Kiberbiztonság a járműiparban

Palkovics László

Innovációs és Technológiai Minisztérium, Budapest

Beérkezett: 2020. szeptember 18.; Elfogadva: 2020. október 27.

Összefoglalás

Jelen cikk célja a járműipar egyes területeit érintő kiberbiztonsági kockázatok vizsgálata. Fentiekkel összhangban a cikk első részében a járműipar kiberbiztonsági szempontból releváns területei kerülnek meghatározásra. Ezt követően megtörténik a 2018. évben rögzített járműipari kibertámadások kockázatalapú értékelő elemzése.

Kulcsszavak: járműipari kiberbiztonság, kibertámadások, sérülékenységek

Automotive Cybersecurity

László Palkovics

Ministry for Innovation and Technology, Budapest, Hungary

Summary

Nowadays, cybersecurity has a critical impact on our lives. The Internet has also got a substantial role in our days since many people are constantly connected to the Internet (e.g., through online social networks) *(Török et al. 2020a)*. Besides, numerous personal and individual devices are connected. The growing number of connected devices and cyberspace expansion make our lives easier. However, this affects our privacy, with the potential for unauthorized use of personal information. In summary, life in a networked world carries unknown dangers.

In the future, many new risk factors are expected to occur, which will significantly increase the level of cybersecurity threats. Examining the aspects of the automotive industry, we should mention the summary of Cheng et al., which explores the field's problems through novel theoretical solutions and related practical considerations. The book pays special attention to vehicle communication and networked systems. This book examines three main scientific directions for 5G-compliant vehicle-to-vehicle communication and cooperative vehicle control: modeling and testing capabilities for vehicle-to-vehicle communication, state-of-the-art technologies related to the physical layer, and MAC design procedures *(Cheng et al. 2019)*.

Cheng and colleagues *(Cheng et al. 2019)* examined the communication channels currently applied in the automotive industry or that are expected to be applied soon. Particular attention has been paid to examining the tasks and challenges that need to be addressed in order to support the spread of the connected transport systems in the future. The evaluation focused on the cooperation of connected vehicles. Their study also outlined the most important security risks and challenges associated with new communication solutions.

In the light of the above-mentioned considerations, it can be said that the emergence of connected and autonomous vehicles can make a significant contribution to the positive effects of cyberspace, but can also have a disadvantageous impact on the vulnerability of transport processes.

In line with this, it is important to examine and understand the vulnerabilities of connected and autonomous vehicles, the threats to vehicles. With this knowledge, automotive cybersecurity professionals' responsibility is to develop appropriate security functions and capabilities for connected and autonomous vehicles and transport systems. This enables the systems to detect, evaluate, and, if necessary, treat different attacks and malicious interventions.

Along with the above objectives, many research studies in the automotive segment have already focused on identifying cybersecurity assessment frameworks for motor vehicles. Among these, it is worth highlighting the projects "HEAling Vulnerabilities to ENhance Software Security and Safety" and "E-safety vehicle intrusion protected applications" *(Cheah et al. 2018)*.

Keywords: automotive cybersecurity, cyberattacks, vulnerabilities

Bevezetés

Napjainkban nem szükséges magyaráznunk, hogy a kiberbiztonság egyre fontosabbá válik életünkben. Az internet életünk nélkülözhetetlen része, többségünk folyamatosan csatlakozik az internethez (pl. online közösségi hálózatokon keresztül) *(Török et al. 2020a)*. Ezen felül egyre több személyesen, egyénileg használt eszközünk, berendezésünk csatlakozik a kibertérhez. Nyilvánvaló, hogy egyrészt a hálózatba kapcsolt eszközök növekvő száma és a kibertér bővülése megkönnyíti mindennapjainkat, a lehetőségek tárháza korlátlannak tűnik. Ez a megatrend egyértelműen jelentős hatékonyságjavulást eredményez számos kommunikációval kapcsolatos területen. Beszélhetünk az 5G-technológia megjelenéséről, amelyet Alzenad és munkatársai említettek *(Alzenad et al. 2018)*, a mesterséges intelligencia terjedéséről, amint azt Briand és munkatársai ismertetik *(Briand et al. 2007)*. Másrészt a kibertér folyamatos bővülése jelentős mértékben növeli az életünkbe történő illetéktelen behatolás, illetve a személyes élettér megsértésének valószínűségét. Mára ez mindannyiunk magánéletét érinti, magában hordozva a személyes adatok eltulajdonításának és jogosulatlan felhasználásának lehetőségét. Összefoglalásképpen elmondhatjuk, hogy a hálózatba kapcsolt világban az élet eddig ismeretlen veszélyeket hordoz magában. A jövőben számos ma még nem vizsgált kockázati tényezővel kell számolnunk, amelyek az átlagember életében is szignifikáns mértékben növelik a kiberbiztonsági fenyegetettség mértékét. A járműipari szempontokat vizsgálva meg kell említenünk a Cheng és társai által készített összefoglaló kötetet, mely a terület problémáit járja körbe az újszerű elméleti megoldások és a kapcsolódó gyakorlati megfontolások számbavételén keresztül. A könyv különös figyelmet fordít a járművek kommunikációjára és a hálózatba kapcsolt rendszerekre. Az említett könyv három fő tudományos irányt vizsgál az 5G-kompatibilis járművek közötti kommunikációval és a kooperatív járműirányítással kapcsolatban: a járművek közötti kommunikáció modellezését és vizsgálati lehetőségeit, a fizikai réteghez kapcsolódó korszerű technológiákat és a MAC-tervezéshez kapcsolódó eljárásokat *(Cheng et al. 2019)*

Cheng és kollégái *(Cheng et al. 2019)* azokat kommunikációs csatornákat vizsgálták, melyek jelenleg elterjedtek a járműiparban, illetve melyek elterjedése a közeli jövőben várható. Különös figyelmet szenteltek azon feladatok és kihívások vizsgálatára, melyek megoldása szükséges a jövő kommunikációs rendszereinek elterjedéséhez. Az elemző-értékelés kiterjedt a hálózatba kapcsolt járművek kooperációjára. Tanulmányukban ismertették az új kommunikációs technológiákkal kapcsolatos releváns biztonsági kockázatokat és kihívásokat is.

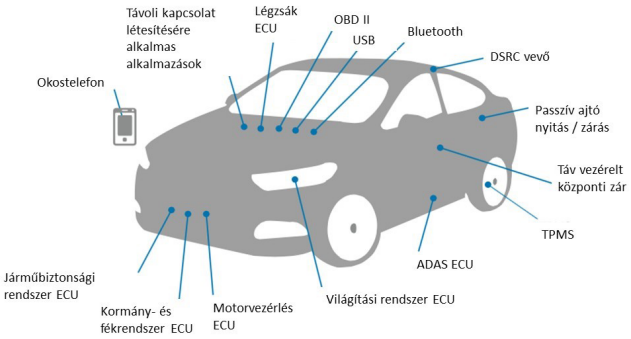
Fentiek tükrében elmondható, hogy a hálózatba kapcsolt és autonóm járművek megjelenése jelentős mértékben hozzájárulhat a kibertér pozitív hatásaihoz, ám rendkívül kedvezőtlenül befolyásolja a közlekedési folyamatok kibertámadásokkal szembeni sérülékenységét.

Ezzel összhangban fontos, hogy megvizsgáljuk és megértsük a hálózatba kapcsolt és autonóm járművek sérülékenységeit, a járműveket érintő fenyegetéseket. Ezek ismeretében a járműipari kiberbiztonság területén dolgozó szakemberek felelőssége, hogy megfelelő védelmi funkciókat és képességeket fejlesszenek a hálózatba kapcsolt és autonóm járművek, illetve közlekedési rendszerek számára. Ezáltal a rendszerek képessé válnak a rájuk irányuló támadások detektálására, elhárítására, vagy, ha szükséges, azok kezelésére.

Fenti célkitűzések mentén a járműpari szegmensben már számos kutatás irányult a gépjárművek kiberbiztonsági értékelési keretrendszerének azonosítására. Ezek közül is célszerű kiemelnünk a „HEAling Vulnerabilities to ENhance Software Security and Safety" (szoftveres járműbiztonsági és -védelmi sérülékenységek csökkentése) és az „E-safety vehicle intrusion protected applications" (behatolás biztos e-biztonsági járműipari alkalmazások) projekteket *(Cheah et al. 2018)*.

Közúti járművek

A közúti közlekedési rendszer biztonsági és védelmi jellemzőit jelentősen befolyásolja a járművek működési folyamatainak megbízhatósága. Tekintve, hogy napjaink autóiban számos alapvető működési folyamatot elektronikus vezérlőegységek irányítanak, egyre több és több mikroprocesszor kerül beépítésre a járművekbe, melyek fontos járműfunkciókat felügyelnek *(SAE, 2016)*. Egyes járműfenntartási műveletek esetében, mint amilyen például a szervíz-, a diagnosztikai és szoftverfrissítési folyamatok, legtöbbször még közvetlen kapcsolatot szükséges a jármű és az adott folyamatot irányító rendszer között. Az ilyen tevékenységek támogatását szolgálja az ember–gép interfész (HMI). A rövid hatótávolságú adatcserével, illetve érzékeléssel kapcsolatos folyamatokat helyi, vezeték nélküli kommunikációs (pl. Bluetooth, WiFi) egységek és több különféle érzékelő, például RADAR (Radio Detection and Ranging – rádiós észlelő és beméro), LIDAR (Light Detection and Ranging – lézeres észlelő és beméro), képérzékelő biztosíthatják. A nagy hatótávolságú hálózatok (például celluláris, vagy műholdas kapcsolat) hivatottak a távoleső objektumok közötti kommunikáció biztonságos megvalósítására. Abban az esetben, azonban amikor a gépjármű egészét, mint kiberbiztonsági rendszert tekintjük; a kommunikációért és a környezetérzékelésért felelős rendszerelemeken túl jelentős hangsúlyt kell helyezni az emberi tényezőre, illetve a kapcsolódó személyes adatokat és a kulcsadatbázisokat szintén kritikus tényezőknek kell tekintenünk. A SAE (Society of Automotive Engineers – Gépjárműmérnökök Társaság) által kiadott „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" *(SAE J3061)* (Kiberbiztonsági útmutató a kiber-fizikai járműrendszerekhez) ajánlásaival összhangban a modern járművek komplex



1. ábra | Járművek kiberbiztonságát befolyásoló kommunikációs és elektronikus modulok architektúrája

kommunikációját és elektronikus architektúráját az *1. ábra* szemlélteti. Hangsúlyozni kell azonban, hogy a hálózatba kapcsolt és önvezető járművek magas szintű architektúrája és a vonatkozó külső interfészek részletes leírása jelen vizsgálatnak nem képezi részét.

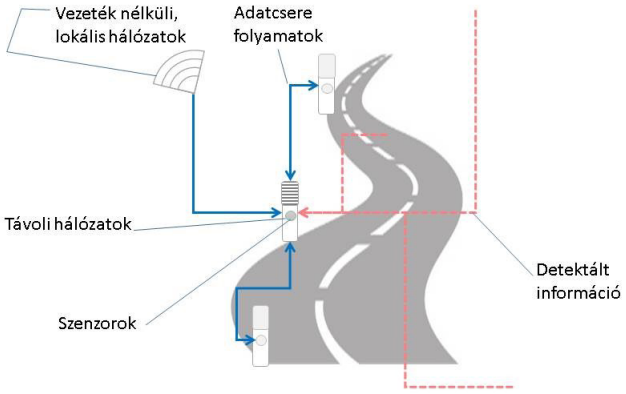
Közúti Infrastruktúra

Az elvégzett irodalomkutatás alapján elmondható, hogy a hálózatba kapcsolt járművek védelmi koncepciójának egyik leghatékonyabb eleme a sérülékenységek csökkentése. Ezt a célt jelentősen támogatja a komplex rendszer védelmét szolgáló intézkedések, mely fő célja a sérülékenységek számának és súlyosságának minimalizálása. A védelmi rendszerek folyamatos fejlesztésén és a legújabb támadási megoldásokhoz történő adaptálásán túl, rendkívül fontos feladat a releváns kibertámadások lehetséges és várható hatásainak megvizsgálása. Az autóipari vizsgálatok első fázisában célszerű a nyilvános forgalomtól elkülönítve végezni a demonstrációs célokat is szolgáló teszttámadásokat. A tesztek és vizsgálatok elvégzése céljából ésszerű olyan tesztpályát választani, mely alkalmas a különböző támadásszcenáriók megvalósítására, illetve ezzel összhangban a szükséges feladat-, illetve tesztteset-specifikus modulokkal van felszerelve. Fentiekkel összhangban autonóm és hálózatba kapcsolt járművek tesztelését szolgáló hazai a ZalaZONE tesztpálya *(Szalay et al. 2018)* már a fenti célokkal összhangban került kialakításra.

Ennek megfelelően a tesztpályának számos tesztmodulja van, melyek lehetőséget biztosítanak a különböző tesztesetek széleskörű vizsgálatára. Az új tesztpálya koncepcióját a legfontosabb magyar ipari szereplők és tudományos intézmények ajánlásainak megfelelően dolgozták ki.

Kiberbiztonsági szempontból célszerű megemlíteni, hogy a tesztpályán olyan aktív modulok érhetők el, melyek a jármű – jármű (V2V), illetve a jármű – infrastruktúra (V2I) kommunikáció megvalósításán és modellezésén keresztül közvetlenül alkalmasak egyes támadástípusok hatásainak vizsgálatára. Fentiekkel összhangban az intelligens forgalomirányítási rendszer, a V2I kommunikáció és az 5G celluláris kommunikációs rendszer egyedülálló lehetőséget kínál az önvezető és hálózatba kapcsolt közlekedési rendszerekre irányuló különböző támadások tesztelésére.

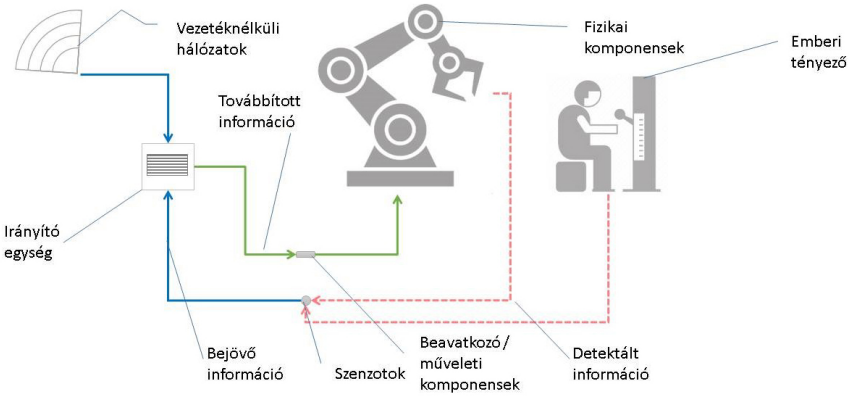
A közlekedési folyamat biztonságát jelentős mértékben befolyásolja a kiszolgáló intelligens infrastrukturális rendszerek (C-ITS) védelmi szintje. Hiszen ezek egyfelől lehetővé teszik a hálózatba kapcsolt és önvezető járművek közötti kommunikációt, illetve kapcsolatot teremtenek a járművek és az infrastruktúra különböző komponensei között (jelzőlámpák, út menti infrastruktúra elemei, és más úthasználók, pl. sérülékeny úthasználók között). Fentiekkel összhangban, a közúti infrastruktúra egyes szakaszait egyre gyakrabban érzékelőkkel és kommunikációs eszközökkel látják el. Ezáltal többek között lehetővé válik a közúti forgalmat és az egyéb úthasználókat jellemző adatok széleskörű gyűjtése, valamint az összegyűjtött információk megosztása a közlekedési folyamat szereplőivel. Az említett kommunikációs komponensek gyakran kapcsolódnak a kibertérhez, információt cserélnek egymással és más külső komponensekkel, mely számos kiberbiztonsági kérdést von maga után. A *2. ábra* az infrastruktúra kiberbiztonsági szempontból releváns elemeit szemlélteti.



2. ábra | A közúti infrastruktúra kiberbiztonsági szempontból releváns elemei (Forrás: Török et al. 2020b)

Járműgyártás

Az elvégzett irodalomkutatás alapján elmondható, hogy a hálózatba kapcsolt közlekedési rendszerek klasszikus értelemben vett működési tényezői és körülményei – például a hálózatba kapcsolt járművek kommunikációjának védelme, az alapvető közlekedési folyamatok integritásának biztosítása vagy megbízható hitelesítési módszerek alkalmazása – jelentősen befolyásolják a közúti közlekedés biztonságát. Fentieken túl, azonban indokoltnak tűnik a járműipari kiberbiztonság által lefedett terület kiterjesztése, összhangban járműfejlesztési és -gyártási folyamatokat meghatározó a termékéletciklus koncepcióval. Ennek megfelelően a kiberbiztonsággal kapcsolatos kérdéseket már a gyártási szakaszban el kell kezdeni vizsgálni. Emellett a gyártási folyamat vizsgálata



3. ábra | A gyártó rendszer kiberbiztonsági szempontból releváns elemei (Forrás: Török et al. 2020b).

során azt is célszerű figyelembe vennünk, hogy ebben a szakaszban az emberi munkaerő és gépi komponensek gyakran együttműködve felelősek a termékek előállításáért. Ezzel összhangban alapvető fontosságú a gyártási folyamat biztonságának és védettségének biztosítása. A gyártási folyamatot érintő támadások érkezhetnek a rendszeren belülről (ebben az esetben a rendszer kritikus sérülékenységét ismerő bennfentes személy szerepe hangsúlyos lehet). Emellett a rosszindulatú beavatkozás érkezhet a kibertérből, vagy irányulhat közvetlenül a rövid-hatótávolságú kommunikációs csatornákon továbbított üzenetek, illetve a szenzorrendszerek által érzékelt információk meghamisítására. *(Khalid et al. 2018)*.

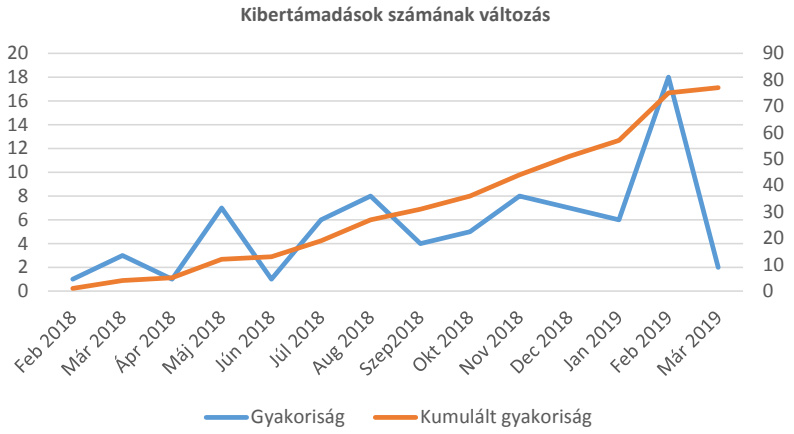
Normál működési mód esetén, a vezérlőközpont az emberi és gépi komponensektől érkező információk figyelembevételével, a rendszerelemek által érzékelt lokáció és dinamikai adatok alapján határozza meg a szükséges döntéseket, rendszerfolyamatokat. Ezen felül, azonban figyelembe kell vennünk, hogy a működő termelési program számos rendszer esetében elérhető (módosítható) a kibertérből. Fenitek tükrében, a védelmi rendszer tervezése és értékelése során, kiberbiztonsági szempontból figyelembe kell vennünk a fizikai komponensek rosszindulatú befolyásolását célzó beavatkozások kockázatát. A *3. ábra* a gyártási folyamat összetevőjét szemlélteti.

Járműipari kibertámadások és rosszindulatú beavatkozások statisztikái

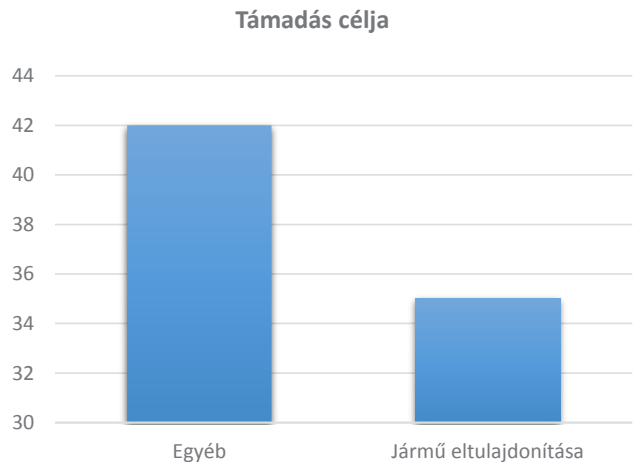
A következő részben az Upstream Security *(Upstream Security 2019)* által regisztrált és rögzített kibertámadások értékelő elemzését végzem el. Az Upstream Security folyamatosan gyűjti és regisztrálja a járműiparban történő kibertámadásokat; beleértve mind a tudományos folyóiratokban, mind a szaksajtóban megjelent és feltárt sérülékenységeket.

Fontos hangsúlyozni, hogy az adatbázis egy bizonyos típusú sérülékenységet egy támadásként kezel, még abban az esetben is, ha ugyanazt a sérülékenységet többször használták ki. Ez a járműipari elemzések esetén különösen fontos, hiszen egy modell sérülékenységének kihasználása pl. esetenként több száz jármű eltulajdonítását is eredményezheti.

A járműipari területén regisztrált rosszindulatú beavatkozások esetében megfigyelhetjük, hogy a támadások egy meghatározó része a járművek eltulajdonítására irányul. Jelen vizsgálat esetében azon elkövetéseket vizsgáljuk a járművek eltulajdonítását célzó beavatkozásokhoz kapcsolódóan, melyek megvalósítása valamely járműszenzorhoz, kommunikációs csatornához, vagy távirányítású járműmodulhoz (különös tekintettel a távirányítású központi zárra) köthető.



4. ábra | Rosszindulatú beavatkozások, támadások számának alakulása a járműipar területén



5. ábra | Rosszindulatú beavatkozások megoszlása a járműipar területén

Ennek fényében elmondható, hogy a fenti tárgykörbe sorolható járműeltulajdonítások a 2018. év februárja és a 2019. év februárja között megvalósított járműipari kibertámadások 1/3-át tették ki.

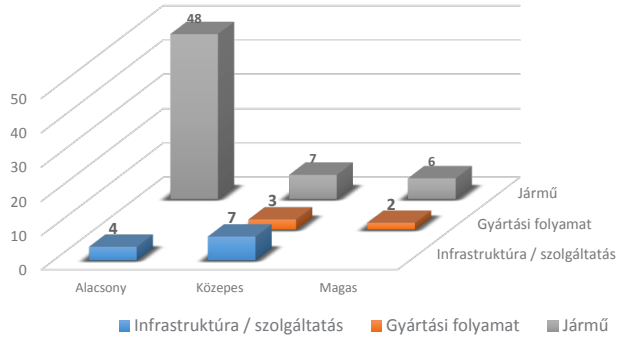
Az adatbázis átfogó értékelése céljából, megvizsgáltam a támadások és a rosszindulatú beavatkozások kockázati szintjének besorolását. Ennek eredményeként összehasonlítottam a járműipar területén végzett támadások súlyosságát és ez alapján azonosítottam a legfontosabb kockázati területeket.

A vizsgálat alapján elmondható, hogy a legtöbb rosszindulatú beavatkozás a járművekre irányul, és abszolút értékben ezen a területen valósult meg a legtöbb súlyos kockázattal jellemezhető beavatkozás is. Relatív értékeket vizsgálva azonban célszerű kiemelni a gyártási folyamatra irányuló támadásokat, tekintve, hogy az itt történő kisszámú beavatkozás mind közepes, vagy magas súlyosságú.

Összefoglalás

Összefoglalásként elmondhatjuk, hogy jelen cikkben elvégeztem a hálózatba kapcsolt és autonóm közlekedési rendszerek sérülékenységeinek, illetve a járműveket érintő fenyegetések vizsgálatát. Ezek alapján világossá vált, hogy a járműipari kiberbiztonság területén dolgozó szakemberek felelőssége a megfelelő védelmi funkciók és képességek kifejlesztése. Így a rendszerek képessé válhatnak a rájuk irányuló támadások detektálására, elhárítására, vagy, ha szükséges, azok kezelésére.

A vizsgálat során a komplex autonóm közlekedési rendszer egyes elemeit külön elemeztem; megkülönböztetve a járműre, az infrastruktúrára és a gyártási folyamatra irányuló rosszindulatú beavatkozásokat és várható hatásaikat.



6. ábra | Rosszindulatú beavatkozások, támadások súlyossága a járműipar területén

A vizsgálat alapján elmondható, hogy a legtöbb rosszindulatú beavatkozás a járművekre irányul, és abszolút értékben ezen a területen valósult meg a legtöbb súlyos kockázattal jellemezhető beavatkozás is. Relatív értékeket vizsgálva azonban célszerű kiemelni a gyártási folyamatra irányuló támadásokat, tekintve, hogy az itt történt kisszámú beavatkozás mind közepes, vagy magas súlyosságú.

Irodalomjegyzék

Alzenad, M., Shakir, M. Z., Yanikomeroglu, H., & Alouini, M. S. (2018) FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks. IEEE Communications Magazine, 56(1), 218–224.

Briand, L. C., Labiche, Y., and Liu, X., "Using machine learning to support debugging with tarantula," In Proceedings of the 18th IEEE International Symposium on Software Reliability, Washington DC, USA, 2007, pp. 137–146.

Cheng, X., Zhang, R., & Yang, L. (2019a) Wireless Toward the Era of Intelligent Vehicles. IEEE Internet of Things Journal, 6(1), 188–202.

Cheah, M., Shaikh, S. A., Bryans, J., & Wooderson, P. (2018) Building an automotive security assurance case using systematic security evaluations. Computers & Security, 77, 360–379.

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., & Pannek, J. (2018) Security framework for industrial collaborative robotic cyber-physical systems. Computers in Industry, 97, 132–145.

SAE Vehicle Electrical System Security Committee. (2016) SAE J3061-Cybersecurity Guidebook for Cyber-Physical Automotive Systems. SAE-Society of Automotive Engineers.

Szalay, Z., Tettamanti, T., Esztergár-Kiss, D., Varga, I., & Bartolini, C. (2018) Development of a Test Track for Driverless Cars: Vehicle Design, Track Configuration, and Liability Considerations. Periodica Polytechnica Transportation Engineering, 46(1), 29–35.

Török, Á., Szalay, Z., & Sághi, B. (2020a) Development of a Novel Automotive Cybersecurity, Integrity Level, Framework. Acta Polytechnica Hungarica, 17(1).

Török Á., Mohammed, O. and Dr. Szalay Zs. (2020b) Reconsidering the Cybersecurity Framework in the Automotive Industry. Acta Polytechnica Hungarica, 17(9).

Upstream Security, (2019) Upstream Security Global Automotive Cybersecurity Report 2019. https://www.upstream.auto/.