BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Kiberbiztonság az autóiparban

Automotive Cybersecurity

Tokody Dániel*, Albini Attila*, Ady László**, Temesvári Zsolt Marcell*, Rajnai Zoltán*
* Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Hungary
** Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, Budapest, Hungary
daniel_tokody@ieee.org attila.albini@gmail.com adylaszlo@gmail.com zsolt.temesvari@gmail.com
rajnai.zoltan@bgk.uni-obuda.hu

***Összefoglalás* — Tanulmányunkban megvizsgáltuk a járművek kiber-fizikai rendszerré válásának és hálózatba kötésének motivációit. A legfőbb motivációk közé tartozik a biztonságos közlekedés és az energiahatékony mobilitás megvalósítása. A járművek hálózatba kapcsolásának több módját is sorba szedve, valamint a járműrendszerek funkcionális- és kiberbiztonságával kapcsolatos észrevételeink alapján egy új biztonság szemléletű tervezési módszert ajánlunk a nemzetközi szabványosításhoz illesztetten az autonóm intelligens járművek és az okos mobilitási rendszer létrehozásához.**

***Kulcsszavak*:** funkcionális biztonság, kiberbiztonság, járműrendszerek, járműfedélzeti rendszerek védelme

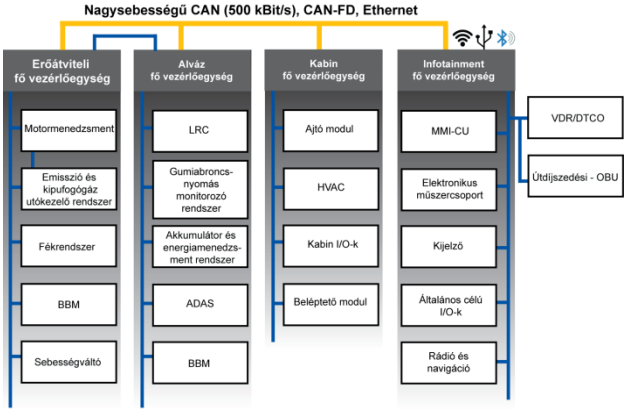
***Abstract* — In our study, we examined the motivation of vehicles becoming cyber-physical systems and their connection. The mentioned main motivations include safe transportation and energy-efficient mobility. We are also suggesting a new safety and security method by our observations about functional and cyber-safety of vehicles to develop new autonomous intelligent vehicles and a smart mobility system based on the international standards.**

***Keywords*:** functional safety, cyber security, vehicle systems, in-vehicle network security

1 BEVEZETÉS - ÚT A HÁLÓZATBA KAPCSOLT JÁRMŰVEK FELÉ

Az elmúlt években világszinten évente kb. 1,25 millió ember halt meg az utakon a közúti járművekkel kapcsolatos balesetek során a WHO statisztikái szerint. [1] A kooperatív intelligens közlekedési rendszerek létrehozásának célja a folyamatos és közvetlen információcsere a közlekedés valamennyi résztvevője között. Az ez irányú járműkommunikáció legfontosabb motivációit a közúti közlekedés biztonságának növelése, a forgalmi dugók és torlódások számának, időtartalmának (idő- és üzemanyag takarékosság magas szintű megvalósítása) és a közlekedés CO_2, illetve károsanyag-kibocsátásának csökkentése jelenti.

Az átlagos gépjárműhasználó ma már azzal szembesül, hogy a korszerű járművek keréken guruló komputerként egy közlekedési célú kiber-fizikai rendszerként definiálhatók. A mai modern gépjárművek kb. 70 darab elektronikus vezérlő egységet (ECU-t azaz Electronic Control Unit) tartalmaznak. [2] Egy felsőkategóriás járműben ez a szám már elérheti a 150-et is. Az autonóm intelligens járművek esetében pedig jelentősen több és még összetettebb intelligens vezérlőegységek és érzékelők sora határozza meg az adott jármű autonóm működését. A legismertebb ECU-k között említhető a motorvezérlő modul vagy éppen a fékvezérlőegység. [3] Az első ábrán egy általános haszongépjármű elektromos/elektronikus elosztott szabályozási rendszerének architektúrája látható az említett és néhány további főbb vezérlőegységek feltüntetésével. Ez szemlélteti a járművek belsőhálózatát, azaz a járműrendszerek hálózatba kapcsolását.



1. ábra: Haszongépjárművek elektromos/elektronikus elosztott szabályozási rendszerének architektúrája (saját szerkesztés) [3][4]

Az autó- és járműgépészet ma már inkább olyan interdiszciplináris járműmérnöki tudományt jelent, amely kapcsán a gépészeti, villamosmérnöki, informatikai, adattudományi és anyagtudományi stb. területek együttes felhasználására is szükség van.

A járművek és a közlekedés biztonságának növelése érdekében az európai szintű kooperatív közlekedési rendszer létrehozása és az ezzel kapcsolatos kommunikációs hálózatba való kapcsolás megvalósítása folyamatban van. A hálózatosodás új kihívások elé állítja a teljes iparágat. Így a járművek kiberbiztonságának növelése az elmúlt pár évben egyre nagyobb hangsúlyt kap.

1.1 Az intelligens autonóm járművekkel kapcsolatos legfontosabb fogalmak

Az **intelligens közlekedési rendszerek** általános definíciója szerint a biztonság elérése érdekében és a mobilitás környezeti hatásainak csökkentésére az infokommunikációs rendszerek alkalmazásával törekszünk az intelligens közlekedési rendszerben. [5][6]

Néhány fontos fogalom az intelligens közlekedési rendszerekben:

Automatizált jármű, olyan jármű melynek járműrendszerei lehetővé teszik a vezető számára, hogy bizonyos vezetési funkciókat a járműre bízzon. [7]

Autonóm jármű (teljesen automatizált jármű), olyan jármű, amely járműrendszerei lehetővé teszik az autonóm közúti jármű számára, hogy biztonságosan közlekedhessen az adott közlekedési rendszerben megfelelő keretek között. [7]

Az **intelligens autonóm közúti jármű,** azaz interaktív kooperációra képes közúti jármű, amely emberi beavatkozás nélkül önmaga irányításával és navigációjával a közlekedési helyzet figyelembevételével képes működni.

Az **intelligens autonóm közúti járműrendszerek** azon technológiai rendszerek, fődarabok összessége, amelyek segítségével az autonóm intelligens jármű, autonóm működésre képes, pl.: intelligens szenzorok és beavatkozók.

Összekapcsolt vagy hálózatba kötött jármű, olyan közúti jármű, amely rendelkezik olyan járműrendszerrel, ami biztosítja a vezeték nélküli kommunikációt a közlekedési rendszer egyéb külső elemei, más járművek, hálózatok és szolgáltatások között a minél magasabb szintű vezetés automatizáltsághoz. [7] [5] [6] A járművek automatizálásával, kommunikációs összekapcsolásával, hálózatba kötésével csökkenthető az emberi járművezető közlekedésben betöltött szerepe.

Az autóipari kiberbiztonság az autóipari kibertérben az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását jelenti, a járművek, a járműveket használók, a járművel kapcsolatos szoftverek és szolgáltatások, eszközök, illetve hálózatok komplex környezetében. [8]

1.2 A közúti járművek biztonsági rendszereinek fejlődése

Az 1950-es évektől a 2000-es évekig a közúti járművek tekintetében a biztonságos közlekedés és a kényelmes fáradságmentes vezetési élményt pl.: a biztonságiöv, a blokkolásgátló rendszerek vagy éppen a tempomat (sebességtartó rendszer) jelentette. 2000 – 2010 között az elektronikus stabilitás szabályozás (menetstabilizáló), a holttér figyelő rendszer, a ráfutásos ütközést megelőző figyelmeztető rendszer, illetve például a forgalmi sáv tartásának gépi úton történő megvalósítása volt a biztonság növelésének eszköze. 2010 – 2016 között a intelligens tolatókamera, az automatikus vészfékezés, a gyalogos-felismeréssel egybeépített automatikus járműmegállító rendszer, az automatikus tolatást segítő rendszer, a sávelhagyásra figyelmeztető rendszer vált általánossá a magasabb kategóriás járművekben. 2016 – 2025 közötti években a már közkeletűvé vált iparági vízió szerint az adaptív sebességtartó rendszer, a forgalmi torlódásban segédkező rendszer vagy éppen az automata parkolási rendszer fogja segíteni a járművezetők tevékenységét. 2025-at követően pedig várható a teljesen automata biztonsági rendszerek elterjedése, valamint az autópályák esetében már valószínűleg alkalmazható lesz a járművekbe épített autópilóta is. [9]

1.3 Európai törekvések, a biztonság növelésének új eszköze az összekapcsoltság megvalósítása

Első lépésként a kommunikáció útján való összekapcsoltság irányába 2015. április 29-én „az Európai Parlament és a Tanács 2015/758 rendeletével a 112-es egységes európai segélyhívó szolgáltatáson alapuló fedélzeti e-segélyhívó rendszer kiépítésével összefüggő típus-jóváhagyási követelményekről és a 2007/46/EK irányelv módosításáról” szóló rendeletében megalapozta és általánossá tette a gépjárművek közös rendszerbe való kötését. [10] Amely folyományaképpen az Európai Unióban 2018. március 31-től minden újonnan forgalomba helyezett közúti járműbe kötelező beszerelni az eCall segélyhívó rendszert, amelyet a nemzeti hatóságoknak ellenőrizni kell. [10]

„Az eCall-funkcióhoz szükséges hardvert az autóban a beépített telematikai egység jelenti, ami elsősorban egy modemből – a közös hálózati kapcsolódást biztosító készülékből – egy műholdas helymeghatározó antennából (pl.: Galileo műholdas navigációs és helyzetmeghatározó rendszer), és a járművel való kapcsolódást biztosító elektronikából áll.” A rendszerhez illesztetten van lehetőség tartalék a jármű elsődleges villamos rendszerétől független tápellátás biztosítani a segélyhívást megvalósító eszköz számára. [11] Mindez annyit jelent, hogy a jövőben az új gépjárművek már legalább egy hálózatához alapvetően csatlakozni fognak.

A közlekedési telematikai rendszerek fejlődésével például a járművek távoli diagnosztikai lehetőségei is bővültek. Ezt a kapcsolatot általában a járművek vezeték nélküli helyi hálózathoz csatlakoztatásával egy mobil eszközön keresztül az internet elérése érdekében alakítják ki. Amely lehetőséget ad például egy online járműszervizzel való kapcsolatfelvételre vagyis az interneten keresztül egy újabb hálózathoz csatlakozik már az adott jármű.

A harmadik típusú példa a járművek hálózatba kapcsolásának olyan folyamata, amelynek már az ember nem szükségképpen szereplője. Vagyis a járművek kommunikációs lehetőségeinek bővülésével létrejöhetett egy új féle minden eddiginél hatékonyabb formája a hálózatba kapcsolt járműveknek. A kommunikáció kialakítására már többféle biztonságkritikus formát is létrehoztak. A többszereplős rövid hatótávú vezeték nélküli megoldások között a célorientált rövid távolságú kommunikáció megvalósítása a cél (pl.: Dedicated Short Range Communications - DSRC). [12]

Az említett technológiai fejlesztése kihatással vannak az utasbiztonságra, üzembiztonságra vagy akár a közlekedésbiztonságra.

1.4 A hálózatba kapcsolás modern vezetéknélküli kommunikáció alapú módszerei

Az információtovábbítás egyik módja az intelligens közlekedési rendszerekben a célorientált rövid távolságú kommunikáció (DSRC) megvalósítása. [12] Amely a következő kommunikációs lehetőségeket jelenthetik:

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. [12] [13] [14]

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. [12] [13]

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. [15] [16] [17]

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. [18]

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. [13][18][19]

A kooperativitáson alapuló hatékonyság és közlekedés biztonsága a célorientált rövid távolságú kommunikáción (DSRC) és a fejlett vezetőtámogató rendszerek és szolgáltatások (Advanced Driver-Assistance Systems - ADAS) együttműködésén keresztül valósítható meg.

A közös rendszerhez, hálózathoz kapcsolódik a rendszerben lévő számos jármű érzékelőhálózata, az infrastruktúra kommunikációra képes elemi (pl.: vezetéknélküli érzékelő hálózatok [20]) és a közlekedési rendszer összes résztvevőjének alhálózatai. A közös hálózatban rejlő információk alapján azonnali automatikus reakciókat (megfigyelés, riasztás, fékezés és kormányzás stb.) válthatnak ki a közlekedés folyamán előálló megfelelő információ konstellációk. Ezeknek a funkcióknak a hatékony megvalósítása csak is márkafüggetlen módon és a nemzeti határokon átívelő [21] infrastrukturális megoldásokkal való létrehozása adhat megfelelő funkcionális biztonsági szintet a közös integrált európai kooperatív közlekedési rendszerben.

2 A BIZTONSÁG ÉRTELMEZÉSE AZ AUTONÓM INTELLIGENS JÁRMŰVEK KIBER-FIZIKAI JÁRMŰRENDSZEREINEK ESETÉBEN

A UNECE 29-es munkacsoportja 2017-ben elfogadta és közreadta az automatizált, összekapcsolt és hálózatba kötött közúti járművek üzemeltetésére vonatkozó szempontokat, követelményeket, elősegítve ezzelaz automatizált vezetési funkciókkal rendelkező közúti járművek biztonságos használatát. A szabályozás az autonóm járművek részletes funkcióira még nem kidolgozott, így például az autonóm járművek kiberbiztonságának terén még szükség van a szabályozást is érintő további fejlesztésekre. [8] [22]

Az automatizált és együttműködő intelligens közlekedési rendszerek fontos elemei a földi járművek. Az autonóm intelligens földi járművek biztonság szempontú vizsgálata, tervezése során elsődlegesen a SAE International szerinti biztonság összetevőket vesszük figyelembe.

A SAE szerint a biztonság összetevőit: a funkcionális biztonság, az aktív biztonság (pl.: ADAS), az elektronikus és elektromos rendszerek hardver és szoftver megbízhatósága, valamint az emberi tényező rendszer biztonságra gyakorolt hatásai alkotják. Más besorolás szerint a biztonság háromféle területre bontható: funkcionális biztonság („functional safety”), műszaki biztonság („technical safety”), függő biztonság („contextual safety”) (EN 50126-2:2017). [23]

Az említett felsorolásban csak mögöttes értelmet keresve találjuk a járművek és járműrendszerek informatikai, kiber részének biztonságát. A "kiber" és a "biztonság" szavaknak autóipari területen korábban meglehetősen más értelme volt, mint például az informatikában. A "biztonság" fogalmát szinte kizárólagosan a jármű fizikai, funkcionális biztonságával összefüggésben használták.

A gépjárműveken belüli, a járművek elektromos/elektronikus alrendszerei közötti kommunikációs rendszerek fejlődésével és a belső villamos kábelezések bonyolultságának csökkentésének igényével, a belső hálózat rugalmasságának, valamint megbízhatóságának növelésével a fedélzeti buszok alkalmazása terjedt el járműipari alkalmazásokban az 1990-es évektől. Létrehozva ezzel a kommunikációs hálózatra és beágyazott irányítástechnikai rendszerekre alapozott úgynevezett Drive-by-Wire struktúrákat. [24] [25]

A járművekbe épített funkcionalitások bővülése (pl.: fedélzeti tájékoztató és szórakoztató elektronika – Infotainment stb.) a buszrendszerek számának növekedését és jellegének bővülését jelentette. A biztonsági funkciókat megvalósító buszokat elválasztották a kényelmi funkciókat biztosító hálózattoktól. A járművek funkcionális biztonsága a járművekben található hardver és szoftver elemektől vált függővé. [25]

A gyakorlati tapasztalatok szerint a forgalomba került gépjárművek jelentős része kiber támadhatóság szempontjából kitett a kiberbiztonsági szempontokat csak részlegesen figyelembe vevő tervezési folyamatból adódóan is. Tipikusan az adott kényelmi funkciót megvalósító jármű fedélzeti rendszerek (pl.: navigációs rendszer, Bluetooth kapcsolat, In-car Internet stb.) a megvalósítás során nem kielégítő védelemmel vagy akár védelem nélkül kerülnek létrehozásra. Ezeket a hibákat kihasználva és a járművek nem megfelelően védett kommunikációs hálózatokhoz való csatlakoztatásával [26] elérhetővé válhatnak olyan biztonsági funkciók, amelyek működése megzavarható, az irányítása átvehető, akár közvetlen fizikai kapcsolat nélkül. Ezért az okos mobilitási rendszer fő elemét az autonóm intelligens járművet már kiberbiztonság szempontjából is tervezni kell. Az intelligens autonóm járművek kiberbiztonság szempontú tervezése új és szabványosítás alatt álló terület. [25] [27] [28] [29] [22]

2.1 Az autonóm intelligens járművek kiber-fizikai járműrendszereinek funkcionális biztonsága

A funkcionális biztonság azt jelenti az autonóm intelligens járműrendszerek kapcsán, hogy az adott járművet olyan állapotban kell tartani, hogy az emberi élet védelme a legnagyobb mértékben biztosított legyen. Más szavakkal „a funkcionális biztonság azt a törekvést jelenti, amely során a jármű alapvető funkcióinak hibáit megakadályozzuk az utasok biztonsága érdekében. Többek között ilyen alapvető funkciók, amelyek közvetlen kapcsolatban állnak a biztonsággal a kormányzási vagy éppen a fékezési funkciók. A légzsákok, a gyűrődési zóna, az ESP vagy az ABS is a jármű funkcionális biztonságát befolyásoló tényezők.”[30]

Az autonóm intelligens járművek közlekedés biztonsággal összefüggő kiber-fizikai rendszereire a 2. ábrán láthatunk példát a jármű környezetére vonatkozó rendszerekkel egyetemben. Ez a példa jól mutatja, hogy a járművek biztonságos közlekedését aktívan vagy akár passzívan befolyásoló informáló, figyelmeztető, felügyelő, biztonsági, beavatkozó, hatásokat csökkentő vagy mentést könnyítő rendszerek mind-mind kihatással vannak az informatikai- és kiberbiztonságra.

„A biztonsági integritás (safety integrity – a biztonság sértetlensége) annak valószínűsége, hogy egy biztonsági rendszer az előírt biztonsági funkciókat egy adott időszakban meghatározott körülmények között megfelelően végrehajtja, azaz nem lépett fel veszélyeztető meghibásodás. Egy rendszerhez rendelt biztonsági integritási szint (SIL) meghatározza az alkalmazandó fejlesztési, tervezési, gyártási, üzemeltetési módszereket.” [31] Mindazonáltal a funkcionális biztonsághoz köthetően a járművek elektromos és elektronikus rendszereinek biztonságát is jellemezhetjük a biztonság integritással. A jármű ipari biztonságkritikus rendszerek esetében az ASIL (Automotive Safety Integrity Level) értékek használatosak a járművek életciklusa során.

2.2 Az autonóm intelligens járművek kiber-fizikai járműrendszereinek informatikai biztonsága

A informatikai biztonság azt jeleni, hogy ügyelünk rá, hogy más ne kaparinthassa meg a tulajdonunk. Erre jó példa a bankautomatákban tárolt pénz védelme, vagy az informatikában a jelszavak/adatok biztonsága is. Így a autonóm intelligens földi járművek informatikai biztonság szempontú vizsgálata, tervezése során elsődlegesen a kiberbiztonság megvalósítása a cél. Az intelligens közlekedési rendszerek jármű, járműrendszerek és intelligens infrastruktúra konstellációjában az informatikai biztonság értelmezése kapcsán több összetevőt azonosítottunk kutatásunk során.

„A informatikai biztonság a járművek szoftvereinek és az ezzel kapcsolatos rendszereinek biztonságát jelenti. Az esetleges szoftveres véletlenszerű vagy szisztematikus hibák és a külső kibertámadások elleni védelmet. A járműipari szoftverek különböző szerepet töltenek be a járművek működésének és funkcionális biztonságának biztosításában.” [30] A közlekedési rendszerben például a ‘0231512’ számsor lehet egy adat. Viszont, ha ez az adat az egyik jármű kommunikációs azonosítója a közlekedő járművek ad hoc hálózatában, akkor ez már egy információ az adott rendszerben.

Muha szerint az informatikai biztonság rendszertana alapján a védendő elemek között találhatóak a rendszert használó személyek, az informatikai rendszer fizikai környezete, a működéséhez szükséges infrastruktúra, a hardver, a szoftver, a kommunikációs eszközök és hálózat, az adat hordozók, valamint a rendszerrel kapcsolatos szabályozás. [32] Ez nem csak általánosan, de az autóiparban is igaz, vagyis az informatikai biztonság azt jelenti, hogy az információ bizalmasságára, sértetlenségére és rendelkezésre állására fokuszálunk. Mindemellett az autóipari kiberbiztonság alatt az iparági infokommunikációs rendszerek védelmét is értjük. Az autóipari kiberbiztonság magába foglal mindent és mindenkit, akik a kibertéren keresztül a járműipari alkalmazásokhoz hozzáférhetnek.

3 KIBERFENYEGETÉS, KIBERVÉDELEM, KIBERBIZTONSÁG KÉRDÉSE AZ AUTÓIPARBAN

A járművek fizikai védelmére, például a ballisztikai szempontból való külső támadhatóságára már hosszú ideje megfelelő figyelmet fordítanak a fejlesztők, a katonai alkalmazások jól példázzák ezt. [33] [34] A kiberfenyegetések, mint például a vírusfertőzések, célzott adatvesztés előidézése, hardver hiba előidézése szándékos törlésből adódó adatvesztés elleni felkészülés elengedhetetlen a járműipari alkalmazásokban is. A fenyegetésekből adódóan keletkezhetnek fizikai károk, kritikus szolgálatás kimaradás, kompromitálódás, funkció vesztés stb. [35]

Ugyanakkor az előzőekben leírt jármű architektúra és az intelligens közlekedési rendszerek működése is felveti a járművek kibervédelmének kérdését.

A közlekedési rendszer növekvő automatizáltságával egyenes arányban növekszik a kibervédelemre szoruló közlekedési rendszerben kulcs szerepet játszó eszköz pl: járművek, intelligens infrastruktúra, út menti egységek stb.

„A kiberbiztonság a kibertérben lévő szolgáltatás vagy adat meghatározott kiberfenyegetések ellen, előre meghatározott védelmi szintű állapotát jelenti.” [35]

Mit jelent a kiberbiztonság a járművek és járműrendszerek esetében? A 2.1 pontban általánosságban megfogalmazottakon túl az intelligens autonóm járművek belső struktúrájában, külső környezetében létrehozott, illetve alkalmazott információs és kommunikációs hálózatok, rendszerek és ebben a hálózatban, rendszerben létrejövő, áramló információ megfelelő védettségének, bizalmasságának, hitelességének stb. a biztosítása, azaz a károsodástól, illetéktelen hozzáféréstől és módosítástól stb. való védelmének megvalósítása.

3.1 *Kibervédelmi módszerek járművek esetében*

A modern járművek egyre több támadható felületének (pl.: kihasználható szoftverhibák) illetve a járműhasználók magánszférájának megsértésének komoly biztonsági kockázata van. A járművek ellen irányuló kibertámadások (pl.: malware támadások, fedélzeti diagnosztikai rendszer biztonsági rései stb.) egyre növekvő és aggasztó számban jelentek meg az utóbbi időben. [36] [37]

A járművek, járműrendszerek kibervédelmének lépéseit a következő pontokban fogalmazzuk meg:

A járműrendszerek (járművek belső rendszerei közötti) és járművek közötti kommunikáció biztonságának és az autóipari és közlekedési informatikai és információs rendszereinek fizikai infrastruktúrájának védelmének megvalósítása. [38]

A járműrendszerek és járművek működésbiztonságának megvalósítása a közlekedési folyamatok szándékos megzavarása, megváltoztatása elleni védelem létrehozása során. [38]

Az intelligens közlekedési rendszerek, a járművek és járműrendszerek informatikai és információs biztonságágának megvalósítása a rendszerben gyűjtött, tárolt és továbbított adatok lopásával, törlésével vagy megváltoztatásával szembeni védelme. [38]

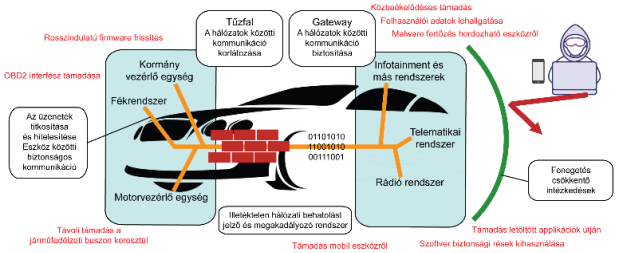
A járművek fizikai biztonsága az informatikai és információs rendszer védelme során a fizikai veszélyektől (pl.: járművezérlő egységekhez való illetéktelen hozzáférés, fertőzött, átalakított bűnös célú hardver beépítése a járműbe stb.) [38]

A közlekedési rendszer, mint kritikus infrastruktúra védelme a kibertérből érkező, akár fizikai rendszereket és az autóipari és közlekedési kritikus információs infrastruktúrákat és a ráépülő szolgáltatásokat érintő támadások elleni védelmet kell megvalósítani. [38]

Az NHTSA (National Highway Traffic Safety Administration, USA) szerint a járművek kiber támadás ellenei védelmét többszintű védelmi megközelítés alapján mind a vezetékes mind pedig a vezeték nélküli belépési pontok esetében biztosítani kell.[9]

Az autonóm intelligens járművek esetében az autonómiát biztosító többféle intelligens járműrendszer pl.: adatbiztonsági szoftver, HMI, beágyazott modem, V2X, beavatkozók, beágyazott vezérlők, ultrahangos érzékelők, odometriai érzékelők, LIDAR, radar, kamerák működésének kiberbiztonsággal kapcsolatos kérdései még nem váltak általánosan kezelt iparági kérdéssé. Számos tanulmány foglalkozik az autonóm járművek szenzorjainak a megzavarásával. [39]

Az elektromos, elektronikus és programozható elektronikus biztonsági rendszerek járműipari kiber biztonsági integritási szintjét az ACSIL (Automotive Cybersecurity Integrity Level) értékekkel határozhatjuk meg.



2. ábra: Járműfedélzeti hálózatok kiberbiztonsági kérdései hagyományos felsőkategóriás járművek esetében [40]

3.2 Biztonság szemléletű autonóm intelligens járműtervezés

Magyarország élenjár az autonóm járművek tervezésében, kivitelezésében és tesztjében. Ugyanakkor még csak nem rég nyílt jogi lehetőség a fejlesztett járművek közúti tesztjére.

A közúti járművek műszaki megvizsgálásáról rendelet így fogalmaz: a 2. § (3b) bekezdés b) pontjában a „fejlesztési célú autonóm jármű: olyan fejlesztési célú jármű, amely részben vagy teljesen automatizált működések fejlesztésére szolgál, és amelyben a jármű vezetőjének minősülő tesztvezető tartózkodik, aki az automatizáltság szintjétől függően vagy bármely, a közlekedés biztonságát veszélyeztető helyzetben, a működés közben szükséges mértékben kézi irányítást gyakorol, illetve a kézi irányítást bármikor átveheti a jármű felett”. [41]

„A fejlesztési célú autonóm járművek közúton történő tesztelését végző járműfejlesztő akkor vehető nyilvántartásba, ha valamely tevékenységét az ISO 26262 szabvány szerint végzi, illetve valamely tevékenységre vonatkozó, folyamatban levő ISO 26262 szabvány szerinti tanúsítási folyamat részese, vagy az ISO 26262 szabvány tanúsítására feljogosított valamely tanúsító szervezet szakvéleménye alátámasztja az autonómjármű-technológia funkcionális biztonságára vonatkozó, a járműfejlesztőnél alkalmazott fejlesztési gyakorlat megfelelőségét. Amennyiben a fenti feltételek nem állnak fenn, a közlekedésért felelős miniszter a 2. § (3b) bekezdés b) pontjában meghatározott járművek tekintetében a nyilvántartásba vételt megtagadja, illetve az azokra vonatkozó adatokat törli a nyilvántartásból.” [41]

Kiberbiztonságra vonatkozóan a közúti járművek forgalomba helyezésének és forgalomban tartásának műszaki feltételeiről szóló rendelet a következőket írja elő:

„9.1. A járműfejlesztőnek biztosítania kell, hogy valamennyi fejlesztési célú autonóm jármű prototípus automatizált vezérlése és egyéb járműrendszere megfelelő beépített biztonsági szinttel rendelkezzen a jogosulatlan hozzáférésből adódó kockázat kezelése érdekében.

9.2. A járműfejlesztő az elvárható legjobb minőségben alkalmazza a biztonságkritikus járműipari rendszerek fejlesztésére vonatkozó szabványokat és technológiákat.” [42]

A járművek hálózatba kapcsolása olyan fenyegetéseket jelent, mint a termékbiztonság, az adatintegritás és adatbiztonság vagy akár az interoperabilitás. Az ISO 26262 szabvány szerint a közúti járművek elektronikus rendszerének funkcionális biztonságára vonatkozóan fellelhetőek szabályok és tervezési irányelvek. A szabvány második kiadása már megköveteli az interfészekre vonatkozó kiberbiztonsági eljárások alkalmazását. Viszont átfogó formalizált járműipari specifikus kiberbiztonsági szabványokkal még nem rendelkezik ez a szakterület.

A ISO esetében a vonatkozó kiberbiztonsági szabvány javaslati szakaszban van SAE szabvány pedig kidolgozás alatt áll, de a kapcsolódó javasolt jó gyakorlat (SAE J3061™ - Cybersecurity Guidebook for Cyber-physical Vehicle Systems) első kiadása 2016 januárjában megtörtént. Természetesen további szabványok is befolyásolják az autóipari fejlesztéseket a kiberbiztonsági tervezési folyamat szempontjából, ilyen általános IT biztonsági szabványok (ISO 27001, ISO 15408) vagy a speciális biztonsági szabvány V2X kommunikációhoz (IEEE 1609.2, ETSI TR 102 638 V1.1.1).

A tématerület kiforratlansága miatt szükség van az autóipari kiberbiztonsági tervezési eljárás kifejlesztésére a kapcsolódó szabványok és jó gyakorlatok alapján (SEA - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061). A kiberbiztonsági tervezési folyamatnak illeszkednie kell a funkcionális biztonság és minőségi folyamatok meglévő rendszeréhez és a megfelelő szakértelemmel rendelkezők számára végrehajthatónak kell lennie a biztonsági tevékenységnek.

A fejlesztési folyamat során nem csak a funkcionális biztonság létrehozását, hanem a kiberbiztonság megvalósítását is szem előtt kell tartani. Az IEC 62443

definiál négy biztonsági szintet, amely minőségi mutatókat, készségeket és erőfeszítés szinteket határoz meg a sikeres rendszertámadáshoz. A járművek kibertámadhatóságához szükséges erőforrások számbavételét kockázatelemzés útján el kell végezni és eredményeit implementálni kell a fejlesztési folyamatba.

A kockázatelemzés és kockázatértékelés segítségével olyan fejlesztési biztonsági koncepciót és követelmény előírást kell létrehozni, amely már rendszerterv szintjén foglalkozik a mélységi védelem kialakításával és a védelmi megoldásokat egymásra épülő rétegekként határozza meg. [43]

A 3. ábrán láthatjuk a járművek funkcionális és kiberbiztonság szempontú tervezési folyamatát. A kiberbiztonságnak a fejlesztési folyamatban nem csak egy hozzáadott elemnek kell lennie, hanem a tervezési folyamat szerves részét kell, hogy képezze egészen a koncepció fázisától, a gyártás, üzemeltetés, szervizelés és rendszer leszereléséig. Ez jelenti azt, hogy a kiberbiztonságot a járművek teljes életciklus alatt folyamatosan fent kell tartani. [22]

3. ábra: Járművek funkcionális és kiberbiztonság szempontú tervezési folyamata [43] [44] (saját szerkesztés)

4 Összegzés

Cikkünkben az elektromos, elektronikus és programozható biztonságkritikus rendszerek funkcionális biztonsági és kiberbiztonsági szempontú tervezésének elveit mutattuk be az okos mobilitási rendszer létrehozásának útján. A kiberbiztonság kapcsán fontos szempont, hogy az adott biztonsági szint csak időben korlátozott ideig tartható fent, hiszen a kibertámadások eszközrendszere folyamatosan változik. Viszont egy megvásárolt jármű esetében ma nagyon kevés esetben tudjuk elképzelni azt, hogy este a garázsban biztonsági javításokat telepítsen az autonóm intelligens járművünk. Cohen szerint az okos város egyik fő építőeleme az okos mobilitás, cikkünkben ennek az újszerű mobilitási rendszernek a tervezését tárgyaltuk. Kutatásunk szerint az okos mobilitás két pillére az autonóm intelligens járművek, járműrendszerek illetve az intelligens közlekedési infrastruktúra. Az okos mobilitás kialakításának szükségessége az kooperatív intelligens közlekedési rendszerek létrehozásának motivációban gyökerezik. Ezek a tényezők a produktivitás növelése (pl.: szállítási kapacitás növelése), a kevesebb baleset és a károsanyag-kibocsátás csökkentése akár a városi közlekedésben is. Az okos városi közlekedés kialakítása lényegében egy továbbfejlesztett ITS rendszerként kell elképzelni. Az okos város mobilitás marketingének a lényege, hogy olyan plusz szolgáltatásokat nyújtson, mint amit a hagyományos rendszerek nem. Cikkünkben számos okos mobilitási szolgáltatást predesztináltunk. Az autonóm intelligens járművek terjedése időszerű (robotok, drónok, önvezető autók) az össztársadalmi előnyösségük végett. A mai korszerű robotrendszerek, ilyenek az önvezető autók is már képesek egymás követése útján a konvojban haladásra vagy akár egy kitűzött cél önálló elérésére. A járművek közötti kommunikáción kívül a V2X (Vehicle-to-everything) kommunikáció segíti a okos város létrehozását. A járművek funkcionális, működési biztonsága már régóta kutatott terület viszont mára már a fizikai infrastruktúra a járművek fizikai rendszerei mellett egyre hangsúlyosabb szerep jut a kiber-fizikai komplex rendszereknek. Az autóipari fejlesztések kiberbiztonság szempontú megközelítése új és fejlődő terület.

A járművek és jármű rendszerek biztonságának fontos része a gyártók, szervizelők és a járművet használók, a jármű működésének résztvevőinek az adott életciklusi fázishoz tartozó biztonságmenedzsment tevékenységének megvalósítása, mivel a járművek és járműrendszerek biztonságorientált alkalmazása ma már nem csak a tervező feladata. Ahogy a hagyományos járművek vezetői felelősek járművük biztonságáért úgy az autonóm járművek üzemeltetését végzőknek a kibertér autóipart érintő veszélyeire, valamint a járművek és járműrendszerek kiberbiztonságára is figyelemmel kell lenniük a jövőben.

Összegzésképpen a járművek fejlesztésének kiberbiztonsági elvei szerint a mindennemű kommunikáció védelmére, az érzékelők, a működést befolyásoló mikrokontrollerek és mikroprocesszorok védelmére, és a lehetséges folyamatosan változó fenyegetések enyhítésére kell törekedni az autóipari fejlesztések során. [45] A mesterséges intelligencia alkalmazása - a kognitív mobilitási platform kialakítása vagy éppen a tudás alapú kritikus vezetési funkciók megvalósítása a végponttól végpontig terjedő mély tanulás segítségével - a járművek és járműrendszerek biztonságának új dimenzióját jelenti. [46]

Köszönetnyilvánítás

A cikk kutatásaihoz az Új Széchenyi Terv keretein belül az EFOP-3.6.2-16-2017-00016 számú projekt biztosított forrást. A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.

Irodalomjegyzék

[1] WHO. (2015). WHO fact sheet on road traffic injuries. http://www.who.int/violence_injury_prevention/road_safety_status/2015/magnitude_A4_web.pdf?ua=1. Letöltve: 2018.05.20.

[2] Hamada, Y., et al. (2018). Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks. SAE Int. J. Transp. Cybersecurity Priv., 1(1), 39–56.

[3] Dürrwang, J. et al. (2017). Security Hardening with Plausibility Checks for Automotive ECUs. Icwmc 2017, 38–41.

[4] Continental Co. (2018) Vehicle Control Units in commercial vehicles.

[5] HNTB. (2018). Connected and Automated Vehicles. http://www.hntb.com/Newsroom/Media-Kits/Intelligent-Transportation-Systems. Letöltve: 2018.05.05

[6] HNTB. (2018). The Road to Autonomous Vehicles - 2018.

[7] SAE. (2018). Surface Vehicle Recommended Practice J3016TM, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. 35.

[8] United Nations. (2016). Proposal for draft guidelines on cyber security and data protection. 1–5.

[9] NHTSA. (2018) Automated Vehicles for Safety. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety. Letöltve: 04-Apr-2018.04.04.

[10] Európai Parlament és a Tanács. (2015). Az Európai Parlament és a Tanács (EU) 2015/758 rendelete (2015. április 29.) a 112-es egységes európai segélyhívó szolgáltatáson alapuló fedélzeti e-segélyhívó rendszer kiépítésével összefüggő típus-jóváhagyási követelményekről és a 2007/46/EK irányelv. Az Európai Unió Hivatalos Lapja.

[11] E. S. Hunyor. (2018). Alapfelszereltség lesz az autókban a vészhívó. https://www.hirado.hu/belfold/gazdasag/cikk/2018/05/03/alapfelszereltseg-lesz-az-autokban-a-veszhivo/#. Letöltve: 2018.05.20.

[12] Outay, F. et al. (2017).ConVeh: Driving Safely into a Connected Future. Procedia Comput. Sci., 113, 460–465,

[13] Dey, K. C. et al. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation. Transp. Res. Part C Emerg. Technol., 68, 168–184.

[14] Gheorghiu, R. A. et al. (2018) Messaging capabilities of V2I networks. Procedia Manuf., 22, 476–484.

[15] Ericsson. (2018). Connected Vehicle Cloud - Under The Hood. https://archive.ericsson.net/service/internet/picov/get?DocNo=28701-FGD101192. Letöltve: 2018.04.08.

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

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

[18] Delgrossi, L. and Zhang, T. (2012). Vehicle Safety Communications. Veh. Saf. Commun.

[19] Connected car. https://en.wikipedia.org/wiki/Connected_car#cite_note-1. Letöltve: 2018.04.18.

[20] Turc, T. et. al. (2017). Web-based Wireless Sensor System for SCADA Environment. Procedia Eng., 181, 546–551.

[21] Federal Ministry of Transport and Digital Infrastructure. (2017). Action plan automated and connected driving.

[22] Mester, Gy. (2018) Autonóm önvezető robot autók. (kézirat)

[23] European Committee for Electrotechnical Standardization. EN 50126-2:2017. European Committee for Electrotechnical Standardization, Brussels, p. 79, 2017.

[24] Schuster Gy. and Terpecz, G. (2011). Járműiparban gyakran alkalmazott fedélzeti buszok," Repüléstudományi közlemények, 23(2).

[25] Fodor, D. és Szalay, Zs. (2014). Autóipari kommunikációs rendszerek. Pannon Egyetem.

[26] Dobrilovic, D. et al. (2016). A method for comparing and analyzing wireless security situations in two capital cities. Acta Polytech. Hungarica, 13(6), 67–86.

[27] Tokody, D. et al. (2017). Autonóm intelligens járművek helyzete Európában. Köztes Európa Társadalomtudományi Folyóirat A VIKEK Közleményei, 1–2(19–20),199–206.

[28] Schuster, Gy. et al. (2017). Software Reliability of Complex Systems Focus for Intelligent Vehicles. Lecture Notes in Mechanical Engineering (LNME) - Vehicle and Automotive Engineering, K. Jármai and B. Bolló, Eds. Miskolc: Springer Heidelberg, 309–321.

[29] Tokody, D. et al. (2017). An overview of autonomous intelligent vehicle systems. Lecture Notes in Mechanical Engineering (LNME) - Vehicle and Automotive Engineering, K. Jármai and B. Bolló, Eds. Miskolc: Springer Heidelberg, 287–307.

[30] Deloitte GmbH. (2017). Automotive Software Quality What do OEM's have to consider for the future?, 8, 14.

[31] Abonyi J,. és Fülep, T. (2014) Chapter 3 - Safety critical systems. http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch03.html. Letöltve: 2018.05.18.

[32] Muha, L. (2004). Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szle., 17(4), 137–156.

[33] Pető, R. (2012). Gépjárművek ballisztikai védelme. Hadmérnök, 7(1), 32–39.

[34] Iantovics, L. B. et al. (2017). MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents. Cogn. Syst. Res., 45, 17–29.

[35] Kassai, K. (2012). Kiberveszély és a magyar honvédség. Hadmérnök, 7(4), 128–141.

[36] Parkinson, S. et al. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Trans. Intell. Transp. Syst., 18(11), 2898–2915.

[37] Hashem Eiza, M. és Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Veh. Technol. Mag., 12(2),45–51.

[38] Beláz, A. és Berzsenyi, D. (2017). Kiberbiztonsági Stratégia 2.0 - A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 1-15.

[39] Petit, J. et al. (2015). Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Black Hat Europe, 1–13.

[40] United States Government Accountability Office. (2016) Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack.

[41] 5/1990. (IV. 12.) KöHÉM rendelet, a közúti járművek műszaki megvizsgálásáról. http://njt.hu/cgi_bin/njt_doc.cgi?docid=12356.351598. Letöltve: 2018.06.06.

[42] 6/1990. (IV. 12.) KöHÉM rendelet, a közúti járművek forgalomba helyezésének és forgalomban tartásának műszaki feltételeiről." http://njt.hu/cgi_bin/njt_doc.cgi?docid=12392.351571. Letöltve: 2018.06.06.

[43] Wooderson, P. (2016). Automotive Cyber Security Testing. Presentation

[44] Schmittner, C. et al. (2016) Using SAE J3061 for automotive security requirement engineering. Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, 9923, 157-170. Springer, Cham

[45] Fachot, M. (2017). Protecting road vehicles from cyber attacks. IEC e-tech, https://iecetech.org/issue/2017-03/Protecting-road-vehicles-from-cyber-attacks. Letöltve: 2018.05.20.

[46] Federal Ministry of Transport and Digital Infrastructure. (2017) Report-Ethics-Commission. https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile. Letöltve: 2018.05.20.