2025/5

2025.1.10.

A nemzetközi közjog értelmében jogi hatállyal kizárólag az ENSZ EGB eredeti szövegei rendelkeznek. Ennek az előírásnak a státusza és hatálybalépésének időpontja az ENSZ EGB TRANS/WP.29/343 sz. státuszdokumentumának legutóbbi változatában ellenőrizhető a következő weboldalon: https://unece.org/status-1958-agreement-and-annexed-regulations

155. számú ENSZ-előírás – Egységes rendelkezések a járműveknek a kiberbiztonság és a kiberbiztonsági irányítási rendszer tekintetében történő jóváhagyásáról [2025/5]

Tartalmaz minden érvényes szöveget a következő változatig bezárólag:

Az előírás eredeti változatának 3. kiegészítése – A hatálybalépés időpontja: 2025. január 10.

Ez a dokumentum kizárólag dokumentációs eszközként szolgál. A hiteles és jogilag kötelező érvényű szövegek a következők:

— ECE/TRANS/WP.29/2020/79 (az ECE/TRANS/WP.29/2020/94 és az ECE/TRANS/WP.29/2020/97 által módosítva)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 és

— ECE/TRANS/WP.29/2024/55

TARTALOMJEGYZÉK

Előírás

1. Alkalmazási kör
2. Fogalommeghatározások
3. Jóváhagyási kérelem
4. Jelölések
5. Jóváhagyás
6. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány
7. Követelmények
8. A járműtípus módosítása és a típusjóváhagyás kiterjesztése
9. A gyártás megfelelősége
10. Szankciók nem megfelelő gyártás esetén
11. A gyártás végleges leállítása
12. A jóváhagyási vizsgálat elvégzéséért felelős műszaki szolgálatok és a típusjóváhagyó hatóságok neve és címe

Mellékletek

1. Adatközlő lap
2. Értesítés
3. A jóváhagyási jel elrendezése
4. A kiberbiztonsági irányítási rendszer megfelelőségi tanúsítványának mintája
5. A fenyegetések és a megfelelő kockázatcsökkentő intézkedések jegyzéke

1. Alkalmazási kör

1.1. Ez az előírás a kiberbiztonság tekintetében alkalmazandó az L, az M, az N és az O kategóriájú járművekre, amennyiben rendelkeznek legalább egy elektronikus vezérlőegységgel.

1.2. Ez az előírás nem érinti az engedéllyel rendelkező feleknek a járműhöz, annak adataihoz, funkcióihoz és erőforrásaihoz való hozzáférését, valamint a hozzáférés feltételeit szabályozó egyéb ENSZ-előírásokat, illetve regionális vagy nemzeti jogszabályokat. Nem érinti továbbá a magánélet védelmére és a természetes személyeket a személyes adataik kezelése tekintetében megillető védelemre vonatkozó nemzeti és regionális jogszabályok alkalmazását.

1.3. Ez az előírás szintén nem érinti a fizikai és digitális cserealkatrészek és -alkotóelemek fejlesztését és telepítését/rendszerintegrálását a kiberbiztonság tekintetében szabályozó egyéb ENSZ-előírásokat, illetve nemzeti vagy regionális jogszabályokat.

2. Fogalommeghatározások

Ezen előírás alkalmazásában:

2.1. „járműtípus”: olyan járművek csoportja, amelyek legalább a következő lényeges jellemzők tekintetében nem különböznek egymástól:

a) a járműtípus gyártó által megadott megjelölése;

b) az elektromos/elektronikus architektúra és a külső interfészek alapvető kiberbiztonsági jellemzői;

2.2. „kiberbiztonság”: az az állapot, amelyben a közúti járművek és funkcióik védettek az elektromos vagy elektronikus alkotóelemeket érintő kiberfenyegetésekkel szemben;

2.3. „kiberbiztonsági irányítási rendszer (CSMS)”: olyan szisztematikus, kockázatalapú megközelítés, amely szervezeti folyamatokat, felelősségi köröket és irányítási intézkedéseket határoz meg a járműveket fenyegető kiberfenyegetésekhez kapcsolódó kockázatok kezelése és a járművek kibertámadásokkal szembeni védelme érdekében;

2.4. „rendszer”: alkotóelemek és/vagy alrendszerek olyan együttese, amely egy vagy több funkció megvalósítására szolgál;

2.5. „fejlesztési szakasz”: a járműtípus típusjóváhagyását megelőző időszak;

2.6. „gyártási szakasz”: a járműtípus gyártásának időtartama;

2.7. „gyártás utáni szakasz”: az az időszak, amely egy járműtípus gyártásának befejezésétől a járműtípushoz tartozó összes jármű élettartamának végéig tart. A meghatározott járműtípushoz tartozó járművek ebben a szakaszban továbbra is üzemben vannak, de már nem gyártják őket. A szakasz akkor ér véget, amikor az adott járműtípushoz tartozó egyetlen jármű sincs már üzemben;

2.8. „kockázatcsökkentő intézkedés”: a kockázatok csökkentésére szolgáló intézkedés;

2.9. „kockázat”: annak lehetősége, hogy egy adott fenyegetés a jármű sebezhetőségét kihasználva kárt okoz egy szervezetnek vagy egyénnek;

2.10. „kockázatértékelés”: az az átfogó folyamat, amely magában foglalja a kockázatok felkutatását, felismerését és leírását (a kockázatazonosítást) a kockázatok jellegének megértése és a kockázatok szintjének meghatározása (kockázatelemzés) érdekében, valamint a kockázatelemzés eredményeinek a kockázati kritériumokkal való összehasonlítását (a kockázatminősítést) annak megállapítása érdekében, hogy a kockázat és/vagy annak nagysága elfogadható vagy tolerálható-e;

2.11. „kockázatkezelés”: azon összehangolt tevékenységek, amelyek egy szervezetnek a kockázatok tekintetében történő irányítására és ellenőrzésére irányulnak;

2.12. „fenyegetés”: egy nem kívánt esemény lehetséges oka, amely kárt okozhat valamely rendszernek, szervezetnek vagy egyénnek;

2.13. „sebezhetőség”: valamely elem vagy kockázatcsökkentő intézkedés sérülékenysége, amelyet egy vagy több fenyegetés kihasználhat.

3. Jóváhagyási kérelem

3.1. A járműtípusnak a kiberbiztonság tekintetében történő jóváhagyására vonatkozó kérelmet a járműgyártó vagy megfelelően meghatalmazott képviselője nyújtja be.

3.2. A kérelemhez három példányban csatolni kell az alábbi dokumentumokat, és meg kell adni a következő adatokat:

3.2.1. A járműtípus leírása az ezen előírás 1. mellékletében meghatározott tételek tekintetében.

3.2.2. Amennyiben kiderül, hogy ezen adatok szellemitulajdon-jog tárgyát vagy a gyártó vagy annak beszállítója különleges know-how-jának részét képezik, a gyártónak vagy beszállítójának elegendő információt kell rendelkezésre bocsátania ahhoz, hogy az ezen előírásban meghatározott ellenőrzéseket megfelelően el lehessen végezni. Az ilyen adatokat bizalmasan kell kezelni.

3.2.3. Az ezen előírás 6. szakasza szerinti, a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány.

3.3. A dokumentációt a következő két részben kell rendelkezésre bocsátani:

a) a jóváhagyás céljából benyújtott hivatalos dokumentációcsomag, amely tartalmazza az 1. mellékletben meghatározott dokumentumokat, melyeket a típusjóváhagyási kérelem benyújtásakor kell a jóváhagyó hatóság vagy műszaki szolgálat rendelkezésére bocsátani. Ezt a dokumentációcsomagot a jóváhagyó hatóságnak vagy a műszaki szolgálatnak a jóváhagyási eljárás során alapvető referenciaként kell használnia. A jóváhagyó hatóságnak vagy a műszaki szolgálatnak gondoskodnia kell arról, hogy ez a dokumentációcsomag a járműtípus gyártásának végleges leállításától számított legalább 10 évig rendelkezésre álljon;

b) az ezen előírás követelményei szempontjából releváns egyéb dokumentumok, melyeket a gyártó megőrizhet, de amelyekbe a típusjóváhagyás alkalmával ellenőrzés céljából betekintést kell nyújtania. A gyártónak gondoskodnia kell arról, hogy minden olyan dokumentum, melybe a típusjóváhagyás időpontjában ellenőrzés céljából betekintést biztosított, a járműtípus gyártásának végleges leállításától számított legalább 10 évig rendelkezésre álljon.

4. Jelölések

4.1. Minden olyan járművön, amely megfelel egy ezen előírás szerint jóváhagyott járműtípusnak, a jóváhagyási értesítésben megadott, könnyen hozzáférhető helyen, jól látható módon fel kell tüntetni a következőkből álló nemzetközi jóváhagyási jelet:

4.1.1. egy kör, benne az „E” betű és a jóváhagyó ország egyedi azonosító száma;

4.1.2. ezen előírás száma, amelyet egy „R” betű, egy kötőjel és a jóváhagyási szám követ a fenti 4.1.1. szakaszban előírt kör jobb oldalán.

4.2. Ha a jármű megfelel a megállapodáshoz mellékelt egy vagy több további előírás szerint egy abban az országban jóváhagyott járműtípusnak, amely ezen előírás alapján megadta a jóváhagyást, akkor a fenti 4.1.1. szakaszban előírt jelet nem szükséges megismételni. Ilyen esetben az előírások számát, a jóváhagyási számokat, valamint az összes olyan előírás kiegészítő jelét, amelyek szerint a jóváhagyást megadták ugyanabban az országban, amely ezen előírás alapján is megadta a jóváhagyást, a fenti 4.1.1. szakaszban előírt jel jobb oldalán egymás alatt kell feltüntetni.

4.3. A jóváhagyási jelnek jól olvashatónak és eltávolíthatatlannak kell lennie.

4.4. A jóváhagyási jelet a gyártó által a járműre szerelt adattáblán vagy annak közelében kell elhelyezni.

4.5. Ezen előírás 3. mellékletében példák találhatók a jóváhagyási jel elrendezésére.

5. Jóváhagyás

5.1. A jóváhagyó hatóságok az adott esetnek megfelelően csak olyan járműtípusokra adhatnak típusjóváhagyást a kiberbiztonság tekintetében, amelyek megfelelnek ezen előírás követelményeinek.

5.1.1. A jóváhagyó hatóságnak vagy a műszaki szolgálatnak a dokumentumok vizsgálatával ellenőriznie kell, hogy a jármű gyártója megtette-e a járműtípus vonatkozásában szükséges intézkedéseket a következők biztosítása érdekében:

a) az ezen előírásban meghatározott információk összegyűjtése és ellenőrzése a szállítói láncon keresztül annak bizonyítása érdekében, hogy a beszállítókkal kapcsolatos kockázatok azonosítása és kezelése biztosítva van;

b) a (fejlesztési szakaszban vagy visszamenőlegesen elvégzett) kockázatértékelés, a vizsgálati eredmények és a járműtípus esetében alkalmazott kockázatcsökkentő intézkedések dokumentálása, beleértve a kockázatértékelést alátámasztó tervezési információkat is;

c) megfelelő kiberbiztonsági intézkedések alkalmazása a járműtípus tervezése során;

d) az esetleges kiberbiztonsági támadások észlelése és reagálás azokra;

e) a kibertámadások észlelését elősegítő naplóadatok rögzítése, valamint a megkísérelt vagy sikeres kibertámadások vizsgálatát lehetővé tévő kriminalisztikai adatelemzési képesség biztosítása.

5.1.2. A jóváhagyó hatóságnak vagy a műszaki szolgálatnak a járműtípusba tartozó jármű vizsgálatával ellenőriznie kell, hogy a jármű gyártója alkalmazta-e a dokumentált kiberbiztonsági intézkedéseket. A vizsgálatokat a jóváhagyó hatóságnak vagy a műszaki szolgálatnak önállóan vagy a jármű gyártójával együttműködve, mintavétel útján kell elvégeznie. A mintavételnek a kockázatértékelés során magasnak értékelt kockázatokra kell összpontosítania, de nem korlátozódhat kizárólag azokra.

5.1.3. Ha a jármű gyártója a 7.3. szakaszban említett követelmények közül egyet vagy többet nem teljesített, a jóváhagyó hatóságnak vagy a műszaki szolgálatnak el kell utasítania a típusjóváhagyás megadását a kiberbiztonság tekintetében, különösen az alábbi esetekben:

a) a jármű gyártója nem végezte el a 7.3.3. szakaszban említett átfogó kockázatértékelést; beleértve azt az esetet is, ha a gyártó nem vette figyelembe az 5. melléklet A. részében említett fenyegetésekhez kapcsolódó valamennyi kockázatot;

b) a jármű gyártója nem biztosította a járműtípus védelmét a gyártói kockázatértékelésében azonosított kockázatokkal szemben, vagy nem alkalmazta a 7. szakaszban előírt arányos kockázatcsökkentő intézkedéseket;

c) a jármű gyártója nem hozott megfelelő és arányos intézkedéseket annak érdekében, hogy (adott esetben) az utópiaci szoftverek, szolgáltatások, alkalmazások vagy adatok tárolására és használatára erre a célra kialakított környezeteket biztosítson a járműtípuson;

d) a jármű gyártója a jóváhagyást megelőzően nem végzett megfelelő és elégséges vizsgálatot az alkalmazott biztonsági intézkedések hatékonyságának ellenőrzésére.

5.1.4. Az értékelést végző jóváhagyó hatóságnak abban az esetben is el kell utasítania a típusjóváhagyás megadását a kiberbiztonság tekintetében, ha a jóváhagyó hatóság vagy a műszaki szolgálat nem kapott elegendő információt a jármű gyártójától a járműtípus kiberbiztonságának értékeléséhez.

5.2. Egy járműtípusnak az ezen előírás szerinti jóváhagyásáról, illetve a jóváhagyás kiterjesztéséről vagy elutasításáról értesíteni kell az 1958. évi megállapodásban részes és ezen előírást alkalmazó feleket az ezen előírás 2. mellékletében található mintának megfelelő formanyomtatványon.

5.3. A jóváhagyó hatóságok nem adhatnak típusjóváhagyást annak ellenőrzése nélkül, hogy a gyártó megfelelő intézkedéseket és eljárásokat vezetett-e be az ezen előírás hatálya alá tartozó kiberbiztonsági szempontok megfelelő kezelésére.

5.3.1. A jóváhagyó hatóságnak és a műszaki szolgálatnak az 1958. évi megállapodás 2. jegyzékében megállapított kritériumok teljesítésén túlmenően biztosítaniuk kell, hogy:

a) kompetens, megfelelő kiberbiztonsági készségekkel és speciális gépjármű-kockázatértékelési ismeretekkel ([1]) bíró személyzettel rendelkeznek;

b) eljárásokat vezettek be az ezen előírás szerinti értékelés egységessége érdekében.

5.3.2. Az ezen előírást alkalmazó valamennyi szerződő félnek a jóváhagyó hatóságán keresztül értesítenie és tájékoztatnia kell az ezen ENSZ-előírást alkalmazó többi szerződő fél jóváhagyó hatóságát azokról a módszerekről és kritériumokról, amelyeket az értesítést küldő hatóság alapul vett az ezen előírással és különösen az 5.1., a 7.2. és a 7.3. szakaszokkal összhangban hozott intézkedések megfelelőségének értékeléséhez.

Ezeket az információkat a következő alkalmakkor kell megosztani: a) az ezen előírás szerinti jóváhagyás első megadása előtt; b) minden alkalommal, amikor az értékelés módszereit vagy kritériumait aktualizálják.

Ezeket az információkat a legjobb gyakorlatok összegyűjtése és elemzése céljából, valamint annak érdekében kell megosztani, hogy az ezen előírást alkalmazó valamennyi jóváhagyó hatóság egységesen alkalmazhassa ezen előírás rendelkezéseit.

5.3.3. Az 5.3.2. szakaszban említett információkat angol nyelven fel kell tölteni az Egyesült Nemzetek Európai Gazdasági Bizottsága által létrehozott „DETA” biztonságos internetes adatbázisba ([2]), kellő időben, de legkésőbb 14 nappal az érintett értékelési módszerek és kritériumok szerinti első jóváhagyás megadása előtt. Elégséges információt kell biztosítani annak megértéséhez, hogy a jóváhagyó hatóság milyen minimális teljesítményszinteket fogadott el az 5.3.2. szakaszban említett egyes követelmények tekintetében, és hogy milyen eljárásokat és intézkedéseket alkalmaz e minimális teljesítményszintek teljesülésének ellenőrzésére ([3]).

5.3.4. Az 5.3.2. szakaszban említett információkat fogadó jóváhagyó hatóságok észrevételeket nyújthatnak be az értesítést küldő jóváhagyó hatóságnak az értesítés napjától számított 14 napon belül, észrevételeiknek a DETA-ba történő feltöltése útján.

5.3.5. Amennyiben a típusjóváhagyás megadásáért felelős jóváhagyó hatóság nem tudja figyelembe venni az 5.3.4. szakasz szerint kapott észrevételeket, az észrevételeket küldő jóváhagyó hatóságoknak és a típusjóváhagyás megadásáért felelős jóváhagyó hatóságnak az 1958. évi megállapodás 6. jegyzékével összhangban kell tisztázniuk az értelmezési kérdéseket. A Járműelőírások Harmonizálása Világfórum (WP.29) ezen előírás tekintetében illetékes kiegészítő munkacsoportjának ([4]) meg kell állapodnia az értékelési módszerek és kritériumok egységes értelmezéséről ([5]). Ezt az egységes értelmezést kell alkalmazni, és valamennyi jóváhagyó hatóságnak ennek megfelelően kell megadnia az ezen előírás szerinti típusjóváhagyásokat.

([1]) Lásd például a következő szabványokat: ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) A feltöltendő részletes információkra (pl. módszerek, kritériumok, teljesítményszintek) és a formátumra vonatkozó iránymutatást a kiberbiztonsági és vezeték nélküli szoftverfrissítési kérdésekkel foglalkozó munkacsoport által a GRVA hetedik ülésére összeállítandó értelmező dokumentum fogja tartalmazni.
([4]) Az automatizált/önvezető és a hálózatba kapcsolt járművekkel foglalkozó munkacsoport (GRVA).
([5]) Ezt az értelmezést az 5.3.3. szakasz lábjegyzetében említett értelmező dokumentumnak is tükröznie kell.

5.3.6. Az ezen előírás szerinti típusjóváhagyást megadó valamennyi jóváhagyó hatóságnak értesítenie kell a többi jóváhagyó hatóságot a jóváhagyás megadásáról. A jóváhagyó hatóságnak a jóváhagyás megadását követő 14 napon belül fel kell töltenie az angol nyelvű típusjóváhagyást és kiegészítő dokumentációt a DETA adatbázisba ([6]).

5.3.7. A szerződő felek az 5.3.6. szakasz szerint feltöltött információk révén tanulmányozhatják a megadott jóváhagyásokat. Amennyiben a szerződő felek álláspontja eltér, azt az 1958. évi megállapodás 10. cikkével és 6. függelékével összhangban kell rendezni. A szerződő feleknek a Járműelőírások Harmonizálása Világfórum (WP.29) illetékes kiegészítő munkacsoportját is tájékoztatniuk kell az 1958. évi megállapodás 6. függeléke szerinti eltérő értelmezésekről. Az illetékes munkacsoportnak elő kell segítenie az eltérő álláspontok közös nevezőre hozását, és erről szükség esetén konzultálhat a WP.29-cel.

5.4. Ezen előírás 7.2. szakaszának alkalmazásában a gyártónak biztosítania kell az ezen előírás hatálya alá tartozó kiberbiztonsági szempontok érvényre juttatását.

6. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány

6.1. A szerződő feleknek ki kell jelölniük a gyártó értékelésének elvégzéséért és a kiberbiztonsági irányítási rendszer megfelelőségi tanúsítványának kiadásáért felelős jóváhagyó hatóságot.

6.2. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány iránti kérelmet a járműgyártó vagy megfelelően meghatalmazott képviselője nyújtja be.

6.3. A kérelemhez három példányban csatolni kell az alábbi dokumentumokat, és meg kell adni a következő adatokat:

6.3.1. a kiberbiztonsági irányítási rendszer leírását tartalmazó dokumentumok;

6.3.2. az 1. melléklet 1. függelékében meghatározott mintának megfelelő, aláírt nyilatkozat.

6.4. Az értékeléssel összefüggésben a gyártónak az 1. melléklet 1. függelékében meghatározott minta használatával nyilatkoznia kell arról, hogy bevezette és alkalmazza az ezen előírás szerinti valamennyi kiberbiztonsági követelménynek való megfeleléshez szükséges folyamatokat.

6.5. Amennyiben ez az értékelés kielégítő eredménnyel zárult, és a gyártó az 1. melléklet 1. függelékében meghatározott minta szerinti, aláírt nyilatkozata beérkezett, akkor a gyártó számára ki kell állítani az ezen előírás 4. melléklete szerinti, a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítványt (a továbbiakban: a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány).

6.6. A jóváhagyó hatóságnak vagy a műszaki szolgálatnak a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány kiállításához az ezen előírás 4. mellékletében meghatározott mintát kell használnia.

6.7. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány a kiállítás napjától számítva legfeljebb három évig érvényes, kivéve ha visszavonásra kerül.

6.8. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítványt kiállító jóváhagyó hatóság bármikor ellenőrizheti, hogy a tanúsítvány megadásának feltételei továbbra is teljesülnek-e. Ha az ezen előírásban meghatározott követelmények már nem teljesülnek, a jóváhagyó hatóságnak vissza kell vonnia a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítványt.

([6]) A dokumentációcsomagra vonatkozó minimumkövetelményekkel kapcsolatos további információkat a GRVA hetedik ülésén fogják kidolgozni.

6.9. A gyártónak tájékoztatnia kell a jóváhagyó hatóságot vagy a műszaki szolgálatot minden olyan változásról, amely befolyásolja a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány érvényességét. A gyártóval folytatott konzultációt követően a jóváhagyó hatóság vagy a műszaki szolgálat határoz arról, hogy szükség van-e új ellenőrzésekre.

6.10. Annak érdekében, hogy a jóváhagyó hatóság a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány érvényességi idejének lejárta előtt elvégezhesse az értékelést, a gyártónak megfelelő időben kérelmeznie kell a kiberbiztonsági irányítási rendszerre vonatkozó új megfelelőségi tanúsítvány kiadását vagy a meglévő megfelelőségi tanúsítvány meghosszabbítását. A jóváhagyó hatóságnak kedvező értékelés esetén ki kell állítania a kiberbiztonsági irányítási rendszerre vonatkozó új megfelelőségi tanúsítványt, vagy további három évre meg kell hosszabbítania a korábbi tanúsítvány érvényességét. A jóváhagyó hatóságnak ellenőriznie kell, hogy a kiberbiztonsági irányítási rendszer továbbra is megfelel-e ezen előírás követelményeinek. A jóváhagyó hatóságnak új tanúsítványt kell kiadnia abban az esetben, ha a jóváhagyó hatóság vagy a műszaki szolgálat módosításokról kapott értesítést, és azok újraértékelése kedvező eredménnyel zárult.

6.11. A kiberbiztonsági irányítási rendszerre vonatkozó gyártói megfelelőségi tanúsítvány lejártát vagy visszavonását azon járműtípusok tekintetében, amelyek az érintett kiberbiztonsági irányítási rendszerrel vannak felszerelve, a jóváhagyás 8. szakaszban említett módosításának kell tekinteni, amely a jóváhagyás visszavonásával is járhat, ha a jóváhagyás megadásának feltételei már nem teljesülnek.

7. Követelmények

7.1. Általános követelmények

7.1.1. Ezen előírás követelményei nem korlátozzák más ENSZ-előírások rendelkezéseit vagy követelményeit.

7.2. A kiberbiztonsági irányítási rendszerre vonatkozó követelmények

7.2.1. Az értékeléshez a jóváhagyó hatóságnak vagy a műszaki szolgálatnak ellenőriznie kell, hogy a jármű gyártója rendelkezik-e kiberbiztonsági irányítási rendszerrel, és ellenőriznie kell, hogy az megfelel-e ennek az előírásnak.

7.2.2. A kiberbiztonsági irányítási rendszernek ki kell terjednie a következő szempontokra:

7.2.2.1. A jármű gyártójának igazolnia kell a jóváhagyó hatóság vagy a műszaki szolgálat számára, hogy kiberbiztonsági irányítási rendszere lefedi a következő szakaszokat:

a) fejlesztési szakasz;

b) gyártási szakasz;

c) gyártási utáni szakasz.

7.2.2.2. A jármű gyártójának igazolnia kell, hogy a kiberbiztonsági irányítási rendszerén belül alkalmazott folyamatok keretében megfelelően figyelembe veszik a biztonsági szempontokat, beleértve az 5. mellékletben felsorolt kockázatokat és kockázatcsökkentő intézkedéseket is. Ezek közé tartoznak a következők:

a) a gyártó szervezetén belül a kiberbiztonsággal kapcsolatos kérdések kezelésére szolgáló folyamatok;

b) a járműtípusokat érintő kockázatok azonosítására szolgáló folyamatok. E folyamatok keretében figyelembe kell venni az 5. melléklet A. részében felsorolt fenyegetéseket és az egyéb releváns fenyegetéseket;

c) az azonosított kockázatok értékelésére, kategorizálására és kezelésére szolgáló folyamatok;

d) az azonosított kockázatok megfelelő kezelésének ellenőrzésére szolgáló folyamatok;

e) a járműtípus kiberbiztonságának vizsgálatára szolgáló folyamatok;

f) a kockázatértékelés aktualizálását biztosító folyamatok;

g) a járműtípusokat érintő kibertámadások, kiberfenyegetések és sebezhetőségek ellenőrzésére, észlelésére és az azokra való reagálásra szolgáló folyamatok, valamint az annak értékelésére szolgáló folyamatok, hogy az alkalmazott kiberbiztonsági intézkedések az újonnan azonosított kiberfenyegetések és sebezhetőségek fényében továbbra is hatékonyak-e.

h) a megkísérelt vagy sikeres kibertámadások elemzését elősegítő, releváns adatok biztosítására szolgáló folyamatok.

7.2.2.3. A jármű gyártójának igazolnia kell, hogy a saját kiberbiztonsági irányítási rendszerében alkalmazott folyamatok biztosítják, hogy a 7.2.2.2. szakasz c) pontjában és a 7.2.2.2. szakasz g) pontjában említett kategorizálás alapján a jármű gyártójának reakcióját igénylő kiberfenyegetések és sebezhetőségek észszerű időn belül mérséklődjenek.

7.2.2.4. A jármű gyártójának igazolnia kell, hogy a kiberbiztonsági irányítási rendszerében alkalmazott folyamatok biztosítják, hogy a 7.2.2.2. szakasz g) pontjában említett ellenőrzés folyamatos legyen. A nyomon követésnek:

a) az első nyilvántartásba vételt követően ki kell terjednie a járművekre;

b) magában kell foglalnia a kiberfenyegetéseknek, sérülékenységeknek és kibertámadásoknak a járműadatok és járműnaplók alapján való elemzésére és észlelésére vonatkozó képességet. Ennek a képességnek összhangban kell lennie az 1.3. szakaszban foglaltakkal, valamint a járműtulajdonosok és járművezetők magánélethez való jogával, különös tekintettel a hozzájárulásra.

7.2.2.5. A jármű gyártójának be kell mutatnia, hogy kiberbiztonsági irányítási rendszere hogyan fogja kezelni a szerződéses beszállítókkal, szolgáltatókkal vagy a gyártó alszervezeteivel kapcsolatban esetlegesen fennálló függőségeket a 7.2.2.2. szakasz követelményei tekintetében.

7.3. A járműtípusokra vonatkozó követelmények

7.3.1. A gyártónak a jóváhagyási eljárás tárgyát képező járműtípus tekintetében rendelkeznie kell a kiberbiztonsági irányítási rendszerre vonatkozó érvényes megfelelőségi tanúsítvánnyal. Az M, az N és az O kategóriájú járművek első alkalommal 2024. július 1-je előtt kiadott típusjóváhagyásai, valamint az L kategóriájú járművek első alkalommal 2029. július 1-je előtt kiadott típusjóváhagyásai és azok valamennyi kiterjesztése esetében azonban, ha a jármű gyártója igazolni tudja, hogy a járműtípust nem lehetett a kiberbiztonsági irányítási rendszerre vonatkozó követelményekkel összhangban kifejleszteni, akkor azt kell bizonyítania, hogy a kiberbiztonságot megfelelően figyelembe vették az érintett járműtípus fejlesztési szakaszában.

7.3.2. A jármű gyártójának a jóváhagyási eljárás tárgyát képező járműtípusra vonatkozóan azonosítania és kezelnie kell a beszállítókkal kapcsolatos kockázatokat.

7.3.3. A jármű gyártójának azonosítania kell a járműtípus kritikus elemeit, teljes körű kockázatértékelést kell végeznie a járműtípusra vonatkozóan, és megfelelően kell kezelnie az azonosított kockázatokat. A kockázatértékelésnek figyelembe kell vennie a járműtípus egyedi elemeit és az azok közötti kölcsönhatásokat. A kockázatértékelés keretében továbbá számításba kell venni a külső rendszerekkel fennálló kölcsönhatásokat is. A kockázatok értékelése során a jármű gyártójának tekintetbe kell vennie az 5. melléklet A. részében említett valamennyi fenyegetéshez kapcsolódó kockázatokat, valamint minden egyéb releváns kockázatot.

7.3.4. A jármű gyártójának védenie kell a járműtípust a gyártói kockázatértékelés során azonosított kockázatokkal szemben. A járműtípus védelme érdekében arányos kockázatcsökkentő intézkedéseket kell alkalmazni. Az alkalmazott kockázatcsökkentő intézkedéseknek magukban kell foglalniuk az 5. melléklet B. és C. részében említett valamennyi olyan kockázatcsökkentő intézkedést, amely az azonosított kockázatok szempontjából releváns. Ha azonban az 5. melléklet B. vagy C. részében említett kockázatcsökkentő intézkedés nem releváns vagy nem elégséges az azonosított kockázat tekintetében, a jármű gyártójának gondoskodnia kell egy másik, megfelelő kockázatcsökkentő intézkedés alkalmazásáról.

Különösen az M, az N és az O kategóriájú járművek első alkalommal 2024. július 1-je előtt kiadott típusjóváhagyásai, valamint az L kategóriájú járművek első alkalommal 2029. július 1-je előtt kiadott típusjóváhagyásai és azok valamennyi kiterjesztése esetében a járműgyártónak biztosítania kell, hogy egy másik, megfelelő kockázatcsökkentő intézkedést hajtsanak végre, ha az 5. melléklet B. vagy C. részében említett kockázatcsökkentő intézkedés műszakilag nem megvalósítható. A műszaki megvalósíthatóságra vonatkozó értékelést a gyártónak be kell nyújtania a jóváhagyó hatósághoz.

7.3.5. A jármű gyártójának megfelelő és arányos intézkedéseket kell hoznia annak érdekében, hogy (adott esetben) az utópiaci szoftverek, szolgáltatások, alkalmazások vagy adatok tárolásához és használatához erre a célra kialakított környezeteket biztosítson a járműtípuson.

7.3.6. A jármű gyártójának a típusjóváhagyást megelőzően megfelelő és elégséges vizsgálat elvégzésével ellenőriznie kell az alkalmazott biztonsági intézkedések hatékonyságát.

7.3.7. A jármű gyártójának intézkedéseket kell alkalmaznia a járműtípus vonatkozásában a következő célok megvalósítása érdekében:

a) a járműtípusba tartozó járművek elleni kibertámadások észlelése és megelőzése;

b) a járműgyártó ellenőrzési képességének támogatása a járműtípussal kapcsolatos fenyegetések, sebezhetőségek és kibertámadások észlelése tekintetében;

c) a megkísérelt vagy sikeres kibertámadások vizsgálatát lehetővé tévő kriminalisztikai adatelemzési képesség biztosítása.

7.3.8. Az ezen előírás alkalmazásában használt kriptográfiai moduloknak összhangban kell lenniük az egységesen elfogadott szabványokkal. Ha az alkalmazott kriptográfiai modulok nem felelnek meg az egységesen elfogadott szabványoknak, a jármű gyártójának meg kell indokolnia a használatukat.

7.4. A jelentéstételre vonatkozó követelmények

7.4.1. A jármű gyártójának évente legalább egyszer – vagy adott esetben ennél gyakrabban – jelentenie kell a jóváhagyó hatóságnak vagy a műszaki szolgálatnak a 7.2.2.2. szakasz g) pontjában meghatározott ellenőrzési tevékenységeinek eredményét, és e jelentésnek tartalmaznia kell az új kibertámadásokra vonatkozó releváns információkat is. A jármű gyártójának azt is jelentenie kell és meg kell erősítenie a jóváhagyó hatóság vagy a műszaki szolgálat számára, hogy a járműtípusaira alkalmazott kiberbiztonsági kockázatcsökkentő intézkedések továbbra is hatékonyak, valamint jelentenie kell minden egyéb meghozott intézkedést is.

7.4.2. A jóváhagyó hatóságnak vagy a műszaki szolgálatnak ellenőriznie kell a benyújtott információkat, és szükség esetén fel kell szólítania a jármű gyártóját, hogy orvosolja a hatékonysággal kapcsolatban észlelt esetleges hiányosságokat.

Ha a jelentés vagy válasz nem elégséges, a jóváhagyó hatóság úgy dönthet, hogy a 6.8. szakasznak megfelelően visszavonja a kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítványt.

8. A járműtípus módosítása és a típusjóváhagyás kiterjesztése

8.1. A járműtípus minden olyan módosításáról, amely a kiberbiztonság és/vagy az ezen előírásban előírt dokumentáció tekintetében befolyásolja a járműtípus műszaki teljesítményét, értesíteni kell a járműtípust jóváhagyó hatóságot. A jóváhagyó hatóság ezt követően a következőképpen járhat el:

8.1.1. úgy ítéli meg, hogy az elvégzett módosítások továbbra is megfelelnek a meglévő típusjóváhagyás követelményeinek és dokumentációjának; vagy

8.1.2. az 5. szakasszal összhangban elvégzi a szükséges kiegészítő értékelést, és adott esetben további vizsgálati jegyzőkönyv kiállítását kell kérnie a vizsgálatok elvégzéséért felelős műszaki szolgálattól.

8.1.3. A jóváhagyás megerősítéséről, kiterjesztéséről vagy elutasításáról, a módosítások részletes leírásával együtt, az ezen előírás 2. mellékletének megfelelő nyomtatványon kell értesítést küldeni. A jóváhagyást kiterjesztő jóváhagyó hatóságnak sorszámot kell rendelnie a kiterjesztéshez, és az ezen előírás 2. mellékletében szereplő mintának megfelelő nyomtatványon értesítenie kell erről az 1958. évi megállapodásban részes és ezen előírást alkalmazó többi felet.

9. A gyártás megfelelősége

9.1. A gyártásmegfelelőség ellenőrzésére szolgáló eljárásoknak meg kell felelniük az 1958. évi megállapodás 1. jegyzékében (E/ECE/TRANS/505/Rev.3) megállapított eljárásoknak, különösen pedig az alábbi követelményeknek:

9.1.1. a jóváhagyás jogosultjának gondoskodnia kell arról, hogy a gyártás megfelelőségére vonatkozó vizsgálatok eredményeit rögzítsék, és a mellékelt dokumentumok a jóváhagyó hatósággal vagy műszaki szolgálattal egyetértésben meghatározott ideig rendelkezésre álljanak. Ez az időtartam nem haladhatja meg a gyártás végleges leállításától számított tíz évet;

9.1.2. a típusjóváhagyást megadó hatóság bármikor ellenőrizheti az egyes gyártóüzemekben a gyártás megfelelőségének ellenőrzésére alkalmazott módszereket. Ilyen ellenőrzésekre általában háromévente kerül sor.

10. Szankciók nem megfelelő gyártás esetén

10.1. A járműtípus tekintetében az ezen előírás alapján megadott típusjóváhagyás visszavonható, ha az ezen előírásban megállapított követelmények nem teljesülnek, vagy ha a mintajárművek nem felelnek meg az ezen előírásban megállapított követelményeknek.

10.2. Ha a jóváhagyó hatóság visszavon egy előzőleg általa megadott jóváhagyást, erről haladéktalanul tájékoztatnia kell az ezen előírást alkalmazó szerződő feleket az ezen előírás 2. mellékletének megfelelő nyomtatványon.

11. A gyártás végleges leállítása

11.1. Ha a jóváhagyás jogosultja véglegesen leállítja az ezen előírás szerint jóváhagyott járműtípus gyártását, akkor erről értesítenie kell a jóváhagyást megadó hatóságot. A hatóságnak az értesítés kézhezvételét követően haladéktalanul tájékoztatnia kell a megállapodásban részes és ezen előírást alkalmazó többi szerződő felet a következők szerint: a jóváhagyási értesítés végén nagy betűkkel, aláírással és keltezéssel feltünteti a „PRODUCTION DISCONTINUED” („gyártás leállítása”) kifejezést.

12. A jóváhagyási vizsgálat elvégzéséért felelős műszaki szolgálatok és a típusjóváhagyó hatóságok neve és címe

12.1. A megállapodásban részes és ezen előírást alkalmazó szerződő felek megadják az Egyesült Nemzetek Titkárságának a jóváhagyási vizsgálatok elvégzéséért felelős műszaki szolgálatok nevét és címét, valamint a jóváhagyásokat megadó, illetve a más országok által kiadott jóváhagyásokat, kiterjesztéseket, elutasításokat vagy visszavonásokat igazoló értesítéseket fogadó típusjóváhagyó hatóság nevét és címét.

1. MELLÉKLET

Adatközlő lap

Az alábbi adatokat értelemszerűen, három példányban, tartalomjegyzékkel együtt kell benyújtani. A rajzokat megfelelő méretarányban és kellő részletességgel, A4-es formátumban vagy A4-es formátumra összehajtva kell benyújtani. A fényképeknek – amennyiben vannak – kellően részletesnek kell lenniük.

1. Gyártmány (a gyártó kereskedelmi neve): .....

2. Típus és általános kereskedelmi megnevezés(ek): .....

3. Típusazonosító jelölés, ha fel van tüntetve a járművön: .....

4. A jelölés helye: .....

5. A jármű kategóriája (kategóriái): .....

6. A gyártó / a gyártó képviselőjének neve és címe: .....

7. Az összeszerelő üzem(ek) neve és címe: .....

8. A jóváhagyandó járműtípust képviselő jármű fényképe(i) és/vagy rajza(i): .....

9. Kiberbiztonság

9.1. A járműtípus általános felépítésére vonatkozó jellemzők, beleértve a következőket:

a) a járműtípus kiberbiztonsága szempontjából releváns járműrendszerek;

b) a rendszerek kiberbiztonság szempontjából releváns alkotóelemei;

c) e rendszerek kölcsönhatásai a járműtípuson belüli más rendszerekkel és a külső interfészekkel.

9.2. A járműtípus sematikus ábrázolása

9.3. A kiberbiztonsági irányítási rendszer megfelelőségi tanúsítványának száma: .....

9.4. A jóváhagyandó járműtípusra vonatkozó dokumentumok, amelyek ismertetik a kockázatértékelés eredményét és az azonosított kockázatokat: .....

9.5. A jóváhagyandó járműtípusra vonatkozó dokumentumok, amelyek ismertetik a felsorolt rendszerek vagy a járműtípus tekintetében alkalmazott kockázatcsökkentő intézkedéseket, valamint azt, hogy ezek hogyan kezelik az említett kockázatokat: .....

9.6. A jóváhagyandó járműtípusra vonatkozó dokumentumok, amelyek bemutatják az utópiaci szoftverek, szolgáltatások, alkalmazások vagy adatok számára kialakított környezetek védelmét: .....

9.7. A jóváhagyandó járműtípusra vonatkozó dokumentumok, amelyek ismertetik, hogy milyen vizsgálatokat végeztek a járműtípus és rendszerei kiberbiztonságának ellenőrzésére, valamint bemutatják e vizsgálatok eredményét: .....

9.8. Annak ismertetése, hogy a kiberbiztonság szempontjából hogyan vették figyelembe az ellátási láncot: .....

1. melléklet – 1. függelék

A kiberbiztonsági irányítási rendszerre vonatkozó gyártói nyilatkozat mintája

A gyártó nyilatkozata a kiberbiztonsági irányítási rendszerre vonatkozó követelményeknek való megfelelésről

A gyártó neve: ……

A gyártó címe: ……

…… (*gyártó neve*)

tanúsítja, hogy a 155. számú ENSZ-előírás 7.2. szakaszában a kiberbiztonsági irányítási rendszerre vonatkozóan megállapított követelményeknek való megfeleléshez szükséges folyamatokat bevezette és azokat rendszeresen aktualizálni fogja.

Kelt: …… (*hely*)

Dátum: ……

Az aláíró neve: ……

Az aláíró beosztása: ……

(A gyártó képviselőjének pecsétje és aláírása)

2. MELLÉKLET

Értesítés

(legnagyobb formátum: A4 [210 × 297 mm])



Kibocsátó: Hatóság neve:
.....
.....
.....

Tárgy: (2) Jóváhagyás kiterjesztése
Jóváhagyás megadása Jóváhagyás visszavonása éééé/hh/nn-i hatállyal
Jóváhagyás elutasítása
A gyártás végleges leállítása

valamely járműtípus vonatkozásában, a 155. számú ENSZ-előírás alapján

Jóváhagyási szám: .....

Kiterjesztés száma: .....

A kiterjesztés indokolása: .....

1. Gyártmány (a gyártó kereskedelmi neve): .....

2. Típus és általános kereskedelmi megnevezés(ek): .....

3. Típusazonosító jelölés, ha fel van tüntetve a járművön: .....

3.1. A jelölés helye: .....

4. A jármű kategóriája (kategóriái): .....

5. A gyártó / a gyártó képviselőjének neve és címe: .....

6. A gyártóüzem(ek) neve és címe: .....

7. A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány száma: .....

8. A vizsgálatok elvégzéséért felelős műszaki szolgálat: .....

9. A vizsgálati jegyzőkönyv kelte: .....

10. A vizsgálati jegyzőkönyv száma: .....

11. Megjegyzések: (ha vannak). .....

12. Hely: .....

(1) A jóváhagyást megadó/kiterjesztő/elutasító/visszavonó ország azonosító száma (lásd az előírás jóváhagyásra vonatkozó rendelkezéseit).
(2) A nem kívánt rész törlendő.

13. Dátum: ……

14. Aláírás: ……

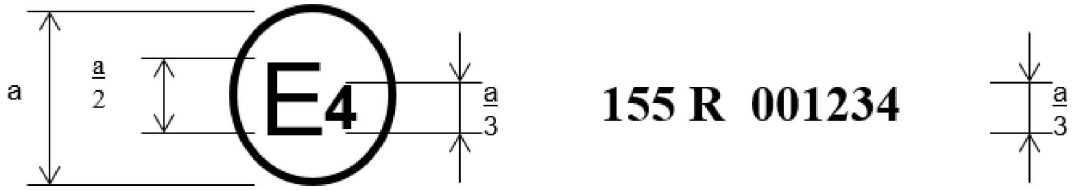
15. A jóváhagyó hatósághoz benyújtott – és kérésre kiadható – információs csomag tartalomjegyzéke mellékelve.

3. MELLÉKLET

A jóváhagyási jel elrendezése

A. MINTA

(lásd ezen előírás 4.2. szakaszát)



a = legalább 8 mm

A járművön elhelyezett fenti jóváhagyási jel azt mutatja, hogy az adott közúti járműtípust a 155. számú előírás szerint hagyták jóvá Hollandiában (E4), a 001234 jóváhagyási számon. A jóváhagyási szám első két számjegye (00) azt jelzi, hogy a jóváhagyást ezen előírás eredeti változatának követelményei alapján adták meg.

4. MELLÉKLET

A KIBERBIZTONSÁGI IRÁNYÍTÁSI RENDSZER MEGFELELŐSÉGI TANÚSÍTVÁNYÁNAK MINTÁJA

A kiberbiztonsági irányítási rendszerre vonatkozó megfelelőségi tanúsítvány

a 155. számú ENSZ-előírás alapján

A tanúsítvány száma [*hivatkozási szám*]

[…… *Jóváhagyó hatóság*]

igazolja, hogy

(gyártó) ……

(a gyártó címe) ……

megfelel a 155. számú előírás 7.2. szakaszában foglalt rendelkezéseknek

Az elvégzett vizsgálatok időpontja: ……

A vizsgálatokat végző jóváhagyó hatóság vagy műszaki szolgálat neve és címe: ……

A jelentés száma: ……

Ez a tanúsítvány …… [*dátum*]-ig érvényes

Kelt: […… *hely*]

[…… *dátum*]

[…… *aláírás*]

Mellékletek: a kiberbiztonsági irányítási rendszer gyártó által készített leírása.

5. MELLÉKLET

A fenyegetések és a megfelelő kockázatcsökkentő intézkedések jegyzéke

1. Ez a melléklet három részből áll. Az A. rész ismerteti az alapvető fenyegetéseket, sebezhetőségeket és támadási módszereket. A B. rész a járműveket érintő fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket mutatja be. A C. rész a járműveken kívüli, például informatikai back-end területeket érintő fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket írja le.

2. Az A., B. és C. részt figyelembe kell venni a járműgyártók által végrehajtandó kockázatértékelés és kockázatcsökkentő intézkedések során.

3. A sebezhetőségek fő kategóriái és a kapcsolódó példák az A. részben hivatkozási számmal vannak ellátva. Ugyanezen hivatkozási számok fel vannak tüntetve a B. és C. részben található táblázatokban is, összekapcsolva az egyes támadásokat/sebezhetőségeket a megfelelő kockázatcsökkentő intézkedésekkel.

4. A fenyegetések elemzése során figyelembe kell venni a támadások lehetséges hatásait is. Ezek segíthetnek a kockázat súlyosságának megállapításában és a további kockázatok azonosításában. A támadások lehetséges hatásai közé tartozhatnak a következők:

   a) a jármű biztonságos működésének befolyásolása;

   b) a jármű funkcióinak leállása;

   c) a szoftverek és azok teljesítményének módosítása;

   d) a szoftverek módosítása a működésre gyakorolt hatás nélkül;

   e) az adatok integritásának megsértése;

   f) az adatok titkosságának megsértése;

   g) az adatok rendelkezésre állásának káros befolyásolása;

   h) egyéb, beleértve a bűncselekményeket is.

A. RÉSZ

A fenyegetésekhez kapcsolódó sebezhetőségek vagy támadási módszerek

A fenyegetések fő kategóriáinak és a kapcsolódó sebezhetőségeknek, illetve támadási módszereknek a leírása az A1. táblázatban található.

A1. táblázat

A fenyegetésekhez kapcsolódó sebezhetőségek vagy támadási módszerek jegyzéke

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
4.3.1. A forgalomban lévő járművekhez kapcsolódó back-end szerverekkel kapcsolatos fenyegetések	1.	A back-end szerverek felhasználása a jármű elleni támadásra vagy adatok kinyerésére	1.1.	A személyzet visszaélése a jogosultságokkal (belső támadás)
			1.2.	Jogosulatlan internetes hozzáférés a szerverhez (például „hátsó ajtók” [backdoorok] révén, a rendszerszoftverek ki nem javított [unpatched] sérülékenységeinek kihasználásával, SQL-támadások vagy más eszközök segítségével)
			1.3.	Jogosulatlan fizikai hozzáférés a szerverhez (például USB-kulcsok vagy a szerverhez csatlakoztatott egyéb adathordozók révén)
	2.	A jármű működését befolyásoló fennakadás a back-end szerver által nyújtott szolgáltatásokban	2.1.	A back-end szerver elleni támadás miatt leáll a szerver működése, például nem tud kommunikálni a járművekkel és nem tudja biztosítani a járművek által igénybe vett szolgáltatásokat

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
	3.	A back-end szervereken tárolt, a járművekkel kapcsolatos adatok elvesztése vagy az azokhoz való illetéktelen hozzáférés („adatszivárgás”)	3.1.	A személyzet visszaélése a jogosultságokkal (belső támadás)
			3.2.	Információvesztés a felhőben. Ha az adatokat harmadik felek által szolgáltatott felhőben tárolják, támadás vagy baleset következtében érzékeny adatok veszhetnek el.
			3.3.	Jogosulatlan internetes hozzáférés a szerverhez (például „hátsó ajtók” [backdoorok] révén, a rendszerszoftverek ki nem javított [unpatched] sérülékenységeinek kihasználásával, SQL-támadások vagy más eszközök segítségével)
			3.4.	Jogosulatlan fizikai hozzáférés a szerverhez (például USB-kulcsok vagy a szerverhez csatlakoztatott egyéb adathordozók révén)
			3.5.	Információszivárgás nem szándékos adatmegosztás (pl. adminisztrációs hibák) miatt
4.3.2. A járműveket a kommunikációs csatornáik kapcsán érintő fenyegetések	4.	A jármű által fogadott üzenetek vagy adatok meghamisítása (spoofing)	4.1.	A személyazonosság meghamisítása révén az üzenetekkel kapcsolatban alkalmazott megtévesztés (spoofing) (pl. a V2X típusú [a járműtől más rendszerek felé irányuló] kommunikációban: a kooperatív tájékoztató [cooperative awareness, CAM] üzenetek vagy a manőverkoordinációs üzenetek, illetve a GNSS-üzenetek terén stb.)
			4.2.	Sybil-támadás (más járművek megtévesztése azt a látszatot keltve, mintha sok jármű lenne az úton)
	5.	A járművön tárolt kódok/adatok jogosulatlan manipulálása, törlése vagy egyéb módosítása a kommunikációs csatornákon keresztül	5.1.	A kommunikációs csatornák lehetővé teszik a rosszindulatú kóddal való fertőzést (code injection), például egy szoftver manipulált bináris állományai bejuttathatók a kommunikációs adatfolyamba
			5.2.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok manipulálását
			5.3.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok felülírását
			5.4.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok törlését
			5.5.	A kommunikációs csatornák lehetővé teszik adatok/kódok bevitelét a járműbe (adatok/kódok írása)
	6.	A kommunikációs csatornák lehetővé teszik nem megbízható/megbízhatatlan üzenetek elfogadását vagy a kommunikációs csatornák sebezhetők a munkamenet-eltérítésekkel (session hijacking) / visszajátszásos támadásokkal (replay attack) szemben	6.1.	Nem megbízható forrásból származó információk elfogadása
			6.2.	Közbeékelődéses támadás (man in the middle attack) / munkamenet-eltérítés (session hijacking)
			6.3.	Visszajátszásos támadás (replay attack), például ha egy kommunikációs átjáró elleni támadás során a támadó visszaállítja egy korábbi verzióra egy elektronikus vezérlőegység szoftverét vagy az átjáró belső vezérlőprogramját
	7.	Az információk könnyű hozzáférhetősége (például a kommunikáció lehallgatása vagy az érzékeny fájlokhoz vagy mappákhoz való jogosulatlan hozzáférés lehetővé tétele révén)	7.1.	Információ elfogása / zavaró sugárzás / a kommunikáció megfigyelése
			7.2.	Jogosulatlan hozzáférés a fájlokhoz vagy az adatokhoz

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
	8.	Túlterheléses (DoS) támadás a kommunikációs csatornákon keresztül a jármű funkcióinak megzavarása érdekében	8.1.	Nagyszámú adathulladék küldése a jármű információs rendszerébe annak érdekében, hogy az ne tudjon a szokásos módon szolgáltatásokat nyújtani
			8.2.	„Fekete lyuk” (black hole) típusú támadás, melynek során a járművek közötti kommunikáció megszakítása érdekében a támadó blokkolja a járművek közötti üzeneteket
	9.	A megfelelő jogosultsággal nem rendelkező felhasználó képes jogosultsághoz kötött hozzáférést szerezni a jármű rendszereihez	9.1.	A megfelelő jogosultsággal nem rendelkező felhasználó képes jogosultsághoz kötött, például rendszergazdai (root) hozzáférést szerezni
	10.	A kommunikációs eszközökbe ágyazott vírusok képesek megfertőzni a jármű rendszereit	10.1.	A kommunikációs eszközökbe ágyazott vírus megfertőzi a jármű rendszereit
	11.	A jármű által fogadott vagy azon belül továbbított üzenetek (például X2V vagy diagnosztikai üzenetek) rosszindulatú tartalommal rendelkeznek	11.1.	Rosszindulatú belső üzenetek (pl. CAN)
			11.2.	Rosszindulatú V2X üzenetek, pl. infrastruktúra–jármű vagy jármű–jármű közötti üzenetek (pl. CAM, DENM)
			11.3.	Rosszindulatú diagnosztikai üzenetek
			11.4.	Rosszindulatú, zárt forráskódú üzenetek (pl. általában az eredetiberendezés-gyártótól vagy az alkotóelem/rendszer/funkció beszállítójától származó üzenetek)
4.3.3. A járműveket a frissítési folyamataik szempontjából érintő fenyegetések	12.	A frissítési folyamatokkal való visszaélés vagy azok veszélyeztetése	12.1.	A vezeték nélküli szoftverfrissítési folyamatok veszélyeztetése. Ez magában foglalja a rendszerfrissítési program vagy a belső vezérlőprogram hamisítását is.
			12.2.	A helyi/fizikai szoftverfrissítési folyamatok veszélyeztetése. Ez magában foglalja a rendszerfrissítési program vagy a belső vezérlőprogram hamisítását is.
			12.3.	A szoftver manipulálása (és károsítása) a frissítési folyamat előtt, amely azonban nem érinti magát a frissítési folyamatot
			12.4.	A szoftverszolgáltató titkosítási kulcsainak illetéktelen módosítása egy érvénytelen frissítés lehetővé tétele érdekében
	13.	Lehetőség a szabályszerű frissítések elutasítására	13.1.	Túlterheléses (DoS) támadás a frissítést végző szerver vagy hálózat ellen a kritikus fontosságú szoftverfrissítések kitelepítésének és/vagy a felhasználóspecifikus funkciók engedélyezésének megakadályozása érdekében
4.3.4. A járműveket érintő azon fenyegetések, amelyek a kibertámadásokat nem szándékosan elősegítő emberi beavatkozásból fakadnak	15.	A jogosult szereplők olyan intézkedéseket hozhatnak, amelyekkel akaratlanul elősegítik a kibertámadásokat	15.1.	Egy ártatlan áldozatot (például tulajdonost, üzemeltetőt vagy karbantartó mérnököt) megtévesztéssel rávesznek arra, hogy akaratlanul betöltsön egy rosszindulatú szoftvert vagy lehetővé tegyen egy támadást
			15.2.	Nem követik a meghatározott biztonsági folyamatokat

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
4.3.5. A járműveket a külső csatlakozás és kapcsolatok kapcsán érintő fenyegetések	16.	Az összekapcsolt járműfunkciók (például a telematika, a távműködtetést lehetővé tevő rendszerek vagy a rövid hatótávolságú vezeték nélküli kommunikációt alkalmazó rendszerek) manipulálása kibertámadást tesz lehetővé	16.1.	A rendszerek távműködtetésére szolgáló funkciók, például a távoli kulcs, az indításgátló és az elektromos töltőoszlopok manipulálása
			16.2.	A járművek telematikájának manipulálása (pl. érzékeny áruk hőmérsékletmérésének manipulálása, raktérajtók zárjainak távolról történő kinyitása)
			16.3.	A kis hatótávolságú, vezeték nélküli hálózatok vagy az érzékelők zavarása
	17.	Harmadik fél által üzemeltetett szoftverek, pl. szórakoztató alkalmazások felhasználása a járműrendszerek megtámadására	17.1.	Hibás vagy gyenge szoftverbiztonsággal rendelkező alkalmazások felhasználása a járműrendszerek megtámadására
	18.	Külső interfészekhez, pl. USB- vagy OBD-portokhoz csatlakoztatott eszközök felhasználása a járműrendszerek megtámadására	18.1.	A külső interfészek, például USB- vagy más portok támadási pontként való felhasználása, például rosszindulatú kóddal való fertőzés (code injection) révén
			18.2.	Vírussal fertőzött adathordozó csatlakoztatása a járműrendszerhez
			18.3.	A diagnosztikai hozzáférés (pl. az OBD-porthoz csatlakoztatott adapterek) felhasználása támadásra, például a jármű paramétereinek manipulálására (közvetlenül vagy közvetve)
4.3.6. A járműadatokat/-kódokat érintő fenyegetések	19.	A járműadatok/-kódok kinyerése	19.1.	Szerzői jog által védett vagy zárt forráskódú szoftver kinyerése a járműrendszerekből (termékkalózkodás)
			19.2.	Jogosulatlan hozzáférés a tulajdonos magánjellegű adataihoz, például személyazonosságához, számlainformációihoz, címjegyzékéhez, helymeghatározási információihoz, a jármű elektronikus azonosítójához stb.
			19.3.	A titkosítási kulcsok kinyerése
	20.	A járműadatok/-kódok manipulálása	20.1.	A jármű elektronikus azonosítójának jogosulatlan/nem engedélyezett megváltoztatása
			20.2.	Személyazonossággal való visszaélés (például ha a felhasználó más azonosítót akar használni az útdíjszedési rendszerekkel vagy a gyártó back-end rendszerével való kommunikáció során)
			20.3.	Az ellenőrző rendszerek megkerülésére irányuló intézkedések (például az ODR Tracker [működési adatok naplója] adatainak, az utak számának vagy egyéb hasonló üzeneteknek a feltörése/manipulálása/blokkolása)
			20.4.	Adatmanipuláció a jármű vezetési adatainak (például futásteljesítmény, vezetési sebesség, vezetési irányok stb.) meghamisítása érdekében
			20.5.	A rendszerdiagnosztikai adatok jogosulatlan módosítása
	21.	Az adatok/kódok törlése	21.1.	A rendszer eseménynaplójának jogosulatlan törlése/manipulálása
	22.	Rosszindulatú szoftverek bevezetése	22.2.	Rosszindulatú szoftver vagy rosszindulatú szoftvertevékenység bevezetése

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
	23.	Új szoftver bevezetése vagy meglévő szoftver felülírása	23.1.	A járművezérlő vagy járműinformációs rendszer szoftverének hamisítása
	24.	A rendszerek vagy műveletek megzavarása	24.1.	Túlterheléses (DoS) támadás, amely a belső hálózatban megvalósítható például a CAN-busz elárasztásával (flooding) vagy nagyszámú üzenet küldése révén a motorvezérlő egység meghibásodásának előidézésével
	25.	A jármű paramétereinek manipulálása	25.1.	Jogosulatlan hozzáférés a fő járműfunkciók konfigurációs paramétereinek (például a fékadatoknak, a légzsák kinyílási küszöbértékének stb.) manipulálása érdekében
			25.2.	Jogosulatlan hozzáférés a töltési paraméterek (például a töltési feszültség, töltési teljesítmény, akkumulátor-hőmérséklet stb.) manipulálása érdekében
4.3.7. Kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhető-ségek	26.	A titkosítási technológiák sérülésének lehetősége vagy nem megfelelő alkalmazása	26.1.	A rövid titkosítási kulcsok és a hosszú érvényességi idő kombinációja lehetővé teszi a támadó számára a titkosítás feltörését
			26.2.	Az érzékeny rendszerek védelmére szolgáló titkosítási kulcsok nem megfelelő használata
			26.3.	Elavult vagy hamarosan érvényét vesztő titkosítási algoritmusok használata
	27.	Az alkatrészek vagy tartozékok károsítása, ami lehetővé teszi a jármű megtámadását	27.1.	A támadások lehetővé tételére kifejlesztett vagy a támadások megállításával kapcsolatos tervezési követelményeket nem teljesítő hardverek vagy szoftverek
	28.	Sebezhetőséget előidéző szoftver- vagy hardverfejlesztés	28.1.	Szoftverhibák. A szoftverhibák lehetőséget adhatnak egyes sebezhetőségek kihasználására. Ez különösen igaz abban az esetben, ha a szoftvert nem tesztelték annak érdekében, hogy igazolják az ismert kód-/szoftverhibák hiányát és csökkentsék az ismeretlen kód-/szoftverhibák előfordulásának kockázatát.
			28.2.	A fejlesztés időszakából fennmaradt elemek (pl. hibakeresési [debug] portok, JTAG-portok, mikroprocesszorok, fejlesztési tanúsítványok, fejlesztői jelszavak stb.) használata lehetővé teszi az elektronikus vezérlőegységhez való hozzáférést, vagy lehetővé teszi a támadók számára, hogy felsőbb szintű jogosultságokat szerezzenek
	29.	A hálózat kialakítása sebezhetőségeket idéz elő	29.1.	Szükségtelen internetportok nyitva hagyása, ami hozzáférést biztosít a hálózati rendszerekhez
			29.2.	A hálózati szétválasztás megkerülése az irányítás megszerzése érdekében. Konkrét példa erre a védelem nélküli átjárók vagy hozzáférési pontok (például tehergépjármű-pótkocsi átjárók) felhasználása a védelem megkerülése és a további hálózati szegmensekhez való hozzáférés érdekében, rosszindulatú beavatkozások végrehajtása, például önkényes CAN-buszüzenetek küldése céljából.
	31.	Fennáll a nem szándékos adattovábbítás lehetősége	31.1.	Információszivárgás. Személyes adatok szivároghatnak ki, amikor a járművet új személy használja (például tulajdonosváltás vagy járműbérlés esetén).

A sebezhetőségek/fenyegetések fő és alkategóriáinak leírása			Példa a sebezhetőségre vagy a támadási módszerre	
	32.	A rendszerek fizikai manipulációja támadásokat tehet lehetővé	32.1.	Az elektronikus hardverek manipulálása, például olyan nem engedélyezett elektronikus hardver hozzáadása a járműhöz, amely lehetővé teszi a közbeékelődéses támadást (man in the middle attack). Az engedélyezett elektronikus hardverek (pl. érzékelők) kicserélése nem engedélyezett elektronikus hardverekre. Az érzékelők által gyűjtött információk manipulálása (például a sebességváltóhoz csatlakoztatott Hall-érzékelő manipulálása mágnessel).

B. RÉSZ

A járműveket érintő fenyegetésekkel szembeni kockázatcsökkentő intézkedések

1. A „járművek kommunikációs csatornáihoz” kapcsolódó kockázatcsökkentő intézkedések

A B1. táblázat a „jármű kommunikációs csatornáihoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B1. táblázat

A „jármű kommunikációs csatornáihoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „járművek kommunikációs csatornáihoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
4.1.	A személyazonosság meghamisítása révén az üzenetekkel kapcsolatban alkalmazott megtévesztés (spoofing) (pl. a V2X típusú [a járműtől más rendszerek felé irányuló] kommunikációban: a kooperatív tájékoztató [cooperative awareness, CAM] üzenetek vagy a manőverkoordinációs üzenetek, illetve a GNSS-üzenetek terén stb.)	M10	A járműnek ellenőriznie kell az általa fogadott üzenetek hitelességét és sértetlenségét.
4.2.	Sybil-támadás (más járművek megtévesztése azt a látszatot keltve, mintha sok jármű lenne az úton)	M11	Biztonsági ellenőrzéseket kell alkalmazni a titkosítási kulcsok tárolása során (pl. biztonsági hardvermodulok használata)
5.1.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok rosszindulatú kóddal való fertőzését (code injection), például egy szoftver manipulált bináris állományai bejuttathatók a kommunikációs adatfolyamba	M10 M6	A járműnek ellenőriznie kell az általa fogadott üzenetek hitelességét és sértetlenségét. A kockázatok minimalizálása érdekében meg kell valósítani a beépített biztonság érvényesülését a rendszerekben.
5.2.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok manipulálását	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében.
5.3.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok felülírását		
5.4. 21.1.	A kommunikációs csatornák lehetővé teszik a járművön tárolt adatok/kódok törlését		
5.5.	A kommunikációs csatornák lehetővé teszik adatok/kódok bevitelét a járműrendszerekbe (adatok/kódok írása)		

Az A1. táblázat szerinti hivatkozási szám	A „járművek kommunikációs csatornáihoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
6.1.	Nem megbízható forrásból származó információk elfogadása	M10	A járműnek ellenőriznie kell az általa fogadott üzenetek hitelességét és sértetlenségét.
6.2.	Közbeékelődéses támadás (man in the middle attack) / munkamenet-eltérítés (session hijacking)	M10	A járműnek ellenőriznie kell az általa fogadott üzenetek hitelességét és sértetlenségét.
6.3.	Visszajátszásos támadás (replay attack), például ha egy kommunikációs átjáró elleni támadás során a támadó visszaállítja egy korábbi verzióra egy elektronikus vezérlőegység szoftverét vagy az átjáró belső vezérlőprogramját		
7.1.	Információ elfogása / zavaró sugárzás / a kommunikáció megfigyelése	M12	A járműbe vagy a járműből továbbított bizalmas adatokat védeni kell.
7.2.	Jogosulatlan hozzáférés a fájlokhoz vagy az adatokhoz	M8	A rendszer megfelelő kialakítása és a hozzáférés-engedélyezés révén meg kell akadályozni, hogy illetéktelenek személyes vagy a rendszer szempontjából kritikus fontosságú adatokhoz férhessenek hozzá. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
8.1.	Nagyszámú adathulladék küldése a jármű információs rendszerébe annak érdekében, hogy az ne tudjon a szokásos módon szolgáltatásokat nyújtani	M13	Intézkedéseket kell alkalmazni a túlterheléses (DoS) támadások észlelésére és az azt követő helyreállításra.
8.2.	„Fekete lyuk” (black hole) típusú támadás, melynek során a más járműveknek küldött üzenetek blokkolásával megszakítják a járművek közötti kommunikációt	M13	Intézkedéseket kell alkalmazni a túlterheléses (DoS) támadások észlelésére és az azt követő helyreállításra.
9.1.	A megfelelő jogosultsággal nem rendelkező felhasználó képes jogosultsághoz kötött, például rendszergazdai (root) hozzáférést szerezni	M9	Intézkedéseket kell alkalmazni a jogosulatlan hozzáférés megakadályozására és észlelésére.
10.1.	A kommunikációs eszközökbe ágyazott vírus megfertőzi a jármű rendszereit	M14	Fontolóra kell venni a rendszerek beágyazott vírusok/rosszindulatú szoftverek elleni védelmére irányuló intézkedések bevezetését.
11.1.	Rosszindulatú belső üzenetek (pl. CAN)	M15	Fontolóra kell venni a rosszindulatú belső üzenetek vagy tevékenységek észlelésére irányuló intézkedések bevezetését.
11.2.	Rosszindulatú V2X üzenetek, pl. infrastruktúra–jármű vagy jármű–jármű közötti üzenetek (pl. CAM, DENM)	M10	A járműnek ellenőriznie kell az általa fogadott üzenetek hitelességét és sértetlenségét.
11.3.	Rosszindulatú diagnosztikai üzenetek		
11.4.	Rosszindulatú, zárt forráskódú üzenetek (pl. általában az eredetiberendezés-gyártótól vagy az alkotóelem/rendszer/funkció beszállítójától származó üzenetek)		

2. A „frissítési folyamathoz” kapcsolódó kockázatcsökkentő intézkedések

A B2. táblázat a „frissítési folyamathoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B2. táblázat

A „frissítési folyamathoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „frissítési folyamathoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
12.1.	A vezeték nélküli szoftverfrissítési folyamatok veszélyeztetése. Ez magában foglalja a rendszerfrissítési program vagy a belső vezérlőprogram hamisítását is.	M16	Biztonságos szoftverfrissítési folyamatokat kell alkalmazni.
12.2.	A helyi/fizikai szoftverfrissítési folyamatok veszélyeztetése. Ez magában foglalja a rendszerfrissítési program vagy a belső vezérlőprogram hamisítását is.		
12.3.	A szoftver manipulálása (és károsítása) a frissítési folyamat előtt, amely azonban nem érinti magát a frissítési folyamatot		
12.4.	A szoftverszolgáltató titkosítási kulcsainak illetéktelen módosítása egy érvénytelen frissítés lehetővé tétele érdekében	M11	Biztonsági ellenőrzéseket kell alkalmazni a titkosítási kulcsok tárolása során.
13.1.	Túlterheléses (DoS) támadás a frissítést végző szerver vagy hálózat ellen a kritikus fontosságú szoftverfrissítések kitelepítésének és/vagy a felhasználóspecifikus funkciók engedélyezésének megakadályozása érdekében	M3	Biztonsági ellenőrzéseket kell alkalmazni a back-end rendszerek vonatkozásában. Ha a back-end szerverek kritikus fontosságúak a szolgáltatásnyújtás szempontjából, a rendszer kiesése esetén helyreállítási intézkedéseket kell alkalmazni. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.

3. A „kibertámadásokat nem szándékosan elősegítő emberi beavatkozásokhoz” kapcsolódó kockázatcsökkentő intézkedések

A B3. táblázat a „kibertámadásokat nem szándékosan elősegítő emberi beavatkozásokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B3. táblázat

A „kibertámadásokat nem szándékosan elősegítő emberi beavatkozásokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „nem szándékos emberi beavatkozásokhoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
15.1.	Egy ártatlan áldozatot (például tulajdonost, üzemeltetőt vagy karbantartó mérnököt) megtévesztéssel rávesznek arra, hogy akaratlanul betöltsön egy rosszindulatú szoftvert vagy lehetővé tegyen egy támadást	M18	Intézkedéseket kell alkalmazni a felhasználói szerepek és a hozzáférési jogosultságok meghatározására és ellenőrzésére a legkisebb hozzáférési jogosultság elve alapján.

Az A1. táblázat szerinti hivatkozási szám	A „nem szándékos emberi beavatkozásokhoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
15.2.	Nem követik a meghatározott biztonsági folyamatokat	M19	A szervezeteknek gondoskodniuk kell a biztonsági folyamatok meghatározásáról és követéséről, beleértve a biztonsági funkciók kezeléséhez kapcsolódó tevékenységek és hozzáférések naplózását.

4. A „külső csatlakozáshoz és kapcsolatokhoz” kapcsolódó kockázatcsökkentő intézkedések

A B4. táblázat a „külső csatlakozáshoz és kapcsolatokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B4. táblázat

A „külső csatlakozáshoz és kapcsolatokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „külső csatlakozáshoz és kapcsolatokhoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
16.1.	A járműrendszerek távműködtetésére szolgáló funkciók, például a távoli kulcs, az indításgátló és az elektromos töltőoszlopok manipulálása	M20	Biztonsági ellenőrzéseket kell alkalmazni a távoli hozzáféréssel rendelkező rendszerek vonatkozásában.
16.2.	A járművek telematikájának manipulálása (pl. érzékeny áruk hőmérsékletmérésének manipulálása, raktérajtók zárjainak távolról történő kinyitása)		
16.3.	A kis hatótávolságú, vezeték nélküli hálózatok vagy az érzékelők zavarása		
17.1.	Hibás vagy gyenge szoftverbiztonsággal rendelkező alkalmazások felhasználása a járműrendszerek megtámadására	M21	A szoftvereket biztonsági értékelésnek kell alávetni, továbbá a szoftvereknek hitelesítéssel és integritásvédelemmel kell rendelkezniük. Biztonsági ellenőrzéseket kell alkalmazni annak érdekében, hogy minimalizálható legyen a harmadik felektől származó, kifejezetten vagy feltételezhetően a járműbe telepítendő szoftverekkel kapcsolatos kockázat.
18.1.	A külső interfészek, például USB- vagy más portok támadási pontként való felhasználása, például rosszindulatú kóddal való fertőzés (code injection) révén	M22	Biztonsági ellenőrzéseket kell alkalmazni a külső interfészek vonatkozásában.
18.2.	Vírussal fertőzött adathordozó csatlakoztatása a járműhöz		
18.3.	A diagnosztikai hozzáférés (pl. az OBD-porthoz csatlakoztatott adapterek) felhasználása támadásra, például a jármű paramétereinek manipulálására (közvetlenül vagy közvetve)	M22	Biztonsági ellenőrzéseket kell alkalmazni a külső interfészek vonatkozásában.

5. A „támadás potenciális célpontjaihoz vagy indokaihoz” kapcsolódó kockázatcsökkentő intézkedések

A B5. táblázat a „támadás potenciális célpontjaihoz vagy indokaihoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B5. táblázat

A „támadás potenciális célpontjaihoz vagy indokaihoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „támadás potenciális célpontjaihoz vagy indokaihoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
19.1.	Szerzői jog által védett vagy zárt forráskódú szoftver kinyerése a járműrendszerekből (termékkalózkodás/szoftverlopás)	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
19.2.	Jogosulatlan hozzáférés a tulajdonos magánjellegű adataihoz, például személyazonosságához, számlainformációihoz, címjegyzékéhez, helymeghatározási információihoz, a jármű elektronikus azonosítójához stb.	M8	A rendszer megfelelő kialakítása és a hozzáférés-engedélyezés révén meg kell akadályozni, hogy illetéktelenek személyes vagy a rendszer szempontjából kritikus fontosságú adatokhoz férhessenek hozzá. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
19.3.	A titkosítási kulcsok kinyerése	M11	Biztonsági ellenőrzéseket kell alkalmazni a titkosítási kulcsok tárolása során (pl. biztonsági modulok használata)
20.1.	A jármű elektronikus azonosítójának jogosulatlan/nem engedélyezett megváltoztatása	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
20.2.	Személyazonossággal való visszaélés (például ha a felhasználó más azonosítót akar használni az útdíjszedési rendszerekkel vagy a gyártó back-end rendszerével való kommunikáció során)		
20.3.	Az ellenőrző rendszerek megkerülésére irányuló intézkedések (például az ODR Tracker [működési adatok naplója] adatainak, az utak számának vagy egyéb hasonló üzeneteknek a feltörése/manipulálása/blokkolása)	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat. Az érzékelőkre vagy a továbbított adatokra irányuló adatmanipulálási támadások kockázata a különböző információforrásokból származó adatok összevetésével mérsékelhető.
20.4.	Adatmanipuláció a jármű vezetési adatainak (például futásteljesítmény, vezetési sebesség, vezetési irányok stb.) meghamisítása érdekében		
20.5.	A rendszerdiagnosztikai adatok jogosulatlan módosítása		
21.1.	A rendszer eseménynaplójának jogosulatlan törlése/manipulálása	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
22.2.	Rosszindulatú szoftver vagy rosszindulatú szoftvertevékenység bevezetése	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
23.1.	A járművezérlő vagy járműinformációs rendszer szoftverének hamisítása		

Az A1. táblázat szerinti hivatkozási szám	A „támadás potenciális célpontjaihoz vagy indokaihoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
24.1.	Túlterheléses (DoS) támadás, amely a belső hálózatban megvalósítható például a CAN-busz elárasztásával (flooding) vagy nagyszámú üzenet küldése révén a motorvezérlő egység meghibásodásának előidézésével	M13	Intézkedéseket kell alkalmazni a túlterheléses (DoS) támadások észlelésére és az azt követő helyreállításra.
25.1.	Jogosulatlan hozzáférés a fő járműfunkciók konfigurációs paramétereinek (például a fékadatoknak, a légzsák kinyílási küszöbértékének stb.) manipulálása érdekében	M7	Hozzáférés-engedélyezési technikákat és terveket kell alkalmazni a rendszeradatok/-kódok védelme érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
25.2.	Jogosulatlan hozzáférés a töltési paraméterek (például a töltési feszültség, töltési teljesítmény, akkumulátor-hőmérséklet stb.) manipulálása érdekében		

6. A „kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhetőségekkel” szembeni kockázatcsökkentő intézkedések

A B6. táblázat a „kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhetőségekkel” szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B6. táblázat

A „kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhetőségekhez” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhetőségekhez” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
26.1.	A rövid titkosítási kulcsok és a hosszú érvényességi idő kombinációja lehetővé teszi a támadó számára a titkosítás feltörését	M23	Követni kell a szoftver- és hardverfejlesztésre vonatkozó legjobb kiberbiztonsági gyakorlatokat.
26.2.	Az érzékeny rendszerek védelmére szolgáló titkosítási kulcsok nem megfelelő használata		
26.3.	Elavult titkosítási algoritmusok használata		
27.1.	A támadások lehetővé tételére kifejlesztett vagy a támadások megállításával kapcsolatos tervezési követelményeket nem teljesítő hardverek vagy szoftverek	M23	Követni kell a szoftver- és hardverfejlesztésre vonatkozó legjobb kiberbiztonsági gyakorlatokat.
28.1.	A szoftverhibák lehetőséget adhatnak egyes sebezhetőségek kihasználására. Ez különösen igaz abban az esetben, ha a szoftvert nem tesztelték annak érdekében, hogy igazolják az ismert kód-/szoftverhibák hiányát és csökkentsék az ismeretlen kód-/szoftverhibák előfordulásának kockázatát.	M23	Követni kell a szoftver- és hardverfejlesztésre vonatkozó legjobb kiberbiztonsági gyakorlatokat. Megfelelő részletességű kiberbiztonsági tesztelést kell alkalmazni.

Az A1. táblázat szerinti hivatkozási szám	A „kellő mértékű védelem vagy megerősítés hiányában kihasználható, lehetséges sebezhetőségekhez” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
28.2.	A fejlesztés időszakából fennmaradt elemek (pl. hibakeresési [debug] portok, JTAG-portok, mikroprocesszorok, fejlesztési tanúsítványok, fejlesztői jelszavak stb.) használata a támadók számára, hogy hozzáférjenek az elektronikus vezérlőegységekhez vagy felsőbb szintű jogosultságokat szerezzenek		
29.1.	Szükségtelen internetportok nyitva hagyása, ami hozzáférést biztosít a hálózati rendszerekhez		
29.2.	A hálózati szétválasztás megkerülése az irányítás megszerzése érdekében. Konkrét példa erre a védelem nélküli átjárók vagy hozzáférési pontok (például tehergépjármű-pótkocsi átjárók) felhasználása a védelem megkerülése és a további hálózati szegmensekhez való hozzáférés érdekében, rosszindulatú beavatkozások végrehajtása, például önkényes CAN-buszüzenetek küldése céljából.	M23	Követni kell a szoftver- és hardverfejlesztésre vonatkozó legjobb kiberbiztonsági gyakorlatokat. Követni kell a rendszer kialakítására és integrációjára vonatkozó legjobb kiberbiztonsági gyakorlatokat.

7. Az „adatvesztéshez/a jármű irányából történő adatszivárgáshoz” kapcsolódó kockázatcsökkentő intézkedések

A B7. táblázat az „adatvesztéshez/a jármű irányából történő adatszivárgáshoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B7. táblázat

Az „adatvesztéshez/a jármű irányából történő adatszivárgáshoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	Az „adatvesztéshez/a jármű irányából történő adatszivárgáshoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
31.1.	Információszivárgás. Személyes adatok szivároghatnak ki, amikor a járművet új személy használja (például tulajdonosváltás vagy járműbérlés esetén).	M24	A személyes adatok tárolása során követni kell az adatok sértetlenségének és titkosságának védelmére vonatkozó legjobb gyakorlatokat.

8. A „rendszerek támadást lehetővé tévő fizikai manipulációjához” kapcsolódó kockázatcsökkentő intézkedések

A B8. táblázat a „rendszerek támadást lehetővé tévő fizikai manipulációjához” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

B8. táblázat

A „rendszerek támadást lehetővé tévő fizikai manipulációjához” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „rendszerek támadást lehetővé tévő fizikai manipulációjához” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
32.1.	Az eredetiberendezés-gyártóktól származó hardverek manipulálása, például olyan nem engedélyezett hardver hozzáadása a járműhöz, amely lehetővé teszi a közbeékelődéses támadást (man in the middle attack)	M9	Intézkedéseket kell alkalmazni a jogosulatlan hozzáférés megakadályozására és észlelésére.

C. RÉSZ

A járműveken kívüli fenyegetésekkel szembeni kockázatcsökkentő intézkedések

1. A „back-end szerverekhez” kapcsolódó kockázatcsökkentő intézkedések

A C1. táblázat a „back-end szerverekhez” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

C1. táblázat

A „back-end szerverekhez” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „back-end szerverekhez” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
1.1. és 3.1.	A személyzet visszaélése a jogosultságokkal (belső támadás)	M1	Biztonsági ellenőrzéseket kell alkalmazni a back-end rendszerek vonatkozásában a belső támadás kockázatának minimalizálása érdekében.
1.2. és 3.3.	Jogosulatlan internetes hozzáférés a szerverhez (például „hátsó ajtók” [backdoorok] révén, a rendszerszoftverek ki nem javított [unpatched] sérülékenységeinek kihasználásával, SQL-támadások vagy más eszközök segítségével)	M2	Biztonsági ellenőrzéseket kell alkalmazni a back-end rendszerek vonatkozásában a jogosulatlan hozzáférés kockázatának minimalizálása érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
1.3. és 3.4.	Jogosulatlan fizikai hozzáférés a szerverhez (például USB-kulcsok vagy a szerverhez csatlakoztatott egyéb adathordozók révén)	M8	A rendszer megfelelő kialakítása és a hozzáférés-engedélyezés révén meg kell akadályozni, hogy illetéktelen személyek személyes vagy a rendszer szempontjából kritikus fontosságú adatokhoz férhessenek hozzá.
2.1.	A back-end szerver elleni támadás miatt leáll a szerver működése, például nem tud kommunikálni a járművekkel és nem tudja biztosítani a járművek által igénybe vett szolgáltatásokat	M3	Biztonsági ellenőrzéseket kell alkalmazni a back-end rendszerek vonatkozásában. Ha a back-end szerverek kritikus fontosságúak a szolgáltatásnyújtás szempontjából, a rendszer kiesése esetén helyreállítási intézkedéseket kell alkalmazni. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.
3.2.	Információvesztés a felhőben. Ha az adatokat harmadik felek által szolgáltatott felhőben tárolják, támadás vagy baleset következtében érzékeny adatok veszhetnek el.	M4	Biztonsági ellenőrzéseket kell alkalmazni a felhőalapú számítástechnikával kapcsolatos kockázatok minimalizálása érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt és az NCSC felhőalapú számítástechnikával kapcsolatos iránymutatása kínál példákat.
3.5.	Információszivárgás nem szándékos adatmegosztás (pl. adminisztrációs hibák, garázsban elhelyezett szervereken tárolt adatok) miatt	M5	Biztonsági ellenőrzéseket kell alkalmazni a back-end rendszerek vonatkozásában az adatszivárgás megelőzése érdekében. A biztonsági ellenőrzésekre az OWASP alkalmazásbiztonsági projekt kínál példákat.

2. A „nem szándékos emberi beavatkozásokhoz” kapcsolódó kockázatcsökkentő intézkedések

A C2. táblázat a „nem szándékos emberi beavatkozásokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

C2. táblázat

A „nem szándékos emberi beavatkozásokhoz” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „nem szándékos emberi beavatkozásokhoz” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
15.1.	Egy ártatlan áldozatot (például tulajdonost, üzemeltetőt vagy karbantartó mérnököt) megtévesztéssel rávesznek arra, hogy akaratlanul betöltsön egy rosszindulatú szoftvert vagy lehetővé tegyen egy támadást	M18	Intézkedéseket kell alkalmazni a felhasználói szerepek és a hozzáférési jogosultságok meghatározására és ellenőrzésére a legkisebb hozzáférési jogosultság elve alapján.
15.2.	Nem követik a meghatározott biztonsági folyamatokat	M19	A szervezeteknek gondoskodniuk kell a biztonsági folyamatok meghatározásáról és követéséről, beleértve a biztonsági funkciók kezeléséhez kapcsolódó tevékenységek és hozzáférések naplózását.

3. A „fizikai adatvesztéshez” kapcsolódó kockázatcsökkentő intézkedések

A C3. táblázat a „fizikai adatvesztéshez” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedéseket sorolja fel.

C3. táblázat

A „fizikai adatvesztéshez” kapcsolódó fenyegetésekkel szembeni kockázatcsökkentő intézkedések

Az A1. táblázat szerinti hivatkozási szám	A „fizikai adatvesztéshez” kapcsolódó fenyegetések	Hivatkozási szám	Kockázatcsökkentő intézkedés
30.1.	Harmadik fél által okozott kár. Az érzékeny adatok lopás vagy közlekedési balesetben bekövetkező fizikai károsodás miatt elveszhetnek vagy sérülhetnek.	M24	A személyes adatok tárolása során követni kell az adatok sértetlenségének és titkosságának védelmére vonatkozó legjobb gyakorlatokat. A biztonsági ellenőrzésekre az ISO/SC27/WG5 szabvány kínál példákat.
30.2.	A digitális jogok kezelésével (DRM) kapcsolatos konfliktusokból eredő adatvesztés. A digitális jogok kezelésével (DRM) kapcsolatos problémák miatt felhasználói adatok kerülhetnek törlésre.		
30.3.	Az érzékeny adatok elveszhetnek vagy sérülhetnek az informatikai alkatrészek kopása és elhasználódása miatt, ami továbbgyűrűző problémákat okozhat (például kulcsfontosságú módosítások esetén)		