

Katona Gergő¹

Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész

Cybersecurity Aspects and Public Perception of Autonomous Road Vehicles Part 1

Absztrakt

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 egyes rendszerelemei egy belső hálózatban, továbbá a járművek egymással és a forgalomirányítási 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.

Kulcsszavak: autonómia, közlekedés, kiberbiztonság

Abstract

With the rise of embedded technologies and wireless capabilities, today's vehicles are no longer isolated mechanical machines. They are becoming part of an interconnected system

¹ Puskás Tivadar Műszaki Szakkollégium, e-mail: katona.gergo@uni-nke.hu

in which vehicles are constantly communicating with their individual system components in an internal network, as well as with each other and with the traffic control centre. This set of interconnected data is called a self-driving traffic management system. This system has the potential to support the future deployment of autonomous transport and to use artificial intelligence to significantly improve the safety, efficiency and sustainability of transport. However, the emergence of autonomous means of transport raises new security issues that make the whole system a potential target for cybersecurity attacks, which could endanger both transport safety and human life.

Keywords: autonomy, transport, cybersecurity

Problémafelvetés

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, ami 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 fogyatékossgal élők és a nem járművezetők számára is. Nagy fokú rugalmasságot és kényelmet kínálnak a pihenéshez, az olvasáshoz vagy akár a munkavégzéshez utazás közben, ami javítja a személyek hatékonyságát.²

Azonban ezt a fokú növekedést le kell követnie a biztonsági fejlesztéseknek és szabályozásoknak is. A technológiák műszaki-technikai és emberi oldala közötti^{3,4} megfelelő összhang csak így biztosítható. Egy önvezető közúti jármű számos olyan technológiából áll, amelyek képesek kommunikálni egymással egy belső hálózaton, illetve képesek egy külső hálózatba adatokat továbbítani és onnan adatokat fogadni. Ezenfelül a járművek különböző megoldásokkal térképezik fel a környezetet, és más-más döntési mechanizmust alkalmaznak. Mind a kommunikáció, mind az egyes rendszerelemek rendelkeznek gyengeségekkel, sérülékenységekkel, amelyek kihasználása súlyos következményekkel jár.⁵ Továbbá vizsgálandó terület e technológiáknak a társadalmi elfogadottsága is, illetve fontos felmérni azokat a félelmeket, amelyek megjelennek a társadalomban az önvezető járművek témakörében.

Jelen téma egy kétrészes cikksorozatban jelenik meg, amelynek ez a része bemutatja az autonóm közúti járművek felépítését, valamint a téma előfordulását a különböző közösségimédia-felületeken, illetve hírportálokon.

A második cikk az egyes autonóm rendszerelemeket fenyegető kockázatokat tárja fel, illetve azokat a megoldásokat, amelyek e kihívásokat hivatottak megszüntetni.

² Lásd: www.precedenceresearch.com/autonomous-vehicle-market

³ DEUTSCH et al. 2019.

⁴ DEUTSCH-BERÉNYI 2023: 10–15.

⁵ MEGYERI-FARKAS 2017: 205–206; PARÁDA-FARKAS 2020: 159–182.

Ezenfelül bemutatom kérdőíves felmérésem eredményét, amelynek középpontjában az autonóm közúti járművek társadalmi megítélésének vizsgálata állt.

Kutatási módszertan

A cikkben megjelenő eredménytermékekhez megvizsgáltam egy state-of-art analízissel, hogy milyen technológiai megoldásokra van szükség az önvezető közúti járművek kialakításához. Szentimentanalízist végeztem, amelyben megvizsgáltam, hogy a világhálón, globális szinten az önvezető járművekkel kapcsolatos tartalmak hol és milyen formában jelennek meg.

Eredmények

Az autonóm vezetés műszaki aspektusai

Autonóm vezetés definiálása

Ahhoz, hogy megvizsgáljuk az autonóm közlekedési eszközök egyes aspektusait, fontos tisztázni, hogy mit is értünk autonóm jármű alatt. Ki kell hangsúlyozni, hogy az önvezetés fogalmát jelen kutatásban műszaki kontextusban használom fel.

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.⁶ Tehát az autonóm rendszer olyan műszaki egység, amely bizonyos feladatokat ellát anélkül, hogy bármilyen emberi parancsoktól függene. Azonban, hogy műszaki értelemben részletesen tudjuk vizsgálni az önvezető járműveket, pontosabb definícióra lesz szükség. Ehhez szükséges egy olyan definíciós rendszer, amely kategorikus különbségeket tesz az automatizálás különböző módjai (szintjei) között. Erre az autóiipari mérnökök globális szövetsége, a SAE International jelentését használtam fel, amelynek címe *A közúti gépjárművek vezetési automatizálási rendszereivel kapcsolatos kifejezések taxonómiája és meghatározása* (J3016™ szabványként is ismert).

A jelentés a vezetési automatizálás hat szintjét határozza meg az automatizálás nélkülítől a teljes automatizálásig. A kulcsfontosságú különbség a 2. és a 3. szint között van, hogy míg a 2. szinten a vezető végzi a dinamikus vezetési feladat egy részét, addig 3. szinten az automatizált vezetési rendszer látja el a dinamikus vezetési feladatok többségét. A 3. szint felett szintenként egyre nagyobb részt végez el a jármű e vezetési feladatokból. Azonban fontos definiálnunk a „dinamikus vezetési feladat” fogalmát, amely magában foglalja a vezetési feladat operatív részét (például

⁶ Jo-KIM-SUNWOO 2018.

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 utazástervezés).⁷

Jelen cikkben az önvezető közúti járművek három fő rendszerelemét azonosítjuk és elemezzük kiberbiztonsági szempontból. E rendszerelemek megvizsgálásakor törekedtem a teljesen automatizált járműkategória feltérképezésére. A három rendszerelem csoportosításánál fontos azt kiemelni, hogy ezek a rendszerek nem szeparálhatók el egymástól teljesen, hiszen például egy GNSS- (Global Navigation Satellite System) technológia elősegíti az önvezetést mint képességet, illetve a kommunikációt is, hiszen képes a helyzetét kommunikálni a környezetével.

Gépjárművezérlő rendszerek

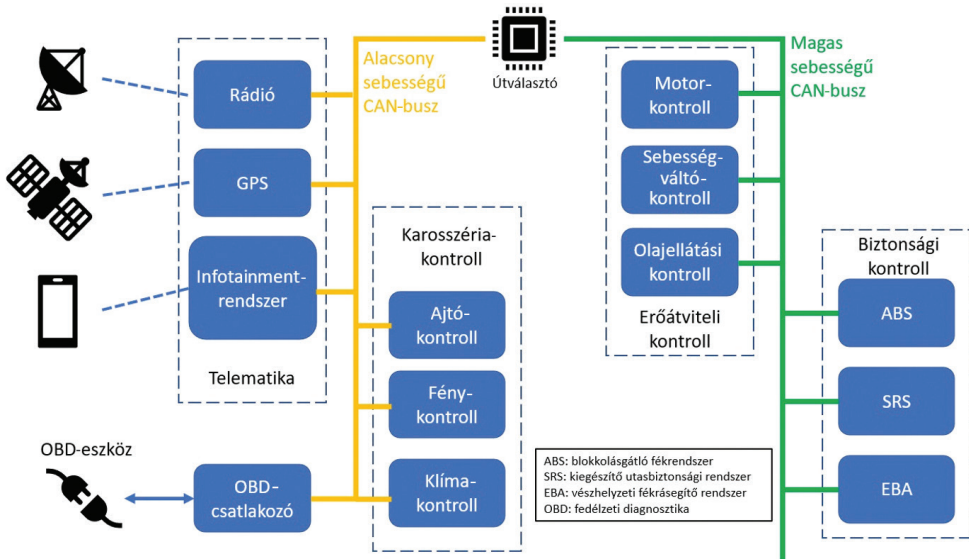
Az egyik legfontosabb egység ebben a kategóriában az elektronikus vezérlőegység (*electronic control units*, ECU). Az ECU vezérli például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zár, a légzsák, a légkondicionáló rendszer és a fényvezérlés moduljait.⁸ Jellemzően a kis és közepes méretű járművek körülbelül 50 ECU-t tartalmaznak, és legalább 70-et foglalnak magukban a luxusautók. Egyes csúcscategóriás 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*, CAN), a helyi összekötő hálózatot (*local interconnect network*, LIN), ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak. A FlexRay egy új generációs busztechnológia, amely nagy sebességű és hibatűrő kommunikációt biztosít.⁹ Jelen vizsgálat a CAN-hálózat felépítésére és sebezhetőségeire fókuszál, mivel ez a hálózat a legelterjedtebb az autópárhazban. Az 1. ábra mutatja be egy közúti gépjármű belső hálózatát, amely CAN-buszhálózatot használ. Jól látható, hogy ennek a buszrendszernek két típusa van. Az alacsony sebességű CAN-hálózat főleg a telematika és a karosszéria kontrollegységeiért felel, míg a magas sebességű rendszer főleg a jármű konkrét vezérléséért. Itt található meg az erőátvitelért felelős ECU-k, mint például a sebességváltó kontrollja vagy a motor kontrollja.¹⁰

⁷ SAE International 2021.

⁸ TÓTH 2017: 195–206.

⁹ KIM et al. 2021: 102–150.

¹⁰ LIU et al. 2017: 50–58.



1. ábra: A CAN-hálózat felépítése

Forrás: a szerző szerkesztése Liu et al. 2017: 50–58. alapján

Az ebbe a CAN-hálózatba kapcsolt ECU-k az üzeneteket CAN-keretbe küldik meg egymásnak. A CAN-keret felépítése az 1. táblázatban látható.

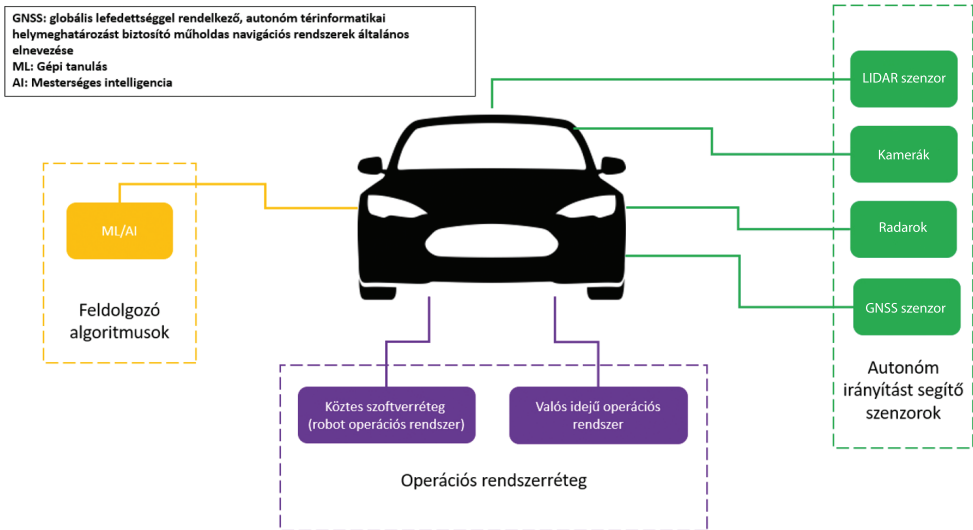
1. táblázat: A CAN-keret felépítése

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 végén van, és ezt a bitet a vevő felülírja, ezzel tudatja a küldővel, hogy a küldés sikeres.
End of Frame	Ez a szakasz jelenti az üzenet végét.

Forrás: a szerző szerkesztése www.kvaser.com/can-protocol-tutorial/##canMessages alapján

Autonóm vezetési rendszerelemek

A 2. ábrán láthatók azon rendszerelemcsoportok, amelyek az önvezetést mint funkciót biztosítják. E fejezetben az ábrán megjelölt rendszerelemek bemutatása következik.



2. ábra: Az önvezetést biztosító rendszerelemek

Forrás: a szerző szerkesztése

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 átalakítja és feldolgozza, legtöbbször a gépi tanulás technológiáját alkalmazva. Ezen érzékelőknek különböző feladata van távolságérzékelés szerint:

- Közel érzékelés (0–5 m): az ultrahangos érzékelők olyan közelségérzékelők, amelyek célja az akadályok érzékelése a karosszériától néhány méteren belül. Elsősorban alacsony sebességű forgatókönyvekhez, például parkolásegítéshez tervezték őket.
- Kis hatótávolságú érzékelés (5–30 m): az előre néző kamerákat a sávelhagyásra figyelmeztetésre, a jelzőtáblák felismerésére, a hátrafelé néző kamerákat pedig parkolásegítésre használják.
- Közepes hatótávolságú érzékelés (80–160 m): a LiDAR és a közepes hatótávolságú radarok (*medium range radars*, MRR) az ütközésselkerülést és a gyalogosok felismerését biztosítják.

- Nagy hatótávolságú érzékelő (160–250 m): A nagy hatótávolságú radarok (*long-range radars*, LRR) adaptív sebességtartó automatika számára biztosítanak információkat, főleg nagy sebességnél.¹¹

Ezeket az autonóm vezetést elősegítő érzékelőket a következő módon definiálhatjuk:

- A globális navigációs műholdrendszer egy műholdalapú helymeghatározó, navigációs és időmérő (Position, Navigation and Timing, PNT) rendszer. Jelenleg számos GNSS van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által használt globális helymeghatározó rendszer (Global Positioning System, GPS) vitathatatlanul a legismertebb. Mindazonáltal az európai vezetésű GALILEO, az orosz vezetésű GLONASS, a kínai BeiDou, az India által vezetett IRSS és a japán QZSS mellett áll.¹² 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. Továbbá az intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges e szenzorok alkalmazása.
- Több érzékelő, például a fényérzékelő és távolságmérő szenzor (Light Detection and Ranging, LiDAR), a kamerák, a radar és az 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 koordinátákkal, valamint a pont intenzitásából. Ezeket az adatokat dolgozza fel a rendszer, és detektálja az akadályokat.¹³
- 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 környezetéről. A kamerák olyan fontos autonóm feladatokhoz nyújtanak információkat, mint például a közlekedési táblák felismerése és a sávfelismerés.¹⁴ 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.
- A radar olyan érzékelő, amely elektromágneses hullámokat bocsát ki a rádió- vagy mikrohullámú tartományban, hogy észlelje a tárgyakat és mérje távolságukat és sebességüket a visszavert jelek érzékelésével. Az önvezető járművek esetében a radarok számos alkalmazásban hasznosak. Például a kis hatótávolságú

¹¹ YAN-XU-LIU 2016.

¹² SANTRA et al. 2019: 2995–3008.

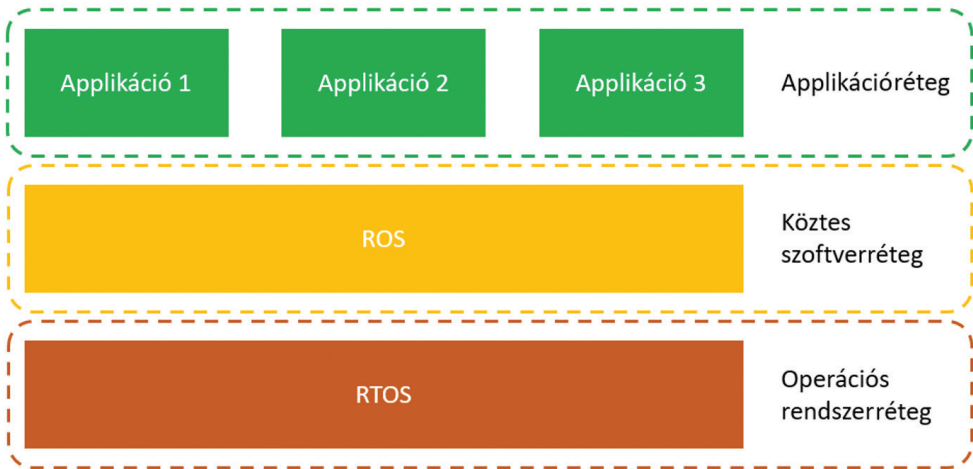
¹³ CAO et al. 2019: 2267–2281.

¹⁴ BAR HILLEL et al. 2014: 727–745.

radarok lehetővé teszik a parkolás elősegítését. A nagy hatótávolságú radarok pedig segítik az automatikus távolságszabályozást és fékrásegítést.¹⁵

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 rendszer (*real-time operating system*, 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*, ROS) segítségével éri el.



3. ábra: Az operációs rendszerréteg bemutatása

Forrás: a szerző szerkesztése Azumi–Maruyama–Kato 2020. alapján

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 határidőket határoznak meg, és a feladatokat az adott időkereten belül kell végrehajtani, különben a késlekedés katasztrofális következményekkel járhat, például légszákrendszer esetében. A puha rendszernél annak válaszideje 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 üzeneteket tesz közzé a ROS-on keresztül, és mind a lokalizációs

¹⁵ YAN–XU–LIU 2016.

szolgáltatás, mind az akadályérzékelő szolgáltatás lekéri a közzétett képeket, hogy helyzet- és akadályfrissítéseket generáljon.¹⁶

Feldolgozó algoritmusok

Az automatizált vezetési rendszerek gyors fejlődésével a biztonságos vezetési környezethez elengedhetetlen a stabil és megbízható környezetelemzés. A feldolgozó algoritmusok olyan megoldások, amelyek az egyes autonóm közlekedést segítő szenzorok adatait dolgozzák fel, például a kameraalapú útszegmentálásnak mára már számos megoldása létezik. Ez a feldolgozás a 3. ábrán, az applikációrétegen megy végbe. E 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 lévő objektumok helyét is. Ezenkívül pontos objektumhatár-információkat szolgáltat.¹⁷ Az egyik ilyen technológiai megoldás a konvolúciós neurális hálózat (*convolutional neural networks*, CNN), amelyet már alkalmaznak számos járműmodellnél.

Külső kommunikációt támogató rendszerelemek

A külső kommunikációt részlegesen érintettem a szenzorok esetében, amikor például a GNSS-szenzort vizsgáltam, illetve a CAN-rendszerrel 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, amely nem más, mint az intelligens közlekedési rendszer (*intelligent transport system*, ITS), amely az összekapcsolt járművek rendszere. Ahol a járművekbe épített érzékelők és egy központi közlekedésirányítási rendszer adatai alapján a jármű képes az intelligens döntéshozatalra.¹⁸

Ez a rendszer azért is hangsúlyos, mert ezáltal a járműveknek nem csak a saját adataikra kell támaszkodniuk, például olyan esetekben, amikor a beépített szenzorok nem, vagy csökkent képességekkel rendelkeznek,¹⁹ 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*, VANET) megy végbe. Ez a VANET három fő kommunikációs típust különböztet meg:

¹⁶ AZUMI–MARUYAMA–KATO 2020.

¹⁷ CHEN et al. 2020.

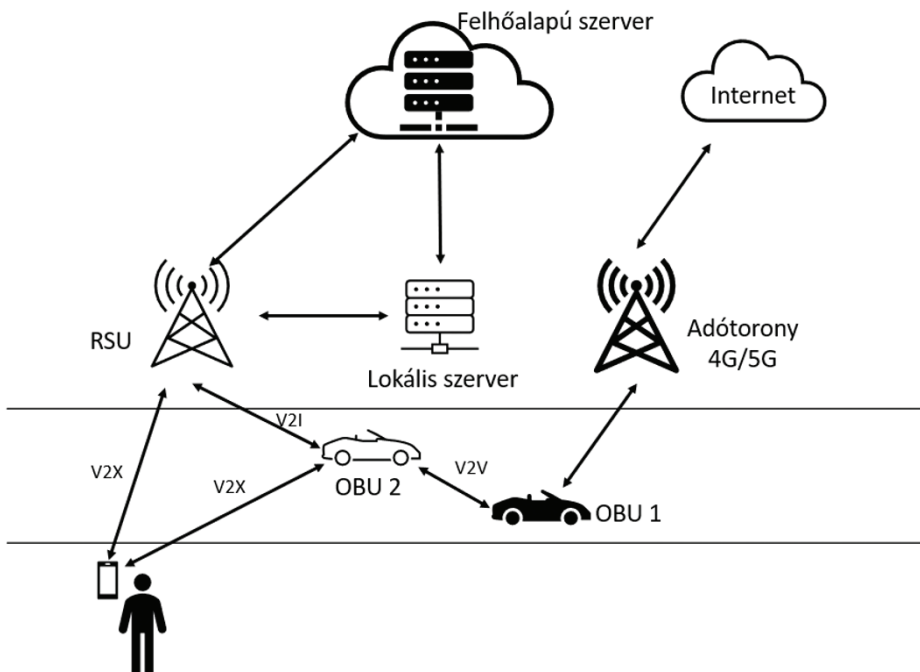
¹⁸ ZHAO–WALKER–WANG 2012: 107–115.

¹⁹ ORBÓK 2015: 221–226.

- V2V (vehicle-to-vehicle) kommunikáció, amely a járművek egymással való kommunikációja;
- V2I (vehicle-to-infrastructure) kommunikáció, amely a járművek és a környező infrastruktúra kommunikációja;
- V2X (vehicle-to-everything) kommunikáció, amely a legtágabb csoport, magában foglalja az előző két területet, és tovább bővíti olyan eszközökkel, amelyek képesek a kommunikációra, illetve helyzetmeghatározásra, ilyen például a gyalogosok okostelefonja.²⁰

Fontos az ITS-ben részt vevő elemeket is azonosítani, amelyek kommunikálnak egymással. Ezek a következők:

- fedélzeti egység (*on-board unit*, OBU), amely a járművekbe szerelt adóvevő;
- út menti egység (*road-side unit*, RSU), olyan adóvevő, amely 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;
- felhőalapú számítási réteg az, amely kezelheti a földi szervereken kívül az ITS-adatokat.²¹



4. ábra: Intelligens közlekedési rendszer lehetséges felépítése

Forrás: a szerző szerkesztése AL-KAHTANI 2012; SYFULLAH–LIM 2017. alapján

²⁰ MOSTAFA et al. 2011: 756–761.

²¹ AL-KAHTANI 2012; SYFULLAH–LIM 2017.

A VANET három fő kommunikációs szabványt használ, amelyeket dedikáltak a járművek kommunikációjára alakítottak ki.

- Dedikált rövid távú kommunikáció (Dedicated Short Range Communications, DSRC) 75 MHz-es sávzélességű spektrumban található 5850–5925 GHz között. Ezt az amerikai Szövetségi Kommunikációs Bizottság (Federal Communication Commission, FCC) jelölte ki a jármű kommunikációja számára. A DSRC sáv 7 dedikált csatornára lett felosztva.
- A Villamos és Elektronikai Mérnöki Intézet (Institute of Electrical and Electronics Engineers, IEEE) által kiadott 1609 szabványcsalád a vezeték nélküli hálózati hozzáférésekkel foglalkozik a járműkörnyezetben (Wireless Access in Vehicular Environments, WAVE). E szabványok olyan architektúrát és szabványosított szolgáltatásokat, valamint interfészeket határoznak meg, amelyek lehetővé teszik a biztonságos VANET kommunikációt.²²
- 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.²³

Az autonóm vezetés társadalmi megítélése

A cikkben 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. Jelen cikkben a téma online platformokon való megjelenésének különböző aspektusait mutatom be. A cikksozart második részében a társadalmi megítélés vizsgálatának kérdőívől származó eredménye jelenik majd meg.

Onlinetartalom-analízis

Ebben a fejezetben megvizsgáljuk, hogy az önvezető járművek témája miként jelenik meg az interneten. Ehhez a SentiOne²⁴ weboldalt használtam, amely teljes világot lefedő, 70 nyelvet feldolgozó és webes szöveganalitikán alapuló social listening szoftver. Ez kulcsszavas keresés alapján, valós időben vagy akár 3 évre visszamenőleg figyel, indexálja és elemzi az internetes fórumokon, blogokon, weboldalakon és közösségimédia-csatornákon közzétett publikus szöveges tartalmak minden típusát, amelyek önmagukban vagy kontextusukban tartalmazzák a felhasználó által már előre definiált és a platformra felvitt kulcskifejezések bármelyikét. A SentiOne jelenlegi adattárházában

²² MEJRI – BEN-OTHTMAN – HAMDI 2014: 53–66.

²³ IEEE 2010.

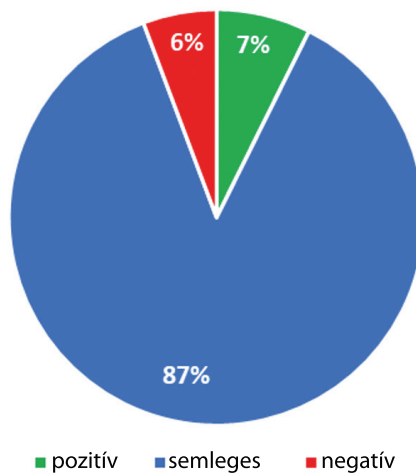
²⁴ Lásd: <https://sentione.com/hu>

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 socialmedia-oldalokról a hivatalos és nyilvános API-hozzáféréseken keresztül gyűjti be az adatokat. Például a legnépszerűbb Facebook-oldalak automatikusan bekerülnek a rendszerbe, az új oldalakat pedig a rendszerben már korábban is használt, felhasználói kulcsszóbázis alapján keresi és találja meg a technológia. A releváns tartalmakat kvantitatív kutatás céljából és ezt megkönnyítendő, különböző fókuszpontok és kutatási paraméterek mentén rendezi össze, amelyeket interaktív grafikonokon ábrázol. A kvalitatív mélyelemzéseket is támogató módszertani, technológiai felépítés pedig biztosítja a kutatáshoz kapcsolódó összes indexált tartalom, poszt, komment, cikk és említés egyenkénti elemzésének és kategorizálásának lehetőségét is.²⁵

Az elemzés részletei

A vizsgált időtartam 2019. április 3-tól 2022. március 5-ig terjedt, ahol a következő kulcsszavakra 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, amelyek a szentimentanalízis szerint 86,93%-a semleges megjegyzés volt, közel 5,73%-a negatív és 7,33%-a pozitív.



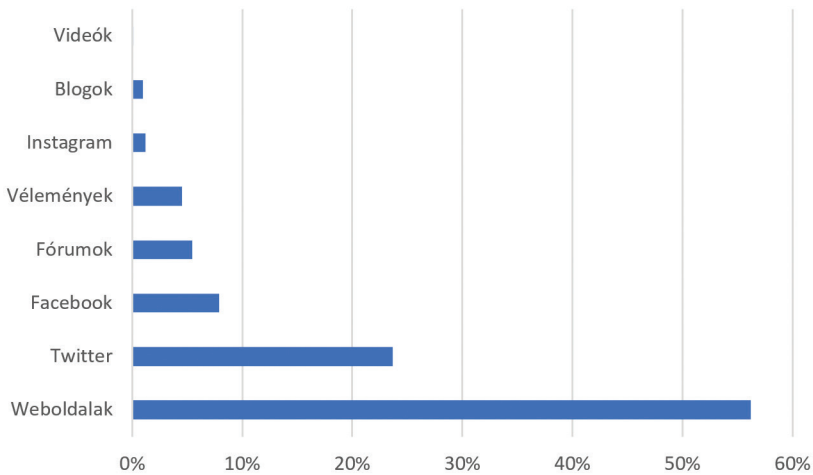
5. ábra: A posztok érzelmi töltete

Forrás: a szerző szerkesztése a SentiOne alapján

²⁵ BÁNYÁSZ-TÓTH-LÁSZLÓ 2022: 99–125.

A SentiOne algoritmus 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, amelyben nem írnak semmit az adott tartalomról, amelyben a kulcsszavak szerepelnek, így az algoritmus nem tudja a megosztó látásmódját vizsgálni. Azonban ez a magas arány azzal is magyarázható, hogy a megosztások nagy része informatív jellegű volt, vagyis a megosztó személy vagy oldal információt akart megosztani a témában, nem pedig véleményét kifejezni.

Ezenfelül megvizsgáltam, hogy milyen platformokon fordultak elő a vizsgált kifejezések. Itt az látható, hogy a weboldalakon jelenik meg legnagyobb arányban az önvezető járművekről tartalom 56%-kal, ezt követi az X (amely a vizsgálat ideje alatt a Twitter nevet viselte) 24%-kal, majd a Facebook 8%-kal és a fórumok és vélemények 5-5%-kal, míg a blogok és az Instagram 1-1%-kal. Ez a megosztás magyarázatot ad arra, hogy a szentimentanalízis során miért volt ilyen nagy arányú a semleges érzelmű tartalom, mivel a weboldalakon a szerzők nem a véleményüket írták le, hanem a témával kapcsolatban információt szándékoztak megosztani.



6. ábra: A posztok megjelenési platformjai

Forrás: a szerző szerkesztése a SentiOne alapján

Jelen esetben a weboldalak olyan szakmai és hírközlő oldalakat jelentenek, mint a VentureBeat,²⁶ a Green Car Reports²⁷ vagy a Forbes²⁸ magazin.

Így azt lehet megállapítani, hogy az önvezetés témája az online térben szakmai és híroldalakra korlátozódik, és nem épült be még szervesen a közösségimédia-platformokra. Ennek magyarázata az lehet, hogy jelenleg csak egyes autonóm funkciók

²⁶ VentureBeat: <https://venturebeat.com/>

²⁷ Green Car Reports: www.greencarreports.com/

²⁸ Forbes: www.forbes.com/

érhető el a közúti járművekben, ami még nem alkalmas biztonságos önvezetés biztosítására.

Összegzés

A jelen cikkben megjelenő kutatási eredmény rámutatott arra, hogy az önvezető közúti járművek nem azonosíthatók különálló rendszerként, hanem inkább egy ökoszisztéma tagjaként. Ezen ökoszisztémának számos más szereplője is lehet, más-más technológiával és céllal. A technológiai vizsgálat azonban arra is rámutatott, hogy a jármű egyes rendszerelem típusait sem tudjuk elszigetelten külön kezelni. A járművön belüli rendszerek is nagyban függenek az egymástól kapott információktól, ami felértékeli a kiberbiztonság három alapelvének (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos meglétét. Az online térben az látható, hogy az önvezetés témaköre jelenleg a szakmai és híroldalakra korlátozódik.

Irodalomjegyzék

- AL-KAHTANI, Mohammed Saeed (2012): Survey on Security Attacks in Vehicular ad hoc Networks (VANETs). *2012 6th International Conference on Signal Processing and Communication Systems*. IEEE, 1–9. Online: <https://doi.org/10.1109/ICSPCS.2012.6507953>
- AZUMI, Takuya – MARUYAMA, Yuya – KATO, Shinpei (2020): ROS-lite: ROS Framework for NoC-Based Embedded Many-Core Platform. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 4375–4382. Online: <https://doi.org/10.1109/IROS45743.2020.9340977>
- BÁNYÁSZ Péter – TÓTH András – LÁSZLÓ Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom*, 22(1), 99–125. Online: <https://doi.org/10.22503/inftars.XXII.2022.1.6>
- BAR HILLEL, A. et al. (2014): Recent Progress in Road and Lane Detection: A Survey. *Machine Vision and Applications*, 25, 727–745. Online: <https://doi.org/10.1007/s00138-011-0404-2>
- BEDERNA, Zsolt – SZÁDECZKY, Tamás (2021): Modelling Computer Networks for Further Security Research. *Security and Defence Quarterly*, 36(4), 51–66. Online: <https://doi.org/10.35467/sdq/141572>
- CAO, Yulong et al. (2019): Adversarial Sensor Attack on Lidar-based Perception in Autonomous Driving. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2267–2281. Online: <https://doi.org/10.1145/3319535.3339815>
- CHEN, Ping-Rong et al. (2020): DSNet: An Efficient CNN for Road Scene Segmentation. *APSIPA Transactions on Signal and Information Processing*, 9(1), e27. Online: <https://doi.org/10.1017/ATSIP.2020.25>

- DEUTSCH Nikolett et al. (2019): *A technológia szerepének stratégiai felértékelődése: Szemlvények a stratégiai technomenedzsment témaköréből*. Budapest: Budapesti Corvinus Egyetem.
- DEUTSCH Nikolett – BERÉNYI L. (2023): A technomenedzsment funkciói. *Magyar Minőség*, 32(6), 10–15.
- IEEE (2010): 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, 2010: 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), 1–51. Online: <https://doi.org/10.1109/IEEESTD.2010.5514475>
- JO, Kichun – KIM, Chansoo – SUNWOO, Myoung-ho (2018): Simultaneous Localization and Map Change Update for the High Definition Map-Based Autonomous Driving Car. *Sensors*, 18, 3145. Online: <https://doi.org/10.3390/s18093145>
- KIM, Kyounggon et al. (2021): Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Computers & Security* 103, 102–150. Online: <https://doi.org/10.1016/j.cose.2020.102150>
- LIU, Jiajia et al. (2017): In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. *IEEE Network*, 31(5), 50–58. Online: <https://doi.org/10.1109/MNET.2017.1600257>
- MEGYERI Lajos – FARKAS Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök*, 12(3), 198–209.
- MEJRI, Mohamed Nidhal – BEN-OTHTMAN, Jalel – HAMDJ, Mohamed (2014): Survey on VANET Security Challenges and Possible Cryptographic Solutions. *Vehicular Communications*, 2(1), 53–66. Online: <https://doi.org/10.1016/j.veh-com.2014.05.001>
- MOSTAFA, Ahmad et al. (2011): A V2X-based Approach for Reduction of Delay Propagation in Vehicular Ad-Hoc Networks. In *2011 11th International Conference on ITS Telecommunications*, IEEE, 756–761. Online: <https://doi.org/10.1109/ITST.2011.6060155>
- ORBÓK Ákos (2015): Az autonóm közlekedési technológia kihívásai. *Társadalom és Honvédelem*, 19(1), 221–226. Online: <http://real.mtak.hu/50243>
- PARÁDA István – FARKAS Tibor (2020): Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák. *Hadmérnök*, 15(1), 159–182. Online: <https://doi.org/10.32567/hm.2020.1.11>
- SAE International (2021): *J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Online: www.sae.org/standards/content/j3016_202104/
- SANTRA, Atanu et al. (2019): Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region. *Advances in Space Research*, 63(9), 2995–3008. Online: <https://doi.org/10.1016/j.asr.2018.04.020>
- SYFULLAH, Mohammad – LIM, Joanne Mun-Yee (2017): Data Broadcasting on Cloud-VANET for IEEE 802.11p and LTE Hybrid VANET Architectures. *2017 3rd International*

- Conference on Computational Intelligence Communication Technology (CICT), IEEE*, 1–6. Online: <https://doi.org/10.1109/CICT.2017.7977321>
- TÓTH András (2017): Information Security for Electric Cars in Accordance with Nist Critical Infrastructure Cybersecurity Framework. *Hadmérnök*, 12(4), 195–206.
- YAN, Chen – XU, Wenyuan – LIU, Jianhao (2016): *Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle*. Def Con.109.
- ZHAO, Meiyuan – WALKER, Jesse – WANG, Chieh-Chih (2012): Security Challenges for the Intelligent Transportation System. In *Proceedings of the First International Conference on Security of Internet of Things*, ACM, 107–115. Online: <https://doi.org/10.1145/2490428.2490444>