Doktori (PhD) értekezés

TERVEZET

Dr. Répás József

-2026-

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

Dr. Répás József

„Önvezető járművek biztonságitechnikai vizsgálata, forensics módszertanának kidolgozása”

Doktori (PhD) értekezés

Témavezető:

Prof. Em. Dr. Berek Lajos (CSc)

- 2026 -

Tartalomjegyzék

Bevezetés

A közlekedési járművek folyamatos fejlesztése, az egyre komplexebb vezetéstámogató rendszerekkel ellátott járművek megjelenése a közlekedésben, jól reprezentálja az autóipar paradigmaváltását. A járművezetők támogatása, a különböző funkciók automatizálása és a gyártók törekvései az elektromobilitás mellett az autonóm vezetés irányába mutatnak. Még nem látható pontosan, hogy mikor terjednek el széles körben a közutakon a teljesen önvezető járművek. Egyes tanulmányok 5-10 éves, kevésbé optimista becslések azonban még mindig 10-15 éves időtávra teszik az ilyen járművek megjelenését. Annyi biztos, hogy hosszú ideig együtt kell majd „élniük" a hagyományos járművekkel, ami részben megnehezíti alkalmazásukat. Az elmúlt években a jogszabályi háttér hazánkban és Európában is egyre nagyobb teret enged a fejlett vezetéstámogató rendszerrel ellátott járműveknek, lehetőséget teremtve a nem csak fejlesztési és tesztelési célból történő alkalmazásnak is.

A magas automatizáltságú, fejlett vezetéstámogató rendszerrel, önvezető, vagy ahhoz közeli funkciókkal rendelkező polgári és katonai közúti közlekedési járművek megjelenése átalakította a közúti közlekedést, valamint megalapozta az intelligens közlekedési rendszerek kialakítását, elősegítve azok hatékonysági, biztonsági, céljainak elérését. Ezen járművek elterjedése túlmutat a közúti közlekedési szempontokon és a balesetek számának csökkenésén. Az egyes járműtípusok és a járművekkel kapcsolatos bűncselekmények, vagy katonai műveletekhez kapcsolódó információgyűjtés, igazságügyi szakértői vizsgálatok szempontjából számos új kihívást és feladatot is jelent.

Napjaink modern járműveinek egyik új hajtóanyaga a digitális információ, amit a jármű saját érzékelőhálózatán keresztül gyűjt, kommunikációs hálózatán keresztül forgalmaz a közlekedés további résztvevőitől, a környezeti és pálya infrastruktúrával, vagy a gyártói és szolgáltatói háttérinfrastruktúrával. Ezen adatok feldolgozása és tárolása történhet helyben a járműben és azon kívül is, mely adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása elsődleges szempont. A járművek, hálózatba kapcsolt komplex informatikai, infokommunikációs és IoT (Internet of Things) eszközökként is értelmezhetőek, vezérlő egységei, szoftveres megoldásai, szolgáltatásai és összetevői közötti kommunikáció mind sérülékenyek lehetnek.

A disszertációm témája a modern és egyre inkább önvezetővé váló közúti közlekedési járművekben tárolt adatok digitális forenzikus igazságügyi szakértői vizsgálati szempontú hozzáférhetősége, vizsgálhatósága és értelmezhetősége és a különböző módszertanok alkalmazhatóságának vizsgálata, az esetleges hiányosságok kiküszöbölése és új módszertan készítése. A Digital Forensics domain vizsgálati módszertanainak szakirodalmi és gyakorlati vizsgálatával, a szakértői vizsgálatok lehetőségeinek, korlátainak és kihívásainak elméleti és gyakorlati alapú összegyűjtése és csoportosítása által, valamint a vizsgálatokhoz szükséges tudás, képesség és kompetencia meghatározásával elkészítettem a digitális járművek szakértői vizsgálatához javasolt módszertant.

Az elvégzett munka eredményeként mélyreható elméleti és gyakorlati ismeretek álltak elő és kerültek módszertanként összefoglalva a modern járművek szakértői vizsgálatainak kihívásairól és lehetőségeiről, a vizsgálatok elvégzéséhez nélkülözhetetlen elméleti és gyakorlati ismeretekről, a jelenlegi módszertanok és módszertani levelek alkalmazhatóságáról, korlátairól annak érdekében, hogy hatékony, eredményes és szükség szerint gyors vizsgálatokat lehessen végezni ilyen járművekkel kapcsolatos balesetek, kiberbiztonsági incidensek, katonai műveletek, vagy nemzetbiztonsági feladatok elvégzéséhez kapcsolódóan.

A disszertációmban bemutatott eredmények lényegében relevánsak mind a polgári, katonai és nemzetbiztonsági területen lévő digitális forenzikus kutatók és gyakorló szakemberek számára a modern járművekkel kapcsolatos események kivizsgálása során. Végső soron célom elősegíteni egy hazai szakértői módszertani levél kidolgozását.

Kutatási téma aktualitása

Az elmúlt években az autóipar paradigmaváltáson ment keresztül, a hangsúly egyre inkább összekapcsolt és magas automatizáltságú járművekre helyeződik. A félautonóm és autonóm autók mellett megjelennek a fejlett gépi tanulási (machine learning) és mesterséges intelligencia (MI) megoldásokat alkalmazó járművek is.[100]

„*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 2021és 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 fogyatékossággal 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.*”.[191]

Bár az Európai Unió közutak biztonságára vonatkozó mutatószámai világviszonylatban jónak számítanak, ennek ellenére közlekedési balesetben évente több, mint 25 000 ember hal meg, és több, mint 135 000 ember sérül meg súlyosan.[3] A modern közlekedési rendszerek elsődleges céljai közé tartoznak a közlekedésbiztonság fokozása és az infrastruktúra kihasználtságának maximalizálása, a forgalom racionalizálása, a környezeti terhelés csökkentése.[77] A közlekedési rendszerek fejlesztésével és a közlekedésbiztonság fokozásával, 2030-ra a 2020-ban mért számokhoz képest felére tervezik csökkenteni a súlyos balesetek számát, az ún. *Vision Zero* célkitűzés alapján pedig 2050-re nullára redukálják a súlyos sérüléssel járó vagy halálos kimenetelű balesetek számát az európai utakon.

A közlekedési rendszerek fejlesztése, a közlekedés digitalizálása, az intelligens közlekedési rendszerek alkalmazása hozzájárul a fenti célok eléréséhez, biztonságosabbá, hatékonyabbá és fenntarthatóbbá tehetik a közlekedést. Az intelligens közlekedési rendszerek „*tényleges (emberi) intelligencia megtestesítése nélkül biztosítanak innovatív szolgáltatásokat a különböző közúti közlekedési módokhoz és forgalmi menedzsmenthez kapcsolódóan*”.[3] Az ITS-ek az információs és kommunikációs rendszerek alkalmazása mellett a meglévő technológiák hatékony integrálását is megvalósítják. „*Tágabb értelemben az ITS rendszerek a közlekedési hálózatokon és járművekben alkalmazott információs és kommunikációs (telematikai) megoldások összessége, melyek dinamikus, valósidejű (real-time) adatok alapján működnek.*”.[77]

Az ITS-rendszerek következő generációja a kooperatív intelligens közlekedési rendszerek (Cooperative Intelligent Transport Systems, C-ITS), amelynek célja a hatékony adatcserével, a vezeték nélküli technológiák alkalmazásával megvalósulhat a közlekedés automatizálása. A közúti közlekedési rendszer elemei, az infrastruktúra, a jármű, a járművezető, az utazó, gyalogos stb. közötti információmegosztás valósítható meg, annak érdekében, hogy tevékenységeiket, közlekedésüket összehangolhassák. A kommunikációt az összes olyan közlekedési résztvevő között meg kell valósítani, akik „érintkezésben" vannak, konfliktushelyzetbe kerülhetnek egymással.[76]

A technológiai fejlődés nem csupán a közlekedési rendszerekre van nagy hatással. Az egyre komplexebb összekapcsoltság és a fejlett automatizálás interdependenciája új lehetőségeket teremt a közlekedés hatékonyságának és biztonságának növeléséhez. Ehhez az egyik lépés, hogy a jármű segíti a járművezetőt, a forgalmi helyzethez való alkalmazkodásban és a megfelelő döntések meghozatalában, illetve az emberi tényező hatásának csökkentése, ellensúlyozása, a vezető nélküli járművekre való átállás. Az autonóm módon működő járművek hosszú távon nagyobb biztonságot eredményeznek.

Nemzetközi és hazai aktualitások

Az Egyesült Államok kormánya a világelsők között szerepel a közlekedési innovációk területén, az automatizált járművek fejlesztésében és integrációjában, azonban egyaránt nagy hangsúlyt helyez a kiberbiztonságra, a közlekedésbiztonságra és a személyes adatok védelmére. Az Amerikai Közúti Közlekedésbiztonsági Hivatal (NHTSA) korábban az Automated Driving Systems: A Vision for Safety 2.0 dokumentumában határozott meg iránymutatást a magas automatizáltságú, önvezető funkcióval rendelkező járművekre vonatkozóan. Ezután az Ensuring American Leadership in Automated Vehicle Technologies, 4.0 verziójú dokumentumában 2020-ban meghatározták, hogy az önvezetésben rejlő lehetőségek kiaknázásához az ipari, állami és akadémiai szereplők, szabványügyi és nonprofit szervezetek közötti információmegosztása szükséges. A dokumentum hangsúlyozza az Egyesült Államok kormányának támogatását az önvezető járműtechnológiák tervezésére és fejlesztésére, a kockázatarányos biztonsági (safety) és a kiberbiztonsági (security) szempontokat, az adatvédelem mellett. A dokumentumban megjelenik a járművezető vezető és az utasok személyes adatainak védelme, valamint a passzív harmadik felek – például a gyalogosok – adatainak védelme is.[229]

Az ENSZ által 2021-ben kiadott Új értékelési és tesztelési módszer autonóm vezetéshez (New Assessment/Test Method for Automated Driving) átfogó áttekintést nyújtott a tesztelési és szabványosítási környezetről, az önvezető járművek forgalomba helyezéséhez, azonban a kiberbiztonsági szempontok nem kapnak jelentős szerepet.

Európa vezető szerepet tölt be a magas automatizáltságú járművek széleskörű felhasználásban és a járművek közötti közvetlen kommunikáció használatában, az intelligens közlekedési rendszerek kialakításában. Az Európai Parlament és a Tanács 2010/40/EU irányelve [36] már 2010-ben foglalkozott az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésével és azok más közlekedési módokhoz való kapcsolódásának kereteivel. Ezt követően az Európai Parlament és a Tanács 2023/2661 irányelve [35] 2023. évben módosította a korábbi jogi és szakmai tartalmat.

Emellett a „Fenntartható és intelligens mobilitási stratégia – az európai közlekedés időtálló pályára állítása" című, 2020. december 9-i bizottsági közleményben [3] is az intelligens közlekedési rendszerek (ITS-ek) kiépítését tekintették az európai közlekedési rendszer átalakításának egyik alapelemeként. Ez alapján az EU-nak nagy hangsúlyt kell helyezni az intelligens digitális megoldásokra és az intelligens közlekedési rendszerekre, hogy a teljes közlekedési rendszer működését javítása, a fenntarthatósági és biztonsági célokat elérhesse.

„*Az intelligens közlekedési rendszerek (ITS-ek) olyan rendszerek, amelyekben információs és kommunikációs technológiákat alkalmaznak a közúti közlekedés területén, beleértve az infrastruktúrát, a járműveket és a felhasználókat is, a forgalomirányításban és a mobilitás kezelésében, valamint a más közlekedési módokhoz való kapcsolódási pontok vonatkozásában.*"[36]. A modern járművek kommunikációs csatornáikon keresztül csatlakoznak már most is és a közeljövőben még inkább az ITS-ekhez, kommunikálnak egymással, a környezeti- és pályaelemekkel, gyártói és szolgáltatói háttérrendszerekkel.

Hazai vonatkozásban a 48/2012. (VIII. 23.) NFM rendelet szól az intelligens közlekedési rendszerek fejlesztésének és üzemeltetésének általános feltételeiről, valamint más közlekedési módokhoz való kapcsolódásáról, az önvezető járművek tesztelésére vonatkozóan pedig a KöHÉM rendeletek határoznak meg követelményeket.[305] Ezek megkülönböztetnek fejlesztési célú nem autonóm járművet és fejlesztési célú autonóm járművet. Előbbi esetben a jármű vezetője manuális módon vezeti a járművet, az autonóm jármű esetén a vezető a működés közben szükséges mértékben avatkozik be a jármű működésébe és bármikor átveheti a jármű felett az irányítást.[2]

Mint a fentiekből látszik, nincs egységes tesztelési és jóváhagyási eljárás az önvezető járművek forgalomba helyezésére vonatkozóan. Egyes országokban (pl.: USA, Kína) rugalmasabbak a követelmények, az EU-ban jellemzően tesztelési célú engedélyeztetés, elsősorban a közlekedésbiztonsági (safety) követelmények a hangsúlyosak.

A SAE J3061 szabványa 2016-ban az első olyan szabványként jelent meg, ami az autóipari kiberbiztonsággal is foglalkozik. Magas szintű kiberbiztonsági alapelveket és útmutatást nyújt a modern járművekre vonatkozóan. ISO/SAE 21434 szabvány szintén az autóipari kiberbiztonságra vonatkozik, követelményeket határoz meg és ajánlásokat tesz a járművek (beleértve azok alkatrészeit, szoftvereit és interfészeit) kiberbiztonsági kockázatkezelésére, azok teljes életciklusa során.

Az ENISA 2019-ben kiadott jelentésében (ENISA Good prctice for security of smart cars) meghatározta a hálózatba kapcsolt és (félig) autonóm járművek biztonságának jó gyakorlatait. A dokumentumban felmérésre kerültek a kapcsolódó szabványosítási, jogalkotási és politikai kezdeményezések, emellett felhívja a figyelmet a kiberbiztonsági szempontokra, releváns fenyegetésekre és kockázatokra is. A hálózatba kötött járművek, a gyors kommunikációs megoldások és a járművekben elérhető funkciók, szolgáltatások új kiberbiztonsági kockázatokat és fenyegetéseket jelenthetnek. Az ITS-ek és a járművek (V2X) kommunikációs megoldásai tovább bővítik a potenciális támadási felületet, új támadási vektorok jelennek meg a járművekhez kapcsolódóan.

A modern járművek elleni kibertámadások a jármű leállásához, közúti balesetekhez, terrortámadásokhoz, anyagi veszteséghez, bizalmas, személyes adatok kompromittálódásához is vezethetnek. Ezek kiküszöbölésére kockázatokkal arányos védelmi intézkedéseket kell alkalmazni, annak érdekében, hogy a jármű vezető és utasok, a közlekedők és környezet védelmét biztosítani lehessen.[100]

Az Európai Unió kiberbiztonsági stratégiájának [33] egyik kiemelt eleme az összekapcsolt rendszerek és azok kiberbiztonsága. Mind a rendszerek védelme, mind azok vizsgálata vonatkozásában. Utóbbi érdekében *„A bűnüldöző hatóságokat teljes mértékben fel kell szerelni ahhoz, hogy képesek legyenek digitális nyomozások végzésére.”*[33]*, mivel a* nyomozásoknak, szinte valamennyi bűncselekménytípus esetében van digitális eleme. Így van ez a modern járművek esetén is, ami azért különösen hangsúlyos, mert a bűncselekmények több mint 80 %-ában járművek is érintettek.

Napjainkban az önvezető járművek a tesztelési cél mellett, közúti forgalomban jellemzően valamilyen taxiszolgáltatás (Waymo, Tesla, Uber, stb.), vagy shuttle megoldásban (Navya, Zoox, Ohmio, stb.) vannak jelen, elsősorban az Egyesült Államokban. Az európai önvezető taxi szolgáltatás várhatóan idén indulhat el a Stellantis csoport és az észt Bolt együttműködésében.[32]

Hazánkban az elmúlt időszakban jelentek meg újabb tesztüzemben működő önvezető járművek. Budapesten és a Zalazone-on a Zeekr járművei, a Tesla pedig idén tette elérhetővé Magyarországon is az FSD (Full Self-Driving (Supervised)) szolgáltatását, vagyis az emberi felügyelet mellett használható önvezető rendszerét, ami vezet és parkol is a járművezető helyett.[98][235][299][317][337]

Igazságügyi szakértői aktualitások

Igazságügyi szakértői feladatok oldaláról a jogszabályi keretet az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (Szakértői törvény) adja meg. „*A szakértői bizonyítás jelentőségének növekedése szoros összefüggésben áll azzal a fejlődési folyamattal, amely a tudomány és technika terén, valamint ennek hatására a társadalomban az elmúlt évtizedekben végbement. Ennek eredményeként nőtt a különleges szakértelmet igénylő területek száma, a társadalmi viszonyok egyre bonyolultabbá váltak, amely az igazságszolgáltatásban úgy jelent meg, hogy a peres és hatósági eljárások tárgyi és szerkezeti összetétele jelentős változáson ment át. Jellemzővé vált a jogi problémáknak más szakmákhoz tartozó kérdésekkel való összefonódása és emiatt megítélésük egyre nehezebbé válása. Ezzel párhuzamosan a bírósági eljárásokban megnőtt az igény a modern természettudományok eredményeinek a bizonyítási eljárásban történő felhasználása iránt.*”. Ezek az „*új tendenciák olyan minőségi változásokat idéztek elő a bírósági és hatósági eljárásokban, különösen a szakértői bizonyítással kapcsolatban, amelyek egyre több országban tették szükségessé e jogintézmény minden részletre kiterjedő, átfogó elemzését és újraszabályozását.*”.[1]

Valamennyi utólagos szakértői tevékenységet igénylő eljárás (büntetőeljárás, polgári eljárás, közigazgatási eljárás, hatósági eljárás, magán szakértői megbízás) vonatkozásában, kirendelés vagy megbízás alapján, a Szakértői törvényben rögzített feladatokat végzi a szakértő, amely így került meghatározásra: „*a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását*”.[1]

A modern járművek szakértői vizsgálata esetén a járműben lévő, vagy hozzá kapcsolódó elektronikus adatok azonosítása, megszerzése, feldolgozása, elemzése alapján történik a tényállás megállapításának elősegítése és a szakkérdés eldöntése. Az Európa Tanács, Számítástechnikai Bűnözésről szóló 2001. november 23-án kelt Egyezménye meghatározza a számítástechnikai adat fogalmát: „*tényeknek információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, amely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja*". A büntetőeljárásról szóló 2017. évi XC. törvényben ez a fogalom az alábbiak szerint került meghatározásra: „*Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.*".[82][116][149]

A vizsgálat során gyűjtött digitális bizonyítékok olyan adatok („*bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak*"), amelyek a vizsgálat szempontjából releváns tényekre vonatkoznak, olyan forrásokból származnak, ezeket olyan bizonyítási eszközökből szerezték be (megismerhetővé váltak), amit jogszabály lehetővé tesz. „*A digitális bizonyíték megismerhető:*

- *megkereséssel (Be. 71. §);*
- *az adathordozónak, illetve az adatnak a lefoglalásával (Be. 151. §);*
- *információs rendszerben tárolt adatok megőrzésére kötelezéssel (Be. 158/A §);*
- *titkos információgyűjtéssel (1994. évi XXXIV. törvény a rendőrségről 63. §); illetve*
- *titkos adatszerzéssel (Be. 200–202. §)*" (Sorbán, 2016).

„A bizonyítási eszköz tehát a bizonyíték hordozója, a bizonyíték pedig az az információ, amelyhez a bizonyítási eszközből jutunk".[287]

A szakértői feladat ellátásához a modern és egyre inkább önvezetővé váló és hálózatba kapcsolt járművek elterjedése kapcsán a kiindulási alapot az igazságügyi kamara elnöksége által előkészített és elfogadott, a módszertani levél kiadásának részletes szabályairól szóló szabályzat alapján készített módszertani levelek adják. A Szakértői törvény 89. § (1) alapján „*Az elnökség az igazságügyi szakértői tevékenység egységes és magas színvonalú ellátása érdekében módszertani levelet ad ki*".[1] Az informatikai szakterületen jelenleg három módszertani levél hatályos:

- Módszertani leírás a digitális adattároló eszközök vizsgálatának általános eljárásainak meghatározásáról (4/2019. (XII.17.) NSZKK főigazgatói körlevél)
- Módszertani leírás a mobilkommunikációs eszközök vizsgálatának általános eljárásainak meghatározásáról (5/2019. (XII.17.) NSZKK főigazgatói körlevél)
- A Magyar Igazságügyi Szakértői Kamara 6/2020 számú Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről (Hatályos: 2020-12-04. napjától)

Ezen módszertani levelek a digitális forenzikus módszertanokat veszik alapul és határozzák meg a digitális adatok (elektronikus adatok) azonosításának, gyűjtésének, feldolgozásának, elemzésének és a vizsgálat eredményeinek nem szakemberek számára is értelmezhető formában történő bemutatásának gyakorlatát. Ezek az eljárások olyan technikák és eszközök gyűjteménye, amelyek segítségével a vizsgálati eljárás céljának megfelelő információk előállíthatóvá válnak.

A módszertani levelek kiadása óta eltelt évek és a technológiai fejlődés, a modern és egyre inkább önvezetővé váló járművek sajátosságai miatt szükséges és indokolt felülvizsgálni ezek relevanciáját a digitalizálódó járművek szakértői vizsgálata kapcsán és szükség szerint módosított, vagy új módszertan elkészítése.

Kapcsolódás a katonai műszaki tudományokhoz

A harctéri feladatok professzionális ellátását modern technikai eszközök és magas szintű szakértelem segíti. Az autonómia, a magas automatizáltágú (valamilyen szintű önvezető képességgel rendelkező) közlekedési járművek széleskörű elterjedése mind a katonai, mind a polgári felhasználásban megfigyelhető.

Ezek a járművek megjelennek, részt vesznek a műveleti tevékenységekben, nagy mennyiségű információt gyűjtenek, dolgoznak fel és tárolnak a műveletekről, környezetükről, és kapcsolatban állnak a vezetési-irányítási (Command Control - C2) rendszerekkel. A katonai felhasználás során olyan szempontok is megjelennek, mint az emberi erőforrás megóvása, a bevetési hatékonyság javítása, a körülmények, a környezet megfigyelése, érzékelése, az információk feldolgozása, a gyors és pontos döntéshozatal, valamint az adott lépés végrehajtása. Az autonómia a katonai rendszerekben várhatóan az alábbi öt területen kap majd nagy szerepet:

- logisztika, flottaszervezés,
- a nagy mozgékonyságú katonai rendszerek fizikai felépítése,
- az autonóm eszközök egyedi viselkedése,
- az emberek és az autonóm rendszerek közötti együttműködés,
- műveleti és csoportstratégiák.[38][41]

Az autonomitás szintjének növekedésével, a felelősségek átrendeződésével egyre nagyobb hangsúlyt kap a tevékenységek utólagos vizsgálata és elemzése, az objektív bizonyítékok előállítása, melyhez a forenzikus vizsgálatok során a tudomány és a technológia eredményeit és módszereit használják a szakértők. A jelenleg hatályos (digitális adattároló és mobilkommunikációs eszközökre, valamint az elektronikus adatok vizsgálatának alapelveiről szóló) igazságügyi módszertani levelek alkalmazása és alkalmazhatósága katonai vonatkozásban széleskörű.

Az autonóm rendszerek a hidegháború óta átkerültek a kísérleti fázisból a katonai szolgálatba. A vezérléstechnika, a kamera- és szenzortechnika és a rakétatechnika fejlődése új lehetőségeket teremtett az autonóm rendszerek alkalmazásához a világűrben és a víz alatti környezetben. Mind

- funkcionális szempontból (gépkezelés, információgyűjtés, célfelderítés),
- az autonómia szintjét tekintve (autonóm, részben autonóm, távvezérelt),
- az élettartam alapján (egyszer használatos, illetve visszatérő)

vizsgálva az autonóm platformokat, a működési biztonság alapvető feltétele a pontosság és az adat.

A pontosságot az biztosítja, hogy a pilóta nélküli rendszerek jóval hosszabb bevetési időt tesznek lehetővé, jóval meghaladva a személyzettel ellátott eszközök képességeit. Az ember által jelentett fizikai korlátok mellőzésével, ami valós idejű helyzetfelismerést eredményez.

A szakértői vizsgálatok alapján az eszközökben, rendszerekben és környezetekben található kulcsfontosságú nyomok/adatok azonosítása, elemzése történik meg az utólagos vizsgálatához szükséges adatok hozzáférhetővé és elemzésre alkalmassá tételével.

Tudományos probléma megfogalmazása

A technológiai fejlődés nem csupán a közlekedési rendszerekre van nagy hatással. Az egyre komplexebb összekapcsoltság és a fejlett automatizálás interdependenciája új lehetőségeket teremt a közlekedés hatékonyságának és biztonságának növeléséhez. Ehhez az egyik lépés, hogy a jármű segíti a járművezetőt, a forgalmi helyzethez való alkalmazkodásban és a megfelelő döntések meghozatalában, illetve az emberi tényező hatásának csökkentése, ellensúlyozása, a vezető nélküli járművekre való átállás. Az autonóm módon működő járművek hosszú távon nagyobb biztonságot eredményeznek, azonban az általuk tárolt, gyűjtött és feldolgozott információk védelmét és utólagos szakértői vizsgálatban való elérhetőségét biztosítani szükséges, amihez jelenleg nincs kidolgozott módszertan, a meglévő módszertanok korlátozott módon alkalmazhatóak, a szükséges kompetencia és tudáselemek nem kerültek meghatározásra és rendszerezésre.

A szakértői feladat ellátásához a modern és egyre inkább önvezetővé váló és hálózatba kapcsolt járművek elterjedése kapcsán a kiindulási alapot az igazságügyi kamara elnöksége által előkészített és elfogadott, a módszertani levél kiadásának részletes szabályairól szóló szabályzat alapján készített módszertani levelek adják. A jelenleg hatályos módszertani levelek a digitális forenzikus módszertanokat veszik alapul és határozzák meg a digitális adatok (elektronikus adatok) azonosításának, gyűjtésének, feldolgozásának, elemzésének és a vizsgálat eredményeinek nem szakemberek számára is értelmezhető formában történő bemutatásának gyakorlatát. Ezek az eljárások olyan technikák és eszközök gyűjteménye, amelyek segítségével a vizsgálati eljárás céljának megfelelő információk előállíthatóvá válnak. A módszertani levelek kiadása óta eltelt évek és a technológiai fejlődés, a modern és egyre inkább önvezetővé váló járművek sajátosságai miatt szükséges és indokolt felülvizsgálni ezek relevanciáját a digitalizálódó járművek szakértői vizsgálata kapcsán és szükség szerint módosított, vagy új módszertan elkészítése.

A biztonságos katonai műveletek – ellenséges környezetben végzett katonai műveletek, terrorelhárítás, hírszerzés stb. – egyik fontos összetevője a digitális eszközök szakértői vizsgálatának elvégzése. Legyen szó az ellenség digitális rendszereinek vizsgálatáról, műveleti területeken történő adatkinyerésről, a potenciális incidensek utólagos vizsgálatáról, a fenyegetések azonosításáról, a sérülékenységek mérsékléséről vagy a biztonsági szint, a működési folyamatok, a katonai műveletek fejlesztése érdekében végzett tevékenységekről. A digitális információk közlekedési eszközökből történő kinyerése, a digitális nyomok/adatok

gyűjtése, elemzése katonai felhasználásban stratégiai kérdés, elengedhetetlen a műveleti és nemzetbiztonsági célok támogatásához, ami indokolja egy felülvizsgált vagy új módszertan elkészítését.

A biztonságos katonai műveletek mellett olyan esetekben is szükséges a járművek szakértői vizsgálata, amikor a járművet bűncselekmény elkövetésénen eszközeként használták. Ilyen esetben a járműben keletkezett, tárolt és kinyerhető adatok kellő időben történő megszerzése hozzájárulhat egy kiemelt bűncselekmény, például egy terrortámadás elkövetőinek gyorsabb és hatékonyabb felderítésében és az esemény körülményeinek tisztázásában. Ezen túlmenően a járművek tartalmazhatnak evidenciát olyan esetekben is, amikor egy megtörtént esemény utólagos vizsgálatát végzik, például baleset vagy titkos információgyűjtés esetén.

Járművekhez kapcsolódó szakértői vizsgálatok elvégzésére mind polgári, mind katonai vonatkozásban szükség lehet, ha:

- a jármű egy cselekmény célpontja (például támadás, feltételezett visszaélés),
- valamilyen módon kapcsolódik a vizsgált eseményhez (például bűncselekményhez),
- a jármű tartalmazza a nyomot (például a hibák gyártó általi azonosításához).

Kutatási hipotézisek megfogalmazása

A járművek fejlődése - mind polgári, mind katonai vonatkozásban-, a mobil kommunikációs eszközök elterjedése és a kooperatív közlekedés rendszerek kialakulása eredményezi a széleskörű, összetett elektronikus bizonyítékok feltárásának lehetőségét. A modern közlekedési eszközök és rendszerek számos új, potenciális bizonyítékforrást hoztak létre. Az adatok hozzáférhetősége, összegyűjtése, értékelése területén számos kihívás, probléma, nehezítő tényező van, és jelenleg lényegesen kevesebb megoldás létezik, komplex, hatékonyan alkalmazható módszertan, megoldás pedig egyelőre nem áll rendelkezésre.

Az általános vizsgálati elvek a katonai megközelítés és a harctéri körülmények ellenére sem változnak. A nyomok gyűjtésének, megőrzésének, kezelésének és tárolásának folyamata során nem változhatnak meg, csak felhatalmazott és kvalifikált személyek végezhetik el az egyes műveleti lépéseket. A digitális forenzikus domain-ek vonatkozásában nem állapítható meg, hogy a modern járművek szakértői vizsgálata mely szakterülethez tartozik, egyáltalán besorolható-e ezekbe, vagy szükséges egy új domain létrehozása.

Katonai műveletekben a forenzikus vizsgálatokat általában specialisták végzik, különféle digitális forenzikus eszközökkel. Idetartoznak például a szakképzett operátorok, az alkalmazott forenzikus technikák, taktikák, eljárások és módszerek egyaránt, amelyek a digitális nyomok azonosításától a feldolgozásáig és elemzéséig végzik feladatukat. Az ehhez szükséges kompetencia és tudás elemek meghatározása és rendszerezése, mely lehetővé teszi a magas automatizáltságú járművek vizsgálatának elvégzését nem áll rendelkezésre.

A Nemzeti Szakértői és Kutató Központ szervezeti felépítése alapján az látható, hogy a közlekedési szakértői tevékenység és az informatikai szakértői tevékenység elkülönül egymástól. Utóbbinál jelenik meg például a digitális adattároló eszközök, vagy a mobilkommunikációs eszközök vizsgálata, azonban a járművekhez kapcsolódó informatikai vizsgálatok, a jármű vagy annak környezetében megtalálható digitális információk vizsgálata módszertani vonatkozásban nem meghatározott terület. A modern járművekhez kapcsolódó szakértői vizsgálatok túlmutatnak az általánosságban ismert közlekedési és informatikai szakértői vizsgálatokon.

A biztonságos katonai műveletek mellett olyan esetekben is szükséges a járművek szakértői vizsgálata, amikor a járművet bűncselekmény elkövetésénen eszközeként használták. A szakértők jelenleg nem rendelkeznek olyan rendszerezett tudásbázissal, ami tartalmazza, hogy

a járműben milyen keletkezett, tárolt és kinyerhető adatok hol érhetőek el, azonban ezen adatok kellő időben történő megszerzése hozzájárulhat egy kiemelt bűncselekmény, például egy terrortámadás elkövetőinek gyorsabb és hatékonyabb felderítésében és az esemény körülményeinek tisztázásában.

H1: A magas automatizáltságú, egyre inkább önvezetővé váló járművek szakértői vizsgálatához jelenleg nem áll rendelkezésre olyan definiált módszertan vagy módszertani levél melyek alapján a modern járművek szakértői vizsgálata szakszerűen elvégezhető.

H2: A járművekkel kapcsolatos események, új vizsgálati célok kikényszerítették, hogy az informatikával vagy járművek szakértői feladatait ellátók járművekhez, járművekben található adatokhoz kapcsolódóan is végezzenek eseti jelleggel vizsgálatokat, azonban ezen vizsgálatok jellemzően informatikai módszertan és eljárás hangsúlyosak, eszköz és technológia specifikusak, nem kerültek meghatározásra a vizsgálatokhoz kapcsolódó kihívások és a járművekben keletkezett, tárolt és kinyerhető adatok, valamint az információszerzési módszerekkel való összerendelése.

H3: Az informatika hangsúlyos szakértői vizsgálati tevékenység miatt, ezidáig nem kerültek definiálásra mely kompetenciák, képességek és tudáselemek szükségesek azon szakértők számára, akik modern és önvezető járművek vizsgálatával foglalkoznak, vagy terveznek foglalkozni.

H4: Az alkalmazott vizsgálati eljárások nem alkotnak egységes rendszert, nem biztosítják kielégítő módon a szakértői vizsgálatokkal kapcsolatos vizsgálati elveket. A digitális forenzikus domain-ek vonatkozásában nem állapítható meg, hogy a modern járművek szakértői vizsgálata mely szakterülethez tartozik, egyáltalán besorolható-e ezekbe, vagy szükséges egy új domain létrehozása.

Kutatási célkitűzések

Kutatásom célja hozzájárulni a hazai és nemzetközi vonatkozású, modern és egyre inkább önvezetővé váló, polgári és katonai felhasználású, közúti közlekedési járművek szakértői vizsgálatának hatékony és eredményes elvégzéséhez.

A járművek fejlődésével, a beépített mobil kommunikációs eszközök elterjedésével és a kooperatív közlekedés rendszerek széleskörű alkalmazásának küszöbén nagy számban meg fognak jelenni a modern járművekhez kapcsolódó szakértői vizsgálatok, az elektronikus bizonyítékok feltárásának igénye. Az adatok hozzáférhetősége, összegyűjtése, értékelése nem mindig triviális, számos kihívást jelent a szakértők számára. Széles körben elérhető és alkalmazható technikai megoldások egyelőre nem léteznek, a feladatok komplexitása várhatóan növekedni fog. Célom egy a modern és egyre inkább önvezetővé váló járművek vizsgálatához kapcsolódó kihívásokat is figyelembe vevő, hatékonyan alkalmazható vizsgálati módszertan kidolgozása, ami alapja lehet egy szakértői módszertani levél kidolgozásának. Kutatásom eredményeként, a releváns digital forensics domainek vizsgálata alapján meghatároztam az Autonomous Vehicles Forensics szakmai definícióját és módszertani leírását.

A nyomok gyűjtésének, megőrzésének, kezelésének és tárolásának folyamatát megfelelő kvalifikációval rendelkező személyek végezhetik, ezért kutatásom egyik célja a vizsgálatok elvégzéséhez szükséges kompetencia és tudáselemek meghatározása.

Mivel a digitális forenzikus domain-ek vonatkozásában nem állapítható meg, hogy a modern járművek szakértői vizsgálata mely szakterülethez tartozik, egyáltalán besorolható-e ezekbe, vagy szükséges egy új domain létrehozása, kutatásom célja ennek megállapítása, a modern járművek szakértői vizsgálatának fogalmi meghatározása.

Kutatási módszerek

A kutatási hipotézisek igazolásához, továbbá a kutatási célkitűzések eléréséhez az alábbi kutatási módszereket alkalmaztam:

- felkutattam, tanulmányoztam és feldolgoztam a kutatási témához kapcsolódó kiadványokat, szakirodalmakat, szabályzókat, eljárásokat, ajánlásokat, módszertanokat és irányelveket, amelyekre alapozva dokumentumelemzést végeztem,
- kutatási eredményeim nemzetközi és hazai szakmai és tudományos folyóiratokban publikáltam, részt vettem szakmai képzéseken és több tudományos és szakmai konferencián is részt vettem hallgatóként és előadóként is.
- rendszeresen konzultáltam a kutatási eredményeim és a járművekhez kapcsolódó igazságügyi szakértői munka kapcsolatáról, valamint az elképzeléseim megvalósíthatóságáról a Nemzeti Szakértői és Kutató Központ szakértőivel,
- felhasználtam a saját korábbi kiberbiztonsági és műszaki tapasztalataimat, releváns hazai és nemzetközi szakmai képzéseken szerzett ismereteimet, valamint szakértői vizsgálatokban szerzett ismereteimet,
- elvégeztem a digital forensics domain egyes elemeinek modern járművek vizsgálatában történő alkalmazhatóságának vizsgálatát, összehasonlító elemzést végeztem az egyes domainek módszertani lépéseihez kapcsolódóan,
- a járművekben gyűjtött, tárolt és feldolgozott adatokra vonatkozóan adatgyűjtést végeztem szakértői rendszerekben és adatbázisokban,
- az eredményeket rendszereztem és új módszertani lépéseket határoztam meg.
- a szakértői vizsgálatok során külön hangsúlyt fektettem a nemzetközi kitekintésre
- kutatásom során nemcsak az elméleti, hanem a gyakorlati aspektusokat is figyelembe vettem.

Kutatómunka korlátai, elhatárolások

A kutatási időszakban nem terveztem, és az értekezés sem tartalmazza a modern járművekhez kapcsolódó szakértői vizsgálatok kiterjesztését a jármű gyártói és szolgáltatói felhő rendszereire, a közlekedési hatóságok és mobilkommunikációs szolgáltatók rendszereire és információira. Az értekezésben csak a modern járművekben található, általuk gyűjtött, tárolt és feldolgozott információk kinyerésére és elemzésére vonatkozó eljárások jelennek meg. Az általam kidolgozott módszertan vonatkozásában ezek rendszerek és információk tekintetében csak illeszthetőségi szempontok kerültek figyelembe vételre.

Az értekezés nem tárgyalja részletesen a járművek live forensics vizsgálati lehetőségeinek felmérését, melynek célja a jármű működése közben keletkező illékony adatokhoz, a működés során a memóriában található információkhoz, a belső és külső irányú kommunikációs hálózathoz való közvetlen hozzáférés és az adatok feldolgozása és vizsgálata.

Releváns szakirodalom áttekintése

A kutatómunkám kezdeti szakaszában felmértem kutatási területemmel kapcsolatos szakirodalomi hátteret, elvégeztem a nyomtatott és elektronikusan elérhető forrásokra is kiterjedő irodalomkutatást. A kutatási téma aktualitása szempontjából megkerülhetetlen az Amerikai Közúti Közlekedésbiztonsági Hivatal (NHTSA) Automated Driving Systems: A Vision for Safety 2.0 dokumentuma, melyben iránymutatást adott a magas automatizáltságú, önvezető funkcióval rendelkező járművekre vonatkozóan, ami kiindulási alapot jelentett a következő időszak szabályozási hátterének. Az önvezető járműtechnológiák tervezését és fejlesztését kiemelt területként kezelik, a kockázatarányos biztonsági (safety) és a kiberbiztonsági (security) szempontokra nagy hangsúlyt fektetnek. [229]

Az ENSZ Új értékelési és tesztelési módszere az autonóm vezetéshez (New Assessment/Test Method for Automated Driving) dokumentuma alapján megállapítható, hogy átfogó áttekintést kívánnak nyújtani a tesztelési és szabványosítási környezetekről, az önvezető járművek forgalomba helyezéséhez. Az elemzés során azonban megállapítható, hogy a kiberbiztonsági szempontok nem kapnak jelentős szerepet a dokumentumban.

Áttekintésre került továbbá az Európai Parlament és a Tanács 2010/40/EU irányelve [36], ami az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésével és azok más közlekedési módokhoz való kapcsolódásának kereteivel foglalkozik. Az Európai

Parlament és a Tanács 2023/2661 irányelve [35] később módosította a korábbi jogi és szakmai tartalmat. A dokumentumok biztonságos közlekedésre és az intelligens közlekedési rendszerek működésére vonatkozóan határoznak meg kereteket.

A 48/2012. (VIII. 23.) NFM rendelet hazai vonatkozásban ad meg követelményeket az intelligens közlekedési rendszerek fejlesztésének és üzemeltetésének általános feltételeiről, az önvezető járművek tesztelésére vonatkozóan pedig a KöHÉM rendeletek határoznak meg követelményeket.[305]

Kiberbiztonsági vonatkozású elvárások a SAE J3061 szabványban jelentek meg először, 2016-ban. Ez magas szintű kiberbiztonsági alapelveket és útmutatást nyújt a modern járművekre vonatkozóan. Egyéb szabványok, például az ISO/SAE 21434, vagy a 26262 szabvány szintén foglalkozik az autóipari kiberbiztonsággal.

Igazságügyi szakértői feladatok oldaláról a hazai jogszabályi keretet az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (Szakértői törvény) adja meg, ami alapját képezi az általam kidolgozott szakértői módszertannak is. Fenyvesi Csaba Kriminalisztika és a Kriminalisztika elmélete és gyakorlata könyvei a szakmai háttér megalapozását segítette elő. Korábban Illési Zsolt a számítógépekre, hálózatokra vonatkozóan vizsgálta a kriminál technika alkalmazását.

A digitális forenzikus vizsgálatok értelmezésénél fontos megemlíteni André Årnes munkásságát és Digital foresics című könyvét, melyben a témakör alapjait fogalmazza meg, határozza meg és jó alapot biztosított a modern és egyre inkább önvezetővé váló járművek vizsgálatához, vizsgálati módszertanának kialakításához.

A szakmai háttér jellemzően nemzetközi munkacsoportok és szakmai szervezetek munkásságai eredményeként jelenik meg. A Digital Forensics Research Workshop 2001-ben elfogadott módszertana az azonosítás, adatmegőrzés, adathordozó összegyűjtés, adatkinyerés, vizsgálat és elemzés tekintetében tekinthető alapforrásnak. A Scientific Working Group on Digital Evidence szervezet és az European Network of Forensic Science Institutes dokumentumaiban szereplő ajánlások tekintetében relevánsak a kutatási téma szempontjából.

Értekezés felépítése

Az értekezés bevezető részében bemutatom a modern és egyre inkább önvezetővé váló közúti közlekedési járművek szakértői vizsgálati kutatási témám aktualitását, a nemzetközi és hazai vonatkozású aktualitásokat, valamint a téma igazságügyi szakértői relevanciáját. bemutatásra kerül a téma kapcsolódása a katonai műszaki tudományokhoz.

A következő részben megfogalmazom a tudományos problémát, a hipotéziseket és kutatási célkitűzéseimet. Ezt követően bemutatom az alkalmazott kutatási módszereket, a kutatómunkám korlátait, illetve azokat a kapcsolódó területeket, amelyek kizárásra kerültek a kutatásomból.

Az első fejezetben bemutatom a magas automatizáltságú járművek szerepét, polgári és katonai felhasználását, valamint az autonóm eszközök katonai alkalmazását. Egy-egy alfejezetben tárgyalom a modern járművek információgyűjtését, érzékelőhálózatait és funkcióit. Ismertetem a modern járművek kommunikációs megoldásait, továbbá a felmerülő kiberbiztonsági kockázatokat is.

Meghatároztam az autóipari kiberbiztonsághoz tartozó releváns szabványkövetelményeket, a jogszabályi elvárásokat. A kutatómunka megtervezéséhez behatárolom azokat a részterületeket, amelyekre összpontosítva hatékonyan teljesíthetem a kutatási célkitűzéseimet, elemezem a digitális forenzikus szakértői vizsgálatok meglévő módszertanait, figyelembe véve a modern és egyre inkább önvezetővé váló járművek vizsgálatában történő alkalmazhatóságukat.

Összegyűjtöm a járművek, mint adatforrásokként történő alkalmazhatósági lehetőségeit a szakértői vizsgálatokhoz kapcsolódóan.

Következő fejezetben kutatómunkám eredményét, a modern járművek szakértői vizsgálatának kihívásait tárgyalom, az általános kihívások, vizsgálati eljárások és vizsgáló eszközökhöz kapcsolódó kihívásokra kiterjedően. Kitérek az egyes vizsgálati lépések katonai műveletek során fellépő kihívásaira is.

A modern és önvezető járművek digitális forenzikus vizsgálata című fejezetben kitérek a kutatómunkám alapját képező vizsgálati módszertanokra, az egyes módszertani lépések vizsgálata által meghatározom ezek felhasználhatóságát a járművek esetén, figyelembe véve az előző fejezetben meghatározott kihívásokat is.

Definiálom az önvezető járművek szakértői vizsgálatát, annak módszertani lépéseit és rendszerezem ennek kapcsolódásait egyéb vizsgálati módokhoz.

Az utólsó fejezetben felmérem a szakértői vizsgálatok elvégzéséhez szükséges kompetenciákat, meghatározom a járművekkel kapcsolatos eltéréseket, valamint összegyűjtöm a kiegészítő tudás- és készségelemeket.

Értekezésem befejező részében összegzem az elvégzett kutatómunkát, illetve a levont következtetéseket, illetve megfogalmazom a tudományos eredményeket, javaslatokat és ajánlásokat fogalmazok meg.

1. Autonóm eszközök katonai alkalmazásban

A katonai műveletek tervezése egy komplex folyamat, ami egy sokszereplős rendszerben, a bonyolultság kezelésére létrehozott műveleti szinteken, korlátozottan rendelkezésre álló időtartamban valósul meg. A végrehajtásához létfontosságú az eltérő szintek művelettervező törzseinek rálátása a többi tervezési szint folyamataira, elengedhetetlen a rendelkezésre álló képességek ismerete, illetve létfontosságú az egységes műveleti, ezen belül logisztikai helyzetkép kialakítása és fenntartása. A művelettervezés célja a reális számvetésekre alapozott műveleti elgondolásra épülő, megvalósítható művelet terv kidolgozása, amely a kijelölt katonai szervezet eszközeivel valósítható meg.

A teljesen autonóm platformok, különösen azok, amelyeknél nincs szükség erőforráscserére (például műholdak vagy víz alatti észlelőrendszerek), jelentősen megnövelhetik a hírszerzés hatóidejét, miközben pontos információkat biztosítanak, ami lehetővé teszi a nagy távolságokból irányított fegyverek alkalmazását. Ez azt is jelenti, hogy egyes esetekben elegendő a megfelelően védett járműnek, a fegyverrendszernek, a felszerelt szenzoroknak és a kommunikációs csatornáknak jelenléte, mivel személyzet nem szükséges, hogy a helyszínen tartózkodjon. Ez azonban hálózatokra és érzékelőkre támaszkodik amellett, hogy magas az üzemeltetési költség.[279] Megkezdődött a drónrajok katonai fejlesztése és tesztelése is, amelynek során számos kicsi, olcsó, együttműködő és pilóta nélküli repülőgép hangolja össze tevékenységét, összefüggő egységként működve. A pilóta nélküli eszközöknek megfelelő autonómiával és intelligenciával kell rendelkezniük.[237] Napjainkban számos országban tesztelik a drónkötelékek mint osztott együttműködési rendszerek működését, amelyek sok kicsi, olcsó, pilóta nélküli repülőeszközből állnak. Az önállóan működő vagy autonóm

fegyverek ezen típusa új stratégiai, etikai és jogi kérdéseket vet fel. A rajzó drónok valódi előnyökkel járhatnak, de potenciális veszélyeket is hordozhatnak. A kutatók szerint a rajzó drónok által jelentett kockázatokat mérlegelni kell, mielőtt pusztító képességük kifejlődik. A rajzórendszerek jellemzően egyedi ágensekből állnak, amelyek kapcsolatban állnak egymással és környezetükkel. Az ágensek egyszerű szabályokat követnek, de az ágensek közötti interakciók meglehetősen bonyolult és kifinomult kollektív viselkedésekhez vezethetnek, ideértve a kialakuló intelligenciát is. Például egy raj alakzatban maradhat, miközben többször változtatja az irányt.[195] Az autonóm eszközök alkalmazása kapcsán megkerülhetetlen a mesterséges intelligencia (a továbbiakban: MI) érintése. A NATO MI-stratégiája rögzíti, hogy a mesterségesintelligencia-alkalmazások fejlesztése és használata a nemzeti és nemzetközi joggal összhangban történik, és megfelelő szintű mérlegelés és gondosság mellett fejlesztik és használják, és az elszámoltathatóság biztosítása érdekében egyértelmű emberi felelősséget kell alkalmazni. A dokumentumban kinyilvánítják, hogy az MI megfelelően érthető és átlátható lesz, többek között felülvizsgálati módszerek, források és eljárások alkalmazása révén, továbbá az ilyen képességek biztonságát, védelmét és robusztusságát tesztelésnek és bizonyosságnak vetik alá ezekben a felhasználási esetekben azok teljes életciklusa során.[219] A halálos autonóm fegyverrendszerek programozásuktól függően képesek érzékelni és reagálni emberi beavatkozás nélkül is, ennek köszönhetően képesek a célokat felderíteni, és megsemmisíteni azokat. Egy kibertámadás vagy meghibásodás kockázata azonban kétségessé teszi a „megszakítási" mechanizmus megbízhatóságát. A halálos autonóm fegyverrendszerek alkalmazásánál szükséges a szenzoradatok priorizálása, annak érdekében, hogy a fegyver a tervezett célnak megfelelően működjön. Félő, hogy enélkül a neurális hálózat nem tud reagálni a fegyver közvetlen környezetéből származó újonnan érzékelt eseményekre. A harctéri környezet dinamikus változékonysága miatt az új paraméterek vagy heterogén adatok beérkezése azokhoz az adatokhoz, amelyek alapján a fegyvert betanították, összezavarhatja a fegyver tűzkiváltáshoz szükséges folyamatait.[328] A rendkívül összetett gépi tanulási jelleg látszólag azt a benyomást kelti, hogy az eszközök maguk hozzák meg döntéseiket, így kezelőik kivonhatják magukat a felelősségre vonás alól. A szakirodalom különbséget tesz az autonóm MI-fegyverek és az autonómiával rendelkező mesterséges intelligencia között, ami két különböző etikai problémát vet fel a használatukkal kapcsolatban. Az autonóm fegyverek esetében korlátozott önállóságuk a gépi tanulással kombinálva azt jelenti, hogy üzemeltetőik továbbra is felelősek tetteikért, miközben nem képesek ellenőrizni a gépi döntéseket. Ha viszont a mesterséges intelligencia elérné az autonómia szintjét, az kiszámíthatatlanná és veszélyessé tenné döntéseit egy fegyverben.[39] Az MI-komponensnek kiszámítható, céltudatos és jól

kommunikált viselkedést kell produkálnia, helyesen azonosítva az emberi szándékokat és az emberi viselkedést. Mások szándékainak felismerése és azonosítása azonban bonyolult és szinte lehetetlen a megtévesztés, a manipuláció, illetve az érzelmi állapotok és a jelzések rejtése miatt.[181] A jövőben a mesterségesérzelem-technológia kutatási intenzitásának növekedése várható, amely idővel kiküszöbölheti a fenti problémát, és az MI-alkalmazásokat biztonságosabbá és hatékonyabbá teheti az autonóm fegyverrendszerek társadalmi elfogadottságának javulása mellett.[113] Az extrém környezeti körülmények között működtetett automatizált rendszerek jelenleg távolról működtethetők vagy korlátozott autonómiával bírnak, és nem rendelkeznek jelentős döntéshozatali, feladattervezési és intelligens vezérlési felhatalmazással. A kutatók szerint a zord környezet okozta kiszámíthatatlanság és bizonytalanság robusztusabb és alkalmazkodóbb megoldásokat tesz szükségessé, hogy magasabb szintű autonómiát és döntéshozatalt tegyen lehetővé a robotokban.[336] A szélsőséges külső körülmények továbbá az érzékelők meghibásodásához vezethetnek, amelyek téves információkat továbbítva az eszköz hibás működését vagy meghibásodását okozhatják.[137] A jövőben pedig számolni kell azzal, hogy az éghajlatváltozás hatásai az időjárási extremitások gyakoriságának növekedésével és intenzitásának erősödésével járnak, ami sok más mellett negatívan befolyásolja a technikai eszközök alkalmazási spektrumát.[236] Jól behatárolt és megfelelő módon felügyelt környezetben magas fokú autonómiával lehet felruházni robotikai rendszereket, azonban kilépve a „steril” labor-, üzemi környezetből rengeteg olyan külső, elsősorban környezeti hatás léphet fel, amely kockázatossá teszi a teljes körű autonóm rendszerek használatát. A mesterséges intelligenciát használó komplex autonóm rendszerek fejlődése megváltoztatja a konfliktusok természetét. A gyakorlatban az autonóm rendszereket alaposan tesztelik, mielőtt üzembe helyeznék őket, hogy biztosítsák a rendszer viselkedésének megbízhatóságát a várható helyzetekben. Az autonóm rendszerek összetettsége azonban valószínűsíti, hogy a valós harctéri környezet dinamikájában nem várt, felbukkanó viselkedést mutatnak. Ha autonóm rendszereket akarunk használni valós konfliktushelyzetekben, akkor figyelemmel kell lenni a kiszámíthatatlanság és a megbízhatóság közötti arányokra különböző rendszerszinteken.[310] Az MI megjelenése a katonai döntéshozatalban és a vezetési rendszerekben, hasonlóan az autonóm fegyverekhez, sok esetben ellenérzéseket vet fel. Az MI alkalmazása jelenleg az adatfeldolgozás és az információ-előállítás területén támogatja a döntéshozatalt, de kutatók hatékony felhasználási lehetőséget látnak a tervezési feladatok, illetve a műveletek vezetésének felgyorsítása területén is.[221]

A katonai vonatkozású digitális forenzikus vizsgálatok nemcsak számítógépekre, laptopokra vonatkoznak, idetartoznak a mobileszközök, a hálózatok, a felhőalapú rendszerek, valamint a különböző magas automatizáltságú közlekedési eszközök is, melyek a fenti területeket támogatják. A vizsgálatok célja azon eszközökben, rendszerekben és környezetekben található kulcsfontosságú nyomok/elektronikus adatok azonosítása, elemzése és utólagos vizsgálata, amelyeket katonai műveletekhez, hírszerzéshez, tevékenységekhez használnak. A nyomok alapján hiteles bizonyítékot kell szolgáltatni a vizsgált eseménnyel kapcsolatban, meg kell állapítani a felelősségi kérdéseket.

Az általános vizsgálati elvek a katonai megközelítés és a harctéri körülmények ellenére sem változnak. A nyomok gyűjtésének, megőrzésének, kezelésének és tárolásának folyamata során nem változhatnak meg, csak felhatalmazott és kvalifikált személyek végezhetik el az egyes műveleti lépéseket. Ehhez szükséges meghatározni azon tudás, képesség és tudáselemeket is, melyek lehetővé teszik a magas automatizáltságú járművek vizsgálatának elvégzését.

Ezen túl, minden olyan tevékenységet, vizsgálati fázist, amely az eszközök vagy az adatok vizsgálatához szükséges, ellenőrizhető módon, megfelelően dokumentálni szükséges. Katonai műveletekben a forenzikus vizsgálatokat általában specialisták végzik, különféle digitális forenzikus eszközökkel. Idetartoznak például a szakképzett operátorok, az alkalmazott forenzikus technikák, taktikák, eljárások és módszerek egyaránt, amelyek a digitális nyomok azonosításától a feldolgozásáig és elemzéséig végzik feladatukat.[60] A speciális körülmények között megszerzett digitális nyomok döntő jelentőségűek lehetnek a műveletek sikere szempontjából, a műveleti, a hírszerzési és a jogi célok tekintetében egyaránt.[67][247][289][292]

Magas automatizáltságú és önvezető közúti közlekedési járművek

A modern járművek közlekedése és annak összehangolása hatással van a teljes közlekedési ökoszisztémára. Az automatizált közlekedés jelenős potenciált és új kiberbiztonsági fenyegetéseket is jelent. A járművek működéséhez és közlekedéséhez egyre inkább nélkülözhetetlen informatikai és infokommunikációs háttér segítségével, az okos eszközökkel történő összekapcsolódás, a jármű felhasználási lehetőségei, különböző mobilitási szolgáltatások, a különböző forgalmi szituációkban történő interakciók által a járművek napjainkban is szerves részét képezik a digitális környezetnek. Ez a jövőben várhatóan tovább fokozódik, a járművek még inkább integrált részei lesznek a kibertérnek.

A társadalom működéséhez, az egyének és a közösség életéhez nélkülözhetetlen a mozgás, a helyváltoztatás, ami a közlekedés lényege és egyben alapfolyamata. „*A közlekedés személyek, dolgok, gondolatok (információk) speciális technikai eszközök igénybevételével lebonyolított tömeges, rendszeres, szervezett helyváltoztatása*.”.[77] A magas automatizáltság, az IT, IoT és kiber-fizikai rendszerek fejlődése nagy mértékben átalakította napjaink közlekedését. Az önvezetés széleskörű elterjedésével pedig további átalakulás várató.

A helyváltoztatási igényeket és magát a helyváltoztatást valósítják meg a különböző közlekedési alágazatok. A járműipar fejlődésével, az egyre modernebb járművek, valamint a fejlett elektronikus rendszerek megjelenésével és széleskörű elterjedésével az utakon, megnövekedett a balesetek száma. Bár az Európai Unió közutak biztonságára vonatkozó mutatószámai világviszonylatban jónak számítanak, a halálos kimenetelű közúti balesetek számát az évi ~25 000-ről 2030-ra a 2020-as érték felére tervezik csökkenteni. Hasonlóképpen a súlyos sérüléssel járó balesetek esetén, a jelenlegi ~135 000-es értékről az ún. *Vision Zero* célkitűzés alapján.[106] A közlekedési rendszerek elsődleges céljai közé tartoznak a közlekedésbiztonság fokozása és az infrastruktúra kihasználtságának maximalizálása, a forgalom racionalizálása, a környezeti terhelés csökkentése.[77]

A közlekedési rendszerek fejlesztése, a közlekedés digitalizálása, az intelligens közlekedési rendszerek (ITS) alkalmazása hozzájárul a fenti célok eléréséhez, biztonságosabbá, hatékonyabbá és fenntarthatóbbá tehetik a közlekedést. „*Az ITS kifejezést hivatalosan 1994 óta használják. A közúti telematika (transport telematics) kifejezés az ITS szinonimájaként is értelmezhető, mely kifejezést Európában 1990-es évek kezdetétől használják*”.[76] „*Tágabb*

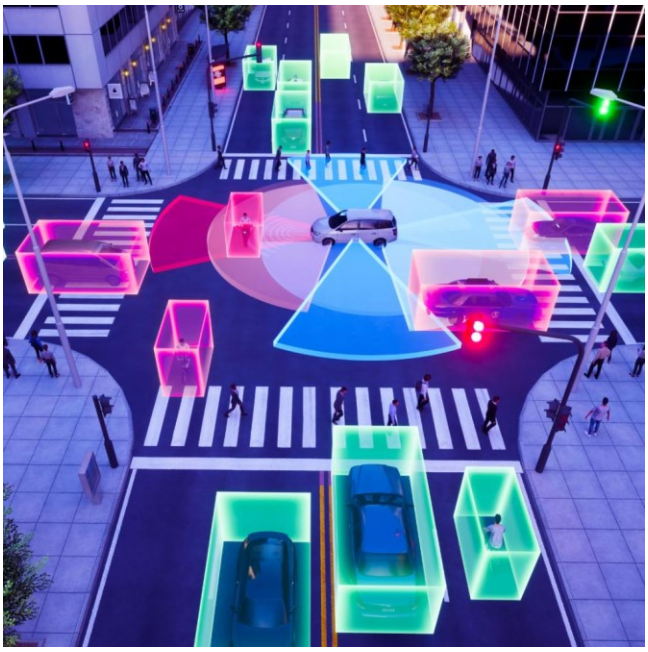
értelemben az ITS rendszerek a közlekedési hálózatokon és járművekben alkalmazott információs és kommunikációs (telematikai) megoldások összessége, melyek dinamikus, valósidejű (real-time) adatok alapján működnek.".[76]

Az intelligens közlekedési rendszerek „*tényleges (emberi) intelligencia megtestesítése nélkül biztosítanak innovatív szolgáltatásokat a különböző közúti közlekedési módokhoz és forgalmi menedzsmenthez kapcsolódóan*".[3] Az ITS-ek az információs és kommunikációs rendszerek alkalmazása mellett a meglévő technológiák hatékony integrálását is megvalósítják. „*Tágabb értelemben az ITS rendszerek a közlekedési hálózatokon és járművekben alkalmazott információs és kommunikációs (telematikai) megoldások összessége, melyek dinamikus, valósidejű (real-time) adatok alapján működnek.*"[77].

A magas automatizáltságú járművek jelentősen javíthatják a közlekedési biztonságot, a valós idejű információmegosztásnak köszönhetően időben értesíthetik a veszélyekről a többi felhasználót. Az ITS-eknek több alkalmazási lehetősége van, például:

- navigációs rendszerek,
- forgalom és parkolóhely elérhetősége,
- figyelmeztetések útépítésekről és torlódásról,
- elektronikus díjszedés,
- forgalomirányítás,
- autómegosztási szolgáltatások,
- támogatás az automatizált vezetéshez.

Sok ilyen megoldás szabványosított specifikációkra épül, amelyek lehetővé teszik Európa különböző szolgáltatóinak adatcseréjét és használatát.[147]



1. ábra Járművek érzékelése és digitális környezetük leképezése [165]

Az ITS digitális kommunikációs technológiák felhasználásával javítja a közlekedésbiztonságot, a forgalomirányítás hatékonyságát és az eltérő közlekedési módok közötti koordinációt az utasok, és a vezetők számára. A járművek és a többi úthasználó összekapcsolása, lehetővé teszi az adatok gyűjtését és cseréjét a forgalom és a közlekedésbiztonság fejlesztése érdekében. Zöldebb, biztonságosabb, hatékonyabb közlekedést tesz lehetővé, hozzájárul a torlódások csökkentéséhet, a forgalmi dugók elkerüléséhez, ösztönzi az alacsony CO_2 kibocsátású közlekedés használatát, valós idejű adatokon alapuló elemzéseket tesz lehetővé. Segít összehangolni, összekapcsolni és koordinálni a különböző közlekedési módokat rendkívüli helyzetekben, például baleset, természeti katasztrófa esetén.[147]

Az ITS-ek előnyei mellett számos kihívás is felmerül. Új szolgáltatásokat és munkahelyeket teremthet, amennyiben összehangolt és következetes módon kerülnek bevezetésre és nagy hangsúly kerül a kiberbiztonsági szempontokra is, függetlenül attól, hogy az egyes szolgáltatások, ITS elemek vagy résztvevők milyen szolgáltatóhoz, vagy szervezethez tartoznak.

Az Európai Bizottság a digitális évtizedre vonatkozó kiberbiztonsági stratégiájában meghatározta, hogy biztosítani kívánja a megfelelő csatornákat, szabályokat a nyomozások során szükséges elektronikus bizonyítékokhoz való hozzáférést, abban az esetben is, ha a szolgáltatók eltérő joghatóság alá is tartoznak („*a nyomozások 85 %-ában szükség van erre, és az összes megkeresés 65 %-a más joghatóság alá tartozó szolgáltatókhoz érkezik*) […] Az

elektronikus bizonyítéknak olvashatónak kell lennie, ezért a Bizottság továbbra is azon dolgozik, hogy támogassa a bűnüldözési kapacitást a digitális nyomozások területén, beleértve a titkosítást a bűnügyi nyomozásokban, teljes mértékben betöltve az alapvető jogok és a kiberbiztonság védelmére irányuló feladatát.”.[33]

Az ITS-rendszerek következő generációja a kooperatív intelligens közlekedési rendszerek (Cooperative Intelligent Transport Systems, C-ITS), amelynek célja a hatékony adatcserével, a vezeték nélküli technológiák alkalmazásával megvalósulhat a közlekedés automatizálása. A közúti közlekedési rendszer elemei, az infrastruktúra, a jármű, a járművezető, az utazó, gyalogos stb. közötti információmegosztás valósítható meg, annak érdekében, hogy tevékenységeiket, közlekedésüket összehangolhassák. A kommunikációt az összes olyan közlekedési résztvevő között meg kell valósítani, akik „érintkezésben” vannak, konfliktushelyzetbe kerülhetnek egymással.[76]

2. ábra Kooperatív intelligens közlekedési rendszer az egymással és környezetükkel kommunikáló járművekkel [65]

C-ITS rendszer alapja a vezeték nélküli technológiákon alapuló gyors, hatékony adatcsere, hogy a közlekedési járművek egymással, a környezeti és pályaelemekkel, a közúti infrastruktúrával és a többi úthasználóval kapcsolatba léphessenek.[47][217]

A technológiai fejlődés nem csupán a közlekedési rendszerekre van nagy hatással. Az egyre komplexebb összekapcsoltság és a fejlett automatizálás interdependenciája új lehetőségeket teremt a közlekedés hatékonyságának és biztonságának növeléséhez. Ehhez az egyik lépés, hogy a jármű segíti a járművezetőt, a forgalmi helyzethez való alkalmazkodásban és a megfelelő döntések meghozatalában, illetve az emberi tényező hatásának csökkentése, ellensúlyozása, a vezető nélküli járművekre való átállás. Az autonóm módon működő járművek hosszú távon nagyobb biztonságot eredményeznek majd.

A SAE J3016 számú nemzetközi szabvány hat szintet határoz meg a polgári felhasználású közlekedési járművek vezetésautomatizáltságára. Az első három szinten (SAE 0-2) a jármű vezetője felügyeli az eseményeket, a második három szinten (SAE 3-5) maga a jármű végzi mind a felügyeleti, mind a járművezetési feladatokat. Itt megjelennek az önvezető képességek, automatizált vezetési szolgáltatások, azonban a vezető felügyelete és beavatkozása még elengedhetetlen. A jármű jelzése esetén a vezető át kell vegye az irányítást, vagyis korlátozott módon valósul meg az autonóm működés. A közeljövőben megjelenő, SAE 4-es szintű automatizált vezetési szolgáltatásokkal felszerelt járművek esetén már nem lesz szükség arra, hogy a vezető beavatkozzon, átvegye az irányítást. A SAE 5-ös szint pedig a teljesen autonóm járműveket jelenti majd, olyan automatizált vezetési szolgáltatásokkal, amelyek a járművet minden helyzetben, körülmény között képesek lesznek vezetni.[25][85][323][331]

A járművek automatizáltságának szintjei az alábbi ábrán láthatóak a Society of Automotive Engineers (SAE) által meghatározott módon.

3. ábra A járművek automatizáltságának szintjei [5]

A SAE felosztása közúti vagy terepjáró járművek esetén megfeleltethető az Amerikai Védelmi Minisztérium (Department of Defense; a továbbiakban: DoD) által meghatározott evolúciós lépcsőknek. Az első lépcsőhöz, szinthez a nem autonóm, vagyis az ember által üzemeltetett rendszerek tartoznak (SAE 0). A második (ember által delegált) lépcsőben egyes vezetési funkciók (például az adaptív tempomat működése során a gyorsítás, a lassítás vagy/és a kormányzás) már támogatottak, ez a SAE 1-es és 2-es szintjének feleltethető meg. Ezen a szinten például a célkiválasztás továbbra is az ember által történik. Az ember által felügyelt DoD 3-as lépcsőhöz a SAE 3-as szint rendelhető hozzá. Ezen a szinten az ember felügyelete alatt történik az eszközök működése (például a drónok rajban vagy a járművek menetoszlopban való közlekedése). A járművezető (meghatározott körülmények között és helyzetekben) nem vesz részt a közlekedési vagy repülési szituációk végrehajtásában (nem vezeti a járműveket), azonban erre utaló jelzés esetén (SAE 3) a vezetőnek át kell vennie az irányítást a járműtől. A SAE 4-es szint esetén a jármű közlekedéséhez nem szükséges a járművezetői irányítás, teljes a jármű autonómiája (ideértve a közlekedési és önálló célkiválasztási feladatokat, akár az emberi élet kioltására irányuló döntés meghozatalát is).

Az autonómia a katonai rendszerekben várhatóan az alábbi öt területen kap majd nagy szerepet:

- logisztika, flottaszervezés,
- a nagy mozgékonyságú katonai rendszerek fizikai felépítése,
- az autonóm eszközök egyedi viselkedése,

- az emberek és az autonóm rendszerek közötti együttműködés,
- műveleti és csoportstratégiák.[38]

Az autonomitás szintjének növekedésével, a felelősségek átrendeződésével egyre nagyobb hangsúlyt kap a tevékenységek utólagos vizsgálata és elemzése, az objektív bizonyítékok előállítása, amelyhez a forenzikus vizsgálatok során a tudomány és a technológia eredményeit és módszereit használják a szakértők.[41]

Figyelembe véve a járművek átlag életkorát, várhatóan a hagyományos járművek és a ténylegesen autonóm járművek még legalább 10–15 évig együtt lesznek jelen a közlekedésben, amely új kockázatokat és kihívásokat jelent.[4]

A modern és a jövőbeni autonóm közúti közlekedési járművek bőséges adatforrást jelentenek a szakértői vizsgálatok elvégzéséhez. Az ilyen járműveknek képesnek kell lennie a pontos helymeghatározásra, a környezetükben történő lokalizációra. Ez azt jelenti, hogy a járműveknek minden időpillanatban, néhány cm-es pontossággal, teljes megbízhatósággal kell ismerniük a pontos helyzetüket a környezetükhöz, illetve a környezetükben lévő járművekhez viszonyítva. Az elmúlt időszak műszaki fejlődésének egyik jelenségeként figyelhető meg, hogy a valós világról egyre pontosabb, részletesebb információkkal rendelkeznek a közlekedési járművek és az információk sokrétű felhasználása egyre szélesebb körben jelenik meg.

A modern járművek és az intelligens közlekedési rendszerek működéséhez, működtetéséhez megfelelő mennyiségű és minőségű információra van szükség. Az információhoz való hozzáférés és gyűjtés elsődleges feladat a járművek esetén, amelynek során az információk valamilyen érzékelési cselekvéssel (sensing action) kerülnek szenzorhálózatok közreműködésével begyűjtésre.

A közlekedésben az információ, az adatok a tárgyakról, környezetei és pálya elemekről, személyekről, folyamatról szerzett ismeretek egy bizonyos szerkezetben való egyesítését jelenti. Már a modern közlekedési járművek is szenzoraik segítségével érzékelik környezetüket (például az optikai érzékelők, lézeres radar, képelemzés stb.), az érzékelők által szerzett információkból – ideértve a navigációs információkat is – meg tudják határozni helyzetüket a környezetben, valamint a többi járműhöz viszonyítva. A járművek pedig képessé váltak egyes funkciók ellátására emberi irányítás, beavatkozás nélkül is, például elkerülni az ütközéseket.[77]

A modern vagy önvezető járművek esetén - mint gördülő számítógépek vagy „IoT device on wheels”[94] - különféle összetevők (elemek és ezek működése) és kapcsolataik alkotják a rendszereket. Ezekben az információt az információkat kezelő elemek a jármű biztonságos működésének fenntartása és a jármű működési, működtetési feladatai érdekében dolgozzák fel. Egy-egy művelet, részfolyamat, folyamat végrehajtása érdekében egyre összetettebb E/E (elektromos/elektronikus architektúra) architektúra megoldások segítségével. Az elektromos/elektronikus architektúra az elektronikus hardverek, a hálózati kommunikáció, a szoftveralkalmazások és a kábelezés egyetlen integrált rendszerbe való konvergenciáját jelenti, ami egyre több járműfunkciót vezérel, a járművezetés, a karosszéria és biztonság, az infotainment, az aktív biztonság, valamint egyéb kényelmi, praktikus és csatlakoztatási funkciók területén.[329] Az E/E a megoldások, az egyre szélesebb körű igények (pl.: sebesség, közlekedésbiztonság, költség, funkcionalitás, flexibilitás és egyre kevesebb emberi beavatkozásra való igény), az automatizált vezetés által generált elvárások, a V2X kommunikáció és a járművek növekvő elektronikussá válása miatt egyre inkább szoftver vezérelté válnak a járművek. A járművek E/E rendszereihez kapcsolódó kulcsfontosságú területek a következők:

- belső tér és utastér:
    - ember-gép interfész (műszerfal),
    - infotainment,
    - telematika,
- jármű alváz és karosszéria:
    - járművezérlés, alvázelektronika
    - Karosszériavezérlés

A jelenlegi (flat hálózat) struktúrák nem biztosítják a célok hatékony megvalósítását, egy átlagos autóban közel száz vezérlőegység működik, „*az elektromos rendszerek bonyolultsága a jövőben sem lesz egyszerűbb*” [24] és ez jelentős költséget jelent. Külön modul vezérli a légkondicionálót, a motorvezérlést, az ajtónyitást, az infotainment-et, stb. „*Elengedhetetlen, hogy ez a komplexitás kezelhető legyen, hiszen csak így biztosítható, hogy a jármű funkciói az élettartama során bármikor frissíthetők, és így biztonságosak maradjanak. Minden eddiginél nagyobb szükség van tehát a különféle autóelektronikai alkatrészek és rendszerek zavartalan együttműködését szabályozó előírásokra.”.* [24] Különböző projektek (pl.: SofDCar projekt), szabványok (pl.: ISO/SAE 21434:2021, ISO 26262-1:2011), regulációk (UN R 155 és UN R 156) célja, hogy szabályokat pontos folyamatokat alakítson ki a járművek jövőbeli

szoftverfrissítéseinek ellenőrzésére, emellett következetes funkcionális és kiberbiztonsági módszertant alakítson ki, az iparági szereplők számára.[24] Ezek által megelőzhetővé válik, hogy az egyes szoftverek megzavarják egymást, káros hatással legyenek egymás működésére és biztosítani kell, hogy a rendszeren belül megfelelően, hiba nélkül működjenek, csökkentve a szoftverhibák okozta kihasználható sebezhetőségek valószínűségét.[61] A járművekben található szoftverkódok mennyiségének növekedése szélesíti a potenciális támadási felületet, új támadási vektorokat jelenthet és sérülékeny rendszerekhez vezethet. A kockázat csökkentése érdekében a gyártók biztonságos fejlesztési életciklust (Secure Software Development Life Cycle) szükséges alkalmazzanak, azonban a 100 %-os biztonság ezen rendszerek esetén sem lesz garantálható.

„*A szoftveresen definiált járművek két kiemelkedő előnnyel rendelkeznek*”[294]:

- fejlesztés és fejlődés sebessége,
- a szoftver- és hardverfejlesztés szétválasztása, frissítések letöltési lehetősége (OTA), hasonlóan a mobiltelefonokhoz.[294]

Új szoftverfrissítések, firmware-k vagy egyéb adatok (pl.: titkosítási kulcsok) gyártók általi vezeték nélküli továbbítása. Korábban mobilszolgáltatók a mobileszközök vagy a sim kártyán lévő adatok frissítéséhez küldtek vezeték nélkül információkat. Az IoT eszközök elterjedésének hatására már a modern járművekben is használják ezt a frissítési megoldást. Erre korábban a felhasználóknak memóriakártya, vagy CD lemez behelyezésével volt lehetőségük (pl.: térkép frissítése), vagy a szervízben végezték a frissítések telepítését. A frissítések vezeték nélküli (pl.: mobil hálózaton keresztüli) továbbítása, a járműhöz való eljuttatása hatékony és költségkímélő módja a hibák javításának, szoftverfrissítések elvégzésének és az új funkciókhoz való hozzáférésnek. A járművekhez tartozó vezeték nélküli adattovábbítási módok lehetnek:

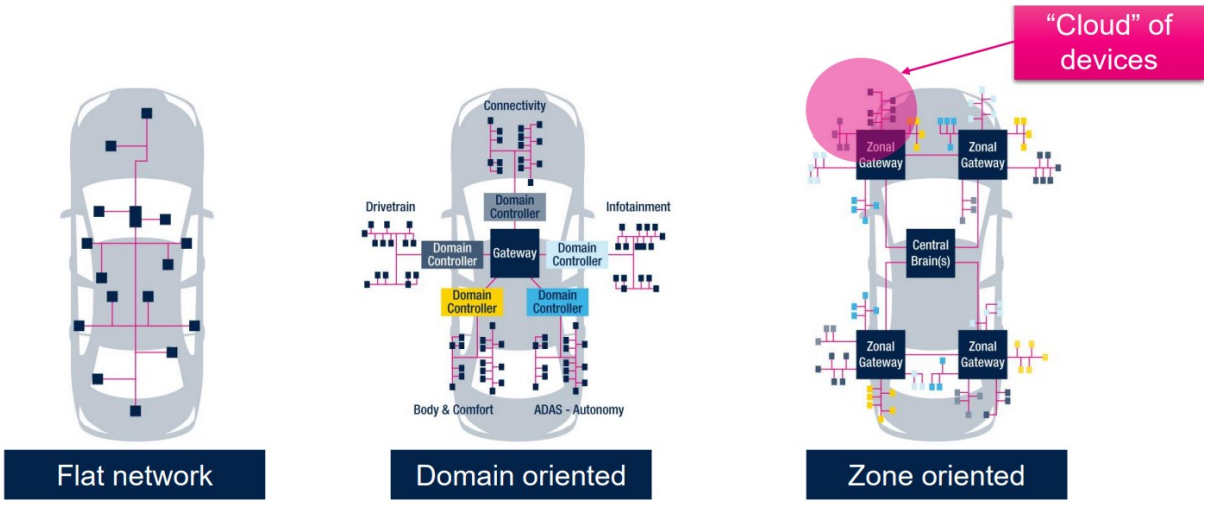
- Firmware-over-the-air (FOTA),
- Software over-the-air (SOTA),
- Over-the-air provisioning (OTAP),
- Over-the-air service provisioning (OTASP),
- Over-the-air parameter administration (OTAPA).

FOTA esetén a járműhöz, a jármű egyes egységeihez tartozó firmware kerül kiküldésre. SOTA esetén szoftverfrissítés, OTAP segítségével beállítások, konfigurációk, OTASP esetén szolgáltatás nyújtás, beállítás, míg OTAPA révén paraméterezés, konfigurálás történik. A

frissítések abban az esetben érkeznek meg az autóhoz, ha az kapcsolódik az internethez, amíg a frissítések letöltődnek.[84][232] Ezen kommunikációk vizsgálata és elemzése az élő adatforgalom lehallgatása által vagy rögzítése esetén utólagosan történhet.

4. ábra Jármű frissítések over-the-air [318]

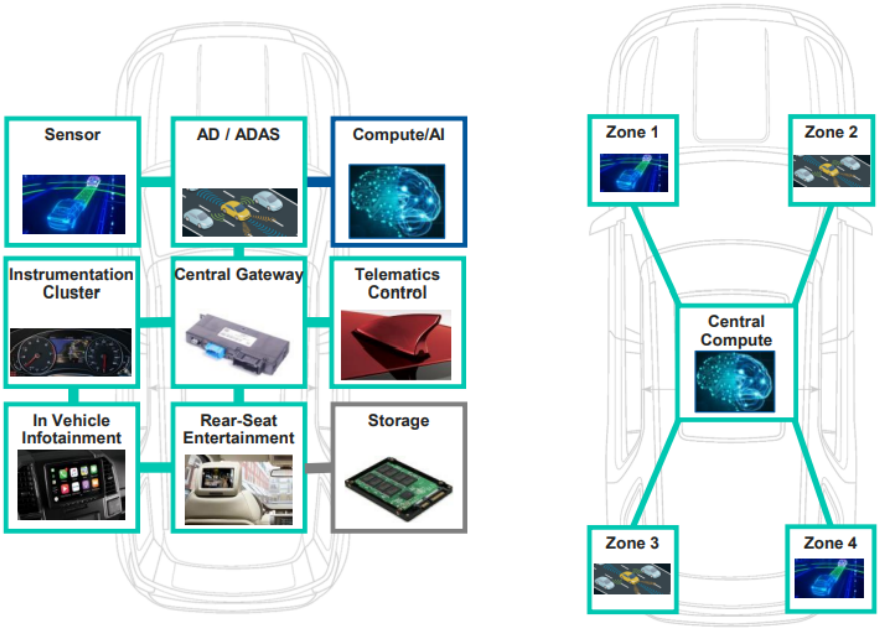
A gyártók egyre inkább elmozdulnak a funkcióktól a szolgáltatások irányába. Az architektúráknak ezen változásokhoz alkalmazkodniuk kell. Az új igényekre a központosított rendszerek (centralized system) és a komplex szoftver megoldások jelentik a megoldást.[29]



5. ábra Járművek belső kommunikációs hálózatának átalakulása[140]

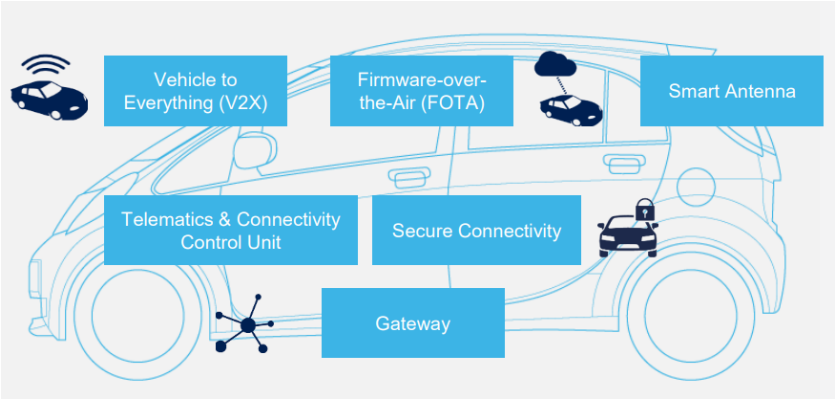
Ahogyan a járművek belső hálózata az ún. egyszerű/flat hálózattól mára eljutott a központi, domain orientált hálózatokig, a magas automatizáltságú és egyre inkább önvezetővé váló járművek esetén a zónás kialakítás, a zónák közötti átjárók (Zonal Gateway) és a központi „agy”

(Central Brain(s)) alkalmazásával lép a következő szintre. A központi agy által és a mesterséges intelligencia megoldások alkalmazásával a járművek még intelligensebbekké válnak. „*Az elemzők előrejelzései szerint, az évtized végére az újonnan értékesített járművek több mint a fele egy nagy teljesítményű központi architektúrával rendelkezik majd*.”.[186]



6. ábra Modern járművek belső, központosított, zóna alapú hálózata [303]

A hatékonyabb E/E architektúrák segítik az adatgyűjtést, akár 20 %-al kevesebb ECU kerülhet a járművekbe ezáltal rövid távon enyhíti az alapanyag hiány (pl.: chiphiány) hatását, hozzájárul a gyártási költség csökkentéséhez, továbbá a gyártó számára lényeges adatok visszacsatolására is lehetőség nyílik. Ezzel párhuzamosan az autógyártók oldalán, az over-the-air (OTA) frissítési megoldásnak köszönhetően csökkenhetnek a költséges visszahívások is.[94][140][329][339]



7. ábra Modern járművek belső és külső hálózati kapcsolatai [140]

Járművek információgyűjtése

A modern járművek vezetéstámogató rendszereinek biztonságos és megbízható működésének alapját a különféle érzékelők és az általuk gyűjtött érzékelőadatok képezik. A jármű a radar, kamera és lidar szenzorok adatainak szükség szerinti kombinálásával térképezi fel pontosan a környezetét, az összegyűjtés és gyors feldolgozás, valamint az adatok értelmezése által lehetőség nyílik a döntéshozásra, majd az autó által végrehajtandó reakció/beavatkozás, ami különböző jármű manővereket jelent (pl.: lassítás, irányváltoztatás, gyorsítás). [259][296]

„Az intelligens járművek és járműrendszerek „olyan megoldások, melyek a járművekbe épített – az emberi feldolgozásnál – fejlettebb (gyorsabb, nagyobb számítási kapacitással rendelkező stb.) érzékelő és beavatkozó rendszerek segítségével" támogatják az alábbi célok megvalósítását:

- *Közlekedésbiztonság növelése (pl. aktív biztonsági rendszerek, melyek a balesetek megelőzésére koncentrálnak, a balesetveszélyes helyzetek korai felismerésével).*
- *A közlekedési infrastruktúra fokozottabb kihasználtsága (pl. járművek közötti követési távolság csökkentése a járművezetést támogató megoldásokkal).*
- *Utazási kényelem növelése (egyes járművezetői funkciók vagy a teljes járművezetés átvállalásával).*
- *Járművezetési hatékonyság növelése és a környezeti terhelés csökkentése (pl. a forgalmi és infrastrukturális körülményeknek megfelelően takarékos üzemanyag-felhasználás).*[76]

Az intelligens közlekedési járművek és rendszerek funkció szerint csoportosíthatóak:

- észlelést támogató rendszerek,
- menetdinamikai támogató rendszerek,
- veszélyre figyelmeztető rendszerek,
- veszélyhelyzeti támogató rendszerek,
- kapacitás és hatékonyság növelő,
- járművezetői kényelmet fokozó rendszerek,
- ellenőrző rendszerek.[76]

Az észlelést támogató rendszerek segítik a járművezetőt például a holttér figyelésben, a vizuális észlelésben (pl.: éjszaka, infravörös kamerák segítségével), felismerik a jelzőtáblákat, vagy figyelmeztetik a vezető éberségét).

A menetdinamikai támogató rendszerek olyan vészhelyzeti szituációban vagy standard körülmények között aktiválódó rendszerek, amelyek biztosítják a stabil úttartást, szabályozzák a fékerőt, megakadályozzák a kerekek kipörgését. A járművek stabilitásának és kormányozhatóságának fenntartásával segítik a vezetőt a jármű feletti irányítás megtartásában.

Veszélyre figyelmeztető rendszerek vizuális jelekkel, hanghatásokkal vagy egyéb ingerek által potenciális veszélyforrásokra figyelmeztetik a jármű vezetőjét. A rendszerek figyelmeztetését kiválthatja a sáv elhagyás, ütközéshez közeli állapot. A figyelmeztető rendszerek, támogató rendszerekkel történő összekapcsolásával a jármű segíti a sávváltást, segít elkerülni az ütközést, vagy balesetet. A kooperatív közlekedési rendszerek elterjedésével, a különböző kommunikációs csatornákat felhasználva hatékonyabbá teszik a balesetek elkerülését és a vészhelyzetek kialakulásának lehetőségét.

A vészhelyzeti támogató rendszerek közé tartozik még a vészhelyzet, vagy baleset esetén aktiválódó passzív biztonsági rendszerek, melyek célja a vezető és az utasok védelme.

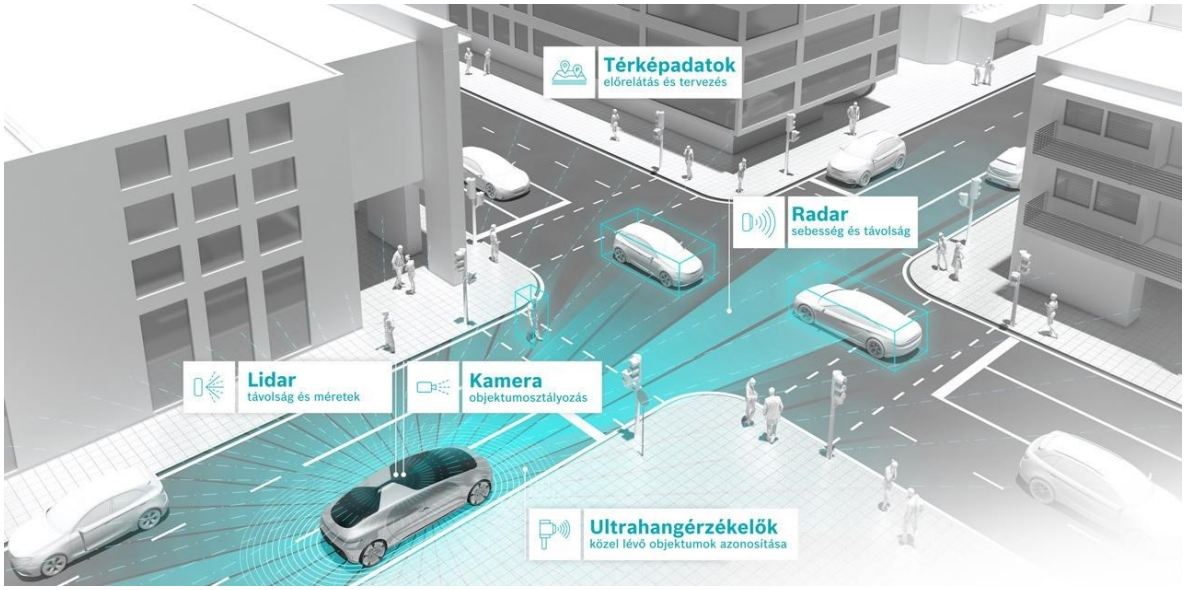
A kapacitás és hatékonyság növelő rendszerek segítik a hatékony üzemanyag felhasználást és a pálya kapacitásának kihasználását segítik a sebesség harmonizálásával. Az adaptív sebesség és távolságtartó rendszerek, a sebességváltás esedékességét jelző rendszerek és a járműszerelvények mozgását összehangoló rendszerek elsősorban a járművek hajtás- és fékrendszerét szabályozzák.

A járművezetői kényelmet fokozó rendszerek egyes funkció végrehajtását végzik a vezető helyett. Kényelmi rendszerek például az adaptív fényszóró-vezérlés, a sebességfüggő szervokormány, az esőérzékelős ablaktörlő, head-up display és a hangvezérlés. A vezetői feladatokat támogató rendszerek közé tartoznak a sávtartó rendszerek, a stop and go rendszer, a parkolási asszisztens és az elöl lévő járművet automatikusan követő rendszer is.

Az ellenőrző rendszerek mind a vezető, mind a jármű ellenőrzésére szolgáló megoldások. A digitális tachográf, a fedélzeti járműdiagnosztikai rendszer vagy a fogyasztás és károsanyag kibocsátás ellenőrző rendszer segítségével a járművek működése ellenőrizhető, emellett lehetővé teszik az utólagos elemzést is. [76][260]

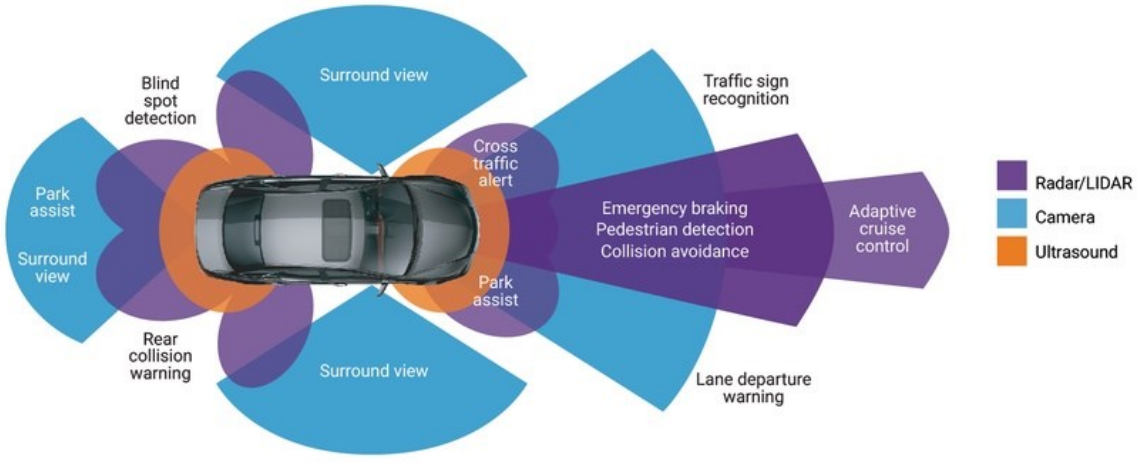
A modern járműveken a fenti funkciók megvalósításához, napjainkban különféle szenzorokat, külső állapotérzékelőket helyeznek el, melyek kiemelt szerepet játszanak a járművek környezetének feltérképezésében, lokalizációjában, az önvezető technológia fejlesztésében. Ezen szenzorok (pl.: lidar, radar, GPS, ultrahang) és a kamerák által gyűjtött adatok nagy

mennyiségben dolgozzák fel és tárolják (másodpercenként nagyjából egy GB adatot) a modern járművekben.



8. ábra Modern járművek szenzorai által érzékelt környezeti elemek [12]

A közlekedésbiztonsági rendszerek (automotive safety) hosszú utat jártak be az első alkatrészek beszerelésétől a számítógép vezérlésű automatikus, érzékelőhálózatokon alapuló rendszerekig.



9. ábra A hajtáslánc vezérlő által végrehajtott irányítási funkcióhoz kapcsolódó érzékelők és azok lefedettsége [11]

A fejlesztések célja vezetők, utasok, gyalogosok, környezet és maga a jármű védelme volt, melyek megvalósítására két területen figyelhető meg gyors fejlődés: az aktív és a passzív biztonság esetén.

A passzív biztonsági eszközök alatt azon elemeket értjük, melyek feladata az utasok védelme, valamint az okozott és elszenvedett kár csökkentése, vagyis reaktív védelmi intézkedéseket foglal magában. Ezen passzív védelmi rendszerek fejlődése az 1880-as évekre vezethető vissza, melyektől eljutottunk a mai modern biztonsági rendszerekig. Az első és mai napig a legfontosabb passzív biztonsági elem a jármű lámpái és a biztonsági öv.

Aktív biztonságot értelmezhetjük a technológiaként, mint preventív és proaktív védelmi megoldások, melyek célja a balesetek megelőzése. Az aktív rendszerek a baleset elkerülése érdekében képesek átvenni az irányítást a gépjármű felett, vagy felülírni a járművezető utasításait. Az 1970-80-as években az elektronika kiemelt szerepet kap in vehicle safety technology, előkészítve aktív safety elemek fejlődését. 1971-ben a Crysler Imperial volt az első sorozatgyártott jármű, ami alapfelszereltségben tartalmazott an anti-lock braking system (ABS) rendszert.

Később megjelent a menetstabilizáló (ESC), a vészfék asszisztens (BAS), elérhetővé vált a sávelhagyásra figyelmeztető asszisztens (LWDS). A Volvo által bevezetésre került a holttérfigyelő rendszer (BLIS), emellett a gyalogos felismerő rendszer, amely növelte a gyalogosok biztonságát. A rendszer, amint beazonosítja a gyalogost (úttesten való áthaladás során) szükség szerint automatikusan lelassítja a járművet. Az ütközést megelőző biztonsági rendszer (PCS) a jármű felgyorsításával vagy épp kikerülő manőverek alkalmazásával segíti a balesetek megelőzését.[65][253]

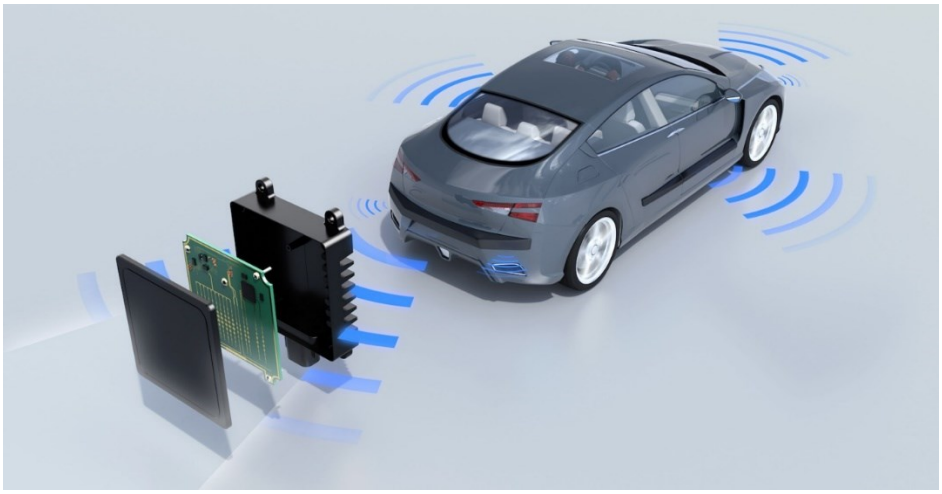
Ezen aktív biztonsági rendszerek és az idő közben megjelent további megoldások is a jármű szenzorainak adatai, az elektronikus vezérlőegységekben feldolgozott és tárolt adatok alapján működnek, melyek hasznos adatforrást jelenthetnek a szakértői vizsgálatok során.

Radar szenzor

A RADAR szó az angol Radio Detection and Ranging származik, mely jelentése magyarul „rádiós észlelés és távolság mérés”. „*A radar megbízható adatokat szolgáltat az objektumok sebességéről és távolságáról, szögéről, különösen olyan kedvezőtlen időjárási körülmények között, ahol az optikai érzékelők nehézségekkel küzdhetnek, például magas fényerő, eső, köd, hó és por esetén*”.[245] Amennyiben egy nagyon rövid ideig (kb. 1 milliomod másodpercig) tartó, szűk nyalábú, nagy frekvenciájú (9,5 GHz, vagyis 3,2 cm a hullámhosszú) rádióimpulzust bocsátunk ki egy irányított antennán keresztül az adóból, akkor a rádióhullámok útjában lévő tárgyak miatt a rádióhullámok nagyobb része szétszóródik. A szórt jelek közül egy kevés az adó irányába visszaverődve visszajut az adó antennával azonos vevőantennához is. Ezeket az

antenna felfogja, majd megfelelő erősítés után a képernyőn egy képpontként megjeleníti. Ez az észlelés folyamata. A távolság mérés azon alapszik, hogy a rádióhullámok fénysebességgel terjednek, a kibocsátás és visszaérkezés közötti időt mérve, a céltárgy távolsága kiszámítható.

Előnye, hogy a fényviszonyoktól független, kis méretű, „olcsó” eszközök, melyek biztonságkritikus funkciókhoz használhatóak. A kamerával ellentétben kis felbontásúak, az időjárási körülmények befolyásolhatják, a visszaverődések zavarhatják.

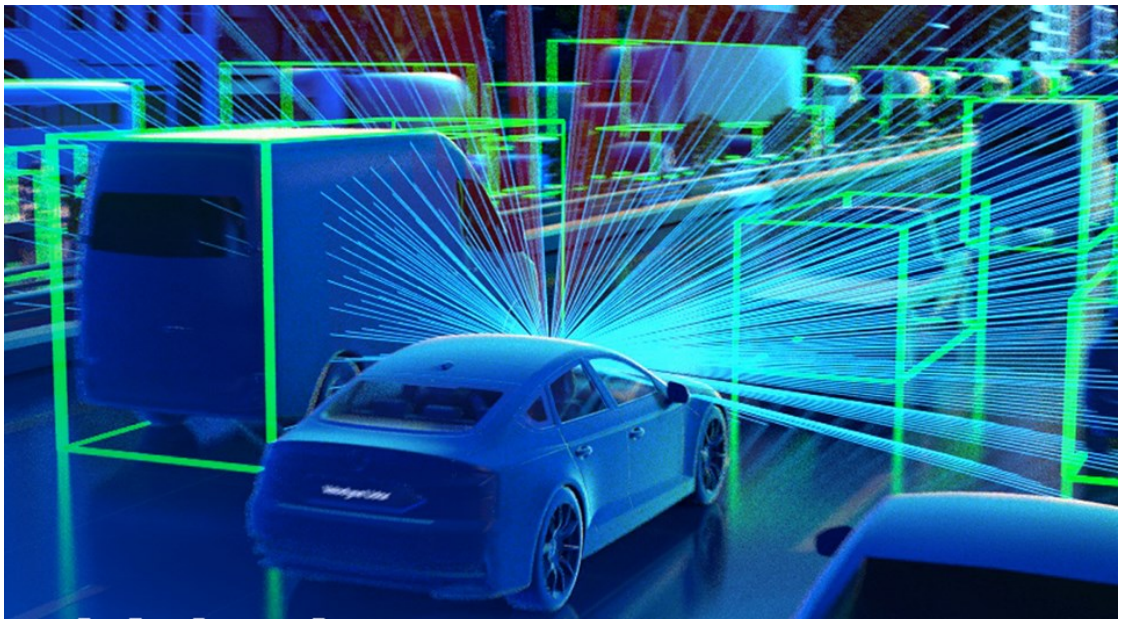


10. ábra Radar szenzorok elhelyezkedése a járművekben [240]

A radaroknak 3 nagy típusát különböztetjük meg: a nagy távolságú, a kis távolságú és a jármű környezetét feltérképező radart. Nagy előnyük a nagy hatótávolság, akár 250-500 méterre is „ellát”, valamint az időjárási tényezők nem befolyásolják működésüket.[129][297] A radarok hátránya a rádióhullám interferencia hatása, ami miatt nagy forgalomban egymást is zavarhatják az érzékelők.[200][233] Az interferencia kiküszöbölésére folyamatban van a digitális radarok fejlesztése.

LIDAR - Light Detection And Ranging

A LIDAR az emberi szemre nem ártalmas lézersugarak segítségével 3 dimenzióban „látja” a környezetét. „*A LiDAR-szenzorok pontos, nagy felbontású, valós idejű 3D ábrázolást nyújtanak a jármű környezetéről, lehetővé téve a hosszú távú méréseket szinte minden fényviszony mellett, ami vonzóvá teszi őket autonóm alkalmazásokhoz*.”.[200][272] Tipikus esetben a LIDAR érzékelő impulzusos fényhullámokat bocsált ki a körülötte levő környezetbe. Ezek a kibocsátott impulzusok visszaverődnek a környező tárgyakról és visszatérnek a szenzorhoz. Az érzékelő a visszatérő impulzusok idejéből és a nagyságából számolja ki az egyes tárgyak távolságát. Ezt a folyamatot másodpercenként milliószor megismételve a környezetről precíz, valós idejű 3D-s térkép jön létre. Ezt a 3D térképet pontfelhőnek is nevezik.



11. ábra Lidar szenzor által érzékelt környezet [324]

A LIDAR technológia alkalmazásával pontos, részletes környezeti kép alakítható ki, nagy távú feltérképezést tesz lehetővé (200-300 m), a domborzati viszonyokat pontosan képes felmérni. A kamerákkal ellentétben drágább technológia, autóipari vélemények szerint rontja a jármű összképét, emellett színeket nem megfelelően érzékel. Hátránya, hogy kedvezőtlen időjárási körülmények között nem jól alkalmazható, az interferencia ennél a technológiánál is megjelenik, a mérete kötött, nem csökkenthető az alkalmazhatóság csökkenése nélkül. Emellett a súly, energiafogyasztás és költséghatékonysági szempontokat is figyelembe véve egyes gyártók nem is alkalmazzák.[55][200][273]

Kamera

A fejlett vezetéstámogató rendszerek és az önvezetővé váló járművek egyik legfontosabb érzékelői a kamerák, amely részletes információt adnak a környezetről, helyéről, az objektumok színéről, formájáról. Olyan támogató funkciók alapulnak kamerás rendszereken, mint a:

- sávtartás,
- objektum detektálás és klasszifikálás,
- jelzőtábla és jelzőlámpa felismerés,
- parkolás,
- éjszakai vezetés.

Kamerák hátrányaként meg kell említeni, hogy a fényviszonyokra és a szennyeződésekre érzékenyek, jelentős számítási kapacitást igényel az adatok feldolgozása, valamint a távolság mérés, mélység érzékelése mono kamerával kevéssé megbízható.

Infravörös szenzorok

A járművek közlekedésében elsődleges szempont a pontosság, hogy a járművek helyzete a környezetükben való elhelyezése nagy pontossággal történhessen meg. Ezt szoftveres megoldásokkal, a különböző érzékelők által gyűjtött információk, azok kombinációja alapján, akár kedvezőtlen időjárási körülmények között. Az egyik ilyen általában más szenzorokkal kombinált autóipari megoldás az infravörös szenzor, ami rossz időjárási körülmények között, sötétben teszi lehetővé a jármű fényszóróján túli környezet érzékelést. Az úgynevezett Night Vision Devices NVD – éjjellátó eszközök) lehetővé teszik a jármű által érzékelt kép továbbfejlesztését, az infravörös képalkotást és az aktív megvilágítást. Először a gyalogosok védelme érdekében alkalmazott technológia segíti az önvezető járművek biztonságos közlekedését is.[26][56][223]

Szenzorinformációk gyűjtése, feldolgozása

Az automatizált rendszerektől nagyságrendekkel magasabb biztonsági szintet várunk el, ennek teljesítésére a szenzorok fúziója jelent megoldást. Szenzorfúzió esetén minden térrészt egy időben több szenzor is megfigyel és kiértékel, ami biztosítja:

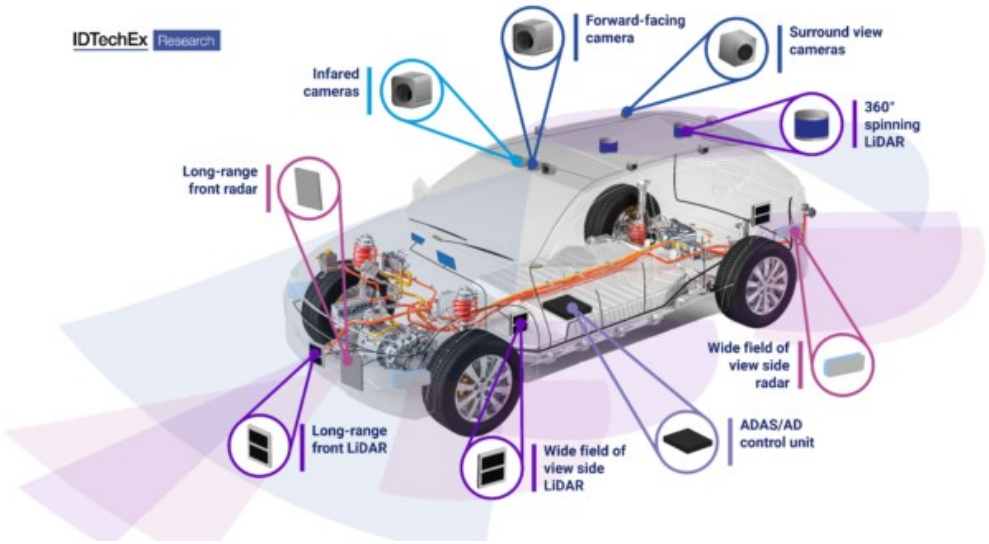
- redundanciát (meleg tartalék),
- konfidenciát (nagyobb hatótávolság, objektum jellemzők),
- egymás hátrányos tulajdonságait is kiküszöbölhetik.[105]

Fontos megjegyezni, hogy a jármű által gyűjtött információkat a jövőben nem csupán maga a jármű használja fel például a mozgásának tervezéséhez, az önvezetéshez a többi jármű, a környezeti és pályaelemekből származó információk megosztásra kerülnek egymással és különböző gyártói és szolgáltatói felhő alapú rendszerekkel. Ez elősegíti az operatív közlekedés javítását, fejleszti a különféle navigációhoz használt térképek pontosságát, részletezettségét.[56][204]

Az érzékelők által rögzített forgalmi információkat a szenzorok gyűjtik, ezáltal a jármű figyelemmel kíséri a környezetet, annak változásait, állapotát. A másodpercenként akár több gigabájt adat szűretlen feldolgozása, tárolása és elemzése költség- és időigényes feladat, emellett a járműnek el kell tudnia dönteni, hogy ezen adatok közül melyik mennyire fontos egy adott időpillanatban (például a járdán a jármű irányába haladó gyalogos esetén). Vagyis ilyen

helyzetben például figyelembe kell venni a gyalogosok és a jármű helyzetét, a köztük lévő távolságot, a mozgások irányát és sebességét, stb.

A szenzorokkal történő környezet érzékelés egyik következő fázisában várhatóan integrálásra kerülnek a különböző érzékelők adatai. Egyrészt az adatok szűrése, másrészt az érzékelők „közös nyelvének" kialakítása érdekében, hogy a mesterséges intelligenciával történő feldolgozást elősegítsék. „*A vezető nélküli járművekben a biztonságot tehát csak a három érzékelő-rendszer párhuzamos használata biztosítja, csupán önállóan egyik megoldás sem állja meg a helyét minden esetben.*"[57] Az információk értékelése, hasznosítása során figyelembe kell venni például ezek hozzáférhetőségét, időszerűségét (például a késleltetés mértéke), pontosságát, megbízhatóságát, „felhasználási" hatékonyságát is.[77] Ezen szempontok nem csupán a jármű helyváltoztatásához szükségesek, hanem a szakértői vizsgálatok során is elsődlegesek. Annak érdekében, hogy minőségi információhoz juthassunk egy vizsgálat során nélkülözhetetlen az információ forrástól való közvetítése/eljuttatása a feldolgozási helyre.



12. ábra Járművek érzékelőhálózatának főbb elemei [31]

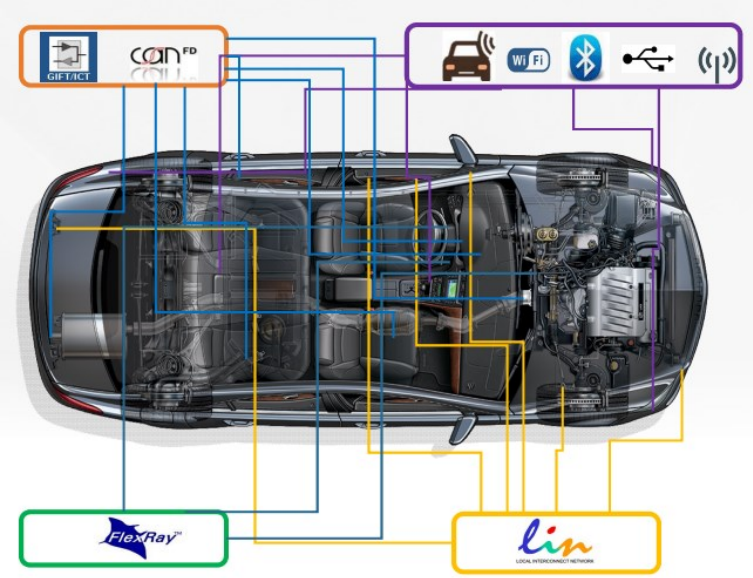
Az önvezető járművektől leginkább várt eredmény a közlekedésbiztonság javítása, a technológia fő ígérete a biztonság, melynek alapja az érzékelőkből szerzett információ. A balesetek bekövetkezésének nagy része még ma is emberi hibára vezethető vissza. Akár figyelmetlenség, rossz döntés, helytelen reakció vagy fáradtság miatt. Az önvezető technológia, a magas automatizáltságú rendszerek ezen kockázatoknak csökkentésében kapnak nagy szerepet, melynek alapja a szenzorok által gyűjtött információ, azok gyors feldolgozása és elemzése. Ebben a mesterséges intelligencia alkalmazása fontos szereplő lesz, ami elősegíti a

gyorsabban és pontosabban értékelését a forgalmi szituációknak, az emberi képességekkel és reakcióidőkkel összehasonlítva sokkal jobban.[52][58][210][212][231][235][296]

Modern járművek kommunikációs megoldásai

Az autóipar, az alkalmazott megoldások, technológiák, rendszerek folyamatos fejlődésen mennek keresztül. Ami tegnap még modernnek számított, az mára már elavult. A gépjárművek fedélzeti rendszereinél, a különböző elektronikai egységek kommunikációja decentralizált architektúra alkalmazásával valósul meg, különböző fizikai kábelezési megoldásokat alkalmazva. Az egyes egységek (csomópontok) egy nagy közös buszra kerülnek felfűzésre. Ez a megoldás speciális protokollok alkalmazását igényli, ilyen például a CAN, a LIN, a FlexRay, A2B, Ethernet, stb.[69][211]

A modern közlekedésben alkalmazott legfontosabb távközlési és adatátviteli technikák (jellemzően V2X -Vehicle to Everything) „*fontos alkalmazási terület a járművek közötti (Vehicle-to-Vehicle: V2V) és a járműinfrastruktúra-hálózatok (Vehicle-to-Infrastructure: V2I). Ezek segítségével a járművek kicserélhetik egymás menetdinamikai változóit (pozíció, sebességvektor, gyorsulásvektor, szögsebességek stb.), valamint távolról elérhetik az infrastruktúra jelzéseit és állapotát. Ennek segítségével a szenzoradatok megbízhatóságát képesek növelni, illetve akár új eszközöket adhatnak a hatóságok kezébe a közlekedésirányítás vagy a szabályok betartatása területén.*”.[128] A járműgyártás kezdetén a járművek a kézjelek, fényszórók, féklámpa, irányjelzők, vagy a duda, kürt hangjával kommunikáltak, napjainkra a mobil kommunikáció fejlődésével a járművek kommunikációja is új szintre lépett. A 4. és 5. generációs mobilhálózatok, a V2X kommunikáció által nagy mennyiségű adat osztható meg rendkívül nagy adatsebesség mellett.[6]



13. ábra Járművek belső hálózata, alkalmazott protokollok [231]

Az 1990-es években olyan járművek álltak forgalomba, amelyek elosztott hálózattal rendelkeztek. Ez a megoldás azt eredményezte, hogy több kis hálózat létezett egymás mellett, ami növelte a komplexitást, az új rendszerek, eszközök implementálására nem adott nagy mozgásteret, minimális rugalmasságot biztosított. Ezen járművek és egységeik is olyan főbb kommunikációs szabványok szerinti kommunikációt alkalmaztak, mint a CAN, LIN stb.

CAN, CAN-FD, CAN-XL

„*A modern járműarchitektúrákban – ahol az elektronikus vezérlő egység (ECU) ezredmásodpercek alatt dolgoz fel adatokat – fontos a hálózatok magas szintű stabilitása. Ennek gerincét a CAN (Controller Area Network) hálózati rendszer adja*.”.[51] A járműgyártásban, a kommunikációra vonatkozó fejlesztések iránti igény már nagyon korán megjelent. Az egyik első kommunikációs megoldást a CAN protokollt a Robert Bosch GmbH fejlesztette ki 1983-ban, amelyet 1986-ban mutattak be Detroitban. Az általános elterjedéséig a 2000-es évek elejéig kellett várni. Ez az üzenet alapú, soros kommunikációs protokoll nagy átviteli sebességgel és hibatűrő képességgel rendelkezik, képes több csomópontot is támogatni.

A CAN fejlődésének főbb mérföldkövei:

- 1986: Bosch megtervezi a CAN protokollt
- 1991: Bosch publikálja a CAN 2.0 (CAN 2.0A: 11 bit, 2.0B: 29 bit) protokollt
- 1993: CAN nemzetközi szabvány lesz (ISO 11898)
- 2003: ISO 11898 szabványsorozat

- 2012: Bosch kiadja a CAN FD 1.0-t
- 2015: A CAN FD protokoll szabványosításra kerül (ISO 11898-1)
- 2016: 5 Mbit/s definiál a ISO 11898-2 szabvány
- 2018: A CAN in Automation (CiA) a CAN nemzetközi felhasználói és gyártói csoportja fejleszteni kezdi a CAN XL szabványt
- 2024: A CAN XL szabvány szabványosításra kerül (ISO 11898-1:2024, 11898-2:2024).[51][63][64][295]

Tekintettel arra, hogy ez a protokoll egyre több felhasználási területen terjedt el, a szabványosítása a mai napig tart. Az ISO 11898 szabvány sorozat a CAN soros kommunikációs protokollt írja le, melyhez számos kiegészítés, módosítás jelent meg az elmúlt években:

- ISO 11898-1: CAN adatkapcsolati rétegét definiálja
- ISO 11898-2: CAN nagysebességű fizikai rétegét adja meg
- ISO 11898-3: CAN kissebességű fizikai rétegét adja meg
- ISO 11898-4: meghatározza az idővezérelt kommunikációt a CAN-ben (TTCAN). Ez alkalmazható a CAN-nel felszerelt közúti járművek elektronikus vezérlőegységei (ECU) közötti idővezérelt digitális információcsere létrehozására és meghatározza a keretszinkronizáló egységet.
- ISO 16845-1: meghatározza az ISO 11898-1-ben megadott CAN-nek való megfelelés ellenőrzéséhez szükséges módszertant és absztrakt tesztcsomagot bármely CAN-megvalósítás esetében.
- ISO 16845-2: teszteseteket és tesztkövetelményeket határoz meg egy olyan teszterv megvalósításához, amely ellenőrzi, hogy a CAN adó-vevő megfelel-e a meghatározott funkcióknak.[62][156][157][158][159][160][161][251]

LIN

A LIN buszt azért fejlesztették ki, hogy a járművekben használt hálózatokhoz létezzen egy olcsó, kis teljesítményű, szabványosított busz, a multiplexelt kommunikációhoz. Bár a CAN (Controller Area Network) busz megfelel a nagy sávszélességű, fejlett hálózatok iránti igénynek, a CAN megvalósításának hardver- és szoftverköltségei megfizethetetlenné váltak az alacsonyabb teljesítményű eszközök, például a motoros ablak- és ülésvezérlők számára. A LIN költséghatékony kommunikációt biztosít olyan helyeken, ahol nincs szükség a CAN sávszélességére és sokoldalúságára. A LIN költséghatékonyan megvalósítható a legtöbb

modern, olcsó 8 bites mikrokontrollerbe beágyazott szabványos soros univerzális aszinkron vevő/adó segítségével.[69][196][251]

FlexRay

A FlexRay kommunikációs busz egy determinisztikus, hibatűrő és nagysebességű buszrendszer, amelyet az autógyártókkal és vezető beszállítókkal közösen került kifejlesztésre. A FlexRay biztosítja az x-by-wire alkalmazások (pl.: drive-by-wire, steer-by-wire, brake-by-wire stb.) hibatűrési és idődeterminációs teljesítménykövetelményeit.

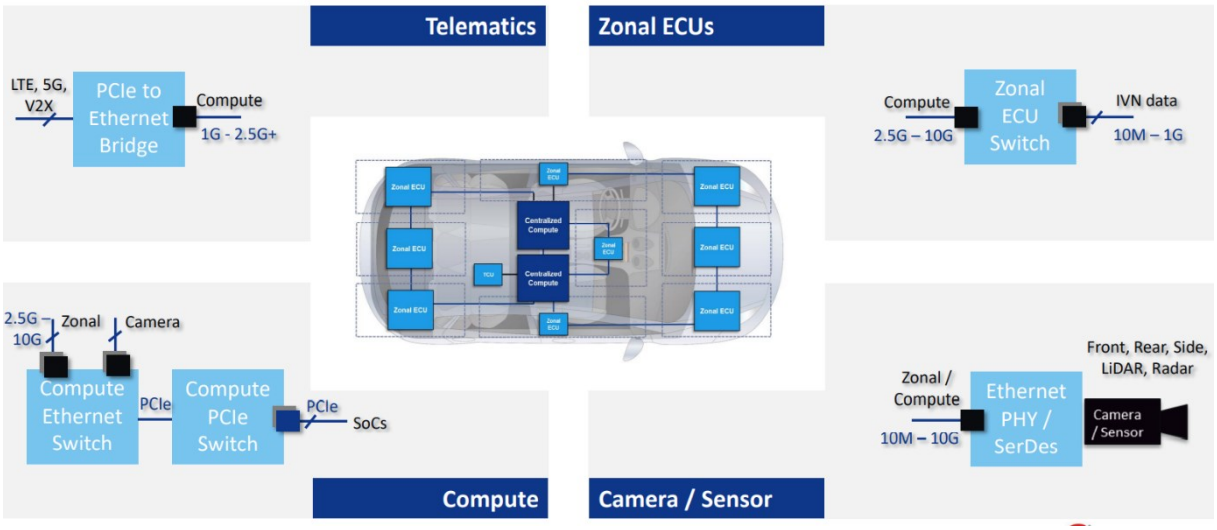
Ahhoz, hogy az járművekben növelhető legyen a biztonság és a teljesítmény, csökkenthető a környezeti terhelés és fokozható legyen a kényelem, az elektronikus vezérlőegységek (ECU) közötti kommunikáció sebességének, az adatátvitel mennyiségének és megbízhatóságának növekednie kell. A fejlett vezérlő- és biztonsági rendszerek - amelyek több érzékelőt, aktuátort és elektronikus vezérlőegységet egyesítenek - megkövetelik a szinkronizációt és a magas teljesítményt. Ez az igény már meghaladja a CAN (Controller Area Network) által biztosított lehetőségeket. A növekvő sávszélesség igény mellett, mivel a mai fejlett járművekben több CAN-buszt is használnak, egy következő generációs, beágyazott hálózat kifejlesztése kezdődött meg. A gyártókkal, az eszközök beszállítóival és a végfelhasználókkal való együttműködés eredményeként a FlexRay szabvány olyan járműfedélzeti kommunikációs buszként jelent meg, amely megfelel ezeknek az új kihívásoknak melyek a modern és önvezető járművek támasztanak.

Bár a FlexRay megoldja a jelenlegi csúcskategóriás és a jövőbeni általános járműhálózati kihívásokat, nem helyettesíti a másik két domináns járműfedélzeti szabványt. Sem a CAN-t sem a LIN-t, a költségek optimalizálása és az átmeneti kihívások csökkentése érdekében az autók következő generációja tartalmazni fogja a FlexRayt a csúcskategóriás alkalmazásokhoz, a CAN-t a főáramú hajtáslánc kommunikációjához és a LIN-t az alacsony költségű karosszériaelektronikához.[119][224][251]

Automotive Ethernet

Az Ethernet technológia egy hosszú és sikeres múltra tekint vissza az informatikában. Az 1973-ban feltalált és 1985-ben az Institute of Electrical and Electronics Engineers (IEEE) által szabványosított technológiát a mai napig széleskörűen alkalmazzák. Sokoldalú és rugalmas szabványnak bizonyult, amely évtizedeken keresztül a kommunikáció fejlődését segítette elő. Az Ethernet különböző változatai koaxiális kábelen, optikai szálakon és árnyékolatlan sodrott páros vezetékeken működnek, az átviteli sebesség 10 Mbit/s-ról az évek során több mint 100

Gbit/s-ra növekedett. Az autóipari által kialakított hálózatokban egyre több informatikai erőforrást kapcsoltak össze, az Ethernet járművekben való megjelenése és térnyerése elkerülhetetlen volt. 2016-ban az IEEE közzétette az első Automotive Ethernet szabványt, az IEEE 802.3bw-t vagyis a 100Base-T1-et. A kommunikáció árnyékolatlan, csavart páros vezetékeken történik az elektromágneses interferencia és áthallás (cross-talk) védelem érdekében. Az Automotive Ethernet technológia egy vezetékpárt használ, melyen az átvitt jelek megegyeznek, de a rajtuk eső feszültség ellentétes előjelű. Az IEEE 802.3bw szabvány 100 Mbit/s sebességgel számos autóipari alkalmazást, megoldást képes támogatni. A nagyfelbontású videó információk és a különböző szenzorokból származó adatok átviteléhez azonban ennél is nagyobb sebességre lesz szükség. A 802.3bp vagyis a 1000Base-T1 szabvány szerinti kommunikáció a járművekben is gigabites átviteli sebességet tesz lehetővé, árnyékolt vagy árnyékolatlan sodrott érpárú vezetékeken. 2020-ban az IEEE létrehozta a 802.3ch szabványt, amely több gigabites (2,5 Gbit, 5 Gbit és 10 Gbit) átviteli sebességet biztosít. 2023-ban került kiadásra az IEEE 802.3cy szabvány, amely által 25 Gbit/s-os sebesség is elérhetővé válik, amely a telematikai rendszer és a központi egységek információellátását, az egyes zónák ECU-it és az érzékelők információinak átvitelét képes biztosítani.[142]



14. ábra Jármű zónák és ECU-k nagy sebességű kommunikációi [212]

Az Ethernet egyik legnagyobb előnye a könnyű átkonfigurálhatóság, illetve az adatjelekkel együtt továbbítható áramellátás, a "Power over Data Lines" (PoDL) funkció. Ezáltal elérhetővé válik, hogy az egyes szenzorok egyetlen vezetékpárral kerüljenek összekötésre, mind az

adatokat mind az áramellátást biztosítva, csökkentve ezzel a súlyt és egyszerűsítve a hálózati architektúrát.[251]

MOST

Ahogy az autók egyre kifinomultabb konzum elektronikai platformokká fejlődnek, egyre nagyobb az igény a megbízható és egyszerű megoldások iránt az audio-, video- és adatkommunikáció kiszolgálására. A MOST (Media-Oriented Systems Transport) technológia a nagy sávszélességű autós multimédia-hálózatok de facto szabványa. Az eszközök optikai vagy fém kábeleken keresztüli, közvetlenül egymáshoz vagy hálózati konfigurációban történő csatlakoztatására használható. Szinkron hálózatként a MOST technológia kiváló szolgáltatásminőséget (QoS) és zökkenőmentes csatlakozást biztosít az audio/video streaminghez.[110][251]

A2B – Analog Devices' Automotive Audio Bus

Az autóipari tervezéskor kényes egyensúly uralkodik az eltávolított és hozzáadott funkciók tekintetében. Egyrészről a jármű súlyát, a rendszerek bonyolultságát és a többletköltségeket kell csökkenteni, ugyanakkor az autógyártók és vásárlók oldaláról is növekedő elvárás az autók funkciókban gazdag felszereltsége és a kiváló minőségű szórakoztató rendszerek alkalmazása. A hangfelismeréstől kezdve, az autón belüli kommunikáción és az aktív zajszűrésen át, a felhasználói élmény egyre inkább előtérbe kerül a járművek tervezésekor. Annak érdekében, hogy ez a kihívás megvalósítható legyen, a korábbi analóg eszközök (Analog Devices - ADI) alkalmazása helyett, kifejlesztésre került az A2B, a digitális audio busz. Ez a digitális technológia magas hangminőséget biztosít a járművek és vezetőik számára, emellett további pozitívum, hogy a költséges, nagy mennyiségben szükséges, nehéz kábelek kiváltásra is alkalmas. Mára az A2B adó-vevők képesek a hang- és vezérlő adatokat, az órajellel és az áramellátással együtt, egyetlen, kedvező áron elérhető, árnyékolatlan csavart érpárú (UTP) kábelen keresztül átvinni.[251]

V2X kommunikáció

A járművek közötti és a járművek és egyéb közlekedési résztvevők közötti kommunikáció megoldásaként a V2X, vagyis a Vehicle-to-Everything technológia jelent meg és terjedt el (elnevezésben használatos még a C-V2X, vagyis Cellular V2X, a mobilkommunikációs háttérre utalva). Lehetővé teszi a közvetlen adatcserét a jármű és környezete között. Ezáltal vizuális kapcsolat nélkül is információt kapnak egymás pozíciójával, mozgásával és egyéb a közlekedéssel és biztonsággal kapcsolatosan (pl.: vészhelyzeti események), közvetlenül a

közelben lévő másik féltől, vagy valamilyen gyártói/szolgáltatói felhőn keresztül, vagy a kettő valamilyen kombinációjaként.

A V2X technológiában rejlő potenciál akkor érvényesülhet, ha a közlekedési résztvevők jelentős része képessé válik a technológia alkalmazására. „A bevezetés korai szakaszában ezért kulcsfontosságúak lesznek az azonnal érzékelhető előnyök. Ilyen például a V2X-alapú prioritásos forgalomirányítás, amely elsőbbséget biztosíthat a közösségi közlekedésnek, a mentőjárműveknek és a kerékpárosoknak”.[59]

„*V2X – jármű- és minden lehetséges dolog közötti együttműködés, kommunikáció lehetővé teszi, hogy összekapcsolja az összes járműtípust és a különféle infrastrukturális rendszereket. Ez a kapcsolat magában foglalja az autókat, az autópályákat, a hajókat, a vonatokat, a repülőgépeket, valamint a gyalogosokat stb. is, ezáltal megvalósítva a teljes körű kooperativitást a közlekedésben*”.[304]

A V2X kommunikáció lehetővé teszi a járművek kommunikációját a közlekedés szereplőivel és a közlekedés megvalósulásához szükséges infrastruktúrával egyaránt, optimalizált és biztonságosabb közlekedést eredményezve. A jármű kommunikációs rendszerek által hozzáférhetővé vált információk a vezetőt a vezetés során folyamatosan segítik. A V2X funkcióját tekintve szélesebb körű szolgáltatásokat, információkat nyújt, mint a mobiltelefonos navigáció, a közeledési információkkal ellátott applikációk (pl.: Waze). A V2X milliszekundumos frissítési időt biztosít, ezáltal alkalmassá tehető veszélyes szituációk vagy ütközés elkerülésben való közreműködésben. „*A V2X egyik alapköve a Cooperative Awareness Message, röviden CAM. Ezek szabványosított adatcsomagok, amelyeket a járművek és infrastruktúraelemek másodpercenként akár többször is cserélhetik. A CAM tartalmazza a pozíciót, a sebességet, a haladási irányt, a jármű típusát, méreteit és még a világítás állapotát is.*”.[59]

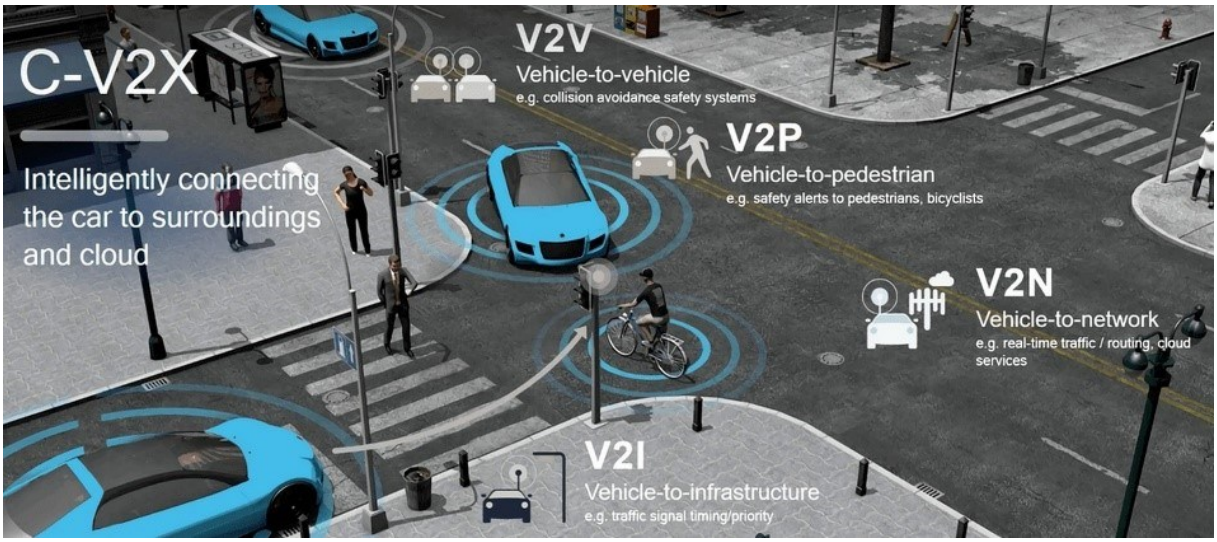
A mobil applikációs vezetéssegítő alkalmazások nem alkalmasak ilyen funkciók megvalósítására. A járműkommunikációs megoldás egyik fő célkitűzése a balesetek, a közúti halálesetek visszaszorításának elősegítése, melyhez nem feltétlenül követelmény az információk nagy távolságokra való eljuttatása. A közvetlen, viszonylag kis hatótávolságú, elosztott kommunikációsegítségével hatékonyan megvalósíthatóvá válnak egyes biztonsági alkalmazások.

V2X szolgáltatásokat a biztonságra való törekvés elve mellett, a takarékosság elve hangsúlyos. Alkalmazásával megvalósíthatóak a járműkonvojok vezérlése, ahol a szenzorok segítésével menetoszlopban, egymáshoz nagyon közel tudnak haladni a járművek.

Az okos városok által kitűzött célok egy része a V2X kommunikáció segítségével gyakorlatban is megvalósíthatóvá válik, azaz valós-idejű forgalmi információkkal csökkenthetőek, elkerülhetőek lesznek a közlekedési torlódások, dugók, mellyel hozzájárul a káros anyag kibocsátás csökkentéséhez.

A V2X technológia alapköve lehet az autonóm járművek forgalomban való biztonságos közlekedésének. A V2X segítségével több információ biztosítható az autonóm járművek számára, mint ha csak saját szenzorai által gyűjtött információkra támaszkodna. A gyors kommunikáció elősegíti a megalapozott döntéshozatalt.

A V2X megoldás nem tökéletes rendszer, számos probléma és kérdéskör felmerül az alkalmazásával kapcsolatban, ami a közeljövő folyamatos fejlesztései által kerülnek kijavításra, megoldásra. Ilyen probléma lehet az autópályákon egymással szemben haladó járművek nagy sebesség különbsége, ami akár 200-300 km/h is lehet. Ebből eredően a topológia is gyorsan változik. Az egymással szemben haladó járművek nagyon rövid ideig vannak egymás „hatótávolságában”, az interakcióra rövid időablak áll rendelkezésre, az üzenetek továbbításának ebben az időszakban kell(ene) megtörténnie. Másik probléma a gyakorlati alkalmazásnál az egyidőben nagyszámú kommunikációs eszköz jelenléte. A kommunikációs közeg túlterhelése is előfordulhat, például egy közlekedési dugóban állva. Az ilyen és ehhez hasonló kihívásokat tartalmazó komplex igényrendszert kell tudnia kezelni a kooperatív intelligens közlekedési rendszerek architektúráinak és a megvalósítandó járműkommunikációs szolgáltatási rendszereknek.[139][261][286][304][320][321]



15. ábra V2X kommunikáció a környező járművek és a közlekedés egyéb résztvevői között [322]

V2V együttműködés, kommunikáció

„*V2V – jármű-jármű közötti együttműködés, kommunikáció a járművek bizonyos csoportjára vonatkozó sebességek, pozíció információk vezeték nélküli kommunikáció útján történő megosztása azzal a céllal, hogy a balestek és forgalmi torlódások elkerülhetőek legyenek. A cél megvalósítása pozitív hatással van az élőkörnyezetre.*”. [80][234][304]

V2I együttműködés, kommunikáció

„V2I – jármű-infrastruktúra közötti együttműködés, kommunikáció, amelynek során a jármű által - közlekedés közben - gyűjtött adatok kerülnek továbbításra a közlekedési infrastruktúra felé, beleértve a közlekedés biztonságára, a közlekedési környezetére vonatkozó információkat, valamint a mobilitás további részleteit”. [13][23][79][103][130]

V2C együttműködés, kommunikáció

„*V2C – jármű-felhő közötti együttműködés, kommunikáció olyan információcserét megvalósító technológia, amely során a jármű számára lehetővé válik, hogy más, a felhőhöz kapcsolódó rendszereket, például az energiaellátó rendszert, töltő infrastruktúrát, okos otthonokat, okos parkolókat stb. használjon, információt osszon meg és szerezzen a kapcsolódó rendszerektől működésének tökéletesítéséhez és szolgáltatásainak bővítéséhez*”. [13][23][79][103][130]

V2P együttműködés, kommunikáció

„*V2P – jármű-gyalogos közötti együttműködés, kommunikáció lehetővé teszi, hogy a közlekedési környezettel kapcsolatos információkat a járművekkel, infrastruktúrával és a*

járókelők mobileszközeivel megosztva a jármű képes legyen jelezni a gyalogos számára az adott közlekedési helyzetet, ezáltal növelve a biztonságos közlekedés esélyét.".[13][23][79][103][130]

A járművek, a közlekedés egyéb résztvevői, a környezet és pálya érzékelői (pl.: közlekedési csomópontban elhelyezett kamera) közötti kommunikáció nélkülözhetetlen eleme a megbízható, folyamatos és gyors információcserének, ami az önvezetővé váló járművek és a kooperatív közlekedés alapja. „Ehhez a világ különböző pontjain eltérő technológiát használnak". A Bosch például jelenleg is dolgozik az 5G-V2X (vehicle-to-eveything communication) rendszeren. A kommunikációs rendszerek fejlődése is folyamatos, a 4. és 5. generációs kommunikációs megoldások után, már folyamatban van a 6. generációs megoldás kidolgozása, ami a járművekbe integrált kommunikáció és szenzortámogatott, kooperatív intelligens közlekedés egyik alapja lehet.

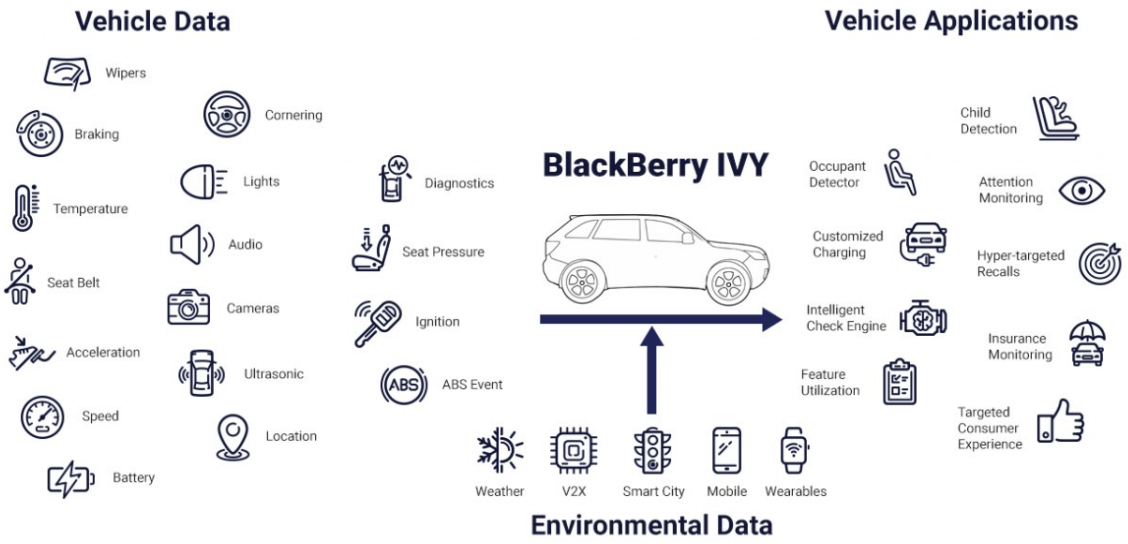
„*A vezeték nélküli spektrum, a hardver és a jelfeldolgozás megosztott használata hatékonyabbá teszi a járművekben lévő rendszereket, ráadásul jelentős költség- és energiamegtakarítást is eredményez. A két jármű közötti közvetlen kommunikációt lehetővé tevő „sidelink" fontos szerepet játszik, például azért, mert a meglévő mobilkommunikációs infrastruktúrától függetlenül is használható. Ez azt jelenti, hogy a jövőben az önvezető rendszerek olyan régiókban is működőképesek lesznek, ahol gyenge a hálózati lefedettség.*".[50]

DSRC

A DSRC - Dedicated Short Range Communications, volt az első V2X kommunikációs szabvány, amelyet az Egyesült Államok Szövetségi Kommunikációs Bizottsága (FCC) fejlesztett ki, a járművek kis hatótávú kommunikációs technológiájaként, melyet korábban széles körben alkalmaztak például Ausztria és Németország közútjain. A DSRC WiFi-szabványon alapuló (IEEE 802.11p) kommunikációs megoldás, amelyet szabványos Wi-Fi-ből fejlesztettek, kifejezetten autóipari és közlekedési alkalmazásokhoz. A technológia a megbízható és hatékony kommunikáció érdekében került kialakításra, a közlekedési rendszerekben történő alkalmazáshoz. Például elektronikus út- és parkolódíj beszedés, korlátozott területekre történő behajtás ellenőrzése, járművek vészjelző rendszeréhez, megkülönböztetett jelzést használó járművek elsőbbségének jelzésére, közúti akadályokra és vasúti átjáróra figyelmeztetés, stb. érdekében. Nagy megbízhatóság, gyors adatkapcsolat és alacsony késleltetési idő jellemzi az 5,8 GHz-es frekvenciasávban működő megoldást.[91][93]

A V2X és DSRC megoldások alapvetően ugyanazt a célt szolgálják: javítani a közúti biztonságot és az utazás hatékonyságát gyors és biztonságos adatkommunikációval, alacsony késleltetést biztosítani, 5,9 GHz-es frekvenciasávot felhasználva, rövid hatótávolságú adatküldéssel. A két megoldás nem átjárható, a gyártók jellemzően a V2X használatát preferálják. A DSRC dedikált és szabványosított megoldást nyújt, alacsony késleltetéssel, azonban további infrastruktúra kiépítését igényli, míg a V2X a már meglévő mobilkommunikációs hálózatokat is képes használni, de valamivel nagyobb késleltetéssel működhet.[89][90][91]

A járművek különböző kommunikációs csatornákon keresztül olyan adatokat forgalmaznak, melyek egy része, vagy egésze a különböző vezérlő egységekben is megtalálható.[259]



16. ábra Az intelligens járművek adatai, vezérlőegységei mint adatforrások [45]

Modern járművek belső formációtárolása

A modern és az egyre inkább önvezetővé váló járművek által hozzáférhető adatok forrása lehet a jármű saját szenzorhálózata vagy a hatósugáron belül észlelhető V2X kommunikációs egyéb jármű, infrastruktúra, gyalogos stb. adatai, a különböző felhőalapú rendszerek (pl. gyártói és szolgáltatói cloud), a digitális iker, műholdas kommunikációs rendszerek, a közúthálózat üzemeltetői informatikai rendszere stb.

A járművekhez kapcsolódóan a digitális iker fejlesztése a járművekhez tartozó fejlesztési és üzemeltetési adatok virtuális adatbankja. Különböző gyártók a fejlesztéshez, minőségi követelménynek növeléséhez folyamatosan gyűjtenek információkat a járművekből. „*A jövőben*

ez az ikerpár magában foglalja majd az autóban és a felhőben tárolt adatokat – a gyártásától a leselejtezésig. Ez messze túlmutat azon, amit a digitális iker kifejezés korábban jelentett: most először fedi le egy modern jármű teljes életciklusát, és magában foglalja a felhőtartományt, az alkalmazásokat, valamint a háttér- és a fejlesztőrendszereket.".[24] Ezáltal a járművek teljes élettartama követhető lesz, a karbantartástól, a műszaki állapotig, a sérülésekig, ami a jövő szakértői vizsgálatait is elősegítheti.[24]

A jelen kutatásban elsődlegesen a járművekben tárolt, kezelt adatok tartoztak bele, melyek a jármű különböző adattárolóiban kerülnek rögzítésre és az utólagos szakértői vizsgálatok szempontjából relevánsak lehetnek. Ilyen tárolók például:

- az Event Data Recorders (EDR), vagyis eseményadat-rögzítő,
- a Telematics/Infotainment rendszer,
- a jármű központi egysége/fejegysége,
- a fedélzeti kamera (első és hátsó vagy 360°-os) adattároló képességgel,
- a „Self-Driving and Autonomous Vehicle ECU"-k,
- az egyéb ECU-k adattároló képességgel,
- az intelligens kulcsok,
- az E-call rendszer,
- az utángyártott és járműbe épített vagy csatlakoztatott eszközök.

Az adatok járműbéli tárolása felejtő (Volatile) és nem felejtő (Non-volatile) memóriákban történik. Felejtő (Volatile) memória:

- RAM (Random Access Memory):
- Dinamikus RAM (DRAM),
- Statikus RAM (SRAM).

Nem felejtő (Non-volatile), emlyek tápfeszültség nélkül is megőrzik a beírt adatokat:

- ROM (Read-Only Memory),
- PROM (Programmable ROM),
- EPROM (Erasable Programmable ROM),
- EEPROM (Electrically Erasable Programmable ROM),
- Flash memória (pl.: eMMC 5.x, microSD és SD kártyák, SSD-k).

Utólagos szakértői vizsgálatok szempontjából utóbbi tárolócsoport lesz releváns.

17. ábra Modern járművek adattároló egységei a felejtő és nem felejtő memóriák [285]

Járművek elektronikus vezérlőegységei

A járművek elektronikus vezérlőegységei, az autók és a modern járművek egyik legfontosabb alkatrészei, ami a fent meghatározott adattárolókhoz kapcsolódik, vagy maga az ECU végzi az adatok tárolását. Feladatuk a különféle járműfunkciók irányítása és szabályozása, például a motort, a befecskendező rendszert, a fényszóró és ülésvezérlést, a klíma és több más rendszert. A mai modern járművekben közel 100 ECU található a különféle vezérlési funkciók ellátására. Az ECU adatokat gyűjt a kapcsolódó szenzorokból, majd ezek alapján hoz döntést és avatkozik be, például optimalizálja a motor működését. Egy motorvezérlő ECU „*meghatározza, hogy mennyi üzemanyagot kell befecskendezni a hengerekbe, és milyen időzítéssel, hogy a motor hatékonyan működjön, és a károsanyag-kibocsátás minimális legyen*”.[1]

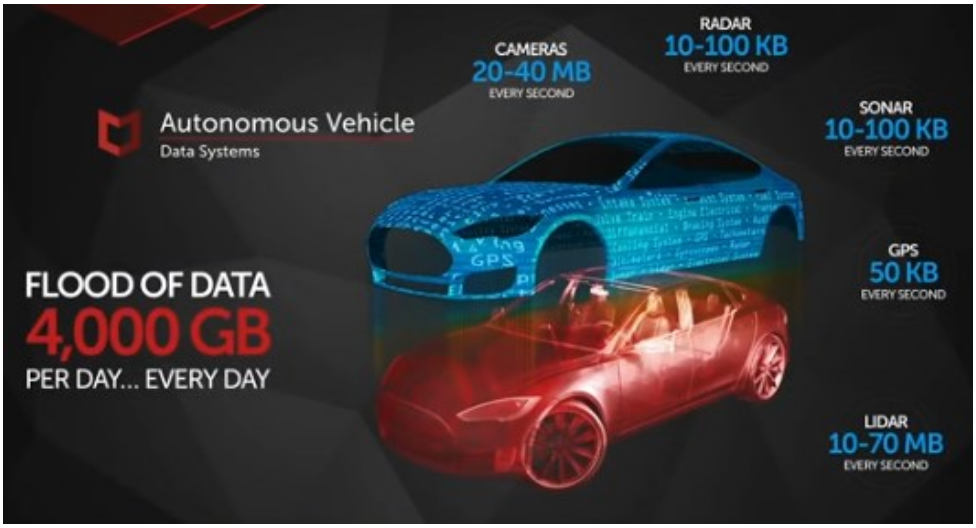
„*Az autókban található ECU-kat funkciójuk alapján általában a következő nagyobb csoportokba sorolják:*

- *powertrain systems (erőátviteli rendszerek, pl. motorvezérlő, váltóvezérlő),*
- *chassis systems (váz vagy „kaszni” rendszer, pl. fékek, sebességszenzorok),*
- *body systems (utastér-elektonika, pl. ablakemelő, világítás, központi zár),*
- *multimedia systems (multimédia rendszer, pl. autórádió, hangosítás).*
- *biztonsági rendszerek (safety, pl. légzsák, ABS),*

[1] https://dubnicz.hu/2024/08/az-ecu-szerepe-az-autoszerelesben-hogyan-javitsuk-es-diagnosztizaljuk-az-elektronikus-vezerloegyseget/

- *a védelmi rendszerek (security, pl. ugrókódos ajtónyitó, indításgátló)*
- *a vezetői információs rendszerek (driver info, pl. GPS, tolatóradar).*”.[278]

A modern járművekben megtalálhatóak SD kártya olvasására létrehozott slot-ok, vagy USB porton keresztül csatlakoztathatók adattárolók. Emellett a belső HDD, flash és SSD háttértárak biztosítják a járműben keletkező és a jármű által hozzáférhető adatok biztonságos tárolását.



18. ábra Autonóm járművekben keletkező adatmennyiség legnagyobb része a különböző szenzorokból keletkezik [166]

Az Universal Flash Storage (UFS) az autóiparban használt legújabb interfész gyors hozzáférést kínál az új alkalmazásokhoz, mint például az e-műszerfalakhoz és az AI-kompatibilis autonóm hajtásrendszerekhez.[127]

Magas automatizáltságú és önvezető közúti közlekedési járművek kiberbiztonsági kockázatai

A modern járművek vonatkozásában fentebb meghatározott elemek, kommunikációs megoldások, adatgyűjtő és feldolgozó rendszerek tekintetében, biztonsági szempontból három kulcsfontosságú rendszerelem azonosítható be:

- gépjárművezérlő rendszerek (ECU-k),
- autonóm vezetési rendszerelemek (szenzorok, Global Positioning System, GPS - Global Positioning System, vezérlés, szabályozás, vezetési funkciók),
- kommunikációs technológia (V2X).

A járművek kommunikációs hálózatainak és az elektronikus vezérlő egységeinek számos sebezhetőségét tárták fel és dokumentálták az elmúlt időszakban. A magas automatizáltságú, hálózatba kapcsolt járművek egyre inkább a rosszindulatú támadók figyelmébe fognak kerülni, a mesterséges intelligencia támogatott sebezhetőség felderítés pedig nagyon lerövidítheti további hiányosságok, sérülékenységek feltárását. Ezen sebezhetőségek mind a járművön belül, mind a járművek közötti, mind a járművek és egyéb közlekedési szereplők közötti kommunikáció vonatkozásában kockázatot jelentenek.

A járművek belső hálózatai számos belső sebezhetőséggel rendelkeznek, mint a broadcast üzenetek, a hitelesítés és titkosítás hiánya, az azonosítóalapú prioritási séma és az elérhető interfészek. A rosszindulatú támadásokkal szemben ezen sebezhetőségek miatt a támadók végrehajthatnak különféle támadásokat, beleértve a közbeékelődést, kommunikációs keretek lehallgatását, hamisítását, visszajátszásos támadást, a keret-befecskendezést és a szolgáltatás megtagadás támadást. Az ilyen támadások ellen szükség van a jármű hálózatainak védelmére, hogy csökkenteni lehessen a támadási vektorokat. A következő fejezetben részletezésre kerülnek azon járműbiztonsági és kiberbiztonsági vonatkozású követelmények, szabványok, melyek a modern járművekre vonatkoznak.

A járművek vezérléséhez kapcsolódóan felmerülő kockázatok egyike, a szoftversérülékenység, a fentebb már említett online frissítések (F-OTA) által lehetőség van a jármű központi szoftverének, vagy egyes vezérlőinek újraprogramozására. Emellett a helytelen protokoll-végrehajtás jelenthet kockázatot, különös tekintetben a katonai felhasználásban. „*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. 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.".[53][54][55][168][169][188][191][203]

A modern járművek másik kiberbiztonsági vonatkozású kockázatát az érzékelők és azok jeleinek kompromittálása jelenti. Ide tartozik a radar jelek hamisítása, a LIDAR jelek hamisítása, a kamera elvakítása különböző hullámhosszú fénysugarak kibocsátásával, radarzavarás, a GPS jelek zavarása vagy hamisítása. A módosított, manipulált zavarjelek hatására az egyes érzékelők nem észlelik a tárgyakat, téves információt továbbítanak, vagy nem működnek.[190]

További kockázatot jelent a járművek által forgalmazott adatok tekintetében az adatvédelmi nem megfelelősség. Olyan információk megosztása, mint a jármű és utasainak tartózkodási helye, személyazonossága, baleseti információk adatvédelmi kockázatot jelent.

Valós idejű válaszüzenetek küldése és fogadásához gyors kommunikáció szükséges, az erőforrás-igényes hitelesítési folyamatok miatt késedelmet okozhatnak. A járművek gyors haladása, a közlekedési szituációk dinamikus változása miatt a kommunikációs kapcsolatok dinamikus támogatása szükséges, a járművek közötti és egyéb résztvevők, környezeti és pályaelemek közötti hitelesített kommunikációs handover/roaming érdekében. A modern közlekedési rendszerekben az járművek által generált és forgalmazott információk feldolgozását a felhasználók és járművek hitelesítése mellett is hatékonyan kell megvalósítani. El kell kerülni, hogy egy rosszindulatú támadó lassú forgalomra, vagy balesetre vonatkozó adatokat küldhessen.[7][30]

Az egyes támadások nyomainak elemzése is a járművek szakértői vizsgálatainak témaköréhez tartozik. A támadások nyomainak felfedése, felderítése, a nyomok vizsgálata nélkülözhetetlen a járművekkel kapcsolatos események vizsgálatában.

Autóipari kiberbiztonság

Az autóipari kiberbiztonság a járművekben és a közlekedési rendszerekben kezelt információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását jelenti, a járművek, a járműveket használók, a járműhöz kapcsolódó szoftverek és szolgáltatások, eszközök, illetve hálózatok komplex környezetében. A mai modern autók számos elektronikus vezérlő egységet tartalmaznak a különböző járműfunkciók működtetésére. Az előző fejezetben összegyűjtött kockázatok csökkentése érdekében jelen fejezet célja a különböző járműipari szabványok kiberbiztonsági vonatkozása kerül azonosításra.

A modern járművek számos támadható felülettel rendelkeznek, melyeket kihasználva a járművek ellen irányuló – a kibertérből érkező – támadások száma az elmúlt években növekvő tendenciát mutatott. A járművek és járműrendszerek kibervédelmére Tokody és szerzőtársai az alábbi lépéseket határozták meg:

- a járművek közötti kommunikáció biztonságának és a járművek információs rendszereinek fizikai infrastruktúravédelmének biztosítása;
- a járműrendszerek és járművek működésbiztonságának megvalósítása annak érdekében, hogy a közlekedési folyamatok megzavarása ellen védett legyen a rendszer;
- a járművek által gyűjtött és tárolt információk védelme a továbbított adatokhoz való jogosulatlan hozzáférés, törlés és módosítás ellen;
- az informatikai és információs rendszerek védelme a fizikai fenyegetésektől, például a járművezérlő egységekhez való illetéktelen hozzáféréstől, a közlekedési rendszer, mint kritikus infrastruktúra kiberbiztonságának a megvalósítása.[304]

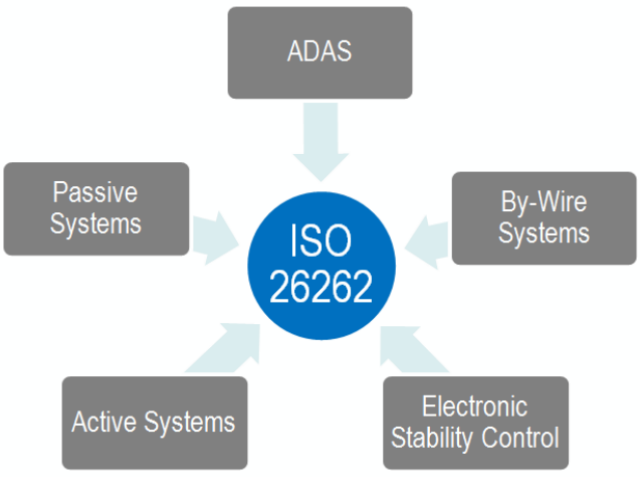
A jövő közlekedési eszközeiben már a tervezésnél kiemelt figyelmet kell fordítani a kiberbiztonság kérdéskörére annak érdekében, hogy megfelelő védelemmel lássák el a járműveket. Az autonóm járművek kiberbiztonsági szempontú tervezése új és szabványosítás alatt álló terület. A járművekhez, mint biztonságkritikus rendszerekhez a teljes életciklusukra vetített ún. ASIL- (Automotive Safety Integrity Level) értékek kerülnek meghatározásra. Az ASIL-érték autóipari biztonsági funkcionalitási képességi paraméter, az ISO 26262 számú szabványban a közúti járművek funkcionális biztonságára vonatkozóan meghatározott kockázatalapú osztályozási rendszerként vezették be. A szabvány a koncepciótól a fejlesztésen át az analitikáig biztosítja a rendszerfelépítést, az egységekre, elemekre, komponensekre bontást. A szabvány célja egységes biztonsági standard biztosítása minden autóipari elektronikus/elektronikus (E/E) rendszer számára a termékfejlesztési folyamat során. Ismerteti

az elfogadható kockázati szint hozzárendelését egy rendszerhez vagy alkatrészhez, és a teljes tesztelési folyamat dokumentálását. A szabvány:

- biztosítja az autóipari biztonsági életciklust (automotive safety lifecycle), a menedzsmentre (safety menedzsment), fejlesztésre (specifikáció, design, validáció, HW és SW fejlesztés), gyártásra és támogató folyamatokra (üzemeltetésre, szervizre, leszerelésre) kiterjedően, valamint támogatja az egyes tevékenységek testre szabását,
- autóipari-specifikus kockázatokon alapuló megközelítést biztosít a kockázati osztályok (autóipari biztonsági integritási szintek, ASIL-ok) meghatározásához,
- ASIL-eket használ a biztonsági követelmények meghatározására, az elfogadható maradványkockázat eléréséhez,
- követelményeket biztosít a validációs és jóváhagyási intézkedésekre vonatkozóan, a megfelelő és elfogadható biztonsági szint elérése érdekében.[163][333]

„*Az ISO 26262 az autóipari E/E rendszerek és alkatrészek széles skáláját szabályozza, beleértve, de nem kizárólagosan:*

- *Erőátviteli vezérlőrendszerek (pl. motorvezérlés, sebességváltó vezérlés)*
- *Alvázrendszerek (pl. fék, kormányzás, felfüggesztés)*
- *Fejlett vezetősegítő rendszerek (ADAS)*
- *Testelektronika (pl. világítás, HVAC, infotainment, ha biztonsági szempontból fontos)*
- *Akkumulátorkezelő rendszerek elektromos járművekben*
- *Érzékelő és aktuátor interfészek*
- *A funkcionális biztonságot befolyásoló szoftverek és beágyazott rendszerek.*”.[164]



19. ábra Az ISO 26262 által szabályozott autóipari E/E rendszerek és alkatrészek [333]

A megfelelés érdekében meghatározásra kerülnek az egyes funkciók és körülmények. Az egyes ASIL-osztályokat fenyegetés- és kockázatelemzéssel állapítják meg, emellett minőségi és mennyiségi biztonsági analíziseket végeznek el. A jármű minden egyes elektronikus alkatrészét három konkrét paraméter szerint osztályozzák:

- a súlyosság (a járművezető és az utasok sérülésének mértéke, módja),
- a kitettség (milyen gyakran van a jármű kitéve a veszélynek) és
- az irányíthatóság (mennyit tehet a járművezető a sérülés megelőzése érdekében) mértéke szerint.

Az osztályozás lehetővé teszi a biztonsági követelmények meghatározását oly módon, hogy a kockázatokat elfogadható szintre csökkenti. A meghatározott biztonsági követelmények biztosítják a fenyegetések, kockázatok kezelhetőségét és nyomon követhetőségét, az elkészült termékkel kapcsolatban az incidensek megelőzését vagy az azok kezelése érdekében szabványosított biztonsági eljárások bevezetését.[66][124][281][330]

Az ISO 26262 szabványcsalád világszerte széles körben elfogadott, kiterjedt biztonsági elemzési módszereket tartalmaz, amelyek figyelembe veszik a véletlenszerű hibákat. A szabvány azonban nem számol a rendszerszintű hibákkal, ideértve a szoftverhibákat. Az ASPICE (Automotive Software Process Improvement and Capability Determination) a legfrissebb nemzetközileg elfogadott, széles körben használt szabvány az autóipari szoftverek területén, amelyet az eddig kialakult „legjobb gyakorlatok” alapján hoztak létre. A BMW, a Bosch, a Continental, a Daimler, Chrysler és a Volkswagen által az 1990-es évek végén kifejlesztett közös keretrendszer feladata az autóiparban alkalmazott szoftverfejlesztési folyamatok értékelése és fejlesztése, valamint a megbízható szoftverek fejlesztésének támogatása volt. Az ASPICE első verziója (2003) az úgynevezett V-modellre, más néven a verifikációs és validációs modellre épült, amely a fejlesztés teljes életciklusát lefedi, megfelelő tesztelési fázist ír elő, biztosítva a fejlesztési folyamatok értékelését és fejlesztését. A 2005-ben megjelent második verzió bevezette az ún. PAM (Process Assessment Model) folyamatértékelési modellt, ami olyan irányelvek és kritériumok gyűjteménye, amelyek az autóipari szoftverfejlesztési folyamatok hatékonyságának és eredményességének értékelését szolgálják. Az ASPICE célja a folyamatos innováció és termékfejlesztés biztosítása a fejlesztés minden fázisban, ennek érdekében folyamatosan felülvizsgálják. A kezdeti fázisokban a V betű bal oldalának lépései tartalmazzák

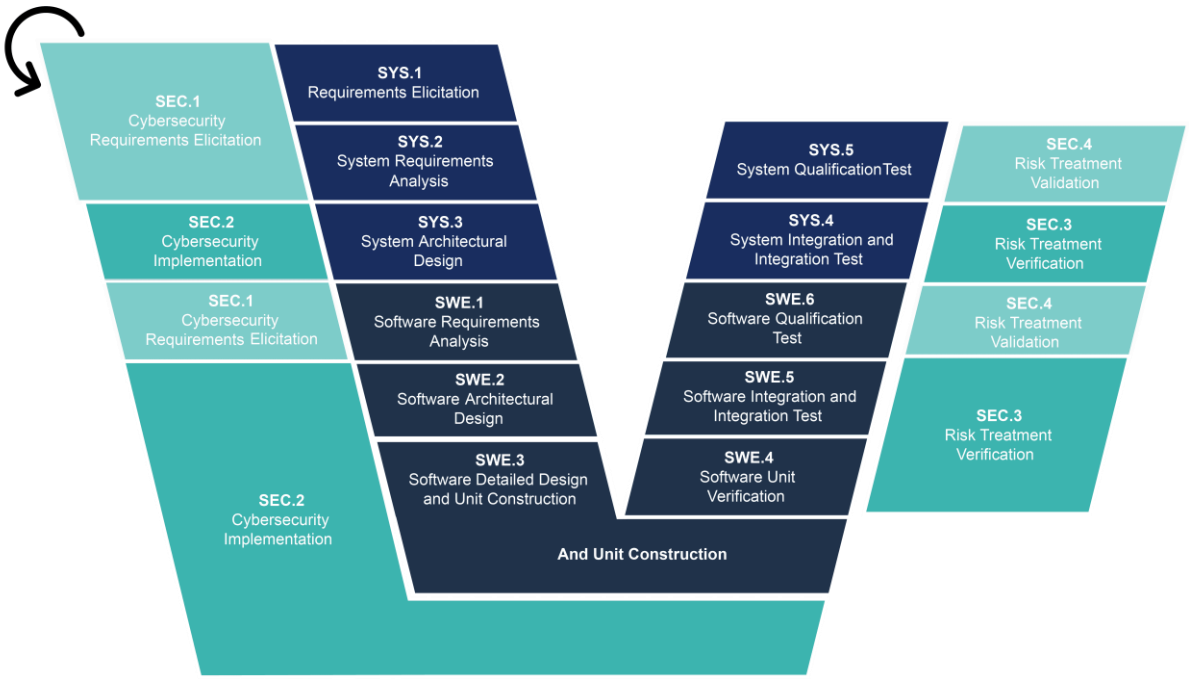
- a követelményelemzést: vagyis az ügyfél által támasztott követelmények megállapítását és rendszerezését;
- a rendszertervezést: vagyis az ügyfél és az érdekelt felek igényeinek feltérképezését, hogy azokat megvalósítható munkafolyamatba szervezzék át;
- az architektúratervezést: vagyis a követelmények logikai műveletekké szervezését, amely a hardvert, a szoftvert és a kommunikációt foglalja magában;
- a modultervezést: vagyis a rendszerkövetelményeknek megfelelő szoftverkövetelmények létrehozását és a szolgáltatási egységek fejlesztését; valamint
- a kódolást: ahol az egységek tervezése és megvalósítása történik.

A másodlagos fázisok, a V betű jobb oldalának lépései tartalmazzák:

- az egységek tesztelését: vagyis annak megállapítását, hogy a kód megfelel-e a tervnek, és hogy az alapvető szabványok és követelmények teljesültek-e;
- az integráció tesztelését: vagyis a szoftverarchitektúra értékelését és annak megállapítását, hogy a szolgáltatási egységek működőképesek-e;
- a rendszertesztelést: vagyis az összes szolgáltatás integrálását a teljes rendszerbe, valamint a funkcionalitás és a követelmények teljesítésének tesztelését; illetve
- az átvételi tesztelést: vagyis az ügyfél által végzett végső teszteket.

Mindegyik ponthoz tartozik egy-egy megfelelő tesztelési fázis, valamint további nyomonkövethetőségi és irányítási folyamatok. A szállítók ezen szabványosított teljesítési fázisok szerint szerezhetik meg az ASPICE-tanúsítványt, és értékelésük eredményeképpen az ügyfelek által figyelembe vehető konkrét ASPICE-szinteket kapnak. 2021-ben közzétételre került az ún. ASPICE CS (Automotive SPICE for Cybersecurity – Process Reference and Assessment Model), amely az ISO/SAE 21434:2021 Road Vehicles – cyber security engineering szabvány tartalmát veszi át, és meghatározza a kiberbiztonsági követelményeket a fejlesztési projektekhez. A kiberbiztonsági követelmények kiegészítik az eredeti V-modellt a következő lépésekkel:

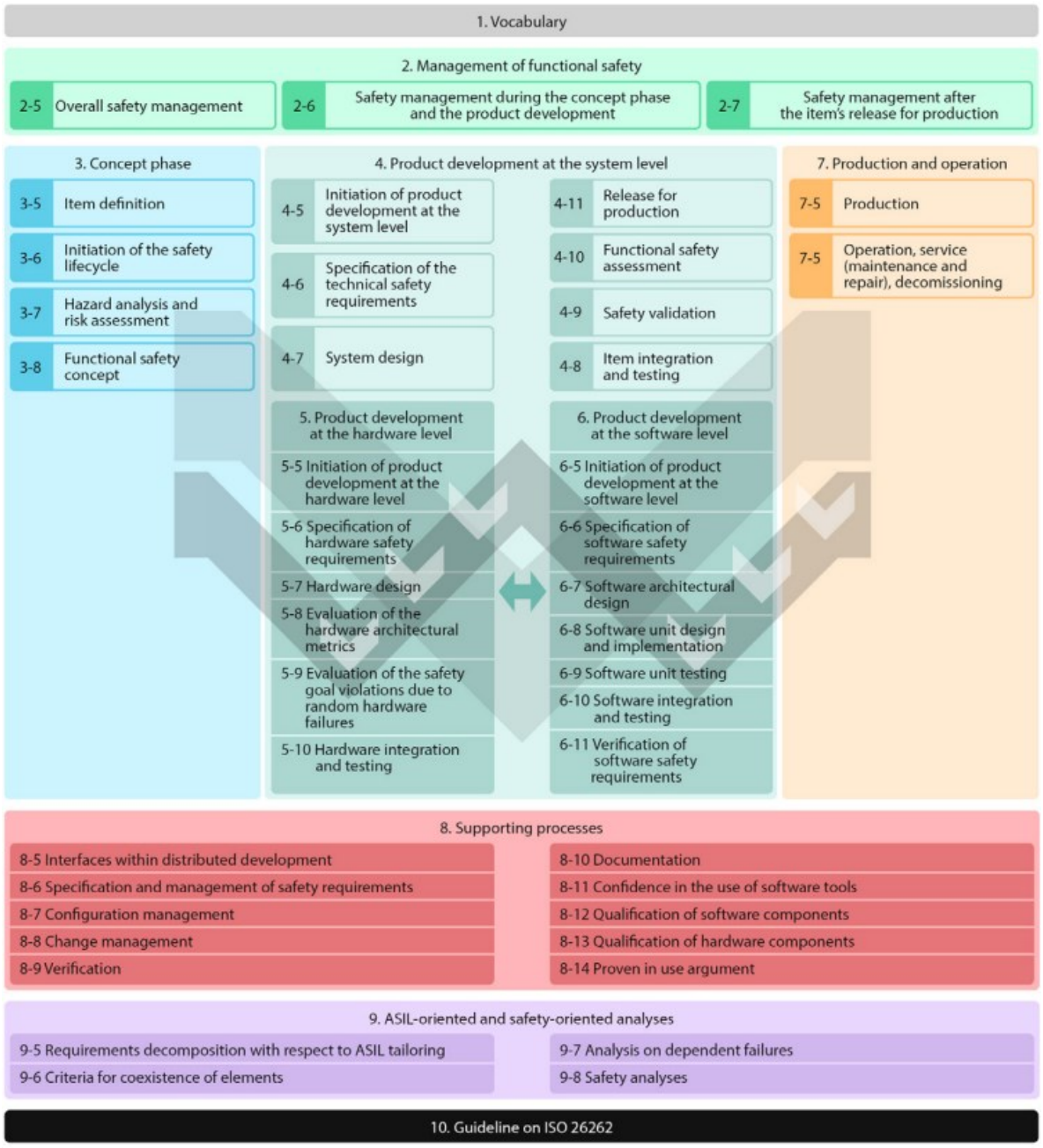
- a kiberbiztonsági követelmények megállapítása,
- a kiberbiztonság megvalósítása,
- a kockázatkezelés verifikálása, valamint
- a kockázatkezelés validálása.



20. ábra ASPICE és ASPICE CS lépések [27]

Az ASPICE-szabványt 0–5 közötti szinteken értékelik. A folyamatértékelési modell az ASPICE kulcsfontosságú összetevője, szabvány, amelyet az autóiparban szoftverfejlesztési folyamatok értékelése és javítása érdekében használnak. Az ASPICE és az ASPICE CS nagyrészt általános, nem konkrét eszközöket vagy technikákat írnak elő, hanem keretet biztosítanak a szoftverfejlesztési folyamatok értékeléséhez és javításához, valamint garantálják, hogy az autóipar számára gyártott szoftverek minősége megfelel az előírt szabványoknak.[20][21][27][182][192][220][281]

Konfliktusok előfordulhatnak a rendszerbiztonsági követelmények és a kiberbiztonsági követelmények között. A 10 fejezetből álló ISO 26262 szabvány előírja a kiberbiztonság és a funkcionális biztonság területei közötti kommunikációt, hogy megakadályozzák a másik számára hasznos információk elhanyagolását. Mindkét területnek szűkös az átviteli kapacitása, a security és safety intézkedések számításigényesek lehetnek.[28][183]



21. ábra Az ISO26262 szabványcsalád áttekintése [151]

Kiberbiztonság vonatkozásában az autóipar számára az UNECE WP29 rendeletevár el preventív intézkedéseket a kiberbiztonsági kockázatok kezelésére. *„A WP29 két új ENSZ-rendeletet vezet be a kiberbiztonságról és a 2021 januárjában hatályba lépett szoftverfrissítésről, amely négy különböző szakterület végrehajtását írja elő:*

- *a járművekkel kapcsolatos kiberkockázatok kezelése*
- *a járművek tervezési biztonsága a kockázatok csökkentése érdekében az értéklánc mentén,*
- *a biztonsági incidensek felderítése és az azokra való reagálás a járműparkban*

- *a biztonságos és biztonságos szoftverfrissítések biztosítása és annak biztosítása, hogy a járművek biztonsága ne sérüljön, jogalapot teremtve a fedélzeti szoftverek úgynevezett „Over – the – Air" (O.T.A.) frissítésére."*. [162]

A WP29 által bevezetett UN R155. és UN R156. rendeletek célja az autóipari szereplők kiberbiztonságának szabályozása. UN R155 szervezeti szinten elvárja egy kiberbiztonsági irányítási rendszer (CSMS) kialakítását és működtetését, míg az UN R156 szervezeti szintű Szoftverfrissítési irányítási rendszer (SUMS) kialakítására és működtetésére vonatkozik. Előbbi rendelet közvetlenül hivatkozik az ISO/SAE 21434 szabványra. A szabvány mögöttes motívációját a járművekben megjelenő egyre több interfész, több szoftverréteg, ami gördülő számítógépekké alakítják autóinkat. A járművek támadási felülete növekszik, ami potenciális sebezhetőségeket jelent. A járművek működését biztosító szoftverekben található több millió kódsor növeli a lehetséges szoftverhibák mennyiségét.

A szabvány elvárja, hogy kiberbiztonság tervezett módon működjön, ezért a szervezetnek fenn kell tartania a kiberbiztonsági irányítási rendszert és kiberbiztonsági kultúrát, beleértve a tudatosság- és kompetenciamenedzsmentet, valamint a folyamatos fejlesztést. Ez magában foglalja a szervezeti szabályok és folyamatok meghatározását, amelyeket rendszeres időközönként, független audittal (tanúsító audit) kell igazolni.

„*Az ISO/SAE 21434 egy egyedi megfelelőségértékelési követelményeket rögzítő szabvány, amely megköveteli egy minőségirányítási rendszer működtetését, ezért átfedések vannak az IATF 16949 és az ISO 9001 megfeleléssel. Az ISO/SAE 21434 szabvány a kiberbiztonsági irányítás következő szempontjairól rendelkezik:*

- *Általános - A kiberbiztonsági tevékenységek irányítása*
- *Projektfüggő - A kiberbiztonsági tevékenységek tervezése és végrehajtása a felelősségi körökkel együtt.*
- *Folyamatos - Állandó kiberbiztonsági tevékenységek (monitoring, sebezhetőségi elemzés stb.)*
- *Kockázatértékelési módszerek - Kockázatértékelés*
- *Biztonság a tervezés során - Kiberbiztonsági tevékenységek a tervezés, fejlesztés, gyártás és üzemeltetés során elosztva - A kiberbiztonság biztosítása az ellátási láncban (a beszállítók ellenőrzése)*.".[162]

A járművekhez kapcsolódó szakértői vizsgálatok célja és érdekelt felei

A modern és egyre inkább önvezetővé váló járművekhez kapcsolódó szakértői vizsgálat során elengedhetetlen a vizsgálat főbb érdekelt feleinek figyelembe vétele, annak érdekében, hogy a vizsgálat teljes körű volta biztosítható legyen. A szakértői vizsgálat érdekelt felei akkor relevánsak, ha szignifikáns negatív vagy pozitív hatásuk van a vizsgálati tevékenységre. A jármű gyártója (OEM: Original Equipment Manufacturer)[i] az egyik fő érdekelt lehet egy vizsgálat során, amely a jármű fejlesztési, gyártási és használati, karbantartási (pótalkatrészek) életciklusában helyezkedik el. Az OEM érdekelt a termékei problémáinak azonosításában, melyek hatással vannak a gyártásra és a termékfejlesztésre, továbbá érdekelt olyan kérdések megválaszolásában is, mint hogy „A jármű okozta a balesetet?" vagy „Megfelelően kezelték-e a személyes adatokat a járműben?" Az OEM-ek hozzáférhetnek a jármű olyan belső információihoz, melyek a szakértő által nem vagy jelentős idő- és költségráfordítással lennének elérhetőek, azonban a szakértői vizsgálat fontos részét képezhetik. Az ezen információkhoz történő hozzáférés érdekében a szakértői szervezeteknek ki kell alakítaniuk a megfelelő kapcsolatot az egyes OEM-ekkel.

A céges autók tulajdonosai egész flottával rendelkezhetnek, és a jármű használati életciklusában helyezkednek el. Számukra a vállalathoz kapcsolódó adatok védelme és az alacsony költségek a legfontosabbak, tehát a vizsgálat során érdekeltek olyan kérdések tekintetében, mint „Ki fért hozzá a járműben lévő (személyes) adatokhoz?" vagy „A járművezető vagy a jármű okozta a balesetet?". A magánautó tulajdonosai szintén a használati életciklusban helyezkednek el, és fontos számukra a személyes adataik, az utazási útvonalak, híváslisták stb. védelme vagy a jármű kiberbiztonsága.

A beszállítók részt vesznek az OEM által gyártott jármű alkatrész- vagy szolgáltatásfejlesztésében, gyártásában és szállításában. A szakértői vizsgálat támogathatja a beszállítók által kezelt alrendszerek hibakezelését. Elemezni és adott esetben bizonyítani kell a felszerelt alkatrészek hibás működését, módosítását vagy helytelen használatát.[132]

A vizsgálatokat végző intézetek saját, hivatalos tesztelési lehetőségekkel, karbantartó felszereléssel és szerződésekkel rendelkeznek a járművek tesztelésének végrehajtásához (pl. a TÜV Rheinland). Ezekkel az erőforrásokkal határozzák meg a vonatkozó törvényeknek, előírásoknak és szabványoknak való megfelelést.

A vizsgálatot végző igazságügyi szakértő feladata, hogy kirendelés vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a

függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását.[1]

Modern járművekhez kapcsolódó jogszabályi követelmények

Az Európai Parlament és a Tanács (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, vagyis a NIS 2 irányelv hatályba lépésével az Európai Unió célja az egységesen magas szintű kiberbiztonság megteremtése a különböző kritikus ágazatokba tartozó szervezetekre vonatkozó követelmények meghatározásával. Valamennyi tagállam nemzeti jogával összhangban meg kell, hogy határozza azon követelményeket, amelyek az érintett szervezetekre vonatkoznak. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint a NIS2 irányelv hazai implementációjának eredményeképpen elkészült 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről azon követelményeket tartalmazza, amelyek a kiemelten kockázatos és kockázatos ágazatokban működő szolgáltatók és szervezetek által alkalmazandóak. A közlekedés, mint kiemelten kockázatos ágazat, valamint a kockázatosnak minősített gyártás, azon belül jelen tanulmány szempontjából releváns gépjármű gyártási tevékenységet végző érintetteknek a kiberbiztonsági szint növelése érdekében meg kell feleljenek a jogszabályi elvárásoknak.[1][107]

A technológia és szabályozás gyakran egymás ellentéteinek tűnnek, hiszen a technológia a haladást, a szabályozás pedig éppen a haladás gátját, a bürokratizmust testesíti meg.[334] Az új technológiák, mint például az önvezető járművek, a joggal szemben hármas elvárást támasztanak:

- biztosítani kell, hogy a technológiai fejlődés ne ássa alá az emberi szabadságjogokat,
- biztosítani kell az önvezető képességgel rendelkező járművek prototípusai számára – a fejlettségi szintjüknek megfelelő – valós körülmények közötti tesztelését, egyben szavatolni kell a közlekedés többi résztvevőjének az élet-, egészség- és vagyonbiztonságát, valamint, hogy
- a jog ne korlátozza a technológiai fejlődést.[238]

Az európai adatvédelmi jogszabályi környezet sok esetben megnehezíti a járművekben található adatokhoz történő hozzáférést, valamint a gyártókkal történő szakértői együttműködést. A GDPR alapján vagy arra való hivatkozással a gyártók nem, vagy nehezen biztosítanak hozzáférést az adatokhoz. Erre jó példa az eseményadat-rögzítő kiolvasásához szükséges szoftvermegoldás, ami az USA-hoz képest korlátozott információkat biztosít az európai piacon.

A mai modern ember életének szinte minden területén megjelenik a járműforgalom, a bűncselekmények közel 90 %-ánál valamilyen módon érintettségbe kerül az autó is. Így van ez a különféle jogterületekkel is, szinte mindegyikhez kapcsolódik, kapcsolódhat az önvezető járművek problémaköre. A legrelevánsabb területeknek közlekedési jog, a büntetőjog, a polgári jog és a munkajog tekinthető.

Az önvezetővé váló járművek „– *ugyanúgy, ahogy az emberi vezérlésű gépek – okoz hatnak baleseteket, amelyek anyagi károkkal és emberi életek elvesztésével járhatnak, azonban mégsem ugyanaz a helyzet, mintha emberi vezérlés útján következtek volna be ezen események. A kérdés sokkal komlexebb a gépi vezérlés esetében, például, hogy miként lehet meghatározni a felelősséget a robotautók által okozott baleseteknél közvetlen emberi mulasztás hiányában, vagy egy krízis helyzetre szóló reakció parancsainak kialakítása során milyen szempontok kerülnek előtérbe*”.[48][179]

„*Az autonóm járműnél elveszítheti jelentőségét a közúti veszélyeztetés, a járművezetés ittas állapotban, a járművezetés bódult állapotban, mint bűncselekmény típus, de például a gyorshajtás is. Azonban jelentősebb szerepet kaphat a járműben működő számítógépes rendszer feltörése miatt a közlekedés biztonsága elleni bűncselekmény.*”.[194] Utóbbi esetén a modern járművek szakértői vizsgálata nagy hangsúlyt és szerepet kap.

„*A hagyományos közlekedési bűncselekmények esetében a vezető személye egyértelmű, azonban autonóm járművek esetén ez a kategória új értelmezést igényel. Tekintve, hogy ezek a járművek tökéletesnek még korántsem mondhatóak, számos félelem és aggály merül fel, mind jogi, mind etikai, mind informatikai téren.*”.[194] „*A hatályos magyarországi büntető törvénykönyv szerinti bűncselekmény fogalom – elsősorban az alanyi oldal megkövetelésével – kizárólag természetes személy büntetőjogi felelősségre vonását teszi lehetővé. Egy önvezető jármű esetén azonban a döntéseket a mesterséges intelligencia hozza.*”. [194]

„*Az autonóm járművek esetében felmerül a kérdés, hogy ki tekinthető vezetőnek: a jármű tulajdonosa, az utas, a gyártó vagy esetleg a jármű szoftvere. A magyar jog jelenlegi keretei*

között a vezető fogalma emberi személyhez kötődik, így az autonóm járművek esetében szükség lehet a jogszabályok módosítására vagy kiegészítésére.”. [194]

„*Az automatizáltság fokának emelkedésével egyre nehezebb megállapítani a büntetőjogi felelősség kérdését. Alapesetben, a 0. szintű önvezető járműnél a jármű vezetője vonható felelősségre. Magasabb automatizáltságú járműveknél már az is kérdéses, hogy egyáltalán ki felel az okozott balesetért és ettől függően változhat a jogtalanság kérdése is.*”. [194] Több olyan szereplő is felmerülhet felelősként, aki a humán vezette járművek esetén nem merülne fel. Ilyen például:

- az üzembentartó, aki „*a magyar jogban az üzembentartó objektív felelősséggel tartozik a jármű üzemeltetéséből eredő károkért. Az autonóm járművek esetében is fennállhat ez a felelősség, különösen, ha a jármű karbantartásának elmulasztása vagy nem megfelelő használata okozza a balesetet.*” [194],
- a gyártó, amennyiben „*a baleset a jármű szoftverének vagy hardverének hibájából ered, a gyártó termékfelelőssége merülhet fel. Ez különösen akkor releváns, ha a hiba a gyártás során keletkezett, és az a jármű rendeltetésszerű használata mellett okozott kárt.*” [194],
- a szoftverfejlesztő, „*amennyiben a baleset a jármű vezérlőszoftverének hibájából adódik, a szoftverfejlesztő is felelősségre vonható lehet. Ez a felelősség azonban nehezen körül határolható, mivel a szoftverek komplexitása és a folyamatos frissítések miatt a hibák forrásának azonosítása kihívást jelenthet.*”.[194]

„*A polgári jogban (magánjogban) alapvetően három felelősségi forma alkalmazása jöhet szóba, amennyiben az önvezető jármű működésével összefüggésben károkozás következik be. A kellékszavatosság, illetve a termékszavatosság általános elvei (Ptk. 6:159-170. §) mellett nem lehet figyelmen kívül hagyni a veszélyes üzemi felelősség szigorú, a kimentés lehetőségét jóformán kizáró szabályait (Ptk. 6:535. §) sem. Végül a polgári jogban, a termékfelelősségre (Ptk. 6:550–559. §) vonatkozó rendelkezések alapján akár az önvezető jármű gyártója is – objektív alapon – felelőssé tehető.”.* [16]

A munkajog területén „*a munkáltató kártérítési felelőssége (a munka törvénykönyvéről szóló 2012. évi I. törvény 166. §) ugyanúgy felmerülhet, miként az üzemi balesetre [a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXIII. törvény 52. § (1) bek.], illetve a munkabalesetre (a munkavédelemről szóló 1993. évi XCIII. törvény 87. § 3. pont) vonatkozó ágazati szabályozás.*”. [16]

„*Az önvezető járművek esetleges balesetei megítélésének vonatkozásában a polgári, illetve a munkajogi jogalkalmazásnak lényegesen könnyebb dolga van a büntetőjogban tapasztalhatónál.* […] *A büntetőjogi felelősség megítélése ezzel szemben már sokkal problematikusabb lehet: itt nem él a jogellenesség vélelme, továbbá a fordított bizonyítási teher mellett a társadalomra veszélyességet, illetve a személyes bűnösséget, felróhatóságot is bizonyítani szükséges a büntetőeljárásban a konkrét terhelt felelősségre vonásához.*". [16]

„*A közlekedési jog – mint a közigazgatási jog speciális területe – maga is összetett normarendszer. Magában foglalja mindenekelőtt a közúti közlekedés szabályairól szóló 1/1975. (II. 5.) KPM–BM együttes rendeletet (a továbbiakban: KRESZ), az 1968. évi november hó 8. napján Bécsben aláírásra megnyitott Közúti Közlekedési Egyezmény kihirdetéséről szóló 1980. évi 3. törvényerejű rendeletet, illetve a közúti közlekedésről szóló 1988. évi I. törvényt.*".[16]

„*Prognosztizálható, hogy a hagyományos büntetőjog koordináta-rendszerében nem, illetve nehezen lehet majd csak elhelyezni a jövőben felmerülő társadalomra veszélyes cselekményeket. Ezen előrejelzés pedig feltétlenül új utak kitaposását tehetik szükségessé. Felvethető végül, hogy a büntetőjog ultima ratio jellege egyes közlekedési bűncselekmények büntetési tételeinek mérséklése, majd a későbbiekben esetlegesen akár dekriminalizációjuk megfontolása mellett szólhat, hiszen nagyobb társadalmi előny várható az önvezető járművek elterjedéséből fakadó csökkenő számú balesettől, mint attól, hogy a felmerülő, várhatóan egyre csekélyebb számú elkövetőket a jelenlegi tényállások és büntetési tételek alapján, feltétlenül felelősségre vonjuk.*".[16]

Nem csupán a jogszabályi környezet, a különböző jogágak nem készültek még fel az autonóm közlekedéshez kapcsolódó helyzetekre, a modern járművek érintettsége az igazságügyi szakértői tevékenységekben is jelenthetnek, okozhatnak és okoznak is új kihívásokat.

A modern járművek által elszenvedett vagy okozott közlekedési balesetek utólagos vizsgálata, rekonstrukciója, valamint olyan esetek, amikor a jármű tartalmaz valamilyen elektronikus nyomot, bizonyítékot, továbbá a jármű volt maga egy támadás célpontja vagy a bűncselekmény elkövetési eszköze szükség lehet szakértői vizsgálatokra.

Abban az esetben is, ha egy magas automatizáltságú járművel bűncselekményt követnek el, meg kell találni az elkövetőt, aki elkövette a cselekményt. A fentiekből látszik, hogy ez nem egyszerű feladat, a vezető, a szoftverfejlesztő, a gyártó, stb. is felmerülhet, aki nem gondoskodott megfelelően a jármű védelméről. „A törvényi tényállások kialakításánál azonban nem csak a robotautó szempontjából, hanem a környezet tekintetében is meg kell vizsgálni,

hogy milyen követelmények mellett lehetséges olyan környezet kialakítása, amellyel lehetséges a jogszabályok be tartása.”.[48][180] Ilyen lehet például:

- gondatlanság,
- objektív felelősség,
- gyártási hibák,
- tervezési hibák,
- tájékoztatás elmulasztása,
- megtévesztés, és
- garancia.

A jogi eljárásokban alkalmazható „*bizonyítási eszközök: a felek meghallgatása; közokiratok; magánokiratok; szakvélemények; bírósági vizsgálatok; a tanúk meghallgatása; valamint szavak, hangok és képek reprodukciója, illetve olyan eszközök, amelyek lehetővé teszik a szavak, adatok, ábrák és számviteli vagy az eljárás szempontjából releváns egyéb célból elvégzett matematikai műveletek tárolását, lehívását és reprodukcióját.*”[108] A járművek, mint adatforrás jelennek meg az eljárásokban. A fenti eseteket figyelembe véve a járművekből, a járművekre és környezeti paraméterekre, utasokra és vezetőre vonatkozóan információk gyűjtésére van szükség, hogy nyilvánvalóvá lehessen tenni, mi történt, még olyan esetekben is, ami nem megismételhető.[48][180]

Az információ gyűjtés a digitális forenzikus vizsgálati módszertanok alkalmazásával válik lehetségessé, ami a következő fejezetekben részletesen tárgyalásra kerül. A vizsgálatok célja az adatok azonosítása, megszerzése, feldolgozása, elemzése történik, amelyek alapján jelentés készül.[82][149]

Az Európa Tanács, Számítástechnikai Bűnözésről szóló 2001. november 23-án kelt Egyezménye meghatározza a számítástechnikai adat fogalmát: „*tényeknek információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, amely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja*”. A büntetőeljárásról szóló 2017. évi XC. törvényben a fogalom az alábbiak szerint került meghatározásra: „*Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.*”.[116][270]

Az elmúlt években végbement társadalmi, tudományos-technikai változások, hatások új fogalmakat hoztak magukkal a forensics területén is, például a digitális nyom fogalmát.[167] A társadalom digitalizációja, mint folyamat jelentősen befolyásolta a kriminalisztikai tevékenységet, szükségessé vált a korábban bevett eljárások és gondolkodásmód megreformálása. A helyszíni szemléken indokolt lett informatikus szakértő igénybevétele, és a nyomozó hatóságoknak a digitális nyomok rögzítésére és tárolására alkalmas berendezések beszerzése.[338] A digitális nyomok, az elektronikus adatok, mint bizonyítékok, a digitális eszközökből vagy a kibertérből nyerhető bizonyíték magán viseli annak változékonyságát, manipulálhatóságát. Emiatt ezekkel szemben különleges követelményeket támasztanak annak érdekében, hogy a bíróságok számára elfogadható legyen, mert bizonyítékot csak az képez, amely hitelt-érdemlő és a bizonyítandó tények megállapítására szolgál, más nem.[325]

A modern járművekben található, általuk gyűjtött, feldolgozott, továbbított és tárolt információ gyűjtése, az adatokhoz való hozzáférés, azok kinyerése, elemzése a különböző vizsgálati célok eléréséhez és a bűnmegelőzési tevékenységekhez egyaránt nagyban hozzájárulnak és megfelelő módszertan alkalmazása mellett teljesíthetik a bizonyítékokra vonatkozó követelményeket. Az adatok modern járművekből történő megszerzése, feldolgozása és értelmezése magas szintű technológián alapul, melyhez komplex, érvényes és megbízható technikák, eljárások és módszertanok szükségesek.

Digitális forenzikus szakértői vizsgálatok

A jogi eljárások fejlődése, a perbeli képviselet lehetőségeinek változása lehetővé tette, hogy a felek igazolhassák, bizonyíthassák az „igazukat”. Ennek egyik módja a bizonyítékok szakértő általi feldolgozása, elemzése, melynek eredményéről állásfoglalást készít.

A Forensics sciences, a forenzikus tudományok, vagy más néven kriminalisztika a bűncselekmények felderítésével és bizonyításával, annak eszközeinek és módszereinek feltárásával rendszerezésével foglalkozik.[49][134]

A forenzikus tudományokban természettudományos módszereket és technikákat – típusuktól függetlenül – szisztematikusan alkalmazzák – számítástechnika, katonai tudomány, gépészet, vegyipar, építőmérnöki tudományok és elektrotechnika –, mint eszközöket, amelyek segítenek feltárni az okokat és az igazságot a bizonyítékok gyűjtésével, kinyerésével és vizsgálatával. A forenzikus tudomány támogatja a polgári és büntetőeljárásokat, rekonstruálja az eseményeket, igazolja az elfogulatlanságot egy jogi ügyben. Alkalmazott tudományként a forenzikus tudomány vizsgálati eszközként szolgál.[49][134][274][284][326]

A forenzikus szó a latin forensis szóból származik, jelentése nyilvános, fórum vagy nyilvános vita, érvelő, retorikai, vitához vagy megbeszéléshez tartozó. A forenzikus tudomány meghatározására számos definíciót használnak. Az egyik a tudományos módszerek és technológiák széles spektrumának alkalmazása a büntető- vagy polgári joggal kapcsolatos tények kivizsgálására és megállapítására. Egy modern definíció szerint a forenzikus a bírósághoz kapcsolódó, abban használt vagy ahhoz alkalmas. Bármely, a jog céljaira használt tudomány, forenzikus tudománynak számít.

A mai modern kriminalisztikai alapismereteket Arkhimédész (Kr. e. 287-212), a görög feltaláló, matematikus és fizikus már az ókorban is alkalmazta. Arkhimédész Eureka-legendája forenzikus tudományok korai alkalmazásának tekinthető. A víz kiszorításának elveit vizsgálta annak érdekében, hogy az uralkodó koronájának sűrűsége és felhajtóereje alapján bebizonyítsa, hogy az aranyból készült-e vagy sem. Egy másik törvényszéki megközelítés az ujjlenyomatok segítségével történő személyazonosság-igazolás bevezetése volt a 7. században, valamint az orvosi bizonyítékok gyűjtése és felhasználása volt a halál módjának megértéséhez a 11. században Kínában, később pedig a 16. századi Európában. Richárd király már a 12. században megalakította az úgynevezett halottkémi hivatalt (Office of the Coroner) Angliában, hogy

ötvözze az orvosi és jogi megközelítést a bűncselekmények kezelésében. Ezt a megközelítést az Egyesült Államokban még mindig alkalmazzák.[8][187]

Büntető és peres eljárások fejlődése, a perbeli képviselet változása lehetővé tette, elősegítette a felek azon érdekét, hogy igazolhassák, bizonyíthassák az igazukat. A 19. században, Francis Galton ujjlenyomat vizsgálata volt az jelentős lépés a modern kori vizsgálatok között, amely később tovább fejlődött például a vércsoportok megállapításával. A 20. századi kriminalisztika kiemelkedő eredményei a ballisztikai vizsgálatok kialakítása és elvégzése volt. Az első forenzikus labort az FBI alapította 1932-ben. A 19. századi technológiai vívmányok büntető és peres eljárásokban való alkalmazása magával hozta egyéb tudományágak bevonását, újabb forenzikus laborok kialakítását. 1984-ben az FBI vizsgálati gyakorlatában először jelenik meg a számítógépes forenzikus vizsgálat.[326]

A hatékony és szakszerű bűnüldözés, a nyomozás modern, tényfelderítő, interdiszciplináris alkalmazott tudománya, ami a 19. század második felében indult a tudományos bizonyítékok előretörésével.

„A kriminalisztika a „*bűnügyi nyomozástan, azaz a bűnügyi tudományoknak az az ága, amely a bűncselekmények felderítésének és bizonyításának eszközeit és módszereit tárja fel és rendezi elvi és gyakorlati szempontból egyaránt*".[308] A kriminalisztika „*fő feladata a természettudományok eredményeinek felhasználása annak érdekében, hogy a bűnüldözés és a büntető igazságszolgáltatás az állam büntető hatalmát törvényes eljárásban, az igazság megállapítására alapozva érvényesítse*".[117] Szinte minden tudományos tevékenység tekinthető kriminalisztikai tevékenységnek, mivel hozzájárulhat a bizonyítékok felleléséhez, feltárásához. A kriminalisztikában szisztematikus módon alkalmazzák a természettudományos módszereket, technikákat, azok típusától függetlenül, emellett saját módszereket is kialakítottak.

Egyes vizsgálatokban máig szükség lehet a különböző területek együttműködésére, specializálódott szakértőkre, mint orvosszakértő, kriminológus és egyéb mérnökség, a jogi esetek támogatásában, megoldásában, esetenként átfedésben is vannak ezen területek. Mivel minden eset más és más, elsődleges feladat a pártatlanság biztosítása és a bizonyítékok védelme (feltárástól a megőrzésig folyamatosan), az események idővonalának rekonstruálása. Alapos vizsgálat elvégzésével igazolni kell, nyilvánvalóvá kell tenni a megtörtént eseményeket, azon esetekben is, melyek nem megismételhetőek. A vizsgálat során az evidenciák fellelésétől,

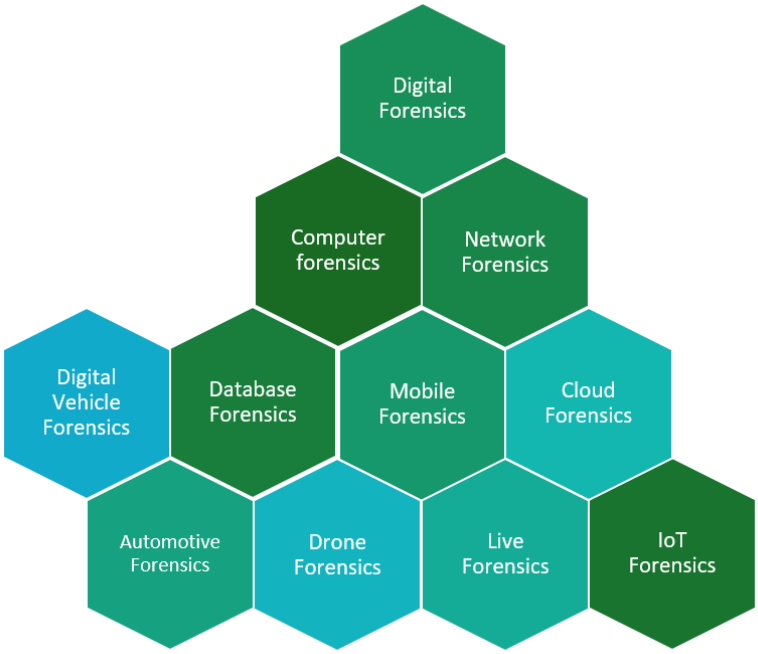
feltárásától kezdve, több, folyamatosan dokumentált lépésből álló folyamatok keresztül át juthatunk el a vizsgálati eredményig, ezek prezentálásáig, az evidenciák tárolásáig.[274][326]

Napjainkban ritka olyan személyt találni, aki ne használna valamilyen digitális eszközt, folyamatosan körül vagyunk véve és függünk a különböző okos eszközeinktől, egyes megközelítésben az eszközök kezdtek el használni minket.[283] Szinte nincs olyan tevékenység, amely ne lenne az információtechnológiai fejlődés és az infokommunikáció eredményei által támogatott, a mindennapi feladataink elvégzéséhez is valamilyen digitális eszköz (például: notebook, mobiltelefon, stb.) használata szükséges vagy célszerű. Ahogy egyre inkább életünk részévé váltak ezek az eszközök, a hozzájuk kapcsolódó szakértői vizsgálatok szerepe is egyre inkább növekedett. A felhasználók sok esetben nem is gondolnak bele, hogy mennyi információt tárolnak róluk az egyes IT és mobil eszközeik, amit nap mint nap használnak. Napjainkban éves szinten annyi adatot állítunk elő, mint amit az emberiség az egész történelme alatt előállított. Ezen adatok vizsgálatával, értelmezésével vagy visszaállításával, a digitális forenzikus eljárások segítségével megállapítható, hogy mely IT eszközt használták egy adott eseménykor. A digitális forenzikus vizsgálatok a forenzikus tudományok egyik új, modern területe, amely digitális eszközökön található adatok visszaszerzésével és vizsgálatával foglalkozik.[202] Segítségével meghatározható, hogy az egyes felhasználók milyen alkalmazásokat futtattak, milyen tartalmakat értek el az interneten. Ezen információk visszaállíthatóak, még abban az esetben is elérhetőek, ha az evidenciákat törölték.

A digitális kriminalisztika a digitális bizonyítékokkal kapcsolatos tények azonosításának, megőrzésének, visszaszerzésének, elemzésének és bemutatásának tudománya. Az EcCouncil fogalmi meghatározása szerint a digitális kriminalisztika az elektronikus adatok feltárásának és értelmezésének folyamata. A folyamat célja, hogy bármilyen bizonyítékot a legeredetibb formájában megőrizzen, miközben strukturált vizsgálatot végez a digitális információk gyűjtésével, azonosításával és validálásával a múltbeli események rekonstruálása érdekében.[95][150][298] Az Interpol megközelítése szerint a digitális kriminalisztika a forenzikus tudományok egy olyan ága, amely az elektronikusan tárolt adatok azonosítására, megszerzésére, feldolgozására, elemzésére és jelentésére összpontosít. Fő célja adatok kinyerése elektronikus bizonyítékokból, azok hasznosítható információkká való feldolgozása és az eredmények bemutatása a jogi eljárásban.[149][201]

Gyakorlati megközelítésben a digitális kriminalisztika a digitális eszközökön, például számítógépeken, mobileszközökön, felhőben, hálózaton, stb. elkövetett bűncselekmények

kivizsgálásáról szól. A digitális kriminalisztika így többféleképpen értelmezhető, a vizsgálat tárgyától és az eszköz jellegétől függően.



22. ábra Digital forensics és kapcsolódó domain-ek, melyek modern járművekben történő alkalmazhatóságának vizsgálata került elvégzésre

Egyes értelmezésben külön kategóriaként értelmezett a műholdak, GPS, Operational Technology (OT) rendszerek digitális kriminalisztikai vizsgálata is.[120]

A járművek fejlődése a mobil kommunikációs eszközök elterjedése és a kooperatív közlekedés rendszerek kialakulása eredményezi a széleskörű, összetett bizonyítékok feltárásának lehetőségét, a modern közlekedési eszközök és rendszerek számos új, potenciális bizonyítékforrást hoztak létre. Az adatok hozzáférhetősége, összegyűjtése, értékelése területén számos probléma, nehezítő tényező van, és jelenleg lényegesen kevesebb megoldás létezik, komplex, hatékonyan alkalmazható módszertan, megoldás pedig egyelőre nem áll rendelkezésre.[316]

Forensics vizsgálatok fő kérdései (7W)

A modern és egyre inkább önvezetővé váló járművekkel kapcsolatos bizonyítási eljárások eszközei között egyre inkább az elektronikus adatok és az ezeket tároló adathordozók, eszközök válnak hangsúlyossá. A kriminalisztika egyik alapelve szerint a múltbéli esemény megismételhető a bizonyítékok/nyomok segítségével, azonban nem tárható fel minden esetben, minden bizonyíték.[171]

Digitális környezetben ez azt jelenti, hogy a rendelkezésre álló digitális bizonyítékokat felhasználva kerülnek megválaszolásra az úgynevezett 5WH/6W, vagy egyes megközelítés szerint a 7W formula kérdései. A tudományos irodalomban egyaránt megtalálható az 5WH (**w**ho, **w**hy, **w**here, **w**hen, **w**hat, **h**ow), vagy más elnevezésben 6W formula (**w**ho, **w**hy, **w**here, **w**hen, **w**hat, ho**w**), vagy ennek Fenyvesi Csaba által bővített változata a 7W, ami az eredeti formula kiegészítése a „with whom", vagyis kivel kérdéssel, ami társas elkövetés és az összekapcsolt járművek vizsgálata során esetén játszik szerepet.

A vizsgált eseményhez kapcsolódó fő kérdések tehát:

- ki (who): a vizsgálathoz kapcsolódóan érintett személyek (például: sértettel közvetlen kapcsolatba hozhatószemély, vagy személyek, azon személyek azonosítása, akik a bűncselekmény elkövetésével kapcsolatba hozhatóak, vagy akik szemtanúi lehettek a cselekmény elkövetésének),
- miért (why): az esemény motivációja/kiváltó oka (például: a cselekményt előre eltervezték, vagy azt ad-hoc jelleggel követték el),
- hol (where): az esemény helyszíne és egyéb a vizsgálat szempontjából fontos helyszínek (például: a kábítószer előállításának, tárolásának és kereskedelmének különböző helyszínei),
- mikor (when): a vizsgált esemény és egyéb kapcsolódó események időpontok (például: egy közlekedési baleset bekövetkezésének pontos időpontja, amelyből ellentmondás esetén egyértelműen megállapítható a forgalmi jelzőlámpa jelzése),
- mi (what): az esemény és az események idővonalának összeállítása (például: informatikai eszközön elkövetett támadás során mi (és mikor) változott meg),
- hogyan (how): hogyan történt, milyen módon következett be az esemény (például: megtévesztéssel telepítenek kártékony kódot a sértett számítástechnikai eszközére),
- kivel (with whom): az eseményben érintett, vagy résztvevő személyek meghatározása (például: több elkövető esetén az egyes személyek szerepe a cselekmény elkövetésében).[18][115][138][171]

A ki kérdés megválaszolása az egyik legnehezebb az egyre inkább önvezetővé váló járművek esetén. Erre a kérdésre abban az esetben lehet választ adni, ha:

- ismert a jármű automatizációjának/önvezetésének szintje,
- meghatározásra kerültek a vonatkozó jogszabályi kérdések.

A járművek önvezető képességi szintjének ismerete mellett, a miért kérdés megválaszolása során a szakértői vizsgálatnak ki kell terjednie annak meghatározására, hogy az adott jármű biztonsági szintje megfelelt-e a gyártói követelményeknek, beállításoknak. Valamint történt-e olyan jogosulatlan módosítás, hiba amely hatással lehetett a jármű működésére, vagy az időszakos karbantartások megtörténtek-e, a kopó alkatrészek szervíz intervalluma megfelelő-e, maga a jármű programozására vonatkozó hiba felfedezésre került-e. Amennyiben nem történt külső beavatkozás (például nem gyártói módosítás, vagy hacking), nincs külső hiba, vizsgálandó, hogy a jármű saját belső utasításai, vagy a járművezető által végrehajtott tevékenységek eredményezték az adott eseményt. Külső beavatkozás, jogellenes behatolás, jogosulatlan módosítás, utasítás kiadás hiányában a jármű belső működése és/vagy a vezető által kiadott utasítások, tevékenységek kerülnek vizsgálatra. Amennyiben feltételezhető a visszaélés, jogosult vagy jogosulatlan beavatkozás, a működés manipulációja, a megtörtént eseményt ezek figyelembevételével és vizsgálatával kell kiegészíteni. A vizsgálat során feltárásra kerülhet, hogy a járműben kártékony kód került-e alkalmazásra, valamilyen terrorcselekményhez kapcsolódóan történt-e olyan beavatkozás, amely a járművet a támadás célpontjává teszi, vagy maga a jármű a cselekmény eszköze.[138]

A hol kérdés már a mai járművekben is egyre inkább elterjedt beépített navigációs rendszerek segítségével egyszerűen megválaszolható lesz. A vizsgálat során a mobil eszközökből származó helyadatokkal kiegészítve a vizsgálati pontosság is javítható lehet.

A mikor kérdés az önvezető járművek esetén nem eredményez vizsgálati sajátosságot, a válasz szempontjából nincs nagy jelentősége annak, hogy a jármű önvezető vagy sem, azonban az elsőre egyszerűnek tűnő dolog, mint a dátum és idő jelenthet kihívást. A dátum (nap-hó-év, vagy év-hó-nap), az idő adatformátuma megfelelő kontextusba helyezés, időformátum (12h vagy 24h) és beállított időzóna nélkül nem egyértelmű.[171] Központi óraszinkron nélkül vagy a felhasználó által manuálisan beállított (akár szándékosan rossz) időpont ellentmondásokat eredményezhet a vizsgálat során.

Maga az esemény és az események idővonalának összeállítása során kerül meghatározásra, hogy milyen esemény történt, melyben érintetté vált a jármű. Nem csupán közlekedési balesetekben, hanem személyek követésében, titkos információgyűjtésben, különböző bűncselekményekben, kábítószer szállítmányok nyomon követésében, gyilkosságokhoz kapcsolódóan is releváns eszköz lehet a gépjármű.

A hogyan kérdésre való válasz kialakítása a modern és egyre inkább önvezetővé váló járművek esetén egyszerűbb, egyúttal komplexebb feladat. Az járművek a szenzorok hálózata által és a hálózatba kapcsoltság (mind a környezettel, mind a közeli járművekkel, pályával stb.) révén az emberi érzékelésnél sokkal részletesebb és összetettebb környezetérzékelést valósítanak meg. A gyűjtött információkat az emberi agynál gyorsabban és hatékonyabban dolgozzák fel, elemzik a helyzeteket, majd feldolgozási eredmények alapján avatkoznak be, hajtják végre az adott feladatot, műveletet, vagyis vezérlik az autót. Az összegyűjtött és feldolgozott adatok tárolásra kerülnek, általuk a megoldott közlekedési szituációk információi hozzáférhetőek lesznek az utólagos vizsgálat során, segítségükkel nagy pontossággal válik meghatározhatóvá, hogy a vizsgált esemény hogyan következett be.[138]

A kivel kérdés esetén az eseményben érintett, vagy abban résztvevő személyek meghatározása történik. A járművek egymással, digitális eszközökkel és környezetükkel való összekapcsoltsága által, olyan információk is rendelkezésre fognak állni, amellyel a vizsgált eseményben résztvevők, vagy az esemény által érintettek köre egyszerűen meghatározható.[249][270]

A járművekhez kapcsolódó szakértői vizsgálatok célja lehet a modern és önvezető járművek által elszenvedett vagy okozott balesetek utólagos vizsgálata, emellett egyéb hatósági, jogi, büntetőjogi eljárásokban való, a járművekben megtalálható információk elemzése, a megtörtént események igazolása is.

A járművekhez kapcsolódó szakértői vizsgálatok alatt általában:

- sérült, vagy balesetet szenvedett járművek szakértését (kárszámítását, értékcsökkenés meghatározást, javítási kalkuláció készítést),
- hibás járművek szavatossági problémáinak vizsgálatát,
- állapotfelmérést,
- hibafeltárást,
- baleset-elemzési szakvélemény készítést értünk.

Jellemzően ezekhez kapcsolódóan fordulunk szakértőhöz és kérünk valamilyen szakvéleményt. A Nemzeti Szakértői és Kutató Központ szervezeti felépítése alapján az látható, hogy a közlekedési szakértői tevékenység és az informatikai szakértői tevékenység elkülönül egymástól. Utóbbinál jelenik meg például a digitális adattároló eszközök, vagy a mobilkommunikációs eszközök vizsgálata, azonban a járművekhez kapcsolódó informatikai vizsgálatok, a jármű vagy annak környezetében megtalálható digitális információk vizsgálata

módszertani vonatkozásban nem meghatározott terület.[292] A járművekhez kapcsolódó szakértői vizsgálatok túlmutatnak az általánosságban ismert szakértői vizsgálatokon, melyek kapcsolódhatnak még például személyek követéséhez, kábítószer szállítmányok nyomon követéséhez, gyilkosságokhoz stb.

Szakértői vizsgálatok válhatnak szükségessé továbbá olyan esetekben, amikor a jármű:

- tartalmazza az elektronikus nyomot, bizonyítékot,
- egy támadás célpontja,
- a bűncselekmény elkövetési eszköze.

Abban az esetben, ha a vizsgált esemény kapcsán a jármű (volt) a támadás célpontja, a szakértői vizsgálat során az alábbi fő kérdések megválaszolásához történik a nyomok keresése:

- ki támadta meg a járművet,
- annak mely része ellen, mi ellen irányult a támadás,
- milyen célból történt a támadás,
- mikor és milyen időintervallumban történt a támadás,
- hogyan hajtották azt végre,
- milyen támadási vektor került alkalmazásra,
- hol volt észrevehető a támadás,
- milyen további hatása volt a támadásnak?

Abban az esetben, ha a jármű valamilyen módon kapcsolódik a vizsgált eseményhez, akár bűncselekményhez, a szakértői vizsgálat során az alábbi fő kérdések megválaszolásához történik a nyomok keresése:

- mely személy(ek)hez kapcsolódik a jármű,
- milyen módon használták fel a járművet,
- hol használták a járművet,
- mikor történt az esemény,
- milyen egyéb digitális eszközök kapcsolódnak az eseményhez,
- kik és milyen módon kapcsolódnak az eseményhez?

Azokban a szakértői vizsgálatokban, amelyekben a vizsgálati cél eléréséhez a jármű tartalmazza a nyomot (például a hibák gyártó általi azonosításához), a vizsgálathoz az alábbi fő kérdések kapcsolódnak:

- mely személyekről található információ,
- milyen eseményhez kapcsolódnak a járműben található információk,
- milyen információk találhatóak a járműben,
- milyen időtartamban érhetőek el az információk,
- mikor keletkeztek az információk,
- hogyan keletkeztek az információk,
- hol találhatóak az információk,
- hogyan érhetőek el a releváns információk,
- manipulálásra kerültek-e az információk?

Az új technológiák megjelenése és megnövekedett adatmennyiség, az új adatforrások új szakértői megoldásokat, eszközöket, megközelítéseket, folyamatokat igényelnek a korábbi és az esetlegesen új kérdések megválaszolására. A szakértői vizsgálatokhoz kapcsolódóan elérhető új adatok és adatforrások által, például olyan új kérdésekre is adható válasz mint, hogy egy eseményhez kapcsolódóan kik tartózkodtak annak közvetlen közelében, vagy mely személyek, járművek milyen gyakorisággal, hol érintkeztek egymással.

Szinte minden tudományterület és -ág alkalmazhat forenzikus módszereket, amelyekkel hozzájárulhatnak a szükséges információk, bizonyítékok felleléséhez, feltárásához. Szisztematikus módon alkalmazott természettudományos módszerek, technikák segítségével történik a bizonyítékok gyűjtése, kinyerése, vizsgálata. A cél minden esetben az okok, a megtörtént események, az igazság megállapítása a büntető és polgári eljárásokban.

A járművek szakértői vizsgálatainak céljai, hasonlóan a digitális forenzikus vizsgálatok céljához a következők:

- az esemény meghatározása,
- hiteles bizonyítékok szolgáltatása,
- bizonyítékok felkutatása és feltárása,
- a bizonyítékok forrásának meghatározása, információk kinyerése,
- válaszadás a 7W szerinti kérdésekre,[42]
- bizonyítékok megőrzése.[18]

Ezen célok teljesítéséhez az alábbi vizsgálati alapelvek figyelembe vétele szükséges:

- az esemény/bűncselekmény helyszínének biztosítása és a nyomok biztonságban tartása, a folyamatok dokumentálása, stb.
- a bizonyítékhoz való hozzáférés/interakció korlátozása annak érdekében, hogy „a RAM rögzítésével biztosítsuk a bizonyítékok korlátozott interakcióját,
- a felügyeleti lánc fenntartása, a bizonyítékok rögzítésének sorrendjének fenntartása dátummal és időbélyegekkel, valamint a hozzáférők azonosítása.[67]

Kutatásomban a digitális forenzikus domainek folyamatainak és módszereinek áttekintését és vizsgálatát végeztem el, kiemelten a modern járművek sajátos működéséhez, kommunikációs megoldásaihoz és közös megközelítéseihez viszonyítva. Ennek érdekében nagy hangsúlyt fektettem a számítógépes, a felhő alapú rendszerek, drónok és hálózatok vizsgálataira és azok alkalmazhatóságára a járművek esetén.

A számítógépek forenzikus vizsgálata (**Computer Forensics**) a digital forensics család egyik alapvető eleme, amely az adatok azonosításából, gyűjtéséből, vizsgálatából és elemzéséből áll, miközben megőrzi az információk integritását és fenntartja az adatok szigorú felügyeleti láncolatát. A számítógépek vizsgálatának célja az adattárolón lévő adatok kinyerése, megőrzése, visszakeresése és az adatok prezentálása. Forenzikus tudományként a DNS-technológia óta semmi sem gyakorolt akkora potenciális hatást specifikus szakértői vizsgálatokra és büntetőeljárásokra, mint a számítógépes vizsgálat. Ugyanakkor napjainkban a hagyományos forenzikus tudományágak többsége nagy mértékben eltér egymástől. Mind a vizsgált eszközök, mind az alkalmazott technikák, és az alapesetben laboratóriumi körülmények között végzett vizsgálatokat gyakran a helyszínen végzik el. Ezért az elemzések eredménye közvetlen információ lesz, következtetések helyett, ami egy ügyben nagy jelentőséggel bír. Tekintettel arra, hogy a járművek egyre inkább szoftverorientált eszközökké válnak, gördülő számítógépekként is értelmezhetők, a számítógépes vizsgálati eljárások és technikák a jövőbeli járművizsgálatok elkerülhetetlen részét képezik majd.[67][82][111][112]

A **Network Forensics**, a hálózati kommunikáció forenzikus/szakértői vizsgálata, a digitális forenzikus vizsgálatok egyik területe, amely kommunikációs hálózatok mozgásban lévő adatainak (data in motion) azonosításához, vizsgálatához, értékeléséhez és elemzéséhez, illékony és dinamikus információkkal foglalkozik. A vizsgálatok célja a hálózaton keresztül átvitt adatok megértése és a végpontok felé irányuló, vagy közötti interakciók és tevékenységek feltárása. A hálózati forgalom eseményeinek, naplóinak és kommunikációs mintáinak

monitorozásával és elemzésével foglalkozik, annak érdekében, hogy biztosítsa a vizsgálati célok eléréséhez szükséges információkat. Járművek esetén is szükség lehet a kommunikációs csatorna vizsgálatára, ami a network forensics eszközrendszerével történhet meg.

Az információszerzés, mint kezdeti lépés mind a járművek, mind a hálózatok szakértői vizsgálata szempontjából fontos lépés. Ennek keretében a vizsgálati kérdésekhez kapcsolódóan előzetes információk gyűjtése történik a vizsgálandó eseményről, a vizsgálati tárgyról, a környezetről. Ide tartozhatnak például az időpontok, érintettek (pl.: járművezető), a jármű típusa, kommunikációs csatornák. Az előzetes információk alapján lehetőség nyílik az adott vizsgálat megtervezésére, a vizsgálati stratégia kialakítására. Tervezési szempontok közé tartoznak a vizsgálati célok és kérdések, a nyomok forrása és megbízhatósága, az idővonal (nyomok összegyűjtési sorrendjének meghatározása) és a szükséges technikák, taktikák, módszerek és eszközök is.

Az adatgyűjtés lépésben két eljárást követnek a hálózatok vizsgálata során:

- Catch it as you can, - a teljes hálózati forgalom rögzítése,
- Stop, look and listen – a gyanúsnak tűnő forgalom rögzítése.

Catch it as you can eljárás során a teljes forgalom rögzítése biztosítja, hogy ne maradjanak ki fontos hálózati események. A Stop, look and listen eljárás során az adatforgalomnak csak a monitorozása történik meg és azok a forgalmak kerülnek rögzítésre, amelyek valamilyen szempontból gyanúsnak tartanak és további vizsgálatuk szükséges.[288] Járművek esetén jellemzően utólagos vizsgálatok kerülnek elvégzésre, ezért ezek a megoldások nem, vagy csak kevés esetben végezhetőek el. A forgalmi adatok mellett, járművek vizsgálata során nagyobb szerepet kapnak a belső és külső kommunikációért felelős vezérlő egységek, gateway-ek és ezek naplóállományai. Az elemzési fázisban a rögzített nyomok vizsgálata történik. Ide tartozik a hálózati keretek azonosítása és egymástól való elkülönítése, valamint a keretek belső szerkezetének és tartalmának feltárása, az adatok értelmezése. „A protokoll információk dekódolása, a hálózati protokoll hierarchia „visszafejtése” és az átvitt adatok […] összeállítása, a hálózati események időbeli sorrendjének rekonstruálása”. [86][144][184][198][206][248][288]

A network forensics főbb lépéseinek vizsgálat alapján megállapítható, hogy a modern járművekhez kapcsolódóan a főbb vizsgálati lépések (pl.: adatgyűjtés, elemzés) alkalmazhatóak lesznek a járművek kommunikációjának vizsgálata során. Emellett megállapítható, hogy a vizsgálati kihívásokat is figyelembe véve, a Network forensics-ben használt vizsgálati stratégia lépés implementálandó a készülő modern járművek szakértői vizsgálati módszertanába.

Mobil telefonok széleskörű elterjedésével mára szinte mindenki magánál tartja saját eszközét. Az emberiség közel 70 %-a mobile felhasználó, az életünk jó részét online jelenlétben töltjük. A világszerte több milliárd mobil előfizető, az exabyte-ban mérhető mobil internet forgalom, az eszköz funkciók számának növekedésével és az egyre nagyobb teljesítménynek köszönhetően a digitális forenzikus vizsgálatok egyik legjelentősebb adatforrásává váltak. Nem csupán előnyt, kihívást is jelent az ilyen vizsgálatokkal foglalkozók számára, a technológia gyors változása, a vezetéknélküli kommunikációs technológiák, szabadalmaztatott interfészei, mobile platformok, stb. kapcsán. Definíció szerint a **Mobile Forensics** a mobil eszközökön vizsgálata és elemzése, a tárolt információk azonosítása, gyűjtése, vizsgálata és elemzése.[44][133][135][148][214][215][300] Ezek a vizsgálati lépések megjelennek egyéb forenzikus domainek esetén is, mint fő lépések, járművek esetén ezek tartalmi mélysége és az alkalmazott technikák térnek el.

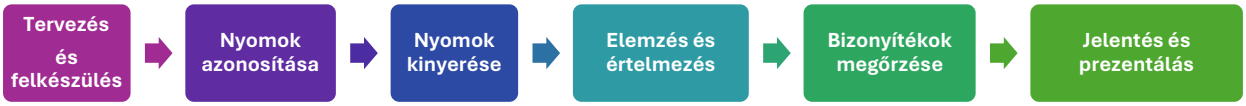
A növekvő számú, elektronikus eszközökkel elkövetett jogszerűtlen cselekmények és az információs rendszerekben kezelt, adatbázisokban tárolt kritikus adatok kapcsán az adatbázis forenzikus vizsgálatok (**Databasa Forensics**) egy feltörekvő, fejlődő terület.[44][123] A rendszerekben keletkező nagy mennyiségű adatokkal kapcsolatban kiemelt szempont az elvégzett műveletek (pl.: módosítás, komromittálódás, stb.) visszakövetése, sérült vagy törölt adatbázisok rekonstruálása. Az adatbázis forenzikus vizsgálatok feladata az adatbázisok tartalmának, a kapcsolódó metaadatok vizsgálata, az adatbázishoz kapcsolódó incidensek azonosítása, kapcsolódó információk elemzése és rekonstruálása.[14][15][135] A járművekhez kapcsolódó vizsgálatok esetén az adatbázisok vizsgálata kiemelt feladat, hiszen az egyik vizsgálati kihívás maga a nagy mennyiségű adat és annak értelmezése, a releváns nyomok kinyerése.

Az elmúlt több, mint egy évtized egyik legelterjedtebb számítástechnikai fogalma a felhő (cloud), a felhő alapú rendszerek volt. Napjainkra az autógyártók is széles körben támaszkodnak az ilyen megoldásokra, szinte minden új autótípushoz elérhető az online elérés, a mobiltelefonos applikáció segítségével történő hozzáférés. Egy olyan megoldásban, ami lehetővé teszi, hogy kényelmesen, bárhonnan, igény szerinti erőforrásokhoz férhessünk hozzá, a járművek szenzorai által gyűjtött, a járműben feldolgozott, tárolt és továbbított adatok széles tárháza jelenik meg. Felhasználói oldalról a rugalmasság mellett olyan kihívások jelennek meg például, mint a komplexitás, az az átláthatóság, a biztonság, auditálás hiánya. Míg a szolgáltatói oldalon például a biztonsági kihívások, magas költségek, szolgáltatások integrálásának nehézségei állnak. A felhő alapú rendszerek főbb biztonsági fenyegetéseit az adatszivárgás és

adatvesztés, a fiókok kompromittálása, a nem kellően biztonságos API-k (Application Programming Interface - alkalmazásprogramozási interfész), a DoS támadások és a megosztott technológia problémái állnak. A felhő alapú rendszerek szakértői vizsgálata, a **Cloud Forensics**, a felhő alapú rendszerekben található digitális információk (elektronikus adatok) azonosításához, gyűjtéséhez, megőrzéséhez, vizsgálatához, elemzéséhez a tudomány és a műszaki fejlődés eredményeit használja fel. A Cloud Security Alliance (CSA, 2013) meghatározása alapján bizonyítékként szolgálhatnak például a felhőben található webszerver napló állományok, alkalmazás szerver és adatbázis naplók, hozzáférési naplók, virtualizációs és vendég operációs rendszerek naplói, hálózati forgalmak, DNS szerver naplók, API logok, számlázási információk, stb.[71][78][176][185][209][213]

Definíció szerint a Cloud forensics, vagyis felhő alapú rendszerek szakértői vizsgálata a digitális forensics alkalmazása felhő környezetekben, ahol virtuális szerverek és hálózatok, „vékony" és „vastag" kliensek[2], távoli elérések stb. vizsgálata történik, a szükséges bizonyítékokhoz való hozzáférés érdekében.

A felhő alapú rendszerek forenzikus vizsgálatának szakirodalomban meghatározott lépései megegyeznek a számítógépes forenzikus vizsgálatok lépéseivel. Figyelembe véve, hogy a felhő alapú rendszerek is informatikai erőforrások, csupán nem helyben, saját eszközünkön érjük el azokat, hanem távoli hozzáféréssel „más valaki számítógépéhez", szerveréhez csatlakozunk, a sztenderd vizsgálati lépések alkalmazhatóak, csupán az eszközök, technikák változtatására lehet szükség.[71][78][176][184]



23. ábra Felhő alapú rendszerek forenzikus vizsgálatának lépései

A járművekhez kapcsolódó különböző felhőszolgáltatásokban tárolt adatok hasznos nyomoknak bizonyulhatnak egy esemény, bűncselekmény vagy incidens kivizsgálása során.

---

[2] A kliens olyan alkalmazás vagy rendszer, amely egy távoli szolgáltatást egy másik számítógépről, a szerverről kéri le a hálózat segítségével. A böngészők maguk is olyan kliensek, amelyek a webszerverekhez csatlakozva képesek megjeleníteni az egyes weboldalak tartalmát. A klienseknek három fajtája van:
a *vastag kliens* (fat client) önállóan is képes működni anélkül, hogy csatlakozna egy szerverhez (asztali számítógép, notebook);
a *vékony kliens* (thin client) nem képes szerver nélkül működni, saját funkciója csupán annyi, hogy grafikusan megjeleníti a szerverről érkező adatokat;
a hibrid kliens képes önálló működésre, ugyanakkor adatbázisait a szerveren tárolja.

Ilyen adatok lehetnek a navigációs előzmények, útvonalak, a jármű sebességével kapcsolatos adatok, kamera és szenzor adatok, telemetriai információk, a tárolt időbélyegek és metaadatok, melyek segíthetnek az események idővonalának meghatározása során.[71][78][176][185][255]

A felhő alapú rendszerek vizsgálati eljárása, annak egyes vizsgálati lépéseivel kapcsolatban megállapítható, hogy a modern járművek vizsgálata során figyelembe vehetőek és alkalmazhatóak.[254]

Míg korábban a járművek vizsgálatában a **Vehicle forensics** jellemzően fizikai evidenciák (pl.: ujjlenyomat, egyéb nyomanyagok) összegyűjtésére és a jármű fizikai vizsgálatára vonatkozott, a járművek egyre intelligensebbé válásával megjelent a járművekhez kapcsolódó Digital Vehicle Forensics: a digitális forenzika egyik kialakulóban lévő ága, amely a jármű moduljaiban, hálózataiban és operációs rendszerében található digitális bizonyítékok vagy adatok visszaszerzésével foglalkozik.[277] Ez a terület a járművek útvonalával, úticéljával, különböző menetinformációk megismerésével járul hozzá a szakértői vizsgálatok sikeréhez. Mivel a vezetők az infotainment rendszer által kerülnek kapcsolatba a járművel, szinkronizálják mobil telefonjuk adatait, személyre szabják egyes funkcióikat, a jármű nagy mennyiségű információval rendelkezik a felhasználóról.[10][277] Figyelembe véve a járművek által hozzáférhető, visszaállítható, kinyerhető és vizsgálható információk széles körét, Kevin Klaus, Gomez Buquerin és társai, a „*A generalized approach to automotive forensics*” tanulmányukban már Automotive forensics-nek nevezik a vizsgálatot, azonban a fogalom még nem alkalmazott széles körben.[121][207][268]

Az intelligens járművek térnyerésének alapvető elemei az IoT és különböző kiber-fizikai eszközök, szenzorok, környezetek, amelyek utólagos igazságügyi szakértői vizsgálata nélkülözhetetlen eleme az események rekonstruálásának. Az **IoT Forensics**, vagyis az IoT eszközök vizsgálatának célja az IoT-vel kapcsolatos események, az internetes csatlakozással rendelkező eszközök, szenzorok által előállított, továbbított és tárolt adatok forrásainak megállapítása, az adatok azonosítása, begyűjtése, vizsgálata. Az IoT forensics terület magába foglalja a különböző IoT eszközökből származó digitális bizonyítékok széles skálájának megszerzését, megőrzését és elemzését, a kapcsolódó alkalmazásokat, az internetet és a felhő alapú technológiát, magukat az eszközöket és más kapcsolódó rendszereket, amelyek az IoT ökoszisztéma (polgári vagy katonai) részeként működhetnek.[88][118][152][189]

Az IoT vizsgálatok vonatkozásában három vizsgálati szintet különböztetünk meg, amely a modern és egyre inkább önvezetővé váló járművek vizsgálata esetén is figyelembe vételre kell kerüljenek:

- eszköz szintű vizsgálat,
- hálózati szintű vizsgálat,
- felhő alapú szakértői vizsgálat.[22]

24. ábra Az IoT szakértői vizsgálat három szintje (A szerző szerkesztése [154] alapján)

Eszköz szintű vizsgálatok esetén, elsődleges bizonyíték forrásként maga az IoT eszköz szerepel. Az IoT eszközök szakértői vizsgálatba számos eszköz bevonható, például érzékelők, egészségügyi implantátumok, nyomkövető eszközök, intelligens mérők, okos háztartási készülékek, okoskamerák, hálózatba kapcsolt járművek és drónok. Mivel az eszközök hardverükben és funkcióikban különböznek egymástól, a bizonyítékok azonosítása és megszerzése gyakran nagy kihívást jelent, és nem mindig kivitelezhető.[153]

Hálózati szintű vizsgálatok esetén az IoT-eszközöket egymással összekötő különféle kommunikációs hálózatok eseményeinek vizsgálata történik. Ez a hálózati forgalom, az információk és események begyűjtése, rögzítése és elemzése annak érdekében, hogy egy hálózat elleni támadás forrása megállapítható legyen, egy behatolás észlelésére és vizsgálatára kerülhessen sor.[9][178][197][222]

A felhő alapú megoldások elterjedésével digitális átalakulás történik. Mivel az IoT-eszközök korlátozott adattárolási és feldolgozási képességekkel rendelkeznek, az általuk generált

adatokat vagy annak egy részét továbbítják egy felhő szolgáltatáshoz további feldolgozás és tárolás céljából, így a felhő a szakértői vizsgálati folyamat egyik fő részévé válik.[22][121][185][275][276][282]

Az IoT forensics módszertan célját, lépéseit áttekintve megállapítottam, hogy mivel a járművek tekinthetőek komplex IoT rendszerekként, a modern és egyre inkább önvezetővé váló járművek esetén az IoT eszközök vizsgálati lépései alkalmazhatók, különös tekintettel az eszközök és adatok feltérképezésére. Az alkalmazott eszközök tekintetében azonban a járművek esetén komplexebb eszközök és hozzáférési módok szükségesek egy vizsgálat elvégzéséhez. Az IoT-hez kapcsolódó szakértői vizsgálati szintek (eszköz, hálózati, felhő szint) a modern járművekben is megjelennek, járművek vizsgálata esetén is különbséget kell tenni az eszköz szintű, hálózati szintű vizsgálat, és a felhő alapú megoldások vizsgálatában. Ezen szintek adatforrásainak és adatainak elemzése ezen járművek esetén is elengedhetetlen.[262]

A drónokkal kapcsolatos szakértői vizsgálatok (**Drone Forensics**) elvégzése komplex feladat, melynek egyik célja egy esemény idővonalának rekonstruálása, nyomok rögzítése és elemzése. A vizsgálatok három fő kategóriába sorolhatóak. Az első kategóriába az érintett személyek (elkövető, sértett) és az irányítás módjának azonosítása tartozik. A második kategória a repülési adatok elemzése, harmadik kategória az adathordozón található adatokhoz történő fizikai és logikai hozzáférés.

Jellegénél fogva a büntetőeljárásról szóló 2017. évi XC. törvény. 204. §-a szerinti tárgyi bizonyítási eszközként értékelhető lényegében mind a pilóta nélküli légijármű, mind pedig az általa szolgáltatott bizonyíték. Ennek kapcsán jelentősége van a Be. 204. § (2) bekezdésében foglalt kiterjesztő értelmezésnek, miszerint irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Az (1) bekezdés alapján az irat tárgyi bizonyítási eszköz, így nem vitás, hogy ilyennek minősül a pilóta nélküli légijármű is.[75][118][264] Mint eszköz, a járműhöz hasonlóan figyelembe vehető egy eljárás során, emellett a drónok adattároló megoldása (memóriakártyás adattárolás) hasonlóságot mutat egyes járműgyártók tárolási megoldásával, akik szintén a jármű fejegységében lévő memóriakártyát használják adattárolásra. Ennek fényében a drónok vizsgálati eljárása is implementálható a modern járművek vizsgálati módszertanába.

A modern és egyre inkább autonómmá váló járművek nem csupán az „általános” jármű állapot információkat, csatlakoztatott eszköz információkat, navigációs adatokat, hívás naplókat, képeket és videókat fogják megőrizni és feldolgozni. A jelenleginél is nagyobb mennyiségű

információval fognak rendelkezni a környezetükről, a környezetükben található környezeti és pálya elemekről, a közelükben lévő járművekről, gyalogosokról, vagyis a kooperatív intelligen közlekedési rendszerekről, résztvevőiről és szolgáltatásairól. Ezen információkhoz való hozzáférés, az adatok kinyerése, feldolgozása, elemzése nem valósítható meg a Digital Forensics standard eljárásaival, módszertanának alkalmazásával. Új megközelítés, eszközök, technológia és módszertanok kidolgozása és alkalmazása szükséges, figyelembe véve a fent is felsorolt forenzikus domain-ek sajátosságait. Álláspontom szerint számítógépek forenzikus vizsgálata után a következő nagy potenciális hatású domain lehet az autonóm járművekre vonatkozó vizsgálati módszer és kapcsolódó eljárások, vagyis az **Autonomous Vehicles Forensics**. Kutatásom eredményeként, a releváns digital forensics domainek vizsgálata alapján meghatároztam az Autonomous Vehicles Forensics szakmai definícióját és módszertani leírását.

Definíció szerint az autonóm járművek forenzikus vizsgálata a digital forensics egyik új ága, amely az „*önvezető járművekben és a kooperatív intelligens közlekedési rendszerekben tárolt adatok azonosítására, megszerzésére, feldolgozására, elemzésére és jelentéskészítésére összpontosít*” [248], alapul véve a számítógépek, hálózatok, IoT eszközök, drónok vizsgálati módszertanait. Segítségével rekonstruálhatóak lesznek olyan események, amelyben a jármű a támadás célpontja, a jármű eszköz a bűncselekmény végrehajtásához, jármű és/vagy a közlekedési rendszer tartalmazza a bizonyítékul szolgáló elektronikus nyomot.[268]

Az Autonomous Vehicles Forensics szinte kivétel nélkül felhasználja és egyesíti a Digital Forensics egyes területeit és módszertani alapjául szolgál a Digital Vehicles Forensics. Mivel a vizsgálatok tárgya alapvetően a modern járművek lesznek, a Digital Vehicle és Automotive Forensics-re került kialakításra ezen új forenzikus domain.

Modern járművek, mint adatforrások a szakértői vizsgálatokban

A járművekhez kapcsolódó, utólagos szakértői vizsgálatok a járművek folyamatos fejlődése (gyártók egyre inkább elmozdulnak a funkcióktól a szolgáltatások irányába), szoftver orientálttá való alakulása, a belső struktúra változása okán új eszközöket, módszereket és folyamatokat igényel. Függetlenül attól, hogy milyen egység és milyen adattárolási módot alkalmaz a gyártó az egyes járművekben, a nyomok sértetlensége a teljes vizsgálati folyamatban kiemelten fontos. A balesetek, vagy egyéb járművel kapcsolatos események vizsgálata során több belső adatforrást, a bennük tárolt adatokat is figyelembe kell venni, ennek érdekében meghatároztam az ilyen vizsgálatokhoz kapcsolódóan a járművekben releváns adatforrásokat.

Eseményadat-rögzítő és adatai

A balesetek utólagos vizsgálata esetén az egyik elsődleges adatforrásként az eseményadat-rögzítő, az EDR szolgál, melyek az új járművekbe – az (EU) 2022/545 számú rendelete alapján – kötelezően kerülnek beépítésre. Az EDR koncepciója szerint a berendezés a valós időben keletkezett adatokat illékony adattároló egységen egy előre meghatározott ideig tárolja. Az adatokat valamely előre meghatározott feltétel bekövetkezése (pl. légzsák aktiválása vagy ütközés miatt bekövetkező hirtelen lassulás) esetén automatikusan a beépített adathordozójára továbbítja. Az illékony adattárolási technológia lehetővé teszi az adatok folyamatos frissítését, az elavult információk folyamatos és gyors felülírását, amennyiben a fent említett feltétel nem következik be. A technológia segítségével az EDR rögzíti – a jármű különböző szenzoraiból származó – az ütközés előtt, a baleset során és azután keletkezett, az utólagos kivizsgálás szempontjából releváns adatokat (pl. a jármű ütközéskori sebességét, a motor fordulatszámát, a fékezési információkat, a jármű összes biztonsági rendszerének állapotát). A készülék segítségével – a repülőgépek fekete dobozához hasonlóan – a balesetet követő vizsgálat során a szakértő és az eljáró hatóság rendkívül pontos képet kap a baleset körülményeiről.

Az EDR – Event Data Recorder alkalmazásának célja, az (EU) 2022/545 számú rendelete alapján „*az, hogy röviddel ütközés előtt, ütközéskor és közvetlenül az ütközést követően az ütközés szempontjából kritikus adatokat és információkat rögzítse és tárolja annak érdekében, hogy a balesetekkel kapcsolatban pontosabb, részletesebb adatok álljanak rendelkezésre*”.

Az eseményadat-rögzítők tehát olyan eszközök, amelyek rögzítik a járművek műszaki paramétereit, jellemzően baleset vagy ütközésközeli esemény előtt, közben és után.

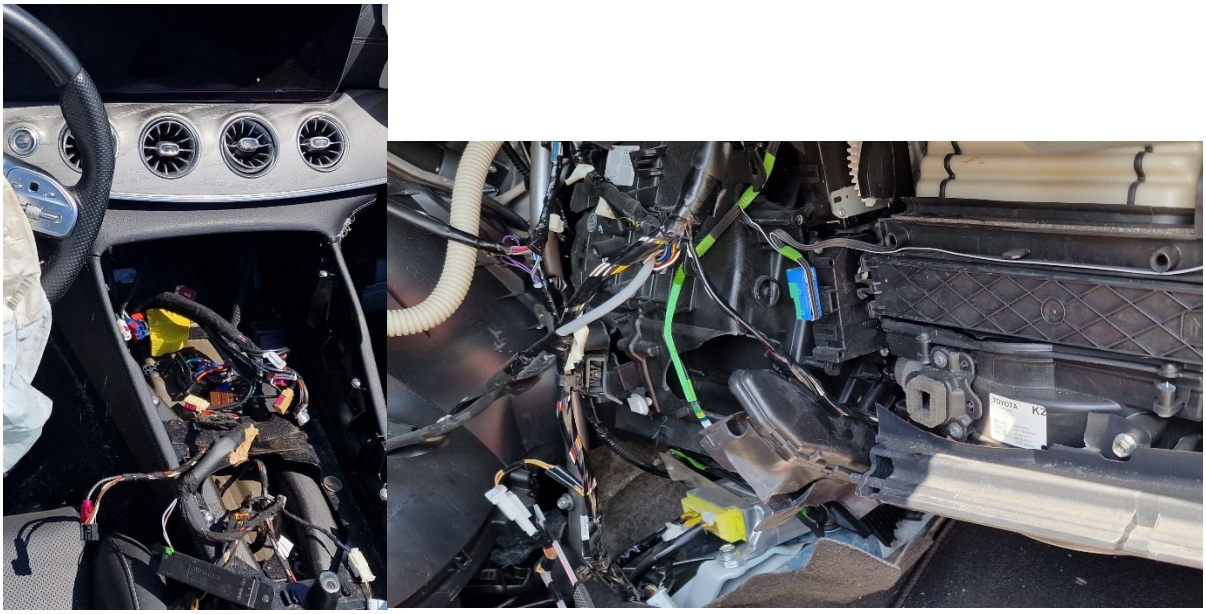
Személygépjárművek, SUV-k esetén ezeket az adatokat a légzsák vezérlő (Air Bag Control Module - ACM) tartalmazza. Az eseményt az EDR általában a jármű túlzott lassulásával detektálja, ehhez elég egy erős fékezés is, ilyen esetben nem mindig következik be baleset. Tehergépjárművek esetén a motorvezérlő egységben (Engine Control Module - ECM) találhatóak. Az ECM szabályozza a motor teljesítményt, a károsanyag-kibocsátást az üzemanyag-felhasználást stb. és rögzíti a biztonsággal összefüggő adatokat is.[34][109][309]

Az EDR által rögzített adatok folyamatosan frissülnek és az ideiglenes memóriában tárolódnak a légzsákok kioldásáig, melynek hatására adatok az állandó memóriába kerülnek, amelyből visszakereshető marad.[170] Anonimizált módon tartalmazza a jármű sebességét, a motor fordulatszámát a baleset időpontjában, a fékezési információkat, a jármű pozícióját és dőlését az úton, a jármű összes biztonsági rendszerének állapotát és aktiválási sebességét, a járműbe épített eCall rendszer jelzését, a fék aktiválását és a releváns bemeneti jellemzőit a fedélzeti aktív biztonsági és balesetelhárító rendszereknek. A rendszer utasbiztonsághoz kapcsolódóan is gyűjt adatokat például a biztonsági öv, légzsákok státusza. Ezeket az információkat egyre gyakrabban használják fel tárgyi bizonyítékok kiegészítésére baleset rekonstruálása érdekében.[34][109][126]

Az EDR-ben tárolt eseményadatokhoz történő hozzáféréshez, kinyerésre azonban nem állnak rendelkezésre szabványosított kommunikációs protokollok. Jelenleg a járműgyártók adnak tájékoztatást arról, hogy milyen módon férhetőek hozzá és értelmezhetőek ezen adatok. A lekérdezése az alkalmazott módszerek licensszel védettek. Meghatározott gyártók (például: GM, Ford, Chrysler és bizonyos partnerei) és a Bosch által használhatóak. A Hexadecimális Fordító eszközöket (HTT- Hex To Text) az EDR gyártók készítik el. A Bosch 2008. óta gyártja a Crash Data Retrieval Tool (CDR) eszközt, ami az egyetlen olyan nyilvánosan elérhető, harmadik féltől származó (nem gyártói) eszköz, amely képes az EDR-ekben tárolt adatok kinyerésére és értelmezésére.[263]

A járművek fedélzeti diagnosztikai rendszercsatlakozóján (OBD-II) keresztül, vagy közvetlenül a baleseti adatok biztonságos tárolását végző ECU-hoz (például légzsákvezérlő) csatlakozva lehetőség van olyan a balesetet megelőző, a jármű működéséhez kapcsolódó információk kiolvasására, mint a jármű sebessége, a motor fordulatszáma, a fék státusza, az ütközéshez kapcsolódó sebességváltozás (delta-V), stb.[73] Balesetekhez kapcsolódó vizsgálatokban a járművek jellemzően működésképtelenek, nem helyezhetőek feszültség alá, ezért az EDR-hez (event data recorder) offline módon kell hozzáférni. Attól függően, hogy mely gyártóhoz tartozik a jármű, a vezérlő a középkonzolban, a vezető vagy utas lábterében, a kesztyűtartó

mögött, stb. található meg. A jármű állapotától függően a fizikai hozzáférés is jelenthet problémát.



25. ábra EDR egység elhelyezkedése a jármű középkonzoljában

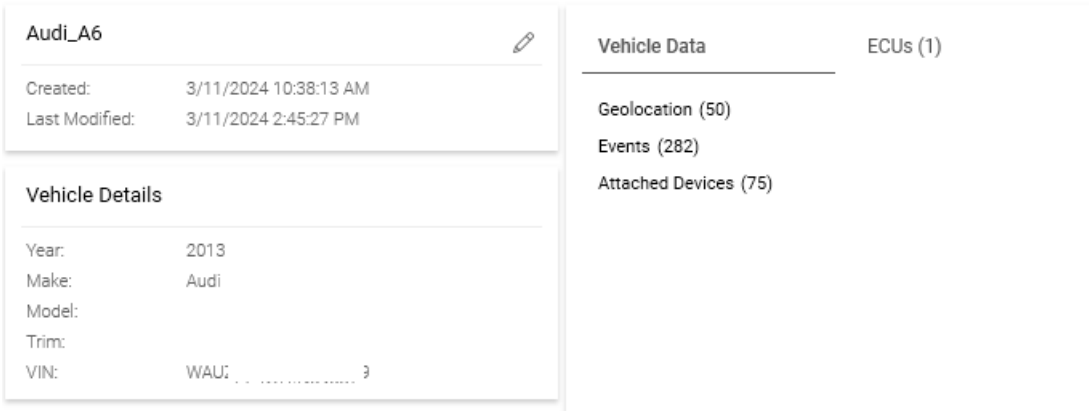
Jármű központi egység, fejegység és adatai

Bár az EDR-ek fontos adatforrásként jelennek meg egy esemény, baleset körülményeinek a szakértői vizsgálatakor, a vezérlőegységek számának növekedése, az egyre inkább önvezetővé váló járművek fejlődésével párosulva, egyre inkább szerepet kapnak a jármű központi egységek (fejegységek), telematikai-infotainment rendszerek és a bennük tárolt adatok, számos lehetőséget és kihívást jelentve a vizsgálatot elvégző szakembereknek. Az elérhető adatok mennyisége és a „választék”, az adatok köre folyamatosan növekszik és egyre fontosabbá válnak. A vizsgálatok folyamatára és eredményeire egyre nagyobb hatást gyakorolnak, mivel az összes gyártó beépít már valamilyen szintű beágyazott rendszert új járműveibe, melyek egyre több járművön belüli és azon kívüli kapcsolattal fognak rendelkezni. Ahogy a magas automatizáltságú és egyre inkább önvezető járművek aránya a napi közlekedésben növekszik, úgy fog emelkedni az ellenük elkövetett bűncselekmények, vagy az olyan balesetek száma, mely során az ilyen jármű kerül konfliktusba, vagy ütközik emberi vezető által irányított autóval. Egyre gyakoribbá válhatnak az járműrendszerek elleni támadások, valamint a járművek távoli táveltérítése, irányítása is. Az ilyen bűncselekmények során keletkező adatok megszerzése és elemzése kulcsfontosságú lesz a szakértők számára.[332]

A központi egységekben tárolt adatok mennyisége és forrása gyártónként eltérő, esetenként a járműmodellek vagy gyártási évek között is lehetnek különbségek. Tárolásra kerülnek a

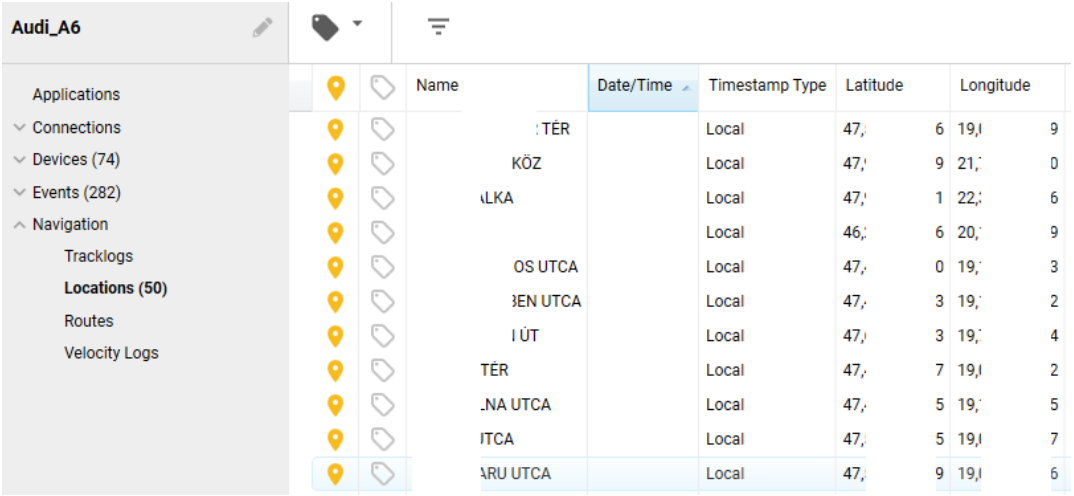
járműben található vezérlő egységek ECU-k azonosító adatai (például sorozatszám, frissítési és újraindítási információk, szoftver verzió, gyártási számok), vagy a járműhöz vezetékes vagy vezeték nélküli módon csatlakoztatott eszközök adatai (például USB eszköz, SD-kártya, mobiltelefon stb.), navigációs adatok (például útvonal, korábbi úti célok stb.), eszközinformációk és a jármű működési eseményei (például indítás, leállítás, sebességváltás, gyorsítás, fékezés stb.). A járművekre, vezérlő egységekre vonatkozó általános információk lehetnek:

- jármű gyártója,
- motorszám/kód,
- hengerűrtartalom,
- teljesítmény,
- üzemanyag,
- környezetvédelmi osztály,
- vezérlő egység neve,
- vezérlő egyedi azonosító típusa,
- vezérlő egyedi azonosító száma,
- sorszáma
- alváz szám,
- évjárat,
- jármű típusa,
- jármű felszereltsége.



26. ábra Vizsgált járműben elérhető navigációs, esemény és csatlakoztatott eszköz adatok megjelenítése

A csatlakoztatott eszközről olyan adatokat tárol a rendszer, mint például az eszköz neve, gyártója, interfész típusa és az eszköz egyedi száma vagy MAC-címe. A GPS és a jármű működési eseményadatok tartalmazzák a navigációs adatokat minden rögzített eseményhez, valamint a jármű pontos helyzetét. Részletes információk ismerhetőek meg az aktív és inaktív útvonalakról, mentett helyekről, korábbi úticélokról, ezekhez megőrzésre kerül dátum, idő, város- és utcanév is.



27. ábra Járműben rögzített navigációs adatok

Ezek az információk egy szakértői vizsgálat során felhasználhatóak egy esemény vagy eseménysorozat idővonalának létrehozásához, helyszíneinek és az érintett személyek meghatározásához.[40][97][265]

Key Fobs - távirányítók

Egyes források szerint a járművek távirányítói is egyre több digitális bizonyítékot tartalmaznak, potenciális adatforrássá válhatnak. Ezek a kulcsrendszerek a vizsgálathoz kapcsolódóan tárolhatnak hasznos információt, mint például a jármű azonosítót, kulcs ID-t, idő- és dátumbélyegzőket, kilométeróra állást, vagy éppen a kulcs utolsó használati időpontját.[37]

Egyéb adatforrások

A jármű által érzékelt, szerzett, rögzített információk mellett a közlekedési rendszerek fejlődésével egyre több külső adatforrás is elérhetővé válik/válhat a szakértői vizsgálatok elvégzéséhez. A kooperatív intelligens közlekedési rendszerek által a környezeti elemekből, pályaelemekből is rendelkezésre állnak információk, amelyek az adott üzemeltető, hatóság által válnak hozzáférhetővé, vizsgálhatóvá.

A keréknyomás ellenőrzését végző TPMS (Tire Pressure Monitoring Systems) szenzor jeleinek élő nyomon követése, rögzítése a szakértői vizsgálatok szempontjából és katonai műveletek vonatkozásában nem releváns. Utóbbi esetben azonban a jármű működésének kompromittálásában, téves információk adatforgalomba illesztéssel, a TPMS szenzor azonosítója általi nyomon követéssel kapcsolatban, vagy az ECU meghibásodásának elérésével befolyásolható a jármű működése. A vizsgálatok esetén az ilyen beavatkozások nyomainak felderítése is lehet az egyik cél.

A különböző kooperatív intelligens közlekedési rendszer elemek, szolgáltatások, cloud megoldások, azok szolgáltatói, a járművekkel kapcsolatban álló szerverek és alkalmazások naplói kiegészítő információt jelenthetnek az egyes vizsgálatokhoz. A különböző telekommunikációs rendszer és szolgáltatói naplók napjainkban is elérhetőek a jogosult szervezetek számára, ezek szerepe a járművek önálló kommunikációs csatornáinak elterjedésével még hangsúlyosabbá válnak a jövőben. Bár ezek a járművön kívüli, külső adatforrások javítják a vizsgálatok teljesítményét, hatékonyságát, az adatok hozzáférhetősége, begyűjtési lehetőségei, tulajdonjoga új kihívásokat jelentenek.[214]

2. Modern járművek szakértői vizsgálatának kihívásai

A digitális információk járművekből történő begyűjtése, új kihívás elé állítja a polgári és katonai nyomozati és igazságszolgáltatási tevékenységeket támogató, digitális forenzikus vizsgálatot végző szakértőket. A közlekedési ökoszisztémában alkalmazott összetett informatikai és infokommunikációs rendszerek miatt, valamint a járművek által gyűjtött és feldolgozott adatmennyiség közel exponenciális növekedésének eredményeként a már meglévő szakértői vizsgálati eljárások nem, vagy csak korlátozott módon lesznek alkalmazhatók.[262]

A járműelektronika megjelenésével megkezdődött a járművek adatainak egyre szélesebb körű felhasználása. Kezdetben az adatok működéshez kapcsolódó, eseti jellegű vizsgálatán kívül (például motorvezérlés, légzsák, klímavezérlés, ABS-adatok ellenőrzése, a hibatárolók adatainak kiolvasása) nem voltak összetett vizsgálatok. Komplex vizsgálatok a járművek központi egységének/fejegyégének fejlesztésével, a járművek hálózati komplexitásának növelésével jelentek meg. A navigáció adatok járművekben való megjelenése és a mobil eszközökkel való kapcsolat kialakítása révén megjelentek olyan mennyiségű és minőségű információk is melyek egyre nagyobb szerepet kaptak a szakértői vizsgálatok elvégzése során. A modern járművekhez kapcsolódóan kidolgozandó vizsgálati módszertan elkészítéséhez

meghatároztam azon kihívásokat, melyekre az új módszertannak lehetőség szerint válaszolnia kell.

A modern járművek szakértői vizsgálati kihívásai három csoportba sorolhatóak:

- általános kihívások,
- vizsgálati eljárás kihívásai,
- vizsgáló eszköz kihívásai.[267]

Modern járművek szakértői vizsgálatának általános kihívásai

A modern járművek szakértői vizsgálatának elvégzésének egyik általános kihívása, hogy mára a járművek által hozzáférhető adatok forrása is megváltozott, valamint nem garantált, hogy egy vizsgálat lefolytatásához, a vizsgálat céljának eléréséhez elegendőek a járműben elérhető adatok. A forrás lehet:

- a jármű saját szenzorhálózata,
- a V2X kommunikáció által hozzáférhető egyéb jármű, infrastruktúra rendszerek,
- a különböző felhő alapú rendszerek (például gyártói felhő [cloud], szolgáltatói felhő [cloud]),
- közúthálózat üzemeltetői informatikai rendszere, stb.

További általános kihívásként jelentkezik, hogy a járművekben található digitális adatok típusa és forrása különböző lehet. A számítógépek szakértői vizsgálatától eltérően nem elégséges az adathordozók begyűjtése, esetenként a memóriában található adatok mentése. A járművek több, logikailag (és fizikailag) elkülönített alrendszerben is tárolhatnak információt:

- magáról a járműről (például sorozatszám, alkatrész azonosítók, kulcs ID stb.),
- a telepített alkalmazásokról (például navigáció, Facebook stb.),
- a csatlakoztatott eszközökről (például USB-meghajtók, SD-kártyák, vezeték nélküli hozzáférési pont stb.),
- a navigációról (például előzmények, mentett helyek, korábbi úticélok stb.),
- csatlakoztatott mobil eszközökről (például eszköz azonosító, híváslista, kontaktok, SMS-üzenetek, képek, hangok stb.),
- egyéb működési eseményekről (például ajtó nyitás/zárás, világítás be-/kikapcsolás, Bluetooth kapcsolatok, WiFi-kapcsolatok, sebesség, kormányszög, kilométeróra állás, sebességváltás, erős gyorsítás-lassítás, vezetői figyelmeztetések stb.).[268]

A járművek adataihoz való hozzáférés nem oldható meg centralizáltan, több egység, alrendszer elérése szükséges hozzá. Több hozzáférési megoldás/csatorna állhat rendelkezésre, az ezeken keresztül elért adatok nem azonosak. Hozzáférési csatornák lehetnek:

- vezetékes kommunikációs csatlakozók, pl.: USB-port,
- vezeték nélküli kommunikációs megoldások, pl.: WiFi, Bluetooth,
- OBD-II járműdiagnosztikai port,
- JTAG (Joint Test Action Group), standard teszt port és architektúra, amely segítségével kapcsolatot alakítható ki a jármű egyes vezérlő egységeivel),
- belső hálózatok (LIN - Local Interconnect Network, CAN - Controller Area Network, FlexRay, Automotive Ethernet, MOST - Media Oriented Systems Transport, stb.),
- memóriakártya foglalat (egyes gyártók a jármű teljes adatstruktúráját memóriakártyán tárolják),
- chip-off (a jármű egyes vezérlőinek vagy a központi egységének memória chip-jeinek kiszedését és tesztpanelen történő vizsgálatát jelenti).
- EVSE - Electric Vehicle Supply Equipment, elektromos járművek töltő csatlakozója

A járművek többféle csatornát használnak környezetükkel való kommunikációra. Ilyenek például a vezeték nélküli alapú technológiák. A szélessávú kommunikáció széleskörű felhasználást eredményez. Vezeték nélküli csatlakozási lehetőségek a járművekhez:

- Bluetooth, Bluetooth low energy,
- WiFi,
- RFID - Radio Frequency Identification,
- DSRC - Dedicated Short Range Communications, járművek kis hatótávú, WiFi-hez hasonló kommunikációs megoldása,
- V2X - Vehicle to Everything, mobilkommunikációs technológián alapul, a járművek és környezetük közötti kommunikációt valósítja meg,
- elektronikus vezérlő egységek (ECU),
- GPS – Global Positioning System,
- TPMS - Tire-pressure monitoring system, 314.9-433.92 MHz közötti frekvencián történő kommunikáció,
- infotainment/fejegység (head unit/central unit), gyártói eredeti vagy utángyártott konzolrendszer, ami a járművezető és az utasok számára járműspecifikus információkat, navigációt, önálló vagy integrált alkalmazásokat és/vagy multimédiás lehetőségeket - beleértve az audiót és videót - nyújtson.[302]

- NFC – Near Field Communication,
- VSM – Vehicle Security Module, olyan a CAN hálózatra csatlakoztatott járműbiztonsági rendszer, amely meghatározott szabályrendszer alapján különbséget tehet az OBD-II csatlakozón keresztül bevitt engedélyezett és jogosulatlan jelek között. Az engedélyezett jelek továbbításra kerülnek a CAN hálózatra, például a diagnosztikai és nyomkövető eszközök vagy hardverkulcs stb. jelei.[301]
- OTA – Over The Air, vezeték nélküli hálózaton keresztüli szoftver, firmware frissítésre szolgál.[242][250][267]

Az adatok forrásául szolgálhatnak például felejtő (Volatile) és nem felejtő (Non-volatile) memóriák; a jármű flash memóriája, memóriakártya, SIM-kártya, alkalmazások adatai, vezérlő egységek adatai, stb.[244] A tárolt adatok pedig megjelenhetnek például a(z):

- Event Data Recorders (EDR)-ben,
- navigációs/infotainment rendszerben,
- kommunikációs modul,
- jármű központi egységben/fejegységben,
- mobil vagy beépített fedélzeti kamera (első és hátsó, vagy 360°-os) adattároló képességgel,
- elektornikus vezérlő egységekben (Electronic Control Unit, ECU).

Az adatok tárolása nem csak fizikai megoldásban térhet el egymástól, a különböző gyártók eltérő a logikai tárolási megoldás alkalmazhatnak, különböző helyeken, különböző adatokat, eltérő struktúrában tárolnak el, ami befolyásolja azok használhatóságát és vizualizációját.

Új általános kihívásként jelentkezik, hogy – a digitális forensics vizsgálatoktól eltérően – a vizsgálat során, annak eredményei alapján is szükségessé válhat további, külső adatforráshoz való hozzáférés. Például a jármű navigációs adatainak elemzésével, a feltárt útvonal információk alapján további az infrastruktúra és a jármű között továbbított – a járműben tartósan nem tárolt – információk ellenőrzése. Ilyen információk lehetnek például a(z):

- adott útszakaszra, a közlekedés státuszára vonatkozó forgalmi információk,
- a pályaelemek azonosító adatai,
- vészjelzések,
- jelzőlámpák státuszai, és az aktuális jelzéskép,
- közelben elérhető parkolólétesítmények, és az aktuális szabad férőhelyek száma,

- baleset, sávzárás.

Az adatok egy részét, pontos időbélyegekkel őrizhetik meg a járművekben, más járművekben, környezeti vagy pályaelemekben is, míg más részük illékony adatként nem kerül tárolásra. Egy esetleges jármű elleni kibertámadás kapcsán vizsgálandó lehet a járműhöz eljuttatott információk tartalma, annak megfelelősége. A járművekhez esetlegesen eljuttatott szándékosan téves információk alapján például befolyásolható a jármű mozgása, ezáltal a közlekedés biztonsága is. Annak értékelésére, hogy a jármű milyen információkat kapott a környezetéből, szükséges lehet a környezeti elemek vizsgálata is.

Egy forgalmi szituáció vizsgálata esetén szükség lehet a jármű(vek) és az infrastruktúra továbbított információkhoz való hozzáférésre is, ilyen adatok lehetnek például a(z):

- pozíció, sebesség és irány adatok,
- jármű státusz adatok,
- vészjelzések,
- útvonal adatok,
- diagnosztikai adatok.[76]

A vizsgált járműhöz kapcsolódóan az egyik legnagyobb általános kihívást a gyártmányok és a gyártmányokon belüli széleskörű típusválaszték jelenti. Az egyes gyártók a különböző járműgyártási szabványok és ajánlások követelményeit a saját céljaiknak megfelelően valósítják meg. Ennek eredményeként az alkalmazott hardver elemekben, belső hálózati kialakításban (például topológia, protokollok stb.), szoftver megoldásokban is lényeges eltérések lehetnek, amelyek megnehezítik a vizsgálathoz szükséges eszközök és eljárások standardizálását. A járművekben használt belső operációs rendszer is lényeges eltéréseket mutat a gyártók között – a gyártók a járműtípusok között jellemzően azonos operációs rendszer használnak, de egy operációs rendszer csere után már típusonként is lehet eltérés –, ami a vizsgálathoz szükséges eszközök és eljárások kialakítását bonyolítja.

Jövőbeli kihívást jelenthet a titkosított adattárolási megoldás járművekben történő bevezetése. A platformmegbízhatósági modul (Trusted Platform Module, TPM) megoldások, vagy hasonló technikák alkalmazásával a járműben található adatok biztonságának javítását eredményezné, egyúttal nehezítené, adott esetben megakadályozná a szakértői vizsgálatok elvégzését. A biztonságos titkosítási kulcs létrehozásához és tárolásához használt megoldás használható lenne annak igazolására is, hogy a járműben lévő gyártói operációs rendszer és a vezérlő egységek programjai megfelelnek az elvártaknak, azok nem kerültek módosításra.[267]

Modern járművek szakértői vizsgálatának eljáráshoz kapcsolódó kihívásai

A modern és jövő autonóm járműveihez és az intelligens közlekedési rendszerekkel kapcsolatos szakértői vizsgálati módszerek egyrészt támaszkodnak digitális forenzikus módszertanra, másrészt a járművek, pálya és környezeti sokszínűsége kapcsán lehetnek olyan elemei, amelyek az eddig eljárásoktól, eszközöktől eltérő megoldásokat igényelnek. A szakértői vizsgálati eljáráshoz kapcsolódóan a korábbiakban felsorolt általános kihívásokhoz kapcsolódnak az eljárás kihívásai.

- nagy, összekapcsolat adathalmazok,
- live forensics vizsgálatok szükségessége,
- eseménylánc követése,
- adatvédelmi követelmények,
- felügyeleti lánc biztosítása és az adatokhoz való hozzáférés szabályozása,
- anti-forensics megoldások.

A vizsgálat során elsődleges szempont megbízhatóság, valamint az agilitás, rugalmasság és moduláris kialakítás. A vizsgálatihoz olyan módszertant kell kialakítani, amely lépést tud tartani a közlekedési rendszerek fejlődésével, illeszthető a vizsgálati feladatokhoz, valamint a vizsgálatok céljaihoz, sajátosságaihoz kapcsolható eszköz, készség és tudás elemekből áll.

A bizonyítékul szolgáló adatok összefüggéseinek megtalálása a nagy mennyiségű adathalmazokban is megnehezíti a szakértői vizsgálat elvégzését. Az adatbányászat segítségével hasznos, gyakran nem várt mintázatok felismerése válhat lehetővé az adatok között.

Amennyiben a járműben keletkező illékony adatokról van szó, melyek vagy a jármű pillanatnyi működéséhez, a helyváltoztatási feladathoz kapcsolódnak és folyamatosan felülíródnak, vagy a jármű leállítása után kerülnek törlésre, egyes szakértői vizsgálatokhoz kapcsolódóan nélkülözhetetlenek lehetnek. Új kihívást jelent egy jármű, vagy közlekedési rendszer vonatkozásában a post-mortem vagy *live* vizsgálatok elvégzése is. A járművek vizsgálata során felmerülhet olyan vizsgálati cél, melyhez olyan információkhoz való hozzáférés szükséges, melyek az utólagos (post-mortem) vizsgálatok során nem állnak rendelkezésre. Ilyen live forensics vizsgálatok célja a jármű működése közben keletkező illékony adatokhoz, a működés során a memóriában található információkhoz, a belső és külső irányú kommunikációs hálózathoz való hozzáférés és az adatok feldolgozása és vizsgálata.

További kihívást jelenthet az eseménylánc végig követése, vezetése. A jármű mellett egyéb rendszerek, adatforrások is megjelennek a szakértői vizsgálatban, melyek nem, vagy nem minden esetben használnak valamilyen központosított időszinkronizációt, vagy nem azonos időbélyegeket használnak, akkor egy esemény/baleset ideje, eltérhet a járműben lévő adatok idejétől.

A szakértői vizsgálat sem mentesül a vonatkozó adatvédelmi jogszabályok, követelményeknek való megfelelés alól. Jellemzően a vizsgálat során személyes adatok is részévé válnak az adatgyűjtésnek, ezért ezek megfelelő kezeléséről is gondoskodni kell. Amennyiben a szakértői vizsgálat során harmadik felet is bevonnak, például gyártók, üzemeltetők, akik a feladatok egy részébe, a vizsgálat részeként bevonásra kerülnek, gondoskodni kell a jogszabályi követelményeknek való megfelelésről (például harmadik országba való adattovábbítás).[256]

Biztosítani kell azt, hogy a bizonyítékokhoz történő hozzáférési jogosultság szabályozott és ellenőrzött legyen, ennek megfelelően a vizsgálat is kizárólag megfelelő felhatalmazás birtokában kezdődhet meg. Megfelelően dokumentált eljárásokat és vizsgálati dokumentációt kell kialakítani annak érdekében, hogy a vizsgálat és a bizonyítékok kezelése felügyelt módon történje. Minden lépés során, az adatletöltés helyszínétől, a büntetőeljárás minden szakaszában ki kell zárni a bizonyítékként felhasznált digitális adatok manipulálhatóságát. Az adatok sértetlenségét és hitelességét – szoftveres és hardveres megoldások mellett további garanciális eszközzel – ún. felügyeleti lánc *(Chain of Custody)* segítségével is biztosítani kell, amellyel rögzíteni lehet, hogy a digitális bizonyítékkal ki, mikor és milyen műveletet, vagy tevékenységet végzett.

További kihívást fog jelenteni, különösen a járművek rosszindulatú felhasználása esetén, a különféle anti-forensics megoldások alkalmazásának megjelenése. A szakértői vizsgálatok megelőzésére, megakadályozására, vagy megnehezítésére használt és alkalmazott technikák, trükkök gyűjteménye az anti-forensics. Amelyek kvázi ellenintézkedések a vizsgálat lefolytatása ellen, fő célja a bizonyítékok megszerzésének megakadályozása.[19] Az anti-forensics taktikák, technikák és eljárások (TTPs – tactics, techniques and procedures) elrejtik vagy minimalizálják a felhasználók tevékenységének nyomait, megnehezítik vagy megakadályozzák a kapcsolódó bizonyítékok azonosítását, megszerzését, kihasználják a forenzik eszközök gyengeségeit, hibáit, továbbá bonyolulttá és időigényessé teszik a szakértői vizsgálatok elvégzését, vagy megpróbálják félrevezetni, lehetetlenné tenni azt. Az ilyen megoldások elkövető oldali alkalmazásának célja:

- (meg)akadályozni a szakértői vizsgálat lépéseit,
- a szakértői munka elnyújtása, nehezítése,
- szakértők félrevezetése, megtévesztése,
- nyomok elrejtése, kinyerésének akadályozása,
- jelentés pontosságának és hitelességének megkérdőjelezése,
- a forenzik eszköz (tool) használatának nehezítése,
- a forenzik eszköz (tool) használatának, jelenlétének felfedése,
- a forenzik eszköz kompromittálása, támadó eszközként való felhasználása,
- közvetlen támadás a szakértő ellen,
- az anti-forensics eszköz nyomainak törlése.

Ezekkel csökkentik a releváns digitális bizonyítékok mennyiségét és minőségét is.[19][72][131]

Az információkat vagy a metaadatokat felülíró tradicionális eszközök a legrégebbi és legelterjedtebb anti-forensic megoldások, járművekhez kapcsolódóan még nem terjedtek el. A vizsgálat során különböző technikai nehézségek, nehezítő tényezők merülhetnek fel, melyek a vizsgálatokat hátráltatják, vagy rendkívüli erőforrás-felhasználást (például idő, eszköz, pénz) eredményezhetnek, megnövelve ezzel a vizsgálat idejét és költségeit. Az alkalmazott anti-forensics technikától, taktikától, eljárástól függően lehetőség nyílik az egyes vizsgálati lépések akadályozására, elnyújtására, meghiúsítására, a szakértő félrevezetésére, a vizsgálat pontosságának, hitelességének megkérdőjelezésére. Az alábbi táblázatban látható, hogy a modern járművek utólagos szakértői vizsgálatában, az egyes vizsgálati lépések esetén milyen lehetőségeket nyújtanak az anti-forensics megoldások.

1. számú táblázat: *Vizsgálati lépések és a kapcsolódó anti-forensics célok*

Szakértői vizsgálati lépések	**Anti-forensics**
Azonosítás	Elrejtés, félrevezetés, elnyújtás
Megőrzés	Törlés, akadályozás, elnyújtás
Összegyűjtés	Akadályozás, elnyújtás
Vizsgálat	Félrevezetés, meghiúsítás, elnyújtás
Elemzés	Félrevezetés, pontatlanítás, elnyújtás
Értelmezés	Akadályozás, hiteltelenítés, elnyújtás

Alkalmazhatóak lehetnek a különböző titkosítások, steganográfiai megoldások vagy egyéb adatot elrejtő megközelítések, azonban ezek megvalósítása egy jármű működésére is nagy hatással lehetnek. A felhasználó digitális lábnyomának minimalizálására szolgáló vagy a vizsgáló eszközök sérülékenységeit kihasználó megoldások elterjedése a tényleges autonóm járművek megjelenése után várhatóak. [241][267]

Modern járművek szakértői vizsgálatának vizsgáló eszközökhöz kapcsolódó kihívásai

Az általánosságban ismert jármű szakértői vizsgálatok menetén és azok adatforrásain jellemzően nem igényel gyökeres változtatást az egyre inkább önvezetővé váló járművek megjelenése. Az olyan eszközök és megoldások, amelyekkel a sérült, vagy balesetet szenvedett járművek szakértését, a hibás járművek szavatossági problémáinak vizsgálatát, a baleset-elemzési szakvélemény készítést stb. végzik, valóban nem változnak meg alapjaiban. A fenti általános kihívások kapcsán azonban a modern járművek tárolt adatfókuszú szakértői vizsgálata azonban messze túlmutat a jelenleg rendelkezésre álló módszertanokon, kompetenciákon, eszközökön.[289] Jelenleg lényegesen kevesebb vizsgálati megoldás létezik a modern járművekhez kapcsolódóan.

A járművek digitális szakértői vizsgálata jelenleg kezdeti stádiumban van. Az általános kihívások mellett nehézséget okoz, hogy a járműgyártók nem engednek hozzáférést az ipari és üzleti titkaikat képző járművek központi egységeinek és vezérlőegységeinek működéséhez, adattárolási struktúrájához, forráskódjához, ezért nem állnak rendelkezésre olyan hardveres-szoftveres megoldások, amelyek segítségével, globálisan az egyes járművekben keletkező adatok kinyerhetőek, vizsgálhatóak lennének. Néhány nagyobb szoftvergyártó, *reverse engineering* módszerrel fejlesztett olyan megoldásokat, amelyek alkalmasak néhány autó típus adatainak vizsgálatára.

28. ábra Járműből kiszerelt központi egység vizsgálati eszközei Forrás: a szerző felvétele

Ezek az eszközök nem elterjedtek széles körben, rendkívül költségesek, speciális szaktudást igényelnek, nem alkalmazhatók minden járműgyártó esetén, továbbá nem biztosítják minden jármű esetén ugyanazon adatok hozzáférhetőségét. A jelenlegi megoldások által lefedett terület meglehetősen szűk, nem csak a teljes gyártói spektrum nincs lefedve, de az egyes gyártók eltérő járműtípusai sem. Azokban a járművekben, amelyekhez hozzáférést biztosítanak ezek a megoldások sem érhető el minden olyan adat, ami egy vizsgálat során szükséges lehet.

Az olyan adatok esetén, amelyekhez ezen megoldások biztosítanak hozzáférést, az adatok kinyerése nem minden esetben valósul meg strukturált, értelmezhető formában, a nyers adatok gyártói információk nélkül nem minden esetben értelmezhetők.

A modern járművekhez kapcsolódó szakértői vizsgálatok vonatkozásában meghatároztam és rendszereztem a vizsgálatokhoz kapcsolódó kihívásokat, megállapítást nyert, hogy a kihívások kapcsán a modern járművek digitális szakértői vizsgálata messze túlmutat a jelenleg rendelkezésre álló módszertanokon, kompetenciákon, eszközökön. Jelenleg kevés vizsgálati megoldás létezik, a rendelkezésre állók felhasználhatósága korlátozott, komplex, hatékonyan alkalmazható módszertan, megoldás nem áll rendelkezésre, ezért indokolt és szükséges egy új módszertan kidolgozása.[267]

A szakértői vizsgálati lépések kihívásai katonai műveletek során

Fenti kihívások mellett a harctéri és közlekedési járművek vizsgálata során újak is megjelennek, illetve egyes kihívások nagyobb súllyal szerepelnek. Katonai műveletek során a szakértői vizsgálatok elvégzésének folyamata (azonosítás, előkészítés, digitális nyomok gyűjtése, vizsgálat, elemzés, értelmezés, dokumentálás, prezentálás) módosul, az egyes lépések nem sztenderd (nem harctéri vagy katonai) módon valósulnak meg a vizsgálatok helyszíni sajátosságai miatt.

Az azonosítási, előkészítési lépéseket megelőzi egy kezdeti felderítési, keresési fázis, ahol elsődleges szempont a gyorsaság és a hatékonyság. Ennek során a műveletben részt vevő szakértő vagy a szakértői feladatokra kiképzett személyzet elvégzi a helyszín felmérését. Vizuálisan felméri, feltérképezi a környezetet, a jármű elhelyezkedését, kommunikációs kapcsolatait (vezetékes vagy vezeték nélküli hálózatok), a csatlakoztatott eszközöket, egységeket, különös tekintettel a rejtett vagy álcázott egységekre. Ebben a kezdeti lépésben is szükséges a tények, eredmények megfelelő dokumentálása, vagyis a felderített vezetékes, vezeték nélküli kapcsolatok és eszközök rögzítése. Korábban egy egység valószínűleg kiürítette volna a épületet, vagy fel robbantotta volna az ott lévő járművekkel együtt. Most azonban előfordulhat, hogy képesített szakértők segítségével ujjlenyomatokat vesznek, DNS-t vizsgálnak és digitális adatokat is gyűjtenek. A terroristák összekapcsolásával különböző bűncselekményekkel, a hírszerzési információk frissítésével, a jogi eljárások megalapozásával és a műveleti bázisokon elvégzett vizsgálatokkal az egységek sok időt megspórolnak, ami akár a katonák életét is megóvhatja, fontos információt szolgáltatva a harcoló csapatoknak.[199]

A kezdeti felderítési fázis a polgári, magyarországi igazságügyi szakértői gyakorlatban és feladatmeghatározásban nem jellemző, mivel a szakértői feladatok elvégzése a kirendelés alapján, az abban meghatározott vizsgálati tárgyakon (eszközökön és adathordozókon) történik. A bűnjel helyszíni lefoglalásában, a helyszíni hatósági műveletekben a szakértő jellemzően nem vesz részt (kivéve bizonyos fedett bűnüldözési tevékenységeket, például az eszközök éles környezetben, működés közben történő vizsgálatát, amikor a nyomok, az eszköz és az adat tartalom utólag nem vizsgálható átfogóan).[248] A felderítési fázist követően az azonosítási fázisban (három szempontot figyelembe véve) rögzítik (például fotó, videó formájában) a jármű (egyes egységei), továbbá a csatlakoztatott eszközök, adathordozók fizikai jellemzőit, állapotát, az esetleges sérüléseket. A szakértői vizsgálat során törekedni kell arra, hogy a vizsgálandó eszközök fizikai és logikai állapota ne változzon meg. Járművek vizsgálata esetén ez azonban nem minden esetben valósítható meg, ugyanis a központi fejegység, a vezérlő egységek rejtett

módon, a műszerfal vagy a burkolatok alatt, védett módon vannak elhelyezve, ezért azok megbontása szükségessé válhat (például, ha nincs kivezetett csatlakozó, illetve vezetékes vagy vezeték nélküli csatlakozással nem férhetőek hozzá az adatok). Elektronikai szempontú felmérés során a jármű és az adattároló egységek működőképességének vizsgálata történik meg. Amennyiben működő járművet vizsgálnak, annak leállítása vagy kikapcsolása adatvesztéssel járhat. Emellett a kijelzők, a műszerfal tartalmazhat hasznos információt. Katonai műveletek során az azonosítás sajátosságai közé tartozik például a különböző csapdák, kártékony kódok, rejtett adathordozók, hamis bizonyítékok, fake hálózatok, kill-switchek, improvizált robbanó szerkezetek vagy egyéb anti-forenzikus technikák nyomainak keresése. Katonai vonatkozásban ezek a technikák és taktikák még hangsúlyosabbak (például eszköz csatlakoztatásának hatására vagy a hálózati kapcsolat megszakadására elinduló törlés vagy az eszköz automata leállítása), akár a szigorúbb titkosítási elvárások, az információk érzékenysége miatt.

Csapda lehet egy szoftver, egy eszköz, a rendszer konfigurációja vagy ezek kombinációja azzal a céllal, hogy kárt tegyen vagy megnehezítse a vizsgálatot. Informatikai szempontú felmérés során a hálózati csatlakozások azonosítása történik meg, valamint az adathordozókat írásvédő segítségével (kivéve valós idejű vizsgálatok vagy integrált adathordozó esetén) csatlakoztatják a vizsgálógéphez, az adatok kompromittálódásának megelőzése érdekében. Vizsgálják, hogy a járműhöz milyen fizikai vagy logikai hozzáférési pontokon keresztül lehet hozzáférni, és azokon keresztül milyen adatok érhetőek el. Kihívást jelent az elektronikus információ, a digitális nyomok felismerése a változó és sajátos környezet miatt, továbbá a kompromittált adattartalom felismerése is. Az előkészítés vagy a nyomok megőrzése során elkészülnek a lemezképek (járművek esetén ez az adattároló képességgel rendelkező eszközök adattartalmának megszerzését jelenti), az eredeti nyomok sérülési lehetőségének csökkentésére biztonságos központi szerveren tárolják a kinyert adatokat. A vizsgálandó eszközök és elemeik azonosítása és a szállításhoz szükséges megfelelő védelme is kihívást jelent, hiszen a digitális információ illékony, sérülékeny a harctéri környezetben, ezért nagy hangsúlyt kell fordítani az adatok és az adathordozók biztonságos kezelésére. Amennyiben működés vagy üzem közben ideiglenesen vizsgálat alá vont eszközről van szó (például hírszerzési tevékenység során), az adatok kinyerését korlátozott idő alatt kell elvégezni. Az eszközkészletek kompatibilitása, az eszközök gyakorlati ismerete (tapasztalat), a rendelkezésre álló tárhely nagysága is okozhat nehézségeket. Nagy adatmennyiség letöltése ilyen esetben nem mindig valósítható meg, szükségessé válhat a kapcsolat fenntartása, a felügyeleti szoftver telepítése a járműre, amely a meglévő vagy ideiglenes kommunikációs csatornán keresztül biztosítja az adatok átvitelét.

Adatgyűjtés alatt a vizsgálati cél szerint az esemény(ek) körülményeinek, a résztvevők által végrehajtott tevékenységeknek, a helyszíneknek és a körülményeknek a tisztázását értjük. Ennek kapcsán történik meg a vizsgálatban érintett személyekhez kapcsolódó adatok felkutatása, a bizonyítékok beszerzése, a vizsgálat megalapozásához, megtervezéséhez szükséges adatok összegyűjtése is. Katonai műveletek során ez az egyik legnagyobb kihívás a kaotikus és kiszámíthatatlan körülmények miatt, ahol a felügyeleti lánc kialakítása és megtartása alapvető védelmi technikák alkalmazását és sajátos intézkedéseket igényelhet. Az adatgyűjtési lépéseknek ennek ellenére biztosítaniuk kell a megszerzett adatok integritását, és stabil forrást kell biztosítaniuk az adatok elemzéséhez.[289] Az Evidence Based Operation (EvBO) esetén kiemelten fontos a nyomok sértetlensége, ezáltal vizsgálhatósága, megfelelősége és hitelessége. A veszélyes környezet, az egységek információhiánya, a vizsgálatok időbeli elhúzódása végzetes következményekkel is járhat. Az elemzési fázisban a kinyert nagy mennyiségű adat integritását és gyors feldolgozását is biztosítani szükséges. Verifikálni kell, hogy az adatok nem változtak a kinyerés során.[41]

Modern járművek az adat- és információszerzési területeken

Az adat- és információszerzés sikerét modern járművekhez kapcsolódóan alapvetően a hozzáférhető és megszerezhető adatok mennyisége befolyásolja. A nagyobb adatmennyiség nem feltétlenül növeli az információ értékét, a vizsgálatok lefolytatását a túl sok információ meg is hiúsíthatja. Megnehezíti a releváns információk feltárását, lassítja az adatfeldolgozást, az elemzést és értékelést. A modern járművekhez kapcsolódóan az adat- és információszerzési területei, a műveleti vagy vizsgálati cél függvényében relevánsak lehetnek, azonban a képességek hatékony felhasználása érdekében és az időprés miatt a gyakorlatban csak azon módszerek kerülnek alkalmazásra, amelyek leghatékonyabban biztosítják a szükséges adatok és információk megszerzését. Alkalmazható információszerzési területek:

- emberi erőforrásokkal folytatott információ- és hírszerzés (HUMINT),
- rádióelektronikai felderítés (SIGINT),
- nyílt forrású információszerzés (OSINT),
- képfelderítés (IMINT),
- mérés- és jelmeghatározó hírszerzés (MASINT),
- technikai hírszerzés (TECHINT),
- kiberhírszerzés (CYBINT).

Polgári alkalmazásban, ideális esetben a járművekkel kapcsolatos adat- és információszerzési feladatok a felhatalmazáson alapuló, utólagos szakértői vizsgálatokat jelentik. A felhatalmazást a megbízás vagy vállalkozási szerződés, továbbá a kirendelő határozat vagy bírósági végzés jelenti, ami tartalmazza az adatigényt, a megválaszolandó szakértői kérdéseket.

A felhatalmazás és jogosultság nélküli, a járművek belső adataihoz való hozzáférés, azok módosítása, a járművek irányításának, működésének befolyásolása a szakértői feladatokat indukálhatják, ezen tevékenységek a vizsgálati oldalon jelennek meg. A szakértői munka végrehajtásához szükséges lehet személyek, mint információforrások igénybevétele. HUMINT esetén az információhoz, dokumentumokhoz való hozzáférés mindig személyeken keresztül történik. Polgári alkalmazásban főként az üzleti hírszerzéshez tartozik ide.

A járművek szerviz és műszaki dokumentációinak, tudományos közlemények, szabványoknak és egyéb leírásainak elérésére nyílt forrású információszerzés (OSINT) is alkalmazható. A mindenki számára elérhető információk, az interneten megtalálható anyagok tartoznak ide. Ezek az információk nehezen feldolgozhatóak, tévesek vagy hiányosak lehetnek, hitelességük megkérdőjelezhető, nehezen ellenőrizhető. A járművek digitalizációjának gyors üteme miatt ezek az információk naprakészsége sem garantálható.

A járművekhez kapcsolódó digitális szakértői vizsgálatokhoz kapcsolódóan, az adat- és információ igény teljesítésének eszköze a technikai hírszerzés (TECHINT), ami a járművek, a közlekedési rendszer komponenseinek közvetlen vizsgálatát és a hozzáférhető információk feldolgozását jelenti. A SIGINT, IMINT, MASINT, CYBINT megoldások csekély alkalmazási hatékonysága és magas erőforrás ráfordítás miatt jellemzően nem alkalmazott.

2. táblázat Modern járművek vizsgálata esetén alkalmazható információszerzési területek polgári és katonai alkalmazásban

Modern járművek vizsgálata esetén alkalmazható információszerzési területek			
Polgári alkalmazás		Katonai alkalmazás	
HUMINT	X	HUMINT	X
SIGINT		SIGINT	X
OSINT	X	OSINT	X
IMINT		IMINT	X
MASINT		MASINT	X
TECHINT	X	TECHINT	X
CYBINT		CYBINT	X

Katonai alkalmazásban az emberi erőforrásokkal folytatott információ- és hírszerzési tevékenységet a nyílt, legális és az ügynöki, fedett hírszerzés jelenti. „A nyílt, legális pozícióból folytatott információ és hírszerzést alapvetően alapvetően diplomáciai keretek között, valamint a katonai missziók hír- és információs szerző támogatását ellátó hírszerző elemekkel (a katonai hírszerzéshez tartozó NIC – National Intelligence Cell, NIST- National Intelligence Support Team) folytatott hírszerzés alkotja.”. Katonai alkalmazás esetén is személyek által történik az információkhoz, dokumentumokhoz való hozzáférés.

Rádióelektronikai felderítés esetén passzív eszközökkel a távközlési vagy más elektromágneses hullámokat kibocsátó rendszerek felfedése és lehallgatása történik. Járművekhez kapcsolódóan a kommunikációs csatornák felfedésével és lehet hallgatásával érhetőek el a digitális adatok (pl.: távirányított vagy autonóm eszközök adat csatornái telemetriai adatai).

Nyílt forrású információszerzés polgári felhasználáshoz hasonlóan katonai alkalmazásban is használható hasonló feldolgozási nehézségekkel és időszerűségét problémákkal.

Képfelderítés vonatkozásában a térinformatikai felderítéssel összevont műholdas vagy légi felderítés használatával gyűjthető információ a műveleti területen megtalálható modern vagy autonóm járművekről. A műveleti területről, annak objektumairól, a járművekről, eszközökről, készült fényképfelvételek nyújthatnak plusz információt.

Azon alapinformációk megszerzésére melyek egy jármű hollétére, annak idejére, a jelenlét okaira vonatkoznak, a rádióelektronikai felderítés és a képfelderítés mellett felértékelődik a mérés és jel meghatározó hírszerzés - mint technológiai alapú hírszerzési ág. Az azonosítás szenzorok segítségével, a kibocsátott kisugárzott jelek alapján történik.

A jármű a benne található nyomok kinyerése érdekében, továbbá a hírszerzési tevékenység célpontjaként, valamint a működésére vonatkozó információk megszerzése érdekében közvetlen vizsgálat alá vonható, amit technikai hírszerzésnek (TECHINT) nevezünk. A vizsgálat eredményeként technológiai vagy katonai fölény érhető el. A modern járművekben található digitális adatokhoz történő hozzáférés főként a technikai hírszerzés eszközrendszerével, annak járművekhez illeszkedően kialakított módszertana és technikáit alkalmazva, közvetlenül történik, vezetékes vagy vezeték nélküli csatlakozás, illetve az adathordozó ahhoz történő közvetlen csatlakozás által.

Annak függvényében, hogy a járműhöz vagy valamely adattárolójához milyen módon és céllal férünk hozzá, megkülönböztetőek a vizsgálati eljárások:

- ép, működőképes lefoglalt, zsákmányolt, vagy más úton megszerzett eszköz/adattároló vizsgálata,
- működés vagy üzem közben lefoglalt, zsákmányolt, vagy más úton megszerzett eszköz/adattároló vizsgálata,
- működés vagy üzem közben ideiglenesen vizsgálat alá vont eszköz vizsgálata,
- sérült, meghibásodott, megsemmisített eszköz vagy adattárolójának vizsgálata.

A kiberhírszerzés (CYBINT) számítógépes hálózatokban tárolt információk megszerzésére irányul. A modern járművek és a magas automatizáltságot támogató közlekedési rendszerek (ITS, C-ITS) vizsgálatához tartozik mind a nyílt és zárt számítógépes hálózatokban védett információk megszerzése, mind a hálózatok által kisugárzott jelekből folytatott adatszerzés.[8]

3. Modern és önvezető járművek digitális forenzikus vizsgálata és módszertana

A modern járművekhez kapcsolódó szakértői vizsgálatok célja a rendelkezésre álló információk alapján, jellemzően nem megismételhető esetekben nyilvánvalóvá tenni, hogy mi történt a vizsgált eset, esemény kapcsán, hasonlóan egyéb digitális forenzikus vizsgálatokhoz. A vizsgálatokat azok végrehajtása szerint két kategóriába sorolhatóak be:

- az egyik kategória az élő vagy „live" forensics (hasonlóan a számítógépes forenzikus vizsgálatához), másik kategória
- az utólagos (post mortem) forensics vizsgálat.

Élő vagy „live" forensics vizsgálat során a jármű azonnali, működés közbeni vizsgálata történik. Ilyen vizsgálatra katonai műveletekben, hírszerzési tevékenység során, vagy terrorcselekmény elkövetése esetén lehet szükség, amikor az időprés miatt azonnali információkra van szükség a tevékenység hatékony folytatásához. Ilyen esetben nincs mód és lehetőség a vizsgálat laboratóriumi körülmények közötti elvégzésére. Az ilyen vizsgálat számos előnnyel jár, beleértve az illékony adatok (pl.: a memóriában ideiglenesen megtalálható adatok) megszerzését vagy a gyors elemzés és értékelés lehetőségét. Hátránya, hogy az adatok vagy a rendszer nem szándékos, de el nem kerülhető módon manipulálásra kerül, mivel maga az adatbeszerzési folyamat olyan adatokat generálhat, amelyek módosítják, felülírják a meglévő nyomok egy részét.[257]

Utólagos szakértői vizsgálat esetén, a vizsgálni kívánt jármű, eszköz, rendszer kikapcsolt állapotban van. Ilyen esetben az illékony memóriában található adatok már nem elérhetőek, azonban az élő vizsgálatokhoz képest nincs feltétlenül hatással az adatokra lehetséges bizonyítékokra, mivel van lehetőség például írásvédő használatára. Járművek esetén a diagnosztikai hibakód-információk beszerzése, az EDR adatok kiolvasása, vagy a fejegység vizsgálata az utólagos, post mortem vizsgálatok példái.[17]

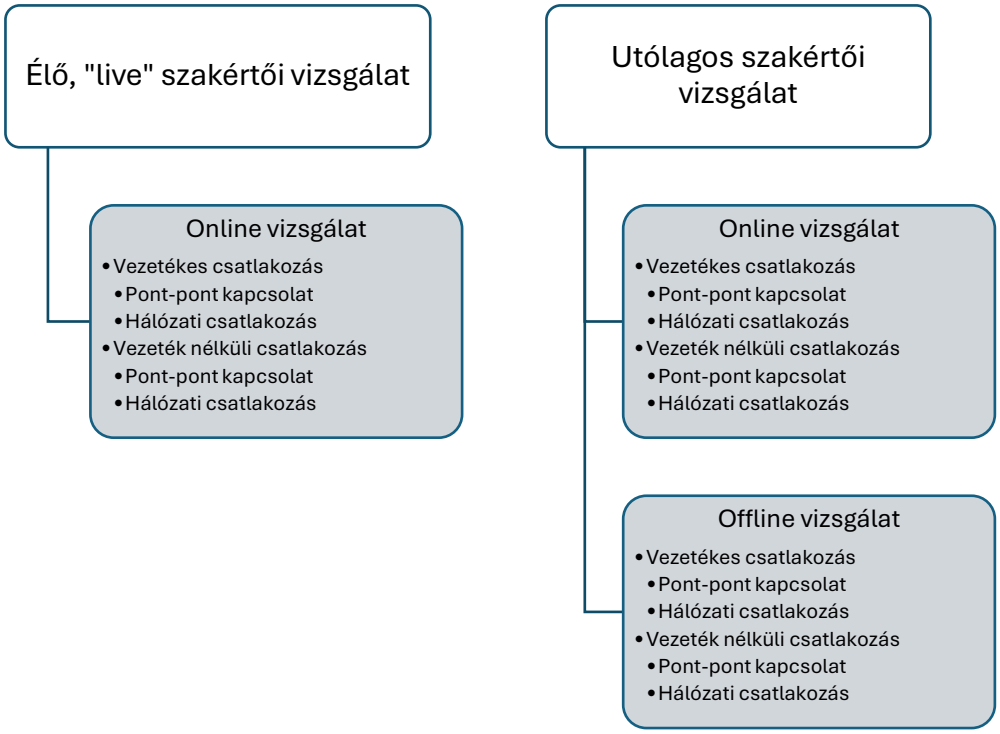
A jármű állapotától függően eltérő állapotú lehet (megsemmisült, sérült vagy ép). A szakértői vizsgálat során az adatkinyerés online vagy offline módon is történhet. Az online szakértői vizsgálat szoftveres megoldással történik, melyhez nincs szükség az autó megbontására, szétszerelésére. A csatlakozókon keresztül a vizsgáló gép (szükség szerint valamilyen interfész segítségével) csatlakoztatásra kerül a járműhöz az adatgyűjtő szoftverrel történik az adatok

kiolvasása. Költségek szempontjából az ilyen vizsgálat kedvezőbb árú, mivel nincs szükség további hardverre vagy szerszámokra, emellett a jármű nem sérül meg.

Offline hozzáférés esetén olyan hardveres megoldások, csatlakozás kialakítás szükséges, ami szükségessé teheti a jármű megbontását, az egyes alkatrészek eltávolítását, az adathordozó elemek (pl.: integrált áramkörök, elektronikus vezérlő egységek) közvetlen elérését, feszültség szintek mérését. Az offline vizsgálat olyan technikákat foglal magában, mint például a fejegység, vagy egyéb vezérlők, adathordozók eltávolítása vagy a változó feszültségszintek vizsgálata oszcilloszkóp vagy logikai analizátor segítségével. Ehhez a jármű részleges szétszerelése szükséges, mert az eszközöket el kell választani a járműben lévő rendszertől. Az ilyen vizsgálat időigényesebb, ezért a már említett katonai műveletek, hírszerzési tevékenység, terrorcselekmény, vagy feltételezett visszaélés esetén, az időprés miatt nehezebben kivitelezhető. Előnye viszont, hogy nagy mennyiségű adat kinyerését teszi lehetővé, mivel az információk közvetlenül az adathordozóról kerülnek kiolvasásra.[17][248]

SIGINT, IMINT, MASINT, TECHINT, CYBINT esetén lehetőség van a live, élő vizsgálatra, vagyis a működő rendszer adatainak (online) megszerzése és gyors elemzés a történik. Ez az eljárás lehetőséget biztosít az illékony például memóriában található adatok vagy a kommunikációs csatornán átvitt információk megismerésére.

Utólagos vizsgálat esetén az adatokhoz történő hozzáférés történhet online és offline módon egyaránt, az ép, vagy nem működő, sérült, meghibásodott vagy megsemmisített eszközön vagy annak adathordozóján. Ebben az esetben az élő vizsgálattal ellentétben, illékony memóriában található adatok visszaállítása már nem lehetséges.



29. ábra Szakértői vizsgálatok csoportosítása

Mind az élő, mind az utólagos szakértői vizsgálatok esetén értelmezhető az online vizsgálat, vagyis a járműhöz közvetlen csatlakozás (vezetékes vagy vezeték nélküli módon). Utólagos szakértői vizsgálat esetén értelmezhető az offline vizsgálat, amikor a jármű megbontása vagy szétszerelése megoldható. Mindkét esetben értelmezhető a pont-pont összeköttetés vagy hálózati csatlakozás. Az utólagos vizsgálatok esetén sem minden esetben történnek a vizsgálatok laboratóriumi körülmények között, különösen műveleti területen.

3. táblázat Szakértői vizsgálatok során alkalmazott csatlakozás, vizsgálati eljárás és hozzáférés

Csatlakozás	Vizsgálat		Hozzáférés	
vezetékes	élő/live	utólagos/post mortem	online	offline
diagnosztikai port	X	X	X	
USB	X	X	X	
EVSE[3]	X	X	X	X
memóriakártya foglalat	X	X	X	
belső hálózatok	X	X		X

[3] Electric Vehicle Supply Equipment, elektromos járművek töltő csatlakozója

elektronikus vezérlő egységek (ECU)		X	X	X
infotainment/ fejegység		X	X	X
EDR				

A különböző hálózatok és vezérlő egységek korlátozás nélküli, közvetlen elérése offline módon lehetséges, a jármű részleges megbontásával jár és az adathálózatra közvetlenül történik a csatlakozás. Logikai analizátorral, oszcilloszkóppal figyelhető meg a forgalom, melynek rögzítésével lehetőség nyílik az egyes adatkeretek részletes elemzésére is.

A járművekhez történő csatlakozás vezetékes vagy vezeték nélküli módon történhet. A vizsgáló eszközt közvetlenül csatlakoztatva a járműhöz, pont-pont összeköttetésről beszélünk. Például az eseményadat rögzítő (EDR – Event Data Recorder) adatainak kiolvasása során a diagnosztikai porton keresztül. Hálózati csatlakozás esetén több eszköz/vizsgálati tárgy vagy jármű a vizsgáló hálózathoz kerül csatlakoztatásra, melynek része a vizsgáló eszköz is.

Vezetékes csatlakozás esetén a járművekben kialakított szabványos csatlakozókon (pl.: OBD-II, USB) keresztül, közvetlenül történik a csatlakozás. A csatlakozók elhelyezése és a jármű belső hálózatához való hozzáférési lehetőség jármű gyártónként, típusonként és évjáratonként is eltérő lehet. Elhelyezésük a kormány közvetlen közelében, a közép konzolban, kesztyűtartóban, könyöklőben, stb. gyakori. Ezek a csatlakozók lehetővé teszi mind a live, mind az utólagos vizsgálatok elvégzését – a jármű műszaki állapotának, működőképességének, illetve a belső hálózat szegmentációjának függvényében. Egyes csatlakozók csatlakoznak a fejegységhez, így egyes adatokat kinyerhetővé tesznek, más csatlakozók csak eszközeink töltését biztosítják, így adatkinyerésre alkalmatlanok.[248]

30. ábra USB csatlakozási lehetőség a jármű középkonzoljában [319]

Az elektromos, vagy plug-in hibrid járművek elterjedésével, a töltőállomások számának növekedésével az elektromos járművek töltő csatlakozóján (EVSE - Electric Vehicle Supply Equipment) keresztüli hozzáférés új fenyegetésként jelent meg. Akár a töltőállomás és hálózata irányába, akár a jármű irányába hozzáférési lehetőséget biztosít a támadók számára. Amennyiben a jármű belső hálózata nem kellően védett, a fizikai hozzáférési ponton keresztül a jármű belső hálózata is elérhetővé válhat. Szakértői vizsgálat során az ilyen hozzáférések megvalósításáról, például a jármű töltésvezérlőjéből is nyerhető ki információ. A jármű megbontása nélkül, online módon, vagy a töltést vezérlő ECU-hoz való offline hozzáféréssel nyerhetőek ki információk.

31. ábra Jármű töltése és EVSE csatlakoztatása [327]

A jármű fejegységéhez történő szakértői csatlakozás egyik módja a gyári memóriakártya foglalatba helyezett, preparált memóriakártyával történhet. Ebben az esetben az adatok a jármű által kerülnek kimásolásra a memóriakártyára. Az ilyen lehetőség elég korlátozott, kinyerhető adatok mennyisége tekintetében is, illetve kevés járműgyártó alkalmazza ezt az adattárolási megoldást.

32. ábra Jármű multimédia egység USB és SIM csatlakozási lehetőséggel

A jármű belső hálózataihoz (pl.: LIN - Local Interconnect Network, CAN - Controller Area Network, FlexRay, Automotive Ethernet, MOST - Media Oriented Systems Transport, stb.) történő csatlakozás lehetőséget biztosíthat live és utólagos vizsgálatra is.

A járművekben keletkezett, tárolt, általuk gyűjtött, feldolgozott, továbbított, stb. digitális adatok lehetőséget biztosítanak különböző vizsgálati célok elérésére. A járművek vagy azok különböző adathordozói mint adatforrás jelennek meg, ami hozzájárulhat az információs műveletek sikeréhez. A járművekből származó adatok kinyeréséhez különböző hardver- és szoftvereszközöknek kell rendelkezésre állniuk. Ezeknek biztosítani kell a konzisztencia, a robusztusság és a reprodukálhatóság követelményeinek teljesítését.

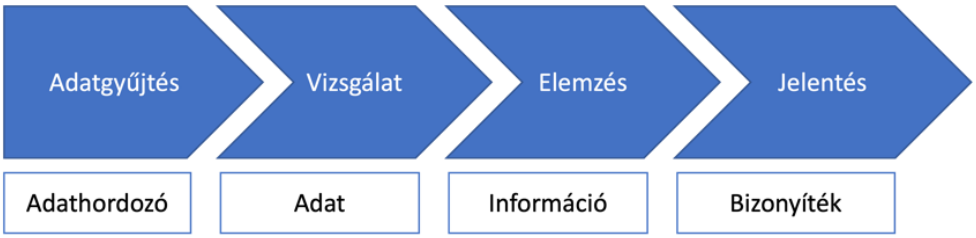
Az igazságügyi szakértői tevékenységet számos szabvány, ajánlás, irányelv, valamint módszertani levelek szabályozzák. A vizsgálati fázisokat áttekintve az elektronikus adatok/digitális nyomok vonatkozásában az egyes módszertanok hasonló alapelveket követnek, azonban ezek felhasználási módja jelentősen eltérhet. A digitális forenzikus vizsgálat egyes doménjeit áttekintve, járművekben történő alkalmazhatóságukat vizsgálva megállapítható, hogy mely módszerek, fázisok vagy azok mely eleme alkalmazható a modern járművek vizsgálata során. Maga a vizsgálat, a szakértői munka (a meghatározott vizsgálati fázisok és

feladatok sorrendi végrehajtása) valamilyen felkérés, felhatalmazás (kirendelés) alapján kezdődik meg.

Az NIST SP 800-86, azaz a National Institute of Standards and Technology ajánlása (Kent et al. 2006) a vizsgálatok elvégzésére négy alaplépést határoz meg:

- adatgyűjtés,
- vizsgálat,
- elemzés,
- jelentés,

amelyek az egyes Digital Forensics domain-ek tekintetében, így a járművek vizsgálatában is nélkülözhetetlenek.



33. ábra A NIST által javasolt digitális vizsgálati folyamat

A járművek, a pálya és a környezet sokszínűsége kapcsán szükséges további elemeket bevezetni, amelyek az eddigi eljárásoktól, eszközöktől eltérő megoldásokat igényelnek.

Az adatgyűjtés lépésében azonosításra kerülnek azok az adatforrások, adathordozók, amelyek relevánsak lehetnek a vizsgálati célok vonatkozásában. A vizsgálat tekintetében ez az egyik olyan fázis, amit a járművek állapota, gyártója és egyéb sajátosságai nagymértékben befolyásolnak, ezért indokolt e folyamat további lépésekre való felbontása. A vizsgálati tárgy, a jármű és annak adathordozója lehet sérült vagy balesetet szenvedett.

A járművek vizsgálatához kapcsolódóan az adatforrás meghatározása külön lépésként jelenik meg, ahol a lehetséges adatforrások beazonosítása történik meg, függően a jármű műszaki állapotától, gyártójától, típusától stb. Vannak olyan adatforrások (pl. EDR, infotainment), amelyeken a tárolt adatok közvetlenül kapcsolódnak az adott esemény rekonstruálásához. A vizsgálatot végző szakértőknek azonban minden alternatív adatforrást is azonosítaniuk kell, amelyek támogathatják a vizsgálat elvégzését. Előfordulhatnak olyan esetek, amikor az elsődleges adatforrás nem elérhető (pl. az autóba szerelt adattároló – HDD – meghibásodott a

baleset következtében), így a vizsgálatokat másodlagos adatforrások alapján kell elvégezni (pl. az eseményadat rögzítő - EDR).

Az adatforrások azonosítása és dokumentálása után az adatok begyűjtése az integritás biztosítása mellett történik meg – közvetlen csatlakozással vagy hálózati elérés útján –, ami jellemzően másolatkészítéssel történik – fizikai, logikai másolat, letöltés vagy lemezkép.

A begyűjtött adatok elemzését a szakértő végzi, amely folyamat magában foglalja a bizonyítékok mélyreható és szisztematikus feltárását, azok hitelességének és érvényességének vizsgálatát, valamint az adott ügyhöz kapcsolódó rejtett vagy törölt adatok azonosítását és visszanyerését. Ebben a szakaszban minden bizonyítékot alaposan megvizsgálnak a bizonyítékok jellegének megfelelően. Az adatelemzés jellemzően interaktív eszközök használatát jelenti a megszerzett adatokban található adatszerkezetek és metaadatok felismerésére és elemzésére. Ez a folyamat magában foglalhatja olyan, a vizsgálat szempontjából hasznos információk megszerzését, mint a GPS-adatok, a járműmozgási információk, a hívásnaplók, a szöveges üzenetek, az eszközkapcsolatok és egyéb adatok elemzését. Ebben a szakaszban olyan technikák alkalmazhatók, mint a kulcsszavas keresés, az idővonal-elemzés és a hivatkozáselemzés. Szükséges lehet az adatok vagy adattípusok leválogatása is. Az elemzést olyan módon szükséges dokumentálni, hogy egy független szakértő képes legyen a vizsgálat és elemzés folyamatait követni, illetve ellenőrizni a következtetések helyességét.[205]

Az adatok elemzése során jellemzően valamilyen interaktív eszközzel fel kell ismerni és elemezni a megszerzett adatokba ágyazott adatstruktúrákat és metaadatokat. Az adatfeldolgozásnak számos metódusa van, amelyek a szakértőt kirendelő határozatban előírt szakértői feladatok jellegéhez illeszkednek. Minden esetben a szakkérdések megválaszolására leginkább alkalmas metódusok kerülnek kiválasztásra. Ezt úgy kell végrehajtani, hogy a digitális adat módosításának lehetősége minimális legyen. Amennyiben az elemzés során az eredeti digitális nyom megváltozik, ennek okait, hatásait részletesen meg kell határozni, és dokumentálni kell. Ez a fázis magában foglalja mindazon releváns adatok azonosítását, feltárását és összekapcsolását, amelyek szükségesek a vizsgált esemény idővonalának rekonstrukciójához, az incidensek és kibertámadások nyomainak feltárásához, a jármű és a közlekedési rendszer működésében jelentkező anomáliák azonosításához, valamint az adatforrások és naplóállományok elemzéséhez és feldolgozásához. A folyamat célja továbbá a kirendelői kérdések megválaszolását megalapozó információk rendszerezése és értelmezése. A fázishoz alkalmazható szakértői eszközök többek között:

- a törölt állományokat helyreállító szoftverek,
- szűrő és kereső algoritmusok,
- adatbázis-kezelő rendszerek,
- karakterfelismerő alkalmazások,
- adatfeldolgozó és -elemző szoftverek,
- a manuális elemzést segítő szoftverek,
- jelentéskészítő megoldások.

Mint a vizsgálathoz kapcsolódó kihívás megjelenik az adatok titkosítása és annak feloldásának nehézsége is. Mind a titkosítás jellegének azonosítása, a szoftver és algoritmus azonosítása, a titkosító kulcs megszerzése és az adattartalom visszafejtése nehezíti a vizsgálati célok elérését.

A jelentési fázisban történik a vizsgálat és elemzés eredményeinek átadása. Ez tartalmazza az alkalmazott folyamatok, eljárások és eszközök leírását, azok kiválasztásának magyarázatát. A dokumentálás olyan folyamat, amelynek konzisztens módon jelen kell lennie a vizsgálat teljes életciklusa során. A szakértői vélemény tartalmára vonatkozóan további követelmények a 31/2008. (XII. 31.) IRM rendeletben található, amely alapján a szakvéleménynek tartalmaznia kell:

- „*a) a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatokat (lelet),*
- *b) a vizsgálat módszerének rövid ismertetését,*
- *c) a szakmai megállapítások összefoglalását (szakmai ténymegállapítás),*
- *d) a szakmai ténymegállapításokból levont következtetéseket, ennek keretében a feltett kérdésekre adott válaszokat (vélemény)*” is.

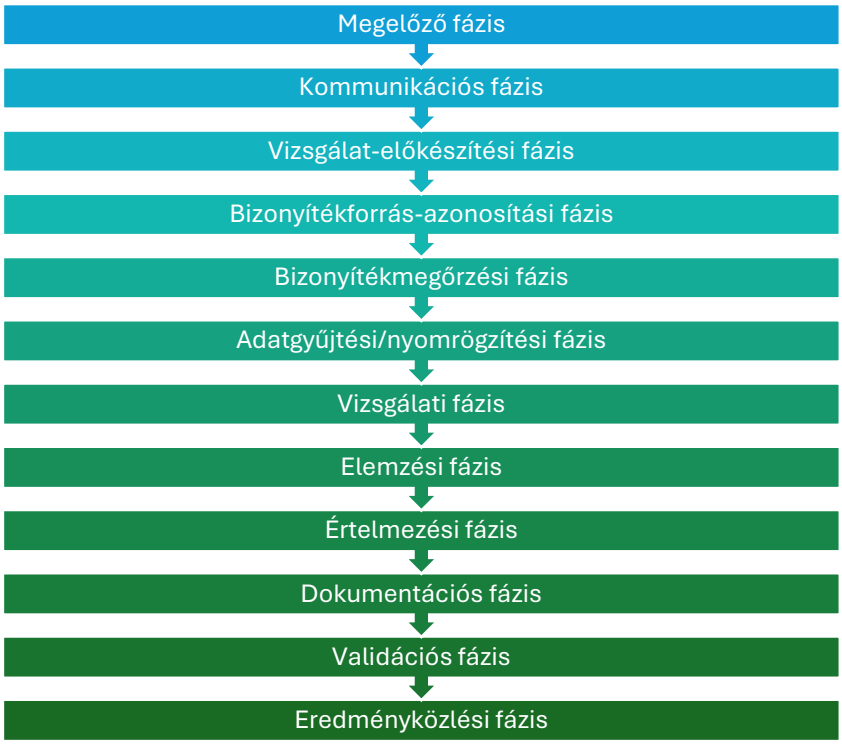
A 2016. évi XXIX. törvény az igazságügyi szakértőkről meghatározza a szakvélemény tartalmát, melynek ez alapján tartalmaznia kell a leletet, a vizsgálat módszerének rövid ismertetését, a szakmai ténymegállapításokat, a szakértő véleményét; ha az ügyben korábban vizsgálat lefolytatására került sor, és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését; a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait és az arra való utalást, hogy az igazságügyi szakértő mely szakterületen jogosult szakvéleményt adni; illetve, hogy az igazságügyi szakértő vagy más személy eseti szakértőként járt el. A szakértői vélemény tartalmára vonatkozó további követelményeket tartalmaz a 31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről. A digitális bizonyítékokkal kapcsolatos ügyekben a

szakértői véleménynek kifejezetten tartalmaznia kell a keresett céladatok részleteit, a különböző eszközökön talált adatok meglétét vagy hiányát, a vizsgálatnak az eszköz működőképességére gyakorolt hatását. Utóbbi a járművek vizsgálata esetén különösen releváns lehet, mert a vizsgálat során annak tárgyát (részben) szükséges lehet szétszerelni, és a tárgy eredeti állapotának visszaállítása nem mindig biztosítható (pl. chip-off eljárás után).[248]

Modern járművek esetén célszerű a négy fő lépést

- az adatok összegyűjtése
- az adatok vizsgálata
- az adatok elemzése
- jelentés (papíralapú [pl. szakértői vélemény], illetve digitális formátumú vizsgálati eredmények összegzése),

további fázisokkal kibővíteni. Annak érdekében, hogy a szakértői vizsgálat eredményes és hatékony legyen, valamint a szervezeti és jogszabályi követelményeknek megfelelően kerüljön elvégzésre, az adatgyűjtési fázist megelőzően több vezetői és szakértői feladatot szükséges definiálni és végrehajtani.[246]



34. ábra Autonóm járművek digitális forenzikus módszertani lépései [246][251]

Egy vizsgálat eredménye annyira pontos, a vizsgálat „annyit ér”, amennyi releváns adatot a szakértő ki tud nyerni a vizsgálati tárgyból. Emellett a járművek digitális forenzikus vizsgálatokra is érvényes az ún. „első csapás” fogalma, mely szerint az eredményes tényfelderítéshez és a 7W kérdések megválaszolásához a lehető legrövidebb időn belül meg kell tenni a szükséges intézkedéseket.[116]

A vizsgálatot **Megelőző**, felkészülési/előkészítő **fázis**ában szükséges egy előzetes stratégia felállítása, amely alapján a szakértő meg tudja tervezni, el tudja kezdeni az adott jármű vizsgálatát. A szakértői vizsgálat elengedhetetlen jogi és szakmai feltétele a vizsgálat lefolytatását elrendelő felhatalmazás/okirat átvétele és megismerése. A felhatalmazás, kirendelés alapján lehetőség szerint meg kell határozni a vizsgálathoz kapcsolódó alapvető információkat:

- a vizsgálat hatóköre,
- a vizsgálat helyszíne és körülményei,
- a jármű paramétereinek meghatározása,
- a vizsgálati célok és a kapcsolódó adatigény,
- az adatforrások előzetes meghatározása,
- a vizsgálathoz szükséges eszközkészlet, azok használatához szükséges tudáselemek,
- a vizsgálati módszerek,
- a vizsgálati feltételek,

annak érdekében, hogy a vizsgálat elvégzéséhez szükséges eszközök rendelkezésre álljanak. Ezen információk a vizsgálat elvégzéséhez szükséges személyi és tárgyi feltételek rendelkezésre állásának biztosításához szükségesek.

A vizsgálat hatóköre, helyszíne és körülményei a felhatalmazás alapján kerülnek meghatározásra. A vizsgálati hatókör meghatározásának egyik lényegi eleme annak tisztázása, hogy a szakértőnek milyen típusú/jellegű információkat kell kigyűjtenie a vizsgálat során. A vizsgálati hatókör meghatározása kiemelten fontos annak érdekében, hogy a szakértő a vizsgálat során a megfelelő rendszerelemeket és eszközöket azonosítsa, amelyekből az vizsgálat szempontjából releváns adatok kinyerhetőek. Megállapításra kerül, hogy a járművön kívül egyéb elemekhez, rendszerekhez (vizsgálandó komponensek) történő hozzáférés szükséges-e. Például járműhöz csatlakoztatott mobiltelefon, utólagosan beépített menetrögzítő kamera, járműkövető rendszer, gyártói vagy szolgáltatói felhő alapú rendszerek, stb.

Vizsgálati helyszín és körülményeinek meghatározása során az egyes lépéseket eltérő helyszínen is végre lehet/kell hajtani. A járművek vizsgálata esetén is törekedni kell arra, hogy azt laboratóriumi körülmények között végezzék el. Amennyiben ez a vizsgálandó jármű vonatkozásában nem megvalósítható, fel kell készülni a helyszíni vizsgálat elvégzésére. A laboratóriumi vizsgálat biztosítja a biztonságos körülményeket, a szükséges hozzáférési és szerelési, valamint az adatkinyerés teljeskörű lefolytatásához szükséges feltételeket, a laboratóriumon kívüli helyszíni vizsgálati helyszínnel szemben. A helyszíni vizsgálat objektív okok (például a jármű mozgásképtelensége, a lefoglalást elszenvedő személlyel szembeni aránytalan hátrány, a nyomozás, vizsgálat érdekei, stb.) indokolhatják.

Jármű paramétereinek meghatározása során a szakértőnek a járművel kapcsolatos előzetes információkat kell gyűjtenie ahhoz, hogy előzetesen fel tudja mérni a vizsgálat elvégzéséhez szükséges lépéseket, eszközöket, feladatokat és megállapítsa, hogy rendelkezik-e az adott jármű vizsgálatához szükséges technológiával, képességeivel és lehetőségeivel kapcsolatos információkkal. Ennek felméréséhez az alábbi információkra van szükség:

- a jármű alvázszáma,
- a jármű márkája,
- a jármű típusa,
- évjárata,
- felszereltség,
- illetve a jármű állapota.

A vizsgálat lefolytatása szempontjából a szakértőnek tisztában kell lennie a vizsgálat céljával, a megválaszolandó kérdésekkel és a vizsgálat tárgyának állapotával, körülményeivel kapcsolatban (pl.: a vizsgálat tárgyát eltávolították-e a járműből). A vizsgálati célok jellemzően egyediek, az adott esethez, eseményhez kapcsolódóak, azonban általánosságban elmondható, hogy valamely, a járműben feltételezhetően elérhető adathoz, adatcsoporthoz kapcsolódnak. Például a jármű fejegységében található navigációs adatok, vagy a benne található valamennyi adat kimentése és értelmezhető formában, formátumban történő prezentálása.

A már meghatározott adatigény alapján, az adott járműhöz kapcsolódó technológiai, gyakorlati és dokumentációs ismeretekből meg kell határozni azon adatforrásokat, melyek a vizsgálati cél szerinti adatigény teljesítéséhez hozzájárulnak. Ennek keretében meghatározásra kerül, hogy az egyes adattípusok melyik adattárolóban érhetőek el (pl.: fejegység, ECU-k, EDR, stb.). A

szakértői szoftverből megállapítható, hogy melyik gyártmány milyen központi egységgel rendelkezik és melyek a potenciálisan kinyerhető adatok.

A szakértői vizsgálat előkészítése, megtervezése során szükségessé válhat a kirendelő, megrendelő által meghatározott kérdések pontosítása, az alapvető információk egyeztetése, amely a **Kommunikációs fázis**ban, a megfelelő kommunikációs csatorna kialakításával kezdődik. Ezen fázisban a vizsgálati célok szükség szerint pontosításra kerülhetnek, illetve az adott esethez kapcsolódó feladatok megtervezéséhez, meghatározásához elengedhetetlen plusz információk is beszerezhetőek.

A vizsgálati célhoz kapcsolódóan, a szakértői vizsgálat gyakorlati megkezdése előtti fázis a **Vizsgálat előkészítése**, ami két részre osztható a vizsgálandó jármű vagy annak egységeinek hozzáférhetősége alapján:

- a jármű jelenléte nélkül elvégezhető előkészítő feladatok,
- a járművel kapcsolatosan elvégzendő előkészítő feladatok.

A jármű jelenléte nélkül elvégezhető előkészítő feladatok közé tartozik például a szükséges vizsgálati lépések és feladatok megtervezése, az erőforrás-allokáció, a vizsgáló eszközök (pl. hardver-, szoftverelemek) meghatározása.

Attól függően, hogy milyen adatok kinyerése szükséges, a **Bizonyítékforrás-azonosítási fázis**ban megkülönböztetünk:

- járműbe gyárilag beépített információs eszközöket (pl.: fejegység, háttér tároló) és azok adatait,
- járműbe utólag beépített információs eszközöket és azok adatait,
    - amelyek adatai a jármű informatikai rendszerében tárolódnak el (pl.: infotainment eszközök),
    - amelyek a jármű informatikai rendszeréből származó adatokat gyűjtik, valamint
- harmadik fél által tárolt jármű működésével kapcsolatos specifikus adatokat (pl.: RSU – Road Site Unit, más autók, szolgáltatók, felhő szolgáltatások).

A vizsgálandó jármű paramétereinek meghatározását különböző erőforrások segítik. Ilyen például az általános irodalom, ami publikusan elérhető, a szakmai irodalom vagy gyártói dokumentációk, valamint a kutatók és szakértők által készített saját dokumentáció, a korábban elvégzett vizsgálatok tapasztalataival, módszereivel, eljárásaival.

BMW

Gyártmány
BMW
Támogatott vezérlő egység (ECU)
BMW NBT
Járműből potenciálisan kinyerhető adatok
Csatlakoztatott eszközök Helyek Események Rendszer Konfiguráció Komponensek Szenzorok Diagnosztika Azonosítók Naplók

35. ábra Járműből potenciálisan kinyerhető adatok a támogatott vezérlő egységtől függően

A vizsgálati célok jellemzően egyediek, az adott esethez, eseményhez kapcsolódóak, azonban általánosságban elmondható, hogy valamely, a járműben feltételezhetően elérhető adathoz, adatcsoporthoz kapcsolódnak. Az adatigény alapján, az adott járműhöz kapcsolódó technológiai, gyakorlati és dokumentációs ismeretekből meg kell határozni azon adatforrásokat, melyek a vizsgálati cél szempontjából relevánsak lehetnek. Ennek keretében meghatározásra kerül, hogy az egyes adattípusok melyik adattárolóban érhetőek el (pl.: fejegység, ECU-k, EDR, stb.) és ezek szakértői szoftver által támogatottak-e, vagy egyedi megoldások alapján vizsgálhatóak lesznek.

A vizsgálathoz szükséges eszközkészlet, azok használatához szükséges tudáselemek összegyűjtése során olyan információk kerülnek meghatározásra, mint, hogy:

- a jármű rendelkezik-e olyan adathordozóval, amelyből kinyerhetőek a vizsgálati célok szerint szükséges adatok,
- a járműben használt vezetékes és vezeték nélküli csatlakozási pontok alkalmasak-e a szükséges adatokhoz történő hozzáférésre,
- milyen mértékben lehet megbontani, szétszerelni a járművet,
- rendelkezésre állnak-e a jármű vizsgálatához szükséges szakértői eszközök, képességek, a szaktudás megfelelő-e.

A járművel kapcsolatosan elvégzendő előkészítő feladatok közé tartozik a járműhöz laboratóriumi vagy külső helyszínen történő hozzáférés, a jármű szükség szerinti megbontása. Lehetséges ugyanis, hogy az egyes járműegységekben (pl. fejegység, ECU, EDR) tárolt adatok kigyűjtéséhez szükséges azok megbontása, illetve a járművekből való eltávolítása.

A szakértői vizsgálati gyakorlatban a vizsgálati tárgy felkutatása – speciális esetek kivételével – nem a szakértői munka része. A szakértő a vizsgálati tárgyat az előző fázisok eredményeként kapja meg, és kezdi meg annak azonosítását. A járművekhez kapcsolódó szakértői vizsgálatok esetén ettől a gyakorlattól eltérő, speciális a helyzet*, ezért a* **Bizonyítékmegőrzési fázis***ban kerül erre sor*. A vizsgálati tárgy fogalmi definíció szerint a jármű adattárolásra, -feldolgozásra, illetve -továbbításra használt eszköze, amelyet a szakértő dokumentált módon elemez, és az azokból kinyert adatokat felhasználja. Ezek az adattárolók járművek esetén a megelőző fázisban tárgyalt módon a jármű különböző részein, eltérő hozzáférhetőséggel érhetőek el, emellett a szakértői szoftver által sem minden esetben ismertek. Az adattárolókhoz való hozzáférés a jármű részleges megbontásával, szétszerelésével jár, amihez szükség lehet autószerelő szakember bevonására is. A járműben található adathordozók felismerése általános esetben az egyes adattároló egységek alapvető jellemzői alapján történhet, elsődlegesen azok fizikai jellemzői és a gyártói, üzemeltetői dokumentáció alapján. Amennyiben az adattároló eszköz elektronikus úton is kiolvasható digitális azonosítót tartalmaz, az az egyéb azonosítók mellett felhasználható az eszköz azonosítására.

Digitális adatok kinyerésének alapvető technikája a vizsgálandó adatokról történő másolat készítése. A járművek szakértői vizsgálat minden fázisában az adathordozókat egymástól elkülönített módon, azok egyedi jellemzőinek, sajátosságainak megfelelően kell kezelni. A cél az egységek védelme, az adathordozók és a lehetséges digitális adatok eredeti állapotának fenntartása. A járművekhez kapcsolódóan a vizsgálatok szempontjából a hozzáférhető adatok négy csoportra oszthatóak:

- aktív adatállományok,
- törölt adatállományok,
- illékony adatállományok,
- átvett, külső adatállományok.

Az első csoportban azok az adatok szerepelnek, amelyek a vizsgált adathordozó aktív adatállományaihoz tartoznak, ezek az információk a járműből eredeti állapotukban kinyerhetőek és feldolgozhatóak, különböző metaadatokat (pl. időbélyeget) tartalmazhatnak.

A második csoportba azok az információk tartoznak, amelyek korábban törlésre kerültek. Ebben az esetben az eredeti adatállomány helyreállításának sikeressége a felülírás mértékétől vagy az alkalmazott technológiától (pl. egyedi vagy ismeretlen fájlrendszer) függően változhat. A helyreállított állomány adattartalma optimális körülmények között megegyezik az eredeti fájllal, illetve a metaadatok is vizsgálhatóvá válnak.

A szakértői vizsgálat szempontjából az adatok harmadik csoportját az ún. illékony adatok alkotják, amelyek kizárólag az adott eszköz memóriájában, korlátozott ideig találhatóak meg. A gyakorlati vizsgálatok során megállapításra került, a jármű saját navigációs rendszere és a csatlakoztatott mobil eszköz által futtatott navigációs alkalmazás magasabb szintű együttműködése. Ennek keretében például az alkalmazás által tervezett útvonalhoz a jármű táblafelismerő rendszere, már a megtervezett út szerint következő közlekedési táblát jelezte elő (a navigációs alkalmazás az autópályáról való lehajtást tervezte meg, a jármű pedig már az ott előírt sebességkorlátozást jelezte előre). Ezek a feldolgozást követően azonnal vagy azután rövid időn belül – legkésőbb az eszköz kikapcsolását, áramtalanítását követően – törlődnek (pl. hibatároló-, naplóállományok, vagy cache adatok). Ezen rövid ideig tárolt (illékony) adatok kinyerése és vizsgálata ún. live forensics (élő adatok vizsgálata) keretein belül lehetséges.

Az adatok negyedik kategóriájába a járműtől alapértelmezetten független, ahhoz valamilyen vezetékes vagy vezeték nélküli módon csatlakoztatott adattárolási technológia útján megőrzött információk tartoznak. Ezek továbbításra kerülhetnek gyártói, szolgáltatói vagy privát szerverekre, felhő- (cloud) vagy köd- (fog) alapú rendszerekbe, ilyen például a forgalomtechnikai eszközök által fogadott vagy érzékelt, majd tárolt adatok köre.

A járművek infotainment rendszere, mint ember-jármű interfész segíti a járművezetőt a különböző vezetési és multimédiás funkció vezérlésében. Lehetővé teszi például - akár hangvezérléssel is - a multimédiás tartalom lejátszását, biztosítja a navigációt, az okos eszköz integrációt, a jármű működési és biztonsági beállításait, az ülés pozíció módosítását, vagy a kameraképek megjelenítését.[145] Szakértői vizsgálati szempontból az egyik leggazdagabb adatkészletet biztosító vezérlőegységről beszélünk. Nem csak specifikus vezérlések adatait tartalmazza, hanem a jármű működésére általánosan befolyást gyakorló elemről.

36. ábra Jármű multimédiás fejegység, az egyik leggazdagabb adatforrást biztosító elem a szakértői vizsgálatokhoz [146]

Attól függően, hogy online, vagy offline vizsgálatról és adatkinyerésről beszélünk, a járműhöz történő kapcsolódás vezetékes és vezeték nélküli csatlakozással történhet. USB csatlakozón keresztül (USB-Ethernet átalakító segítségével), közvetlenül a vizsgáló eszközhöz kapcsolható a jármű, vagy közvetlenül csatlakoztatható egy USB-s adathordozó, amire az adatok másolása történik. Első esetben a szakértői szoftver közvetlenül hozzáfér a jármű fejegységében található adatokhoz, képes azt hiteles módon, változtatás nélkül kinyerni/letölteni a későbbi elemzéshez, értelmezéshez. Második esetben a járművet szerviz módba állítva, a megfelelő lépéseket végrehajtva (az érintő kijelzőn beállítva) kimenthetőek a tárolt adatok az USB-s adathordozóra.

37. ábra Egyes járműtípusok fejegységek adatai USB csatlakozón keresztül kinyerhetőek [306]

A járművek fedélzeti diagnosztikai rendszercsatlakozóján (OBDII) keresztül lehetőség van a jármű működéséhez kapcsolódó információk kiolvasására szakértői szoftverekkel, szerviz szoftverrel, vagy az eseményadatok kinyerésére (EDR) speciális eszköz (CDR - Crash Data Retrieval) segítségével. OBDII csatlakozón keresztül a CDR olvasó hozzáfér a légzsákvezérlőhöz, vagy egyéb biztonsági vezérlőhöz, melynek funkciója az eseményadatok rögzítése, majd kiolvassa a tárolt adatokat.

Pre-Crash Data -5 to 0 sec				
Time Stamp (sec)	Vehicle Speed (MPH)	Engine Speed (RPM)	Service Brake (On, Off)	Steering Wheel Angle (degrees)
-5	92	3574	ON	-2
-4	86	3382	ON	0
-3	82	3190	ON	4
-2	79	3190	OFF	-12
-1	79	3062	OFF	-48
0	72	2788	ON	-37

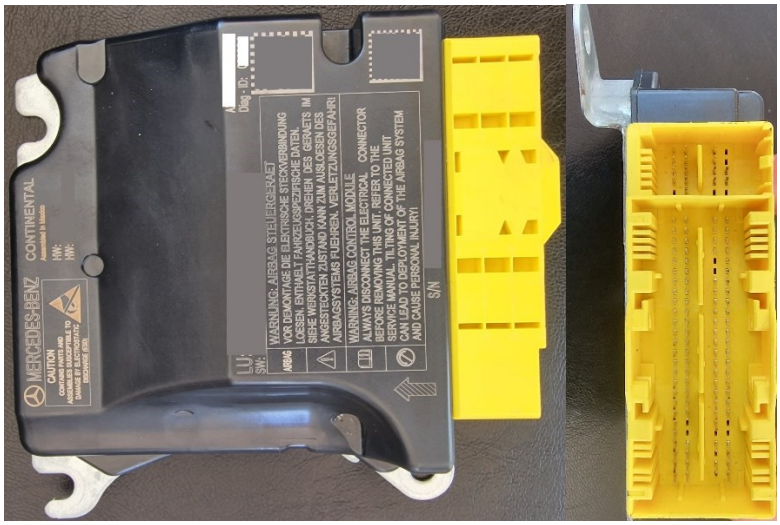
38. ábra Eseményadat rögzítőből kinyert ütközés előtti jármű adatok[73]

Olyan adatok érhetőek el így (jellemzően, de nem minden esetben), mint:

- a jármű sebessége,
- fordulatszám,
- fék státusza,
- kormánykerék forgatási szöge,
- az ütközéshez kapcsolódó sebességváltozás (delta-V),
- a biztonsági öv állapota,
- gázpedál helyzete,
- sebességfokozat,
- légzsák kioldási adatok, stb.[73]

Abban az esetben, ha a jármű állapota nem teszi lehetővé a baleseti adatok diagnosztikai porton keresztüli kinyerését - például a jármű működésképtelensége, túlzott roncsolódása a baleset kapcsán- a baleseti adatok a jármű megbontásával, közvetlenül a tárolóból (pl.: légzsák vezérlőből) is kinyerhetőek. A baleseti adatok rögzítésére szolgáló vezérlők a járműben minél biztonságosabb helyre kerülnek elhelyezésre annak érdekében, hogy egy súlyos baleset esetén is védettek maradjanak, az adatok kinyerhetőek legyenek, hasonlóan a repülőgépek fekete dobozához. Az ilyen vezérlők, például légzsák vezérlők robosztus kialakításúak, a kesztyűtartó mögött, vagy a vezető/utas oldali lábtérben, a középkonzol aljában, stb. találhatóak, a jármű gyártói leírása szerint. A járművet megbontva hozzáférhetőek ezek a vezérlők, melyek így

laboratóriumi körülmények között is vizsgálhatóvá válnak. Speciális csatlakozó segítségével csatlakoztathatóak a CDR olvasóhoz. A csatlakozón keresztül kap tápfeszültséget mind az olvasó, mind a vezérlő.



39. ábra Légzsákvezérlő, mint a baleseti adatok rögzítésére szolgáló vezérlő és speciális csatlakozója

40. ábra Légzsákvezérlő csatlakoztatási módja CDR olvasóhoz

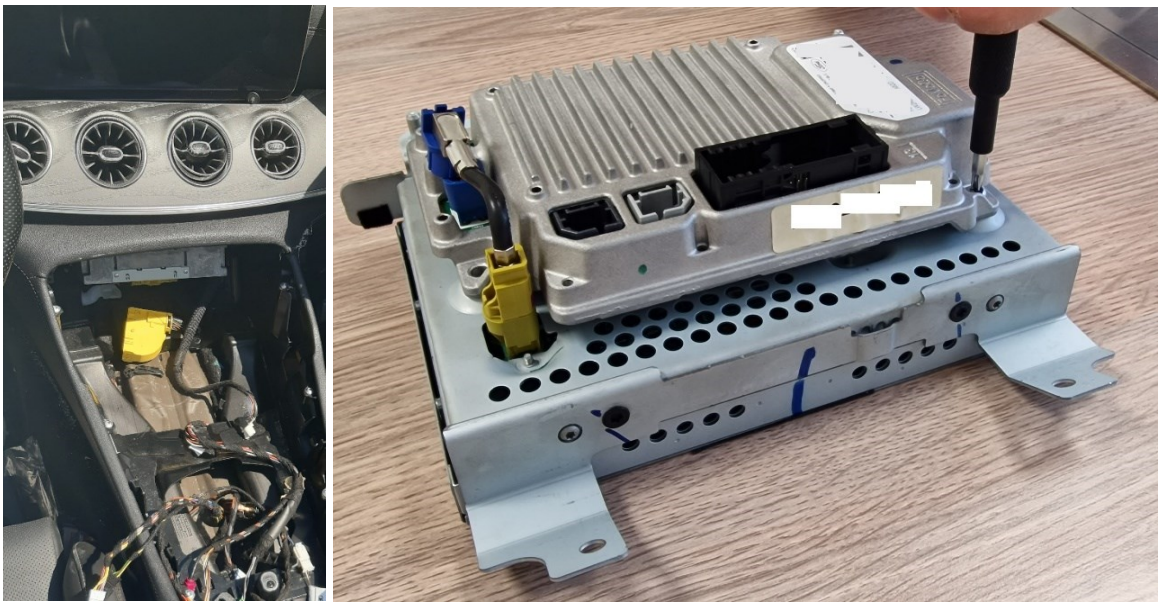
Harmadik, a jármű megbontása nélkül elvégezhető adatkinyerési megoldás az ún. SD-kártyára történő képalkotás. Ebben az esetben a jármű adathordozójához, az azon található állományokhoz – előzetesen, speciális módon, preparált memóriakártya segítségével történik a kapcsolódás, majd az adatok hiteles mentés formájában kerülnek kimentésre. Az adatgyűjtést jellemzően a jármű működőképes - bekapcsolt vagy segédüzemmódjában (auxiliary mode) –

állapotában lehet végrehajtani, az előkészített szakértői adathordozóra (memóriakártya). Ezt követően a jármű fejegységét működésbe hozni, a rendszerindítás befejezését követően csatlakoztatható a memóriakártya. A jármű fejegysége a kártyát beolvasva automatikusan elindítja az ott található szoftvert. A szoftver, szakértői beavatkozást követően - a megfelelő menüpontokon végighaladva az érintő képernyőn – az adathordozóra másolja a járműben elérhető adatokat. A módszer korlátozott számú, „VAG” csoportba (Volkswagen csoport) tartozó gyártmány (pl.: Audi, Lamborghini), típus és fejegység verzió esetén működik.

41. ábra Adatkinyerés jármű fejegységből, memóriakártyával

A jármű megbontásával, szétszerelésével járó szakértői vizsgálatok alatt a releváns adatokat tároló vezérlő egységhez, fejegységhez, adattárolóhoz történő hozzáférést és az adatok kinyerését értjük. Az adathordozókhoz történő hozzáférés módja, annak típusától függően változhat. A jármű központi egysége, fejegysége jellemzően a műszerfal közép konzoljában:

- a center stack-ben (középkonzolban), a kijelzőtől elkülönítve (pl.: a rádió/infotainment alatt, mellett, vagy mögött),
- a center dash-ben (műszerfal központi része) a kijelzővel/infotainment-el egybeépítve található meg.



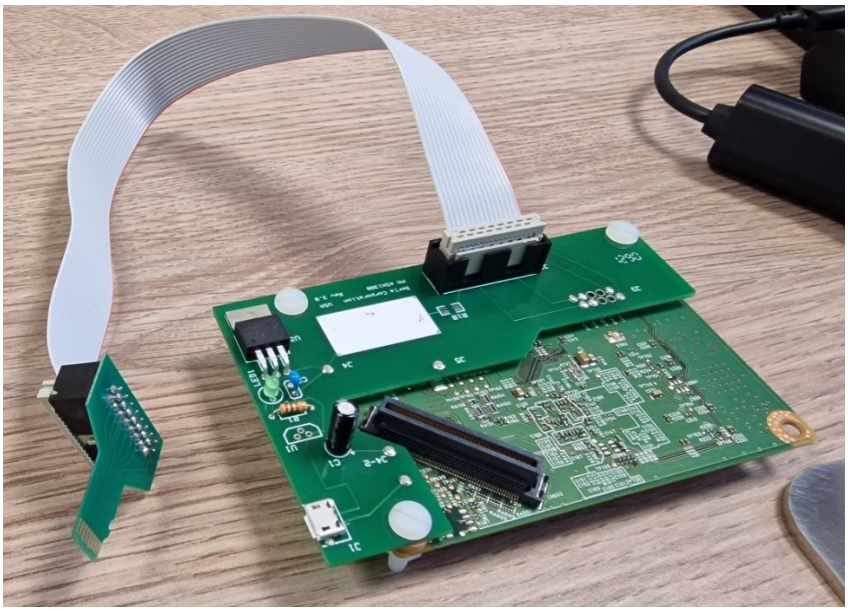
42. ábra Jármű adattároló a közép konzolban. Baloldali képen a légbefúvók alatt található a vezérlő egység, a kijezőtől elkülönítve. A jobb oldali képen a kijelző az asztalra fordítva látható, a vezérlő egység eltávolítása céljából.

Egyes járműtípusokban a fejegység egyéb helyeken található, például a kesztyűtartó mögött, sebváltó mellett, vezető vagy utas oldali lábtérben vezetőülés alatt, csomagtartóban stb. Nincs egységes gyakorlat a vezérlők elhelyezési módjára, azt a gyártók egyedileg kezelik. A fejegység mellett egyéb, a szakértői vizsgálat szempontjából releváns ECU-k helye és helyzete, valamint a fejegység elhelyezési módja szintén egyedi, gyártónként eltérő lehet. Ezek a járművek publikusan elérhető gyártói dokumentációjából, szerviz leírásokból ismerhető meg, vagy a márkaszervízhez és gyártóhoz kell fordulni, amennyiben további információ szükséges az adattárolókra, ECU-kra vonatkozóan. A fejegységekben gyártónként eltérő adattárolási megoldásokat alkalmaznak. A járművekben lévő adathordozó lehet memóriakártya, HDD, SSD is.

43. ábra Jármű fejegységben található HDD

44. ábra Jármű fejegység nyomtatott áramköri lapján találhatóak a releváns adatokat tároló integrált áramkörök

Bench-top adatkinyerési módszernek nevezzük a szakértői eszközkészlettel végzett, a jármű vezérlő vagy fejegységén integrált adathordozón tárolt adatokat kinyerését. A hiteles mentés a járműből kiszerelt vezérlő vagy fejegység alaplapján található szervízpontokhoz csatlakoztatott modulok segítségével történik speciális szakértői szoftver által.



45. ábra Bench-top adatkinyerés esetén a járműből kiszerelt fejegység nyomtatott áramköri lapjához csatlakoztatott modul segítségével csatlakoztatható az adattároló a szakértői számítógéphez.

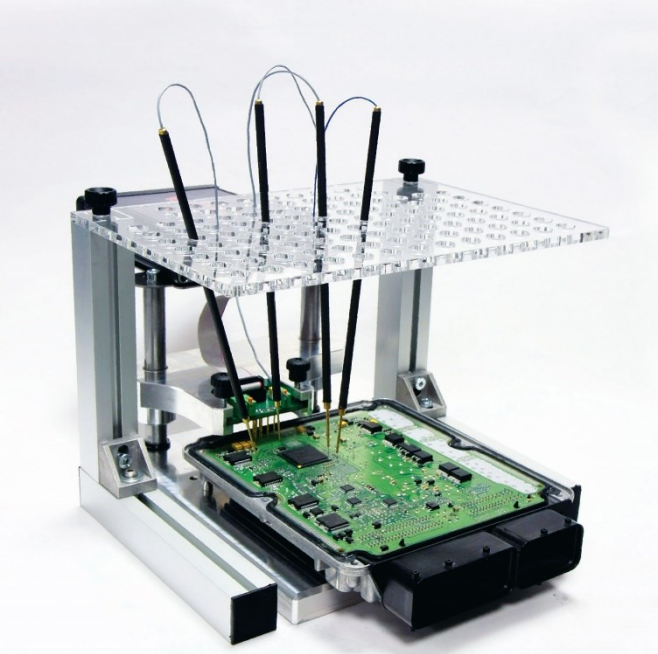
Az eddigi megoldások a jármű és adott esetben a vezérlő vagy fejegység megbontásával járt. Olyan esetekben, amikor az egységekhez történő csatlakozás nem megfelelő eljárás, azokkal a szükséges adatok nem érhetőek el, a chip-off technika segítségével közvetlenül az adattároló integrált áramkörről, memória chip-ről történik az adatkinyerés. Ez nem csupán a vezérlő egység megbontásával jár, az integrált áramkört a nyomtatott áramköri lapról is el kell távolítani, ami roncsolással jár. Az azonosított adattároló integrált áramkör fizikailag, melegítéssel kerül eltávolításra. Az eltávolított adathordozót speciális, a chip „lábaihoz" illeszkedő foglalatba helyezik, így csatlakoztatható a szakértői számítógéphez, majd az adattartalom logikailag olvashatóvá, szakértői szoftverrel elemezhetővé, vizsgálhatóvá válik. A technika alkalmazását követően a nyomtatott áramkör eredeti állapotába történő helyreállítása az esetek többségében nem biztosítható.[252]

Vagyis az adatok kinyerése manuálisan, fizikai vagy logikai hozzáféréssel invazív és nem invazív módon végezhető el. A felsorolt nem invazív módszerek alkalmazása során valamely szabványos csatlakozási lehetőségen keresztül történik az adatokhoz való hozzáférés és azok kinyerése. Ebben a formában ez anélkül biztosítható, hogy fizikailag hozzá kellene férni az egységhez, vagy szét kellene szerelni, meg kellene bontani a jármű műszerfalát vagy az egység burkolatát.

Manuális módon a jármű központi egységének felhasználói felületén navigálva az információk a jármű kijelzőjén jelennek meg. Fizikai hozzáférés esetén az adattároló (például

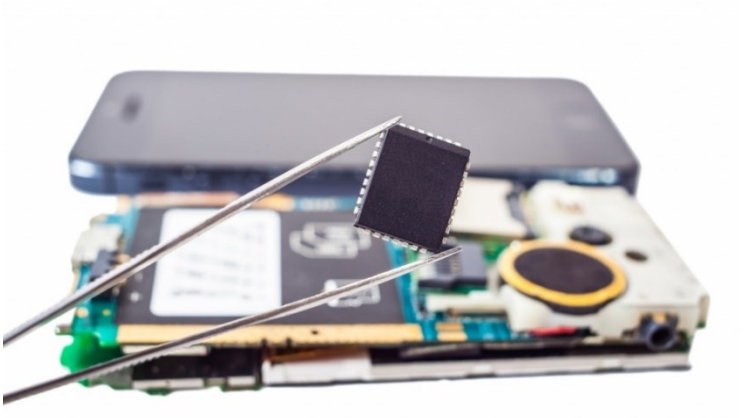
memóriakártya) eltávolítható a járműből. Logikai hozzáférés esetén a fejegységből, vezérlő egységek memóriájából vagy azok egy eleméből nyerhetőek ki információk, függetlenül attól, hogy azok aktívak, vagy korábban már törölt adatokról van szó.

Invazív módszer alkalmazása során az egységekhez és a bennük tárolt adatokhoz a jármű műszerfalának, adott esetben az egység burkolatának szétszerelésével, megbontásával történik a hozzáférés. Az adatok kinyerésére ebben a formában több megoldás alkalmazható, például a JTAG módszer, a „chip-off" eljárás vagy a MicroRead módszer. A JTAG módszer esetén a vezérlőegységen található szervizpontok, kivezetések, csatlakozók felhasználásával, azokhoz való csatlakozással, azokat a vizsgáló eszközzel összekapcsolva válnak kinyerhetővé a tárolt adatok.



46. ábra: JTAG módszer alkalmazása, a vezérlőegység szervizpontjainak kivezetése [4]

Chip-off eljárás esetén a memóriachipet eltávolítják a vezérlőegységből, annak adattartalmát beolvassák a vizsgáló eszközbe, és bitenkénti másolat készül róla a további elemzés elvégzéséhez.



47. ábra: Chip-off eljárás[83]

A MicroRead módszer a leginvazívabb, legkifinomultabb megoldás, melynek alkalmazása során a memória-áramkör tokjának eltávolítása után, nagy teljesítményű elektronmikroszkóppal történik a vizsgálat. Ez a megoldás a NOR és NAND kapuk fizikai állapotának megfigyelésével ad képet a memóriáról, annak működéséről.[97][141][170]

A modern és egyre inkább önvezetővé váló polgári vagy katonai felhasználású közúti járművek esetén a szakértői vizsgálatok elvégzéséhez speciális eszközkészlet, tudás és képesség és módszertan szükséges. Az adatokhoz történő hozzáférés gyártónként, akár jármű típusonként és évjáratonként is változhat. Ez a változatosság és a járművek egyre magasabb automatizáltsági szintje szükségessé teszi a járműdiagnosztikai és szakértői eszközök, megoldások folyamatos fejlesztését.[41][206][242][260][266][301]

Az adatgyűjtési/ nyomrögzítési fázis előtt fel kell mérni a vizsgálat alá vont elemek állapotát. A vizsgálatot megelőzően a járműről, az adattárolók megbontás, szétszerelés előtti állapotáról, a szétszerelési folyamatról képi (digitális fénykép vagy videó, lásd például az alábbi ábrán) dokumentáció készítése szükséges. Be kell azonosítani a jármű jellegét, gyártóját, típusát, egyedi azonosítóit, a jármű és az adattárolók általános állapotát.[40][258]

48. ábra Egy Mini Cooper műszerfala szétszerelés után (szerző saját fotója)

Az **adatgyűjtési/nyomrögzítési fázis** során a járművekben hozzáférhető digitális adatok forenzikus módszerekkel, másolatkészítés útján kerülnek rögzítésre annak érdekében, hogy lehetővé váljon a további szakértői vizsgálatok elvégzése és a kirendelésben meghatározott szakkérdések megválaszolása. A digitális nyomrögzítés eredménye minden esetben maga az elektronikus adat, amely a bizonyítás alapját képezheti. Ebben a szakaszban történik az igazságügyi másolat vagy lemezkép (image file) létrehozása az egyes adattároló egységekről, amely történhet fizikai vagy logikai másolat formájában. A folyamat célja az adatok hiteles és megismételhető módon történő rögzítése, miközben azok integritása és bizonyító ereje megmarad.[238]

A mentési folyamat során a járműben található, illetve onnan letölthető adathordozók, adattároló- és vezérlőegységek, valamint az ezekhez kapcsolódó külső adathordozókon tárolt adatok kerülnek biztonságos rögzítésre. Ide tartozhat például a működőképes járműből történő adatkinyerés vagy a fejegység (head unit), illetve az elektronikus vezérlőegységek (ECU-k) adattárolóinak kiszerelt állapotban történő mentése. A folyamat célja az, hogy a releváns

digitális információk teljes körűen, az adatintegritás megőrzése mellett kerüljenek megőrzésre és hozzáférhetővé váljanak a későbbi szakértői elemzés számára.

Járművek esetén, a mobileszközök vizsgálatához hasonlóan, lehetőség nyílik több logikai adatgyűjtési mód végrehajtására, például:

- Szelektív adatgyűjtés: A támogatott digitális adatok egy részének kinyerése a jármű valamely adattárolási kapacitással bíró egységéről.
- Fájlrendszer kinyerése: A fájlrendszer szerkezetének és tartalmának kinyerése a jármű valamely adattárolási kapacitással bíró egységéről. Ez lehetővé teszi a szakértő számára látható összes adat megszerzését.
- Fizikai adatgyűjtés: Másolat készítése a jármű fizikai memóriájáról. Ez a módszer gyakran destruktív, azaz a memóriachip eltávolítását (chip-off) jelenti, egy, a memóriachipek elérésére szolgáló ipari szabvány (JTAG) használatával. Ez a módszer a legteljesebb, és lehetővé teszi a törölt adatok helyreállítását.
- Univerzális integrált áramköri kártyáról (például SIM) történő adatgyűjtés: Támogatott adatok kinyerése a UICC-ről.
- Távoli adatgyűjtés: Hálózaton keresztül történő hozzáférés az adatgyűjtés elvégzésére.
- Vizuális adatkinyerés: Ez esetben a járműbe épített kijelzőn megjelenő adatok begyűjtése történik meg képrögzítő technológiákkal.

Balesetet szenvedett vagy egyéb behatás által érintett járművek esetén szükség lehet az adathordozón tárolt adatok kinyerése érdekében az egység, eszköz működőképességének helyreállítására. A működőképesség helyreállítása nem a jármű teljes javítására irányul, csupán az adattárolón tárolt adattartalom rögzítésének lehetővé tételére. Az elektronikai működőképesség helyreállítása a bűnjel eredeti állapotának megváltozásával járhat, ezért a metódus alkalmazása előtt a szakértőt kirendelő hatóság előzetes írásbeli hozzájárulása szükséges. Minden adatgyűjtési módnak megvannak az előnyei és korlátai, eszközei, így az adatgyűjtés módszerének kiválasztása a rendelkezésre álló eszközöktől és képességektől, valamint a jármű gyártmányától és típusától is függ.

A járművek, mint a közlekedési rendszer integrált elemei, többféle kommunikációs csatornán keresztül kapcsolódnak egymáshoz, a környezeti és pályainfrastruktúrához, valamint a szolgáltatói és gyártói felhőalapú rendszerekhez. Bizonyos vizsgálati célok esetén szükségessé válhat ezen szolgáltatóktól vagy a jármű gyártójától történő közvetlen adatigénylés, amely a járműhöz, annak vezetőjéhez vagy felhasználójához kapcsolódó, kizárólag ezen szervezetek

rendelkezésére álló információk megszerzését jelenti. A szolgáltatói adatkérés kiterjedhet a vizsgált eszközhöz, illetve az ahhoz kapcsolódó komponensekhez – például SIM-kártyákhoz – tartozó adatok beszerzésére is, amelyet a szolgáltató oldaláról, hitelesített eljárás keretében kell végrehajtani.

A V**izsgálati fázis** során történik a kinyert adatok verifikációja, annak bizonyítására, hogy azok nem változtak meg a kinyerés során, valamint a vizsgálati célokhoz szükséges információk azonosítása. A cél a rögzített adatokból a szakkérdések megválaszolását lehetővé tevő információtartalom kinyerése, rendszerezése, dokumentálása, valamint a digitális adatok laikus által is megjeleníthető formába való hozása. Az összegyűjtött adatok vizsgálata során megtörténik:

- a fizikai vagy logikai lemezkép csatolása (mount),
- virtuális környezetben történő indítása, betöltése,
- a lehetséges anti-forensic tevékenységek nyomainak időbeni azonosítása,
- a jármű operációs rendszerének azonosítása,
- az adatredundancia megállapítása és ellenőrzése,
- a reverse engineering eszközök használata,
- a bizonyítékok mélyreható, szisztematikus keresése,
- a helyreállított adatok vizsgálata,
- a bizonyítékok validálása,
- az üggyel kapcsolatos rejtett adatok visszanyerése,
- az idővonal elkészítése.

A vizsgálati szakaszban minden nyomot meg kell vizsgálni annak jellegének megfelelően. A hozzáférhetővé tett adatok feldolgozása és rendszerezése megvalósítható a törölt állományok helyreállításával, valamint a szakértőt kirendelő határozatban vagy végzésben meghatározott szempontok szerint végrehajtható az adatok célirányos keresése, szűrése, elemzése és dokumentálása a feltett szakkérdések megválaszolása érdekében.

A vizsgálat eredményei alapján az eljáró szakértő a kirendelő határozatban megfogalmazott kérdésekre válaszol. A szakértő az általa megfogalmazott válaszban tényeket közölhet, illetve a nyomok értékelése alapján valószínűsítést alkalmazhat. Az **Elemzési fázis**ban az elemzés olyan mélységű dokumentáltsággal készül, amely alapján végig követhető és megítélhető a vizsgálati eredmények helyessége, illetve a vizsgálat ismételt elvégzése azonos eredményre vezet (megismételhetőség elve).

A vizsgálati eredmények értelmezése (**Értelmezési fázis**) nagyban függ az azt megelőző fázisok eredményeitől, különös tekintettel az esetlegesen figyelmen kívül hagyott elemekre. Egyes szakértői szoftverek lehetővé teszik a strukturált adatok megjelenítését, azok értelmezésének elősegítésére. Többféle elemző, értelmező eszköz segítheti a szakértő munkáját a vizsgált eseményhez kapcsolódó adatok megértésében, például a térkép, az idővonal, amely az események közötti kapcsolatok vizsgálatát segíti elő. Az idővonal-rekonstrukció célja a szakkérdések megválaszolása érdekében a tényállással kapcsolatos releváns események digitális nyomainak időbeli sorrendben, esetlegesen vizuális formában történő megjelenítése.

A szakértői vizsgálat eredménye a dokumentált szakvélemény (**Dokumentációs fázis**), amely leírja a vizsgálat és a digitális adatok elemzésének eredményeit, amely a teljes vizsgálatot vagy csak egy részét ismerteti a jogszabályi és szervezeti követelményeknek megfelelően. A dokumentálás a teljes szakértői folyamatot végig kíséri, az egyes fázisok és végrehajtott lépések teljeskörű, ellenőrizhető módon történő dokumentálása szükséges, a dokumentációs fázis a vizsgálat során folyamatosan dokumentált információk összegzését, rendszerezését és végleges formába öntését jelenti.

A **Validációs fázis**ban a validálás, felülvizsgálat annak megerősítésére szolgál, hogy objektív bizonyítékok gyűjtésével és értékelésével megállapítást nyerjen, hogy a meghatározott követelmények teljesültek-e a szakértői vizsgálat során.

Egyes esetekben a jogi eljárás során a szakértő tanúként is beidézhető (**Eredményközlési fázis**). A hazai jogrendszerben két fő esetet lehet megkülönböztetni, amikor a vizsgálati eredményeket meg kell jeleníteni. Ezek egyike a szakértői jelentés és azon alátámasztó adatok, amelyek alapján egy másik szakértő reprodukálni tudja a vizsgálatot és az eredményeket; a másik a személyes prezentálás a bíróság előtt.[40][246][258][266]

4. Modern és autonóm járművek szakértői vizsgálatához szükséges kompetenciák

A modern közlekedési rendszereket, mint hálózati és információs rendszereket vizsgálva, az általuk működés, használat, védelem és karbantartás céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok alkalmasak lehetnek egy vizsgált esemény, cselekmények részletes feltárására. Valamennyi utólagos szakértői tevékenységet igénylő eljárás (büntetőeljárás, polgári eljárás, közigazgatási eljárás, hatósági eljárás, magán szakértői megbízás) vonatkozásában, kirendelés vagy megbízás alapján a szakértő feladata „*a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását*”[1]. Járművekhez kapcsolódóan két fő vizsgálati típus határozható meg. Egyik a balesetekhez kapcsolódó vizsgálatok, másik a digitális nyomok vizsgálata. A szakértő feladatának ellátásához a hálózati és információs rendszerben, vagyis a járműben, vagy közlekedési rendszer valamely összetevőjében található digitális adatok/nyomok azonosítására van szükség. Vagyis el kell dönteni, hogy a digitális adat releváns-e a vizsgálat szempontjából. „*A digitális bizonyíték olyan digitális adat, amely egy bűncselekmény eseményeinek feltárására, valamely állítás igazolására vagy vitatott kérdés tisztázására, eldöntésére alkalmas*”[206].

A keletkező nagy mennyiségű adat kinyeréséhez, feldolgozásához és elemzéséhez szükséges munka egyre összetettebbé válik, különböző vizsgálati célok mentén a lehetőségek és módszerek jelentős eltérést mutathatnak. Átfogó ismeretek, speciális képességek szükségesek az utólagos szakértői vizsgálatok elvégzéséhez. A szakértői feladat akkor lesz megalapozott (ha a vizsgálat alapelvei betartásra kerülnek), vagyis úgy kell elvégzeni, hogy:

- az adatokról megállapítható, bizonyítható legyen, hogy a vizsgálat szempontjából relevánsak, vagyis olyan információt tartalmaznak, ami a vizsgálati cél teljesítéséhez hozzájárul és ennek okán szükséges annak begyűjtése, kinyerése.
- a vizsgálati eredmények reprodukálhatósága érdekében az adatok vagy az adathordozók kezelési folyamata (azonos eszköz, eljárás és módszer) hitelesíthető és megismételhető kell legyen,
- megállapítható és igazolható legyen, hogy a vizsgálati célok teljesítéséhez a szükséges mennyiségű és minőségű adat és adathordozó összegyűjtése megtörtént,

- „*az elvégzett tevékenységek megfelelő dokumentálásával lehetővé kell tenni azok független vagy egyéb érdekelt fél általi értékelését*” [205],
- igazolható legyen az elvégzett tevékenységek indokoltsága és megfelelősége.

A szakértői vizsgálat során a szakértő a tudomány és a műszaki fejlődés eredményeinek felhasználásával hozzájárul a digitális nyomok kezeléséhez vagy a vizsgált cselekmény (például feltételezett visszaélés, terrorcselekmény stb.) rekonstruálásához, vagy a jogosulatlan tevékenységek megelőzéséhez. Ennek végrehajtásához összetett vizsgálati folyamat végrehajtása és kapcsolódó készség és tudáselemek szükségesek.

Az utóbbi években az IT vonatkozásában egyre hangsúlyosabb munkaerőhiány mellett a kiberbiztonság területén is megnövekedett a munkaerőhiány, valamint a speciális készségek hiánya. Globálisan, a 100 főnél kevesebb munkavállalót foglalkoztató vállalatok 95 %-a nem rendelkezik kiberbiztonsági kompetenciával [99][155] és nincs megfelelő védelmük sem. Ennek kezelésére az Európai Unió megbízásából, az ENISA által elkészítésre került az European Cybersecurity Skills Framework, ami átfogó megoldást képes nyújtani ennek kezelésére.

Az európai kiberbiztonsági kultúra megerősítésére olyan könnyen használható és elérhető, egységes, közös megértést elősegítő, megbízható keretrendszer kialakítása volt a cél, ami bővíthető segíti a kompetenciák értékelését, interoperábilis, szektorokon átívelő és illeszkedik az EU szervezeti struktúrájához.

A keretrendszer kialakítása során felmérésre kerültek a már meglévő hasonló keretrendszerek, kialakításra került egy ún. közös nyelv, ami meghatározza, hogy mit jelent a kiberbiztonság és milyen szerepkörök és feladatok vannak ezen a területen. Ennek eredményeként egy olyan támogató eszköz készült, ami a kiberbiztonsági szerepkörökhöz kapcsolódó feladatokat, kompetenciákat, készségeket és ismereteket határozza meg. A keretrendszer segít a munkaadóknak abban, hogy képesek legyenek megállapítani milyen munkaszerepekre, szerepkörökre lenne szükségük és ehhez milyen kompetenciák szükségesek. Az oktatási, képzési intézmények támpontot ad, hogy milyen területeken milyen képzések nyújtására van szükség a megfelelő kiberbiztonsági oktatás, képzés és munkaerő-fejlesztés biztosításához és harmonizációjához. Az egyéneknek, tanulóknak a karrierválasztásban, hozzájárul a tudásuk és készségeik fejlesztéséhez, segít kiválasztani, hogy milyen irányban, milyen új kompetenciák elsajátítása szükséges.[101]

Nagy előnye a rendszernek, hogy az egyes kiberbiztonsági munkaszerepekre fókuszál, meghatározza azokat az alapkompetenciákat, melyek ahhoz szükségesek, hogy a különféle pozíciók hatékonyan betölthetőek legyenek. 12 profil került meghatározásra:

- Chief Information Security Officer (CISO) – a klasszikus IT biztonsági vezető, vagy felelős szerepkörnek felel meg,
- Cyber Incident Responder – incidenskezelő vagy security operation center (SOC) analist, aki felügyeli a rendszerek állapotát,
- Cyber Legal, Policy and Compliance Officer – adatvédelmi felelős, vagy IT compliance manager a vonatkozó jogszabályoknak és sztenderdeknek való megfelelést biztosítja,
- Cyber Threat Intelligence Specialist – fenyegetettség elemző, fenyegetettségelemzési adatbázisok vizsgálata, trendelemzések, CTI (cyber threat intelligence) elemzések készítése,
- Cybersecurity Architect - biztonsági kockázatok azonosítása, kezelésének támogatása és felügyelete, technológiai követelmények meghatározása, fejlesztések támogatása,
- Cybersecurity Auditor – auditok tervezése és végrehajtása,
- Cybersecurity Educator – képzések végrehajtása, információbiztonsági tudatossági szint növelése,
- Cybersecurity Implementer – kiberbiztonsági rendszerek implementálása, üzemeltetése és használata,
- Cybersecurity Researcher – kutatói feladatok ellátása a kiberbiztonság területén,
- Cybersecurity Risk Manager – kiberbiztonsági kockázatok és hatások menedzselése,
- Digital Forensics Investigator – digitális nyomok vizsgált eseményekkel való összekapcsolása és kapcsolódó feladatok,
- Penetration Tester - rendszerek gyenge pontjainak feltárása és kihasználása, védelmi intézkedések hatékonyságának vizsgálata.[101]

49. ábra ENISA ECSF szerepkörök, beleértve a Digital Forensics Investigator szerepkört [81]

Az ECSF meghatározása szerinti a Digital Forensics Investigator (digitális forenzikus szakértő/vizsgáló), a kiberbűncselekmények vizsgálatához kapcsolódóan biztosítja, hogy minden olyan digitális nyom feltárásra kerüljön, ami a tevékenységek bizonyításához szükséges, vagyis a digitális eszközök és rendszerek utólagos szakértői vizsgálatával, digitális nyomok feltárásával és vizsgálatával foglalkozik. „*A kiberbűncselekmény általános fogalma alatt az informatikai eszközök és/vagy rendszerek segítségével, vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők…*”,[136] azonban „*a kiberbűnözésnek még nincs általánosan elfogadott és egységes definíciója*”.[208] A kiberbűnözést, mint gyűjtőfogalom értelmezve két fő kategória határozható meg:

- információs rendszereken, azokat érintően megvalósuló cselekmények,
- információs rendszerek felhasználásával elkövetett cselekmények.

A rendszereket érintő cselekmények (a cselekmény tárgya a rendszer) közé tartozik például a hálózat vagy rendszer túlterhelésére irányuló támadások (DoS, DDoS támadások[4]), a rendszerek feltörése, vagy kártékony kódok alkalmazása. Online csalás, zsarolás esetén a rendszerek felhasználásával történik a cselekmény.[125]

Napjainkban a modern járművek egyre inkább kitettek a kibertérből érkező fenyegetéseknek. A bűncselekmények több, mint 80 %-a érinti a járműveket.[43] Az egyre inkább önvezetővé váló, hálózatba kapcsolt járművek nem csupán, mint szállító eszköz jelennek meg bűncselekményekben, a cselekmények tárgyaként érintettekké válnak, mint célpontok, vagy felhasználásukkal egyéb rendszerekhez való hozzáférés, behatolás is meg fog jelenni.

A Digital Forensics Investigator profil alternatív megnevezései között az ECSF-ben a Digital Forensics Analyst, a Cybersecurity & Forensic Specialist és a Computer Forensics Consultant is. Ezek a megnevezések hazánkban nem terjedtek el. A piaci gyakorlatban forensics szakértő, vagy a Szakértői tv. alapján igazságügyi szakértő megnevezésekkel találkozhatunk. Utóbbi feladatát a tv. 4. § (1) bekezdése alapján feljogosítással végezheti, névjegyzékbe történő felvétel után. A szakértő küldetése a digitális nyomok és adathordozók azonosítása, az adatok kinyerése vagy visszaállítása és objektív elemzése, vizsgálata.

A modern és egyre inkább önvezetővé váló polgári és katonai járművek szakértői vizsgálata szükséges lehet, amennyiben a jármű alanya vagy célpontja volt a vizsgálandó eseménynek, emellett az összekapcsoltság miatt tartalmazhat olyan digitális nyomot, ami az adott vizsgálatban szükséges. A vizsgálatok célja, a járművekben, járműrendszerekben bekövetkezett események hiteles, rekonstrukciója, felderítése. A releváns eseményekről bizonyítékok szolgáltatása, a későbbi, akár nyomozati és igazságszolgáltatási tevékenységekhez való felhasználáshoz. Az alábbiakban a modern járművek vonatkozásában kerülnek értelmezésre az ECSF-ben meghatározott feladatok.

Mint általános feladat megjelenik a vizsgálati szabályok, tervek és eljárások kidolgozása. A szakértői vizsgálat fentebb tárgyalt alapelveinek betartása érdekében a vizsgálat elvégzéséhez, az egyes vizsgálati lépések végrehajtásához a szakértőnek meg kell határozni, dokumentálni és az érintettek számára közzé kell tenni a vonatkozó szabályokat. Ezekhez alapul szolgálhatnak például egyéb szakértői eljárások és módszerek, szakértői intézetek módszertani levelei,

[4] A szolgáltatásmegtaggadásos (DOS) és az elosztott szolgáltatásmegtagadásos (DDoS) támadások a hálózati szolgáltatások túlterhelésével, megzavarásával a rendszerek, webhelyek és kiszolgáló erőforrásainak kimerítését célozzák. A rendszer lassulásával vagy elérhetetlenségével jár a jogosult felhasználók számára.

kapcsolódó szabványok és ajánlások. A kutatáshoz kapcsolódóan elvégzett vizsgálatok alapján megállapítható, hogy az általános digitális forenzikus vizsgálatok főbb lépései [255], a számítógépekhez kapcsolódó, a hálózatok, cloud és IoT eszközök vizsgálatok egyes elemei alkalmasak a civil és katonai járművek szakértői vizsgálatában történő alkalmazásra, azonban egyedi lépések és megoldások is szükségessé válhatnak. A modern járművek szakértői vizsgálati kihívások (általános kihívások, vizsgálati eljárás kihívásai, vizsgáló eszköz kihívásai [267]) okán, részben a járműipar gyors fejlődése miatt egyelőre nem áll rendelkezésre univerzálisan alkalmazható módszertan a vizsgálatok elvégzéséhez.

A digitális nyomok azonosítása, helyreállítása, kinyerése, dokumentálása és elemzése feladatlépések a digitális forenzikus vizsgálatok egyes folyamatlépéseit jelölik. Járművek vizsgálatához kapcsolódóan – egyebek mellett a számítógépek vizsgálatát is – ez a felsorolás nem teljeskörű, kiegészül további lépésekkel, például adatgyűjtéssel, az adatok vizsgálatával, értelmezésével. A vizsgálat állhat egy folyamatból, vagy lehet iteratív. Ebben az esetben az egyes lépések ismétlése válhat szükségessé.

A digitális nyomok megőrzése és védelme, valamint az érdekelt felekkel történő „megosztás" – számukra történő elérhetővé tétel feladatok lefedik a kinyert adatok integritásának védelmét, ami biztosítja a bemenetet a vizsgálati és elemzési lépésekhez. Limitálni kell a bizonyítékhoz (például jármű vezérlő egységeihez[5], fejegységhez, egyéb adathordozóhoz) való fizikai hozzáférést. Fenn kell tartani az ún. felügyeleti láncot (chain of custody) az esetleges manipuláció elkerülésére, hogy a nyomok kezelésével kapcsolatos idővonal, a hozzáféréssel rendelkezők köre és tevékenységei dokumentált módon rendelkezésre álljon. A felügyeleti lánc alapján megállapítható, hogy az adott adattároló egységet hol tárolták, ki, mikor fért hozzá, ki milyen tevékenységet végzett vele.

A környezet vizsgálata a jogosulatlan, vagy jogellenes tevékenységek azonosítására irányul, mely feladat járművek esetén kettős megközelítésű. Elképzelhető, hogy az egyes adattároló egységek a vizsgált esemény (pl.: baleset) kapcsán megsérültek, vagy külső fizikai beavatkozás történt, vagyis szándékosan megkísérelték a nyomokat eltűntetni. A digitális nyomok szándékos módosítása történhet logikai módon is, valamilyen anti-forensics eljárással, melynek nyomai (pl.: eszköz csatlakoztatáshoz burkolat eltávolítás, karcos csatlakozó) a környezet vizsgálata során megállapíthatóak lehetnek. Annak érdekében, hogy a vizsgálat során a lehető legalaposabban járjon el a szakértő, illetve a vizsgálat során a lehető legtöbb információ

[5] ECU - Electronic Control Unit

rendelkezésre álljon, a fizikai környezetet az eszközök, a jármű állapotát dokumentálni szükséges.

Az elvégzett feladatok, a vizsgálati megállapítások és eredmények szisztematikus dokumentálása és bemutatása feladatok elvégzése részletes, laikusok számára is érthető módon kell történjen. Ebben a feladatban nincs eltérés a járművekhez kapcsolódó vizsgálatok és egyéb digitális forenzikus vizsgálatok között, a dokumentációnak akár eredményekre, akár a vizsgálati eljárásra vonatkozóan kellően alaposnak kell lennie, a megismételhetőség biztosítása érdekében. A Szakértői törvény 47. § alapján a szakvéleménynek „*tartalmaznia kell a leletet, a vizsgálat módszerének rövid ismertetését, a szakmai ténymegállapításokat, a szakértő véleményét, ha az ügyben korábban vizsgálat lefolytatására került sor és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését, a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait és az arra való utalást, hogy az igazságügyi szakértő mely szakterületen jogosult szakvéleményt adni illetve, hogy az igazságügyi szakértő vagy más személy eseti szakértőként járt el*”.[1] Emellett „*A szakvéleményt készítő igazságügyi szakértő az írásbeli szakvéleményt aláírásával köteles ellátni, valamint köteles azon a nyilvántartási számát feltüntetni*.”.[1]

A szakértői vizsgálati, elemzési és jelentési technikák kiválasztása és testre szabása, mint feladat kapcsolódik az első, általános feladathoz, mely szerint a vizsgálat céljának és a járművek sajátosságaiból adódóan szükségessé válhat az egyes vizsgálati lépések módosítása, vagy több technika, megoldás közül szükséges a megfelelő, a hatékonyabb, az eredményesebb kiválasztása. A szakértői feladatok eredményeként rendelkezésre állnak a bizonyítékok, az adatokat is magában foglaló digitális vizsgálati jelentés, illetve az elkészített szakvélemény.

Járművekhez kapcsolódóan a feladatok kiegészülnek a járművek speciális adattároló megoldásaihoz történő fizikai hozzáféréssel, ami a jármű egyes elemeinek (pl.: műszerfal, középkonzol stb.) megbontásával jár. Jármű operációs rendszerének meghatározása, a fájlrendszer vagy titkosítási megoldás meghatározása, továbbá a jármű és környezete (egyéb járművek, környezeti vagy pálya elemek stb.) közti kommunikáció azonosítása, speciális (forensics) eszközök és technikák alkalmazása, vagy az anti-forensics technikák nyomainak azonosítása mind olyan feladat, ami túlmutat a digitális forenzikus vizsgálat során elvégzendő feladatokon és speciális készség és tudáselemeket igényelnek.

A kiberbiztonság területén dolgozók - korosztálytól függetlenül - több, mint feléről elmondható, hogy az IT-ban kezdte munkásságát és innen váltott kiberbiztonságra. Ahhoz, hogy ez a váltás

sikeres legyen új képesség és tudáselemek elsajátítása szükséges. Az ECSF által meghatározott szakértői profilról megállapítható, hogy általánosságban lefedi a főbb forenzikus szakértői feladatokat – a keretrendszer alapvető céljával egyezően -, valamint készség és tudáselemeket, azonban túlnyomórészt ezek a számítógépek és hálózatok vizsgálatain alapulnak, ezért mind polgári, mind katonai járművek vizsgálata során ezek kiegészítése szükséges.

A készség, mint fogalom meghatározható egy megfigyelhető kompetenciaként, egy tanult motoros tevékenység végrehajtásához. A készségmeghatározások leírhatnak egyszerű vagy összetett készségeket. A kiberbiztonsági feladatok ellátásához, ideértve a szakértői feladatok elvégzését is, jellemzően összetett készségekre és azok alkalmazására van szükség. Ilyenek a személyes tulajdonságok, technikai és nem technikai képességek. A gyakorlati tapasztalatok alapján megállapítható, hogy a személyes tulajdonságok közül az analitikus gondolkodás, a problémamegoldás, kritikus gondolkodás, kreativitás, valamint a tanulás iránti elkötelezettség kiemelkedően fontos. Nem technikai készségek közül legfontosabbá az önállóan és csapatban történő munkavégzés, a projektmenedzsment és magas szintű ügyfélkapcsolati gyakorlat, kommunikációs készség vált.[155] Ez összecseng az ECSF által meghatározott kulcs készségekkel, melyek a(z):

- etikus és független munkavégzés, vagyis a belső vagy külső tényezők nem befolyásolják,
- információk begyűjtésének képessége, azok integritásának megőrzése mellett,
- kiberbiztonsági események azonosítása, elemzése és korrelációja,
- bizonyítékok és eredmények egyszerű, könnyen érthető bemutatása, magyarázata,
- részletes, átgondolt és megfelelően alátámasztott vizsgálati jelentés, szakvélemény készítése és kommunikálása.

A fenti készségmeghatározások az egyes szakértői feladatokhoz kapcsolódnak, amiben a szakértő különböző készségeket alkalmaz a feladatok végrehajtása során. A kompetencia a tudás, készségek, képességek, magatartásformák és személyes jellemzők alkalmazásának vagy felhasználásának képessége, munkafeladatok, meghatározott funkciók sikeres végrehajtása, illetve adott szerepkörben vagy pozícióban való működése érdekében.

A tudás alatt az egyértelműen és közvetlen módon felidézhető, könnyen és gyorsan hozzáférhető, a világgal, az adott témával kapcsolatos fogalmak, tények és képzetek összessége, nagyobb egységekbe. A tudás speciális formái: a szakértelem és a műveltség. A szakértelem egy adott szakterület (esetünkben a szakértői tevékenység) által meghatározott ismeretek és

készségek együttese, egy adott szakterületre vonatkozó magas szintű tudás és átlagot meghaladó mennyiségű és szervezettségű tudásséma, magas szintű ismeretek és készségek együttese jellemzi, amelyek lehetővé teszik egy adott szakterület logikája köré szerveződő ismeretek hatékony feldolgozását és alkalmazását. A műveltség a mindennapi életben releváns és felhasználható ismeretek, készségek és képességek összessége.

Az ECSF által meghatározott kulcs tudáselemek a járművekhez kapcsolódó vizsgálatok esetén szintén csak főbb irányokat határoznak meg, ezek mellett kiegészítő ismeretekre is szükség van. A szakértői szerepkörben az ECSF alapján, a feladatok ellátásához kapcsolódóan az alábbi tudáselemekre vagy szükség:

- digitális forenzikus és jogi eljárásokhoz kapcsolódó szabályok, sztenderdek, ajánlások, módszertanok, keretrendszerek és a jó gyakorlatok,
- elemzési, tesztelési eljárásokkal kapcsolatos tudáselemek,
- kiberbiztonsággal kapcsolatos jogszabályok, követelmények,
- számítógépes rendszerek sérülékenységei, támadások, kiberfenyegetések,
- számítógépes hálózatok és operációs rendszerek ismerete,
- kártékony kódok elemzése.

A digitális forenzikus eljárások szabályok, sztenderdek, ajánlások, módszertanok, keretrendszerek és a jó gyakorlatok ismerete nélkülözhetetlen a járművek vizsgálata esetén is. A különböző elemzési és tesztelési eljárások ismerete és alkalmazása szintén szükséges. Mivel a modern járművek, egyre inkább gördülő adatközpontokká, vagy komplex hálózatot alkotó IoT eszközökké válnak, a számítógépes rendszerek és hálózatok sajátosságai, támadási vektorai esetükben is megjelennek, emellett ki is bővülnek (pl.: járművek irányításának távoli átvétele).

A modern és egyre inkább önvezetővé váló közúti járművek esetén a kártékony kódok elterjedése még várat magára, azonban a mobiltelefonokon is népszerű operációs rendszerek (pl.: android) járművekben való elterjedése felgyorsíthatja a járművek ellen irányuló támadásokat. Ezek vizsgálatához a szakértőknek speciális ismeretekre lesz majd szükségük.

A kooperatív intelligens közlekedési rendszerekben működő járművek speciális kommunikációs és hitelesítési eljárásokat alkalmaznak. Ezen forgalmak és protokollok, adattárolási megoldások ismerete nélkül nem végezhető el a járművek szakértői vizsgálata, nem teljesíthetőek a vizsgálati célok. A különböző járműgyártók, színes típusválasztéka és kiadásai szükségessé teszik a járműdiagnosztikai eszközök és hibaazonosítási megoldások, a járművek

fizikai felépítésének és főbb elemeinek, az egyes komponensek funkcióinak ismeretét, a belső topológia értelmezésének képességét.

Modern járművek szakértői vizsgálatához szükséges tudáselemek

A tudás jelentésének értelmezésére többféle leírás használatos, de kijelenthető, hogy a tudás a legtöbb értelmezés szerint tanulás útján jön létre, ami nem más, mint a rögzült tapasztalatok kommunikáció folyamatai révén történő átvitele.[290][311][312] A tudás tág fogalom, lehet gyakorlati vagy elméleti, számos ága és területe van. A tudás az az információ és készség, amelyet az emberek szellemi, kognitív képességeik révén szereznek, oly módon, hogy megszerzik, azonosítják, megfigyelik és elemzik az őket körülvevő tényeket és információkat. A tudás korlátozott, de a rendelkezésre álló, megtanulható források és információk korlátlannak tekinthetők. A tudományos ismeretek tudományos módszerrel szerezhetőek meg, melynek lépései: megfigyelés, indukció, hipotézis, kísérletezés, elemzés és következtetés. A tudás az egyértelműen és közvetlen módon felidézhető, könnyen és gyorsan hozzáférhető tudást írja le. A világgal kapcsolatos fogalmak, tények összessége, nagyobb egységekbe, sémákba szerveződnek és irányítják tudásunk felhasználását. A tudás speciális formái: a szakértelem és a műveltség.[312][313][314][315] A kutatás témájához kapcsolódóan a szakértői tudás a modern járművekkel kapcsolatos fogalmak, tények összessége, amelyek rendezett módon segítik elő ezek felhasználását. Az egyes tudáselemekhez négy fő csoport került meghatározásra a vizsgálatokhoz kapcsolódóan:

- Általános informatikai tudás:
    - Alapvető számítástechnikai tudás,
    - Internetes eszközök ismerete,
    - Speciális szoftverek kezelésének ismerete,[293]
- Szabályozási követelmények:
    - Jogszabályi tudás,
    - Szakmai szabályok ismerete,
- Járművekhez kapcsolódó tudás:
    - Járművek alapvető műszaki ismeretei,
    - Speciális járműelektronikai tudás,
- Vizsgáló eszközökhöz kapcsolódó tudás:
    - Hardver eszközök ismerete,
    - Szoftver eszközök ismerete.

Az általános informatikai tudás csoportba tartozik az alapvető számítástechnikai tudás, amely, mint alapvető digitális kompetencia, nélkülözhetetlen a szakértői tevékenység elvégzéséhez is. Ide tartozik például a számítástechnikai alapfogalmak, a leggyakrabban használatos irodai szoftverek ismerete, szövegszerkesztő, táblázat és adatbázis kezelők, levelező rendszerek, vagy a különböző operációs rendszerek ismerete. Az internetes eszköz ismerethez tartozik például a kollaborációs és projektmenedzsment eszközök, adatlapok kezelésének ismerete, a járművek szakértői vizsgálatához kapcsolódóan azonban ilyen speciális tudás nem feltétlenül szükséges. Speciális szoftverekhez kapcsolódó tudáshoz tartozik például különböző programozási nyelvek és környezetekhez kapcsolódó ismeretek, az alapvető struktúrált programozási alapfogalmak, és programozási nyelvek szintaktikájának ismerete. Továbbá az adatelemző, speciális adatbázis kezelő vagy vállalatirányítási rendszerek felépítésének, funkcióinak, vagy tervező programok ismerete.[173][174][218][225][226][228]

4. táblázat Általános informatikai tudáselemek csoportosítása

Általános informatikai tudás	
Alapvető számítástechnikai tudás	**Speciális szoftverek**
OSI modell ismerete.	Adatmentés és visszaállítás ismerete.
IT és jármű-kommunikációs, valamint hálózati fogalmak, felépítés és protokollok ismerete.	Fájlrendszer típusok ismerete.
Rendszer fájlok (pl.: naplófájlok, adatbázisok, konfigurációs fájlok) általános tartalmának és tárolási helyének ismerete.	Adatok típusainak és felismerési módjának ismerete.
Szerver és kliens operációs rendszerek ismerete.	Virtuális gépek, hálózati monitorozó alkalmazások ismerete.

A szabályozási követelményekhez kapcsolódó tudáselemek két csoportra oszthatóak fel. A jogszabályi környezet ismeretére és a szakértői szakmai tudásra.[218][225][226][228] Ezen ismeretek és tudás elemek hozzájárulnak a szakértői tevékenység szakmai szabályoknak (pl.:

módszertani levelek, akkreditációs szabályok, szakmában elfogadott tények, szabványok) és jogszabályoknak megfelelő végrehajtásához, mellyel biztosítható a szakértői vélemény, mint bizonyíték, bizonyító ereje (a szakértői vélemény ezáltal bizonyítékként használható fel).

5. táblázat Jogszabályi követelményekhez kapcsolódó tudáselemek csoportosítása

Szabályozási követelmények - Jogszabályi tudás
Szakértői tevékenységre vonatkozó jogszabályok ismerete.
Kiberbiztonsággal kapcsolatos jogszabályok, rendeletek, irányelvek és etika ismerete.
Személyes adatok védelmével kapcsolatos jogszabályok, rendeletek, irányelvek és etika ismerete.
Bizonyítási, eljárásjogi szabályok ismerete.
Felügyeleti lánc biztosítására vonatkozó követelmények ismerete.

Ezek alapján a szakértői vélemény az adott jogi környezetnek (polgári peres, közigazgatási eljárási, büntetőjogi) megfelelően alakítható ki.

A kiberbiztonsági követelmények, hazai és nemzetközi jogszabályok, rendeletek, irányelvek és etikai elvek alapján végzett szakértői munka biztosítja a digitális nyomok, bizonyítékok biztonságos kezelését, megőrzését, tárolását. Emellett a szakértő képessé válik egy biztonsági esemény idővonalának összeállítására, a vizsgálat során megállapíthatóvá válnak az események bekövetkezési lépései és okai.

6. táblázat Szakmai tudáshoz kapcsolódó tudáselemek csoportosítása

Szabályozási követelmények - Szakmai tudás
Szakértői tevékenységre vonatkozó eljárások, módszertani levelek ismerete.
Szakértői tevékenységre vonatkozó módszertanok, szabványok ismerete.
Naprakész járművekhez és közlekedési rendszerekhez kapcsolódó fenyegetések és sebezhetőségek ismeretek.

A kiberbiztonság hiányának a jármű működésre vonatkozó hatásait magában foglaló tudás.
Szakértői tevékenységre vonatkozó eljárások, módszertani levelek ismerete.
A szakértői munka során kezelt adatok feldolgozásával kapcsolatos fogalmak és gyakorlatok ismerete.
A vizsgálati tárgy kezelésére és megőrzésére szolgáló eljárások ismerete.
Hardver elemek, operációs rendszerek és hálózati technológiák vizsgálati vonatkozásainak ismerete.
Az elektronikus adatok (digitális nyomok) gyűjtési, kezelési, szállítási és tárolási folyamatainak ismerete.
Illékony adatok típusai és gyűjtésének ismerete.
Fájltípusokkal való visszaélésekre vonatkozó ismeretek.
Forensics ajánlások és legjobb gyakorlatok ismerete.
Titkosítási algoritmusok, a szteganográfia és az adatok elrejtésének egyéb formáinak ismerete.
Anti-Forensics taktikák, technikák és eljárások ismerete.
Forensics elemzési eljárások ismerete.

Járművekhez kapcsolódóan átfogó ismeret szükséges a közúti közlekedési járművek tárgykörének alapvető tényeiről, irányairól és határairól, fogalomrendszeréről, működési elveiről. A szakértői vizsgálatokhoz szükséges továbbá alapismeret a jármű elektronikai építőelemeiről (pl.: passzív és aktív alkatrészek, alapáramkörök, vezérlő egységek), a járművekben alkalmazott rendszerek jellemző felépítéséről, a biztonságkritikus feladatokra kialakított architektúrákról, adattároló egységekről és megoldásokról. [74][174][218][225][226][228][291]

7. táblázat Járművekhez kapcsolódó tudáselemek csoportosítása

Járművekhez kapcsolódó tudás	
Járművek alapvető műszaki ismeretei	**Speciális járműelektronika tudás**
Járművek általános fizikai összetevőinek és architektúrájának ismerete, beleértve a különböző komponensek funkcióit.	Járművekben alkalmazott kommunikációs technikák (UART, CAN, LIN, FlexRay, MOST, Bluetooth, V2X, DSRC stb.).
Érzékelők és beavatkozó elemek (aktuátorok) típusai, jellemzői, osztályozása és működési mechanizmusa.	Szenzorok alapfogalmai, a jelfeldolgozás alapjai.
Vezetékezésre és a komponensekre alkalmazott szabványos jelölések.	Szabványos diagnosztikai interfészek.
Jármű villamos rendszer.	Interfészek szerepe, működése.
Alapvető járműfedélzeti perifériák.	Telekommunikáció alapjai, a korszerű átviteli módszerek és azok jellemzői.
Műszaki feladatokkal kapcsolatos fizikai fogalomrendszer, annak leírási módjai.	A kommunikációkhoz köthető jelfeldolgozási módszerek.
Jármű operációs rendszerek ismerete.	Diagnosztikai rendszerek működése, használata.

A modern járművek szakértői vizsgálatához kapcsolódó, leginkább speciális tudáscsoport a vizsgáló eszközökhöz kapcsolódó tudás. Ide tartoznak az egyes vizsgáló hardver eszközök, valamint a speciális szakértői szoftverek ismerete.[46][218][225][226][228]

Modern járművek szakértői vizsgálatához szükséges készségek

A különleges szakértelmet igénylő területek száma, különösen az IT, IoT és egyéb digitális megoldásokat alkalmazó területeken folyamatosan bővül. A társadalmi viszonyok is egyre bonyolultabbá válnak, ami az igazságszolgáltatásban úgy jelent meg, hogy a peres, illetve a hatósági eljárások tárgyi és szerkezeti összetétele jelentős változáson ment át. Jellemzővé vált, hogy a jogi problémák más szakmákat, szakterületeket érintő előkérdéseket érintenek, emiatt a megítélésük egyre nehezebbé válnak. Ezzel párhuzamosan a bírósági eljárásokban megnőtt az igény a modern tudomány eredményeinek a bizonyítási eljárásban történő felhasználása iránt. Különösen igaz ez, a műszaki vonatkozású kérdésekben, például az informatikában és a kommunikációs technológiákkal egyre inkább átszőtt közlekedésben is, ahol a járművek autonomitási szintjének növekedésével is fennmarad az igény a bekövetkezett események utólagos szakértői vizsgálatára, szakértői tevékenység elvégzésére.

Az igazságügyi szakértők feladatait és kötelezettségeit, valamint az igazságügyi vizsgálatok lefolytatására irányuló jogait a nemzeti jogszabályok állapítják meg. A legtöbb ország követelményeket (oktatás, képzés és/vagy igazolás) ír elő az igazságügyi szakértőként történő elismeréshez és egy adott területen az igazságügyi vizsgálatok lefolytatásához. A 2016. évi XXIX. törvény az igazságügyi szakértőkről (szakértői törvény) az igazságügyi szakértői tevékenységet az alábbiak szerint határozza meg: „*jogszabályban meghatározott követelményeknek megfelelő igazságügyi szakértő, illetve az igazságügyi szakértő munkáját segítő egyéb személyek által, a kirendelő hatóság, bíróság, ügyészség, rendőrség, közjegyző, bírósági végrehajtó (a továbbiakban együtt: hatóság) kirendelése vagy megbízás alapján, e törvény által meghatározott szervezeti keretek között, jellemzően szakértői díj ellenében végzett, a hatóság eljárásaiban különleges szakértelmet igénylő tény vagy egyéb körülmény megállapítását vagy megítélését elősegítő részcselekmények összessége, így különösen a szakvéleményhez szükséges vizsgálatok elvégzése, a szakvélemény előkészítése, elkészítése és előterjesztése, valamint a hatóság kérésére annak kiegészítése és az ezekkel összefüggő valamennyi részcselekmény*”.[1]

Vagyis egy adott szakterületen, a vizsgálandó tárgy vagy helyzet, szakértelmet kívánó vizsgálatát végzi az igazságügyi szakértő (vagy más néven törvényszéki vagy kriminalisztikai szakértő).[143]

A modern járművek igazságügyi szakértői vizsgálata az intelligens közlekedési ökoszisztémában alkalmazott eszközök és a bekövetkező események vizsgálatával foglalkozó,

igazságügyi szakértői terület. Az ilyen vizsgálatok magukba foglalják például a járművön belüli komponensek, mint például az elektronikus vezérlőegységek, központi egység vagy a gyártó IT háttér rendszerében keletkező adatok vizsgálatát, de ide tartozhat a járműben utazók mobil telefonjainak, valamint a jármű és vele kapcsolatba álló egyéb kommunikációs és közlekedési infrastruktúra, közlekedési rendszer, felhő alapú rendszerek adatainak gyűjtése és elemzése is.

A szakemberek kompetenciájának támogatására National Institute of Standards and Technology (NIST) által kidolgozott NICE (National Initiative for Cybersecurity Education) keretrendszer és az European Cybersecurity Skills Framework (ECSF) nyújt szakterületspecifikus alapokat, vagyis a digitális forenzikus vizsgálatokat, mint fő témakört illetően. A NICE keretrendszer ismerteti az egyes munkaszerepekhez kapcsolódóan szükséges feladatokat, valamint ismerteti a feladatok elvégzéséhez szükséges tudás és készség elemeket. Az ECSF egy szilárd, könnyen használható, bővíthető, elérhető, interoperábilis, szektorokon átívelő és az EU szervezeti struktúrájához illeszkedő keretrendszer, ami az európai kiberbiztonsági kultúra megerősítését célozza.

A keretrendszerek fő építőköveit alapul véve meghatározható a modern járművekhez kapcsolódó szakértői vizsgálatok feladatainak elvégzéséhez szükséges készségek. A modern járművek vizsgálatát végző szakértői szerep vagy az elvégzendő munka minden esetben felbontható feladatokra.

A feladat olyan tevékenység, amely szervezeti vagy jelen témakör szerint a szakértői vizsgálatokhoz kapcsolódóan célok elérését szolgálja. A feladat meghatározásnak olyannak kell lennie, hogy könnyű legyen megérteni, egyértelműen határozza meg, hogy milyen tevékenységet kell végrehajtani. A feladat meghatározás nem, vagy nem minden esetben tartalmazza a feladat célját, ez ugyanis vizsgálatonként eltérő lehet. A feladat meghatározása azt írja le, hogy milyen munkát kell elvégezni. Ez a szakértői vizsgálatok kontextusában azt jelenti, hogy definiáljuk, hogy mi lesz a vizsgálatot végző szakember konkrét, megoldandó feladata.

Mivel az önvezető járművek és a modern közlekedési rendszerek szakértői vizsgálata még egy ideig nem képezi majd a napi szakértői gyakorlat részét, ezért egyes feladatmeghatározások valójában hipotézisek arról, hogy milyen feladatokat fog valószínűleg ellátni az ezekkel megbízott szakértő.

Egy adott feladat elvégzéséhez meghatározhatóak a szükséges tudás-, és készségelemek. Ezek meghatározása elősegíti a szakértői feladatok ellátásához szükséges ismeretek egységesítsét,

kategorizálását, meghatározását és kommunikálását. A készség definiálható, mint megfigyelhető kompetencia egy tanult motoros tevékenység végrehajtásához. A kiberbiztonsághoz szükséges készségek kevésbé támaszkodnak az eszközök fizikai manipulálására, inkább olyan eszközök, keretrendszerek, folyamatok és eljárások alkalmazására, amelyek hatással vannak egy szervezet vagy egyén kiberbiztonsági helyzetére.[335] A készségmeghatározások az egyes feladatokhoz kapcsolódnak, amiben munkát végző készségeket mutat be a feladatok végrehajtásában.

A készség egy megfigyelhető cselekvés végrehajtásának képessége. A készségmeghatározások leírhatnak az egyszerű vagy összetett készségeket. Egy adott feladat elvégzéséhez több készségmeghatározás is szükséges lehet. Hasonlóképpen, egy készség gyakorlása több feladat elvégzésére is használható. A készségmeghatározások lehetnek egyszerűek (például az autó multimédia rendszeréhez kapcsolódó Bluetooth eszközök lekérdezése) vagy összetettek (például hipotézis felállítása arról, hogy egy kiberbűnöző hogyan tud ellenőrizetlen eszközzel kapcsolatot létesíteni az autó multimédia rendszeréhez Bluetooth kapcsolaton keresztül) is. A készség tehát azt írja le, hogy a szakember mire képes, a feladat meghatározás pedig az elvégzendő munkát definiálja.[193][291][314][315]

Egyes készségek az egyes feladathoz, folyamatlépéshez tartoznak, több készség azonban a teljes vizsgálat során szükséges. Például az etikus és független munkavégzés, melyet nem befolyásolnak és nem torzítanak a belső vagy külső szereplők. A szakértő feladatkörében nem utasítható, munkáját a függetlenség és etikusság elvei mentén kell végezze.[104]

Az egyes szakértői feladatok elvégzéséhez szükségesek az ún. digitális kompetenciák, valamint speciális, a feleadat jellegéből adódóan elvárt készségek is. A kompetencia a tudás, készségek, képességek, magatartásformák és személyes jellemzők alkalmazásának vagy felhasználásának képessége, kritikus munkafeladatok, meghatározott funkciók sikeres végrehajtása, illetve adott szerepkörben vagy pozícióban való működése érdekében. A szakértői feladatok elvégzéséhez szükséges digitális kompetenciák:

- információ gyűjtése, felhasználása, tárolása,
- a digitális, internet alapú kommunikáció,
- a digitális tartalmak létrehozatala,
- problémamegoldás, gyakorlati alkalmazás,
- IKT biztonság.

Ezek a kompetenciák, illetve ezek alkalmazásának szükséglete minden vizsgálati fázisban szükségesek, az alkalmazott eszközök, módszerek, technikák miatt. A speciális munkaállomások (forensics workstation), használatának készsége, vagy azon eszközkészletek használatának készsége, melyek a speciális vizsgálatok elvégzéséhez szükségesek, elengedhetetlenek a vizsgálati célok teljesítéséhez. Minden fázisban szükséges az elvégzett műveletek és eredményeinek teljeskörű dokumentálása is.

Mivel a vizsgálatok magukba foglalják például a járművön belüli komponensek, mint például az ECU (Engine Control Unit), a központi egység (fejegység), a különböző fedélzeti egységek (OBU – onboard unit) adatainak, vagy akár a gyártó, szolgáltató informatikai háttér rendszerében keletkező adatok vizsgálatát, ezért átfogó jármű, informatikai és hálózati ismeretekre is szükség van. A vizsgálatok elvégzése során lehetőség nyílik továbbá a járműhöz csatlakoztatott fedélzeti eszközök (például kamerák) adatainak, a járműben utazók mobil telefonjainak, valamint a jármű és vele kapcsolatba álló egyéb kommunikációs és közlekedési infrastruktúra adatainak gyűjtésére és elemzésére is, ezért ezen eszközök használatához és működéséhez kapcsolódó ismeretek is szükségesek.

A szakértői vizsgálat, a szakértői munka (meghatározott feladatok sorrendi végrehajtása), valamilyen felkérés, felhatalmazás (kirendelés) alapján kezdődik meg. Annak érdekében, hogy a szakértői vizsgálat eredményes, hatékony és a szervezeti, valamint jogszabályi követelményeknek megfelelően kerüljön elvégzésre, a vizsgálatot megelőző fázisban több vezetői és szakértői feladat végrehajtására is szükség van, melyhez vezetői készségek és stratégiai gondolkodásmód is szükségessé válik.

A szakértői vizsgálat előkészítését megelőzően, a vizsgálat tervezése során szükségessé válhat a vizsgálatre felkérő személlyel, megrendelővel, kirendelővel közvetlen kommunikáció is. Az általa megadott kérdések pontosítása, egyeztetése a megfelelő kommunikációs csatorna kialakításával kezdődik majd a vizsgálati célok szükség szerinti pontosítása történik meg, valamint az vizsgálandó eseményhez kapcsolódó feladatok megtervezéséhez, meghatározásához elengedhetetlen plusz információk is beszerezhetőek.

A szakértői vizsgálat tényleges megkezdése előtti fázisban a szükséges vizsgálati lépések és feladatok megtervezése, az erőforrás allokáció, a vizsgáló eszközök (pl.: hardver, szoftver elemek) meghatározása történik, amely szervezési készségeket igényel.

A vizsgálat tárgya azonosításához, vagyis a jármű azon egységeinek, amiben digitális nyomok találhatóak, jártasság szükséges a modern járművek összetevőinek azonosításában,

módosításában és kezelésében. Mivel a járművek sérülékenyek lehetnek, a szakértőnek képesnek kell lennie azonosítani olyan működéseket, melyek eltérnek a normális működéstől. Ezt okozhatja valamilyen kártékony kód, melynek rosszindulatú viselkedését azonosítani kell. Figyelembe véve a magas automatizáltságú járművek katonai alkalmazását, valamint az ezen a területen széles körben alkalmazásra kerülő anti-forensics technikákat, a szakértőnek rendelkeznie kell azon készségekkel, hogy az ilyen technikák nyomait észlelni, azonosítani tudja.

Az adattároló egységekhez történő fizikai és logikai hozzáférés a modern járművek esetén összetettebb feladat. Ezek az eszközök védett, rejtett módon kerülnek beépítésre a járművekbe, ezért az előkészítési fázisban szükség van a jármű egyes részeinek fizikai szétszerelésére (pl.: műszerfal). Ehhez a járműrészek és a fejegységek, vezérlő egységek ki és szétszerelésének készsége is szükséges a szakértői feladatok elvégzéséhez.[10]

Az adatgyűjtés során a vizsgált esemény körülményeinek, és az érintett személyek tevékenységének, hollétének és személyi körülményének tisztázását értjük, vagyis minden olyan tevékenységet, amely formális eljárásjogi keretek között a meglévő ismeretek bővítésére törekszik. Ennek kapcsán történik meg a(z):

- kapcsolódó adatok felkutatása,
- releváns adatokat tartalmazó adatforrások azonosítása,
- nyomok/bizonyítékok felkutatása, beszerzése-adatok kinyerése,
- vizsgálat megalapozásához, megtervezéséhez szükséges adatok összegyűjtése is.[239]

Ezen feladatok elvégzéséhez szükséges az információk gyűjtésében, feldolgozásában, kezelésében, szállításában és tárolásában való jártasság, azok integritásának megőrzése mellett. E jártasság az adatok védelme szempontjából kritikus, mert ezzel elkerülhető a vizsgálat tárgyát képező adatok szándékolatlan, váratlan megváltozása, elvesztése, fizikai károsodása vagy megsemmisülése. Az adatok gyűjtéséhez használt eszközök, (virtuális) környezetek használatának, a különböző adathordozók adatainak kinyerési készsége.

8. táblázat Vizsgáló eszközökhöz kapcsolódó tudáselemek csoportosítása

Vizsgáló eszközökhöz kapcsolódó tudás	
Hardver eszközök	**Szoftver eszközök**
Szakértői eszközök ismerete.	Szakértői szoftverek ismerete.
Járműdiagnosztikai eszközök ismerete.	Adatfaragásra szolgáló eszközök és technikák ismerete.
Hibaazonosítási technikák ismerete.	Hibakeresési megoldások és eszközök ismerete.

A kinyert adatok verifikációja során biztosítani kell, hogy azok nem változtak a kinyerés során, valamint a vizsgálati célokhoz szükséges információk azonosítása. Ehhez szükséges a különböző operációs rendszerek (pl.: windows, linux, automotive operációs rendszerek stb.), szakértői alkalmazások ismerete, használata. Szükséges továbbá a logikai vonatkozású anti-forensics technikák alkalmazásának azonosítási képessége, vagy a HASH függvények ismerete. Ebben a fázisban történik például a fájl szignatúra összehasonlítás, vagyis az adott fájl fejlécének és kiterjesztésének összehasonlítása és jelölése (extension mismatch), vagy az ismert fájltípusokkal való összehasonlítás (pl.: De-NIST).

Az adatok elemzése során jellemzően valamilyen interaktív eszközzel fel kell ismerni és elemezni a megszerzett adatokba ágyazott adatstruktúrákat és metaadatokat. A fázis a vizsgált esemény idővonalának megalkotásához és a vizsgálati kérdések megválaszolásához szükséges releváns adatok azonosítását a bizonyítékok meghatározását és megkeresését foglalja magába. A szükséges készségek közé tartozik az események az elemző eszközök használata, az események, a járműkommunikáció, az illékony adatok, jármű operációs rendszerek elemzésére.

Többféle elemző, értelmező eszköz segítheti a szakértő munkáját, ezek használatának készsége nélkülözhetetlen a megfelelő vizsgálati eredmények előállításához. Ezen eszközök segítenek a vizsgált eseményhez kapcsolódó adatok megértésében. A mesterséges intelligencia fejlődésével a különböző elemzési technikáknak köszönhetően az egyes elemek közötti „láthatatlan” kapcsolatok is feltárásra kerülhetnek.

Részletes, átgondolt és megindokolt vizsgálati jelentések kidolgozásának és közlésének képessége szükséges ahhoz, hogy a szakértő az elvárásoknak és például a szakértői törvényben

meghatározott tartalmi elemeknek megfeleljen. A dokumentációnak például tartalmaznia kell a vizsgálat módszerének rövid ismertetését, a szakmai ténymegállapításokat, a szakértő véleményét, a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait stb. A digitális bizonyítékok bemutatásának és magyarázatának képessége lehetővé teszi, hogy a szakértő egyértelmű és könnyen érthető módon ismertesse az elért eredményeket. [68][108][243][225][271][269]

Kutatómunka összegzése

A technológiai fejlődés a közlekedési rendszerekre és a járműveinkre is nagy hatással volt az elmúlt időszakban. Ez a jövőben sem változik, az egyre komplexebb összekapcsoltság és a fejlett automatizálás új lehetőségeket teremt a közlekedés hatékonyságának és biztonságának növeléséhez. Ennek egyik módja a járművezető támogatása a forgalmi szituációkban, a megfelelő döntések előkészítésében, meghozatalában. Ez magas automatizáltsággal valósítható meg, melynek egyik alapeleme a jármű által gyűjtött, tárolt és feldolgozott adatok. Az ebből származó információk alkalmasak utólagos szakértői vizsgálatban való elemzésre, ehhez azonban eddig nem volt kidolgozott módszertan, a meglévő módszertanok korlátozott módon voltak alkalmazhatóak. A járművek, jármű rendszerek komplexitásából adódóan új kompetencia és tudáselemek váltak szükségessé, melyek korábban nem kerültek meghatározásra és rendszerezésre. Kutatómunkámban ezt a hiányosságot sikerült pótolnom, elkészítettem az önvezető járművek szakértői vizsgálata során alkalmazható módszertant, ami alapját képezheti egy szakértői módszertani levélnek, továbbá alapot képezhet a jövő modern járművek szakértői vizsgálatainak.

Szakirodalmi és szakértői gyakorlati tapasztalatok alapján összegyűjtöttem és rendszereztem a modern és egyre inkább önvezetővé váló járművek szakértői vizsgálatának elvégzéséhez szükséges kompetenciákat, a szakértői feladatokhoz tartozó tudáselemeket. A meghatározott kompetenciák és tudáselemek elsajátítása alkalmassá teszik a szakértőket műveleti területen történő feladatvégzésre is.

Mivel a biztonságos katonai műveletek – ellenséges környezetben végzett katonai műveletek, terrorelhárítás, hírszerzés stb. – egyik fontos összetevője a digitális eszközök szakértői vizsgálatának elvégzése, a kidolgozott módszertant úgy készítettem el, hogy alkalmazható legyen műveleti területen is. Legyen szó az ellenség digitális rendszereinek vizsgálatáról,

műveleti területeken történő adatkinyerésről, a potenciális incidensek utólagos vizsgálatáról, a fenyegetések azonosításáról, a sérülékenységek mérsékléséről vagy a biztonsági szint, a működési folyamatok, a katonai műveletek fejlesztése érdekében végzett tevékenységekről, számos kihívás jelenik meg. Kutatómunkám által meghatároztam azon kihívásokat, melyek polgári és katonai feladatvégzés során felmerülhetnek.

Kutatásom célja volt hozzájárulni a hazai és nemzetközi vonatkozású, modern és egyre inkább önvezetővé váló, polgári és katonai felhasználású, közúti közlekedési járművek szakértői vizsgálatának hatékony és eredményes elvégzéséhez, amit eredményesen teljesítettem.

Munkám eredményeként elkészült egy a modern és egyre inkább önvezetővé váló járművek vizsgálatához kapcsolódó kihívásokat is figyelembe vevő, hatékonyan alkalmazható vizsgálati módszertan, ami alapja lehet egy hazai szakértői módszertani levél kidolgozásának.

Kutatásom eredményeként, a releváns digital forensics domainek vizsgálata alapján meghatároztam az Autonomous Vehicles Forensics szakmai definícióját és módszertani leírását.

Új tudományos eredmények

A kutatásom során az alábbi új tudományos eredményeket értem el:

1. ***Megvizsgáltam***, hogy magas automatizáltságú, egyre inkább önvezetővé váló járművek szakértői vizsgálatához jelenleg milyen módszertanok, ajánlások állnak rendelkezésre. Szakértői gyakorlati és szakirodalmi kutatómunkával ***bebizonyítottam***, hogy jelenleg nem áll rendelkezésre olyan módszertan, eljárás, amely alapján a modern járművek szakértői vizsgálata szakszerűen elvégezhető.

2. ***Kidolgoztam*** a modern és egyre inkább önvezetővé váló járművek szakértői vizsgálatának kihívásait, az általános kihívásokon túlmenően a vizsgálati eljáráshoz kapcsolódó és a vizsgáló eszközökhöz kapcsolódó kihívásokra kiterjedően, ideértve a katonai műveletek során történő alkalmazás kihívásait.

3. A digitális forenzikus domain-ek vonatkozásában ***megállapítottam***, hogy a modern és egyre inkább önvezető járművek szakértői vizsgálata nem tartozik egyik digital forensics szakterülethez, nem sorolható be ezekbe, ezért szükséges egy új domain létrehozása. Definiáltam az Autonomous Vehicles Forensics fogalmát, mint a Digital Forensics domain új elemét, összehasonlítva a különböző vizsgálati módszerek (számítógépes, felhő, IoT, stb.) folyamatlépéseivel és azok alkalmazhatóságával. ***Elkészítettem***, a gyakorlatban ***teszteltem*** a modern járművekhez kapcsolódó kihívásokat is figyelembe vevő módszertani leírást, igazoltam, hogy a módszer egységes keretet biztosít a vizsgálatok elvégzéséhez.

4. ***Rávilágítottam***, hogy modern járművekkel kapcsolatos események, új vizsgálati célok kikényszerítették, hogy az informatikával vagy járművek szakértői feladatait ellátó szakértők eseti jelleggel, végeznek járművekben található adatokkal kapcsolatos vizsgálatokat, azonban ezek nem módszeres, a járművekben található adattárolókat és adatokat nem teljeskörűen figyelembe vevő vizsgálatok, ahol korlátozott a rendelkezésre álló kompetencia. Emiatt nem garantált, hogy elegendő mennyiségű és/vagy minőségű bizonyíték kerül összegyűjtésre, nem készül megfelelő dokumentáció, a nyomkezelés nem megfelelősége miatt a vizsgálat nem megismételhető, hibák keletkeznek az elemzés vagy az értelmezés során. ***Meghatároztam***, rendszereztem mely kompetenciák és tudáselemek szükségesek azon szakértők számára, akik ilyen járművek vizsgálatával foglalkoznak, vagy terveznek foglalkozni, annak érdekében, hogy a szükséges ismeretek célirányosan elsajátíthatóak legyenek.

Kutatómunkám alapján sikeresen teljesítettem az értekezés kutatási célkitűzéseit, a hipotézisek igazolásra kerültek.

Publikációs jegyzék

[1] Berek, Lajos ; Répás, József ; Schmidt, Miklós, A célzott adatkinyerés szerepe a katonai és civil felhasználású közúti közlekedési járművek szakértői vizsgálatában, In: Gőcze, István; Padányi, József (szerk.) Szemelvények a katonai műszaki tudományok eredményeiből V. : Hallgatói és oktatói kötet Budapest, Magyarország : Ludovika Egyetemi Kiadó (2025) 279 p. pp. 81-96. , 16 p.

[2] Berek, Tamás ; Répás, József, A magas automatizáltságú katonai és polgári közlekedési járművekben megtalálható digitális adatok hozzáférhetőségének és értelmezhetőségének kihívásai In: Gőcze, István; Padányi, József (szerk.) Szemelvények a katonai műszaki tudományok eredményeiből V. : Hallgatói és oktatói kötet Budapest, Magyarország : Ludovika Egyetemi Kiadó (2025) 279 p. pp. 67-79. , 13 p.

[3] Répás, József, Szakértői kompetenciák a magas automatizáltságú közlekedési járművek vizsgálatában (2025)

[4] Répás, József, The Main Steps of the Digital Forensics Examination Methodology of Modern Transport Vehicles LECTURE NOTES IN NETWORKS AND SYSTEMS 1258 pp. 329-333. Paper: Chapter 30 , 5 p. (2025) Folyóirat szakterülete: Scopus - Computer Networks and Communications **SJR indikátor: Q4**

[5] Berek, Tamás ; Répás, József, Az autonóm harctéri és közlekedési járművek forenzikus vizsgálatának lehetőségei és kihívásai In: Gőcze, István; Padányi, József Szemelvények a katonai műszaki tudományok eredményeiből IV. : Hallgatói kötet Budapest, Magyarország : Ludovika Egyetemi Kiadó (2024) 220 p. pp. 7-20. , 14 p.

[6] Répás, József, A magas automatizáltságú közlekedési járművek utólagos szakértői vizsgálatához szükséges készségek In: Gőcze, István; Padányi, József Szemelvények a katonai műszaki tudományok eredményeiből IV. : Hallgatói kötet Budapest, Magyarország : Ludovika Egyetemi Kiadó (2024) 220 p. pp. 127-142. , 16 p.

[7] Répás, József, Cloud Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert; Pinke, Péter (szerk.) Mérnöki Szimpózium a Bánkin Előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2023) Budapest, Magyarország : Óbudai Egyetem (2024) 367 p. pp. 349-354. , 6 p.

[8] Répás, József, Modern közúti közlekedési járművek szakértői vizsgálatához szükséges tudáselemek meghatározása In: Molnár, György; Temesvári, Zsolt; Wührl, Tibor (szerk.) XXXIX. Kandó Konferencia 2023 Budapest, Magyarország : Óbudai Egyetem (2024) 420 p. pp. 213-224. , 11 p.

[9] Répás, József, Examining the Application of Drone Forensics Methodology on Highly Automated Civil and Military Vehicles HADMÉRNÖK 19 : 2 pp. 17-28. , 12 p. (2024)

[10] Répás, József, Magas automatizáltságú harctéri és közlekedési járművek digitális adatainak kinyerési módszerei In: Bátori, Annamária; Mezei, József (szerk.) A Haza

Szolgálatában Konferencia - 2024 – Absztraktkötet, Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2024) 54 p. p. 40

[11] Répás, József, Live Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában In: Felföldi, Péter; Radvánszki, Ronett (szerk.) A rendészettudomány határtudományai 2024 absztraktkötet, Doktoranduszok Országos Szövetsége, Rendészettudományi Osztály (2024) 38 p. p. 34

[12] Schmidt, Miklós ; Répás, József ; Berek, Lajos Informatikai rendszerek fejlődésének hatása az utólagos szakértői vizsgálatokra In: Bátori, Annamária; Mezei, József (szerk.) A Haza Szolgálatában Konferencia - 2024 – Absztrakt kötet, Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2024) 54 p. p. 41

[13] Berek, Lajos ; Berek, Tamás ; Répás, József A komplex vagyonvédelem értelmezése a modern közlekedési és az autonóm harctéri járművek vonatkozásában In: Gőcze, István; Padányi, József (szerk.) Húsz év a katonai műszaki tudományok szolgálatában. A katonai műszaki tudományok tudományág időszerű kérdései, aktuális tudományos kutatási eredményei : Oktatói kötet, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 376 p. pp. 11-28. , 18 p.

[14] A 7W szerepe a magas automatizáltságú járművek szakértői vizsgálatában In: Horváth Richárd (Horváth Richárd Műszaki Tudományok) ÓE/BGK/Kari Kutatásszervező Központ ; Lukács Judit (Lukács Judit Gépészeti tudományok) ÓE/BGK/Mechatronikai és Járműtechnikai Intézet ; Stadler Róbert Gábor (Stadler Róbert Gábor Műszaki tudományok) ÓE/BGK/Gépészeti és Technológiai Intézet (szerk.) Mérnöki Szimpózium a Bánkin előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2022), Konferencia helye, ideje: Budapest, Magyarország 2022.11.22. - 2022.11.22. (Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar), Budapest: Óbudai Egyetem, pp 237-242 (2022)

[15] Pogány, Viktor ; Répás, József, Possibilities of anti-forensics techniques in cooperative intelligent transport systems In: Thomázy, Gabriella (szerk.) III. South America, South Europe International Conference 2023 : Book of Abstracts „Defense and Security in South America and Southern Europe: New Challenges, Struggles, and Tradition”, Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2023) 101 p. pp. 55-55. , 1 p.

[16] Répás, József The Digital Footprint of Vehicles - The Role of Forensics Examinations in Modern Transport Systems / A járművek digitális lábnyoma - Szakértői vizsgálatok szerepe a modern közlekedési rendszerekben In: Thomázy, Gabriella (szerk.) III. South America, South Europe International Conference 2023 : Book of Abstracts „Defense and Security in South America and Southern Europe: New Challenges, Struggles, and Tradition Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2023) 101 p. pp. 56-56. , 1 p.

[17] Répás, József, Definition of Forensic Methodologies for Autonomous Vehicles HADMÉRNÖK 18 : 1 pp. 125-141. , 17 p. (2023)

[18] Répás, József, Anti-forensics technikák szerepe a magas automatizáltságú járművek szakértői vizsgálatában BELÜGYI SZEMLE / ACADEMIC JOURNAL OF INTERNAL AFFAIRS: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-) 71 : 9 pp. 1607-1620. , 14 p. (2023)

[19] Répás, József, What does our car tell about us? – part II. - Access issues of data collected and managed by modern vehicles (2023)

[20] Répás, József ; Pogány, Viktor ; Berek, Lajos, Modern járművek szakértői vizsgálata az European Cybersecurity Skills Framework, Digital Forensics Investigator szerepkörének tükrében (2023)

[21] Répás, József, Digitális adatok földön, vízen, levegőben - A közlekedési járművek és személyes adataink kezelése: Konferencia előadás (2023) "Az ember a legújabb technológiák között" című konferencia, 2023. május 31., Budapest, Magyarország, Megjelenés: Magyarország,

[22] Répás, József ; Pogány, Viktor, Az European Cybersecurity Skills Framework, Digital Forensics Investigator szerepköre, a modern katonai és polgári járművek utólagos szakértői vizsgálatában In: Kovács, István (szerk.) A kor szellemében: tudományos válaszok a világban jelentkező különböző veszélyforrásokra Budapest, Magyarország : Magyar Rendészettudományi Társaság (2023) 171 p. pp. 75-87. , 9 23.

[23] Répás, József, A Modern közúti közlekedési járművek és rendszerek személyes adatkezelése: Előadás (2023) Hétpecsét Információbiztonsági Egyesület - Információvédelem menedzselése CVII. Szakmai Fórum, 2023. szeptember 20., Budapest, Magyarország, Megjelenés: Magyarország

[24] Répás, József ; Pogány, Viktor, IoT Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában HADITECHNIKA 57 : 4 pp. 43-49. , 7 p. (2023)

[25] Répás, József, Downloading modern vehicles SD card data for Forensics examination - A case study: Konferencia előadás (2023) 2nd IEEE International Conference on Cognitive Mobility, 19.10.2023, Budapest, Hungary, Megjelenés: Magyarország

[26] Répás, József ; Schmidt, Miklós, Forensics tevékenységek kihívásai a modern közlekedési járművek fejlődésének tükrében In: Gőcze, István; Padányi, József Húsz év a katonai műszaki tudományok szolgálatában : A katonai műszaki tudományok tudományág időszerű kérdései, aktuális tudományos kutatási eredményei - Hallgatói kötet, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 295 p. pp. 181-194. , 14 p.

[27] Répás, József ; Némedy, László, Modern járművek kiberbiztonsága, biztonsági követelményei a szakértői vizsgálatok céljával és lehetőségeivel összefüggésben In: Borza, Veronika; Főző, Eszter; Kóré, Veronika; Markó, Alexandra; Mell, Péter; Nyiri, Miklós; Tóth, István László (szerk.) Régi és új kihívások az igazságügyi szakértői munkában, Budapest, Magyarország : Nemzetbiztonsági Szakszolgálat (NBSZ) (2023) 226 p. pp. 86-129. , 44 p.

[28] Répás, József, Examination of the application of Drone Forensics methodology of the highly automated civil and military vehicles In: Répás, József (szerk.) I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia : Konferenciakötet, Budapest, Magyarország : Óbudai Egyetem (2023) pp. 20-20. , 1 p.

[29] Répás, József ; Ripszám, Dóra Pilóta nélküli légijárműből kinyerhető digitális nyomok felhasználási lehetőségei, korlátai In: Répás, József (szerk.) I. Alverad-Bánki Nemzetközi

Kiberbiztonsági Konferencia : Konferenciakötet, Budapest, Magyarország : Óbudai Egyetem (2023) pp. 21-21. , 1 p.

[30] Répás, József ; Ripszám, Dóra Drónokban megtalálható digitális bizonyítékok kinyerése és felhasználása In: Berke, J. (szerk.) Dróntechnológia adatfeldolgozási és adatbiztonsági kihívásai konferencia Budapest, Magyarország : Gábor Dénes Egyetem (2023) 35 p. p. 1

[31] Pogány, Viktor ; Répás, József ; Schmidt, Miklós Modern járművek, mint adatforrások az utólagos szakértői vizsgálatokban In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert Gábor (szerk.) Mérnöki Szimpózium a Bánkin előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2022), Budapest, Magyarország : Óbudai Egyetem (2022) 312 p. pp. 219-224. , 6 p.

[32] Répás, József; Berek, Lajos, Security and Safety Systems on Modern Vehicles LECTURE NOTES IN MECHANICAL ENGINEERING Vehicle and Automotive Engineering 4 pp. 84-100. Paper: Chapter 8 , 17 p. (2022) Folyóirat szakterülete: Scopus - Automotive Engineering **SJR indikátor: Q4**

[33] Répás, József ; Schmidt, Miklós ; Berek, Lajos, Downloading modern vehicles data for Forensics examination – A case study In: IEEE - IEEE (szerk.) 2022 IEEE 1st International Conference on Cognitive Mobility (CogMob), Piscataway (NJ), Amerikai Egyesült Államok : Institute of Electrical and Electronics Engineers (IEEE) (2022) pp. 29-30. , 2 p.

[34] Répás, József ; Miklos, Schmidt ; Berek, Lajos, Autonomous Vehicles Forensics - The next step of the Digital Vehicles Forensics In: IEEE - IEEE (szerk.) 2022 IEEE 1st International Conference on Cognitive Mobility (CogMob), Piscataway (NJ), Amerikai Egyesült Államok : Institute of Electrical and Electronics Engineers (IEEE) (2022) pp. 67-72. , 6 p.

Felhasznált irodalom

[1] 2016. évi XXIX. törvény az igazságügyi szakértőkről -. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1600029.tv (A letöltés dátuma: 2023. július 5.)

[2] 5/1990. (IV. 12.) KöHÉM rendelet a közúti járművek műszaki megvizsgálásáról, Forrás: https://net.jogtar.hu/jogszabaly?docid=99000005.koh

[3] A Bizottság közleménye az Európai Parlamentnek, a tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának. Európa mozgásban. Fenntartható mobilitás Európában: biztonságos, összekapcsolt és tiszta közlekedés. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018DC0293&from=HU

[4] A JTAG módszer alkalmazása, https://tinyurl.hu/WW8B (Utolsó megtekintés: 2023. 07. 27.)

[5] A járművek automatizáltsági szintjei (SAE) https://cv.inf.elte.hu/wp-content/uploads/2022/02/1_sae-j3016-visual-chart-5321-hu-1024x576.png

[6] A KOOPERATÍV JÁRMŰKOMMUNIKÁCIÓ ALAPJAI Dr. Bokor László forrás: https://docplayer.hu/25795975-A-kooperativ-jarmukommunikacio.html

[7] A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," in IEEE Wireless Communications, vol. 26, no. 4, pp. 60-65, August 2019, doi: 10.1109/MWC.2019.1800503.

[8] Aafs (2022): Forensic science. Online: https://www.aafs.org/careers-forensic-science/what-forensic-science

[9] Abeis Ab, Iot forensics, https://www.slideshare.net/AbeisAb/iot-forensics-11792666 (Letöltve: 2022.12.12.)

[10] ABForensics, Infotainment & Telematics System Data Acquisition and Analysis, Forrás: https://abforensics.com/infotainment-telematics-system-data-acquisition-and-analysis/

[11] ADAS, https://www.synopsys.com/content/dam/synopsys/designware-ip/diagrams/adas-fig1-color.jpg.imgw.850.x.jpg

[12] Adattenger, https://iot.boschblog.hu/wp-content/uploads/2018/08/Adattenger_iot_boschblog.jpg

[13] Albini A. és Rajnai Z. (2018). General Architecture of Cloud. Procedia Manuf., 22, 485–490.

[14] Al-dhaqm, Arafat – Razak, Shukor – Othman, Siti – Ali, Abdulalem – Ghaleb, Fuad A. – Salleh Rosman, Arieff – Marni, Nurazmallail (2020): Database Forensic Investigation Process Models: A Review. IEEE Access, 8, 48477–48490. Online: https://doi.org/10.1109/ACCESS.2020.2976885

[15] Al-dhaqm, Arafat – Razak, Shukor – Othman, Siti H. – Ngadi, Asri – Ahmed, Mohammed N. – Ali Mohammed, Abdulalem (2017): Development and Validation of a Database Forensic Metamodel (DBFM). Plos, 12(2). Online: https://doi.org/10.1371/journal.pone.0170793

[16] Ambrus István, Az önvezető járművek várható hatása a közlekedési

bűncselekményekre, http://ugyeszeklapja.hu/?p=2271

[17] Analysis of Digital Forensics Capabilities on State-of-the-art Vehicles by Kevin Klaus Gomez Buquerin - Technical University Ingolstadt Faculty of Computer Science - Master Thesis – 2019

[18] André Å. (2017). Digital Forensics, Oslo: Wiley, ISBN: 978 1 119 26241 1

[19] Anu Jain - Gurpal Singh Chhabra: Anti-Forensics Techniques: An Analytical Review. researchgate.net, 2014. https://doi.org/10.1109/IC3.2014.6897209

[20] ASPICE 101: What You Need to Know About Automotive SPICE. In: Intland Software. https://tinyurl.hu/jZ3n (Utolsó megtekintés: 2023. 07. 27.)

[21] ASPICE: Meghatározás, megfelelőség, eszközök és tanúsítványok. https://visuresolutions.com/hu/blog/ automotive/aspice/ (Utolsó megtekintés: 2023. 07. 25.)

[22] Atlam, H. F., Hemdan, E. E., Alenezi, A., Alassafic, M. O., Wills, G. B. Internet of Things Forensics: A Review 2020 February, DOI:10.1016/j.iot.2020.100220

[23] Attila, A. et al. (2018). IT Infrastruktúra Informatikai Biztonsági Aspektusai. Bánki Közlemények, 1(1), 11-16.

[24] Autok IT háttere, https://iot.boschblog.hu/mobilitas/rendet-teszunk-az-autos-it-dzsungelben/

[25] Automotive forensics, Forrás: https://www.digitalforensics.com/digital-forensics/automotive-forensics

[26] Automotive night vision, https://en.wikipedia.org/wiki/Automotive_night_vision

[27] Automotive Spice in the context of cybersecurity (ASPICE® CS) – The new maturity model at a glance. https://tinyurl.hu/Zx7a (Utolsó megtekintés: 2023. 07. 25.)

[28] Automotivetechis, ISO 26262https://automotivetechis.wordpress.com/iso-26262/

[29] Autonóm járművek, szenzorok, https://iot.boschblog.hu/mobilitas/csak-egy-maradhat/

[30] Autonomous Vehicle Security: A Deep Dive into Threat Modeling, Amal Yousseef, Shalaka Satam, Banafsheh Saber Latibari, Jesus Pacheco, Soheil Salehi, Salim Hariri, Partik Satam, Forrás: https://arxiv.org/html/2412.15348v1

[31] Autonomous vehicles sensor, https://www.autonomousvehicleinternational.com/wp-content/uploads/2022/12/Autonomous-Vehicle-Sensor-Suite-01-2-e1671030076556-768x367.png

[32] Autopro, Forrás: https://autopro.hu/gyartok/jovore-indulhat-az-onvezeto-taxik-tesztelese-europaban/1516226

[33] AZ EU kiberbiztonsági stratégiája a digitális évtizedre. JOIN(2020) 18 final https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020JC0018&qid=1533485886151&from=ENl etöltve: 2022.02.22.

[34] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/2144 RENDELETE,

Forrás: https://eur-lex.europa.eu/eli/reg/2019/2144/oj, Letöltve: 2022.06.13.

[35] Az Európai Parlament és a Tanács (EU) 2023/2661 irányelve (2023. november 22.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről szóló 2010/40/EU irányelv módosításáról, Forrás: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32023L2661

[36] Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről EGT-vonatkozású szöveg, Forrás: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A32010L0040

[37] Bates, Eoin A. (2019): Digital Vehicle Forensics. Online: https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf

[38] Bayrak, A., Gorsich, D., and Epureanu, B., "Future of Autonomous High-Mobility Military Systems," SAE Intl. J CAV 3(3):205-215, 2020, https://doi.org/10.4271/12-03-03-0016.

[39] Bellaby, Ross W. (2021): Can AI Weapons Make Ethical Decisions? Criminal Justice Ethics, 40(2), 86–107. Online: https://doi.org/10.1080/0731129X.2021.1951459

[40] Berek Tamás, Répás József 2025. A magas automatizáltságú katonai és polgári közlekedési járművekben megtalálható digitális adatok hozzáférhetőségének és értelmezhetőségének kihívásai. In Gőcze István – Padányi József (szerk.): Szemelvények a katonai műszaki tudományok eredményeiből V. Hallgatói és oktatói kötet. Ludovika Egyetemi Kiadó, Budapest. 67–79.

[41] Berek Tamás, Répás József, Az autonóm harctéri és közlekedési járművek forenzikus vizsgálatának lehetőségei és kihívásai, Szemelvények a katonai műszaki tudományok eredményeiből IV. : Hallgatói kötet, Budapest: Ludovika Egyetemi Kiadó, pp 7-20 (2024)

[42] Bergholtz, Stine (2019): The Six W's of Investigation. Online: https://www.brainspores.com/the-six-ws-of-investigation/

[43] Berla co. (2015): 12 Days of Vehicle Forensics. Forrás: https://berla.co/12-days-of-vehicle-forensics/ (A letöltés dátuma: 2023. március 10.)

[44] BEYERS, Quintus H. (2013): Database Forensics. Investigating Compromised Database Management Systems. MSc dissertation. University of Pretoria. https://repository.up.ac.za/bitstream/handle/2263/41016/Beyers_Database_2013.pdf?sequence=1

[45] BlackBerry's New Intelligent Vehicle Data Platform. DVN. https://www.design-engineering.com/blackberry-amazon-to-develop-vehicle-data-platform-1004035961/

[46] BME Közlekedésmérnöki alapképzési szak Tanterv (2023), https://kozlekedes.bme.hu/wp-content/uploads/2023/07/Tanterv_uj_BSc_K_20230707-1.pdf Letöltve: 2023.11.12.

[47] Bódi Antal, Közlekedésbiztonság fokozását megalapozó Komplex ITS Ökoszisztéma kialakításának kérdései disszertáció 2022. Óbudati Egyetem

[48] Boóc Ádám, Robotautókkal, közösségi taxikkal és kereskedelmi drónokkal kapcsolatos felelősségi kérdések, http://www.kre.hu/ajk/images/doc/Uj_technologia_jog_kotet.pdf

[49] Borbíró A., Gönczöl K., Kerezsi K., Lévay M. (szerk.) 2020. Kriminológia, ISBN 978 963 295 931 3

[50] Bosch blog, 6G fejlesztés, https://iot.boschblog.hu/mobilitas/a-bosch-is-segit-a-6g-fejleszteseben/

[51] Bosch blog, A járművezetés jövője, második fejezet, https://iot.boschblog.hu/mobilitas/a-jarmuvezerles-jovoje-masodik-fejezet/

[52] Bosch blog, Arra figyelnek ami tényleg fontos, https://iot.boschblog.hu/mobilitas/arra-figyelnek-ami-tenyleg-fontos/

[53] Bosch blog, Autonom-jarmuvek-kiberbiztonsagi-kihivasai-1,https://www.ludovika.hu/blogok/cyberblog/2021/04/19/autonom-jarmuvek-kiberbiztonsagi-kihivasai-1-resz/

[54] Bosch blog, Autonom-jarmuvek-kiberbiztonsagi-kihivasai-2https://www.ludovika.hu/blogok/cyberblog/2022/01/20/autonom-jarmuvek-kiberbiztonsagi-kihivasai-2-resz/

[55] Bosch blog, Lidar nélkül nem megy, https://iot.boschblog.hu/mobilitas/lidar-nelkul-nem-megy/

[56] Bosch blog, Mindent feltérképezünk, https://iot.boschblog.hu/mobilitas/mindent-felterkepezunk/

[57] Bosch blog, Önvezetésre felkészülve, https://iot.boschblog.hu/mobilitas/onvezetesre-felkeszulve/

[58] Bosch blog, Új utakon jár a mesterséges intelligencia,https://iot.boschblog.hu/mobilitas/uj-utakon-jar-a-mesterseges-intelligencia/

[59] Bosch Blog, Vizuális akadályok mögé látó járművek, https://iot.boschblog.hu/mobilitas/vizualis-akadalyok-moge-lato-jarmuvek/

[60] Braccini, Christian et al. (2016): Battlefield Digital Forensics. Tallin: NATO Cooperative Cyber Defence Centre of Excellence. Online: https://ccdcoe.org/uploads/2018/10/BDF_Battlefield_Digital_Forensics_final.pdf

[61] BSI - ISO/SAE 21434:2021 Requirements Training Course, 2022

[62] Can bus explained, https://www.autopi.io/blog/can-bus-explained/

[63] CAN Bus, https://www.webfleet.com/hu_hu/webfleet/fleet-management/glossary/can-bus/

[64] CAN knowledge, https://www.can-cia.org/can-knowledge

[65] Carly Hallman: A Chronology of Car Safety, forrás: https://www.titlemax.com/resources/a-chronology-of-car-safety/

[66] Chandel, Ashutosh 2020. Understanding an ASIL in the Functional Safety Standard ISO 26262. https://www.lhpes.com/blog/what-is-an-asil (Utolsó megtekintés: 2023. 07. 25.)

[67] Chandel, Raj (2020): Digital Forensics: An Introduction. Hacking Articles,

2020. szeptember 14. Online: https://www.hackingarticles.in/digital-forensics-an-introduction/

[68] Chester Maciag, Joseph Giordano, Cyber Forensics: A Military Operations Perspective Forrás: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf"

[69] Chetan Somavanshi : Difference Between LIN, CAN, MOST, FlexRay, Communication Protocols, forrás: https://www.cselectricalandelectronics.com/difference-between-lin-can-most-flexray

[70] Chhabra, G. S. (2014). Anti-Forensics Techniques: An Analytical Review, https://doi.org/10.1109/IC3.2014.6897209

[71] Cloud Forensics Tools 2022. Forrás: https://medium.com/@cloud_tips/cloud-forensics-tools-4beed278ea5e, Letöltve: 2023.11.20.

[72] Countering Anti-Forensic Efforts, https://www.forensicfocus.com/articles/countering-anti-forensic-efforts-part-1/

[73] Crach Data Retrieval, Forrás: https://cdr.boschdiagnostics.com/cdr/sites/cdr/files/15-93_cdr_crash_data_retrieval.pdf, Letöltve: 2024.03.22.

[74] Cybersecurity threats facing the automative industry, https://cybersecurity.att.com/blogs/security-essentials/the-top-8-cybersecurity-threats-facing-the-automotive-industry-heading-into-2023 Letöltve: 2023.11.11

[75] Csák Zsolt, A drónok kapcsán felmerülő egyes büntető anyagi és eljárási jogi kérdések. In: Mezei, K. (szerk.) A bűnügyi tudományok és az informatika. Budapest-Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar-MTA Társadalomtudományi kutatóközpont. pp. 26-45.

[76] Csiszár Csaba, Földes Dávid, Csonka Bálint, Közlekedési információs rendszerek, 2018., ISBN 978-963-454-305-3

[77] Csiszár Csaba, Sándor Zsolt Péter: Közlekedés informatika. researchgate.net, 2014. Forrás: https://www.researchgate.net/publication/277015956_Kozlekedesi_informatika

[78] David Tidmarsh, 2022. Introduction to What is Cloud Forensics? Forrás: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-cloud-forensics, Letöltve: 2023.11.20.

[79] Delgrossi, L. and Zhang, T. (2012). Vehicle Safety Communications. Veh. Saf. Commun.

[80] Dey, K. C. et al. (2016). Vehicle-to-vehicle (V2V) and vehicle-toinfrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation. Transp. Res. Part C Emerg. Technol., 68, 168–184.

[81] Digital Forensics Investigator szerepkör az ENISA ECSF-ben. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf

[82] Digital Forensics https://csrc.nist.gov/glossary/term/digital_forensics, Letöltve: 2023.11.13.

[83] Digital Forensics and chip-off, In: Salvationdata honlapja, https://blogsalvationdatacom.files.wordpress.com/2018/04/14.jpg (Utolsó megtekintés: 2023. 07. 27.)

[84] Digital identity and security, https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/ota

[85] Digitpol, Automotive forensics, https://digitpol.com/automotive-forensics/

[86] Dimitar, K. (2020). Network forensics overview, https://resources.infosecinstitute.com/topics/digital-forensics/network-forensics-overview/

[87] Dobák Imre, A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, 2014. ISBN 978-615-5305-49-8

[88] Dolgok internete http://industry4.hu/hu/fogalomtar/dolgok-internete-iot (Letöltve: 2022.12.12.)

[89] Driving the Future: V2X Systems and the role antennas play. Poynting. Beyond a connected life. http://bit.ly/4nNpDCX.

[90] DSRC vs. C-V2X for Safety Applications. Autotalks. https://auto-talks.com/technology/dsrc-vs-c-v2x/

[91] DSRC vs. C-V2X: Understanding the Two Technologies. Ettifos. https://www.ettifos.com/post/dsrc-vs-cv2x

[92] DSRC vs. V2X, https://www.ettifos.com/post/dsrc-vs-cv2x

[93] DSRC, Forrás: https://www.itsstandards.eu/its-application-areas/cen-dsrc/

[94] E/E architecture,https://www.bosch-mobility-solutions.com/en/mobility-topics/ee-architecture/

[95] EC-Council, Digital forensics, https://www.eccouncil.org/what-is-digital-forensics/

[96] ECU szerepe az autószerelésben, https://dubnicz.hu/2024/08/az-ecu-szerepe-az-autoszerelesben-hogyan-javitsuk-es-diagnosztizaljuk-az-elektronikus-vezerloegyseget/

[97] Edin Selimovic, 2017. Forensic Investigation Of Automotive Computers by , A Capstone Project Submitted to the Faculty of Utica College

[98] Elindult a Tesla önvezetés magyarországon, Forrás:https://villanyautosok.hu/2026/01/16/magyarorszagon-is-elindult-a-tesla-onvezetese/

[99] Enisa (2023): Assessing Cyber Skills on the basis of the ECSF, Forrás: https://www.youtube.com/watch?v=wP32kU7PEXU, (A letöltés dátuma: 2023. július 1.)

[100] Enisa Good practices for security of smart cars, Forrás: https://www.enisa.europa.eu/sites/default/files/publications/Good%20practices%20for%20security%20of%20Smart%20Cars.pdf, Letöltve: 2025.05.04.

[101] Enisa, European Cybersecurity Skills Framework, Forrás: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework, (A letöltés dátuma: 2023. május 10.)

[102] Eoin A. Bates, 2019. Digital Vehicle Forensics Forrás:

https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf, Letöltve: 2021.10.22.

[103] Ericsson. (2018). Connected Vehicle Cloud - Under The Hood. https://archive.ericsson.net/service/internet/picov/get?DocNo=2870 1-FGD101192. Letöltve: 2018.04.08.

[104] ERMProtect Staff, What Are the 5 Stages of a Digital Forensics Investigation, Forrás: https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/

[105] Érzékelők az autonóm járművekben Gáspár Péter – Szirányi Tamás, forrás: https://eetb.mfa.kfki.hu/sites/eetb.mfa.kfki.hu/files/2017/Gaspar.pdf

[106] Európa mozgásban: a Bizottság befejezi a biztonságos, tiszta és összekapcsolt mobilitás programját. 2018. Forrás: https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_3708

[107] Európai Parlament és a Tanács (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

[108] European justice, Bizonyításfelvétel, https://e-justice.europa.eu/topics/court-procedures/civil-cases/taking-evidence/es_hu

[109] Event Data Recorder (EDR), Forrás: https://squarell.com/solutions/event-data-recorder-edr, Letöltve: 2022.10.15.

[110] Expert Review Blog: ISO FOR MEDIA ORIENTED SYSTEMS TRANSPORT ROAD VEHICLES, forrás: https://expertreview.world.edu/iso-for-media-oriented-systems-transport-road-vehicles/

[111] FBI (2000): Computer Forensics. Online: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

[112] FBI retired (2022): FBI Computer Forensics. Online: https://fbiretired.com/skillset/fbi-computer-forensics/

[113] Fehér András Tibor – Négyesi Imre (2021): A gépi érzelmek a fegyveres erőknél és az autonóm rendszerekben. Hadtudományi Szemle, 14(3), 163–176. Online: https://doi.org/10.3

[114] Fenntartható és intelligens mobilitási stratégia – az európai közlekedés időtálló pályára állítása, Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0789

[115] Fenyvesi Cs. A kriminalisztika elmélete és gyakorlata, Nyitott Egyetem, Forrás: https://www.youtube.com/watch?v=yBC4Ght7nNk, Letöltve: 2022.09.13.

[116] Fenyvesi Csaba, Herke Csongor, Tremmel Flórián (szerk.): Kriminalisztika, NKE Ludovika Egyetemi kiadó, 2022. ISBN 978-963-531-557-4

[117] Finszter G. (2020). A kriminalisztika ígérete, Magyar Tudomány 2020/5, Forrás: https://mersz.hu/hivatkozas/matud_f41567/#matud_f41567, Letöltve: 2022.10.15.

[118] Flaglien, A. O. The Digital Forensics Process https://www.researchgate.net/publication/318198370_The_Digital_Forensics_Process,

DOI: 10.1002/9781119262442.ch2 (Letöltve: 2022.12.12.)

[119] FlexRay: Járműinformatika 5. óra, forrás: http://www.sze.hu/~korosp/Jarmuinformatika_nappali/05%20-%20Jarmuinformatika%20FlexRay.pdf

[120] Forensicfocus, https://www.forensicfocus.com/articles/25-days-25-questions-part-1-process-and-practice/

[121] Forensics Colleges (2022): Modern Forensic Science Technologies. Online: https://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

[122] Forensics technologies https://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies (Letöltve: 2022.12.24.)

[123] Fowler, Kevvie (2008): SQL Server Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley Professional.

[124] Funkcionális biztonság az autóiparban ISO 26262. In: A CMSW Safexpert Kft. honlapja. https://tinyurl.hu/9vAN (Utolsó megtekintés: 2023. 07. 27.)

[125] Furnell, S. (2016): The evolving landscape of technology-dependent crime In McGuire, M. R. & Holt, T. J. (Eds.), The Routledge Handbook of Technology, Crime and Justice (p. 13–25). Routledge Handbooks. https://doi.org/10.4324/9781315743981-4

[126] Gabler, H. C., Hinch, J, and Steiner, J., 2008. Event Data Recorders: A Decade of Innovation, SAE International, Warrendale, ISBN: 978-0768020663

[127] Garima Mathur: The Storage Challenges of Automotive Edge and Smart Driving https://blog.westerndigital.com/smart-driving-automotive-data-edge-storage/

[128] Gáspár Péter, Németh Balázs, Bokor József: JÁRMŰIRÁNYÍTÁS, 2019, ISBN: 978 963 454 328 2

[129] Gáspár Péter, Szirányi Tamás: Érzékelők az autonóm járművekben, forrás: https://eetb.mfa.kfki.hu/sites/eetb.mfa.kfki.hu/files/2017/Gaspar.pdf

[130] Gheorghiu, R. A. et al. (2018) Messaging capabilities of V2I networks. Procedia Manuf., 22, 476–484.

[131] Gogolin, G. (2021). Digital Forensics Explained. CRC Press. https://doi.org/10.1201/9781003049357

[132] Gomez Buquerin, Kevin – Corbett, Chris – Hof, Hans-Joachim 2021. A generalized approach to automotive forensics. Forensic Science International: Digital Investigation 36. 301111

[133] Good, World of data, https://www.good.is/infographics/the-world-of-data-we-re-creating-on-the-internet

[134] Gönczöl K., Kerezsi K., Korinek L., Lévay M. (szerk.) 2016. Kriminológia-Szakkriminológia, ISBN 978 963 295 627 5

[135] Guru 99, Digital forensics, https://www.guru99.com/digital-forensics.html

[136] Gyaraki Réka, A kiberbűncselekmények megjelenése és helyzete napjainkban - Különös tekintettel a szervezett bűnözéssel kapcsolatos kérdésekre, Forrás: https://jog.tk.hu/uploads/files/05_buntetojog_informatika_GYARAKIR.pdf (A letöltés

dátuma: 2023. június 15.)

[137] Gyarmati József – Simó Réka (2022): Autonóm terepjáró járművek katonai felhasználásának lehetőségei. II. rész. Haditechnika, 55(1), 8–14. Online: https://doi.org/10.23713/HT.55.1.02

[138] Herke Cs. (2021). A kriminalisztika alapkérdései és az önvezető járművek. Belügyi Szemle , 69(1), 87-105. https://doi.org/10.38146/BSZ.2021.1.4

[139] HNTB. (2018). Connected and Automated Vehicles. Forrás: http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/79

[140] How CAN-FD Light enables new car network architectures Michael Luett 2021.10.20. IVN Architecture, Network and Landscape, Silica IVN Event

[141] Hua, Tan Kian 2019. Differences in advance data extraction methods from the mobile phone. https://tinyurl.hu/c0cn (Utolsó megtekintés: 2023. 07. 27.)

[142] IEEE Standard for Ethernet Amendment 8: Physical Layer Specifications and Management Parameters for 25 Gb/s - Electrical Automotive Ethernet, in IEEE Std 802.3cy-2023, vol., no., pp.1-137, 11 Aug. 2023, doi: 10.1109/IEEESTD.2023.10213388

[143] Igazságügyi szakértők, Forrás: https://e-justice.europa.eu/550/HU/forensic_experts

[144] Illési, Zs. (2009). Számítógép hálózatok kriminál technikai vizsgálata, Hadmérnök, IV évf. 4. szám.

[145] Infotainment system, https://www.evanshalshaw.com/blog/what-is-a-car-infotainment-system

[146] Infotainment, Ford, https://www.evanshalshaw.com/-/media/evanshalshaw/blog/what-is-ford-sync/ford-focus-estate-infotainment-screen-1280x720px.ashx?h=720&w=1280&hash=7268B048F2663D9F7F76134FA830DA5F

[147] Intelligent transport systems, Forrás: https://cinea.ec.europa.eu/programmes/connecting-europe-facility/transport-infrastructure/intelligent-transport-systems-eu_en?prefLang=hu

[148] Interpol (2021): Guidelines to Digital Forensics. First Responders. Online: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwih9_7tqsr8AhVK_7sIHYtRC64QFnoECA0QAQ&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F16243%2Ffile%2FGuidelines%2520to%2520Digital%2520Forensics%2520First%2520Responders_V7.pdf&usg=AOvVaw30MzwH6f3XZN9NGPNGT8Ag

[149] Interpol, Digital forensics, https://www.interpol.int/How-we-work/Innovation/Digital-forensics

[150] Interworks, Digital forensics, https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/

[151] Intland, https://www.scribd.com/document/337278901/Automotive-Functional-Safety-Compliance-Intland-Software

[152] IoT biztonság https://www.ldsz.hu/iot-a-dolgok-internete-es-a-biztonsagtechnika-1-resz-68 (Letöltve: 2022.12.12.)

[153] IoT forensics https://en.wikipedia.org/wiki/IoT_Forensics (Letöltve:

2022.11.24.)

[154] IoT szakértői vizsgálat szintjei Forrás: https://www.researchgate.net/figure/Investigation-process-of-IoT-forensics_fig4_337259162, (Letöltve: 2023.1.10.)

[155] ISC2 (2022): Cybersecurity Workforce Study, Forrás: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx (A letöltés dátuma: 2023. július 1.)

[156] ISO 11898-1:2024 Road vehicles — Controller area network (CAN) Part 1: Data link layer and physical coding sublayerhttps://www.iso.org/standard/86384.html

[157] ISO 11898-2:2026 Road vehicles — Controller area network (CAN) Part 2: High-speed physical medium attachment (PMA) sublayerhttps://www.iso.org/standard/90697.html

[158] ISO 11898-3:2006 Road vehicles — Controller area network (CAN) Part 3: Low-speed, fault-tolerant, medium-dependent interfacehttps://www.iso.org/standard/36055.html

[159] ISO 11898-4:2004 Road vehicles — Controller area network (CAN) Part 4: Time-triggered communicationhttps://www.iso.org/standard/36306.html

[160] ISO 16845-1:2016 Road vehicles — Controller area network (CAN) conformance test plan Part 1: Data link layer and physical signallinghttps://www.iso.org/standard/59166.html

[161] ISO 16845-2:2018 Road vehicles — Controller area network (CAN) conformance test plan Part 2: High-speed medium access unit — Conformance test planhttps://www.iso.org/standard/69841.html

[162] ISO 21434, https://www.tamcert.hu/autoipari-kiberbiztonsag-iso-21434/

[163] ISO 26262 functional safety, https://akademia-hu.tuv.com/termek/iso-26262-functional-safety-szabvany-14316

[164] ISO 26262 szabványhttps://visuresolutions.com/hu/autoipari/iso-26262/

[165] ITS benefits, https://cinea.ec.europa.eu/sites/default/files/styles/oe_theme_medium_2x_no_crop/public/2025-05/ITS_Benefits_Square_AdobeStock_224231490.jpeg

[166] ITS & autonomous vehicles data systems, Forrás: https://cinea.ec.europa.eu/sites/default/files/styles/oe_theme_medium_2x_no_crop/public/2025-05/ITS_4CCAM_-AdobeStock_550747203-modified_1x1.jpg?itok=aFEbXmSK

[167] Izabella, Kakuja: Data extraction during CBRN crime scene investigation, Safety and Security Sciences Review, Vol 6, No 1, 2024, 79-85 pp.

[168] J. Liu, S. Zhang, W. Sun and Y. Shi, "In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions," in IEEE Network, vol. 31, no. 5, pp. 50-58, 2017, doi: 10.1109/MNET.2017.1600257

[169] J. Motavalli, “The dozens of computers that make modern cars go (and stop),” The New York Times, Feb 2010, accessed on June 23, 2020. [Online]. Available: https://www.nytimes.com/2010/02/05/technology/05electronics.html

[170] Jackson, Kenneth A., 2020. Infotainment and Telematic Systems Challenges

Effecting Vehicle Forensic Law Enforcement Capabilities, Forrás: https://www.proquest.com/openview/3aaacb26f62e6b75f319bf4cae9bf85a/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y Letöltve: 2022.04.21.

[171] James R. Lyle; Barbara Guttman; John M. Butler; Kelly Sauerwein; Christina Reed; Corrine E. Lloyd, Digital Investigation Techniques: A NIST Scientific Foundation Review, Forrás: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf, Letöltve: 2022.10.10.

[172] Járműinformatika előadásvázlat (2020). http://www.sze.hu/~korosp/Jarmuinformatika_nappali/05%20-%20Jarmuinformatika%20FlexRay.pdf

[173] Járművek biztonsági gyakorlata, https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf Letöltve: 2023.11.20.

[174] Járművek fenyegetései, https://www.qad.com/blog/wp-content/uploads/2020/01/01.16.2020.jpg Letöltve: 2023.11.11.

[175] Járművek kiberbiztonsága, https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity Letöltve: 2023.11.20.

[176] Jayadev Paleri 2023. Cloud Forensics: Understanding the Investigation Process, Forrás: https://www.linkedin.com/pulse/cloud-forensics-understanding-investigation-process-jayadev-paleri, Letöltve: 2023.11.25.

[177] Jiajia Liu és mtsai., „In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions”, IEEE Network 31, sz. 5 (2017): 50–58.

[178] Jinadasa, Anuka. IOT Forensic Challenges, 2021. https://www.slideshare.net/AnukaJinadasa/iot-forensics-249699308 (Letöltve: 2022.12.12.)

[179] John Frank Weaver: Robots are people too, ABC-CLIO LLC, Santa Barbara, California, 2012. 17.

[180] John Villasenor: Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation; April 2004. 8-14.

[181] Johnson, James (2023): Finding AI Faces in the Moon and Armies in the Clouds: Anthropomorphising Artificial Intelligence in Military Human–Machine Interactions. Global Society, 2023. április 27. Online: https://doi.org/10.1080/13600826.2023.2205444

[182] Jonsson, McKenzie 2022. ASPICE 101: What is Automotive SPICE? In: Jama Software. https://tinyurl.hu/EDMM (Utolsó megtekintés: 2023. 07. 27.)

[183] Joseph D. Miller, 2020., Automotive System Safety, Critical Considerations for Engineering and Effective Management, Wiley, ISBN: 9781119579625

[184] Joshi R.C., Emmanuel, S. Pilli. (2016), Fundamentals of Network Forensics, Springer 2016. ISBN 978-1-4471-7297-0

[185] Joshi, R. C., Pilli, E. S. Cloud Forensics, Fundamentals of Network Forensics, ISBN: 978-1-4471-7299-4

[186] Jövő autói, https://iot.boschblog.hu/mobilitas/osszefog-a-bosch-es-az-nvidia-a-jovo-autoiert/

[187] Kai Hüschelrath - Heike Schweitzer (2014): Public and Private Enforcement of Competition Law in Europe. Berlin: Springer-Verlag

[188] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, Experimental Security Analysis of a Modern Automobile, https://www.autosec.org/pubs/cars-oakland2010.pdf

[189] Karthika, D. 2021. IoT Sensors: Security in Network Forensics https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769057.ch8 https://doi.org/10.1002/9781119769057.ch8 (Letöltve: 2022.12.12.)

[190] Katona Gergő, Autonóm járművek kiberbiztonsági kihívásai (3. rész),https://www.ludovika.hu/blogok/cyberblog/2022/06/29/autonom-jarmuvek-kiberbiztonsagi-kihivasai-3-resz/

[191] Katona Gergő, Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése (1. rész) HADMÉRNÖK 18 : 3 pp. 161-176. , 16 p. (2023)

[192] Kawałkowska, Małgorzata é. n. ASPICE 101: Everything you need to know about Automotive SPICE. In: Spyrosoft. https://tinyurl.hu/M4gl (Utolsó megtekintés: 2023. 07. 27.)

[193] Kiss Albert, Kompetenciaelemek, Forrás: https://docplayer.hu/33179006-Kompetenciaelemek-a-kompetencia-elemei-tudas-ismeret-kepessegek-es-attitudok-amelyeket-a-kepesitesi-szint-leirasokban-az-autonomia-es.html

[194] Kocsmárik Gábor: Az elektromos és önvezető járművek büntetőjogi megítélése, https://kuria-birosag.hu/hu/kuriai-dontesek/kocsmarik-gabor-az-elektromos-es-onvezeto-jarmuvek-buntetojogi-megitelese

[195] Lachow, Irving (2017): The Upside and Downside of Swarming Drones. Bulletin of the Atomic Scientists, 73(2), 96–101. Online: http://dx.doi.org/10.1080/00963402.2017.1290879

[196] Lin bus connection, https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/introduction-to-the-local-interconnect-network-lin-bus.html

[197] Liu, Changwei. Anoop Singhal and Duminda Wijesekera, A logic-based network forensics model for evidence analysis https://csrc.nist.gov/CSRC/media/Projects/Measuring-Security-Risk-in-Enterprise-Networks/documents/logic_based_network_forensices_model-for_evidence_analysis.pdf (Letöltve: 2022.12.12.)

[198] Long, A. (2015)., What is FORENSICS? Why do we need Network Forensics?, https://slideplayer.com/slide/6938457/

[199] Lorge, Elizabeth (2010): Shining Light on Battlefield Forensics. ARNEWS, 2010. május 27. Online: www.army.mil/article/39956/

[200] Lukovics Miklós, Az önvezető járművek és a városi társadalom, ISBN 978 963 664 154 2

[201] Main Branches of digital forensics, https://www.researchgate.net/figure/Main-Branches-of-Digital-Forensics_fig1_335694535

[202] Malwarebytes, Digital forensics, https://blog.malwarebytes.com/security-world/2017/08/explained-digital-forensics/

[203] 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.

[204] Martí, E. – Miguel, M. Á. D. – Fernández, F. G. – Pérez, J. (2019): A review of sensor technologies for perception in automated driving. IEEE Intelligent Transportation Systems Magazine, 11(4), 94–108. https://doi.org/10.1109/mits.2019.2907630

[205] Máté István Zsolt – Darabos Zoltán – Morber Szilárd Krisztián – Sándor Gábor 2020. 6/2020. módszertani levél az elektronikus adatok vizsgálatának általános alapelveiről. Magyar Igazságügyi Szakértői Kamara. http://bit.ly/4nd39dC.

[206] Máté István Zsolt, Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe, Forrás: http://real.mtak.hu/116025/1/MateIstvanZsoltBelugyiSzemle2018.evi7-8.szam36-54.pdf (A letöltés dátuma: 2023. június 15.)

[207] Matthew J Parkinson, The Evolution of Vehicle Forensics,https://sytech-consultants.com/the-evolution-of-vehicle-forensics/

[208] Mezei Kitti (2023): A kiberbűnözés szabályozási kihívásai a büntetőjogban, Forrás: http://ugyeszeklapja.hu/?p=2592 (A letöltés dátuma: 2023. június 15.)

[209] Mi az a felhőalapú számítás?Forrás: https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-cloud-computing, Letöltve: 2023.11.25.

[210] Michael Luett, How CAN-FD Light enables new car network architectures, Silica conference, 2021.10.20.

[211] Microchip: The Automotive Information Backbone, forrás: https://www.microchip.com/en-us/solutions/automotive-and-transportation/automotive-products/connectivity/most-technology

[212] Mike Jones, Single Pair Ethernet (SPE) for In-Vehicle Networking, Silica IVN Event, 2021.10.19-20.

[213] Mit kell tudni a felhőtechnológiáról? Forrás: https://kalauz.lib.pte.hu/felho-technologia/#_ftn1, Letöltve: 2023.11.10.

[214] Mobile Forensics, Forrás: https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf, Letöltve: 2022.09.22.

[215] Mobile Forensics, https://study.com/academy/lesson/mobile-forensics-definition-uses-principles.html

[216] Mobile Forensics, https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf

[217] N. Asselin-Miller et al., “Study on the Deployment of C-ITS in Europe : Final Report,” Dg Move, 2016, [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/2016-c-its-deployment-study-final-report.pdf.

[218] National Initiative for Cybersecurity careers and studies:The demand for cybersecurity experts is growing 12 times faster then the current U.S. job market, making cybersecurity one of the most highly sought-after careers in the country. https://niccs.cisa.gov Letöltve: 2023.04.20.

[219] NATO (2021): Summary of the NATO Artificial Intelligence Strategy. 2021. október 22. Online: www.nato.int/cps/en/natohq/official_texts_187617.htm

[220] Neemeh, Steve 2020. What is ASPICE in Automotive? In: LHP. https://tinyurl.hu/ngE8 (Utolsó megtekintés: 2023. 07. 27.)

[221] Négyesi Imre – Fazekas Ferenc (2022): A mesterséges intelligencia integrálásának lehetőségei a vezetési pontok feladatrendszerébe. Hadtudományi Szemle, 15(3), 145–159. Online: https://doi.org/10.32563/hsz.2022.3.9

[222] Network forensics https://resources.infosecinstitute.com/topic/network-forensics-overview/ (Letöltve: 2022.12.10.)

[223] New spotlight function for Active Night View Assist Plus: Enhanced safety for pedestrians, https://web.archive.org/web/20141229212458/http://media.daimler.com/dcmedia/0-921-658892-1-1354042-1-0-0-0-0-0-12639-0-0-1-0-0-0-0-0.html

[224] NI: FlexRay Automotive Communication Bus Overview, forrás: https://www.ni.com/hu-hu/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html

[225] NICE framework https://niccs.cisa.gov/workforce-development/nice framework Letöltve: 2023.04.20.

[226] NICCS: Digital Forensics, forrás: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/digital-forensics Letöltve: 2023.04.20.

[227] NIST (2015): Digital Forensics. Online: https://csrc.nist.gov/glossary/term/digital_forensics

[228] NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework - William Newhouse Stephanie Keith Benjamin Scribner Greg Witte - November 2020 Letöltve: 2023.04.20.

[229] NTSHA - Ensuring American Leadership in Automated Vehicle Technologies Automated Vehicles 4.0 https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf

[230] Nurazmallail Marni, Database Forensic Investigation Process Models: A review https://www.researchgate.net/publication/339542884_Database_Forensic_Investigation_Process_Models_A_Review

[231] Onsemi, IVN Architecture, Network and Landscape, Silica IVN Event 2021.10.19-20

[232] OTA update, https://www.techtarget.com/searchmobilecomputing/definition/OTA-update-over-the-air-update

[233] Oussama, S. – Singh, I. – Pourreza, H. R. (2023): Autonomous vehicles: open-source technologies, considerations, and development. Advances in Artificial Intelligence and Machine Learning, 03(01), 669–692. https://doi.org/10.54364/aaiml.2023.

[234] Outay, F. et al. (2017).ConVeh: Driving Safely into a Connected Future. Procedia Comput. Sci., 113, 460–465,

[235] Önvezető autók Budapesten, Forrás: https://e-cars.hu/2026/03/31/megjelentek-az-onvezeto-autok-budapest-utcain/

[236] Padányi József (2022): Kihívások, kockázatok, válaszok. Az éghajlatváltozás okozta kihívások és azok hatása a katonai erőre. Budapest: Ludovika.

[237] Pashakhanlou, Arash Heydarian (2019): AI, Autonomy, and Airpower: The End of Pilots? Defence Studies, 19(4), 337–352. Online: https://doi.org/10.1080/14702436.2019.1676156

[238] Petersen, Rodney – Santos, Danielle – Smith, Matthew C. – Wetzel, Karen A. – Witte, Greg 2020. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181. Revision 1. https://doi.org/10.6028/NIST.SP.800-181r1

[239] Pilisi Fanni, Bűnügyi adatgyűjtés, különös tekintettel a raszternyomozásra, Forrás: https://ujbtk.hu/dr-pilisi-fanni-bunugyi-adatgyujtes-kulonos-tekintettel-a-raszternyomozasra/

[240] Plastics Today: PBT Delivers More Clarity for Radar Sensors Image: BASF, forrás: https://www.plasticstoday.com/automotive-and-mobility/pbt-delivers-more-clarity-radar-sensors

[241] Pogány Viktor, Répás József, Possibilities of anti-forensics techniques in cooperative intelligent transport systems, III. South America, South Europe International Conference, 2023.

[242] Pogány, Viktor; Répás, József; Schmidt, Miklós, Modern járművek, mint adatforrások az utólagos szakértői vizsgálatokban, In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert Gábor (szerk.) Mérnöki Szimpózium a Bánkin előadásai: Proceedings of the Engineering Symposium at Bánki (ESB 2022), Budapest, Magyarország: Óbudai Egyetem (2022)

[243] Police Executive Research Forum, Utilizing Vehicle Data in Law Enforcement Investigations, Forrás: https://www.iacpcybercenter.org/wp-content/uploads/2020/09/Vehicle-Data_LECC-Article.pdf

[244] Raj Chandel (2020), Digital Forensics: An Introduction. Online: https://www.hackingarticles.in/digital-forensics-an-introduction/

[245] Rangesh, A. – Trivedi, M. M. (2019): No blind spots: full-surround multi-object tracking for autonomous vehicles using cameras and lidars. IEEE Transactions on Intelligent Vehicles, 4(4), 588–599. https://doi.org/10.1109/tiv.2019.2938110

[246] Répás József 2025. The Main Steps of the Digital Forensics Examination Methodology of Modern Transport Vehicles. In Zöldy, Máté (ed.): Proceedings of the 3rd Cognitive Mobility Conference. COGMOB 2024. Lecture Notes in Networks and Systems 1258. Springer, Cham. https://doi.org/10.1007/978-3-031-81799-1_30.

[247] Répás József et al. (2022): What Does Our Car Tell about Us? The Questions and Possibilities of IT Forensic of Modern Vehicles. In János Szentágothai International Multidisciplinary Conference and Student Competition. Pécs, 2022. április 14.

[248] Répás József, 2023. Definition of Forensic Methodologies for Autonomous Vehicles, HADMÉRNÖK 18 : 1 pp. 125-141. , 17 p. (2023)

[249] Répás József, A járművek digitális lábnyoma - Szakértői vizsgálatok szerepe a modern közlekedési rendszerekben, III. South America, South Europe International Conference, 2023.

[250] Répás József, A modern katonai és polgári járművek utólagos szakértői vizsgálatának adatkinyerési eljárásai, MRTT 2024.

[251] Répás József, A modern közúti közlekedés járműveinek szakértői vizsgálata módszertanának kialakítása és annak alkalmazási lehetőségei, SZIMfonia IV. Szakértői kutatások a MILAB égisze alatt, ISBN 978-615-82042-9-3

[252] Répás József, Acquiring electronic data from modern vehicles using the chip-off method, VII. RENDÉSZET – TUDOMÁNY – AKTUALITÁSOK, A rendészettudomány a fiatal kutatók szemével, NKE konf. 2025.

[253] Répás József, Berek Lajos (2023). Security and Safety Systems on Modern Vehicles. In: Jármai, K., Cservenák, Á. (eds) Vehicle and Automotive Engineering 4. VAE 2022. Lecture Notes in Mechanical Engineering. Springer, Cham. https://doi.org/10.1007/978-3-031-15211-5_8

[254] Répás József, Cloud Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában, ESB 2023

[255] Répás József, Definition of Forensic Methodologies for Autonomous Vehicles, HADMÉRNÖK (1788-1919): 18 1 pp 125-141 (2023)

[256] Répás József, Digitális adatok földön, vízen, levegőben - A közlekedési járművek és személyes adataink kezelése, Az ember a legújabb technológiák között, NKE konf. 2023.

[257] Répás József, Examination of the application of Live Forensics methodology of the highly automated vehicles, A rendészettudomány határtudományai, NKE konf. 2024.

[258] Répás József, Magas automatizáltságú harctéri és közlekedési járművek digitális adatainak kinyerési módszerei. In Bátori Annamária – Mezei József (szerk.): A Haza Szolgálatában Konferencia 2024. Absztraktkötet. Doktoranduszok Országos Szövetsége, Budapest. 40.

[259] Répás József, Mit árul el rólunk az autónk? II. rész - A modern járművek által gyűjtött és kezelt adatok hozzáférési kérdései, XXI. Szentágothai konferencia, 2023.

[260] Répás József, Némedy László, Modern járművek kiberbiztonsága, biztonsági követelményei a szakértői vizsgálatok céljával és lehetőségeivel összefüggésben, In: Borza, Veronika; Főző, Eszter; Kóré, Veronika; Markó, Alexandra; Mell, Péter; Nyiri, Miklós; Tóth, István László (szerk.) Régi és új kihívások az igazságügyi szakértői munkában, Budapest, Magyarország: Nemzetbiztonsági Szakszolgálat (NBSZ) (2023) 226 p. pp. 86-129.

[261] Répás József, Network Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában, https://comconf.hu/eloadas/2023/R%C3%A9p%C3%A1s%20J%C3%B3zsef_Network%20Forensics%20m%C3%B3dszertan%20alkalmaz%C3%A1s%C3%A1nak%20vizsg%C3%A1lata%20magas%20automatiz%C3%A1lts%C3%A1g%C3%BA%20j%C3%A1rm%C5%B1vek%20szak%C3%A9rt%C5%91i%20vizsg%C3%A1lat%C3%A1ban.pdf

[262] Répás József, Pogány Viktor, IoT Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában, Haditechnika

[263] Répás József, Relevance of accident data in the digital forensics examination of modern vehicles, A Haza Szolgálatában Konferencia, NKE, 2025.

[264] Répás József, Ripszám Dóra, Drónokban megtalálható digitális bizonyítékok kinyerése és felhasználása, DAAK 2023

[265] Répás József, Schmidt Miklós, Berek Lajos, 2022. Autonomous Vehicles Forensics -The next step of the Digital Vehicles Forensics, 1ST IEEE INTERNATIONAL CONFERENCE ON COGNITIVE MOBILITY

[266] Répás József, Schmidt Miklós, Berek Lajos, Downloading modern vehicles data for Forensics examination – A case study, In: IEEE - IEEE (szerk.) 2022 IEEE 1st International Conference on Cognitive Mobility (CogMob), Piscataway (NJ), Amerikai Egyesült Államok : IEEE (2022) pp. 29-30.

[267] Répás József, Schmidt Miklós, Forensics tevékenységek kihívásai a modern közlekedési járművek fejlődésének tükrében, In: Gőcze, István; Padányi, József Húsz év a katonai műszaki tudományok szolgálatában: A katonai műszaki tudományok tudományág időszerű kérdései, aktuális tudományos kutatási eredményei - Hallgatói kötet, Budapest, Magyarország: Ludovika Egyetemi Kiadó (2023) 295 p. pp. 181-194.

[268] Répás József, Schmidt Miklós, Vitai Miklós, Berek Lajos: What does our car tell about us? The questions and possibilities of IT forensic of modern vehicles. In János Szentágothai International Multidisciplinary Conference and Student Competition. Pécs, 2022. 04. 14. (Pécs, Szentágothai János Szakkollégiumi Egyesület)

[269] Répás József, Szakértői kompetenciák a magas automatizáltságú közlekedési járművek vizsgálatában, Kandó konferencia, 2024.

[270] Répás József: A 7W szerepe a magas automatizáltságú járművek szakértői vizsgálatában, In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert Gábor (szerk.) Mérnöki Szimpózium a Bánkin előadásai: Proceedings of the Engineering Symposium at Bánki (ESB 2022), Budapest, Magyarország: Óbudai Egyetem (2022) 312 p. pp. 237-242., 6 p.

[271] Rick Tontarski, Defense Forensic Enterprise System, Forrás: https://www.nationalacademies.org/documents/embed/link/LF2255DA3DD1C41C0A42D3BEF0989ACAECE3053A6A9B/file/D3A4A5DAA96A5C788CC027B595C0E72D5845D6AC2E57?noSaveAs=1

[272] Roriz, R. – Cabral, J. – Gomes, T. (2021): Automotive LiDAR Technology: A Survey. IEEE Trans. Intell. Transp. Syst., Vol. 23., 6282–6297.

[273] Roriz, R. – Silva, H. – Dias, F. – Gomes, T. (2024). A Survey on Data Compression Techniques for Automotive LiDAR Point Clouds. Sensors, 24(10), 3185. https://doi.org/10.3390/s24103185

[274] Roz Calvert (2017): Types of forensic tests. Online: https://sciencing.com/types-forensic-tests-7551951.html

[275] Ruan, K., Carthy, J., Kechadi, T., Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, Digital Investigation, https://www.sciencedirect.com/science/article/abs/pii/S1742287613000121 (Letöltve: 2022.11.12.)

[276] Ruan, K., Carthy, J., Kechadi, T., Crosbie, M. Cloud forensics: An overview https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview (Letöltve: 2022.11.11.)

[277] Salvation Data (2021): What is Digital Vehicle Forensics. Online:

https://www.salvationdata.com/knowledge/what-is-digital-vehicle-forensics/

[278] Scherer Balázs, dr. Tóth Csaba, Laboratóriumi mérések a Beágyazott és ambiens rendszerek laboratórium tárgyhozhttps://www.mit.bme.hu/data/migrate/oktatas/targyak/8604/Autos_labor_v5h.pdf

[279] Schneider, Jacquelyn – Macdonald, Julia (2023): Looking Back to Look Forward: Autonomous Systems, Military Revolutions, and the Importance of Cost. Journal of Strategic Studies, 2023. január 24. 1–23. Online: https://doi.org/10.1080/01402390.2022.216457

[280] Selimovic, Edin 2017. Forensic Investigation Of Automotive Computers. A Capstone Project Submitted to the Faculty of Utica College.

[281] Shepard, Jeff 2021. What are ASILs and how do they work? In: MicrocontrollerTips. forrás: https://tinyurl.hu/0zlT (Utolsó megtekintés: 2023. 07. 27.)

[282] Shiklo, Boris. Automotive IoT: Smarter Vehicles, Optimized Car Manufacturing https://www.scnsoft.com/blog/iot-in-automotive-industry (Letöltve: 2022.12.12.)

[283] Shipra R., Aman S., Bhavya S., Internet of things Mobility Forensics, Digital Forensics and Internet of things, ISBN: 978 1 119 76878 4

[284] Siegel A. Jay (2017): Forensic science. Online: https://www.britannica.com/science/forensic-science#ref310214

[285] Smart flash auto, https://smartsemi.com/wp-content/uploads/2024/07/smart-flash-auto.jpg

[286] Soós Gábor, Rövid András, Ormos Pál, V2X – A járművek közötti kommunikáció kihívásai, https://eprints.sztaki.hu/10868/1/Soos_29_35647333_ny.pdf

[287] Sorbán K. (2016). A digitális bizonyíték a büntető eljárásban. Belügyi Szemle, 64(11), 81–96. https://doi.org/10.38146/BSZ.2016.11.5

[288] Soundarya, J. (2023). What Is Network Forensics? Basics, Importance, And Tools, https://www.g2.com/articles/network-forensics

[289] Stander, Adrie – Hanlé, Barnard (2017): Digital Forensics and Electronic Evidence. Udemy. Online: www.udemy.com/course/digital-forensics-and-electronic-evidence/

[290] Strohner József, 2013. Tanulási stratégiák kiépítése, http://www.jgypk.hu/mentorhalo/tananyag/Tanulsitantsi_stratgik_kiplse_a_vizulis_aktivits_kompetenciaterletenV2/412_a_tuds_fogalomkre.html Letöltve: 2023.04.20.

[291] SWGDE/SWGIT: Guidelines & Recommendations for Training in Digital & Multimedia Evidence https://www.crime-scene investigator.net/swgde_swgit_training_document_v2-0.pdf Letöltve: 2023.04.20.

[292] Szakmai módszertani leírások [é. n.]. Budapest: Nemzeti Szakértői és Kutató Központ. Online: https://nszkk.gov.hu/modszertani-leirasok

[293] Számítástechnikai ismeretek, https://www.profession.hu/cikk/szamitastechnikai-ismeretek-hol-a-helyuk-az-oneletrajzban Letöltve: 2023.11.27.

[294] Szoftver vezérelt autók, https://iot.boschblog.hu/mobilitas/szoftver-a-lelke-minden-autonak/

[295] Takács József, CAN RÉSZLEGES HÁLÓZATI ESZKÖZ FEJLESZTÉSE,szakdolgozat, 2014., https://dsp.mit.bme.hu/userfiles/szakdolgozat/takacsszakdolgozat14.pdf

[296] Tanulékony radarok, https://iot.boschblog.hu/mobilitas/tanulekony-radarok/

[297] Taohua, Z. – Yang, M. – Jiang, K. – Wong, H. – Yang, D. (2020): MMW Radar-Based Technologies in Autonomous Driving: A Review. Sensors, 20(24).

[298] Techopedia, Digital forensics, https://www.techopedia.com/definition/27805/digital-forensics

[299] Tesla önvezetés teszt, Forrás: https://villanyautosok.hu/2026/01/21/budapesten-probaltuk-ki-a-tesla-legujabb-onvezeto-szoftveret/

[300] The Prof and the Geek, Az adatok évezrede,https://www.youtube.com/watch?v=-0FvULEkpqw

[301] Thomas R. Markham (2016), Vehicle security module system szabadalom, Forrás: https://patents.google.com/patent/US10124750B2/en, Letöltve: 2024.05.23.

[302] TIBCO Software. The connected car: finding the intersection of opportunity and consumer demand. Palo Alto (CA): 2016.

[303] Tim Lau, Avnet Automotive Update, Marvell Automotive Business Unit 2021.10.19-20.

[304] Tokody Dániel, Albini Attila, Ady László, Temesvári Zsolt Marcell, Rajnai Zoltán, 2018. Kiberbiztonság az autóiparban. Bánki Közlemények 1/3. 71–77. https://tinyurl.hu/oYo3

[305] Tóth Bálint, Magasan automatizált és autonóm járművek tesztelésének módszertana a tesztpálya és az ahhoz kapcsolódó szimulációs technológiák szempontjából című Doktori Disszertáció, BME, 2025

[306] Toyota műszerfal, Forrás: https://scene7.toyota.eu/is/image/toyotaeurope/toyota_apple_carplay_android_auto_02_tcm-3033-2100359?wid=1920&fit=fit,1&ts=0&resMode=sharp2&op_usm=1.75,0.3,2,0, Letöltve: 2024.06.10.

[307] Török Péter, Titkos üzenet száll a széllel! (IoT-ben használt vezeték nélküli adatátviteli technológiák összehasonlítása), Hadmérnök, XIV. évfolyam 3. szám 2019.

[308] Tremmel Flórián, Fenyvesi Csaba: Kriminalisztikai Tankönyv és Atlasz Dialóg Campus Kiadó, Budapest-Pécs, 2002. ISBN 963–85756–8–9

[309] Truck EDR (Black box) download and analysis, Forrás: https://crashresponse.com/services/truck-edr-black-box-download-and-analysis/ Letöltve: 2022.11.11.

[310] Trusilo, Daniel (2023): Autonomous AI Systems in Conflict: Emergent Behavior and Its Impact on Predictability and Reliability. Journal of Military Ethics, 22(1), 2–17. Online: https://doi.org/10.1080/15027570.2023.22

[311] Tudás - mi ez, definíció és fogalom, Forrás: https://hu.economy-pedia.com/11040367-knowledge

[312] Tudás definíció, https://www.britannica.com/dictionary/knowledge Letöltve: 2023.04.20.

[313] Tudás definíciója, https://www.thefreedictionary.com/knowledge Letöltve: 2023.04.20.

[314] Tudás fogalma, https://hu.economy-pedia.com/11040367-knowledge Letöltve: 2023.04.20.

[315] Tudásmenedzsment - Dr. Szeghegyi Ágnes - https://kgk.uni-obuda.hu/sites/default/files/TMBSC.pdf Letöltve: 2023.04.20.

[316] Udemy, Digital forensics and electronic evidence, https://www.udemy.com/course/digital-forensics-and-electronic-evidence/

[317] Új járművek Budapesten, Forrás: https://www.vezess.hu/hirek/2026/03/27/uj-jarmuvek-jelennek-meg-budapesten/

[318] Updates over the air, https://www.bosch-mobility.com/media/global/mobility-topics/connected-mobility/updates-over-the-air/stage_internet-connectivity_1800x464_stage_mobile.jpg

[319] USB connector, https://farm2.staticflickr.com/1949/43242707710_b361b78eaf_z.jpg

[320] V2X járműkommunikáció alapjai, https://www.hit.bme.hu/~jakab/edu/litr/V2X/HU/V2X_jarmukommunikacio_alapjai_jegyzetvazlat_v01.pdf

[321] V2X járműkommunikáció, https://utugyilapok.hu/cikkek/a-v2x-jarmukommunikacio-alapjai/

[322] V2X sample, https://www.ctengineeringgroup.com/wp-content/uploads/2024/08/V2X-SAMPLE.jpg

[323] Vehicle forensics, https://berla.co/category/vehicle-forensics/

[324] Velodyne radar sensing, https://www.traffictechnologytoday.com/wp-content/uploads/2020/01/Velodyne-lidar-sensing.png

[325] Vilmos Garamvölgyi - László Viski (eds.): Kriminalisztika. Ministry of Interior, Department of Studies and Methodology, Budapest, 1961, 688. pp.

[326] Vízi Linda (2019): A Computer Forensics jogi vonzata. Online: https://netacademia.hu/courses/take/computer-jog/multimedia/8481853-figyelem-ez-egy-classic-tanfolyam

[327] Volvo recharge, https://d.newsweek.com/en/full/2321525/2024-volvo-c40-recharge-electric-vehicle-charging.jpg

[328] Walker, Paddy (2021): Leadership Challenges from the Deployment of Lethal Autonomous Weapon Systems. The RUSI Journal, 166(1), 10–21. Online: https://doi.org/10.1080/03071847.2021.19

[329] What is an E/E architecture, https://www.aptiv.com/en/insights/article/what-is-an-electrical-electronic-architecture

[330] What is ASIL? In: Synopsys. https://tinyurl.hu/v754 (Utolsó megtekintés: 2023. 07. 27.)

[331] What is automotive forensics, https://www.azolifesciences.com/article/What-is-Automotive-Forensics.aspx

[332] What is Digital Forensics and Why Is It Important?, Forrás:

https://www.provendatarecovery.com/blog/what-is-digital-forensics/ Letöltve: 2022.10.20.

[333] What is the iso26262,https://www.ni.com/en/solutions/transportation/what-is-the-iso-26262-functional-safety-standard-.html

[334] Wiener, Jonathan B. 2004. The regulation of technology, and the technology of regulation. Technology in Society 26. 483–500. https://doi.org/10.1016/j.techsoc.2004.01.033.

[335] William Newhouse Stephanie Keith Benjamin Scribner Greg Witte, NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

[336] Wonga, Cuebong et al. (2018): Autonomous Robots for Harsh Environments: A Holistic Overview of Current Solutions and Ongoing Challenges. Systems Science & Control Engineering, 6(1), 213–219. Online: https://doi.org/10.1080/21642583.2018.1477634

[337] Zalazone, önvezető jármű tesztelés, https://research-and-innovation.zalazone.hu/hu/a-zalazone-on-tesztelik-a-varosi-kozlekedes-jovojet/

[338] Zoltán Mráz: The importance of digital evidence tools in the investigation of crimes against property, Internal Affairs Review, Vol-7-8, 2018, 96 pp

[339] Zonal E/E architecture, https://www.automotiveworld.com/articles/zonal-e-e-architectures-the-cornerstone-of-future-mobility-development/

Kohéziós táblázat

TUDOMÁNYOS PROBLÉMA	*HIPOTÉZIS*	*CÉLKITŰZÉS*	*KUTATÁSI MÓDSZER*	*KÖVETKEZTETÉS*	*HIPOTÉZIS IGAZOLÁSA/ ELVETÉSE*	*ÚJ TUDOMÁNYOS EREDMÉNY*
A technológiai fejlődés nem csupán a közlekedési rendszerekre van nagy hatással. Az egyre komplexebb összekapcsoltság és a fejlett automatizálás interdependenciája új lehetőségeket teremt a közlekedés hatékonyságának és biztonságának növeléséhez. Ehhez az egyik lépés, hogy a jármű segíti a járművezetőt, a forgalmi helyzethez való alkalmazkodásban és a megfelelő döntések meghozatalában,	Az informatika hangsúlyos szakértői vizsgálati tevékenység miatt, ezidáig nem kerültek definiálásra mely kompetenciák, képességek és tudáselemek szükségesek azon szakértők számára, akik modern és önvezető járművek vizsgálatával foglalkoznak, vagy terveznek foglalkozni.	A modern járművekben található nyomok gyűjtésének, megőrzésének, kezelésének és tárolásának folyamatát megfelelő kvalifikációval rendelkező személyek végezhetik, ezért kutatásom egyik célja a vizsgálatok elvégzéséhez szükséges kompetencia és tudáselemek meghatározása.	Felkutattam, tanulmányoztam és feldolgoztam a kutatási témához kapcsolódó kiadványokat, szakirodalmakat, szabályzókat, eljárásokat, ajánlásokat, módszertanokat és irányelveket, amelyekre alapozva dokumentumelemzést és gyakorlati vizsgálatokat végeztem.	Elemzési és vizsgálati feladatok végrehajtásának eredményeként megállapítható, hogy a modern járművekben található nyomok gyűjtésének, megőrzésének, kezelésének és tárolásának folyamatának végig vitelét megfelelő kvalifikációval rendelkező személyek végezhetik, a vizsgálatok elvégzéséhez speciális ismeretek, kompetenciák szükségesek, melyek meghatározása hozzájárul a szakértői munka	A hipotézist igazoltam, a technológiai fejlődés és a járművek digitalizálódása miatt a gyűjtött, tárolt és feldolgozott információk mennyisége és azokhoz történő hozzáférés és elemzés új képességeket igényelnek, melyek meghatározása elengedhetetlen a szakértők felkészítéséhez, képzések szakmai tartalmának összeállításához, valamint a szakértői vizsgálatok	**Rávilágítottam**, hogy modern járművekkel kapcsolatos események, új vizsgálati célok kikényszerítették, hogy az informatikával vagy járművek szakértői feladatait ellátó szakértők eseti jelleggel, végeznek járművekben található adatokkal kapcsolatos vizsgálatokat, azonban ezek nem módszeres, a járművekben található adattárolókat és adatokat nem teljeskörűen figyelembe vevő vizsgálatok, ahol korlátozott a

illetve az emberi tényező hatásának csökkentése, ellensúlyozása, a vezető nélküli járművekre való átállás. Az autonóm módon működő járművek hosszú távon nagyobb biztonságot eredményeznek, azonban az általuk tárolt, gyűjtött és feldolgozott információk védelmét és utólagos szakértői vizsgálatban való elérhetőségét biztosítani szükséges, amihez jelenleg nem áll rendelkezésre a szükséges kompetencia és tudáselemek rendszerezett meghatározás, ami nélkülözhetetlen a szakértők felkészült feladatvégzéséhez.				eredményes elvégzéséhez, a vizsgálati célok teljesítéséhez.	szakmaiságának biztosításához.	rendelkezésre álló kompetencia. Emiatt nem garantált, hogy elegendő mennyiségű és/vagy minőségű bizonyíték kerül összegyűjtésre, nem készül megfelelő dokumentáció, a nyomkezelés nem megfelelősége miatt a vizsgálat nem megismételhető, hibák keletkeznek az elemzés vagy az értelmezés során. **Meghatároztam**, rendszereztem mely kompetenciák és tudáselemek szükségesek azon szakértők számára, akik ilyen járművek vizsgálatával foglalkoznak, vagy terveznek foglalkozni, annak érdekében, hogy a szükséges ismeretek célirányosan elsajátíthatóak legyenek.

A szakértői feladat ellátásához a modern és egyre inkább önvezetővé váló és hálózatba kapcsolt járművek elterjedése kapcsán a kiindulási alapot az igazságügyi kamara elnöksége által előkészített és elfogadott, a módszertani levél kiadásának részletes szabályairól szóló szabályzat alapján készített módszertani levelek adják. A jelenleg hatályos módszertani levelek a digitális forenzikus módszertanokat veszik alapul és határozzák meg a digitális adatok (elektronikus adatok) azonosításának, gyűjtésének, feldolgozásának, elemzésének és a	A magas automatizáltságú, egyre inkább önvezetővé váló járművek szakértői vizsgálatához jelenleg nem áll rendelkezésre olyan definiált módszertan vagy módszertani levél melyek alapján a modern járművek szakértői vizsgálata szakszerűen elvégezhető.	Kutatásom célja hozzájárulni a hazai és nemzetközi vonatkozású, modern és egyre inkább önvezetővé váló, polgári és katonai felhasználású, közúti közlekedési járművek szakértői vizsgálatának hatékony és eredményes elvégzéséhez. A járművek fejlődésével, a beépített mobil kommunikációs eszközök elterjedésével és a kooperatív közlekedés rendszerek széleskörű alkalmazásának küszöbén nagy számban meg fognak jelenni a modern járművekhez kapcsolódó szakértői vizsgálatok, az	Kutatási eredményeim nemzetközi és hazai szakmai és tudományos fórumokon konzultáltam meg, emellett folyóiratokban publikáltam, részt vettem szakmai képzéseken és több tudományos és szakmai konferencián is részt vettem hallgatóként és előadóként is. Rendszeresen konzultáltam a kutatási eredményeim és a járművekhez kapcsolódó igazságügyi szakértői munka kapcsolatáról, valamint az elképzeléseim megvalósíthatóságáról a Nemzeti Szakértői és Kutató Központ szakértőivel, Rendőrséggel. Felhasználtam a saját korábbi kiberbiztonsági és műszaki	A jelenlegi digital forensics domain-ek módszertanai, a hazai módszertani levelek nem biztosítják a modern járművek digitális adatainak azonosításának, gyűjtésének, feldolgozásának, elemzésének és a vizsgálatának kialakítását.	A magas automatizáltságú, járművek szakértői vizsgálatához kapcsolódóan igazoltam hipotézisemet, hogy jelenleg nem áll rendelkezésre olyan definiált módszertan vagy módszertani levél melyek alapján a modern járművek szakértői vizsgálata szakszerűen elvégezhető.	**Megvizsgáltam**, hogy magas automatizáltságú, egyre inkább önvezetővé váló járművek szakértői vizsgálatához jelenleg milyen módszertanok, ajánlások állnak rendelkezésre. Szakértői gyakorlati és szakirodalmi kutatómunkával **bebizonyítottam**, hogy jelenleg nem áll rendelkezésre olyan módszertan, eljárás, amely alapján a modern járművek szakértői vizsgálata szakszerűen elvégezhető. **Elkészítettem**, a gyakorlatban teszteltem a modern járművekhez kapcsolódó kihívásokat is figyelembe vevő módszertani leírást, igazoltam, hogy a módszer egységes keretet biztosít a

vizsgálat eredményeinek nem szakemberek számára is értelmezhető formában történő bemutatásának gyakorlatát. A módszertani levelek kiadása óta eltelt évek és a technológiai fejlődés, a modern és egyre inkább önvezetővé váló járművek sajátosságai miatt szükséges és indokolt felülvizsgálni ezek relevanciáját a digitalizálódó járművek szakértői vizsgálata kapcsán és szükség szerint módosított, vagy új módszertan elkészítése.		elektronikus bizonyítékok feltárásának igénye. Az adatok hozzáférhetősége, összegyűjtése, értékelése nem mindig triviális, számos kihívást jelent a szakértők számára. Széles körben elérhető és alkalmazható technikai megoldások egyelőre nem léteznek, a feladatok komplexitása várhatóan növekedni fog. Célom egy a modern és egyre inkább önvezetővé váló járművek vizsgálatához kapcsolódó kihívásokat is figyelembe vevő, hatékonyan alkalmazható vizsgálati módszertan kidolgozása, ami alapja lehet egy	tapasztalataimat, releváns hazai és nemzetközi szakmai képzéseken szerzett ismereteimet, valamint szakértői vizsgálatokban szerzett ismereteimet.			vizsgálatok elvégzéséhez.

		szakértői módszertani levél kidolgozásának.				
A biztonságos katonai műveletek mellett olyan esetekben is szükséges a járművek szakértői vizsgálata, amikor a járművet bűncselekmény elkövetésének eszközeként használták. Ilyen esetben a járműben keletkezett, tárolt és kinyerhető adatok kellő időben történő megszerzése hozzájárulhat egy kiemelt bűncselekmény, például egy terrortámadás elkövetőinek gyorsabb és hatékonyabb felderítésében és az esemény körülményeinek tisztázásában. Ezen túlmenően a járművek	A járművekkel kapcsolatos események, új vizsgálati célok kikényszerítették, hogy az informatikával vagy járművek szakértői feladatait ellátók járművekhez, járművekben található adatokhoz kapcsolódóan is végezzenek eseti jelleggel vizsgálatokat, azonban ezen vizsgálatok jellemzően informatikai módszertan és eljárás hangsúlyosak, eszköz és technológia specifikusak, nem kerültek meghatározásra a vizsgálatokhoz kapcsolódó	Kutatási célom meghatározni és rendszerbe sorolni azon modern járművek szakértői vizsgálatához tartozó kihívásokat, meghatározni a járművekben megtalálható, elérhető adatokat és hordozóikat, valamint összerendelni az információszerzési módszerekkel.	Rendszeresen konzultáltam a kutatási eredményeim és a járművekhez kapcsolódó igazságügyi szakértői munka kapcsolatáról, valamint az elképzeléseim megvalósíthatóságáról a Nemzeti Szakértői és Kutató Központ szakértőivel, Rendőrséggel. Gyakorlati vizsgálatokat végeztem különböző gyártmányú és gyártási évű járműveken. Felhasználtam a saját korábbi kiberbiztonsági és műszaki tapasztalataimat. Nemzetközi szakmai képzéseken szereztem ismereteket.	A modern járművekhez kapcsolódóan szükséges a kapcsolódó kihívások meghatározása és rendszerezése, az általános kihívásokon túlmenően a vizsgálati eljáráshoz kapcsolódóan és a vizsgáló eszközökhöz kapcsolódóan is meghatároztam kihívásokat, beleértve a katonai műveletek során történő alkalmazás kihívásait is.	A hipotézist igazoltam, nem kerültek meghatározásra és rendszerezésre a szakértői vizsgálatokhoz kapcsolódó kihívások, valamint a járművekben keletkezett, tárolt és kinyerhető adatok és információszerzési módszerek összerendelése.	**Kidolgoztam** a modern és egyre inkább önvezetővé váló járművek szakértői vizsgálatának kihívásait -valamint az adatok, adathorozóhoz kapcsolódó- információszerzési módszerekhez való összerendelést-, az általános kihívásokon túlmenően a vizsgálati eljáráshoz kapcsolódó és a vizsgáló eszközökhöz kapcsolódó kihívásokra kiterjedően, ideértve a katonai műveletek során történő alkalmazás kihívásait.

tartalmazhatnak evidenciát olyan esetekben is, amikor egy megtörtént esemény utólagos vizsgálatát végzik, például baleset vagy titkos információgyűjtés esetén, azonban a kapcsolódó kihívások és az elérhető adattárolók és kinyerhető adatok meghatározása és információszerzési módszerekkel való összerendelése nem történt meg.	kihívások és a járművekben keletkezett, tárolt és kinyerhető adatok, valamint az információszerzési módszerekkel való összerendelése.					
A biztonságos katonai műveletek – ellenséges környezetben végzett katonai műveletek, terrorelhárítás, hírszerzés stb. – egyik fontos összetevője a digitális eszközök szakértői vizsgálatának elvégzése. Legyen	Az alkalmazott vizsgálati eljárások nem alkotnak egységes rendszert, nem biztosítják kielégítő módon a szakértői vizsgálatokkal kapcsolatos vizsgálati elveket. A digitális forenzikus domain-ek	Kutatásom eredményeként célom, a releváns digital forensics domainek vizsgálata és annak meghatározása, hogy a meglévő digital forensics domain-ek alkalmasak-e a modern és egyre inkább önvezetővé váló játművek	Felkutattam, tanulmányoztam és feldolgoztam a kutatási témához kapcsolódó kiadványokat, szakirodalmakat, szabályzókat, eljárásokat, ajánlásokat, módszertanokat és irányelveket, amelyekre alapozva	A digital forensics domaineken belül megállállapítható, hogy ezek egyike sem alkalmazható teljeskörűen a modern járművek vizsgálata során, annak komplexitása és jelenlegi, és a jövőben várható kihívásait tekintve.	A hipotézist igazoltam, a jelenleg alkalmazott vizsgálati eljárások nem alkotnak egységes rendszert, nem biztosítják kielégítő módon a szakértői vizsgálatokkal kapcsolatos vizsgálati elveket.	A digitális forenzikus domain-ek vonatkozásában **megállapítottam**, hogy a modern és egyre inkább önvezető járművek szakértői vizsgálata nem tartozik egyik digital forensics szakterülethez, nem sorolható be ezekbe, ezért szükséges egy új domain

szó az ellenség digitális rendszereinek vizsgálatáról, műveleti területeken történő adatkinyerésről, a potenciális incidensek utólagos vizsgálatáról, a fenyegetések azonosításáról, a sérülékenységek mérsékléséről vagy a biztonsági szint, a működési folyamatok, a katonai műveletek fejlesztése érdekében végzett tevékenységekről. A digitális információk közlekedési eszközökből történő kinyerése, a digitális nyomok/adatok gyűjtése, elemzése katonai felhasználásban stratégiai kérdés, elengedhetetlen a műveleti és	vonatkozásában nem állapítható meg, hogy a modern járművek szakértői vizsgálata mely szakterülethez tartozik, egyáltalán besorolható-e ezekbe, vagy szükséges egy új domain létrehozása.	szakértői vizsgálatának módszertani hátteréül szolgálni, vagy új szakmai és módszertani definíció készítése szükséges.	dokumentumelemzést végeztem. Kutatási eredményeim nemzetközi és hazai szakmai és tudományos fórumokon konzultáltam meg, emellett folyóiratokban publikáltam, részt vettem szakmai képzéseken és több tudományos és szakmai konferencián is részt vettem hallgatóként és előadóként is. Rendszeresen konzultáltam a kutatási eredményeim és a járművekhez kapcsolódó igazságügyi szakértői munka kapcsolatáról, valamint az elképzeléseim megvalósíthatóságáról a Nemzeti Szakértői és Kutató Központ szakértőivel, Rendőrséggel. Felhasználtam a saját korábbi		A digitális forenzikus domain-ek vonatkozásában nem állapítható meg, hogy a modern járművek szakértői vizsgálata mely szakterülethez tartozik, az nem besorolható ezekbe.	létrehozása. **Definiáltam** az Autonomous Vehicles Forensics fogalmát, mint a Digital Forensics domain új elemét, összehasonlítva a különböző vizsgálati módszerek (számítógépes, felhő, IoT, stb.) folyamatlépéseivel és azok alkalmazhatóságával. **Elkészítettem**, a gyakorlatban teszteltem a modern járművekhez kapcsolódó kihívásokat is figyelembe vevő módszertani leírást, igazoltam, hogy a módszer egységes keretet biztosít a vizsgálatok elvégzéséhez.

nemzetbiztonsági célok támogatásához, ami indokolja egy módszertan meglétét és vizsgálni szükséges, hogy ez beilleszthető-e valamelyik már meglévő digital forensics domain-be.			kiberbiztonsági és műszaki tapasztalataimat, releváns hazai és nemzetközi szakmai képzéseken szerzett ismereteimet, valamint szakértői vizsgálatokban szerzett ismereteimet.			