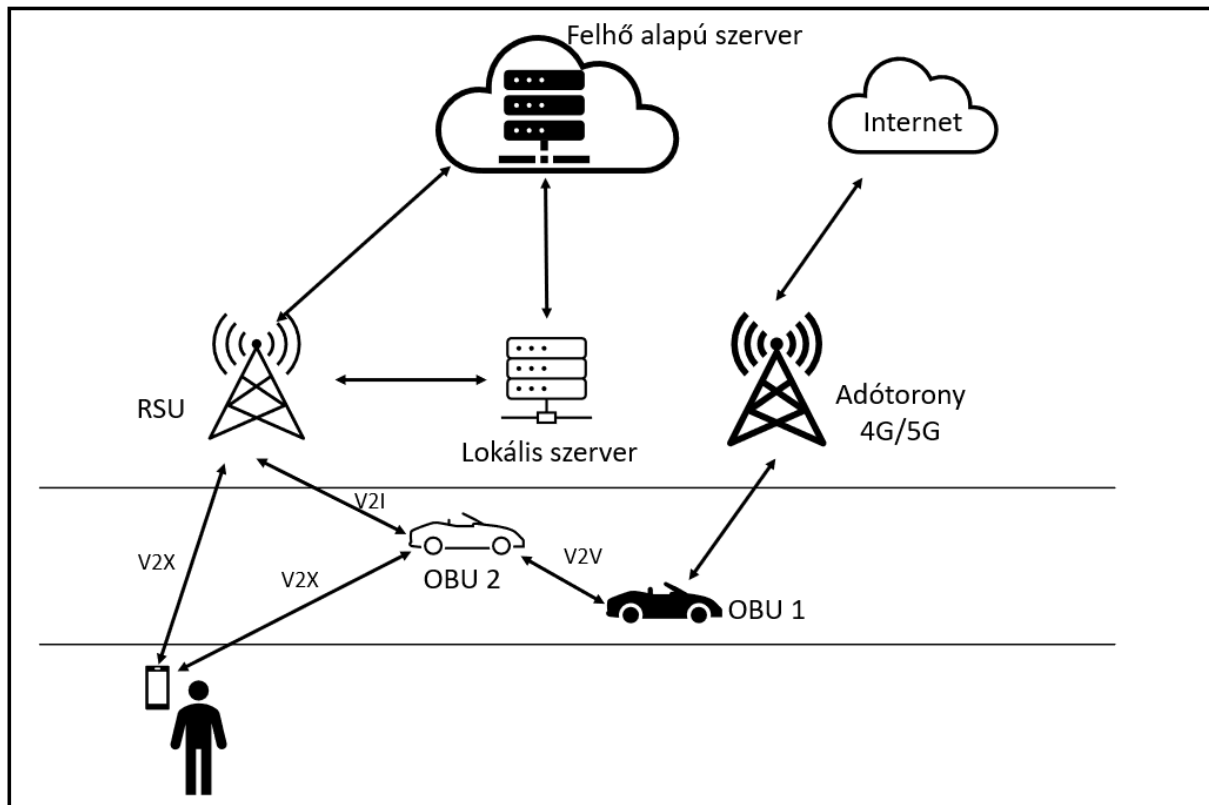
- V2V (vehicle-to-vehicle) kommunikáció, ami a járművek egymással való kommunikációja;
- V2I (vehicle-to-infrastructure) kommunikáció, ami a járművek és a környező infrastruktúra kommunikációja;
- V2X (Vehicle-to-everything) kommunikáció, amely a legágabb csoport, ami magában foglalja az előző kettő területet, és tovább bővíti, olyan eszközökkel, amelyek képesek a kommunikációra, illetve helyzetmeghatározásra, ilyen például a gyalogosok okostelefonja.¹⁶

Fontos az ITS-ben résztvevő elemeket is azonosítani, amelyek kommunikálnak egymással. Ezek a következő elemek:

- fedélzeti egység (on-board unit továbbiakban OBU), amely a járművekbe szerelt adó vevő;
- útmenti egység (road-side unit továbbiakban RSU), amely olyan adó vevő, ami az út mentén biztosítja a kommunikációt a közlekedési központ és a járművek között;
- digitális cellás távközlési állomások, amelyek biztosítják például a 4G és 5G kommunikációt;

¹⁶ Ahmad Mostafa és mtsai., „A V2X-based approach for reduction of delay propagation in vehicular Ad-Hoc networks”, in *2011 11th International Conference on ITS Telecommunications*, 2011, 756–61, <https://doi.org/10.1109/ITST.2011.6060155>.

- felhő alapú számítási réteg az, amely kezelheti a földi szervereken kívül a ITS adatokat.¹⁷¹⁸



5. ábra Intelligens Közlekedési Rendszer lehetséges felépítése (saját szerkesztés, forrás: Mohammed Saeed Al-kahtani 2012; Mohammad Syfullah és Joanne Mun-Yee Lim 2017)

A VANET 3 fő kommunikációs szabványt használ, amely dedikáltan a járművek kommunikációjára kerültek kialakításra.

- Dedikált rövid távú kommunikáció (Dedicated Short Range Communications továbbiakban DSRC) 75 MHz-es sáv szélességű spektrumban található 5850-5925 GHz között. Ezt az amerikai Szövetségi Kommunikációs Bizottság (Federal Communication Commission FCC) jelölte ki a jármű kommunikáció számára. A DSRC sáv 7 dedikált csatornára lett felosztva.¹⁹

¹⁷ Mohammed Saeed Al-kahtani, „Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”, in *2012 6th International Conference on Signal Processing and Communication Systems*, 2012, 1–9, <https://doi.org/10.1109/ICSPCS.2012.6507953>.

¹⁸ Mohammad Syfullah és Joanne Mun-Yee Lim, „Data broadcasting on Cloud-VANET for IEEE 802.11p and LTE hybrid VANET architectures”, in *2017 3rd International Conference on Computational Intelligence Communication Technology (CICT)*, 2017, 1–6, <https://doi.org/10.1109/CICT.2017.7977321>.

¹⁹ Mohamed Nidhal Mejri, Jalel Ben-Othman, és Mohamed Hamdi, „Survey on VANET Security Challenges and Possible Cryptographic Solutions”, *Vehicular Communications* 1, sz. 2 (2014. április 1.): 53–66, <https://doi.org/10.1016/j.vehcom.2014.05.001>.

- A Villamos és Elektronikai Mérnöki Intézet (Institute of Electrical and Electronics Engineers továbbiakban IEE) által kiadott 1609 szabványcsalád a vezeték nélküli hozzáféréshez járműkörnyezetben (Wireless Access in Vehicular Environments továbbiakban WAVE) szabványok olyan architektúrát és szabványosított szolgáltatásokat és interfészeket határoznak meg, amelyek lehetővé teszik a biztonságos VANET kommunikációt.²⁰
- Az IEEE 802.11 eszközök olyan környezetben használhatók, ahol a fizikai réteg tulajdonságai gyorsan változnak, és ahol nagyon rövid ideig tartó kommunikációs adatcserére van szükség. A 802.11p meghatározza a VANET-ek fizikai és köztes hozzáférési rétegét.²¹

1.5 Következtetések

Látható a kialakított és bemutatott csoportosításban átfedések. Ez azért lehetséges, mert ezen eszközök egymást segítik. A gépjárművezérlő elemek esetében kijelenthető, hogy ez ECU-k száma nagyban eltérhet gyártónként, illetve modellenként. Azonban azonosítani lehet ezen ECU-k csoportjait és, hogy ezek a csoportok mely CAN hálózat típust használják. Ezen felül sikerült azonosítani azon rendszerelmeket, amelyek az önvezetést elősegítik. Ezek a rendszer elemek száma és típusa is igen eltérhet gyártók és típusok szerint. Végezetül bemutatásra kerültek azon megoldások, amelyek a külső kommunikációt erősítik. Itt azonosításra került egy igen fontos kifejezés is, ami az intelligens közlekedési rendszer, amely biztosítani tudja az önvezető járművek döntéshozatalát adatokkal, illetve utasításokkal. Ki kell emelnem, hogy ez a rendszerbe kapcsolás számos környezeti felmérési adatot tud szolgáltatni, amely elengedhetetlen a biztonságos közlekedés megteremtéséhez és fenntartásához.

²⁰ Mejri, Ben-Othman, és Hamdi.

²¹ „IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments”, *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, 2010. július, 1–51, <https://doi.org/10.1109/IEEESTD.2010.5514475>.

2 Önvezető közúti járművek kiberbiztonsági kihívásai és megoldásai

Azonosításra és csoportosításra kerültek azok a rendszerelemek, amelyek megjelennek egy autonóm közúti jármű esetében. Ezek a rendszerelemek számos kiberbiztonsági kockázatot hordoznak magukban. Egy adott kockázat hatásának mértéke számos értéket felvehet, hiszen ha már sikerült egy elektronikus vezérlő egységet feltörnie a támadónak, akkor része tud lenni a belső hálózatnak, ahol információkat gyűjthet, illetve módosíthat, ezzel befolyásolva egy teljesen más rendszerelem működését.

2.1 Gépjárművezérlő rendszerek kiberbiztonsági fenyegetései

Mint, ahogy az 2. számú táblázatból is látható, a CAN keret nem tartalmaz sem hitelesítési sem titkosítási funkciót, és ez számos fenyegetést eredményez. Látható az esettanulmányokból és kutatásokból, hogy az ECU-k estében kevés fenyegetés detektálható, a támadók inkább a CAN rendszereket célozzák meg. Ezen fenyegetések a következő pontokba kerültek kigyűjtésre:

- ECU újraprogramozás: lehetőség van az ECU-k illegális programozására új firmware-rel, így ezen egységet a támadók irányítani tudják majd. Ezen újra programozásra példát főleg a telematikai ECU-k esetében lehet látni. Ilyen támadásra példa Checkoway és szerzőtársai által a Bluetooth kommunikáció használata, amivel a Bluetooth-kapcsolatokért felelős ECU firmware-ét módosították.²²
- A CAN protokoll nem tartalmaz hitelesítési részt, így a vevő egység nem tudja megkülönböztetni az érvényes üzeneteket, a hamisaktól. Így véghezvihető egy kerethamisítás, ezek a hamis keretek hamis adatokat tartalmaznak, amelyekkel félrevezethetik a hiteles ECU-kat.
- Adatszórás (továbbiakban Broadcast) átvitel használata: a CAN-adatcsomagokat a CAN-buszhoz csatlakoztatott összes csomópont sugározza. Minden ECU fogadja a CAN-buszon továbbított csomagokat, és a csomagazonosító megvizsgálása után dönti el, hogy megteszi-e a megfelelő lépéseket. A broadcast tulajdonsága miatt a rosszindulatú rendszerelemek könnyen megismerhetik a többi csomóponttól továbbított összes csomagot.²³
- Rossz protokoll végrehajtás: Egyes esetekben a protokoll megvalósítása nem tükrözi megfelelően a protokollszabványt. Például a szabvány előírja, hogy a motorvezérlő modult (ECM) nem lehet programozási módba kapcsolni, miközben a jármű mozog.

²² S. Checkoway és mtsai., „Comprehensive experimental analyses of automotive attack surfaces”, *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 2011.

²³ Liu és mtsai., „In-Vehicle Network Attacks and Countermeasures”.

Nyilvánvalóan ez biztonsági okokból történt. Egyes megvalósításokban azonban valóban lehetséges olyan parancs elindítása, amely letiltja a CAN kommunikációt és az ECU-t programozási módba állítja annak ellenére, hogy a jármű mozog.²⁴

- CAN protokollokkal való visszaélés: a járműben lévő hálózatok elleni támadások végrehajthatók a jól megválasztott protokollok rosszindulatú használatával. Ezek a protokollok lehetnek érvényesek, amelyeket a támadó a múltban lehallgatott majd vissza játszott. Továbbá a CAN protokoll esetében szolgáltatásmegtagadási (Denial of Service továbbiakban DoS) támadás hajtható végre a busz döntési mechanizmusa segítségével. Mivel a CAN protokollban a csomag azonosító nem csak a célpontot jelzi, hanem a csomag prioritását. Ezen prioritás dönti el, hogy melyik üzenetet kell végrehajtani leghamarabb. Így a legmagasabb prioritású üzenetek küldésével senki más nem fogja tudni használni a buszt.
- Titkosítás hiánya: A CAN-csomagok nincsenek titkosítva. A támadók könnyen elemezhetik a CAN-csomagokat.²⁵

2.2 Gépjárművezérlő rendszerek védelmi eljárásai

A fent azonosított fenyegetések 3 fő sebezhetőségből adódnak: a gyenge hozzáférés-szabályozás, nincs titkosítás; és nincs hitelesítés. A biztonságos járműfedélzeti CAN kiépítéséhez ezt a három sebezhetőséget ki kellene küszöbölni. Azonban a hozzáférés szabályozásának kialakítása ezen rendszerben szinten lehetetlen, mivel az üzenet küldés broadcast kommunikációval történik, azaz mindegyik rendszerelem megkapja az üzenetet, és annak tartalmából azonosítják, hogy az egyes rendszerelem a címzett-e vagy sem. Ezért a kitettségek csökkentése érdekében inkább titkosítási és hitelesítési eljárásokat kell alkalmazni.

A szakirodalmi feldolgozása során számos kutatást vizsgáltam a témában^{26 27 28 29}. Végül Samuel Woo és szerzőtársai³⁰ által kialakított megoldása kerül részletezésre, mivel a

²⁴ Karl Koscher és mtsai., „Experimental Security Analysis of a Modern Automobile”, in *The Ethics of Information Technologies* (Routledge, 2017).

²⁵ Marko Wolf, André Weimerskirch, és Christof Paar, „Security in automotive bus systems”, in *In: Proceedings of the Workshop on Embedded Security in Cars (escar) '04*, 2004.

²⁶ B. Groza és mtsai., „LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks”, *ACM Transactions on Embedded Computing Systems* 16, sz. 3 (2017), <https://doi.org/10.1145/3056506>.

²⁷ George Kornaros és mtsai., „Trustnet: ensuring normal-world and trusted-world can-bus networking”, in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (IEEE, 2019), 1–6.

²⁸ Todd R. Andel és mtsai., „Towards Protection Mechanisms for Secure and Efficient CAN Operation”, in *2019 IEEE International Conference on Consumer Electronics (ICCE)* (IEEE, 2019), 1–6.

megoldásában kitér számos biztonsági alapelvre, amelyet kell biztosítani a megfelelő titkosítás és hitelesítés érdekében. Az általuk kialakított eljárás a következő főbb tulajdonságokkal rendelkezik:

- Az adattitkosítási és hitelesítési technikák biztosítják a valós idejű adatfeldolgozást a járművön belüli CAN-ben.
- Az üzenethitelesítési kódot (Message Authentication Code, továbbiakban MAC) használó módszer figyelembe veszi a CAN-adatkeret korlátozott adatmennyiségét. Ami azt jelenti, hogy a MAC kulcsnak nem szabad túlzottan nagy mérettel rendelkezni, mert ez a CAN busz túlzott terheléséhez vezet. Mivel CAN adatkeret 120 bitből áll, beleértve a 64 bites adatmezőt. Ha az adatmezőt MAC-re használjuk, a CAN-adatkeret átvitelének teljes mennyisége legalább kétszeresére nő.
- A kulcskezelési technikák támogatják a titkosságát és hitelesítését továbbá a külső eszköz és a járműfedélzeti CAN közötti biztonságos kapcsolatot is. Ehhez a szerzők használtak egy hitelesítési és egy titkosítási kulcsot. Ezen kulcsok esetében a biztonságos munkamenetkulcs-frissítéshez két tulajdonságot kell biztosítani:
 - Az előre titkosítást, amikor egy csomópont (pl.: ECU) kilép a hálózathoz, és a távozása után nem ismerhet meg jövőbeli üzeneteket. Illetve a visszamenőleges titkosítást, amikor egy új csomópont (pl.: ECU) csatlakozik a hálózathoz, nem olvashat el korábban továbbított üzenetet.
 - Kulcs frissesség: A titkosítási kulcs és a hitelesítési kulcs, amelyeket a CAN-adatkeretek titkosítására és hitelesítésére használnak a megadott munkamenetben, frissen kell generálni. A kulcs frissességének biztosítása érdekében a kulcsgeneráláshoz használt paramétert folyamatosan változtatni kell egy véletlen szám vagy számláló segítségével. A kulcs frissessége alapvető fontosságú az újrajátszási támadások megelőzéséhez.

Ebben a megoldásban implementálásra kerülnének átjáró ECU, amely nagyobb teljesítménnyel rendelkezne. Itt először is, az átjáró és az általános ECU-k előre megosztják a titkosítási és hitelesítési hosszú távú szimmetrikus kulcsokat. Másodszor, a hosszú távú szimmetrikus kulcsok betöltése biztonságos csatornán keresztül kell történnie. Harmadszor, az ECU-k a CAN üzenetszűrési funkcióját kell használnia, még hozzá úgy, hogy minden ECU

²⁹ Megha Agrawal és mtsai., „CAN-FD-Sec: improving security of CAN-FD protocol”, in *Security and Safety Interplay of Intelligent Software Systems* (Springer, 2018), 77–93.

³⁰ Samuel Woo, Hyo Jin Jo, és Dong Hoon Lee, „A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN”, *IEEE Transactions on Intelligent Transportation Systems* 16, sz. 2 (2015. április): 993–1006, <https://doi.org/10.1109/TITS.2014.2351612>.

regisztrálja a feladó-ECU azonosítóját az ID-táblájában, és minden ECU csak akkor kapja meg a csomagot, ha a feladó-ECU azonosítóját megtalálta az ID-táblájában. A többi csomag esetében szűrést kell végezni. Negyedszer, a feladó és a vevő ECU-k egy számlálóval szinkronizálják az adatkereteket. Amikor egy adatkeret teljesen átkerül a vevőhöz, mindkettő növeli az adatkeretszámlálót. A CAN-ben a küldő és a vevő az ACK bitmező segítségével kölcsönösen ellenőrzi a CAN adatkeret átviteli állapotát. Ezért a küldő és a vevő között lehetséges az adatkeretszámláló kezelése és szinkronizálása. Ötödször, az átjáró ECU-nak nagyobb számítási teljesítménnyel kell rendelkeznie, mint egy általános ECU-nak. Hatodszor, az átjáró ECU-ra és a külső eszközökre egy készüléktanúsítványt töltenek be, amely biztosítja a rosszindulatú hozzáférés megakadályozását.

2.3 Autonóm vezetési rendszerelemek kiberbiztonsági fenyegetései

Autonóm irányítást segítő szenzorok kiberbiztonsági kihívásai:

- LiDAR-hamisítás: a támadók hamis jeleket hoznak létre, amelyek egy tárgyat ábrázolnak, és a hamis jeleket egy LiDAR-érzékelőbe juttatják³¹
- Radar jelhamisítás: a támadók a rádió frekvenciás jeleket rögzítik és újra küldik a ezen radarjeleket, hogy torzított adatokat juttassanak el az érzékelőkhöz. Ennek a támadási modellnek a végrehajtásához gyakori eszköz a digitális rádiófrekvenciás memória (Digital Radio Frequency Memory továbbiakban DRFM), amely egy elektronikus módszer a rádiófrekvenciás és mikrohullámú jelek tárolására nagy sebességű mintavételezés és digitális memória segítségével. A tárolt jelek fázisa ezután módosítható, majd a jeleket újra küldik a radarérzékelő felé. A meghamisított jelek ezután a környező objektumok távolságának helytelen kiszámítását okozhatják³². Azonban a hamis jel küldés nem olyan egyszerű, mert például Chen Yan és szerzőtársai³³ megpróbáltak hamis jeleket küldeni egy Tesla Model S radarérzékelőjébe. A kísérlet nem volt sikeres, mert az érzékelőnek alacsony volt a munkaidő és az üresjárat idő közötti aránya, ami megnehezíti a jelek pontos időintervallumban történő elküldését.
- Radarzavarás: ez a támadás is megvalósítható DRFM használatával de itt a támadók a fázis módosítása helyett a tárolt jelek frekvenciáját és amplitúdóját módosíthatják a

³¹ Cao és mtsai., „Adversarial sensor attack on lidar-based perception in autonomous driving”.

³² S. J. Roome, „Digital Radio Frequency Memory”, *Electronics & Communication Engineering Journal* 2, sz. 4 (1990. augusztus 1.): 147–53, <https://doi.org/10.1049/ecej:19900035>.

³³ Yan, Xu, és Liu, „Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle”.

radarérzékelők felé történő újbóli sugárzás előtt. A meghamisított jelek hatására a radarérzékelők nem észlelik azt az objektumot, amelynél a zavaró eszköz található.³⁴

- GNSS hamisítás: A támadó helytelen, de valósághű GNSS-jeleket sugároz, hogy megtéveszse az önvezető járművek GNSS-vevőit. Ebben a támadási modellben a támadók a műholdak valós jeleivel megegyező jelek sugárzásával kezdenek. Ezután fokozatosan növelik a jelek teljesítményét, és a GNSS-jelek fokozatosan eltérnek a célpont valódi helyétől. A GNSS-vevőkészülékeket gyakran úgy konfigurálják, hogy a legerősebb erősségű jeleket használják ki, ezért, amint a hamisított jel erősebb, mint a legális műholdjel, a GNSS-eszközök a hamisított jel feldolgozása mellett döntenek.³⁵
- GNSS zavarás: Mivel a műholdakról érkező rádiójelek általában gyengék, a zavarás erős jelek kibocsátásával érhető el, amelyek túlterhelik a GNSS-vevőt, így a jogos jeleket nem lehet érzékelni. A GNSS-zavarás kevésbé veszélyes, mint a GNSS-hamisítás abban az értelemben, hogy a támadóknak nagyobb kontrolljuk van a GNSS-vevők felett a hamisítási támadással. A GNSS-zavaró támadások azonban fennakadásokat okozhatnak a szolgáltatásban, és lényegében ez egy túlterheléses támadás.³⁶
- Kamera vakítás: Az autonóm járműveken a kamerák általában bemeneti adatokat szolgáltatnak a feldolgozó szoftverek számára az objektumok detektálása érdekében. A támadók célja ennek a funkciónak az ellehetetlenítése úgy hogy a kamerát fénnnyel elvakítják.³⁷

Operációs rendszer réteg:

A RTOS típusa lehet Linux, QNX és Windows Embedded Automotive operációs rendszer, amelyek felépítése hasonlít a tradicionális rendszerekére. Így ha megvizsgáljuk a tipikus operációs rendszerek támadásai vektorait elmondható, hogy a zsarolóvírusoktól a kriptó bányászásig számos fenyegetés azonosítható az RTOS esetében is.³⁸ A támadók a ROS-csomópontokat és/vagy ROS-üzeneteket veszik célba. A ROS futtatási környezetében nincs hitelesítési eljárás az üzenetek továbbítására és új csomópontok létrehozására. Ezen felül a

³⁴ Yan, Xu, és Liu.

³⁵ Sashank Narain, Aanjan Ranganathan, és Guevara Noubir, „Security of GPS/INS Based On-road Location Tracking Systems”, in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, 587–601, <https://doi.org/10.1109/SP.2019.00068>.

³⁶ Ashish Nanda és mtsai., „Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions”, *IEEE Wireless Communications* 26, sz. 4 (2019): 60–65, <https://doi.org/10.1109/MWC.2019.1800503>.

³⁷ Sharath H és Asadullah Ansari, „Autonomous Vehicles Camera Blinding Attack Detection Using Sequence Modelling and Predictive Analytics”, 2020, <https://doi.org/10.4271/2020-01-0719>.

³⁸ „Connected and Autonomous Vehicle Cybersecurity Threats - QA Consultants”, elérés 2022. március 29., <https://qaconsultants.com/blog/connected-and-autonomous-vehicle-cybersecurity-threats/>.

kommunikációban nem történik külön titkosítás. Ebből a hiányosságokból számos fenyegetés ered:

- ROS csomópont készítés vagy eltérítés esetén a támadók a fő csomópont IP-címeit és portjait használják arra, hogy további hitelesítés nélkül új ROS-csomópontot hozzanak létre vagy eltérítsenek egy meglévőt;
- A hitelesítés és titkosítás hiánya miatt az új vagy kompromittált csomópont segítségével az üzeneteket lehallgathatják és visszajátszhatnak egy korábbi üzenetet. Így befolyásolhatják a jármű működését vagy irányítását is. Illetve DoS támadást is intézhetnek, ekkor a releváns üzenetek nem jutnak el a megfelelő helyre időben.³⁹

Feldolgozó algoritmusok:

- Feldolgozó algoritmusok legfőbb kihívása: az elmúlt években felfedezték, hogy a konvolúciós neurális hálózatok érzékenyek olyan ellentétes bemenetekre, amelyek miatt rosszul osztályozzák a képeket (pl. egy autót fának vagy egy személyt közlekedési táblának minősítenek). Mivel a számítógépes érzékelés szinte minden fejlett vezetőtámogató rendszer CNN-t használ, ez jogos kiberbiztonsági fenyegetés. Az ellenséges támadás során a támadó bizonyos mennyiségű zajt ad a kamera által kibocsátott képhez (az emberi szem számára nem érzékelhető), mielőtt azt a számítógépes rendszer feldolgozná. Ezért olyan CNN-architektúrákat kell találni, amelyek elég ellenállóak ahhoz, hogy megvédjék a képadat-folyamatot.⁴⁰

2.4 Autonóm vezetési rendszerelemek védelmi eljárásai

Autonóm irányítást segítő szenzorok védelmi megoldásai:

- LiDAR szenzorok esetében a támadások sikerességét 4 védelmi megoldással lehet csökkenteni:
 - Érzékelők redundanciája: védekezés egy triviális megoldása az, ha redundáns LiDAR és egyéb kamerás és ultrahangos eszközök összehangolása, hogy megnehezítsék a támadók számára az összes eszköz egyidejű befolyásolását. Ennek a megoldásnak a költsége azonban arányos a redundáns eszközök számával.

³⁹ Se-Yeon Jeong és mtsai., „A Study on ROS Vulnerabilities and Countermeasure”, in *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, HRI '17* (New York, NY, USA: Association for Computing Machinery, 2017), 147–48, <https://doi.org/10.1145/3029798.3038437>.

⁴⁰ Naveed Akhtar és Ajmal Mian, „Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey”, *IEEE Access* 6 (2018): 14410–30, <https://doi.org/10.1109/ACCESS.2018.2807385>.

- Randomizációs technikák: a LiDAR lézerimpulzusok kibocsátásának véletlenszerűsége, így a támadó nem tudhatja, hogy a szenzor mikor bocsájt ki lézert. Egy másik alternatíva a lézerimpulzusok hullámformájának véletlenszerű beállítása. Ezekkel az érzékeny berendezésekkel csak olyan reflexiós hullámformák fogadhatók el, amelyek megfelelnek a LiDAR lézer által egyedileg előállított véletlenszerű mintázatoknak.
- Jelszűrő: amely azonosítja és kiszűri a hamis jeleket. Ezek a technikák azonban csökkentik a LiDAR kapacitását a visszavert lézerimpulzusok mérésére, ami korlátozza az eszköz hatótávolságát és érzékenységét.⁴¹
- Radar hamisítás és zavarás: ismert technológiai megvalósítás egy az úgynevezett fizikai kihívás-válasz-hitelesítésen (Physical Challenge-Response Authentication továbbiakban PyCRA) alapszik. Ez a technológia környezetet véletlenszerű szondázó jelekkel vizsgálja. A PyCRA véletlenszerű időpontokban leállítja a tényleges érzékelő jeleket, és feltételezi, hogy a támadók nem tudják azonnal észlelni a szondázó jeleket. E feltételezés alapján a PyCRA a rosszindulatú jeleket úgy tudja felismerni a rendszer, hogy meghatározza, hogy azok egy bizonyos időszak alatt magasabbak-e egy zajküszöbértéknél. Azonban ez a megoldás nem megfelelő, mivel igen veszélyes a radar szenzor lekapcsolása például egy vészfék rendszerénél. A továbbiakban ezen rendszert fejlesztették tovább. Azonban ezek alapján a technológiák alapján meghatározható azok a kritériumok, amelyek szükségesek egy ilyen rendszer esetében:
 - A megoldásnak képesnek kell lennie a támadások időben történő észlelésére.
 - A megoldásnak képesnek kell lennie a támadó jelek kiszűrésére, és pontos távolságméréseket kell levezetnie.
 - Konzisztencia: a megoldásnak képesnek kell lennie az előző két kritérium teljesítésére számos körülmény között és többször is.
 - Megszakításmentesség: a megoldásnak nem szabad befolyásolnia a jármű egyéb szolgáltatásait például: vészfékezés.^{42 43}

⁴¹ Cao és mtsai., „Adversarial sensor attack on lidar-based perception in autonomous driving”.

⁴² Prateek Kapoor, Ankur Vora, és Kyoung-Don Kang, „Detecting and Mitigating Spoofing Attack Against an Automotive Radar”, in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, 1–6, <https://doi.org/10.1109/VTCFall.2018.8690734>.

⁴³ Yasser Shoukry és mtsai., „PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks”, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15* (New York, NY, USA: Association for Computing Machinery, 2015), 1004–15, <https://doi.org/10.1145/2810103.2813679>.

- GNSS hamisítás: A következő biztonság erősítő lépéseket ajánlja Zeeshan Haider és Shehzad Khalid:⁴⁴
 - Az abszolút GNSS-jelerősség figyelése: az átlagos jelerősség rögzítésével és figyelésével a rendszer észlelheti a GNSS hamisító támadást, ha megfigyeli, hogy a jelerősség nagyságrendekkel nagyobb, mint a GNSS műholdakból érkező normál jelek.
 - A relatív GNSS-jelerősség figyelése: a vevőszoftver programozható úgy, hogy egymást követő időtartamokban rögzítse és összehasonlítsa a jeleket. A relatív jelerősség nagymértékű változása hamisító támadásra utalna.
 - Az egyes fogadott műholdak jelerősségének nyomon követése: a relatív és abszolút jelerősséget minden egyes GNSS műhold esetében külön-külön rögzítik és nyomon követik.
 - Figyelje a műholdak azonosító kódjait és a fogadott műholdjelek számát: A GNSS-hamisítók jellemzően több tíz azonosító kódot tartalmazó jeleket továbbítanak, míg a terepen a legális GNSS-jelek gyakran csak néhány műholdról érkeznek. A fogadott műholdjelek számának és a műholdak azonosító kódjainak nyomon követése segíthet a hamisító támadás megállapításában.
 - Ellenőrizze az időintervallumokat: a legtöbb GNSS hamisításnál a jelek közötti idő állandó. A valódi műholdak esetében ez nem így van. A jelek közötti időintervallumok nyomon követése hasznos lehet a hamisító támadások felderítésében.
 - Végezzen időösszehasonlítást: Sok GNSS-vevő nem rendelkezik pontos órával. Ha egy pontos órából származó idő adatokat használunk a GNSS-jelekből származó idővel való összehasonlításhoz, ellenőrizhetjük a fogadott GNSS-jelek valódiságát.
 - Végezzen ellenőrzést egy gyorsulásmérő és egy iránytű használatával, ekkor a rendszer önállóan figyelemmel kísérheti és kétszeresen ellenőrizheti a GNSS-vevő által jelentett pozíciót.
- GNSS zavarás: GNSS zavarása ellen számos GNSS-vevő modulban alkalmaznak zavarás elleni intézkedéseket, amelyek a mindennapi elektronikus eszközökből

⁴⁴ Zeeshan Haider és Shehzad Khalid, „Survey on effective GPS spoofing countermeasures”, in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, 573–77, <https://doi.org/10.1109/INTECH.2016.7845038>.

származó nem szándékos zavarást célozzák. Azonban ezek az ellenintézkedések hatástalanok a szándékos támadásokkal szemben. Léteznek már megoldások a zavaró jelek csökkentésére és a valódi jelek begyűjtésére.⁴⁵ Ezeknek a megoldásoknak a következő paraméterekkel biztos rendelkeznie kell:

- Támadás észlelése: a megoldásnak képesnek kell lennie a zavaró támadás időben történő észlelésére a járművek biztonságának biztosítása érdekében.
- Jelszűrő alkalmazása: a megoldásnak képesnek kell lennie a támadó jelek kiszűrésére, hogy a jármű bizonyos támadási forgatókönyvek esetén is működőképes maradjon, és elkerülje a szolgáltatás megszakadását.
- Kamera vakítás:
 - Az első ellenintézkedés a redundancia alkalmazása több, egymást átfedő lefedettségű kamera telepítésével. Ez azért hatékony, mert a lézer- és LED-foltok kis sugárszélességűek, ami megnehezíti több kamera spontán támadását. Ez a védelmi stratégia nem tudja teljesen csökkenteni ezen támadás kockázatát, de a támadóknak több erőfeszítést kell fordítaniuk egy sikeres támadásra.
 - A második ellenintézkedés egy infravörös szűrő beépítése a kamerába. Ez egy olyan technológia, amely a biztonsági kamerákon elérhető, és igény szerint képes a közeli infravörös fény szűrésére. De a megvalósításhoz kísérletekre lenne szükség.⁴⁶

Operációs rendszerek védelme:

- A ROS védelmének első megközelítése az alkalmazás szintjén valósítható meg. Bevezetünk egy dedikált hitelesítési kiszolgálót, amely nyomon követi, hogy melyik ROS-csomópont férhet hozzá egy témához, vagy melyik adhat információt hozzá egy témához. Ezenkívül ez a kiszolgáló kezeli a csomópontok hitelesítését, és generálja a téma-specifikus titkosítási kulcsokat.
- A másik védelmi megközelítés a ROS kommunikáció biztosítás. Fontos leszögezni, hogy a két megoldás együtt is alkalmazható, sőt közös alkalmazása nyújtja a legnagyobb biztonsági szintet. A kommunikáció esetében külön hitelesítési és titkosítási mechanizmust kell bevezetni. A kommunikációt egy TLS (Transport Layer Security) megoldással biztosítjuk. Ezen kívül minden csomóponthoz témakörönként

⁴⁵ Anupam Purwar, Divya Joshi, és Vinod Kumar Chaubey, „GPS signal jamming and anti-jamming strategy — A theoretical analysis”, in *2016 IEEE Annual India Conference (INDICON)*, 2016, 1–6, <https://doi.org/10.1109/INDICON.2016.7838933>.

⁴⁶ Jonathan Petit és mtsai., „Remote attacks on automated vehicles sensors: Experiments on camera and lidar”, *Black Hat Europe* 11, sz. 2015 (2015): 995.

hajtjuk végre az engedélyezést. A TLS ebben az esetben úgy működik, hogy aszimmetrikus titkosítással kézfogás megy végbe majd a kommunikáció során szimmetrikus titkosítás van jelen. A sértetlenséget MAC kód garantálja.⁴⁷

Feldolgozó algoritmusok biztonsági megoldásai:

Általában az ML algoritmusok hatékonysága nagymértékben függ a bemeneti adat minőségétől, illetve integritásától.⁴⁸ Ez azt jelenti, hogy a támadók fő célja nem is az algoritmusok kompromittálása, hanem azon bemeneti adatok megmásítása, amelyet ezen technológia fel fog majd dolgozni. Ennek elkerülése érdekében az előzőleg bemutatott komponensek fenyegetéseit szükséges megoldani, hogy biztosítva legyen adat hitelessége az érzékelésen át, a továbbítástól kezdve egészen a feldolgozásig.

2.5 Külső kommunikációt támogató rendszerelemek kiberbiztonsági fenyegetései

Fontos megvizsgálni a külső kommunikációt fenyegető kihívásokat, mivel ez a típusú adatsere biztosítja a VANET-en keresztüli intelligens közlekedési rendszer működését. Mivel hálózati kommunikációról beszélünk itt is megjelennek a tradicionális kommunikációs kihívások.

- Szolgáltatás megtagadás támadás: ahol a támadó zavaró jelekkel blokkolja a teljes kommunikációs csatornát. Az ITS környezetben, bizonyos késedelem befolyásolhatja a járművek vezetési biztonságát, akár egy másodperc késlekedés is balesetet okozhat. Ezenkívül, a válaszadási időre vonatkozó kérés viszonylag magas, ezért ez a támadás veszélyes és végzetes az önvezető járművek számára.⁴⁹
- Megszemélyesítő támadások: mint a legtöbb hálózatban az elemke külön egyedi azonosítóval rendelkeznek, ez természetesen az ITS esetében is így van. A megszemélyesítési támadások egy másik valós személyazonosság vagy hamis személyazonosság használatával valósulnak meg. Kétféle megszemélyesítő támadás létezik, nevezetesen a csomópont megszemélyesítő támadások és a sybil támadások. A csomópont megszemélyesítő támadások során egyszerre csak egyetlen

⁴⁷ Bernhard Dieber és mtsai., „Security for the Robot Operating System”, *Robotics and Autonomous Systems* 98 (2017. október 1.), <https://doi.org/10.1016/j.robot.2017.09.017>.

⁴⁸ Laith Alzubaidi és mtsai., „Review of deep learning: concepts, CNN architectures, challenges, applications, future directions”, *Journal of Big Data* 8, sz. 1 (2021. március 31.): 53, <https://doi.org/10.1186/s40537-021-00444-8>.

⁴⁹ Sushil Kumar és Kulwinder Singh Mann, „Prevention of DoS attacks by detection of multiple malicious nodes in VANETs”, in *2019 International Conference on Automation, Computational and Technology Management (ICACTM)* (IEEE, 2019), 89–94.

személyazonosságot hamisítanak meg. A sybil-támadások során egyszerre több hamis személyazonosságot használnak az elkövetők.⁵⁰

- Visszajátszási támadások: során az elkövető rögzíti a hálózati kommunikációt és ezt a hiteles információt küldi be a rendszerbe újra. Ez számos fenyegetést rejthet magában, ami az ITS egészének működését hátráltathatja, vagy akár a közlekedés biztonságát is veszélyeztetheti. Ilyen visszajátszás lehet, ha például egy támadó elfog egy megkülönböztetett jármű magas prioritású jelzését (pl.: mentő autónak azon jelzését, hogy az adott útvonalon át kell haladnia a lehető leggyorsabban és a közlekedők álljanak félre) és ezt később felhasználva egy bűntény elkövetése után menekülés közben ezt a jelzést újra küldi.⁵¹
- Útválasztási támadások: az útválasztási támadások kihasználják az útválasztási protokollok hátrányát és sebezhetőségét. Az útválasztási támadások közé tartoznak a:
 - fekete lyuk támadások amely esetében egy olyan hálózat csomópont keletkezik, amely a kettő hiteles pont közötti kommunikációs csomagokat nem juttatja tovább, eldobja azokat. Ennek egy változata a szürke lyuk támadás, amikor a támadó csak bizonyos csomagokat dob le.⁵²
 - a féreglyuk támadások esetében a támadó egy átjárót biztosít kettő a hálózatban nem közvetlen csomópont között. Ezt megtéve ezen csomópontok az útválasztási táblájukat frissítve egymást szomszédos csomópontként azonosítják. Ezzel a hálózati struktúrát tudják befolyásolni a támadók, amit később például egy szolgáltatás megatagadás támadásra is használhatják ha ezt a féreglyukat ki- bekapcsolgatják a csomópontoknak folyamatosan frissíteni kell az útválasztási táblát ezzel erőforrást elvonva a fő feladatoktól.⁵³
- Adathamisítási támadások: hatalmas gondot tudnak jelenti az ITS hálózatokban, mivel a közlekedés biztonsága a valós adatokon nyugszik. Az adathamisítási támadások

⁵⁰ Ahilan Appathurai, Gunasekaran Manogaran, és Naveen Chilamkurti, „Trusted FPGA-based transport traffic inject, impersonate (I2) attacks beaconing in the Internet of Vehicles”, *IET Networks* 8 (2019. május 1.): 169–78, <https://doi.org/10.1049/iet-net.2018.5171>.

⁵¹ Fatih Sakiz és Sevil Sen, „A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV”, *Ad Hoc Networks* 61 (2017. március 1.), <https://doi.org/10.1016/j.adhoc.2017.03.006>.

⁵² Kamlesh Chandra Purohit, Sushil Chandra Dimri, és Sanjay Jasola, „Mitigation and Performance Analysis of Routing Protocols Under Black-Hole Attack in Vehicular Ad-Hoc Network (VANET)”, *Wireless Personal Communications* 97, sz. 4 (2017. december 1.): 5099–5114, <https://doi.org/10.1007/s11277-017-4770-6>.

⁵³ Parteek Kumar és Sahil Verma, „Detection of Wormhole Attack in VANET”, *National Journal of System and Information Technology* 10, sz. 1 (2017): 71.

során a támadó hamis információkat és biztonsági figyelmeztetéseket küldhet vagy sugározhat.⁵⁴

- Lehallgatási támadások: lényege, hogy a támadó elfogja a kommunikációt így a járművek adatait, illetve használók személyesadatait begyűjti. Ezek az adatok megfelelő alapot adhatnak egy későbbi komplex támadáshoz. Ezeknek a támadásoknak a detektálása nehéz, mivel érzékelhető hatása nincs.⁵⁵
- Jelszó- és kulcstámadások: az ilyen támadásokhoz általában szükségük van a támadóknak néhány speciális hardverre és szoftverekre. A jelszó és a kulcs támadások esetén a mechanizmust különböző értékekkel tesztelik, amíg nem sikerül kompromittálni. Ennek a támadásnak három módját különböztethetjük meg. Az egyik a szótár technológia, amikor a támadó rendelkezik listákkal, amelyeket kombinálva használ a jelszó feltöréshez. A szivárványtábla-támadásokban a támadó egy listát használ fel, amely a lehetséges jelszavak előzetesen kiszámított hash értékét tartalmazza. A nyers erővel végrehajtott támadások hasonlóak a szótári támadáshoz; azonban, a nem szótári szavakat is képesek azonosítani az összes alfanumerikus kombináció átdolgozásával.⁵⁶

2.6 Külső kommunikációt támogató rendszerelemek védelmi eljárásai

Annak érdekében, hogy a járművet minden hálózati támadás ellen megvédjék, a támadások típusai alapján a következő stratégiák léteznek.

- Szolgáltatás megatagadás támadások ellen: a korai észlelés segít megghiúsítani a támadásokat, vagy figyelmeztetni a jármű üzemeltetőt, hogy tegyen néhány hatékony ellenintézkedést. A DoS-támadásokkal szembeni ellenintézkedések során számos megoldás létezik. Az egyik a többszörös rosszindulatú csomópont csomagok észlelési algoritmus (Multiple Malicious Node Packet Detection Algorithm), amely csomagfelismerés alapján tud detektálni több rosszindulatú hálózati csomópontot, és letudja azokat szigetelni.⁵⁷ Egy másik megközelítés a port-hopping mechanizmus által kialakított egy egyszerű, de hatékony védelmi mechanizmus, amelynek előnye, hogy a

⁵⁴ Raj Mani Shukla és Shamik Sengupta, „Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application”, in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (IEEE, 2018), 688–94.

⁵⁵ Sarankumar Balakrishnan és mtsai., „Modeling and analysis of eavesdropping attack in 802.11 ad mmWave wireless networks”, *IEEE Access* 7 (2019): 70355–70.

⁵⁶ Simon Parkinson és mtsai., „Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges”, *IEEE Transactions on Intelligent Transportation Systems* 18, sz. 11 (2017): 2898–2915, <https://doi.org/10.1109/TITS.2017.2665968>.

⁵⁷ Kumar és Mann, „Prevention of DoS attacks by detection of multiple malicious nodes in VANETs”.

rosszindulatú csomagok észlelése és kiszűrése a meglévő protokoll módosítása nélkül is megvalósítható.⁵⁸

- A megszemélyesítési támadások ellen: ezen támadások kivédésére néhány elérhető stratégia létezik, többek között a biztonságos átvitel, integritásellenőrzés. A védett adat átvitel megoldható egy biztonságos téradatátviteli mechanizmussal a VANET hálózaton, amelyben a járművek nagyobb valószínűséggel továbbíthatják az adatokat.⁵⁹ Az integritást biztosítására megoldás lehet a hash-alapú integritásellenőrzési mechanizmus, amely hatékonyan véd ezen támadási formától főleg a felhőalapú infrastruktúrában.⁶⁰
- A visszajátszási támadások ellen: ezen támadások megghiúsítása érdekében a rendelkezésre álló stratégiák közé tartozik a zajos vezérlőjel-módszer és a keresztkorrelátor, valamint az időbélyegzés és az XOR-kódolás technika. A zajos vezérlőjel-módszer és a keresztkorrelátor használata alapján egy decentralizált diagnosztikai algoritmus került kialakításra a visszajátszási támadások felderítésére. Ezt egy azonos sebességgel közlekedő járműcsoporton tesztelték. Ezt a módszert úgy alkalmazták a jelen példában, hogy észlelje a járműcsapatban történő visszajátszást. A zajos vezérlőjelet csak a szakasz vezető járműve állítja elő. Valójában a vezető járműben egy fehér Gauss-zajjelet adnak a tényleges vezérlőjelhez.⁶¹ Egy másik megoldásban időbélyegzés és XOR-kódolás alkalmazásával a rendszer képes ellensúlyozni az újrjátszási támadásokat. Ebben a megközelítésben a titkosított jel továbbít egy időbélyeget egy úgynevezett számláló értékkel együtt. A vevő oldalon a jel dekódolása és az időbélyeg érvényesítése a szinkronszámláló segítségével történik.⁶²

⁵⁸ Yingmo Jie és mtsai., „Dynamic Defense Strategy Against DoS Attacks Over Vehicular Ad Hoc Networks Based on Port Hopping”, *IEEE Access* 6 (2018): 51374–83, <https://doi.org/10.1109/ACCESS.2018.2869399>.

⁵⁹ Trupil Limbasiya és Debasis Das, „Secure and Effective Geo-Data Transmission Scheme for Vehicle-to-Vehicle Communication”, in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, 389–96, <https://doi.org/10.1109/SmartWorld.2018.00096>.

⁶⁰ Nayana Hegde és Sunilkumar S. Manvi, „Hash Based Integrity Verification for Vehicular Cloud Environment”, in *2019 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2019, 75–79, <https://doi.org/10.1109/CCEM48484.2019.00016>.

⁶¹ Roberto Merco, Zoleikha Abdollahi Biron, és Pierluigi Pisu, „Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control”, in *2018 Annual American Control Conference (ACC)*, 2018, 5582–87, <https://doi.org/10.23919/ACC.2018.8431538>.

⁶² Kyle Greene és mtsai., „A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic”, *IEEE Consumer Electronics Magazine* 10, sz. 1 (2021): 101–8, <https://doi.org/10.1109/MCE.2020.3012425>.

- Az útválasztási támadások ellen: ezen támadások kivédésére létezik néhány stratégia, többek között az intelligens útválasztási protokoll, a mesterséges intelligencia swarm algoritmusai. Az intelligens útválasztási protokoll a hálózat élettartamának növelése mellett képes megtalálni az optimális utat a feladótól a vevőig, ezzel sikerül kivédeni az útválasztási támadásokat és növelni lehet a hálózat élettartamát.⁶³ A mesterséges intelligencia swarm algoritmusainak használata 3 fázisból áll: útvonal építése, a meglévő útvonalak karbantartása, és a megbízhatósági becslés frissítése az útválasztás anomáliáinak észleléséhez, és új útvonal építése, amely megkerüli a gyanús csomópontot.⁶⁴
- Az adathamisítási támadások ellen: kutatásom alapján a dinamikus időablak, és a hamisított adatok szűrése lehetnek megoldások. A dinamikus időablak használata alapján egy anomáliastratégia került kialakításra, amely vizsgálja a rendszerben az anomáliákat és kiszűri azokat.⁶⁵ A hamisított adatok szűrése esetén ezen támadások enyhítésére a járműhálózatokban az adatátvitel során eltávolíthatók a hamisított forgalmi állapotadatok.⁶⁶
- A lehallgatás támadások ellen: ezen támadások kivédésére van néhány stratégia, többek között anonimizálás, a bizalomalapú, ütemezési mechanizmus. Az anonimizálást el lehet érni egy ködszerverrel, ami egy kód anonimizáló, ahol a ködcsomópontból érkező üzenetek nem köthető konkrét csomóponthoz közvetlenül.⁶⁷ A többdimenziós bizalmi modell létrehozása során a hálózatban lévő csomópontok állapota felosztható egyszeri mintára és találkozó mintára. Az előbbi magának a csomópontnak az állapotára vonatkozik (például energia, tárolási, feldolgozási képesség), míg az utóbbi akkor írja le a viselkedést, amikor egy csomópont kölcsönhatásba lép más csomópontokkal vagy részt vesz a hálózati átvitelben. Ezek alapján ki lehet szűrni a lehallgatást eszközölő elemeket.⁶⁸

⁶³ Niranjana Panda és B. Kumar Pattanayak, „Energy aware detection and prevention of black hole attack in MANET”, *International Journal of Engineering and Technology (UAE)* 7, sz. 2.6 (2018): 135–40.

⁶⁴ Vasily Krundyshev, Maxim Kalinin, és Peter Zegzhda, „Artificial swarm algorithm for VANET protection against routing attacks”, in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, 795–800, <https://doi.org/10.1109/ICPHYS.2018.8390808>.

⁶⁵ Shukla és Sengupta, „Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application”.

⁶⁶ Jie Lin és mtsai., „Data Integrity Attacks Against Dynamic Route Guidance in Transportation-Based Cyber-Physical Systems: Modeling, Analysis, and Defense”, *IEEE Transactions on Vehicular Technology* 67, sz. 9 (2018. szeptember): 8738–53, <https://doi.org/10.1109/TVT.2018.2845744>.

⁶⁷ Muhammad Arif, Guojun Wang, és Valentina Emilia Balas, „Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing”, *Stud. Inform. Control* 27, sz. 2 (2018): 235–46.

⁶⁸ Wei Liang és mtsai., „TBRS: A trust based recommendation scheme for vehicular CPS network”, *Future Generation Computer Systems* 92 (2018. október 1.), <https://doi.org/10.1016/j.future.2018.09.002>.

- Jelszó- és kulcstámadások ellen: ezeknek a kulcstámadásoknak a kivédésére felhasználhatóak a biztonságos kriptográfiai mechanizmusok és a többfaktoros hitelesítés. Az egyik megoldás a biztonságos kriptográfiai mechanizmusokra támaszkodik, például a nagy méretű kulcsokra, a biztonságos algoritmusokra és a biztonságos kellően bonyolult jelszavakra. A jövőben főleg a kvantum számítógépek megjelenésével szám kriptográfiai algoritmusok könnyen feltörhetőek lesznek. Ezért biztonságos kriptográfiai mechanizmusokra való támaszkodás helyett egy másik megoldás a többfaktoros hitelesítés, amely különböző tényezőket, többek között a hozzáférési kérelem időpontját és a földrajzi elhelyezkedést is figyelhet.⁶⁹

2.7 Következtetések

A kiberbiztonsági fenyegetések és védelmi intézkedések megvizsgálásban az látható, hogy már most számos kihívásra rendelkezésre áll számos megoldási kutatás, technológia. A jövőben ezek részletes tesztelésére lesz szükség, amely során az egyes kihívásokra standardizálva csak pár megoldás alkalmazása ajánlott, ezzel biztosítva a törekvést a járművek homogén felépítésére.

⁶⁹ Nilesh Khankari és Geetanjali Kale, „One Time Password Generation for Multifactor Authentication using Graphical Password”, *International Journal Of Engineering Research and General Science* 3 (2020. augusztus 25.): 489–94.

3 Az autonóm járművek jogszabályi és szabványi kereteinek vizsgálata

A világon már számos ország és nemzetközi szervezet foglalkozik szabályozási és szabványi szinten az autonóm járművek szabályozásával. Ebben a fejezetben megvizsgálom, hogy a jogi szabályozás mire is terjed ki, továbbá a szabványok azon csoportját, amely segítséget tud nyújtani egy biztonságos és hatékony önvezető jármű kiépítésében.

3.1 Jogsabályok

Vizsgálatomban két geopolitikailag is és autógyártás szempontjából is fontos szereplőt vizsgáltam meg, az Egyesült Államokat és az Európai Uniót. Ezen két területen a szabályozások fő része a tesztelési eljárásokhoz szükséges feltételeket és kereteket határozzák meg.

3.1.1 Egyesült Államok szabályozása

Az Egyesült Államokban a Nemzeti Közúti Közlekedésbiztonsági Hivatal (National Highway Transportation Safety Administration, továbbiakban NHTSA) biztonsági keretrendszert határozott meg az autonóm vezetés biztonsági értékelésének strukturálására. Ezt a keretrendszert javasolt, nem kötelezően követendő keretrendszerként adták ki. Ennek ellenére az amerikai autóipar autonóm járművekre vonatkozó biztonsági programjai ezen keretrendszeren alapulnak, ilyen példákat találhatunk a Waymo⁷⁰, a General Motors⁷¹ biztonsági programjaiban. Viszont látni kell, hogy az Egyesült Államoknak nincs egyedi szövetségi szabályozása, és csak iránymutatásokat ad az államok kormányainak a témával kapcsolatban.

Az NHTSA autonóm járművekre vonatkozó biztonsági keretrendszere⁷² 12 területből áll, amelyekre bármely autonóm járművekkal foglalkozó vállalatnak összpontosítania kell. Először is, a biztonság rendszertervezési megközelítést kell alkalmazni, és ez a megközelítés áthatja az egész keretdokumentumot. A jól megtervezett és ellenőrzött szoftverfejlesztési folyamatok elengedhetetlenek, és ahol szükséges, alkalmazni kell a meglévő SAE- és ISO-szabványokat az autóiparban, a repülőgépiparban és más releváns iparágakban. A fennmaradó 11 terület két kategóriába szerveződik: autonómia-tervezés, amely megköveteli, hogy bizonyos komponenseket beépítsenek és figyelembe vegyenek a kialakítandó szoftvercsomagban; valamint tesztelés és balesetsökkentés, amely az autonóm funkciók

⁷⁰ „Safety Publications”, Waymo, elérés 2022. február 27., <https://waymo.com/safety/>.

⁷¹ „Putting Self-Driving Cars On The Roads | General Motors”, general motors, elérés 2022. február 27., <https://www.gm.com/content/public/us/en/gm/home/stories/self-driving-cars.html>.

⁷² „Automated Driving Systems 2.0: A Vision for Safety” (National Highway Transportation Safety Administration, 2017).

tesztelésének megközelítéseire és a hibák negatív hatásainak csökkentésére, valamint a hibákból való tanulásra vonatkozó módszerekre terjed ki.

Fontos megemlíteni, hogy a tesztelési területen belül az NHTSA erős és kiterjedt tesztelési programot javasol, mielőtt bármilyen szolgáltatást elindítanának a nyilvánosság számára. Ez a tesztelés három közös pillérre támaszkodhat: szimuláció, tesztpályán végzett tesztelés és nyilvános közúti vezetés.

A Nemzeti Közúti Közlekedésbiztonsági Hivatal továbbfejlesztette ezen dokumentumát, amely először a „Felkészülés a közlekedés jövőjére: Automatizált járművek 3.0” (AV 3.0)⁷³ címmel újult meg. Ez a dokumentum az összes felszíni közúti közlekedési rendszerre kiterjeszti az alkalmazási kört, és az érdekelt felek sokféle, országszerte zajló részvételének hozzájárulásával került kidolgozásra. Az AV 3.0 három kulcsfontosságú terület köré épül:

- teljeskörű biztonság előmozdítása;
- a szabályozási bizonytalanság csökkentése, és
- az Egyesült Államok Közlekedési Minisztériumával való együttműködés folyamatának felvázolása.

A következő továbbfejlesztés az amerikai vezető szerep biztosítása az automatizált járműtechnológiák terén: Az automatizált járművek 4.0 (AV 4.0) dokumentum az AV 3.0-nak kibővítette a hatályát 38 releváns területre, az Egyesült Államok kormányának azon részeire, amelyek közvetlenül vagy érintőlegesen érdekeltek az autonóm járművek technológiáinak biztonságos fejlesztésében és integrálásában. Ez a dokumentum három kulcsfontosságú terület köré szerveződik:

- az Egyesült Államok kormányának autonóm járművekkel kapcsolatos alapelvei;
- az AV-technológia növekedését és vezető szerepét támogató közigazgatási erőfeszítések;
- az Egyesült Államok kormányának tevékenységei és együttműködési lehetőségei.⁷⁴

Az látható az Egyesült Államok által kialakított stratégia esetében, hogy a AV 2.0-dokumentummal lefektette azokat az alappilléreket, amelyekkel foglalkozni kell az autonóm közlekedéssel kapcsolatban. Ennek továbbfejlesztése az AV 3.0, amely a NHTSA által kiadott

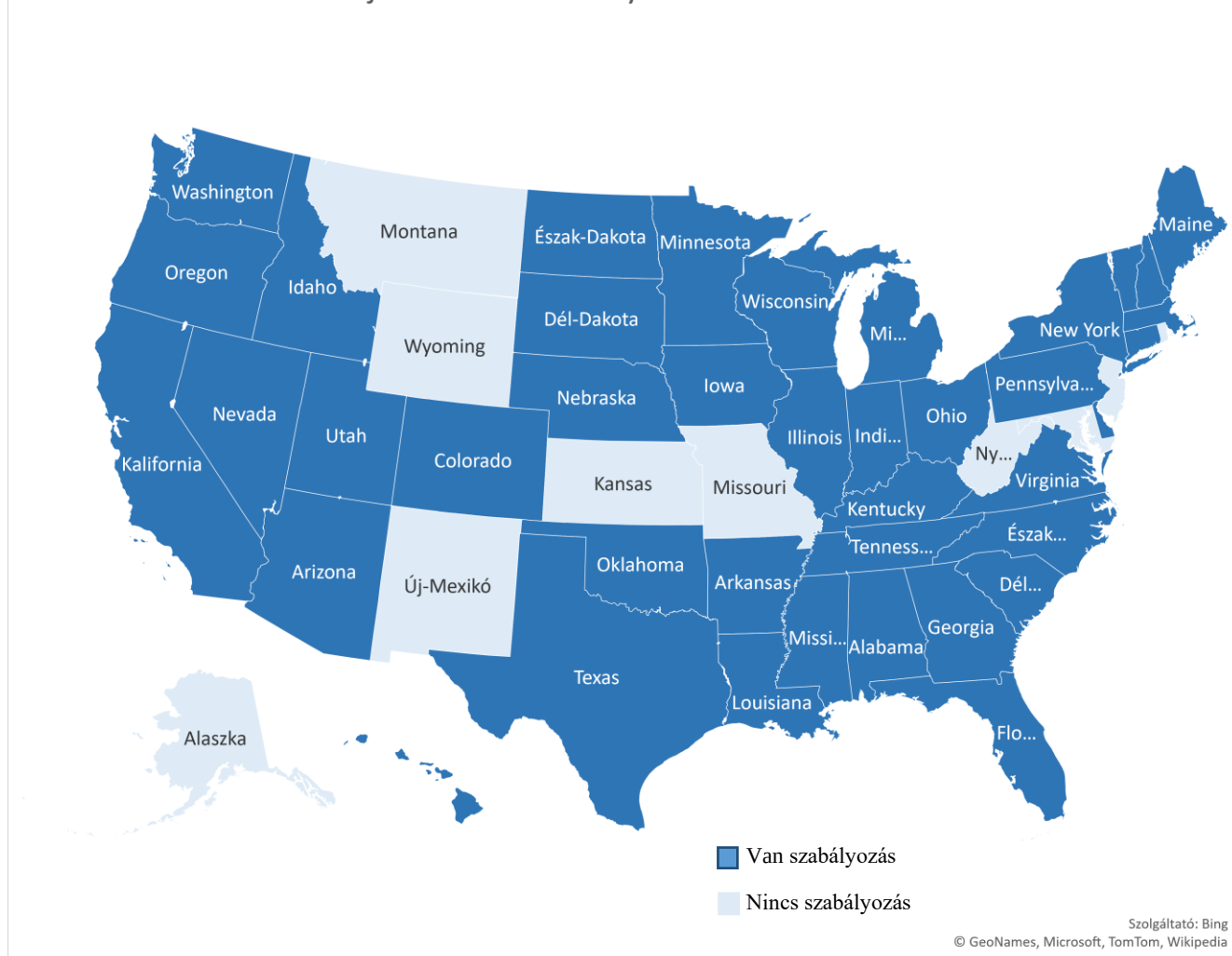
⁷³ U.S. Department of Transportation, *Preparing for the Future of Transportation: Automated Vehicles 3.0* (Washington: U.S. Department of Transportation, 2019), 0.

⁷⁴ „AV 4.0 | US Department of Transportation”, 2019, <https://www.transportation.gov/policy-initiatives/automated-vehicles/av-40>.

olyan dokumentum, amely igen részletesen foglalkozik a technológiai megvalósítással is, tehát ez a dokumentum egy absztrakciós szinttel mélyebben fogalmaz meg elvárásokat az autonóm járművekkel kapcsolatban, melyekhez már létező jó gyakorlatokat is társít. Az AV 4.0 tanulmányozásaim alapján nem egy tovább fejlesztett verziója a 3.0-nak, mert a dokumentum célja és mélysége is eltér az előzőétől. Míg az első kettő dokumentum próbálta a felső szintű stratégiai célokat egy alacsonyabb szinten is definiálni, addig a 4.0 ismét vissza tér a stratégiai szintre, ahol megfogalmazza az Egyesült Államok elköteleződését és támogatását az autonóm járművek kifejlesztésével kapcsolatban. Évről évre fokozatosan nőtt azon államok száma, amelyek fontolgatják az autonóm járművekre vonatkozó jogszabályok bevezetését. 2012-ben hat állam, 2013-ban kilenc, 2014-ben tizenkettő, 2015-ben tizenhat, 2017-ben harminchárom míg 2018-ban tizenöt állam további 18 önvezető járművel kapcsolatos törvényjavaslatot fogadott el.⁷⁵ A lenti ábrán látható, hogy az USA államainak nagy része rendelkezik ezen területen szabályozással. A következőkben részletesebben Kalifornia állam szabályozását mutatom be, mivel az egyik vezető szereplő az autonóm járművek technológiájában az Egyesült Államokban.

⁷⁵ „Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation”, elérés 2022. április 10., <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>.

Önvezető járművekre szabályozással rendelkező államok



6. ábra Önvezető járművekkel kapcsolatos szabályozás az USA-ban (saját szekresztés forrás: <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>)

- Kalifornia:

Kalifornia 2012-es törvénye felhatalmazta az állam Közlekedési Minisztériumát, hogy szabályokat dolgozzon ki a vezető nélküli tesztjárművekre. 2015 decemberében a minisztérium bevezetett egy tervezetet, amely úgy érvényesíti a törvényt, hogy emberi biztonsági vezetőt ír elő a járműben, annak tesztelése során. Ez a dokumentum azt is kimondta, hogy a járművek gyártói saját maguk tanúsítják a jármű biztonságát, hogy megfeleljenek az összes vonatkozó szövetségi gépjármű-biztonsági szabványnak, és megfeleljenek a veszélyes helyzetekre vonatkozó közlekedési törvényeknek is. Ezenkívül szükség volt egy „funkcionális biztonsági tervre”, amely azonosítja és értékeli az összekapcsolat vagy autonóm járművek tesztelés során előforduló

veszélyes helyzeteket. Ezen szabályokat 2018 februárjában a minisztérium tovább fejlesztette, így lehetőség nyílt a az önvezető járművek tesztelését biztonsági sofőr jelenléte nélkül.⁷⁶

Bár a kaliforniai szabályok lehetővé teszik a gyártók számára, hogy a járművet emberi biztonsági vezető jelenléte nélkül teszteljék, szükség van egy távoli emberi kontrollra vagy kezelőre, aki kommunikációs kapcsolatot létesít a járművel. Következésképpen bevezették a második engedélyt, „Gyártói vizsgálati engedély – Vezető nélküli járművek”. Az engedélyt csak akkor adják ki, ha a gyártó megad olyan adatokat mint például a összes közút listáját, ahol a járműveket megvizsgálják, a tesztelés megkezdésének dátumát, a tesztelés napját és időpontját, a vizsgálandó járművek számát és a vizsgálandó járműtípusokat. Egy másik típusú engedély az autonóm járművek közutakra történő telepítése, amely lehetővé teszi a gyártók számára, hogy Kalifornián belül telepítsenek összekapcsolt vagy autonóm járműveket. Ez az engedély kifejezetten az automatizált járművek kaliforniai utakon történő nyilvános használatának szabályozására készült. Az engedély megszerzéséhez a gyártóknak ismertetniük kell a jármű automatizálási szintjét (SAE 3., 4. vagy 5.) és a jármű üzemi tervezési területét (ahol a jármű közlekedni fog), az összes vonatkozó szövetségi gépjármű-biztonsági szabványnak való megfelelést, valamint tanúsítványt kell benyújtaniuk arról, hogy a jármű alkalmas és megfelel a kaliforniai közlekedési törvényeknek, továbbá tanúsítvánnyal rendelkezik arról, hogy megfelel a nemzetközi kiberbiztonsági szabványoknak. A telepítéshez a járművet fel kell szerelni adatrögzítővel, és meg kell felelnie a jelenlegi iparági szabványoknak, hogy segítsen védekezni a kibertámadások ellen.⁷⁷

Mint látható, Kaliforniában külön figyelmet fordítanak a kiberbiztonsági aspektusra is, illetve látható, hogy széles tesztelési skálát biztosítanak az autógyártóknak.

3.1.2 Európai Unió szabályozása

Az Európai Bizottság elfogadta a kooperatív intelligens közlekedési rendszerekről szóló európai stratégiát (C-ITS). Ez a stratégia 2019-től lehetővé teszi az egymással és az infrastruktúrával kommunikálni képes járművek alkalmazását az EU útjain. Célja a belső piac

⁷⁶ Dasom Lee és David J. Hess, „Regulations for On-Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization”, *Transportation Research Part A: Policy and Practice* 136 (2020. június 1.): 85–98, <https://doi.org/10.1016/j.tra.2020.03.026>.

⁷⁷ „California Autonomous Vehicle Regulations”, *California DMV* (blog), elérés 2022. március 15., <https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/california-autonomous-vehicle-regulations/>.

széttöredezettségének elkerülése, a kommunikációs technológiák kombinációjának alkalmazása, a biztonsági és adatvédelmi kérdések kezelése, a megfelelő jogi keret kialakítása és a nemzetközi szintű együttműködés.⁷⁸ Azonban azt lehet látni, hogy az autonóm járművek szabályozása Európai Unió esetében stratégiai szinten jelenik meg csak, amely a legmagasabb absztrakciós szint. Az Unión belül Németország az a tagállam többek között, amely külön stratégiával rendelkezik az önvezető járművekkel kapcsolatban, továbbá jogszabályi szinten is megjelenik ezen terület. Nemzeti szinten elmondható, hogy minden egyes országnak megvan a maga önvezető jármű célú sajátos szabályozási kerete. Az önvezetési funkciók tesztelésére irányuló nyílt utcai vezetési tevékenységek tekintetében Európa több országában általános gyakorlat, hogy a közúti üzemi tesztek nemzeti szintű bevezetésének lehetővé tétele érdekében a következő információkat kéri a kérelmezőtől:

- kérelmező adatai (pl. elérhetőségek, biztosítás)
- járművezető képesítése
- jármű adatai (pl. leírás, az alkalmazandó szabványoknak való megfelelés)
- infrastruktúra / üzemeltetési terület (pl. a vizsgálathoz szükséges terület);
- tesztelendő viselkedés (pl. milyen vezetési feladatok automatizálódnak és kerülnek tesztelésre);
- dokumentáció (pl. veszélyelemzés és kockázatértékelés, elektromágneses összeférhetőség dokumentálása);
- tesztelés eredményei (pl. biztonságos működés, beleértve a stresszteszteket is, naplók, értékelések).⁷⁹

A következőkben részletesebben a német szabályozást vizsgáljuk meg. Azért ezt a szabályozást, mivel Németország az elsők között ültette jogszabályba ezt a területet.

- Németország
2013-ban a Szövetségi Digitális és Közlekedési Minisztérium tanácsadó testületként létrehozta az "Automatizált vezetés" kerekasztalt. Ez lehetővé teszi az ipar, a tudományos élet, a szövetségek és a közigazgatás érdekelt felei közötti szoros eszme- és tapasztalatcserét. A szükséges know-how-t úgy egyesítik, hogy széles körű társadalmi konszenzus jöjjön létre az automatizált és összekapcsolt vezetés minden releváns aspektusában. A kerekasztal általában évente kétszer ülésezik, és kidolgozza azokat a

⁷⁸ „JELENTÉS a kooperatív intelligens közlekedési rendszerek európai stratégiájáról”, elérés 2022. március 15., https://www.europarl.europa.eu/doceo/document/A-8-2018-0036_HU.html.

⁷⁹ „Connected Automated Driving | EU-countries”, elérés 2022. április 10., <https://www.connectedautomateddriving.eu/regulation-and-policies/national-level/eu/>.

kulcsfontosságú kérdéseket, amelyeket az automatizált és összekapcsolt vezetés sikeres bevezetése érdekében figyelembe kell venni. Ezek képezték az alapját a szövetségi kormány 2015-ös stratégiájának, amely a következő cselekvési területeket azonosította:

- infrastruktúra;
- szabályozás;
- innováció;
- összekapcsolhatóság;
- információbiztonság és adatvédelem.⁸⁰

A 2017. június 21-én hatályba lépett automatizált vezetésről szóló törvény (a közúti közlekedésről szóló törvényt módosító nyolcadik törvény), amivel Németország a világon az elsők között szabályozta az automatizált vezetési funkciókat használó járművezetők jogait és kötelezettségeit. A törvény többek között meghatározza azokat a magas műszaki követelményeket, amelyeknek az automatizált rendszereknek meg kell felelniük ahhoz, hogy a járművezetőknek ne kelljen a vezetésre figyelni. Az illetékes járműgyártónak meg kell erősítenie, hogy a rendszer megfelel ezeknek a műszaki követelményeknek. Ezen jogszabály rendelkezik arról, hogy a gépjármű gyártójának folyamatos igazolási kötelezettsége van a Szövetségi Közlekedési Hatóság és az illetékes hatóság felé, hogy a gépjármű teljes fejlesztési és üzemeltetési időszaka alatt a gépjármű elektronikus és elektromos architektúrája, valamint a gépjárműhöz csatlakoztatott elektronikus és elektromos architektúra védett a támadásokkal szemben. Illetve szükséges egy kockázat elemzést is elvégezni a gépjárműre, amely eredményének szükséges azt tükrözni, hogy a gépjármű védett a feltárt kockázatokkal szemben. A törvény a biztonság érdekében ellenőrző rendszer (fekete doboz; StVG §63a. és §63b.) alkalmazását is előírja, és megköveteli a baleseti felelősség megállapításának lehetőségét.⁸¹ A szabályozásból tisztán látszódik, hogy az általános engedélyezési eljárásban csak a korlátozott autonómiával rendelkező gépjárműveket engedélyezik, ahol egy sofőrnek készen kell állnia, hogy bármikor át tudja venni az irányítást.

3.2 Az automatizált közúti járművekkel kapcsolatos szabványok

Céljaim között volt egy komplex szabvány feldolgoz, amely azonosítja azon szabványokat, amelyeket figyelembe kell venni egy önvezető közúti jármű fejlesztése során.

⁸⁰ „BMDV - Automated and connected driving”, elérés 2022. március 15., <https://www.bmvi.de/EN/Topics/Digital-Matters/Automated-Connected-Driving/automated-and-connected-driving.html>.

⁸¹ „Straßenverkehrsgesetz (StVG)”, Pub. L. No. BGBl. I 2003 S. 310 (1909).

3.2.1 Megoldások bemutatása

A szabványok kigyűjtéséhez, illetve rendszerzéséhez az amerikai Nemzeti Közúti Közlekedésbiztonsági Hivatal által kiadott „Felkészülés a közlekedés jövőjére: Automatizált járművek 3.0” (AV 3.0)⁸² publikációt az Európai Unió Kiberbiztonsági Ügynökség (European Union Agency for Cybersecurity továbbiakban ENISA) által publikált „Az ENISA bevált gyakorlatai az intelligens autók biztonságára vonatkozóan” című kiadványt, valamint az összekapcsolt és önvezető járművekkel kapcsolatos adatbázist használtam fel.⁸³

A következő területekre találtam szabványi hivatkozásokat:

- Terminológiákkal és definíciókkal kapcsolatos szabványok;
- Fejlett vezetőt segítő rendszer funkciók;
- Csatlakozás;
- Emberi interakció;
- Járműfedélzeti rendszerek, hálózatok, adatokkal és interfészek;
- Mérnöki tevékenységek;
- Térkép szolgáltatás és helymeghatározás;
- Adatvédelem és Információbiztonság;
- Biztonság;
- Tesztelés, ellenőrzés és validálás.

Ezen 10 területen összesen 172 szabvány került azonosításra. Ezek a szabványok számos megközelítésből vizsgálják a témakört, és természetesen vannak olyan szabványok, amelyek egymásra épülnek vagy éppen átfedésben azonos területet szabályoznak más metodológiával.

A következő táblázatok sorolják fel tematizálva az egyes szabványokat.

3. táblázat Terminológiákkal és definíciókkal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Terminológiákkal és definíciókkal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/SAE PAS 22736	Intelligent transport systems – Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles	Intelligens közlekedési rendszerek - A közúti gépjárművek vezetésautomatizálási rendszereivel kapcsolatos kifejezések taxonómiája és fogalommeghatározásai	2021. augusztus 1.

⁸² U.S. Department of Transportation, *Preparing for the Future of Transportation: Automated Vehicles 3.0.*

⁸³ „Connected Automated Driving | Homepage”, elérés 2022. április 10., <https://www.connectedautomateddriving.eu/>.

Terminológiákkal és definíciókkal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/TR 21718:2019	Intelligent transport systems — Spatio-temporal data dictionary for cooperative ITS and automated driving systems 2.0	Intelligens közlekedési rendszerek – Tér-idő adatszótár együttműködő ITS-ekhez és automatizált vezetési rendszerekhez 2.0	2019. január 1.
SAE_J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles	A közúti gépjárművek vezetésautomatizálási rendszereivel kapcsolatos fogalmak taxonómiája és fogalommeghatározásai	2018. június 1.
SAE J2735D	Dedicated Short Range Communications (DSRC) Message Set Dictionary	Rövid hatótávolságú dedikált kommunikációs (DSRC) üzenetkészlet szótár	2016. március 1.
J3216_202005	Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles	A közúti gépjárművek kooperatív vezetésautomatizálási rendszereivel kapcsolatos fogalmak taxonómiája és fogalommeghatározásai	2020. május 7.
PAS 1883:2020	Operational design domain (ODD) taxonomy for an automated driving system (ADS). Specification	Működtetési tervezési terület (ODD) taxonómia az automatizált vezetési rendszerhez (ADS). Specifikáció	2020. augusztus 1.

4. táblázat Fejlett vezető segítő rendszer funkciókkal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Fejlett vezető segítő rendszer funkciókkal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO 22737:2021	Intelligent transport systems — Low-speed automated driving (LSAD) systems for predefined routes — Performance requirements, system requirements and performance test procedures	Intelligens közlekedési rendszerek - Alacsony sebességű automatizált vezetési rendszerek (LSAD) előre meghatározott útvonalakon - Teljesítménykövetelmények, rendszerkövetelmények és teljesítményvizsgálati eljárások	2021. július 1.
ISO 21202:2020	Intelligent transport systems — Partially automated lane change systems (PALS) — Functional / operational requirements and test procedures	Intelligens közlekedési rendszerek - Részben automatizált sávváltó rendszerek (PALS) - Funkcionális/működési követelmények és vizsgálati eljárások	2020. április 1.
ISO 21717:2018	Intelligent transport systems — Partially Automated In-Lane Driving Systems (PADS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Részlegesen automatizált sávon belüli vezetési rendszerek (PADS) - Teljesítménykövetelmények és vizsgálati eljárások	2018. szeptember 1.
ISO 16787:2017	Intelligent transport systems — Assisted Parking System (APS) — Performance	Intelligens közlekedési rendszerek - Parkolássegítő rendszer (APS) -	2017. december 1.

Fejlett vezetőt segítő rendszer funkciókkal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
	requirements and test procedure	Teljesítménykövetelmények és vizsgálati eljárás	
ISO 20035	ITS – Cooperative adaptive cruise control systems	ITS - Együttműködő adaptív sebességtartó automatika rendszerek	2019. január 1.
ISO 19638	ITS – Road boundary departure prevention systems	ITS - Úthatárelhagyást megelőző rendszerek	2018. szeptember 1.
SAE J3045	Truck & bus lane departure warning systems test procedure	Teherautó- és buszsávelhagyásra figyelmeztető rendszerek vizsgálati eljárása	2018. szeptember 1.
ETSI TS 101 539	Intersection collision risk warning	A kereszteződések ütközésveszélyére való figyelmeztetés	2018. június 1.
PAS 1880:2020	Guidelines for developing and assessing control systems for automated vehicles	Iránymutatások az automatizált járművek vezérlőrendszereinek fejlesztéséhez és értékeléséhez	2020. február 28.
J3171_201911	Identifying Automated Driving Systems-Dedicated Vehicles (ADS-DVs) Passenger Issues for Persons with Disabilities	Automatizált vezetési rendszerek által létrejött járművek (ADS-DV) fogyatékkal élő utasokkal kapcsolatos problémák számára	2019. november 19.
ISO 19237:2017	Intelligent transport systems — Pedestrian detection and collision mitigation systems (PDCMS) — Performance requirements and test	Intelligens közlekedési rendszerek - Gyalogosfelismerő és ütközéscsökkentő rendszerek (PDCMS) - Teljesítménykövetelmények és vizsgálat	2017. december 1.
ISO 22078:2020	Intelligent transport systems — Bicyclist detection and collision mitigation systems (BDCMS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Kerékpáros-érzékelő és ütközéscsökkentő rendszerek (BDCMS) - Teljesítménykövetelmények és vizsgálati eljárások	2020. február 1.
ISO 15622:2018	Intelligent transport systems — Adaptive cruise control systems — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Adaptív sebességtartó automatika - Teljesítménykövetelmények és tesztelési eljárások	2018. szeptember 1.
ISO 20900:2019	Intelligent transport systems — Partially automated parking systems (PAPS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Részben automatizált parkolási rendszerek (PAPS) - Teljesítménykövetelmények és vizsgálati eljárások	2019. május 1.
ISO 11067:2015	Intelligent transport systems — Curve speed warning systems (CSWS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Kanyarsebességre figyelmeztető rendszerek (CSWS) - Teljesítménykövetelmények és vizsgálati eljárások	2015. július 1.

Fejlett vezetőt segítő rendszer funkciókkal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO 11270:2014	Intelligent transport systems — Lane keeping assistance systems (LKAS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Sávtartó segédrendszerek (LKAS) - Teljesítménykövetelmények és vizsgálati eljárások	2014. május 1.
ISO 15623:2013	Intelligent transport systems — Forward vehicle collision warning systems — Performance requirements and test procedures	Intelligens közlekedési rendszerek — Elülső járművel való ütközésre figyelmeztető rendszerek — Teljesítménykövetelmények és vizsgálati eljárások	2013. július 1.
ISO 17361:2017	Intelligent transport systems — Lane departure warning systems — Performance requirements and test procedures	Intelligens közlekedési rendszerek – Sávelhagyásra figyelmeztető rendszerek – Teljesítménykövetelmények és vizsgálati eljárások	2017. június 1.
ISO 17386:2010	Transport information and control systems — Manoeuvring Aids for Low Speed Operation (MALSO) — Performance requirements and test procedures	Közlekedési információs és ellenőrző rendszerek - Manőverezést segítő rendszerek alacsony sebességű üzemmódban (MALSO) - Teljesítménykövetelmények és vizsgálati eljárások	2010. március 1.
ISO 17387:2008	Intelligent transport systems — Lane change decision aid systems (LCDAS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek - Sávváltást segítő rendszerek (LCDAS) - Teljesítménykövetelmények és vizsgálati eljárások	2008. május 1.
ISO 22839:2013	Intelligent transport systems — Forward vehicle collision mitigation systems — Operation, performance, and verification requirements	Intelligens közlekedési rendszerek - Elülső járművel való ütközést mérséklő rendszerek - Működési, teljesítmény- és ellenőrzési követelmények	2013. június 1.
ISO 22840:2010	Intelligent transport systems — Devices to aid reverse manoeuvres — Extended-range backing aid systems (ERBA)	Intelligens közlekedési rendszerek - Tolatási manővereket segítő eszközök - Kiterjesztett hatótávolságú tolatást segítő rendszerek (ERBA)	2010. április 1.
ISO 26684:2015	Intelligent transport systems (ITS) — Cooperative intersection signal information and violation warning systems (CIWS) — Performance requirements and test procedures	Intelligens közlekedési rendszerek (ITS) – Együttműködő kereszteződésjelző-információs és szabálysértési figyelmeztető rendszerek (CIWS) – Teljesítménykövetelmények és vizsgálati eljárások	2015. május 1.
SAE J3114	Human Factors Definitions for Automated Driving and Related Research Topics	Az automatizált vezetés emberi tényezőinek meghatározása és kapcsolódó kutatási témák	2016. december 1.
AUTOSAR	AUTomotive Open System Architecture	AUTomotive nyílt rendszerarchitektúra	2020. november 1.

5. táblázat Csatlakozással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ETSI GS MEC 013 V2.1.1	Multi-access Edge Computing (MEC); Location API	többszörös hozzáférésű peremhálózati számítástechnika (MEC); helymeghatározó API	2019. szeptember 1.
ETSI GS MEC 030 V2.1.1	Multi-access Edge Computing (MEC); V2X Information Service API	többszörös hozzáférésű peremhálózati számítástechnika többszörös hozzáférésű peremhálózati számítástechnika- V2X információk szolgáltatás API	2020. április 1.
ETSI TR 102 638 V1.1.1	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions	Intelligens közlekedési rendszerek (ITS); járműkommunikáció; alapvető alkalmazások; Fogalommeghatározások	2009. június 1.
ETSI TR 103 300-1 V2.2.1	Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 1: Use Cases definition; Release 2	Intelligens közlekedési rendszerek (ITS); a veszélyeztetett úthasználók tudatossága; 1. rész: Használati esetek meghatározása; 2. kiadás	2021. április 1.
ETSI TS 103 300-2 V2.2.1	Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2	Intelligens közlekedési rendszerek (ITS); a veszélyeztetett úthasználók (VRU) tudatossága; 2. rész: Funkcionális architektúra és követelmények meghatározása; 2. kiadás	2021. április 2.
ETSI TS 103 300-3 V2.1.2	Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2	Intelligens közlekedési rendszerek (ITS); A veszélyeztetett úthasználók tudatossága; 3. rész: A veszélyeztetett úthasználók tudatossága alapszolgáltatás specifikációja; 2. kiadás.	2021. április 3.
NEMA TS 10-2020	Connected vehicle infrastructure- roadside equipment	Összekapcsolt jármű- infrastruktúra – közút menti berendezések	2020. március 1.
CEN ISO/TS 19468	Intelligent transport systems – Data interfaces between centers for transport information and control system	Intelligens közlekedési rendszerek - Adatkapcsolatok a közlekedési információk és irányítási központok között.	2019. október 1.
IEEE 1609.12	IEEE standard for wireless access in vehicular environments (WAVE) – Identifiers	IEEE-szabvány a vezeték nélküli hozzáféréshez járműkörnyezetben (WAVE) - Azonosítók	2019. szeptember 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
CEN ISO/TS 19091	Intelligent transport systems – Cooperative ITS – Using V2I and I2V communications for application related to signalized intersections	Intelligens közlekedési rendszerek – Együttműködő ITS – V2I és I2V kommunikáció használata a jelzett kapcsolatos alkalmazásokhoz	2019. július 1.
IEEE 1609.2b	IEEE standard for wireless access to vehicular environment	IEEE-szabvány a járműkörnyezetben történő vezetékek nélküli hozzáféréshez	2019. július 1.
CEN/TR 17297-1	Intelligent transport systems – Location referencing harmonization for urban ITS – Part 1: State of the art and guidelines	Intelligens közlekedési rendszerek - Helymegjelölés-harmonizáció városi ITS-hez. 1. rész: A technika állása és iránymutatások	2019. május 1.
ISO 20078-3	Road vehicles – Extended vehicle (ExVe) web services – Part 3: Security	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 3. rész: Biztonság	2019. május 1.
ISO 20080	Road vehicles – Information for remote diagnostic support	Közúti járművek. Távoli diagnosztikai támogatáshoz szükséges információk	2019. március 1.
ISO 20078-2	Road vehicles – Extended vehicle (ExVe) web services – Part 2: Access	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 2. rész: Hozzáférés	2019. február 1.
ISO 20078-1	Road vehicles – Extended vehicle (ExVe) web services – Part 1: Content	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 1. rész: Tartalom	2019. február 1.
SAE J2945/2	DSRC performance requirements for V2V safety awareness	DSRC teljesítménykövetelmények a V2V biztonsághoz	2018. október 1.
ETSI TS 138 522	5G; NR; User equipment conformance specification	5G; NR; felhasználói berendezésekre vonatkozó megfeleléségi előírás	2018. október 1.
ETSI TS 102 965	Intelligent transport systems; application object identifier	Intelligens közlekedési rendszerek; alkalmazási objektum-azonosító	2018. július 1.
ETSI TR 121 914	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Release description; Release 14	Digitális cellás távközlési rendszer (2+ fázis) (GSM); Univerzális Mobil Távközlési Rendszer (UMTS); LTE; 5G; kiadás leírása; 14. kiadás	2018. június 1.
ETSI TS 124 386	LTE; User equipment to V2X control function	LTE; A felhasználói berendezés és a V2X vezérlőfunkció közötti kapcsolat	2018. június 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO 20077-1: 2017	Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information	Közúti járművek - Kiterjesztett jármű (ExVe) módszertan - 1. rész: Általános információk	2017. december 1.
SAE J2945	Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts	A dedikált rövid hatótávolságú kommunikáció (DSRC) rendszertervezési folyamatának iránymutatása az SAE J2945/X dokumentumaihoz és a közös tervezési koncepciókhoz	2017. december 1.
ISO 20077-2	Road Vehicles — Extended vehicle (ExVe) methodology — Part 2: Methodology for designing the extended vehicle	Közúti járművek - Kiterjesztett jármű (ExVe) módszertan - 2. rész: Módszertan a kiterjesztett jármű tervezéséhez	2017. december 1.
ETSI TS 122 185	LTE; Service requirements for V2X services	LTE; A V2X-szolgáltatások szolgáltatási követelményei	2017. március 1.
ETSI EN 302 571 v2.1.1	Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band	Intelligens közlekedési rendszerek (ITS); Az 5 855 MHz-5 925 MHz frekvenciasávban működő rádiótávközlési berendezések	2017. február 1.
J3067_202010	Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary (SAE J2735) Using Systems Engineering Methods	A dedikált rövid hatótávolságú kommunikációs (DSRC) üzenetkészlet szótárának [SAE J2735] rendszertechnikai módszerekkel történő javítására irányuló javaslatok	2020. október 6.
J2735_202007	V2X Communications Message Set Dictionary™	V2X kommunikációs üzenetkészlet szótár	2006. december 19.
J2945/1A_202007	Vehicle Level Validation Test Procedures for V2V Safety Communications	Járműszintű validálási teszteljárások a V2V biztonsági kommunikációhoz	2020. július 8.
J2945/2A_201907	Dedicated Short Range Communications (DSRC) Performance Requirements for V2V Safety Awareness™ ASN File	dedikált rövid hatótávolságú kommunikációs (DSRC) teljesítménykövetelményi a V2V biztonságához	2019. július 1.
ETSI GR IP6 030	IPv6-based Vehicular Networking (V2X)	IPv6-alapú járműhálózat (V2X)	2020. október 1.
ETSI TR 103 496	Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS) support for transport pollution management applications; Use cases and standardization study	Intelligens Közlekedési Rendszerek (ITS); Kooperatív ITS (C-ITS) támogatás a közlekedési szennyezés-kezelési alkalmazásokhoz; Felhasználási esetek és	2020. október 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		szabványosítási tanulmány	
ETSI EN 302 890-2	Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2	Intelligens Közlekedési Rendszerek (ITS); Létesítmény szintű funkció; 2. rész: Pozíció- és időkezelés (PoTi); 2. kiadás	2020. augusztus 1.
ETSI TS 122 185	LTE; Service requirements for V2X services	LTE; A V2X-szolgáltatások szolgáltatási követelményei	2020. augusztus 2.
ISO-20078-1: 2019	Road vehicles — Extended vehicle (ExVe) web services — Part 1: Content	Közúti járművek - Kiterjesztett jármű (ExVe) webes szolgáltatások - 1. rész: Tartalom	2019. február 1.
ISO-20078-2: 2019	Road vehicles — Extended vehicle (ExVe) web services — Part 2: Access	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 2. rész: Hozzáférés	2019. február 1.
ISO/PRF 21217:2020	Intelligent transport systems — Station and communication architecture	Intelligens közlekedési rendszerek - Állomás és kommunikációs architektúra	2020. december 1.
ISO-20078-3: 2019	Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 3. rész: Biztonság	2019. május 1.
ISO-20078-4: 2019	Road vehicles — Extended vehicle (ExVe) web services — Part 4: Control	Közúti járművek - Kiterjesztett jármű (ExVe) webszolgáltatások - 4. rész: Irányítás	2019. április 1.
ISO 23132:2020	Road vehicles — Extended Vehicle (ExVe) time critical applications — General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)	Közúti járművek - Kiterjesztett jármű (ExVe) időkritikus alkalmazások - A közúti és exVe biztonsággal (RExVeS) kapcsolatos időszűkös helyzetek általános követelményei, fogalommeghatározásai és osztályozási módszertana	2020. július 1.
ETSI TR 138 900	Study on channel model for frequency spectrum above 6 GHz	Tanulmány a 6 GHz feletti frekvenciaspektrum csatornamodelljéről	2018. július 1.
ETSI TR 138 185	Security aspect for LTE support of Vehicle-to-Everything (V2X) services	Biztonsági aspektusa az LTE technológiával támogatott jármű és környezete (V2X) kapcsolódási szolgáltatáshoz	2020. augusztus 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ETSI TR 121 914	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G;	Digitális cellás távközlési rendszer (2+ fázis) (GSM); Univerzális mobil távközlési rendszer (UMTS); LTE; 5G;	2018. október 17.
ETSI EN 302 895	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)	Intelligens közlekedési rendszerek (ITS); járműkommunikáció; alapvető alkalmazási készlet; helyi dinamikus térkép (LDM)	2014. szeptember 1.
ETSI EN 302 686	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 63 GHz to 64 GHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive	Intelligens közlekedési rendszerek (ITS); A 63-64 GHz-es frekvenciasávban működő rádiótávközlési berendezések; Az R&TTE-irányelv 3.2. cikkének alapvető követelményeit tartalmazó harmonizált európai szabvány (EN).	2011. február 1.
ETSI EN 302 663	Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	Intelligens közlekedési rendszerek (ITS); ITS-G5 Hozzáférési réteg specifikáció az intelligens közlekedéshez 5 GHz-es frekvenciasávban működő intelligens közlekedési rendszerek	2019. május 1.
EN 302 571	Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band	Az 5 855 MHz-5 925 MHz frekvenciasávban működő rádiótávközlési berendezések	2017. február 1.
ETSI EN 302 637-2 V1.4.1	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	Intelligens közlekedési rendszerek (ITS); Járműkommunikáció; Alkalmazások alapkészlete; 2. rész: A kooperatív tudatossági alapszolgáltatás specifikációja	2019. január 1.
ETSI EN 302 637-3 V1.3.1	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	Intelligens közlekedési rendszerek (ITS); Járműkommunikáció; Alapvető alkalmazások; 3. rész: Decentralizált környezeti értesítési alapszolgáltatás specifikációja.	2019. április 1.
ETSI TS 102 894-2 V1.3.1	Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	Intelligens közlekedési rendszerek (ITS); Felhasználói és alkalmazási követelmények; 2. rész: Alkalmazások és létesítmények rétegének közös adatszótára	2018. augusztus 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ETSI EN 302 665 V1.1.1	Intelligent Transport Systems (ITS); Communications Architecture	Intelligens közlekedési rendszerek (ITS); Kommunikációs architektúra	2010. szeptember 1.
ETSI TS 102 792 V1.2.1	Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range	Intelligens közlekedési rendszerek (ITS); Az európai CEN dedikált rövid hatótávolságú kommunikációs berendezések (CEN DSRC) és az 5 GHz-es frekvenciatartományban működő intelligens közlekedési rendszerek (ITS) közötti interferencia elkerülésére szolgáló zavarcsökkentési technikák.	2015. június 1.
ETSI TS 103 301 V1.3.1	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	Intelligens közlekedési rendszerek (ITS); járműkommunikáció; Alkalmazások alapkészlete; infrastruktúra-szolgáltatások eszközszintű protokolljai és kommunikációs követelményei	2020. február 1.
ISO/TS 19321:2020	Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures	Intelligens közlekedési rendszerek - Kooperatív ITS - A járműfedélzeti információs (IVI) adatszerkezetek szótára	2020. szeptember 1.
ETSI EN 302 636-5-1 V2.2.1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	Intelligens közlekedési rendszerek (ITS); Járműkommunikáció; GeoNetworking; 5. rész: Közlekedési protokollok; 1. alrész: Alapvető közlekedési protokollok	2019. május 1.
ETSI EN 302 636-4-1 V1.4.1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	Intelligens közlekedési rendszerek (ITS); Járműkommunikáció; GeoNetworking; 4. rész: Földrajzi címzés és továbbítás pont-pont és pont-többpont kommunikációhoz; 1. alrész: Médiafüggetlen funkcionalitás	2019. november 1.
IEEE 1609.4	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation	IEEE-szabvány a vezeték nélküli hozzáférés járműkörnyezetben (WAVE) - Többcsatornás működés	2016. január 1.
IEEE 1609.3	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services	IEEE-szabvány a vezeték nélküli hozzáféréshez járműves környezetben (WAVE) -- Hálózati	2016. január 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		szolgáltatások	
ETSI EN 303 613	Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	LTE-V2X Hozzáférési réteg specifikációja az 5 GHz-es frekvenciasávban működő intelligens közlekedési rendszerek számára	2020. január 1.
ISO 17515-3:2019	Intelligent transport systems — Evolved-universal terrestrial radio access network — Part 3: LTE-V2X	Intelligens közlekedési rendszerek. Fejlett-univerzális földfelszíni rádió-hozzáférési hálózat. 3. rész: LTE-V2X	2019. augusztus 1.
ISO 17427-1:2018	Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co- operative ITS architecture(s)	Intelligens közlekedési rendszerek - Kooperatív ITS - 1. rész: Szerepek és felelősségi körök az együttműködő ITS- architektúra(k) keretében	2018. június 1.
ISO 17419:2018	Intelligent transport systems — Cooperative systems — Globally unique identification	Intelligens közlekedési rendszerek - Együttműködő rendszerek - Globálisan egyeti azonosítás	2018. május 1.
ISO 17423:2018	Intelligent transport systems — Cooperative systems — Application requirements and objectives	Intelligens közlekedési rendszerek - Együttműködő rendszerek - Alkalmazási követelmények és célkitűzések	2018. május 1.
ISO 24102 (part 1- 6)	Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management	Intelligens közlekedési rendszerek - Kommunikációs hozzáférés szárazföldi mobilok számára (CALM) - ITS-állomáskezelés	2018. január 1.
ISO/TS 17429:2017	Intelligent transport systems — Cooperative ITS — ITS station facilities for the transfer of information between ITS stations	Intelligens közlekedési rendszerek - Együttműködő ITS - ITS-állomások közötti információátadásra szolgáló ITS-állomási létesítmények	2017. március 1.
ISO/TR 13185- 1:2012	Intelligent transport systems — Vehicle interface for provisioning and support of ITS services — Part 1: General information and use case definition	Intelligens közlekedési rendszerek - Jármű-interfész az ITS-szolgáltatások nyújtásához és támogatásához - 1. rész: Általános információk és használati esetek meghatározása	2012. május 1.
ISO 13185-2:2015	Intelligent transport systems — Vehicle interface for provisioning and support of ITS services — Part 2: Unified gateway protocol (UGP) requirements and specification for	Intelligens közlekedési rendszerek - Jármű interfész ITS-szolgáltatások nyújtásához és támogatásához - 2. rész: Az egységes átjáró	2015. április 1.

Csatlakozással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
	vehicle ITS station gateway (V-ITS-SG) interface	protokoll (UGP) követelményei és a jármű ITS-állomás átjáró (V-ITS-SG) interfész specifikációja.	
ISO 13185-3:2018	Intelligent transport systems — Vehicle interface for provisioning and support of ITS Services — Part 3: Unified vehicle interface protocol (UVIP) server and client API specification	Intelligens közlekedési rendszerek - Jármű interfész ITS-szolgáltatások nyújtásához és támogatásához - 3. rész: Az egységesített jármű interfész protokoll (UVIP) szerver és ügyfél API specifikációi	2018. június 1.
ISO 13185-4:2020	Intelligent transport systems — Vehicle interface for provisioning and support of ITS Services — Part 4: Unified vehicle interface protocol (UVIP) conformance test specification	Intelligens közlekedési rendszerek - Jármű interfész ITS-szolgáltatások nyújtásához és támogatásához - 4. rész: Az egységesített jármű-interfész protokoll (UVIP) megfelelési tesztelési specifikációja.	2020. május 1.
ISO 14813-1:2015	Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 1: ITS service domains, service groups and services	Intelligens közlekedési rendszerek - Referenciamodell-architektúra(k) az ITS-ágazat számára - 1. rész: ITS-szolgáltatási területek, szolgáltatáscsoportok és szolgáltatások.	2015. október 1.
ISO 14813-5:2020	Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 5: Requirements for architecture description in ITS standards	Intelligens közlekedési rendszerek - Referenciamodell architektúra(k) az ITS-ágazat számára - 5. rész: Az architektúra leírására vonatkozó követelmények az ITS-szabványokban.	2020. január 1.
ISO 14813-6:2017	Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 6: Use of ASN.1	Intelligens közlekedési rendszerek - Referenciamodell-architektúra(k) az ITS-ágazat számára - 6. rész: Az ASN.1 használata	2017. november 1.

6. táblázat Emberi interakcióval kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Emberi interakcióval kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma

Emberi interakcióval kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/TR 21959-1:2020	Road vehicles — Human performance and state in the context of automated driving — Part 1: Common underlying concepts	Közúti járművek - Az emberi teljesítmény és állapot az automatizált vezetés összefüggésében - 1. rész: Közös alapfogalmak	2020. január 1.
ISO/TR 21959-2:2020	Road vehicles — Human performance and state in the context of automated driving — Part 2: Considerations in designing experiments to investigate transition processes	Közúti járművek - Az emberi teljesítmény és állapot az automatizált vezetés összefüggésében - 2. rész: Az átmeneti folyamatok vizsgálatára irányuló kísérletek tervezési szempontjai	2020. február 1.
ISO/TR 23049:2018	Road Vehicles — Ergonomic aspects of external visual communication from automated vehicles to other road users	Közúti járművek - Az automatizált járművek által más úthasználókkal folytatott külső vizuális kommunikáció ergonómiai szempontjai	2018. szeptember 1.
ISO 15007:2020	Road vehicles — Measurement and analysis of driver visual behaviour with respect to transport information and control systems	Közúti járművek - A járművezetők vizuális viselkedésének mérése és elemzése a közlekedési információs és vezérlőrendszerekkel kapcsolatban	2020. augusztus 1.

7. táblázat Járműfedélzeti rendszerekkel, hálózatokkal, adatokkal és interfészekkel kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Járműfedélzeti rendszerekkel, hálózatokkal, adatokkal és interfészekkel kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/DIS 23150	Road vehicles — Data communication between sensors and data fusion unit for automated driving functions — Logical interface	Közúti járművek - Adatkommunikáció az érzékelők és az adatfúziós egység között az automatizált vezetési funkciókhoz - Logikai interfész	2021. május 1.
SAE J3134	Automated driving system marking lights	Automatizált vezetési rendszer jelölőfényei	2019. május 1.
SAE J3197	Automated Driving System Data Logger	Automatizált vezetési rendszer adatgyűjtője	2020. április 11.
ISO 21111 -1-10	Road vehicles — In-vehicle Ethernet — Part 1 - 10	Közúti járművek - Járműfedélzeti Ethernet - 1. rész - 10	2020. október 1.

8. táblázat Mérnöki tevékenységekkel kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Mérnöki tevékenységekkel kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/TR 20545:2017	Intelligent transport systems — Vehicle/roadway warning and control systems — Report on standardisation for vehicle automated driving systems (RoVAS)/Beyond driver assistance systems	Intelligens közlekedési rendszerek - Járművek/útvonalak figyelmeztető és ellenőrző rendszerei - Jelentés a járművek automatizált vezetési rendszereinek (RoVAS)/a vezetőtámogató rendszereken túli rendszerek szabványosításáról	2017. július 1.
CEN/TS 17400:2020	Intelligent transportation systems – Urban ITS – Mixed vendor environments, methodologies & translators	Intelligens közlekedési rendszerek - Városi ITS - Vegyes szállítói környezetek, módszertanok és fordítók	2020. április 15.

9. táblázat Térképpel szolgáltatással és helymeghatározással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Térkép szolgáltatással és helymeghatározással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO 20524-2:2020	Intelligent transport systems — Geographic Data Files (GDF) GDF5.1 — Part 2: Map data used in automated driving systems, Cooperative ITS, and multi-modal transport	Intelligens közlekedési rendszerek - Földrajzi adatfájlok (GDF) GDF5.1 - 2. rész: Automatizált vezetési rendszerekben, kooperatív ITS-ben és multimodális közlekedésben használt térképi adatok	2020. november 1.
EN 16803-1	Space – Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) – Part 1: Definitions and system engineering procedures for the establishment and assessment of performances	Intelligens közlekedési rendszerek - Földrajzi adatfájlok (GDF) GDF5.1 - 2. rész: Automatizált vezetési rendszerekben, kooperatív ITS-ben és multimodális közlekedésben használt térképi adatok	2016. október 1.
ETSI TS 103 246-1	Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 1: Functional requirements	Műholdas földi állomások és rendszerek (SES); GNSS-alapú helymeghatározó rendszerek; 1. rész: Funkcionális követelmények	2020. október 1.
ISO 14296:2016	Intelligent transport systems — Extension of map database specifications for applications of cooperative IST	Intelligens közlekedési rendszerek. A térképadatbázisokra vonatkozó előírások kiterjesztése a	2016. február 1.

Térkép szolgáltatással és helymeghatározással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		kooperatív IST alkalmazásaihoz.	
ISO 14825:2011	Intelligent transport systems — Geographic Data Files (GDF) — GDF5.0	Intelligens közlekedési rendszerek - Földrajzi adatfájlok (GDF) - GDF5.0	2011. július 1.
ISO 18750:2018	Intelligent transport systems — Co-operative ITS — Local dynamic map	Intelligens közlekedési rendszerek - Együttműködő ITS - Helyi dinamikus térképek	2018. május 1.
ISO 17572-1:2015	Intelligent transport systems (ITS) — Location referencing for geographic databases — Part 1: General requirements and conceptual model	Intelligens közlekedési rendszerek (ITS) - Helymegjelölés földrajzi adatbázisokhoz. 1. rész: Általános követelmények és fogalmi modell	2015. január 1.
ISO 17572-2:2018	Intelligent transport systems (ITS) — Location referencing for geographic databases — Part 2: Pre-coded location references (pre-coded profile)	Intelligens közlekedési rendszerek (ITS) - Helymegjelölés földrajzi adatbázisokhoz - 2. rész: Előre kódolt helymegjelölések (előre kódolt profil)	2018. szeptember 1.
ISO 17572-3:2015	Intelligent transport systems (ITS) — Location referencing for geographic databases — Part 3: Dynamic location references (dynamic profile)	Intelligens közlekedési rendszerek (ITS) - Helymegjelölés földrajzi adatbázisokhoz - 3. rész: Dinamikus helymegjelölések (dinamikus profil)	2015. január 1.
ISO 17572-4:2020	Intelligent transport systems (ITS) — Location referencing for geographic databases — Part 4: Precise relative location references (precise relative profile)	Intelligens közlekedési rendszerek (ITS) - Helymegjelölés földrajzi adatbázisokhoz - 4. rész: Pontos relatív helymegjelölés (pontos relatív profil)	2020. április 1.

10. táblázat Adatvédelemmel és Információbiztonsággal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Adatvédelemmel és Információbiztonsággal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO/SAE DIS 21434:2021	Road vehicles – Cybersecurity engineering	Közúti járművek - Kiberbiztonsági mérnöki tevékenység	2021. augusztus 1.
ISO/TS 21177:2019	Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices	Intelligens közlekedési rendszerek - ITS-állomásbiztonsági szolgáltatások a megbízható eszközök közötti biztonságos munkamenet létrehozásához és hitelesítéséhez	2019. augusztus 1.
CEN ISO/TS 21177	Intelligent transport systems – ITS station security services for secure session establishment and authentication between trusted	Intelligens közlekedési rendszerek - ITS-állomásbiztonsági szolgáltatások a megbízható	2019. október 2.

Adatvédelemmel és Információbiztonsággal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
	devices	eszközök közötti biztonságos munkamenet létrehozásához és hitelesítéséhez	
BSI PAS 1885	Fundamental principles of automotive cyber security	A gépjárművek kiberbiztonságának alapelvei	2018. december 1.
BSI PAS 11281	Connected automotive ecosystems. Impact of security on safety. Code of practice.	Összekapcsolt gépjármű-ökoszisztémák. A biztonság hatása a biztonságra. Gyakorlati kódex.	2018. december 1.
SAE J3061	Cybersecurity guidebook for Cyber-Physical vehicle Systems	Kiberbiztonsági útmutató a kiber-fizikai járműrendszerekhez	2016. január 1.
ETSI TR 103 460	Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehaviour Detection; Release 2	Intelligens közlekedési rendszerek (ITS); Biztonság; szabványosítás előtti tanulmány a hibás viselkedés észleléséről; 2. kiadás	2020. október 1.
ETSI TS 103 097 V1.4.1	Intelligent Transport Systems (ITS); Security; Security header and certificate formats	Intelligens közlekedési rendszerek (ITS); Biztonság; Biztonsági fejléc- és tanúsítványformátumok	2020. október 1.

11. táblázat Biztonsággal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Biztonsággal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
AVSC00007202 107	AVSC Information Report for Adapting a Safety Management System (SMS) for Automated Driving System (ADS) SAE Level 4 and 5 Testing and Evaluation	AVSC tájékoztató jelentés a biztonságirányítási rendszer (SMS) automatizált vezetési rendszerek (ADS) SAE 4. és 5. szintű teszteléséhez és értékeléséhez való hozzáigazításáról	2021. július 1.
ISO/CD TR 4804:2020	Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation methods	Közúti járművek - Automatizált vezetési rendszerek biztonsága és kiberbiztonsága - Tervezési, ellenőrzési és validálási módszerek	2020. december 1.
UL 4600	A safety standard governing self-driving cars	Az önvezető autókra vonatkozó biztonsági szabvány	2020. április 1.
ISO/PAS 21448	Road vehicles – Safety of the intended functionality	Közúti járművek - A tervezett funkciók biztonsága	2019. január 1.
ISO 26262-11	Road vehicles – Functional safety – Part 11: Guidelines on application of ISO 26262 to semiconductors	Közúti járművek - Funkcionális biztonság. 11. rész: Irányelvek az ISO 26262 félvezetőkre történő alkalmazásához.	2018. december 1.

Biztonsággal kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ISO 26262-10	Road vehicles – Functional safety – Part 10: Guidelines on ISO 26262	Közúti járművek. Funkcionális biztonság. 10. rész: Iránymutatások az ISO 26262 szabványhoz.	2018. december 1.
ISO 26262-9	Road vehicles – Functional safety – Part 9: Automotive safety integrity level (ASIL) – oriented and safety-oriented analyses	Közúti járművek - Funkcionális biztonság - 9. rész: Autóipari biztonsági integritási szint (ASIL) - orientált és biztonságorientált elemzések	2018. december 1.
ISO 26262-7	Road vehicles – Functional safety – Part 7: Production, operation, service and decommissioning	Közúti járművek. Funkcionális biztonság. 7. rész: Gyártás, üzemeltetés, szervizelés és leszerelés.	2018. december 1.
ISO 26262-6	Road vehicles – Functional safety – Part 6: Product development at the software level	Közúti járművek. Funkcionális biztonság. 6. rész: Termékfejlesztés a szoftver szintjén.	2018. december 1.
ISO 26262-5	Road vehicles – Functional safety – Part 5: Product development at the hardware level	Közúti járművek - Funkcionális biztonság - 5. rész: Termékfejlesztés a hardver szintjén	2018. december 1.
ISO 26262-4	Road vehicles – Functional safety – Part 4: Product development of the system	Közúti járművek - Funkcionális biztonság - 4. rész: A rendszer termékfejlesztése	2018. december 1.
ISO 26262-3	Road vehicles – Functional safety – Part 3: Concept phase	Közúti járművek - Funkcionális biztonság - 3. rész: Konceptiófázis	2018. december 1.
ISO 26262-2	Road vehicles – Functional safety – Part 2: Management of functional safety	Közúti járművek - Funkcionális biztonság - 2. rész: A funkcionális biztonság irányítása	2018. december 1.
ISO 26262-1	Road vehicles – Functional safety – Part 1: Vocabulary	Közúti járművek - Funkcionális biztonság - 1. rész: Fogalomtár	2018. december 1.
PAS 1881:2020	Assuring safety for autonomous vehicle trials and testing	A biztonság biztosítása az autonóm járművek kísérletei és tesztelése során	2020. február 27.

12. táblázat Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, <https://www.connectedautomateddriving.eu/>)

Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
ASAM OpenDRIVE	Open Dynamic Road Information for Vehicle Environment	Nyílt dinamikus útinformáció a	2021. augusztus 3.

Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		járműkörnyezet számára	
OGC CityGML	Open Geospatial Consortium - City Geographic Markup Language	Nyílt térinformatikai konzorcium - Városi földrajzi jelölőnyelv	2019. december 1.
Khronos glTF	Khronos Graphic Language transmission format	Khronos Graphic Language adatátviteli formátum	2021. július 1.
ASAM OpenSCENARIO	ASAM Open Scenario	ASAM nyílt forgatókönyv	2021. március 19.
ASAM OSI	ASAM Open Simulation Interface	ASAM nyílt szimulációs interfész	2021. március 16.
FMI	Functional Mock-up Interface	Funkcionális minta darab interfész	2021. július 1.
SSP	System Structure and Parametrization	Rendszerkezet és paraméterezés	2019. március 5.
ASAM XIL	Generic Simulator Interface for testing purpose	Általános szimulátor interfész tesztelési célokra	2020. március 13.
DCP	Distributed Co-Simulation Protocol	Elosztott társ-szimulációs protokoll	2019. március 1.
SAE J3206	Taxonomy and Definition of Safety Principles for Automated Driving System (ADS)	Az automatizált vezetési rendszer (ADS) biztonsági elveinek taxonómiája és meghatározása	2021. július 7.
ASAM OTX Extensions	Open Test Sequence eXchange Format	Nyílt teszt sorozat-csere formátum	2020. szeptember 4.
ISO 13209-2:2012	Road vehicles — Open Test sequence eXchange format (OTX) — Part 2: Core data model specification and requirements	Közúti járművek - Nyílt teszt sorozat-csere formátum (OTX) - 2. rész: Az alapadatmodell specifikációja és követelményei	2012. augusztus 1.
ASAM MDF	ASAM Measurement Data Format	ASAM mérési adatformátum	2019. szeptember 30.
ASAM ODS	ASAM ODS (Open Data Services) focuses on the persistent storage and retrieval of testing data	Az ASAM ODS (nyílt adatszolgáltatások) a vizsgálati adatok tartós tárolására és visszakeresésére összpontosít.	2021. június 30.
AVSC00001201911	AVSC Best Practice for In-Vehicle Fallback Test Driver Selection, Training, and Oversight Procedures for Automated Vehicles Under Test	Az AVSC legjobb gyakorlata a járművön belüli tartalék teszteléshez A járművezető kiválasztása, képzése és a tesztelés alatt álló automatizált járművek felügyeleti eljárásai	2019. november 8.
SAE J3018	Guidelines for safe on-road testing of SAE level 3,4 and 5 prototype automated driving systems	Iránymutatások az SAE 3., 4. és 5. szintű automatizált vezetési rendszerek	2019. október 3.

Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		prototípusainak biztonságos közúti teszteléséhez	
CEN ISO/TS 21189	Intelligent transport systems – Cooperative ITS – Test requirements and protocol implementation conformance statement (PICS)	Intelligens közlekedési rendszerek - Együttműködő ITS - Vizsgálati követelmények és a protokoll megvalósításának megfelelési nyilatkozata (PICS)	2019. május 1.
ISO 19206-1:2018	Road vehicles — Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions — Part 1: Requirements for passenger vehicle rear-end targets	Közúti járművek. Céljárművek, veszélyeztetett úthasználók és egyéb objektumok vizsgálati eszközei az aktív biztonsági funkciók értékeléséhez. 1. rész: A személygépkocsik hátulról felhajtott célpontjaira vonatkozó követelmények	2018. december 1.
ISO 19206-2:2018	Road vehicles — Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions — Part 2: Requirements for pedestrian targets	Közúti járművek - Céljárművek, veszélyeztetett úthasználók és egyéb objektumok vizsgálati eszközei az aktív biztonsági funkciók értékeléséhez. 2. rész: Gyalogos célpontokra vonatkozó követelmények	2018. december 1.
ISO 19206-4	Road vehicles — Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions — Part 4: Requirements for bicyclist targets	Közúti járművek. Céljárművek, veszélyeztetett úthasználók és egyéb tárgyak vizsgálati eszközei az aktív biztonsági funkciók értékeléséhez. 4. rész: Kerékpáros célpontokra vonatkozó követelmények	2020. november 1.
ISO 19364:2016	Passenger cars — Vehicle dynamic simulation and validation — Steady-state circular driving behaviour	Személygépkocsik - Járműdinamikai szimuláció és validálás - Állandó körkörös vezetési viselkedés	2016. október 1.
ISO 19365:2016	Passenger cars — Validation of vehicle dynamic simulation — Sine with dwell stability control testing	Személygépkocsik - Járműdinamikai szimuláció validálása - Szinuszos stabilitásszabályozó tesztelés a	2016. október 1.

Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok			
Szabvány száma	Szabvány Cím/Angol	Szabvány Cím/Magyar	Publikálás dátuma
		stabilitásszabályozással együtt	
ISO 22140:2021	Passenger cars — Validation of vehicle dynamics simulation — Lateral transient response test methods	Személygépkocsik - Járműdinamikai szimuláció validálása - Oldalirányú átmeneti reakció vizsgálati módszerei	2016. október 1.
ISO 19206-3:2021	Road vehicles — Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions — Part 3: Requirements for passenger vehicle 3D targets	Közúti járművek. Céljárművek, veszélyeztetett úthasználók és egyéb tárgyak vizsgálati eszközei az aktív biztonsági funkciók értékeléséhez. 3. rész: A személygépkocsik 3D céltárgyaira vonatkozó követelmények.	2021. május 1.
ISO 22735:2021	Road vehicles — Test method to evaluate the performance of lane-keeping assistance systems	Közúti járművek. Vizsgálati módszer a sávtartó asszisztens rendszerek teljesítményének értékelésére.	2021. május 1.
ISO/DIS 22733-1:2021	Test method to evaluate the performance of autonomous emergency braking systems — Part 1: Car-to-car	Vizsgálati módszer az autonóm vészfékrendszerek teljesítményének értékelésére. 1. rész: Autóról autóra	2021. július 1.

3.3 Következtetések

Látható, hogy számos állam és nemzetközi szervezet foglalkozik már a témával. Az is látható, hogy a vizsgált államok már jogszabályi szinten is lefektették az autonóm közúti járművek tesztelésének szabályait. Kialakításra kerültek azon eljárások, amelyek alapján ezen tesztelést igényelni, kivitelezni, ellenőrizni lehet. Az is elmondható, hogy szövetségi szinten az Egyesült Államok sokkal részletesebb stratégiával rendelkezik, mint az Európai Unió. Továbbá az is látható, hogy míg Kaliforniában van lehetőség vezető nélküli tesztelésre, addig Németországban erre nincs lehetőség. Azonban a jelentés készítése és adattárolás esetében az látható, hogy míg Kaliforniában csak az autonóm képesség be és kikapcsolását illetve a baleseteket kell részletesen rögzíteni, addig Németország esetében ez jóval részletesebb:

- a pozíciós adatok;

- az alternatív manőverek adatai;
- az autonóm vezetés be- és ki kapcsolása;
- ezen mód használatának száma és időtartama.

A legtöbb szabályozásban, illetve stratégiában az autonómia szintjét a korábban bemutatott SAE szintekkel határozták meg. Illetve az összes vizsgált állam megemlíti különböző mélységben a nemzetközi kooperáció fontosságát. Az is megfigyelhető, hogy míg az Egyesült Államokban vannak olyan államok, amelyek még nem rendelkeznek az önvezető járművekkel kapcsolatos jogi szabályozással, addig Európában minden tagállam rendelkezik valamilyen szinten ilyen szabályozással. Ezáltal azon tézisémet tudtam felállítani, hogy az Egyesült államokban nem kimutatható konkrétan, hogy magasabb érettséggel rendelkeznek stratégia alkotási és szabályozási területen az autonóm közlekedéssel kapcsolatban mint az Európai Unióban, így H1 hipotézisémet megcáfoltam.

Ezen felül kigyűjtöttem és rendszereztem az autonóm közúti közlekedéssel kapcsolatos szabványokat. Ezek a táblázatok segítséget tudnak nyújtani ahhoz, hogy megvizsgáljuk, hogy mely területeket is kell figyelembe venni, amikor egy önvezető közúti járművet szeretnénk vizsgálni vagy fejleszteni.

4 Az autonóm közlekedés társadalmi megítélése

Dolgozatomban vizsgálat alá vettem az önvezető járművekkel kapcsolatos társadalmi megítélést. Ez az elemzés két fő részből áll, egy közösségimédia elemzésből, ahol megvizsgálom, hogy miként jelenik meg a téma az egyes online felületeken, illetve egy kérdőíves kiértékelésből, amelyben többek között azt nézem meg, hogy mennyire tartanak a kitöltők az autonóm járművek használatától.

4.1 Online tartalom analízis

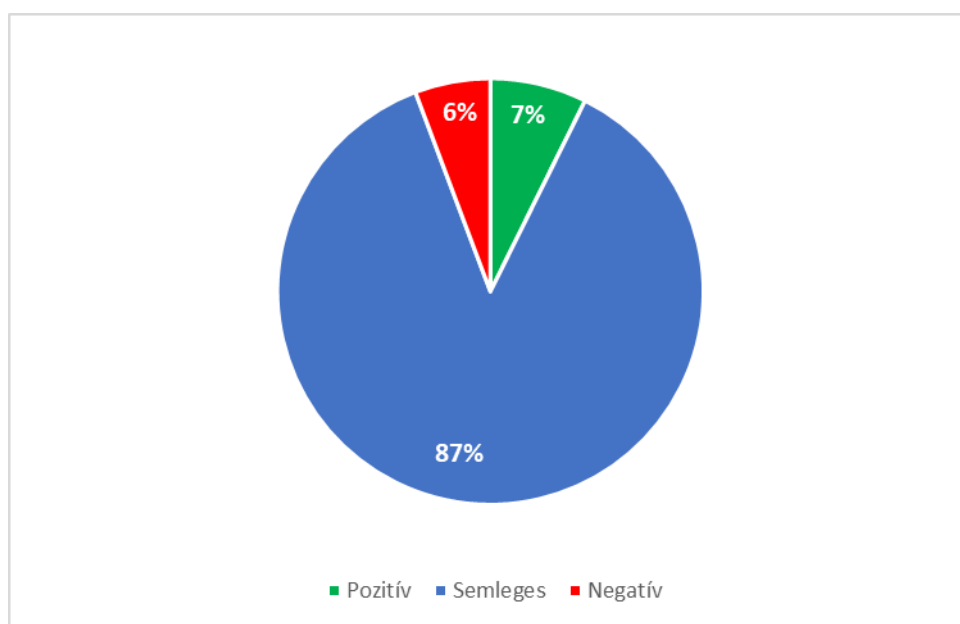
Ebben a részben azt vizsgálom meg, hogy a önvezető járművek témája miként jelenik meg az interneten. Ehhez a SentiOne (www.sentione.hu) weboldalt használtam, ami teljes világot lefedő, 70 nyelvet feldolgozó és webes szöveganalitikán alapuló social listening szoftver. Ami kulcsszavas keresés alapján, valós időben vagy akár 3 évre visszamenően figyeli, indexálja és elemzi az internetes fórumokon, blogokon, weboldalakon és közösségi média csatornákon közzétett publikus szöveges tartalmak minden típusát, melyek önmagukban vagy kontextusukban tartalmazzák a felhasználó által már előre definiált és a platformra felvitt kulcskifejezések bármelyikét. A SentiOne jelenlegi adattárházában több mint 20 milliárd említés érhető el, és ez napról napra bővül. A nyelvfelismeréshez a SentiOne saját fejlesztésű algoritmust használ, amely a lingvisztikai tulajdonságokat és az elérhető metaadatokat is figyelembe veszi, így 99,93 százalékos pontossággal képes detektálni adott nyelvet. A rendszer működését több mint 200 dedikált offline adattároló szerver biztosítja, és nyílt forráskód alapján működik. A SentiOne a különböző social media oldalokról a hivatalos és nyilvános API-hozzáféréseken keresztül gyűjti be az adatokat. Például a legnépszerűbb Facebook oldalak automatikusan bekerülnek a rendszerbe, míg az új Facebook oldalakat pedig a rendszerben már korábban is használt, felhasználói kulcsszóbazis alapján keresi és találja meg a technológia. A releváns tartalmakat, kvantitatív kutatás céljából és ezt megkönnyítendő, különböző fókuszpontok és kutatási paraméterek mentén rendezi össze, melyeket interaktív grafikonokon ábrázol. A kvalitatív mélyelemzéseket is támogató módszertani, technológiai felépítés pedig biztosítja a kutatáshoz kapcsolódó összes indexált tartalom, poszt, komment, cikk és említés egyenként történő elemzésének és kategorizálásának lehetőségét is.⁸⁴

⁸⁴ „Beszélgetésalapú AI-platfom, chatbots, social listening - SentiOne”, elérés 2022. április 3., <https://sentione.com/hu>.

4.1.1 Elemzés részletei

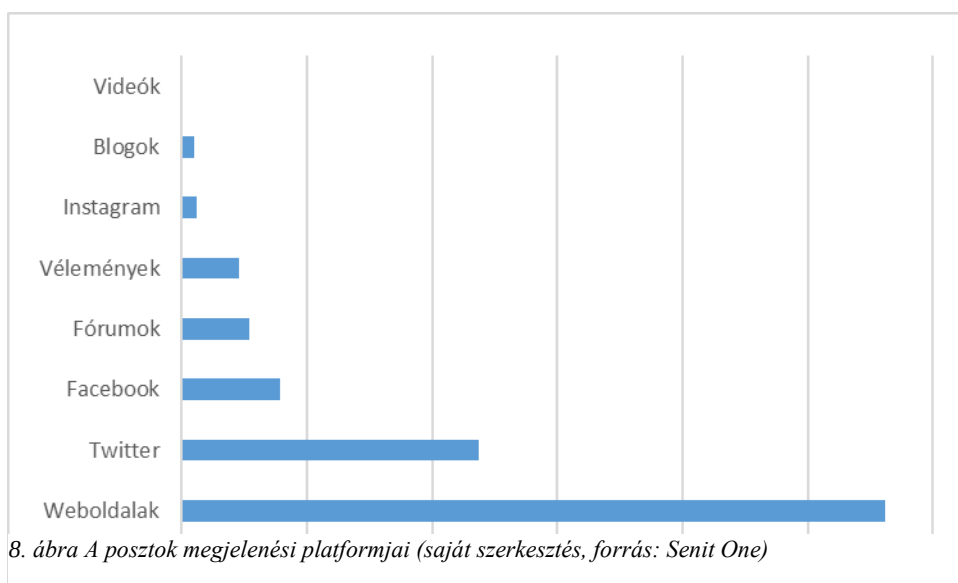
A vizsgált időtartam 2019. április 03.-tól 2022. március 5.-ig terjedt, ahol a következő kulcs szavakra kerestem rá: automated vehicle, intelligent vehicle, automated car, intelligent car, autonomus car, self-driving car, önvezető jármű, önvezető autó, autonóm jármű.

Az látható, hogy összesen ez alatt az idő alatt 221 146 találat született, amelynek a szentiment analízis szerint 86,93%-a semleges megjegyzése volt közel 5,73%-a negatív és 7,33%-a pozitív. A SentiOne algoritmusa mind magyar mind angol nyelven megvizsgálta a tartalmakat, hogy milyen szövegezéssel írták azt a bejegyzést, negatív, pozitív vagy semleges. Ez az eredmény azért jöhetett ki, mert van olyan megosztás, amiben nem írnak semmit az adott tartalomról, amiben a kulcsszavak szerepelnek, így az algoritmus nem tudja a megosztó látásmódját vizsgálni. Azonban ezen magas arány azzal is magyarázható, hogy megosztások nagy része informatív jellegűnek voltak, vagyis a megosztó személy vagy oldal információt akart megosztani a témában nem pedig véleményét kifejezni.



7. ábra A posztok érzelmi töltet (saját szerkesztés, forrás: Senti One)

Ezen felül megvizsgáltam, hogy milyen platformokon jelentek meg a vizsgált kifejezések. Itt az látható, hogy a weboldalakon jelenik meg legnagyobb arányban az övezőt járművekről tartalom 56%-kal, ezt követi a Twitter 24%-kal, majd a Facebook 8%-kal és a fórumok vélemények 5-5%-kal, míg a blogok és az Instagram 1-1%-kal. Ez a megoszlás magyarázatot ad arra, hogy a szentiment analízis során miért volt ilyen nagy arányú a semleges érzelmű tartalom, mivel a weboldalakon a szerzők nem véleményüket írták le, hanem a témával kapcsolatban információt akartak megosztani. Jelen esetben a weboldalak, olyan szakmai és



hírközlő oldalakat jelentenek mint a VentureBeat⁸⁵, Green Car Reports⁸⁶ vagy a Forbes⁸⁷ magazin.

Így azon tézisémet tudom megállapítani hogy az önvezetés témája az online térben szakmai és hír -oldalakra korlátozódik, és nem épült be a közbeszédbe. Ezáltal a H2-es hipotézisem beigazolódott.

4.2 Hazai helyzet felmérése

Kutatásom során fontosnak tartottam felmérni azt, hogy a magyar társadalom miként vélekedik az autonóm vezetésről, mint jövőbeli megoldásról. Ez azért kiemelendő kérdés mert egy technológia elterjedésének gyorsaságát nagyban befolyásolja az, hogy milyen a megítélése az adott felhasználói csoportban.

4.2.1 Kérdőív bemutatás

A kutatásomban felhasznált kérdőív alapját Miltos Kyriakidis és szerzőtársai által publikált „Public opinion on automated driving: Results of an international questionnaire among 5000

⁸⁵ „About VentureBeat”, VentureBeat (blog), elérés 2022. április 3., <https://venturebeat.com/about/>.

⁸⁶ „About Us - Green Car Reports”, elérés 2022. április 3., <https://www.greencarreports.com/aboutus>.

⁸⁷ „Forbes”, Forbes, elérés 2022. április 3., https://www.forbes.com/home_europe/.

respondents”⁸⁸ cikkben használt kérdőív volt. Ennek a kérdőívnek az alapjául dolgoztam ki a sajátomat, amelynek kérdései az 4. számú mellékletben találhatóak.

A kérdőívem elején a demográfiai adatokra kérdeztem rá úgy mint például a nem, iskolázottság, kor, lakhely. Ezt követően az autonóm vezetés egyes szintjeit kértem a kitöltőktől, hogy értékeljék különböző változó alapján. Ilyen változó volt az élvezeti faktor, illetve a könnyű vezetési faktor. A következő kérdéskörök azt vizsgálták, hogy különböző feleknek mennyire szívesen szolgáltatnának adatot a kitöltők. Rákérdeztem még az egyes kihívások esetében (amely tartalmazott többek között adatvédelmi és információbiztonsági kihívásokat is), hogy a kitöltésben résztvevő személyek mennyire tartanak ezen kitettségektől. Ezt követően kíváncsi voltam arra, hogy a felmérésben résztvevő személyek ha használnának önvezető autót, azt mikor és miért tennék. A kérdőívem természetesen anonim volt, mivel olyan adatot nem kértem, amivel ki lehet mutatni a kérdőív kitöltőjének személyazonosságát, így megfelel a 2011. évi CXII. törvénynek, és ezáltal az Általános Adatvédelmi Rendeletnek (General Data Protection Regulation GDPR).

A kérdőívem kiértékelésre az IBM SPSS Statistics 25 programcsomagot használtam, amiben az eredményeim egyrészét Kruskal-Wallis-próba alá vetettem, illetve használtam a kiértékelés során még egyváltozós elemzést, illetve klaszterelemzést.

Kruskal-Wallis-próba egy típusa az összetett kontrollcsoportos vizsgálatnak, ahol kettőnél több részminta összehasonlítása történik ugyanazon változó alapján. Ekkor azt szeretnénk megtudni, hogy a részminták között van-e jelentős különbség ugyanazon változó alapján. A Kruskal-Wallis próba alatt egy tesztváltozót vizsgálunk, egy csoportosító változóval. A kívánt adatok betöltése, és a próba lefuttatása után meg kell vizsgálni az eredményt. Ha a Asymp. Sig. változó vagy is szignifikancia nem haladja meg a 0,005-t ($p < 0,005$) akkor ki lehet jelteni, hogy a részminták között jelentős különbség van a csoportosító változó függvényében. Ezután megvizsgáljuk a rangátlagot, amely megmutatja, a csoportosító változó értékeinek rangsorát a tesztváltozó értékeinek függvényében.

Egyváltozós elemzés során egy adatbázisban szereplő adatok struktúrájába kapunk betekintést egyes változók alapján. Ezt az elemzést akkor szoktuk használni, ha meg akarjuk azt vizsgálni, hogy egy adott kérdésre mi volt a leggyakoribb válasz. Ebben a lekérdezésben szerepelhet a

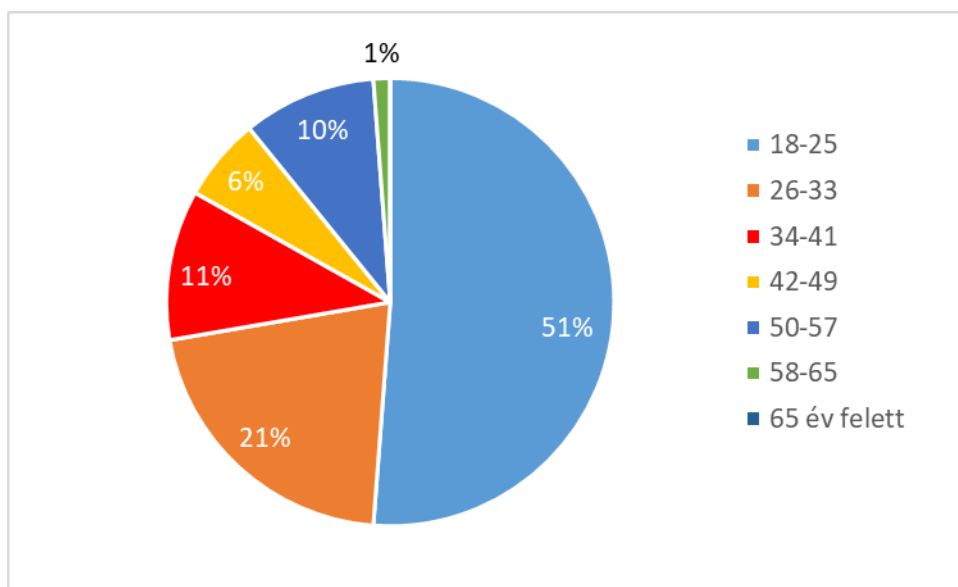
⁸⁸ M. Kyriakidis, R. Happee, és J. C. F. de Winter, „Public Opinion on Automated Driving: Results of an International Questionnaire among 5000 Respondents”, *Transportation Research Part F: Traffic Psychology and Behaviour* 32 (2015. 0 1.): 127–40, <https://doi.org/10.1016/j.trf.2015.04.014>.

helyzet mutatók (módusz, medián, átlag), szóródási mutatók (terjedelem, szórás, variancia) és alakmutató számok, illetve egyéb mutatók mint, például maximum, minimum érték.

A klaszterelemzéssel vizsgáltam meg az egyes kérdések válaszában megjelenő attitűdöket, lehet-e valamilyen téma szerint csoportosítani. A csoportok számát Ward-féle eljárással alakítottam ki, így olyan csoportokat tudtam elkülöníteni, amelyek belső szóródása a legkisebb. Az így kapott csoportokhoz elnevezést Kruskal-Wallis teszttel tudtam rendelni. Ezt követően ezen csoportot csoportosító változó használtam fel az egyes skálás kérdések kiértékeléséhez.⁸⁹

4.2.2 Eredmények

A kérdőívet 163 személy töltötte ki, jellegét tekintve nem reprezentatív a felmérés. Nemek megoszlásában az látható, hogy 61,4%-ban nők, míg 38,6%-ban férfiak töltötték ki. Legnagyobb részben a 18-25 éves korosztály töltötte ki 51,2%-kal majd a korcsoportok emelkedésével csökkent a kitöltők száma, a megoszlás részletes adatait a 8. számú ábra

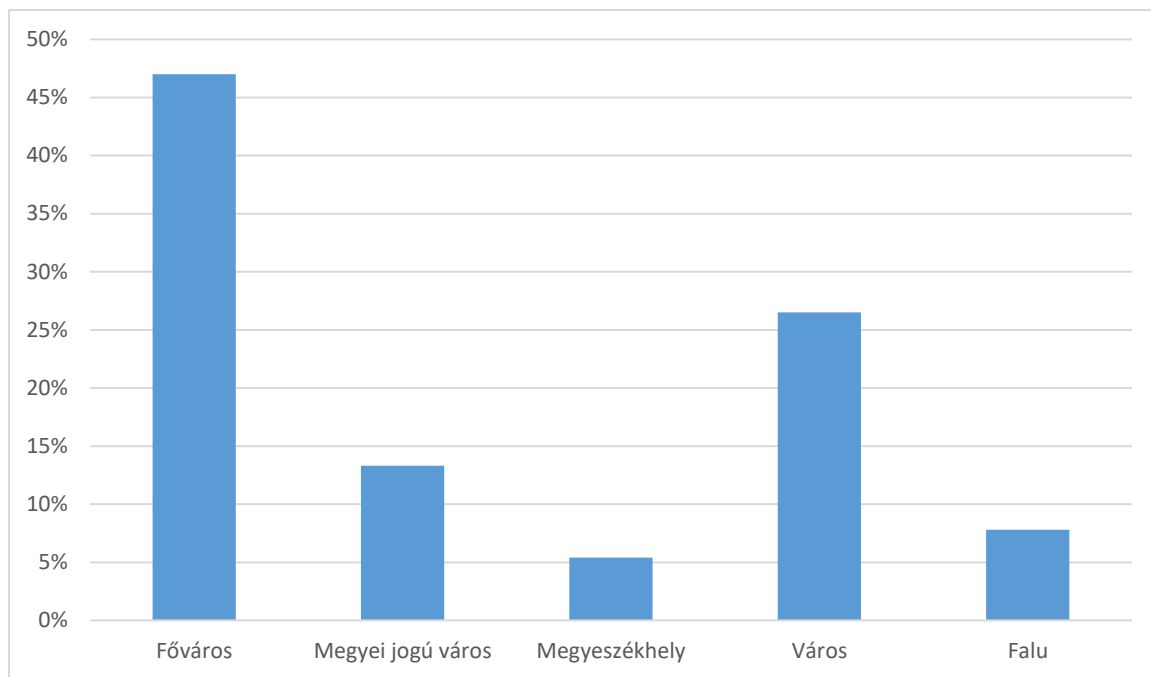


9. ábra Kormegoszlás a kitöltők között (saját szerkesztés, forrás: kérdőív)

tartalmazza.

Az látható, hogy a kérdőívet főleg a fővárosból töltötték ki (47%) ezt követte a város (28,5%), majd a megyei jogú város (13,3%), falu (7,8%), és legkevebb kitöltés a megyeszékhelyekről érkezett (5,4%).

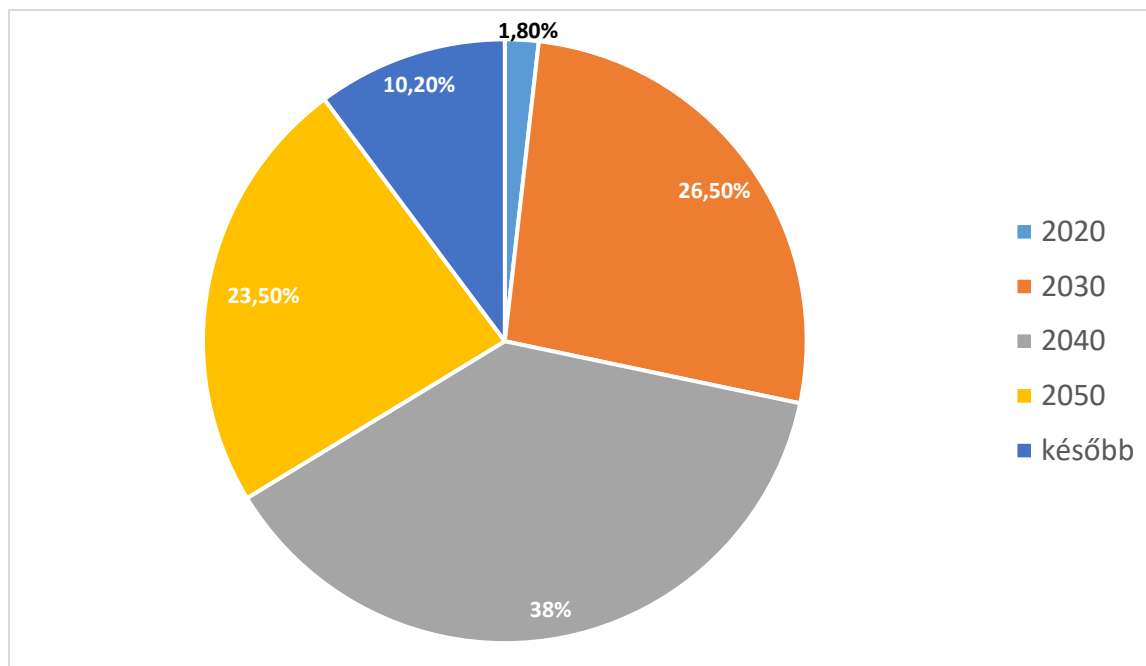
⁸⁹ Ariel Mitev és Laszlo Sajtos, *SPSS kutatási és adatelemzési kézikönyv*, 2007.



10. ábra A kitöltők megoszlása az általuk lakott település méret szerint (saját szerkesztés, forrás: kérdőív)

Megvizsgáltam, hogy a kitöltők körében mi is az elsődleges közlekedési eszköz, itt két nagy csoportot lehetett azonosítani. A felmérésben résztvevő személyek többségének (57,2%) elsődleges közlekedési módja a közösségi közlekedés, a másik nagyobb csoportot azon személyek alkották 31,9%-kal, akik saját tulajdonú közlekedési eszközt használnak.

Továbbá arra kérdésre, hogy melyik évtizedben lesz a legtöbb jármű képes a teljes önvezetésre Magyarországon? A kitöltők 38%-a szerint a 2040-es évekre, míg 26,5%-a véleménye alapján 2030-as évekre, a 23,5% -a szerint 2050-es évekre ezenfelül 10,2%-a szerint később, míg a legkevésbé releváns évtized a kitöltők 1,8%-a szerint a 2020-as.



11. ábra Kitöltés megoszlása a hazai önvezető járművek elterjedésének időbeli meghatározásában (saját szerkesztés, forrás: kérdőív)

Megvizsgáltam azt, hogy az önvezető járművek élvezetének mértékét befolyásolja-e bármely fenyegetés, amely a kérdőívben megtalálható. Ehhez a vizsgálathoz felhasználtam a kérdőívem 9. -tól 12. a kérdésig bezárólag az eredményeit, amely egy Likert skálás⁹⁰ rész volt:

- Mit gondol a következő állításról? A manuális vezetés szórakoztató.
- Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.
- Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.
- Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.

Ezeknél a kérdéseknél a skála értékei a következők voltak:

- 1=teljesen nem értek vele egyet;
- 5=teljesen egyet értek vele.

Ezekre a kérdéskere adott válaszokat klaszter elemzéssel csoportosítottam, ahol a csoportok számát Ward-féle eljárással alakítottam ki. Hogy ezeket a csoportok megnevezését meghatározzam elvégeztem egy Kruskal-Wallis tesztet, amely alapján kettő csoportot azonosítottam, egy „Élvezetesnek tartja az autonóm vezetést”, illetve „Kevésbé tartja élvezetesnek az autonóm vezetést”. Látható az 13. számú táblázatból, hogy ez a két csoport valóban helytálló tud lenni, hiszen a manuális vezetés élvezeténél a rangátlag magasabb a „Kevésbé tartja élvezetesnek az autonóm vezetést” csoportnál, míg a többi esetben, amikor

⁹⁰ a Likert skála két szélsőség közötti mérési skála, amely az attitűdöt vizsgálja az adott kérdés esetében a megadott két szélső érték között.

már megjelenik valamilyen szinten az önvezetés ott a rangátlag az „Élvezetesnek tartja az autonóm vezetést” nagyobb.

13. táblázat Klaszterelemzés eredménye (saját szerkesztés, forrás: SPSS)

Kérdés	Klaszter név	Darab szám	Rangátlag
Mit gondol a következő állításról? A manuális vezetés szórakoztató.	Élvezetesnek tartja az autonóm vezetést	92	68,55
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	99,42
	Összes	163	
Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	Élvezetesnek tartja az autonóm vezetést	92	104,55
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	52,77
	Összes	163	
Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	Élvezetesnek tartja az autonóm vezetést	92	113,78
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	40,82
	Összes	163	
Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.	Élvezetesnek tartja az autonóm vezetést	92	112,39
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	42,63
	Összes	163	

Ezt követően ezen két csoportot használtam csoportosító változónak a Kruskal-Wallis tesztben, ahol az egyes fenyegetésektől való félelmet vizsgáltam meg. Ezek a kérdések többek között tartalmaztak információbiztonsági és adatvédelmi kérdéseket is. Ezek a kérdések a 24.-től tartottak egészen a 28.-ig, amelyek szint úgy az 5 fokozatú Likert skálás módszertant használták, ahol a legalacsonyabb érték jelentése megegyezett „teljesen nem ért vele egyet” véleménnyel míg a felső érték a „teljesen egyetért vele” véleménnyel. A kérdések a következők voltak:

- A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.
- A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.

- A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.
- A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.
- A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.

Ezen kérdések esetében a lefutott teszt során a szignifikancia érték csak egy kihívás esetében volt megfelelő, ami azt jelenti hogy ($p \leq 0,005$). Ez a kontrollérzet elvetésének kihívása volt, ahol megvizsgáltam a rangátlagokat, hogy mely csoportnál ez hogyan alakult, ezt az eredményt az 14. számú ábra mutatja be.

14. táblázat Kruskal-Wallis tesztet szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

	Magán szféra kihívásai	Szoftver feltörés elleni védelem kihívásai	Jogi terület kihívásai	Megbízhatóság kihívásai	Kontroll érzet elvesztésének kihívásai
Kruskal-Wallis H	1,123	,030	,295	,102	14,174
df	1	1	1	1	1
Asymp. Sig.	,289	,863	,587	,750	,000

15. táblázat Kruskal-Wallis tesztet rangátlag eredménye egyes (saját szerkesztés, forrás: SPSS)

Kérdés	Kalszter név	Darab szám	Rangátlag
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.	Élvezetesnek tartja az autonóm vezetést	92	70,06
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	97,47
	Összes	163	

Ebből az látható, hogy azon személyek, akik élvezetesebbnek tartják az autonóm vezetést kevésbé tartanak a kontroll elvesztésétől. Ezáltal a H3-as hipotézisem helyt állt.

Ezen felül megvizsgáltam azt is, hogy az önvezető járművek használatára hatással vannak-e az egyes kihívások. Ezt a vizsgálatot is a Kruskal-Wallis teszttel végeztem el. Ehhez a kérdőívem 30. kérdését használtam fel, mint csoportosító változó:

- Kérem, jelezze, mikor szeretne teljesen önvezető járművet használni? (többet is választhat)
 - ha a vezetés stresszes;
 - ha a munkámmal kell foglalkozzak;
 - ha fáradt vagyok;
 - mindennapi utazás során;
 - ha a vezetés unalmas;
 - ha alkoholt ittam;
 - Nem szeretnék teljesen önvezető járművet használni.

Ezt a kérdést, hogy fel tudjam használni mint csoportosító változó kettő csoportot kellett létrehoznom. Az első csoportban össze vontam az összes olyan lehetőséget, amelyben a résztvevők szertették volna valamilyen célra használni ezt a technológiát, és így ez a csoport lett a „Használna önvezető járművet” míg a nem szeretnék teljesen önvezető járművet használni válasz lehetőség alkotta a másik csoportot, aminek a neve „Nem használna önvezető járművet”.

Ezt követően elvégeztem a tesztet, ahol a teszt változók az egyes fenyegetések lettek. Az eredmény meglepően változatos volt, mivel az 5 kérdésből 3-nál jelent meg szignifikancia. Ezen értékek megtalálhatóak az 16. számú táblázatban.

16. táblázat Kruskal-Wallis tesztet szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

	Magán szféra kihívásai	Szoftver feltörés elleni védelem kihívásai	Jogi terület kihívásai	Megbízhatóság kihívásai	Kontroll érzet elvesztésének kihívásai
Kruskal-Wallis H	11,985	1,752	7,338	11,417	9,747
df	1	1	1	1	1
Asymp. Sig.	,001	,186	,007	,001	,002

Az látható, hogy a használati szándéokra hatással van a magánszférával kapcsolatos kihívások, továbbá a technológia általános megbízhatóságának kérdésköre, illetve a kontroll érzet elvesztésétől való félelem. A rangátlagok vizsgálata a 17. számú táblázatban megtalálható.

17. táblázat Kruskal-Wallis tesztet rangátlag eredménye egyes (saját szerkesztés, forrás: SPSS)

Kérdés	Kalszter név	Darab szám	Rangátlag
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	Használna önvezető járművet	121	74,65
	Nem használna önvezető járművet	42	103,17
	Összes	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	Használna önvezető járművet	121	74,89
	Nem használna önvezető járművet	42	102,48
	Összes	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.	Használna önvezető járművet	121	75,36
	Nem használna önvezető járművet	42	101,13
	Összes	163	

A rangátlagokat szemügyre véve látható, hogy azok a személyek jobban tartanak az adott kihívásoktól, akik nem használnának önvezető járművet. Azonban a H4-es hipotézisem miszerint a kitöltők körében az önvezető járművek használat iránti attitűdöt befolyásolják az egyes kiberbiztonsági és adatvédelmi kockázatoktól való félelem, nem sikerült teljesen be bizonyítanom, mivel a szoftverek feltörésével kapcsolatos fenyegetések esetében a szignifikancia nem volt kimutatható.

Ezt követően még külön egyváltozós elemzés alá vetettem az adatok megosztásával kapcsolatos kérdéseket, hogy megvizsgáljam az azokra adott válaszok helyzet mutatóit (átlagot, móduszt és mediánt). Ezek a 19-től a 23. kérdésig terjednek, ahol Likert skálán kellett meghatározni mennyire szívesen osztaná meg adatai a kitöltő:

- környező járművekkel;
- fejlesztőkkel;
- biztosító társasággal;

- úttest kezelővel;
- hatóságokkal.

Ebből az derült ki, hogy míg a legkülönbözőbb szervezetek felé hasonló mértékben osztanak meg a kitöltők az adataikat azaz azonosak a móduszok vagyis a leggyakrabban előforduló elemek, addig a hatóságnál ez az érték jóval kisebb. Ez számokban kifejezve az első négy esetben 4-es érték, míg a hatóságnál 1-es.

18. táblázat Adatmegosztás hajlandóságának vizsgálata előre meghatározott esetekben (saját szerkesztés, forrás: SPSS)

	Megengedném a járművemnek, hogy adatokat továbbítson a környező járműveknek,.	Megengedném a járművemnek, hogy adatokat továbbítson a jármű fejlesztőknek.	Megengedném a járművemnek, hogy adatokat továbbítson a biztosító társaságoknak.	Megengedném a járművemnek, hogy adatokat továbbítson a az úttest kezelő vállalatoknak.	Megengedném a járművemnek, hogy adatokat továbbítson az egyes hatóságoknak
Átlag	3,59	3,45	2,90	3,26	2,44
Medián	4,00	4,00	3,00	4,00	2,00
Módusz	4	4	4	4	1
Minimum	1	1	1	1	1
Maximum	5	5	5	5	5
Sum	585	562	472	531	398

Itt szeretném kiemelni, hogy ebben az esetben azért a móduszt vizsgáljuk, nem pedig az átlagot, mert az átlag értékét nagyban befolyásolja a már kevés számban megjelenő szélső érték, így torzíthatja a valós képet. Tehát a számokból az látszik, hogy a kitöltők határozottan kisebb mértékben szolgáltatnának adatokat a hatóságoknak mint más szervezeteknek.

4.3 Következtetések

Látható, hogy most még az online felületen maga az önvezető technológia nem közbeszéd tárgya, inkább a szakmai és hír oldalak foglalkoznak a témával. Hazai viszonylatban a kitöltők körében az látható, hogy azok a személyek, akik tartanak a kontroll elvesztésétől kevésbé tartják élvezetesebbnek az önvezető jármű használatát, továbbá kimutatható összefüggés az önvezető járművek használati attitűdje és az egyes fenyegetésektől való félelem között. Viszont ez a félelem csak részben érinti az információbiztonsággal kapcsolatos fenyegetést. Ezen felül további kutatási lehetőség az állam és állampolgárok kapcsolatának mélyebb vizsgálata az autonóm vezetés esetében. Ezen további kutatási lehetőséget az egyváltozós elemzésben mért különbségekere alapozom. Meglátásom szerint

csak akkor tud egy biztonságos és jólműködő autonóm vezetési ökoszisztéma működni, ha a technológia használói megbíznak a rendszerben és az annak a védelmét garantáló államban is.

5 Összegzés

A kutatásom egy részletesebb képet ad arról, hogy pontosan milyen típusú rendszerelemekből áll egy önvezető közúti közlekedési jármű, és ezen rendszerek részeinek milyen feladata van. Látható az is, hogy az egyes rendszerelemek működése szorosan összekapcsolódik, és egyes meghibásodások dominószerű hatásokat tudnak okozni a teljes jármű működését tekintve. Ezért fontos ezen járműveket olyan hibadetektáló rendszerekkel felszerelni, amelyek segítik a gyors és pontos hibameghatározást. Továbbá egy igen fontos rendszer került azonosításra az önvezető járműn kívüli környezetben, ami nem más mint az Intelligens Közlekedési Rendszer. Amely nem csak az egyes közlekedésben résztvevő járműveket köti össze, hanem ezeket a résztvevőket egy központi forgalomirányítási rendszerrel is, amely további adatokkal és utasításokkal szolgál az eszközöknek és felhasználóknak a közlekedés során. Ezt követően azonosításra kerültek azok a fenyegetések, amelyek az egyes rendszerelemeket fenyegetik. Itt az volt látható, hogy az egyes specifikus területeken sajátos kihívások kerültek azonosításra, ilyen például a LiDAR vagy kamera szenzorok vakítása. Azonban az olyan területeken, amelyek más informatikai rendszer esetében is azonosítható, ott a hagyományos támadások jelentek meg. Ilyen területként jelenik meg például a hálózati rendszerelemek. Megvizsgálva a jogi szabályozási hátteret az USA és EU viszonylatában az látható, hogy a központi stratégia részletesebb az Egyesült Államokban, míg az állami/nemzeti szabályozás mennyiségének arányában inkább az Unió vezet. A területi korlát miatt a kettő vizsgált területről kiválasztottam azokat az államokat, amelyek a legnagyobb hangsúlyt fektetik erre a területre. Ezért a részletesebb állami szabályozás elemzésében Kaliforniát, illetve Németországot vizsgáltam meg. Az elemzés eredménye nem mutatott rá egyértelműen, hogy melyik nagy egység rendelkezik részletesebb szabályozással, mivel egyes területeken eltérő ennek a mértéke. A szabványi feldolgozásban számos közlekedésbiztonsági, tervezési, kiberbiztonsági és tesztelési szabvány megjelenik, amelyeket figyelembe kell venni, amikor egy biztonságos önvezető közúti jármű kialakítását vizsgáljuk. Ezek a szabványok a jármű számos funkciójára kiterjed, és egészen a mély technológiai szabványoktól kezdve a módszertani szabványokig bezárólag kigyűjtésre kerültek a releváns dokumentumok. A társadalmi megítélést vizsgálva az látható, hogy a közösségi média platformokon még kevésbé közbeszéd tárgya az önvezető jármű. Ezen téma inkább a szakmai és hír oldalakon jelenik meg. A kérdőíves felmérésből az derül ki, hogy azok a kitöltők akik tartanak a kontroll elvesztésétől kevésbé tartják ezt a

technológiát élvezetesebbnek. Ezen felül az is megfigyelhető volt, hogy a használati attitűdre számos fenyegetés hatással van, de ebben nem szerepel az összes kiber- és információbiztonsági fenyegetés. Fontos azt az eredményt is kiemelni, amely arra mutatott rá, hogy az adatmegosztás során a kitöltők legkevésbé a hatóságokkal szeretnék adatot közölni. Szerintem hazai viszonylatban fontos lesz ezt az eredményt megvizsgálni, mert igen központi kérdés az államba vetett bizalom abban az esetben, amikor annak kell biztosítani a intelligens közlekedés rendszer biztonságát. Ezért, ha a felhasználók nem bíznak az államba próbálnak minél kevesebb információt megosztani (akár a jármű rendszerének manipulálásával) ezáltal az ITS nem tud majd hatékonyan működni. Elmondható továbbá, hogy a jelen kutatás egy olyan széles spektrumot kívánt lefedni, amelyben számos olyan terület azonosításra került, amelyek kiinduló pontot adhatnak számomra a további kutatási irányok definiálásakor.

5.1 Eredmények

A kutatási téma feldolgozása során az alábbi eredményeket értem el:

T1: Az Egyesült államokban nem kimutatható konkrétan, hogy magasabb érettséggel rendelkeznek stratégia alkotási és szabályozási területen az autonóm közlekedéssel kapcsolatban mint az Európai Unióban

T2: Az önvezetés témája az online térben szakmai és hír -oldalakra korlátozódik, és nem épült be a közbeszédbe

T3: Azon személyek, akik élvezetesebbnek tartják az autonóm vezetést kevésbé tartanak a kontroll elvesztésétől

T4: A kitöltők körében az önvezető járművek használat iránti attitűdöt nem az összes kiberbiztonsági és adatvédelmi kockázatoktól való félelem befolyásolja. Azonban azok a személyek jobban tartanak az adott kihívásoktól, akik nem használnának önvezető járművet.

6 Irodalomjegyzék

- „About Us - Green Car Reports”. Elérés 2022. április 3. <https://www.greencarreports.com/aboutus>.
- VentureBeat. „About VentureBeat”. Elérés 2022. április 3. <https://venturebeat.com/about/>.
- Agrawal, Megha, Tianxiang Huang, Jianying Zhou, és Donghoon Chang. „CAN-FD-Sec: improving security of CAN-FD protocol”. In *Security and Safety Interplay of Intelligent Software Systems*, 77–93. Springer, 2018.
- Akhtar, Naveed, és Ajmal Mian. „Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey”. *IEEE Access* 6 (2018): 14410–30. <https://doi.org/10.1109/ACCESS.2018.2807385>.
- Al-kahtani, Mohammed Saeed. „Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”. In *2012 6th International Conference on Signal Processing and Communication Systems*, 1–9, 2012. <https://doi.org/10.1109/ICSPCS.2012.6507953>.
- Alzubaidi, Laith, Jinglan Zhang, Amjad J. Humaidi, Ayad Al-Dujaili, Ye Duan, Omran Al-Shamma, J. Santamaría, Mohammed A. Fadhel, Muthana Al-Amidie, és Laith Farhan. „Review of deep learning: concepts, CNN architectures, challenges, applications, future directions”. *Journal of Big Data* 8, sz. 1 (2021. március 31.): 53. <https://doi.org/10.1186/s40537-021-00444-8>.
- Andel, Todd R., J. Todd McDonald, Adam J. Brown, Tyler H. Trigg, és Paul W. Cartsten. „Towards Protection Mechanisms for Secure and Efficient CAN Operation”. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 1–6. IEEE, 2019.
- Appathurai, Ahilan, Gunasekaran Manogaran, és Naveen Chilamkurti. „Trusted FPGA-based transport traffic inject, impersonate (I2) attacks beaconing in the Internet of Vehicles”. *IET Networks* 8 (2019. május 1.): 169–78. <https://doi.org/10.1049/iet-net.2018.5171>.
- Arif, Muhammad, Guojun Wang, és Valentina Emilia Balas. „Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing”. *Stud. Inform. Control* 27, sz. 2 (2018): 235–46.
- „Automated Driving Systems 2.0: A Vision for Safety”. National Highway Transportation Safety Administration, 2017.
- „Autonomous Vehicle Market Size, Share, Trends, Report 2022-2030”. Elérés 2022. április 4. <https://www.precedenceresearch.com/autonomous-vehicle-market>.
- „Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation”. Elérés 2022. április 10. <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>.
- „AV 4.0 | US Department of Transportation”, 2019. <https://www.transportation.gov/policy-initiatives/automated-vehicles/av-40>.
- Azumi, Takuya, Yuya Maruyama, és Shinpei Kato. „ROS-lite: ROS Framework for NoC-Based Embedded Many-Core Platform”. In *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 4375–82, 2020. <https://doi.org/10.1109/IROS45743.2020.9340977>.
- Balakrishnan, Sarankumar, Pu Wang, Arupjyoti Bhuyan, és Zhi Sun. „Modeling and analysis of eavesdropping attack in 802.11 ad mmWave wireless networks”. *IEEE Access* 7 (2019): 70355–70.
- Bar Hillel, Aharon, Ronen Lerner, Dan Levi, és Guy Raz. „Recent Progress in Road and Lane Detection: A Survey”. *Machine Vision and Applications* 25, sz. 3 (2014. április 1.): 727–45. <https://doi.org/10.1007/s00138-011-0404-2>.
- „Beszélgetésalapú AI-platform, chatbots, social listening - SentiOne”. Elérés 2022. április 3. <https://sentione.com/hu>.

- „BMDV - Automated and connected driving”. Elérés 2022. március 15. <https://www.bmvi.de/EN/Topics/Digital-Matters/Automated-Connected-Driving/automated-and-connected-driving.html>.
- California DMV. „California Autonomous Vehicle Regulations”. Elérés 2022. március 15. <https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/california-autonomous-vehicle-regulations/>.
- Cao, Yulong, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, és Z. Morley Mao. „Adversarial sensor attack on lidar-based perception in autonomous driving”. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2267–81, 2019.
- Checkoway, S., D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, és T. Kohno. „Comprehensive experimental analyses of automotive attack surfaces”. *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 2011.
- Chen, Ping-Rong, Hsueh-Ming Hang, Sheng-Wei Chan, és Jing-Jhih Lin. „DSNet: An Efficient CNN for Road Scene Segmentation”. *APSIPA Transactions on Signal and Information Processing* 9 (2020. ed). <https://doi.org/10.1017/ATSIP.2020.25>.
- „Connected and Autonomous Vehicle Cybersecurity Threats - QA Consultants”. Elérés 2022. március 29. <https://qaconsultants.com/blog/connected-and-autonomous-vehicle-cybersecurity-threats/>.
- „Connected Automated Driving | EU-countries”. Elérés 2022. április 10. <https://www.connectedautomateddriving.eu/regulation-and-policies/national-level/eu/>.
- „Connected Automated Driving | Homepage”. Elérés 2022. április 10. <https://www.connectedautomateddriving.eu/>.
- Dieber, Bernhard, Benjamin Breiling, Sebastian Taurer, Severin Kacianka, Stefan Rass, és Peter Schartner. „Security for the Robot Operating System”. *Robotics and Autonomous Systems* 98 (2017. október 1.). <https://doi.org/10.1016/j.robot.2017.09.017>.
- Forbes. „Forbes”. Elérés 2022. április 3. https://www.forbes.com/home_europe/.
- Greene, Kyle, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, és Vijay Devabhaktuni. „A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic”. *IEEE Consumer Electronics Magazine* 10, sz. 1 (2021): 101–8. <https://doi.org/10.1109/MCE.2020.3012425>.
- Groza, B., S. Murvay, A. Van Herrewwege, és I. Verbauwhede. „LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks”. *ACM Transactions on Embedded Computing Systems* 16, sz. 3 (2017). <https://doi.org/10.1145/3056506>.
- H, Sharath, és Asadullah Ansari. „Autonomous Vehicles Camera Blinding Attack Detection Using Sequence Modelling and Predictive Analytics”, 2020. <https://doi.org/10.4271/2020-01-0719>.
- Haider, Zeeshan, és Shehzad Khalid. „Survey on effective GPS spoofing countermeasures”. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 573–77, 2016. <https://doi.org/10.1109/INTECH.2016.7845038>.
- Hegde, Nayana, és Sunilkumar S. Manvi. „Hash Based Integrity Verification for Vehicular Cloud Environment”. In *2019 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 75–79, 2019. <https://doi.org/10.1109/CCEM48484.2019.00016>.
- „IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular

- Environments". *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, 2010. július, 1–51. <https://doi.org/10.1109/IEEESTD.2010.5514475>.
- „J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International". SAE International, 2021. április. https://www.sae.org/standards/content/j3016_202104.
- „JELENTÉS a kooperatív intelligens közlekedési rendszerek európai stratégiájáról". Elérés 2022. március 15. https://www.europarl.europa.eu/doceo/document/A-8-2018-0036_HU.html.
- Jeong, Se-Yeon, I-Ju Choi, Yeong-Jin Kim, Yong-Min Shin, Jeong-Hun Han, Goo-Hong Jung, és Kyoung-Gon Kim. „A Study on ROS Vulnerabilities and Countermeasure". In *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, 147–48. HRI '17. New York, NY, USA: Association for Computing Machinery, 2017. <https://doi.org/10.1145/3029798.3038437>.
- Jie, Yingmo, Mingchu Li, Cheng Guo, és Ling Chen. „Dynamic Defense Strategy Against DoS Attacks Over Vehicular Ad Hoc Networks Based on Port Hopping". *IEEE Access* 6 (2018): 51374–83. <https://doi.org/10.1109/ACCESS.2018.2869399>.
- Jo, Kichun, Chansoo Kim, és Myoungcho Sunwoo. „Simultaneous Localization and Map Change Update for the High Definition Map-Based Autonomous Driving Car". *Sensors* 18, sz. 9 (2018. szeptember): 3145. <https://doi.org/10.3390/s18093145>.
- Kapoor, Prateek, Ankur Vora, és Kyoung-Don Kang. „Detecting and Mitigating Spoofing Attack Against an Automotive Radar". In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 1–6, 2018. <https://doi.org/10.1109/VTCFall.2018.8690734>.
- Khankari, Nilesh, és Geetanjali Kale. „One Time Password Generation for Multifactor Authentication using Graphical Password". *International Journal Of Engineering Research and General Science* 3 (2020. augusztus 25.): 489–94.
- Kim, Kyounggon, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, és Huy Kang Kim. „Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense". *Computers & Security* 103 (2021. április 1.): 102150. <https://doi.org/10.1016/j.cose.2020.102150>.
- Kornaros, George, Dimitris Bakoyiannis, Othon Tomoutzoglou, Marcello Coppola, és Giovanni Gherardi. „Trustnet: ensuring normal-world and trusted-world can-bus networking". In *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 1–6. IEEE, 2019.
- Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, és mtsai. „Experimental Security Analysis of a Modern Automobile". In *The Ethics of Information Technologies*. Routledge, 2017.
- Krundshev, Vasiliy, Maxim Kalinin, és Peter Zegzhda. „Artificial swarm algorithm for VANET protection against routing attacks". In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 795–800, 2018. <https://doi.org/10.1109/ICPHYS.2018.8390808>.
- Kumar, Parteek, és Sahil Verma. „Detection of Wormhole Attack in VANET". *National Journal of System and Information Technology* 10, sz. 1 (2017): 71.
- Kumar, Sushil, és Kulwinder Singh Mann. „Prevention of DoS attacks by detection of multiple malicious nodes in VANETs". In *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 89–94. IEEE, 2019.
- Kyriakidis, M., R. Happee, és J. C. F. de Winter. „Public Opinion on Automated Driving: Results of an International Questionnaire among 5000 Respondents". *Transportation*

- Research Part F: Traffic Psychology and Behaviour* 32 (2015. 0 1.): 127–40.
<https://doi.org/10.1016/j.trf.2015.04.014>.
- Lee, Dasom, és David J. Hess. „Regulations for On-Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization”. *Transportation Research Part A: Policy and Practice* 136 (2020. június 1.): 85–98.
<https://doi.org/10.1016/j.tra.2020.03.026>.
- Liang, Wei, Jing Long, Tien-Hsiung Weng, X.H. Chen, Kuan-Ching Li, és Albert Zomaya. „TBRS: A trust based recommendation scheme for vehicular CPS network”. *Future Generation Computer Systems* 92 (2018. október 1.).
<https://doi.org/10.1016/j.future.2018.09.002>.
- Limbasiya, Trupil, és Debasis Das. „Secure and Effective Geo-Data Transmission Scheme for Vehicle-to-Vehicle Communication”. In *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 389–96, 2018.
<https://doi.org/10.1109/SmartWorld.2018.00096>.
- Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, és Linqiang Ge. „Data Integrity Attacks Against Dynamic Route Guidance in Transportation-Based Cyber-Physical Systems: Modeling, Analysis, and Defense”. *IEEE Transactions on Vehicular Technology* 67, sz. 9 (2018. szeptember): 8738–53. <https://doi.org/10.1109/TVT.2018.2845744>.
- Liu, Jiajia, Shubin Zhang, Wen Sun, és Yongpeng Shi. „In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions”. *IEEE Network* 31, sz. 5 (2017): 50–58. <https://doi.org/10.1109/MNET.2017.1600257>.
- Mejri, Mohamed Nidhal, Jalel Ben-Othman, és Mohamed Hamdi. „Survey on VANET Security Challenges and Possible Cryptographic Solutions”. *Vehicular Communications* 1, sz. 2 (2014. április 1.): 53–66.
<https://doi.org/10.1016/j.vehcom.2014.05.001>.
- Merco, Roberto, Zoleikha Abdollahi Biron, és Pierluigi Pisù. „Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control”. In *2018 Annual American Control Conference (ACC)*, 5582–87, 2018.
<https://doi.org/10.23919/ACC.2018.8431538>.
- Mitev, Ariel, és Laszlo Sajtos. *SPSS kutatási és adatelemzési kézikönyv*, 2007.
- Mostafa, Ahmad, Anna Maria Vegni, Rekha Singoria, Talmai Oliveira, Thomas D. C. Little, és Dharma P. Agrawal. „A V2X-based approach for reduction of delay propagation in vehicular Ad-Hoc networks”. In *2011 11th International Conference on ITS Telecommunications*, 756–61, 2011. <https://doi.org/10.1109/ITST.2011.6060155>.
- Nanda, Ashish, Deepak Puthal, Joel J. P. C. Rodrigues, és Sergei A. Kozlov. „Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions”. *IEEE Wireless Communications* 26, sz. 4 (2019): 60–65.
<https://doi.org/10.1109/MWC.2019.1800503>.
- Narain, Sashank, Aanjhan Ranganathan, és Guevara Noubir. „Security of GPS/INS Based On-road Location Tracking Systems”. In *2019 IEEE Symposium on Security and Privacy (SP)*, 587–601, 2019. <https://doi.org/10.1109/SP.2019.00068>.
- Panda, Niranjana, és B. Kumar Pattanayak. „Energy aware detection and prevention of black hole attack in MANET”. *International Journal of Engineering and Technology (UAE)* 7, sz. 2.6 (2018): 135–40.
- Parkinson, Simon, Paul Ward, Kyle Wilson, és Jonathan Miller. „Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges”. *IEEE Transactions on Intelligent Transportation Systems* 18, sz. 11 (2017): 2898–2915.
<https://doi.org/10.1109/TITS.2017.2665968>.

- Petit, Jonathan, Bas Stottelaar, Michael Feiri, és Frank Kargl. „Remote attacks on automated vehicles sensors: Experiments on camera and lidar”. *Black Hat Europe* 11, sz. 2015 (2015): 995.
- Purohit, Kamlesh Chandra, Sushil Chandra Dimri, és Sanjay Jasola. „Mitigation and Performance Analysis of Routing Protocols Under Black-Hole Attack in Vehicular Ad-Hoc Network (VANET)”. *Wireless Personal Communications* 97, sz. 4 (2017. december 1.): 5099–5114. <https://doi.org/10.1007/s11277-017-4770-6>.
- Purwar, Anupam, Divya Joshi, és Vinod Kumar Chaubey. „GPS signal jamming and anti-jamming strategy — A theoretical analysis”. In *2016 IEEE Annual India Conference (INDICON)*, 1–6, 2016. <https://doi.org/10.1109/INDICON.2016.7838933>.
- general motors. „Putting Self-Driving Cars On The Roads | General Motors”. Elérés 2022. február 27. <https://www.gm.com/content/public/us/en/gm/home/stories/self-driving-cars.html>.
- Roome, S. J. „Digital Radio Frequency Memory”. *Electronics & Communication Engineering Journal* 2, sz. 4 (1990. augusztus 1.): 147–53. <https://doi.org/10.1049/ecej:19900035>.
- Waymo. „Safety Publications”. Elérés 2022. február 27. <https://waymo.com/safety/>.
- Sakiz, Fatih, és Sevil Sen. „A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV”. *Ad Hoc Networks* 61 (2017. március 1.). <https://doi.org/10.1016/j.adhoc.2017.03.006>.
- Santra, Atanu, Somnath Mahato, S. Mandal, Sukabya Dan, Pratibha Verma, P. Banerjee, és Anindya Bose. „Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region”. *Advances in Space Research* 63, sz. 9 (2019): 2995–3008.
- Shoukry, Yasser, Paul Martin, Yair Yona, Suhas Diggavi, és Mani Srivastava. „PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks”. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1004–15. CCS '15. New York, NY, USA: Association for Computing Machinery, 2015. <https://doi.org/10.1145/2810103.2813679>.
- Shukla, Raj Mani, és Shamik Sengupta. „Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application”. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 688–94. IEEE, 2018.
- Straßenverkehrsgesetz (StVG), Pub. L. No. BGBl. I 2003 S. 310 (1909).
- Syfullah, Mohammad, és Joanne Mun-Yee Lim. „Data broadcasting on Cloud-VANET for IEEE 802.11p and LTE hybrid VANET architectures”. In *2017 3rd International Conference on Computational Intelligence Communication Technology (CICT)*, 1–6, 2017. <https://doi.org/10.1109/CICT.2017.7977321>.
- U.S. Department of Transportation. *Preparing for the Future of Transportation: Automated Vehicles 3.0*. Washington: U.S. Department of Transportation, 2019.
- Wolf, Marko, André Weimerskirch, és Christof Paar. „Security in automotive bus systems”. In *In: Proceedings of the Workshop on Embedded Security in Cars (escar) '04*, 2004.
- Woo, Samuel, Hyo Jin Jo, és Dong Hoon Lee. „A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN”. *IEEE Transactions on Intelligent Transportation Systems* 16, sz. 2 (2015. április): 993–1006. <https://doi.org/10.1109/TITS.2014.2351612>.
- Yan, Chen, Wenyuan Xu, és Jianhao Liu. „Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle”. *Def Con* 24, sz. 8 (2016): 109.
- Zhao, Meiyuan, Jesse Walker, és Chieh-Chih Wang. „Security challenges for the intelligent transportation system”, 2012. 0 17., 107–15. <https://doi.org/10.1145/2490428.2490444>.

Mellékletek

1. számú melléklet (ábrajegyzék)

1. ábra Az önvezető közúti jármű rendszer elemei (saját szerkesztés, forrás: Kyounggon Kim és mtsai.).....	4
2. ábra A CAN hálózat felépítése (saját szerkesztés, forrás: Jiajia Liu és mtsai.)	7
3. ábra Az önvezetést biztosító rendszer elemek (saját szerkesztés).....	8
4. ábra Az operációs rendszerréteg bemutatása (saját szerkesztés, forrás: Takuya Azumi, Yuya Maruyama, és Shinpei Kato).....	11
5. ábra Intelligens Közlekedési Rendszer lehetséges felépítése (saját szerkesztés, forrás: Mohammed Saeed Al-kahtani 2012; Mohammad Syfullah és Joanne Mun-Yee Lim 2017) ..	14
6. ábra Önvezető járművekkel kapcsolatos szabályozás az USA-ban (saját szerkesztés forrás: https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx)	34
7. ábra A posztok érzelmi töltet (saját szerkesztés, forrás: Senit One)	60
8. ábra A posztok megjelenési platformjai (saját szerkesztés, forrás: Senit One).....	61
9. ábra Kormegoszlás a kitöltők között (saját szerkesztés, forrás: kérdőív)	63
10. ábra A kitöltők megoszlása az általuk lakott település méret szerint (saját szerkesztés, forrás: kérdőív).....	64
11. ábra Kitöltés megoszlása a hazai önvezető járművek elterjedésének időbeli meghatározásában (saját szerkesztés, forrás: kérdőív).....	65

2. számú melléklet (táblázat jegyzék)

1. táblázat Automatizálás szintjének meghatározása (saját szerkesztés, forrás: „J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, https://www.sae.org)	5
2. táblázat A CAN keret felépítése (saját szerkesztés, forrás: https://www.kvaser.com/can-protocol-tutorial/##canMessages)	8
3. táblázat Terminológiákkal és definíciókkal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/)	38
4. táblázat Fejlett vezetőt segítő rendszer funkciókkal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	39

5. táblázat Csatlakozással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	42
6. táblázat Emberi interakcióval kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	49
7. táblázat Járműfedélzeti rendszerekkel, hálózatokkal, adatokkal és interfészekkel kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/)	50
8. táblázat Mérnöki tevékenységekkel kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/)	51
9. táblázat Térképpel szolgáltatással és helymeghatározással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	51
10. táblázat Adatvédelemmel és Információbiztonsággal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	52
11. táblázat Biztonsággal kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	53
12. táblázat Teszteléssel, ellenőrzéssel és validálással kapcsolatos szabványok (saját szerkesztés, forrás: NHTSA 2018, ENISA 2019, https://www.connectedautomateddriving.eu/).....	54
13. táblázat Klaszterelemzés eredménye (saját szerkesztés, forrás: SPSS)	66
14. táblázat Kruskal-Wallis tesztet szignifikancia eredmény (saját szerkesztés, forrás: SPSS)	67
15. táblázat Kruskal-Wallis tesztet rangátlag eredménye egyes (saját szerkesztés, forrás: SPSS).....	67
16. táblázat Kruskal-Wallis tesztet szignifikancia eredmény (saját szerkesztés, forrás: SPSS)	68
17. táblázat Kruskal-Wallis tesztet rangátlag eredménye egyes (saját szerkesztés, forrás: SPSS).....	69
18. táblázat Adatmegosztás hajlandóságának vizsgálata előre meghatározott esetekben (saját szerkesztés, forrás: SPSS)	70

3. számú melléklet (rövidítések jegyzéke)

Rövidítés	Rövidítés jelentése
ACK	Acknowledge
CAN	Controller Area Network, továbbiakban
CNN	Convolutional Neural Networks
CRC	Cyclic Redundancy Check
DoS	Denial of Service
DRFM	Digital Radio Frequency Memory
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Units
ENISA	European Union Agency for Cybersecurity
FCC	Federal Communication Commission
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transport System
LiDAR	Light Detection and Ranging
LIN	Local Interconnect Network
MAC	Message Authentication Code
ML	Machine Learning
NHTSA	National Highway Transportation Safety Administration
OBU	On-Borad Unit
PNT	Navigation and Timing
PyCRA	Physical Challenge-Response Authentication
ROS	Robot Operating System
RSU	Road-Side Unit
RTOS	Real-Time Operating System
RTR	Remote Transmit Request
TLS	Transport Layer Security
VANET	Vehicular Ad hoc Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything

Rövidítés	Rövidítés jelentése
WAVE	Wireless Access in Vehicular Environments

4. számú melléklet (kérdőív)

1. Kérem adja meg a nemét?
 - Nő
 - Férfi
2. Kérem válassza ki életkorának megfelelő csoportot.18-25
 - 26-33
 - 34-41
 - 42-49
 - 50-57
 - 58-65
 - 65 év felett
3. Hol lakik Ön?
 - Budapest,
 - Megyei jogú város,
 - Megyeszékhely,
 - Város,
 - Falu
4. Mi az Ön befejezett legmagasabb iskolai végzettsége?
 - Általános iskolai végzettség
 - Szakmunkás bizonyítvány
 - Érettségi
 - Alapszakos diploma
 - Mesterszakos diploma
 - Felsőoktatási szakképzés
 - Posztgraduális képzés
5. Mi az ön elsődleges közlekedési módja?
 - saját tulajdonú közlekedési eszköz
 - tömegközlekedés
 - Motorkerékpár
 - Sétálás/kerékpározás/rollerezés
 - egyéb

6. Milyen gyakran vezetett gépjárművet az elmúlt 12 hónapban?
- nem vezettem
 - havonta egyszer
 - havonta többször
 - hetente egyszer
 - hetente többször
 - minden nap
7. Hallott már valaha önvezető autó kifejezésről?
- igen
 - nem
8. Mit gondol a következő állításról? A teljesen önvezető autó ötlete lenyűgöző tud lenni.
- 1=teljesen nem értek vele egyet
 - 5=teljesen egyet értek vele
9. Mit gondol a következő állításról? A manuális vezetés szórakoztató.
- 1=teljesen nem értek vele egyet
 - 5=teljesen egyet értek vele
10. Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.
- 1=teljesen nem értek vele egyet
 - 5=teljesen egyet értek vele
11. Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.
- 1=teljesen nem értek vele egyet
 - 5=teljesen egyet értek vele
12. Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.
- 1=teljesen nem értek vele egyet
 - 5=teljesen egyet értek vele
13. Van-e vagy valaha volt-e olyan fogyatékosága, amely akadályozta a manuális vezetésben?
- nem volt
 - látás romlás
 - mobilitási problémák
 - egyéb
14. Ön szerint melyik évtizedben lesz a legtöbb jármű képes a teljes önvezetésre Magyarországon?

- 20
- 30
- 40
- 50
- később

15. Mit gondola következő állításról? A részben automatizált vezetés könnyebb tud lenni a manuálisnál.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

16. Mit gondol, a következő állításról? A magasan automatizált vezetés könnyebb tud lenni a manuálisnál.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

17. Mit gondol, a következő állításról? A teljesen automatizált vezetés könnyebb tud lenni a manuálisnál.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

18. Mit gondol, a következő állításról? A teljesen automatizált vezetés egy tévképzet, és a tudósoknak más fontosabb kutatási területre kellene fókuszálniuk.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

19. Mit gondol, a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a környező járműveknek, hogy jobban összehangolhassa útját azokkal.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

20. Mit gondol, a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a jármű fejlesztőknek.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

21. Mit gondol, a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a biztosító társaságoknak.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

22. Mit gondol, a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a az úttest kezelő vállalatoknak.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

23. Mit gondol, a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson az egyes hatóságoknak (pl.: adóhatóság).

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

24. A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

25. A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

26. A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

27. A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

28. A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.

- 1=teljesen nem értek vele egyet
- 5=teljesen egyet értek vele

29. kérem, jelezze, miért szeretne teljesen önvezető járművet használni? (többet is választhat)

- Biztonságosabb
- Mert tudok más dologgal foglalkozni (pl.: ügyintézés)

- Mert felgyorsíthatja az utazást
- Mert csökkentheti a közlekedési dugókat
- Mert környezetbarátabb lehet
- Nem szeretnék teljesen önvezető járművet használni

30. kérem, jelezze, mikor szeretne teljesen önvezető járművet használni? (többet is választhat)

- ha a vezetés stresszes
- ha a munkámmal kell foglalkozzak
- ha fáradt vagyok
- mindennapi utazás során
- ha a vezetés unalmas
- ha alkoholt ittam
- Nem szeretnék teljesen önvezető járművet használni

5. számú melléklet (kérdőív kielemezés)

Quick Cluster

Initial Cluster Centers

	Cluster	
	1	2
Mit gondol a következő állításról? A manuális vezetés szórakoztató.	1	5
Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	4	1
Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	5	1
Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.	5	1

Iteration History^a

Change in Cluster Centers		
Iteration	1	2
1	2,758	2,782
2	,089	,107
3	,086	,110
4	,021	,028
5	,000	,000

a. Convergence achieved due to no or small change in cluster centers. The maximum absolute coordinate change for any center is ,000. The current iteration is 5. The minimum distance between initial centers is 7,550.

Final Cluster Centers		
	Cluster	
	1	2
Mit gondol a következő állításról? A manuális vezetés szórakoztató.	3	4
Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	4	3
Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	4	2
Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.	4	2

Number of Cases in each Cluster		
Cluster	1	2
Cluster	1	92,000
	2	71,000
Valid		163,000
Missing		,000

NPar Tests

Descriptive Statistics					
	N	Mean	Std. Deviation	Minimum	Maximum
Mit gondol a következő állításról? A manuális vezetés szórakoztató.	163	3,75	1,176	1	5
Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	163	3,80	1,084	1	5
Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	163	3,31	1,209	1	5
Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.	163	2,88	1,373	1	5
Cluster Number of Case	163	1,44	,497	1	2

Kruskal-Wallis Test

Ranks			
	Cluster Number of Case	N	Mean Rank
Mit gondol a következő állításról? A manuális vezetés szórakoztató.	1	92	68,55
	2	71	99,42
	Total	163	
Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	1	92	104,55
	2	71	52,77
	Total	163	
Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	1	92	113,78
	2	71	40,82
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.	1	92	112,39
	2	71	42,63
	Total	163	

Test Statistics^{a,b}

	Mit gondol a következő állításról? A manuális vezetés szórakoztató.	Mit gondol a következő állításról? A részben automatizált vezetés élvezetes tud lenni.	Mit gondol a következő állításról? A magasan automatizált vezetés élvezetes tud lenni.	Mit gondol a következő állításról? A teljesen automatizált vezetés élvezetes tud lenni.
Kruskal-Wallis H	18,505	52,404	101,303	91,342
df	1	1	1	1
Asymp. Sig.	,000	,000	,000	,000

a. Kruskal Wallis Test

b. Grouping Variable: Cluster Number of Case

NPar Tests

Descriptive Statistics					
	N	Mean	Std. Deviation	Minimum	Maximum
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	163	2,99	1,310	1	5
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.	163	3,84	1,094	1	5
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.	163	3,69	1,198	1	5

Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	163	3,64	1,138	1	5
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.	163	3,26	1,345	1	5
Cluster Number of Case	163	1,44	,497	1	2

Kruskal-Wallis Test

		Ranks	
	Cluster Number of Case	N	Mean Rank
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	Élvezetesnek tartja az autonóm vezetést	92	78,65
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	86,35
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.	Élvezetesnek tartja az autonóm vezetést	92	81,47
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	82,69
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben	Élvezetesnek tartja az autonóm vezetést	92	80,30
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	84,20

történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	Élvezetesnek tartja az autonóm vezetést	92	81,00
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	83,30
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.	Élvezetesnek tartja az autonóm vezetést	92	70,06
	Kevésbé tartja élvezetesnek az autonóm vezetést	71	97,47
	Total	163	

Test Statistics^{a,b}

	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.
Kruskal-Wallis H	1,123	,030	,295	,102	14,174
df	1	1	1	1	1

Asymp. Sig.	,289	,863	,587	,750	,000
-------------	------	------	------	------	------

a. Kruskal Wallis Test

b. Grouping Variable: Cluster Number of Case

Frequencies

		Statistics				
		Mit gondol a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a környező járműveknek, hogy jobban összehangolhass a útját azokkal.	Mit gondol a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a jármű fejlesztőknek.	Mit gondol a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson a biztosító társaságoknak.	Mit gondol a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson az egyes hatóságoknak (pl.: adóhatóság).	Mit gondol a következő állításról? Megengedném a járművemnek, hogy adatokat továbbítson az egyes hatóságoknak (pl.: adóhatóság).
N	Valid	163	163	163	163	163
	Missing	0	0	0	0	0
Mean		3,59	3,45	2,90	3,26	2,44
Median		4,00	4,00	3,00	4,00	2,00
Mode		4	4	4	4	1
Std. Deviation		1,195	1,282	1,308	1,373	1,267
Variance		1,429	1,644	1,711	1,884	1,606
Range		4	4	4	4	4
Minimum		1	1	1	1	1
Maximum		5	5	5	5	5
Sum		585	562	472	531	398

Kruskal-Wallis Test

		Ranks	
	onvezhasz2	N	Mean Rank
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	Használna önvezető járművet	121	74,65
	Nem használna önvezető járművet	42	103,17
	Total	163	

Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.	Használna önvezető járművet	121	79,26
	Nem használna önvezető járművet	42	89,90
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiléte miatt aggaszt.	Használna önvezető járművet	121	76,31
	Nem használna önvezető járművet	42	98,38
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	Használna önvezető járművet	121	74,89
	Nem használna önvezető járművet	42	102,48
	Total	163	
Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.	Használna önvezető járművet	121	75,36
	Nem használna önvezető járművet	42	101,13
	Total	163	

Test Statistics^{a,b}

	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a magánszféra sérülése miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a szoftverek feltörése vagy más rossz működés miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése az esetleges baleset bekövetkezéséből származó jogi felelősség címzettjének kiséte miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése ezen technológia általános biztonsága és megbízhatósága miatt aggaszt.	Mit gondol a következő állításról? A teljesen automatizált vezetési rendszerek széles körben történő bevezetése a vezetési élmény és kontrollérzet elvesztése miatt aggaszt.
Kruskal-Wallis H	11,985	1,752	7,338	11,417	9,747
df	1	1	1	1	1
Asymp. Sig.	,001	,186	,007	,001	,002

a. Kruskal Wallis Test

b. Grouping Variable: onvezhasz2