Az önvezető technológia alkalmazása

Viktor Patrik

Egyetemi tanársegéd, Óbudai Egyetem Keleti Károly Gazdasági Kar,
viktor.patrik@uni-obuda.hu

Garai-Fodor Mónika

Egyetemi docens, Óbudai Egyetem Keleti Károly Gazdasági Kar,
fodor.monika@kgk.uni-obuda.hu

Absztrakt: A tudományos vizsgálat az autonóm vezetési rendszerek által jelentett veszélyek körülhatárolásával foglalkozik. Kezdetben széles körű szakirodalmi áttekintést végeztek az önvezető technológiával kapcsolatos alapvető fogalmak és értékelési kritériumok kifejtése érdekében. Ezt követően az információbiztonság és annak sokrétű dimenzióinak átfogó feltárására kerül sor. A kutatás tovább vizsgálja a hálózati és informatikai fenyegetéseket, elemezve azok következményeit és következményeit az autonóm vezetési rendszerek összefüggésében. Végül következtetéseket vonunk le ezen eredmények szintézise alapján, betekintést nyújtva az önvezető motorok által jelentett átfogó fenyegetésekbe.

Kulcsszavak: Önvezető, AV, IT

1 Bevezetés

Az önvezető technológia fejlődése az autóipari innováció új korszakát nyitotta meg, amely példátlan kényelmet és biztonságot ígér az utakon. Ahogy azonban ezek a rendszerek fejlődnek, úgy nőnek az általuk támasztott kihívások is, különösen az információbiztonság területén. Ebben a kutatási vállalkozásban a motorok önvezető rendszereinek bonyolultságába merülök bele, elsősorban az információbiztonsági fenyegetésekre való fogékonyságukra összpontosítva - egy olyan területre, amely a jelenlegi kutatások keretein belül még viszonylag feltáratlan. Mivel a piacon nincsenek 3. szintű önvezető motorok, ez a tanulmány kiterjeszti hatáskörét az alacsonyabb szintű önvezető technológiákra is, azzal a céllal, hogy átfogó betekintést nyújtson a működési dinamikájukba és a kapcsolódó kockázatokba. A kutatás kontextusba helyezése érdekében *a* Society of Automotive Engineers (SEA) skálája által meghatározott automatizáltsági fokozatok mélyreható vizsgálatára kerül sor. Ez az osztályozási keretrendszer az

önvezető rendszereken belül az autonómia fokozatosan növekvő szintjeit határozza meg, az ember által irányított járművektől a nulladik szintig, a teljesen automatizált rendszerekig, amelyek képesek önállóan navigálni a különböző út- és környezeti körülmények között az ötödik szinten. Ez a kategorizálás megteremti az alapot az önvezető technológiák és a velük járó kihívások fejlődésének megértéséhez. A vizsgálat továbbá túlmutat a műszaki előírásokon, és kiterjed az önvezető technológiák elterjedésével járó társadalmi-gazdasági és etikai dimenziókra is. Különösen érdekes a felelősség és az etikai döntéshozatal vitatott kérdése, ahol az autonóm járművek tetteiért való felelősséggel kapcsolatos kérdések nagy jelentőséggel bírnak. Ez a sokrétű diskurzus hangsúlyozza, hogy az önvezető technológia bevezetésének jogi, etikai és társadalmi következményeit árnyaltan kell megérteni.

Az empirikus meglátásokra való törekvés során az iparági szakemberekkel készített interjúkat tartalmazó elsődleges kutatás értékes szempontokat kínál az önvezető motorokat fenyegető információbiztonsági veszélyekről. A fizikai támadásoktól a szoftver- és adatbehatolásokig terjedő legfontosabb fenyegetési vektorok azonosításán és elemzésén keresztül e tanulmány célja az önvezető rendszerekben rejlő biztonsági sebezhetőségek sokrétű természetének felvázolása.

Végső soron ez a kutatás arra törekszik, hogy hozzájáruljon az önvezető technológia fejlődő tájképének átfogó megértéséhez, rávilágítva az elterjedését kísérő információbiztonsági kihívásokra. E gyorsan fejlődő terület összetettségének és árnyalatainak megvilágításával a tanulmány célja, hogy tájékoztassa az érdekelt feleket és a politikai döntéshozókat egyaránt, elősegítve a megalapozott döntéshozatalt és a kialakuló fenyegetések elleni védelmet szolgáló szilárd biztonsági keretrendszerek kidolgozását.

2 Szakirodalmi áttekintés

Az önvezető rendszerek fejlesztése és alkalmazása új korszakot nyitott az autóiparban és a közúti közlekedésben. Ezek a technológiák ígéretesek, és óriási potenciállal bírnak a közúti biztonság és mobilitás szempontjából. Az innováció magas foka figyelhető meg ezen a területen (Varga, 2023a; Varga, 2023b), amelyek jelentősen hozzájárulnak nemcsak az autóipar, hanem a nemzetgazdaságok gazdasági növekedéséhez is (Varga, 2023c). Azonban, mint minden új technológiának, az önvezető rendszereknek is számos kihívással és hibával kell szembenézniük(Anderson et al., 2016). Az önvezető rendszerek egyik legjelentősebb hibája az emberi beavatkozás hiánya. Bár az autonóm járművek képesek önállóan navigálni és döntéseket hozni, még mindig vannak olyan helyzetek, amikor emberi beavatkozásra van szükség a biztonságos vezetéshez. Ez különösen akkor jelent problémát, ha a jármű hirtelen és váratlanul rossz döntést hoz, és az emberi vezetőnek nincs ideje reagálni vagy átvenni az irányítást

(Bimbraw, 2015). Az önvezető rendszerek másik gyakori problémája a szoftverhibák és meghibásodások kockázata. Az autonóm járművek működése nagyszámú érzékelőn és szoftveren alapul, amelyek környezeti információkat gyűjtenek és dolgoznak fel. Ha ezen alkatrészek bármelyike meghibásodik, az komoly veszélyt jelenthet az utasokra és a többi közlekedőre. Például egy meghibásodott radarérzékelő vagy egy rosszul kalibrált kamera balesethez vagy más súlyos incidenshez vezethet. (Gkartzonikas & Gkritza, 2019)

Az önvezető rendszerek hibái között fontos megemlíteni az erkölcsi dilemmákat is.(Goodall, 2014) Az autonóm járműveknek olyan helyzetekben kell döntéseket hozniuk, amikor az emberi élet vagy vagyon veszélybe kerülhet.(Grigorescu, 2020) Például egy balesetelkerülő manőver kiválasztásakor az autonóm járműnek el kell döntenie, hogy az ember számára melyik kimenetel a legkevésbé kockázatos.

Ezek a döntések etikai és morális kérdéseket vetnek fel, és további elemzést igényelnek a legjobb megoldások meghatározásához. (Hevelke & Nida-Rümelin, 2015), (Koopman & Wagner, 2017).

Az önvezető rendszerek hiányosságai közül a biztonsági szempontoknak kiemelt figyelmet kell szentelni. Bár az autonóm járművek célja a közlekedésbiztonság javítása, egyes hibák és sebezhetőségek esetén ennek ellenkezője is bekövetkezhet. (Litma, 2020), (Luettel, 2012) Például hackerek kihasználhatják a szoftverhibákat vagy a hálózati sebezhetőségeket, hogy támadásokat hajtsanak végre az autonóm járművek ellen, ami súlyos következményekkel járhat. (Milakis & Van Wee, 2017)

Az önvezető rendszerek hibái és kockázatai ellenére azonban fontos megérteni, hogy ezek a technológiák folyamatosan fejlődnek, és számos pozitív előnnyel járnak. A fejlesztők és a gyártók érdekérvényesítése és elkötelezettsége a biztonság és a megbízhatóság mellett kulcsfontosságú a közúti közlekedésbiztonság és az autonóm közlekedés széles körű elfogadásához. Az önvezető rendszerek hibáinak és kockázatainak kezelése az innováció és a technológiai fejlődés természetes része, és a jövőben további fejlesztések várhatók a szakértők és az iparági szereplők együttműködésével.(Najm et al.,2006) A fejlesztők és a gyártók elkötelezettsége a biztonság és a megbízhatóság mellett kulcsfontosságú.

2.1 Az automatizálás foka és etikai megfontolások

Az önvezető technológián belüli automatizáltsági szintek megértése kiemelkedő fontosságú az autonóm járművek fejlődő tájképének megértéséhez. A Society of Automotive Engineers (SEA) skálája átfogó keretet biztosít e szintek kategorizálására, felbecsülhetetlen betekintést nyújtva az önvezető rendszerek képességeibe és korlátaiba. (Nunes & Coughlin, 2018).

A nulladik szinten nincs automatizálás, a járművek teljes mértékben az emberi irányításra vannak utalva. Az egyes szint korlátozott automatizálást vezet be, lehetővé téve az olyan feladatok részleges átruházását, mint a kormányzás vagy a sebességváltás, miközben az irányítás túlnyomórészt a vezető kezében marad. A második szint jelentős előrelépést jelent a részleges automatizálással, ahol a fékezési, gyorsítási és kormányzási folyamatok egyidejűleg koordinálhatók, bár a vezető megtartja a végső irányítást. (Paden et al., 2016)

A harmadik szintre való áttérés jelentős mérföldkövet jelent, mivel a rendszer átveszi a dinamikus vezetési műveletek irányítását, bár szükség esetén emberi beavatkozásra is lehetőség van. A piacon már elérhető szint célja, hogy kiegészítse a vezető döntéshozatali képességeit, és olyan beavatkozásokkal támogassa, mint az elektronikus stabilitásszabályozás és a sávtartó asszisztens, miközben az összetettebb feladatok továbbra is a vezető hatáskörében maradnak. (Schwartig et al., 2018)

A továbblépés, a negyedik fokozat az automatizálás magas szintjét hirdeti meg, felhatalmazva a rendszert az összetett vezetési műveletek, köztük a kormányzás, a gyorsítás és a lassítás felügyeletére és végrehajtására. Figyelemre méltó, hogy a rendszer még azokban az esetekben is átveszi az irányítást, amikor a járművezető nem reagál megfelelően a beavatkozási kérésekre.(Shladover,2018) Az automatizálás csúcspontja az ötödik szinten valósul meg, ahol a teljes autonómia megvalósul. Ebben az állapotban a rendszer jártasságot mutat a különböző út- és környezeti körülmények között való navigálásban, és képes emberi kezelő jelenléte nélkül vezetni. Az ilyen előrelépések aláhúzzák az önvezető technológia átalakító potenciálját a mobilitási és közlekedési paradigmák újradefiniálásában. (Smith, 2016) A műszaki előírásokon túl az önvezető technológia elterjedése számtalan etikai és erkölcsi dilemmát vet fel, amelyek közül a legfontosabb a felelősség kérdése. Az autonóm járművek által hozott döntésekért való elszámoltathatóság megosztása továbbra is vitatott kérdés, amely különböző területek érdekelt feleinek különböző nézőpontjait váltja ki. (Thrun ,2010)

Egyesek egy egyszerű megközelítés mellett érvelnek, amely az önvezető rendszerek fejlesztésében, gyártásában vagy üzemeltetésében részt vevő személyek felelősségét jelöli ki. A gépi tanulás és az autonóm döntéshozatal bonyolultsága azonban bonyolítja a helyzetet, és kérdéseket vet fel az emberi ellenőrzés és felelősségre vonhatóság mértékét illetően az előre nem látható események vagy rendszerhibák esetén. (Vahidi, & Sciarretta, 2018),(Wadud et al, 2016)

Míg a gépek figyelemre méltó képességeket mutatnak a logikai kereteken alapuló etikai döntések meghozatalában, az erkölcs szubjektív jellege árnyalt megközelítést tesz szükségessé az etikai normák programozásához. Ráadásul az etikai normák közösségek közötti változékonysága aláhúzza az autonóm rendszerek etikus viselkedését szabályozó szabványosított irányelvek szükségességét. (Waymo,2019) Ezen etikai problémák megoldása során feltétlenül

fel kell ismerni a gépi intelligencia korlátait, és el kell ismerni az emberi ítélőképesség nélkülözhetetlen szerepét az erkölcsi keretek kialakításában. Amíg nem születik általánosan elfogadott megoldás, addig az autonóm technológia etikai következményeit övező diskurzus tovább fog fejlődni, utat nyitva új elméletek és nézőpontok megjelenésének. (Xu et al.,2018)

A jármű-jármű kommunikáció, más néven V2V (Vehicle-to-Vehicle) kommunikáció egy olyan technológia, amely lehetővé teszi az autonóm járművek számára, hogy közvetlenül kommunikáljanak egymással, emberi beavatkozás nélkül. Azonban, mint minden új technológiának, a V2V-kommunikációnak is számos kihívással és hibával kell szembenéznie, amelyek megakadályozhatják vagy korlátozhatják hatékonyságát és megbízhatóságát.(Yurtsever et al., 220) A V2V-kommunikáció egyik fő kihívása az interoperabilitás hiánya. Mivel a különböző gyártók különböző kommunikációs rendszereket fejleszthetnek ki, nehézségek merülhetnek fel a járművek közötti összekapcsolt kommunikációban. Az eltérő protokollok és szabványok miatt előfordulhat, hogy egyes járművek nem tudnak megfelelően kommunikálni egymással, ami csökkentheti a rendszer hatékonyságát és megbízhatóságát. (Zhang & Guhathakurta, 2018), (Zhao et al., 2015)

Egy másik fontos probléma a V2V-kommunikáció hibrid infrastruktúrája. Bár a V2V-kommunikáció alapvetően a járművek közötti közvetlen kommunikáción alapul, néha szükség lehet egy hálózati infrastruktúrára, például út menti egységekre vagy felhőalapú szolgáltatásokra a járművek közötti kommunikáció támogatásához és kiegészítéséhez. Ennek következtében az infrastruktúra meghibásodása vagy meghibásodása negatív hatással lehet a V2V-kommunikációra és annak hatékonyságára. (Zmud et al., 2017) Egy másik gyakori probléma a V2V-kommunikáció biztonsága és adatvédelme. Mivel a jármű-jármű kommunikáció során nagy mennyiségű érzékeny adat kerül megosztásra, mint például a pozíció, a sebesség és az útvonalterv, fontos biztosítani, hogy ezek az adatok védve legyenek a rosszindulatú támadások és a hackerek ellen. Az adatok megsértése és a sebezhetőségek kockázatot jelenthetnek a felhasználók személyes adataira és a járművek működésére. (Csiszárik et al., 2022) A V2V-kommunikációs hibák másik fontos problémája az időzítés és a szinkronizáció hiánya. A kommunikációs üzenetek időzítése és szinkronizálása kulcsfontosságú a jármű-jármű kommunikáció hatékonysága és megbízhatósága szempontjából. Az időzítési hibák vagy a szinkronizálás hiánya ahhoz vezethet, hogy a járművek nem képesek megfelelően észlelni és reagálni egymás jelenlétére és viselkedésére, ami balesetekhez vezethet. (Csiszárik et al., 2022), (Csiszárik et al., 2021) Az infrastrukturális korlátok szintén jelentős problémát jelenthetnek a V2V-kommunikációban. Például az alacsony lefedettségű területeken vagy városi környezetben a jármű-jármű kommunikáció hatékonysága csökkenhet, ami növelheti a balesetek kockázatát és csökkentheti a rendszer általános megbízhatóságát. (Csiszárik, 2023)

Összességében a V2V-kommunikáció hibái és kihívásai jelentős akadályai lehetnek az autonóm közlekedés széles körű elfogadásának és bevezetésének. E problémák kezelése kulcsfontosságú ahhoz, hogy a V2V-kommunikáció biztonságos és hatékony eszközzé váljon a közúti közlekedésben, hozzájárulva a balesetek számának csökkentéséhez és az utasok biztonságának növeléséhez. (Csiszárik, 2022)

3 Módszertan

Az elsődleges kutatási módszertan szerves részeként mélyinterjúkat készítettem 14 szakos tanár különböző csoportjával. Az elsődleges cél az volt, hogy aprólékosan értékeljem az önvezető motorokat fenyegető sokrétű veszélyeket, különös tekintettel az információbiztonság területére. Az elemzés megkönnyítése érdekében átfogó Muhai-Bodka fenyegetéstérképet dolgoztam ki, amely egy strukturált keretrendszer, amely az önvezető rendszerekben rejlő potenciális biztonsági sebezhetőségek megkülönböztetésére és kategorizálására készült.

Az egyes interjúkat aprólékosan megterveztem, hogy a releváns területeken nagy tapasztalattal és szakértelemmel rendelkező szakértőktől árnyalt betekintést nyerjek. Különböző hátterük és nézőpontjaik gazdagították az adatgyűjtési folyamatot, felbecsülhetetlen értékű nézőpontokat kínálva az önvezető technológia és az információbiztonsági aggályok bonyolult kölcsönhatásáról.

Az interjúk során számos kiemelkedő téma merült fel, amelyek megvilágították az autonóm rendszerek járműtechnológiába való integrálása által támasztott számtalan kihívást. Az önvezető motorok fizikai támadásokkal szembeni érzékenységétől kezdve a szoftver- és adatbehatolások bonyolultságáig a beszélgetések a biztonsági sebezhetőségek bonyolult árnyalataiba merültek, holisztikus képet nyújtva a fenyegetésekről.

Az interjúk emellett platformként szolgáltak az iparági szakemberek közötti párbeszéd és együttműködés előmozdítására, és elősegítették a lehetséges biztonsági kockázatok közös kezelését és mérséklését célzó együttműködési szellem kialakulását. Az interakciókból származó meglátások nem csak a Muhai-Bodka veszélytérkép kidolgozásához szolgáltak információval, hanem megalapozták a későbbi elemzéseket és ajánlásokat is, amelyek célja az önvezető motorok biztonsági helyzetének megerősítése.

A jövőben az interjúkból származó szintetizált eredmények a további empirikus vizsgálatok alapköveként szolgálnak majd, lehetővé téve az önvezető technológia területén az információbiztonsági fenyegetések és sebezhetőségek átfogó értékelését. Az iparági szakemberek szakértelmének és perspektíváinak felhasználásával ez a kutatás arra törekszik, hogy hozzájáruljon olyan robusztus biztonsági keretrendszerek kialakításához, amelyek képesek megvédeni az

autonóm rendszereket a felmerülő fenyegetésekkel szemben, és ezáltal elősegítik az önvezető technológia elfogadásába vetett bizalmat.

Company	**work experience**	**schedule**
Knorr-Bremse	5-10	Expert
MAGE	2-5	Expert
University of Győr	5-10	Teacher
Bosch	5-10	Manager
Knor-Bremse	30-40	Expert
TATA consulting	30+	Manager
TRW	15-25	expert
Denso	30+	Expert
Audi hungary	40+	Manager
Lear	2-5	Expert
Hyundai Mobis	5-10	Expert
Valeo	15-20	Manager
Yazaki	20-25	Expert
Adient	30+	Expert
Thyssenkrup	2-5	Manager

1. táblázat: Szakértők
Forrás: saját kutatás

A kutatásom megalapozása során alapos vizsgálatba kezdtem a legkritikusabb fenyegetések azonosítását és rangsorolását az iparági szakértőkkel folytatott kiterjedt interjúk segítségével. E megbeszélések során a szakértők között konszenzus alakult ki az önvezető motorkerékpárok sebezhetőségét illetően, különösen a fizikai biztonsági fenyegetések tekintetében, négykerekű társaikhoz képest.A szakértők hangsúlyozták továbbá, hogy az önvezető autók területén a hálózati problémák potenciális kihívásokat jelentenek. Kiemelték, hogy az önvezető motorok eredendő örömszerző jellege, amely a felhasználók jelentős részét (kb. 70-80%-át) vonzza, akadályozhatja a zökkenőmentes jármű-jármű (V2V) kommunikációt, és veszélyeztetheti a balesetmentes vezetésre irányuló kezdeményezéseket. A szakértők emellett megjegyezték, hogy a moduláris önvezető rendszerek motorkerékpárokra történő telepítése inherens módon bonyolult, és ezt a nehézséget öt fő akadályozó tényezőnek tulajdonították:

- Leolvashatóság

- Helyhiány

- Az internetkapcsolat hiánya

- Rezonanciaproblémák

- Változó időjárási körülményeknek való kitettség

E kihívások ellenére a szakértők együttesen elutasították az önvezető járművek terrorcselekményekben való lehetséges felhasználására vonatkozó kérdéseket. Ezt a döntést a szakértők 80%/20%-os megosztottsága indokolta, akik olyan konkrét feltételeket és körülményeket említettek, amelyek miatt az ilyen forgatókönyvek nem megvalósíthatóak. Ehelyett azt állították, hogy a különböző járműtípusok jellemzői és működési dinamikája alapján a hagyományos járműveket alkalmasabbnak tartják az ilyen cselekmények végrehajtására. Összességében ezek a szakértői interjúkból nyert meglátások szilárd alapot nyújtanak az önvezető technológia motorkerékpáros és hagyományos autóipari keretekbe történő integrációját övező árnyalt veszélyek és összetettség megértéséhez. Ezek az empirikus adatok a későbbi elemzések és ajánlások során az önvezető rendszerek biztonságának és ellenálló képességének megerősítését célzó, valós forgatókönyvekben történő megerősítését szolgálják.

• **80% not possible**	• **20% possible**
• Cannot be started independently	• Group attack
• Would be ineffective	• Linking
• driving modification can be modified	• Watch
• Not suitable for Personal Attack	•

2. táblázat : Szakértői vélemény az önvezető autók elleni terrortámadásról
Forrás:Saját kutatás

A következő szakaszokban elmélyedek a kutatásom központi témájában: az információbiztonságot övező fenyegetésekben. Vizsgálatom során a szakértők között e kritikus kérdéssel kapcsolatban eltérő véleményekkel találkoztam, ami arra késztetett, hogy nézőpontjaikat három különböző csoportba soroljam:

Fizikai veszélyek:

Egyes szakértők az önvezető rendszereket fenyegető fizikai fenyegetések jelentőségét hangsúlyozták. Ezek az aggodalmak a rosszindulatú szereplők azon lehetősége körül forognak, hogy fizikailag manipulálják vagy veszélyeztetik az autonóm járművek integritását, veszélyt jelentve mind az utasokra, mind a járókelőkre nézve.

Szoftvertámadás:

A szakértők egy másik csoportja a szoftveres támadás fenyegető veszélyét emelte ki elsődleges aggodalomra okot adó területként. Ez azt jelenti, hogy az önvezető rendszerekbe rosszindulatú szoftverek vagy rosszindulatú programok szivárognak be, amelyek manipulálhatják vagy megzavarhatják a kritikus szoftverkomponensek normális működését, ami potenciális biztonsági kockázatokhoz és működési zavarokhoz vezethet.

Adatfeltörés:

A szakértői vélemények harmadik kategóriája az önvezető rendszerek adatbehatolással szembeni sebezhetőségével foglalkozott. Ez magában foglalja az autonóm járművek által tárolt vagy továbbított érzékeny adatokhoz való jogosulatlan hozzáférést, ami aggályokat vet fel az adatvédelemmel, a titoktartással, valamint a személyes vagy védett információk esetleges kihasználásával kapcsolatban.

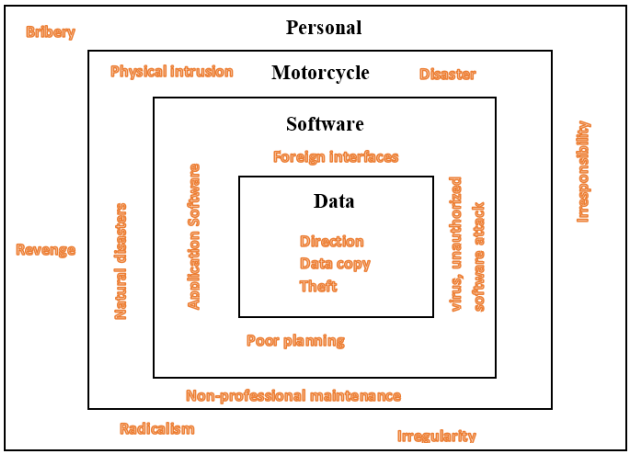
Az e különböző nézőpontokból nyert meglátások összegzése során a szakértők több kulcsfontosságú hatást azonosítottak:

Kompromittált biztonság: Az önvezető rendszerek biztonságát és integritását jelentősen veszélyezteti a fizikai manipuláció vagy a szoftver manipulációjának lehetősége, ami balesetekhez vagy más kedvezőtlen kimenetelű eseményekhez vezethet.

Működési zavarok: A szoftveres behatolások és az adatok megsértése megzavarhatja az autonóm járművek normál működését, ami a rendszer meghibásodásához, kiszámíthatatlan viselkedéshez vagy akár teljes leálláshoz vezethet.

Adatvédelem megsértése: Az adatbehatolások aggodalomra adnak okot az önvezető rendszerekben tárolt érzékeny információkhoz való jogosulatlan hozzáférés vagy azok kihasználása miatt, ami veszélyezteti az egyének személyes adatainak magánéletét és bizalmas jellegét.

E sokrétű fenyegetések és a hozzájuk kapcsolódó hatások átfogó elemzésével e kutatás célja, hogy megvilágítsa az információbiztonság és az önvezető járművek biztonságos és hatékony működése közötti összetett kölcsönhatást. Ezek a meglátások a robusztus biztonsági intézkedések és kockázatcsökkentési stratégiák kidolgozását segítik elő, biztosítva az autonóm technológia folyamatos fejlődését és elfogadását oly módon, hogy a biztonság, a védelem és a felhasználói bizalom prioritást élvezzen.



1. ábra: Kölcsönhatások
Forrás: saját kutatás

A szakértői vélemények alapján a fenyegetések három fő kategóriába sorolhatók. Azok a szakértők, akik a fizikai támadásokra összpontosítottak, a terrortámadások, a szakszerűtlen működés és a megvesztegetés potenciális veszélyeit emelték ki. E csoport szemében a fő kockázati tényezők közé tartoznak az autonóm járművek elleni célzott támadások, amelyeket terrorista cselekmények vagy szándékos gondatlanság okozhat.

Ezzel szemben a szoftveres fenyegetésekre összpontosító szakértők a V2V (vehicle-to-vehicle) kommunikációra és a vezérlés biztonságára összpontosítottak. Számukra a legaggasztóbb kockázatok közé tartoznak a jármű-jármű kommunikáció manipulálására vagy az autonóm vezérlőrendszer manipulálására irányuló potenciális támadások.

A szakértők harmadik csoportja az adatok és az adatvédelem védelmét tartotta kiemelkedően fontosnak. Számukra a legveszélyesebb fenyegetések közé tartoztak az adatvesztés, a vagyoni károk és a rossz tervezés, amelyek az autonóm járművek működésével kapcsolatos adatok biztonságát és sértetlenségét veszélyeztetik.

E különböző veszélykategóriák részletes vizsgálata segít megérteni az autonóm járművekhez kapcsolódó biztonsági kockázatok sokféleségét és összetettségét. A stratégiák és a biztosítékok kifejlesztett alapú az aggodalmak által kifejezett szakértők lehetővé teszi a hatékony védelmet a potenciális veszélyek ellen, hogy autonóm járművek, ezáltal megkönnyíti a megjelenése és a telepítés a biztonságos és megbízható autonóm közlekedés.

4 Eredmények

Az autonóm vezetési rendszerek biztonsági vonatkozásait vizsgáló vizsgálatunk sokrétű veszélytérképet tárt fel, amelyet 14 iparági szakértő meglátásai gazdagítottak. E tanulmány célja az önvezető motorokat fenyegető információbiztonsági fenyegetések körüli komplexitások feltárása volt, a strukturált elemzéshez egy szigorú Muhai-Bodka-féle fenyegetéstérképet használva. Az e szakemberekkel készített interjúk rávilágítottak az önvezető technológiák bonyolult kihívásaira, a fizikai támadásoktól a szoftver- és adatbehatolásokig. A mélyinterjúkat tartalmazó elsődleges kutatás során a szakértők egyetértettek abban, hogy az önvezető motorkerékpárok különösen a fizikai biztonságot fenyegető veszélyek tekintetében kifejezetten sebezhetőek. Kiemelték a hálózati bonyodalmak lehetőségét, különös tekintettel a jármű-jármű (V2V) kommunikációra gyakorolt hatásokra. A szakértők az autonóm technológiák bevezetésének potenciális akadályaként azonosították a felhasználók mintegy 70-80%-a által keresett "flow" élményt, mivel az kihívást jelent a zökkenőmentes V2V interakciók és a balesetek megelőzése szempontjából. A moduláris önvezető rendszerek motorkerékpárokon történő bevezetésének fő akadályai a következők voltak: olvashatósági problémák, térbeli korlátok, következetlen internetkapcsolat, rezonanciaproblémák és a változó időjárási körülményeknek való kitettség. E kihívások ellenére az önvezető járművek terrorista tevékenységekre való felhasználásának gondolatát a szakemberek túlnyomórészt elutasították, a járművek jelenlegi működési dinamikája és a vezérlési mechanizmusok alapján történő kivitelezhetetlenségre hivatkozva. Az elemzés a szakértői vélemények alapján három fő kategóriába sorolta a

fenyegetettséget: Fizikai fenyegetés: Néhány szakértő kiemelte, hogy ezek közé tartoznak az autonóm járművek fizikai integritásának esetleges manipulálásából vagy veszélyeztetéséből eredő kockázatok. Szoftver behatolás: Az egyik jelentős aggodalomra okot adó tényező a rosszindulatú szoftverek behatolása, amelyek manipulálhatják vagy megzavarhatják az autonóm rendszerek működését. Data Intrusion: Az érzékeny adatokhoz való jogosulatlan hozzáféréssel kapcsolatos aggodalmak, hangsúlyozva az autonóm rendszerek sebezhetőségét a magánélet megsértésével és az adatok kihasználásával szemben. A veszélykategóriákba való betekintés kiemeli, hogy az azonosított sebezhetőségek kezelésére átfogó biztonsági intézkedésekre van szükség. A kollektív nézőpontokból árnyalt megértés alakult ki a fenyegetések mérsékléséhez szükséges megelőző intézkedésekről és stratégiai beavatkozásokról. A szakértők egyetértettek abban, hogy kiemelkedően fontos a szilárd biztonsági keretrendszerek és protokollok kidolgozása a fizikai, szoftveres és adatbehatolások elleni védelem érdekében, biztosítva ezzel az önvezető technológiák biztonságát és integritását. A szakemberek meglátásai óvatos optimizmusra utaltak az önvezető járművek V2V-kommunikációjának fejlődési ütemét illetően. Az autonóm vezetési technológiák zökkenőmentes integrációja előtt kihívást jelent, hogy a felhasználók az autózás során az „áramlás" élményét részesítik előnyben. Ezen túlmenően az önvezető motorkerékpárok korlátozott képessége önálló terrorista akciók végrehajtására azt sugallja, hogy a biztonsági megfontolások szűkebb körben, elsősorban a csoportos támadásokra és a biztonságos V2V-működésre összpontosítanak. A szakértők eltérő nézetei a fenyegetettségi szintek részletes vizsgálatához vezettek, és a fizikai támadásokhoz, a szoftverek sebezhetőségéhez és az adatbiztonsághoz kapcsolódó konkrét kockázatokat azonosították. Az adatbiztonság prioritásként való kezelése alapvető kihívásként jelent meg, kiemelve a potenciális támadások elleni védelem kritikus szerepét az önvezető technológiák biztonságos és megbízható közúti közlekedésben való alkalmazásának biztosítása érdekében. Tanulmányunk megvilágítja az autonóm vezetési technológiák és az információbiztonsági fenyegetések összetett kölcsönhatását, szakértői meglátásokra támaszkodva feltérképezi az uralkodó kihívásokat és a lehetséges enyhítési stratégiákat. Az önvezető technológiák fejlődésével párhuzamosan elengedhetetlen a kifinomult biztonsági intézkedések kidolgozása az azonosított fenyegetések kezelése és ezen átalakító innovációk biztonságos, megbízható és a felhasználók bizalmát élvező bevezetésének biztosítása érdekében." Ez az »Eredmények« című szakasz a dokumentum legfontosabb megállapításait foglalja össze, az önvezető technológiák biztonsági fenyegetéseire és az iparági szakértők által nyújtott meglátásokra összpontosítva. Hangsúlyozza e kihívások összetett jellegét és a fejlett biztonsági intézkedések kritikus szükségességét az autonóm vezetési rendszerek biztonságának és megbízhatóságának biztosítása érdekében.

Összefoglalás

Kutatásaim arra a következtetésre vezettek, hogy a V2V (vehicle-to-vehicle) kommunikáció az önvezető járművekben és következésképpen a biztonságosabb vezetés nem fog olyan ütemben megvalósulni, mint ahogy azt a szakértők gondolják. Ez részben azért van így, mert a sok felhasználó által keresett és értékelt „flow" autózás élményét az önvezető technológia nem tudja könnyen elérni. Az is fontos megállapítás, hogy az önvezető motorkerékpárok kevésbé képesek önállóan terrorcselekményeket elkövetni, ami tovább korlátozhatja e technológiák fejlődését.

A szakértők szerint a csoportos támadásoknak nagyobb az esélyük, és hatékonyabbak lehetnek, mint az egyéni támadások, ezért biztonsági szempontból ezekre kellene a fő hangsúlyt fektetni. Ezért, V2V kommunikáció és a biztonságos működés volt tekinthető elsődleges fontosságú.

A fenyegetések terén a szakértők három fő részre osztották a veszélyeket, és ezek alapján különböző veszélyességi szinteket határoztak meg. A különböző fenyegetések és hatásuk részletes elemzése három különböző táblázatban kerül bemutatásra. Ezen belül az adatbiztonságot kiemelték, mint kulcsfontosságú mérföldkövet és az önvezető autók egyik legalapvetőbb kihívását. Az adatbiztonság fenntartása és a potenciális támadások elleni hatékony védekezési stratégiák kidolgozása alapvető fontosságú az önvezető technológia biztonságos és megbízható közúti közlekedésben történő bevezetésének biztosításához.

Hivatkozások

[1] Anderson, J. M., Kalra, N., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, O. A. (2016). Autonomous vehicle technology: A guide for policymakers. RAND Corporation.

[2] Bimbraw, K. (2015). Autonomous cars: Past, present, and future: A review of the developments in the last century, the present scenario, and the expected future of autonomous vehicle technology. Proceedings of the 12th International Conference on Informatics in Control, Automation and Robotics (ICINCO).

[3] Csiszárik-Kocsir, Á. (2021). Customer Preferences in Bank Selection before and after the Pandemic in the Light of Financial Culture and Awareness. Acta Polytechnica Hungarica 18(11), pp. 151-169.

[4] Csiszárik-Kocsir, Á. (2022). The Present and Future of Banking and New Financial Players in the Digital Space of the 21st Century. Acta Polytechnica Hungarica 19(8), pp. 143-160.

[5] Csiszárik-Kocsir, Á. (2023). The Purposes and Motivations of Savings Accumulation based on Generational Affiliation, Financial Education and Financial Literacy. Acta Polytechnica Hungarica, 20(3).

[6] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2021). What has Become Important during the Pandemic?–Reassessing Preferences and Purchasing Habits as an Aftermath of the Coronavirus Epidemic through the Eyes of Different Generations. Acta Polytechnica Hungarica, 18(11), pp. 49-74..

[7] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2022). Generation-specific analysis of the pandemic's impact on financial culture. In: IEEE (ed.) IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) : Proceedings, IEEE, pp. 201-205.

[8] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2022). Preference system for the choice of savings in a generation-specific approach of the financial culture before and after the coronavirus pandemic. In: Szakál, Anikó (ed.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022, pp. 287-291.

[9] Gkartzonikas, C., & Gkritza, K. (2019). What have we learned? A review of stated preference and choice studies on autonomous vehicles. Transportation Research Part C: Emerging Technologies, 98, pp. 323-337.

[10] Goodall, N. J. (2014). Machine ethics and automated vehicles. In Road Vehicle Automation , pp. 93-102. Springer.

[11] Grigorescu, S. M., Trasnea, B., Cocias, T., & Macesanu, G. (2020). A survey of deep learning techniques for autonomous driving. Journal of Field Robotics, 37(3), pp. 362-386.

[12] Hevelke, A., & Nida-Rümelin, J. (2015). Responsibility for crashes of autonomous vehicles: An ethical analysis. Science and Engineering Ethics, 21(3), pp. 619-630.

[13] Koopman, P., & Wagner, M. (2017). Autonomous vehicle safety: An interdisciplinary challenge. IEEE Intelligent Transportation Systems Magazine, 9(1), pp. 90-96.

[14] Litman, T. (2020). Autonomous vehicle implementation predictions: Implications for transport planning. Victoria Transport Policy Institute.

[15] Luettel, T., Himmelsbach, M., & Wuensche, H. J. (2012). Autonomous ground vehicles—Concepts and a path to the future. Proceedings of the IEEE, 100(Special Centennial Issue), pp. 1831-1839.

[16] Milakis, D., van Arem, B., & van Wee, B. (2017). Policy and society related implications of automated driving: A review of literature and

directions for future research. Journal of Intelligent Transportation Systems, 21(4), pp. 324-348.

[17] Najm, W. G., Stearns, M. D., Howarth, H., Koopmann, J., & Hitz, J. (2006). Evaluation of an automated collision notification system. National Highway Traffic Safety Administration.

[18] Nunes, A., Reimer, B., & Coughlin, J. F. (2018). People must retain control of autonomous vehicles. Nature, 556(7700), pp. 169-171.

[19] Paden, B., Čáp, M., Yong, S. Z., Yershov, D., & Frazzoli, E. (2016). A survey of motion planning and control techniques for self-driving urban vehicles. IEEE Transactions on Intelligent Vehicles, 1(1), pp. 33-55.

[20] Pervez, Hamza, et al. "Evaluation of critical risk factors in the implementation of modular construction." Plos one 17.8 (2022): e0272448.

[21] Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. Annual Review of Control, Robotics, and Autonomous Systems, 1, pp. 187-210.

[22] Shladover, S. E. (2018). Connected and automated vehicle systems: Introduction and overview. Journal of Intelligent Transportation Systems, 22(3), pp. 190-200.

[23] Smith, B. W. (2016). Automated driving and product liability. Michigan State Law Review, 2017(1), pp. 1-74.

[24] Thrun, S. (2010). Toward robotic cars. Communications of the ACM, 53(4), pp. 99-106.

[25] Vahidi, A., & Sciarretta, A. (2018). Energy saving potentials of connected and automated vehicles. Transportation Research Part C: Emerging Technologies, 95, pp. 822-843.

[26] Varga, J. (2023a): SMEs as the innovation flagships - where are the real economic drivers? In: Szakál, Anikó (szerk.) IEEE 23rd International Symposium on Computational Intelligence and Informatics (CINTI 2023): Proceedings. Danvers (MA), Amerikai Egyesült Államok: IEEE (2023) pp. 373-377.

[27] Varga, J. (2023b): Exploring the link between competitiveness and innovation. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics. Budapest, Magyarország: IEEE Hungary Section (2023). 663 p. pp. 229-233.

[28] Varga, J. (2023c): The potential benefits of innovation as seen by some domestic businesses. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics. Budapest, Magyarország: IEEE Hungary Section (2023). 663 p. pp. 223-228.

[29] Wadud, Z., MacKenzie, D., & Leiby, P. (2016). Help or hindrance? The travel, energy and carbon impacts of highly automated vehicles. Transportation Research Part A: Policy and Practice, 86, pp. 1-18.

[30] Waymo. (2019). On the road to fully self-driving: Waymo safety report 2019. Waymo.

[31] Xu, Z., Xu, W., & Liu, Y. (2018). Research on intelligent driving technology and system. SAE International Journal of Commercial Vehicles, 11(1), pp. 51-58.

[32] Yurtsever, E., Lambert, J., Carballo, A., & Takeda, K. (2020). A survey of autonomous driving: Common practices and emerging technologies. IEEE Access, 8, 58443-58469.

[33] Zhang, W., & Guhathakurta, S. (2018). Residential location choice in the era of shared autonomous vehicles. Journal of Planning Education and Research, 38(4), pp. 449-463.

[34] Zhao, J., Medenica, Z., & Qin, X. (2015). Improving the safety and mobility of vulnerable road users through vehicle connectivity and automation. Transportation Research Part C: Emerging Technologies, 56, pp. 359-373.

[35] Zmud, J., Tooley, M., Baker, T., & Wagner, J. (2017). Pathways to driverless cars: Strategic roadmaps for autonomous vehicles. Texas A&M Transportation Institute.