Samo izvirna besedila UN/ECE so pravno veljavna v skladu z mednarodnim javnim pravom. Status in datum začetka veljavnosti tega pravilnika je treba preveriti v najnovejši različici dokumenta UN/ECE TRANS/WP.29/343, ki je na voljo na: https://unece.org/status-1958-agreement-and-annexed-regulations

Pravilnik ZN št. 155 – Enotne določbe o homologaciji vozil glede na kibernetsko varnost in sistem za upravljanje kibernetske varnosti [2025/5]

Vključuje vsa veljavna besedila do:

dodatka 3 k prvotni različici pravilnika – začetek veljavnosti: 10. januar 2025.

Ta dokument je mišljen zgolj kot dokumentacijsko orodje. Verodostojna in pravno zavezujoča besedila so:

— ECE/TRANS/WP.29/2020/79 (kot je bil spremenjen z ECE/TRANS/WP.29/2020/94 in ECE/TRANS/WP.29/2020/97),

— ECE/TRANS/WP.29/2022/54,

— ECE/TRANS/WP.29/2023/70 in

— ECE/TRANS/WP.29/2024/55.

VSEBINA

Pravilnik

1. Področje uporabe
2. Opredelitev pojmov
3. Vloga za podelitev homologacije
4. Oznake
5. Homologacija
6. Potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti
7. Specifikacije
8. Sprememba tipa vozila in razširitev homologacije
9. Skladnost proizvodnje
10. Kazni za neskladnost proizvodnje
11. Dokončno prenehanje proizvodnje
12. Nazivi in naslovi tehničnih služb, ki izvajajo homologacijski preizkus, in homologacijskih organov

Priloge

1 Opisni list

2 Sporočilo

3 Namestitev homologacijske oznake

4 Vzorec potrdila o skladnosti za sistem za upravljanje kibernetske varnosti

5 Seznam groženj in ustreznih blažitvenih ukrepov

1. Področje uporabe

1.1 Ta pravilnik se uporablja glede na kibernetsko varnost za vozila kategorij L, M, N in O z vsaj eno elektronsko krmilno enoto.

1.2 Ta pravilnik ne posega v druge pravilnike ZN ali regionalno ali nacionalno zakonodajo, ki urejajo dostop pooblaščenih strank do vozila, njegovih podatkov, funkcij in virov ter pogoje za tak dostop. Prav tako ne posega v uporabo nacionalne in regionalne zakonodaje o zasebnosti in varstvu posameznikov pri obdelavi njihovih osebnih podatkov.

1.3 Ta pravilnik ne posega v druge pravilnike ZN ali regionalno ali nacionalno zakonodajo, ki urejajo razvoj in namestitev/vključevanje nadomestnih in sestavnih fizičnih in digitalnih delov v sistem, kar zadeva kibernetsko varnost.

2. Opredelitev pojmov

Za namene tega pravilnika se uporabljajo naslednje opredelitve pojmov:

2.1 „tip vozila“ pomeni vozila, ki se ne razlikujejo vsaj v naslednjih bistvenih vidikih:

(a) oznaki tipa vozila, ki jo je določil proizvajalec;

(b) bistvenih vidikih električne/elektronske arhitekture in zunanjih vmesnikov, kar zadeva kibernetsko varnost;

2.2 „kibernetska varnost“ pomeni stanje, v katerem so cestna vozila in njihove funkcije zaščitene pred kibernetskimi grožnjami električnim ali elektronskim sestavnim delom;

2.3 „sistem za upravljanje kibernetske varnosti“ pomeni na tveganju temelječ sistematičen pristop, v okviru katerega so opredeljeni organizacijski procesi, odgovornosti in upravljanje za obravnavo tveganj, povezanih s kibernetskimi grožnjami vozilom, in njihovo zaščito pred kibernetskimi napadi;

2.4 „sistem“ pomeni skupino sestavnih delov in/ali podsistemov, ki izvaja funkcijo ali funkcije;

2.5 „razvojna faza“ pomeni obdobje pred homologacijo tipa vozila;

2.6 „proizvodna faza“ pomeni trajanje proizvodnje tipa vozila;

2.7 „poproizvodna faza“ pomeni obdobje, v katerem se tip vozila ne proizvaja več, do konca življenjske dobe vseh vozil zadevnega tipa vozila. Vozila, ki vključujejo določen tip vozila, bodo v tej fazi delovala, vendar se ne bodo več proizvajala. Faza se konča, ko ni več nobenega operativnega vozila določenega tipa vozila;

2.8 „blažitveni ukrep“ pomeni ukrep za zmanjšanje tveganja;

2.9 „tveganje“ pomeni možnost, da bo določena grožnja izkoristila ranljive točke vozila in s tem škodovala organizaciji ali posamezniku;

2.10 „ocena tveganja“ pomeni celoten postopek iskanja, prepoznavanja in opisovanja tveganj (opredelitev tveganja), da bi se razumela narava tveganja in določila stopnja tveganja (analiza tveganja), ter primerjave rezultatov analize tveganja z merili tveganja, da bi se ugotovilo, ali sta tveganje in/ali njegova razsežnost sprejemljiva ali dopustna (ocena tveganja);

2.11 „obvladovanje tveganj“ pomeni usklajene dejavnosti za usmerjanje in nadzorovanje organizacije glede na tveganje;

2.12 „grožnja“ pomeni morebiten vzrok neželenega dogodka, ki bi lahko škodil sistemu, organizaciji ali posamezniku;

2.13 „ranljiva točka“ pomeni pomanjkljivost sredstva ali blažitvenega ukrepa, zaradi katere se lahko uresniči ena ali več groženj.

3. Vloga za podelitev homologacije

3.1 Vlogo za podelitev homologacije tipa vozila glede na kibernetsko varnost vloži proizvajalec vozila ali njegov ustrezno pooblaščeni zastopnik.

3.2 Vlogi se v treh izvodih priložijo dokumenti, navedeni v nadaljevanju, in naslednji podatki:

3.2.1 Opis tipa vozila glede na točke iz Priloge 1 k temu pravilniku.

3.2.2 V primerih, ko se izkaže, da za informacije veljajo pravice intelektualne lastnine ali da informacije predstavljajo posebno tehnologijo proizvajalca oziroma njegovih dobaviteljev, proizvajalec ali njegovi dobavitelji dajo na voljo zadostne informacije, ki omogočajo, da se preverjanja iz tega pravilnika opravijo pravilno. Take informacije se obravnavajo zaupno.

3.2.3 Potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti v skladu z odstavkom 6 tega pravilnika.

3.3 Dokumentacija se predloži v dveh delih:

(a) uradna dokumentacija za homologacijo, ki vsebuje gradivo iz Priloge 1 in ki se predloži homologacijskemu organu ali njegovi tehnični službi ob predložitvi vloge za podelitev homologacije. Homologacijski organ ali njegova tehnična služba to dokumentacijo uporabi kot temeljno referenco za postopek homologacije. Homologacijski organ ali njegova tehnična služba zagotovi, da je ta dokumentacija na voljo vsaj deset let po dokončnem prenehanju proizvodnje tipa vozila;

(b) dodatno gradivo, ki ustreza zahtevam iz tega pravilnika, lahko obdrži proizvajalec, vendar mora biti ob homologaciji dano na voljo za pregled. Proizvajalec zagotovi, da vso gradivo, ki je ob homologaciji dano na voljo za pregled, ostane na voljo vsaj deset let po dokončnem prenehanju proizvodnje tipa vozila.

4. Oznaka

4.1 Na vsakem vozilu, ki je v skladu s tipom vozila, homologiranim po tem pravilniku, je na vidnem in zlahka dostopnem mestu, navedenem na homologacijskem obrazcu, nameščena mednarodna homologacijska oznaka, sestavljena iz:

4.1.1 kroga, ki obkroža črko „E“ in številčno oznako države, ki je podelila homologacijo;

4.1.2 številke tega pravilnika, ki ji sledijo črka „R“, pomišljaj in homologacijska številka, na desni strani kroga iz odstavka 4.1.1.

4.2 Če je vozilo v skladu s tipom vozila, homologiranim po enem ali več drugih pravilnikih, ki so priloženi Sporazumu, v državi, ki je podelila homologacijo v skladu s tem pravilnikom, simbola iz odstavka 4.1.1 ni treba ponoviti; v takem primeru se v navpičnih stolpcih na desni strani simbola iz odstavka 4.1.1 navedejo številke pravilnikov, homologacijske številke in dodatni simboli vseh pravilnikov, v skladu s katerimi je bila podeljena homologacija v državi, ki je podelila homologacijo v skladu s tem pravilnikom.

4.3 Homologacijska oznaka mora biti jasno berljiva in neizbrisna.

4.4 Homologacijska oznaka se namesti na napisno ploščico vozila, ki jo pritrdi proizvajalec, ali blizu nje.

4.5 V Prilogi 3 k temu pravilniku so prikazani primeri namestitve homologacijske oznake.

5. Homologacija

5.1 Homologacijski organi podelijo homologacijo glede na kibernetsko varnost samo tistim tipom vozil, ki izpolnjujejo zahteve iz tega pravilnika.

5.1.1 Homologacijski organ ali tehnična služba s pregledi dokumentov preveri, ali je proizvajalec vozila sprejel potrebne ukrepe, pomembne za tip vozila, da se:

(a) vzdolž dobavne verige zberejo in preverijo informacije, ki se zahtevajo na podlagi tega pravilnika, s čimer se dokaže, da so tveganja, povezana z dobavitelji, opredeljena in obvladovana;

(b) dokumentirajo ocene tveganja (izvedene med razvojno fazo ali za nazaj), rezultati preizkusov in blažitveni ukrepi, ki se uporabljajo za tip vozila, vključno z informacijami o zasnovi, ki podpirajo oceno tveganja;

(c) izvedejo ustrezni ukrepi za kibernetsko varnost pri zasnovi tipa vozila;

(d) odkrijejo morebitni napadi na kibernetsko varnost in zagotovi odziv nanje;

(e) zabeležijo podatki za podporo odkrivanju kibernetskih napadov in zagotovijo podatki o forenzični zmogljivosti, da se omogoči analiza poskusov kibernetskih napadov ali uspešnih kibernetskih napadov.

5.1.2 Homologacijski organ ali tehnična služba s preizkušanjem vozila tipa vozila preveri, ali je proizvajalec vozila izvedel ukrepe za kibernetsko varnost, ki jih je dokumentiral. Preizkuse homologacijski organ ali tehnična služba izvede sam ali v sodelovanju s proizvajalcem vozila z vzorčenjem. Vzorčenje mora biti osredotočeno, vendar ne omejeno na tveganja, ki so med oceno tveganja ocenjena kot visoka.

5.1.3 Homologacijski organ ali tehnična služba zavrne podelitev homologacije glede na kibernetsko varnost, če proizvajalec vozila ni izpolnil ene ali več zahtev iz odstavka 7.3, zlasti:

(a) proizvajalec vozila ni izvedel izčrpne ocene tveganja iz odstavka 7.3.3; tudi kadar proizvajalec ni upošteval vseh tveganj, povezanih z grožnjami iz dela A Priloge 5;

(b) proizvajalec vozila tipa vozila ni zaščitil pred tveganji, opredeljenimi v oceni tveganja, ki jo je izvedel, ali pa sorazmerni blažitveni ukrepi niso bili izvedeni, kot se zahteva v odstavku 7;

(c) proizvajalec vozila ni vzpostavil ustreznih in sorazmernih ukrepov za zaščito namenskih okolij na tipu vozila (če so na voljo) za shranjevanje in izvajanje poprodajne programske opreme, storitev, aplikacij ali podatkov;

(d) proizvajalec vozila pred homologacijo ni izvedel ustreznih in zadostnih preizkusov za preverjanje učinkovitosti izvedenih varnostnih ukrepov.

5.1.4 Homologacijski organ, ki izvaja oceno, podelitev homologacije glede na kibernetsko varnost zavrne tudi, kadar homologacijski organ ali tehnična služba od proizvajalca vozila ni prejela dovolj informacij, da bi ocenila kibernetsko varnost tipa vozila.

5.2 Obvestilo o podelitvi, razširitvi ali zavrnitvi homologacije tipa vozila v skladu s tem pravilnikom se pošlje pogodbenicam Sporazuma iz leta 1958, ki uporabljajo ta pravilnik, na obrazcu, ki je v skladu z vzorcem iz Priloge 2 k temu pravilniku.

5.3 Homologacijski organi ne podelijo nobene homologacije, ne da bi preverili, ali je proizvajalec vzpostavil zadovoljive ureditve in postopke za ustrezno upravljanje vidikov kibernetske varnosti, zajetih v tem pravilniku.

5.3.1 Homologacijski organ in njegove tehnične službe poleg meril iz Dodatka 2 k Sporazumu iz leta 1958 zagotovijo, da imajo:

(a) strokovno osebje z znanjem in spretnostmi na področju kibernetske varnosti ter specifično znanje o oceni tveganj v zvezi z avtomobili; ([1])

(b) izvedene postopke za enotno ocenjevanje v skladu s tem pravilnikom.

5.3.2 Vsaka pogodbenica, ki uporablja ta pravilnik, prek svojega homologacijskega organa drugim homologacijskim organom pogodbenic, ki uporabljajo ta pravilnik ZN, priglasi in jih obvesti o metodi in merilih, na podlagi katerih je priglasitveni organ ocenil primernost ukrepov, sprejetih v skladu s tem pravilnikom in zlasti odstavki 5.1, 7.2 in 7.3.

Te informacije se delijo (a) le pred prvo podelitvijo homologacije v skladu s tem pravilnikom in (b) vsakič, ko se posodobi metoda ali merila za ocenjevanje.

Te informacije naj bi se delile za namene zbiranja in analize dobrih praks ter zaradi zagotavljanja skladne uporabe tega pravilnika s strani vseh homologacijskih organov, ki ga uporabljajo.

5.3.3 Informacije iz odstavka 5.3.2 se pravočasno in najpozneje v 14 dneh pred prvo podelitvijo homologacije na podlagi zadevnih metod in meril ocenjevanja v angleškem jeziku naložijo v varno spletno podatkovno zbirko „DETA“ ([2]), ki jo je vzpostavila Ekonomska komisija Združenih narodov za Evropo. Informacije zadostujejo za razumevanje, katere minimalne ravni zmogljivosti je homologacijski organ sprejel za vsako posebno zahtevo iz odstavka 5.3.2, pa tudi postopke in ukrepe, ki jih uporablja za preverjanje, ali so te minimalne ravni zmogljivosti izpolnjene. ([3])

5.3.4 Homologacijski organi, ki prejmejo informacije iz odstavka 5.3.2, lahko priglastivenemu homologacijskemu organu pripombe predložijo tako, da jih v 14 dneh od dneva priglasitve naložijo v podatkovno zbirko DETA.

5.3.5 Če homologacijski organ, ki bo podelil homologacijo, ne more upoštevati pripomb, prejetih v skladu z odstavkom 5.3.4, homologacijski organi, ki so poslali pripombe, in homologacijski organ, ki bo podelil homologacijo, zahtevajo dodatna pojasnila v skladu z Dodatkom 6 k Sporazumu iz leta 1958. Ustrezna pomožna delovna skupina ([4]) Svetovnega foruma za harmonizacijo pravilnikov o vozilih (WP.29) za ta pravilnik se dogovori o skupni razlagi metod in meril ocenjevanja. ([5]) Navedena skupna razlaga se upošteva in vsi homologacijski organi v skladu s tem podelijo homologacije na podlagi tega pravilnika.

([1]) Npr. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Smernice o podrobnih informacijah (npr. metodi, merilih, ravni zmogljivosti), ki jih je treba naložiti, in formatu bodo zagotovljene v razlagalnem dokumentu, ki ga projektna skupina za kibernetsko varnost in vprašanja glede oddajanja prek radijskih valov pripravlja za sedmo sejo delovne skupine za avtomatizirana/avtonomna in povezana vozila (Working Party on Automated/Autonomous and Connected Vehicles – GRVA).
([4]) Delovna skupina za kibernetsko varnost in vprašanja glede oddajanja prek radijskih valov (GRVA).
([5]) Ta razlaga bo zajeta v razlagalnem dokumentu iz sprotne opombe k odstavku 5.3.3.

5.3.6 Vsak homologacijski organ, ki podeli homologacijo v skladu s tem pravilnikom, o podeljeni homologaciji obvesti druge homologacijske organe. Homologacijski organ homologacijo skupaj z dopolnilno dokumentacijo v angleškem jeziku v 14 dneh od dneva podelitve homologacije naloži v podatkovno zbirko DETA. ([6])

5.3.7 Pogodbenice lahko podeljene homologacije proučijo na podlagi informacij, naloženih v skladu z odstavkom 5.3.6. V primeru razhajanja mnenj med pogodbenicami se to uredi v skladu s členom 10 in Dodatkom 6 k Sporazumu iz leta 1958. Pogodbenice tudi obvestijo ustrezno pomožno delovno skupino Svetovnega foruma za harmonizacijo pravilnikov o vozilih (WP.29) o različnih razlagah v smislu Dodatka 6 k Sporazumu iz leta 1958. Ustrezna delovna skupina podpre uskladitev različnih mnenj in se o tem po potrebi posvetuje s forumom WP.29.

5.4 Proizvajalec za namene odstavka 7.2 tega pravilnika zagotovi, da se izvedejo vidiki kibernetske varnosti, zajeti v tem pravilniku.

6. Potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti

6.1 Pogodbenice imenujejo homologacijski organ, ki izvede oceno proizvajalca in izda potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti.

6.2 Vlogo za potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti vloži proizvajalec vozila ali njegov ustrezno pooblaščeni zastopnik.

6.3 Vlogi se v treh izvodih priložijo dokumenti, navedeni v nadaljevanju, in naslednji podatki:

6.3.1 dokumenti, v katerih je opisan sistem za upravljanje kibernetske varnosti;

6.3.2 podpisana izjava na podlagi vzorca iz Dodatka 1 k Prilogi 1.

6.4 Proizvajalec v okviru ocene z uporabo vzorca, kakor je opredeljen v Dodatku 1 k Prilogi 1, izjavi in homologacijskemu organu ali njegovi tehnični službi zadovoljivo dokaže, da ima potrebne postopke za izpolnjevanje vseh zahtev za kibernetsko varnost v skladu s tem pravilnikom.

6.5 Ko je ta ocena zadovoljivo opravljena in po prejemu podpisane izjave proizvajalca v skladu z vzorcem, kakor je opredeljen v Dodatku 1 k Prilogi 1, se proizvajalcu podeli potrdilo, imenovano potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti, kakor je opisano v Prilogi 4 k temu pravilniku (v nadaljnjem besedilu: potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti).

6.6 Homologacijski organ ali njegova tehnična služba za potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti uporabi vzorec iz Priloge 4 k temu pravilniku.

6.7 Potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti je veljavno največ tri leta od datuma izdaje, razen če je preklicano.

6.8 Homologacijski organ, ki je podelil potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti, lahko kadar koli preveri, ali so zahteve zanj še naprej izpolnjene. Homologacijski organ prekliče potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti, če zahteve iz tega pravilnika niso več izpolnjene.

([6]) Dodatne informacije o minimalnih zahtevah glede dokumentacije bo skupina GRVA pripravila na svoji sedmi seji.

6.9 Proizvajalec obvesti homologacijski organ ali njegovo tehnično službo o vsaki spremembi, ki bo vplivala na ustreznost potrdila o skladnosti za sistem za upravljanje kibernetske varnosti. Homologacijski organ ali njegova tehnična služba po posvetovanju s proizvajalcem odloči, ali so potrebna nova preverjanja.

6.10 Proizvajalec pravočasno zaprosi za novo potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti ali podaljšanje obstoječega potrdila, s čimer homologacijskemu organu dovoli, da zaključi oceno pred koncem obdobja veljavnosti potrdila o skladnosti za sistem za upravljanje kibernetske varnosti. Homologacijski organ na podlagi pozitivne ocene izda novo potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti ali podaljša njegovo veljavnost za nadaljnja tri leta. Preveri, ali sistem za upravljanje kibernetske varnosti še naprej izpolnjuje zahteve iz tega pravilnika. Izda novo potrdilo, če so bile njemu ali njegovi tehnični službi sporočene spremembe in če so bile te spremembe pozitivno ponovno ocenjene.

6.11 Kar zadeva tipe vozil, za katere je bil pomemben zadevni sistem za upravljanje kibernetske varnosti, se iztek veljavnosti ali preklic potrdila o skladnosti za sistem za upravljanje kibernetske varnosti šteje za spremembo homologacije iz odstavka 8, ki lahko vključuje preklic homologacije, če pogoji za podelitev homologacije niso več izpolnjeni.

7. Specifikacije

7.1 Splošne specifikacije

7.1.1 Zahteve iz tega pravilnika ne omejujejo določb ali zahtev iz drugih pravilnikov ZN.

7.2 Zahteve glede sistema za upravljanje kibernetske varnosti

7.2.1 Pri oceni homologacijski organ ali njegova tehnična služba preveri, ali ima proizvajalec vozil vzpostavljen sistem za upravljanje kibernetske varnosti, prav tako pa preveri njegovo skladnost s tem pravilnikom.

7.2.2 Sistem za upravljanje kibernetske varnosti zajema naslednje vidike:

7.2.2.1 Proizvajalec vozila homologacijskemu organu ali tehnični službi dokaže, da se njegov sistem za upravljanje kibernetske varnosti uporablja v naslednjih fazah:

(a) razvojni fazi;

(b) proizvodni fazi;

(c) poproizvodni fazi.

7.2.2.2 Proizvajalec vozila dokaže, da postopki, ki se uporabljajo v okviru njegovega sistema za upravljanje kibernetske varnosti, zagotavljajo ustrezno upoštevanje varnosti, vključno s tveganji in blažitvenimi ukrepi iz Priloge 5. To vključuje:

(a) postopke, ki se v organizaciji proizvajalca uporabljajo za upravljanje kibernetske varnosti;

(b) postopke, ki se uporabljajo za opredelitev tveganj za tipe vozil. V okviru teh postopkov se upoštevajo grožnje iz dela A Priloge 5 in druge ustrezne grožnje;

(c) postopke, uporabljene za oceno, kategorizacijo in obravnavo opredeljenih tveganj;

(d) postopke, vzpostavljene za preverjanje, ali se opredeljena tveganja ustrezno upravljajo;

(e) postopke, ki se uporabljajo za preizkušanje kibernetske varnosti tipa vozila;

(f) postopke, s katerimi se zagotavlja, da je ocena tveganja posodobljena;

(g) postopke, ki se uporabljajo za spremljanje, odkrivanje in odzivanje na kibernetske napade, kibernetske grožnje in ranljive točke na tipih vozila ter postopke, s katerimi se oceni, ali so izvedeni ukrepi za kibernetsko varnost še vedno učinkoviti glede na nove kibernetske grožnje in ranljive točke, ki so bile opredeljene;

(h) postopke, s katerimi se zagotovijo ustrezni podatki za podporo analizi poskusov kibernetskih napadov ali uspešnih kibernetskih napadov.

7.2.2.3 Proizvajalec vozila dokaže, da se bo s postopki, ki se uporabljajo v okviru njegovega sistema za upravljanje kibernetske varnosti, na podlagi kategorizacije iz odstavka 7.2.2.2(c) in (g) zagotovilo, da bodo kibernetske grožnje in ranljive točke, na katere se mora proizvajalec odzvati, odpravljene v razumnem časovnem okviru.

7.2.2.4 Proizvajalec vozila dokaže, da se bo s postopki, ki se uporabljajo v okviru njegovega sistema za upravljanje kibernetske varnosti, zagotovilo stalno spremljanje iz odstavka 7.2.2.2(g). To:

(a) pomeni, da so v spremljanje vključena vozila po prvi registraciji;

(b) vključuje zmožnost analiziranja in odkrivanja kibernetskih groženj, ranljivih točk in kibernetskih napadov na podlagi podatkov iz vozila in dnevnikov vozila. Ta zmožnost upošteva odstavek 1.3 in pravico lastnikov avtomobilov ali voznikov do zasebnosti, zlasti glede privolitve.

7.2.2.5 Proizvajalec vozila mora pokazati, kako se bodo v okviru njegovega sistema za upravljanje kibernetske varnosti upravljale odvisnosti, ki morda obstajajo s pogodbenimi dobavitelji, ponudniki storitev ali podorganizacijami proizvajalca, kar zadeva zahteve iz odstavka 7.2.2.2.

7.3 Zahteve glede tipov vozila

7.3.1 Proizvajalec ima veljavno potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti, pomemben za tip vozila v postopku homologacije. Če lahko proizvajalec vozila za homologacije vozil kategorij M, N in O, ki so bile prvič podeljene pred 1. julijem 2024, in za homologacije vozil kategorije L, ki so bile prvič podeljene pred 1. julijem 2029, ter za vsako njihovo razširitev dokaže, da tipa vozila ni bilo mogoče razviti v skladu s sistemom za upravljanje kibernetske varnosti, mora proizvajalec vozila dokazati, da je bila kibernetska varnost ustrezno upoštevana v fazi razvoja zadevnega tipa vozila.

7.3.2 Proizvajalec vozila za tip vozila v postopku homologacije opredeli in upravlja tveganja, povezana z dobavitelji.

7.3.3 Proizvajalec vozila opredeli kritične elemente tipa vozila in izvede izčrpno oceno tveganja za tip vozila ter ustrezno obravnava/upravlja opredeljena tveganja. V oceni tveganja se proučijo posamezni elementi tipa vozila in njihove interakcije. V oceni tveganja se nadalje prouči interakcija z zunanjimi sistemi. Proizvajalec vozila med ocenjevanjem tveganj prouči tveganja, povezana z vsemi grožnjami iz dela A Priloge 5, ter vsa druga ustrezna tveganja.

7.3.4 Proizvajalec vozil tip vozila zaščiti pred tveganji, opredeljenimi v oceni tveganja, ki jo je izvedel. Za zaščito tipa vozila se izvedejo sorazmerni blažitveni ukrepi. Izvedeni blažitveni ukrepi vključujejo vse blažitvene ukrepe iz delov B in C Priloge 5, ki so pomembni za opredeljena tveganja. Če blažitveni ukrep iz dela B ali C Priloge 5 ni pomemben ali ne zadostuje za opredeljeno tveganje, proizvajalec vozila zagotovi, da se izvede drug ustrezen blažitveni ukrep.

Za homologacije vozil kategorij M, N in O, ki so bile prvič podeljene pred 1. julijem 2024, in za homologacije vozil kategorije L, ki so bile prvič podeljene pred 1. julijem 2029, ter za vsako njihovo razširitev proizvajalec vozila zlasti zagotovi, da je izveden drug blažitveni ukrep, če blažitveni ukrep iz Priloge 5, dela B ali C, tehnično ni izvedljiv. Proizvajalec ustrezno oceno tehnične izvedljivosti predloži homologacijskemu organu.

7.3.5 Proizvajalec vozila vzpostavi ustrezne in sorazmerne ukrepe za zaščito namenskih okolij na tipu vozila (če so na voljo) za shranjevanje in izvajanje poprodajne programske opreme, storitev, aplikacij ali podatkov.

7.3.6 Proizvajalec vozila pred homologacijo izvede ustrezne in zadostne preizkuse za preverjanje učinkovitosti izvedenih varnostnih ukrepov.

7.3.7 Proizvajalec vozila za tip vozila izvede ukrepe za:

(a) odkrivanje in preprečevanje kibernetskih napadov na vozila zadevnega tipa;

(b) podpiranje zmogljivosti proizvajalca vozila za spremljanje, kar zadeva odkrivanje groženj, ranljivih točk in kibernetskih napadov, pomembnih za tip vozila;

(c) zagotavljanje podatkov o forenzični zmogljivosti, da se omogoči analiza poskusov kibernetskih napadov ali uspešnih kibernetskih napadov.

7.3.8 Kriptografski moduli, ki se uporabljajo za namene tega pravilnika, so v skladu s sporazumnimi standardi. Če uporabljeni kriptografski moduli niso v skladu s sporazumnimi standardi, proizvajalec vozila utemelji njihovo uporabo.

7.4 Določbe o poročanju

7.4.1 Proizvajalec vozila vsaj enkrat letno ali po potrebi pogosteje homologacijskemu organu ali tehnični službi poroča o rezultatih svojih dejavnosti spremljanja, kakor so opredeljene v odstavku 7.2.2.2(g), kar vključuje ustrezne informacije o novih kibernetskih napadih. Proizvajalec vozila homologacijskemu organu ali tehnični službi tudi sporoči in potrdi, da so blažitveni ukrepi za kibernetsko varnost, ki jih je izvedel za svoje tipe vozil, še vedno učinkoviti, in ju obvesti o vseh sprejetih dodatnih ukrepih.

7.4.2 Homologacijski organ ali tehnična služba preveri predložene informacije in po potrebi od proizvajalca vozil zahteva odpravo morebitne odkrite neučinkovitosti.

Če poročanje ali odgovor ne zadostujeta, se lahko homologacijski organ odloči, da prekliče potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti v skladu z odstavkom 6.8.

8. Sprememba tipa vozila in razširitev homologacije

8.1 Vsaka sprememba tipa vozila, ki vpliva na njegovo tehnično zmogljivost glede kibernetske varnosti in/ali dokumentacije, zahtevane v tem pravilniku, se sporoči homologacijskemu organu, ki je homologiral zadevni tip vozila. Homologacijski organ lahko nato:

8.1.1 meni, da so izvedene spremembe še vedno v skladu z zahtevami in dokumentacijo obstoječe homologacije ali

8.1.2 izvede potrebno dopolnilno oceno v skladu z odstavkom 5 in po potrebi od tehnične službe, pristojne za izvajanje preizkusov, zahteva dodatno poročilo o preizkusu.

8.1.3 Potrditev, razširitev ali zavrnitev homologacije se z navedbo sprememb sporoči s sporočilom na obrazcu, ki je v skladu z vzorcem iz Priloge 2 k temu pravilniku. Homologacijski organ, ki izda razširitev homologacije, dodeli serijsko številko za tako razširitev in o tem obvesti druge pogodbenice Sporazuma iz leta 1958, ki uporabljajo ta pravilnik, s sporočilom na obrazcu, ki je v skladu z vzorcem iz Priloge 2 k temu pravilniku.

9. Skladnost proizvodnje

9.1 Postopki preverjanja skladnosti proizvodnje morajo biti v skladu s postopki iz Dodatka 1 k Sporazumu iz leta 1958 (E/ECE/TRANS/505/Rev.3) ob upoštevanju naslednjih zahtev:

9.1.1 Imetnik homologacije zagotovi, da se rezultati preizkusov o skladnosti proizvodnje zapisujejo in da so priloženi dokumenti na voljo za obdobje, dogovorjeno s homologacijskim organom ali njegovo tehnično službo. To obdobje ne sme biti daljše od deset let po dokončnem prenehanju proizvodnje.

9.1.2 Homologacijski organ, ki je podelil homologacijo, lahko kadar koli preveri metode preverjanja skladnosti, ki se uporabljajo v vsakem proizvodnem obratu. Ta preverjanja se običajno opravijo enkrat na tri leta.

10. Kazni za neskladnost proizvodnje

10.1 Homologacija, ki je bila podeljena za tip vozila v skladu s tem pravilnikom, se lahko prekliče, če zahteve iz tega pravilnika niso izpolnjene ali če vzorčna vozila niso skladna z zahtevami iz tega pravilnika.

10.2 Če homologacijski organ prekliče homologacijo, ki jo je predhodno podelil, o tem nemudoma uradno obvesti pogodbenice, ki uporabljajo ta pravilnik, s sporočilom na obrazcu, ki je v skladu z vzorcem iz Priloge 2 k temu pravilniku.

11. Dokončno prenehanje proizvodnje

11.1 Če imetnik homologacije povsem preneha proizvajati tip vozila, za katerega je bila podeljena homologacija v skladu s tem pravilnikom, o tem obvesti organ, ki je podelil homologacijo. Ko navedeni organ prejme ustrezno sporočilo, mora o tem obvestiti druge pogodbenice Sporazuma, ki uporabljajo ta pravilnik, tako da jim pošlje izvod homologacijskega obrazca, ki na koncu vsebuje z velikimi črkami napisano opombo „PRENEHANJE PROIZVODNJE“, opremljeno s podpisom in datumom.

12. Nazivi in naslovi tehničnih služb, ki izvajajo homologacijski preizkus, in homologacijskih organov

12.1 Pogodbenice Sporazuma, ki uporabljajo ta pravilnik, sekretariatu Združenih narodov sporočijo nazive in naslove tehničnih služb, ki izvajajo homologacijske preizkuse, ter homologacijskih organov, ki podeljujejo homologacije in ki se jim pošljejo obrazci, ki potrjujejo podelitev, razširitev, zavrnitev ali preklic homologacije v drugih državah.

PRILOGA 1

Opisni list

Naslednje informacije, če so potrebne, se predložijo v treh izvodih skupaj s seznamom priloženih dokumentov. Vse risbe so v ustreznem merilu in dovolj podrobne ter v formatu A4 ali zložene na format A4. Morebitne fotografije morajo biti dovolj podrobne.

1. Znamka (blagovno ime proizvajalca): .....

2. Tip in splošne trgovske oznake: .....

3. Oznake za identifikacijo tipa, če je oznaka na vozilu: .....

4. Mesto navedene oznake:.....

5. Kategorije vozila: .....

6. Naziv in naslov proizvajalca / zastopnika proizvajalca:.....

7. Nazivi in naslovi proizvodnih obratov:.....

8. Fotografije in/ali risbe reprezentativnega vozila:.....

9. Kibernetska varnost

9.1 Splošni konstrukcijski podatki o tipu vozila, vključno s:

(a) sistemi v vozilu, ki so pomembni za kibernetsko varnost tipa vozila;

(b) sestavnimi deli navedenih sistemov, ki so pomembni za kibernetsko varnost;

(c) interakcijami navedenih sistemov z drugimi sistemi znotraj tipa vozila in zunanjimi vmesniki.

9.2 Shematski prikaz tipa vozila

9.3 Številka potrdila o skladnosti za sistem za upravljanje kibernetske varnosti: .....

9.4 Dokumenti za tip vozila v postopku homologacije, v katerih so opisani rezultat ocene tveganja tipa vozila in opredeljena tveganja: .....

9.5 Dokumenti za tip vozila v postopku homologacije, v katerih so opisani blažitveni ukrepi, ki so bili izvedeni na navedenih sistemih ali za tip vozila, in način, kako so z njimi obravnavana navedena tveganja: .....

9.6 Dokumenti za tip vozila v postopku homologacije, v katerih je opisana zaščita namenskih okolij za poprodajno programsko opremo, storitve, aplikacije ali podatke:.....

9.7 Dokumenti za tip vozila v postopku homologacije, v katerih je opisano, s katerimi preizkusi se je preverila kibernetska varnost tipa vozila in njegovih sistemov ter rezultat navedenih preizkusov:.....

9.8 Opis upoštevanja dobavne verige glede kibernetske varnosti: .....

Priloga 1 – Dodatek 1

Vzorec izjave proizvajalca o skladnosti za sistem za upravljanje kibernetske varnosti

Izjava proizvajalca o skladnosti z zahtevami glede sistema za upravljanje kibernetske varnosti

Naziv proizvajalca:.....

Naslov proizvajalca: .....

..... (*naziv proizvajalca*)

potrjujem, da so potrebni postopki za skladnost z zahtevami glede sistema za upravljanje kibernetske varnosti iz odstavka 7.2 Pravilnika ZN št. 155 vzpostavljeni in bodo vzdrževani.

V/na: ..... (*kraj*)

Datum:.....

Ime podpisnika:.....

Funkcija podpisnika:.....

(Žig in podpis zastopnika proizvajalca)

PRILOGA 2

Sporočilo

(največji format: A4 (210 × 297 mm))



Izdal: naziv homologacijskega organa:
……
……
……

o: (2) podeljeni homologaciji
razširjeni homologaciji
preklicani homologaciji z učinkom od dd. mm. llll
zavrnjeni homologaciji
dokončnem prenehanju proizvodnje

tipa vozila v skladu s Pravilnikom ZN št. 155

Št. homologacije: ……

Št. razširitve: ……

Razlog za razširitev: ……

1. Znamka (blagovno ime proizvajalca): ……

2. Tip in splošne trgovske oznake ……

3. Oznake za identifikacijo tipa, če je oznaka na vozilu: ……

3.1 Mesto navedene oznake: ……

4. Kategorije vozila: ……

5. Naziv in naslov proizvajalca / zastopnika proizvajalca: ……

6. Nazivi in naslovi proizvodnih obratov: ……

7. Številka potrdila o skladnosti za sistem za upravljanje kibernetske varnosti: ……

8. Tehnična služba, pristojna za izvajanje preizkusov: ……

9. Datum poročila o preizkusu: ……

10. Številka poročila o preizkusu: ……

11. Morebitne opombe: ……

12. Kraj: ……

(1) Številčna oznaka države, ki je podelila/razširila/zavrnila/preklicala homologacijo (glej določbe o homologaciji v Pravilniku).
(2) Neustrezno črtati.

13. Datum: .....

14. Podpis:.....

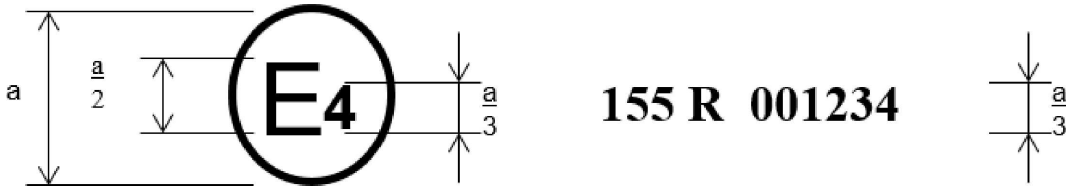
15. Priložen je seznam opisne dokumentacije, ki je shranjen pri homologacijskem organu in se lahko pridobi na zahtevo:

PRILOGA 3

Namestitev homologacijske oznake

VZOREC A

(Glej odstavek 4.2 tega pravilnika)



a = najmanj 8 mm

Zgornja homologacijska oznaka, pritrjena na vozilo, pomeni, da je bil zadevni tip cestnega vozila homologiran na Nizozemskem (E4) v skladu s Pravilnikom št. 155 in pod homologacijsko številko 001234. Prvi dve števki številke homologacije pomenita, da je bila homologacija podeljena v skladu z zahtevami iz tega pravilnika v njegovi prvotni obliki (00).

PRILOGA 4

VZOREC POTRDILA O SKLADNOSTI ZA SISTEM ZA UPRAVLJANJE KIBERNETSKE VARNOSTI

Potrdilo o skladnosti za sistem za upravljanje kibernetske varnosti

s Pravilnikom ZN št. 155

Številka potrdila [*referenčna številka*]

[……. *homologacijski organ*]

potrjuje, da

proizvajalec: ……

naslov proizvajalca:……

izpolnjuje določbe odstavka 7.2 Pravilnika ZN št. 155.

Preverjanje je dne: ……

opravil (naziv in naslov homologacijskega organa ali tehnične službe): ……

Številka poročila:……

To potrdilo velja do […… *datum*]

V […… *kraj*]

dne […… *datum*]

[…… *podpis*]

Priloge: opis sistema za upravljanje kibernetske varnosti, ki ga predloži proizvajalec.

PRILOGA 5

Seznam groženj in ustreznih blažitvenih ukrepov

1. Ta priloga je sestavljena iz treh delov. V delu A te priloge so opisani osnova za grožnje, ranljive točke in metode napadov. V delu B te priloge so opisani blažitveni ukrepi za grožnje, namenjeni za tipe vozil. V delu C so opisani blažitveni ukrepi za grožnje, namenjeni za območja zunaj vozil, npr. na zalednih informacijskih sistemih.

2. Deli A, B in C se upoštevajo pri oceni tveganja in blažitvenih ukrepih, ki jih morajo izvesti proizvajalci vozil.

3. Podroben opis ranljive točke in njeni ustrezni primeri so navedeni v delu A. Enake navedbe so uporabljene v preglednicah v delih B in C, tako da se vsak napad/ranljiva točka poveže s seznamom ustreznih blažitvenih ukrepov.

4. V analizi grožnje se upoštevajo tudi možni učinki napada. Ti lahko pomagajo ugotoviti resnost tveganja in opredeliti dodatna tveganja. Možni učinki napada lahko vključujejo naslednje:

   (a) prizadeto je varno delovanje vozila;

   (b) delovati prenehajo funkcije vozila;

   (c) programska oprema in zmogljivost sta spremenjeni;

   (d) programska oprema je spremenjena, vendar ni operativnih učinkov;

   (e) kršena je celovitost podatkov;

   (f) kršena je zaupnost podatkov;

   (g) podatki niso več na voljo;

   (h) drugo, vključno s kriminaliteto.

DEL A.

Ranljiva točka ali metoda napada, povezana z grožnjami

Podrobni opisi groženj in povezane ranljive točke ali metode napada so navedeni v preglednici A1.

Preglednica A1

Seznam ranljivih točk ali metod napada, povezanih z grožnjami

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
4.3.1 Grožnje v zvezi z zalednimi strežniki, povezane z vozili na terenu	1.	Zaledni strežniki se uporabijo kot sredstvo za napad na vozilo ali za pridobivanje podatkov.	1.1	Zloraba privilegijev s strani osebja (notranji napad).
			1.2	Nepooblaščen internetni dostop do strežnika (ki ga npr. omogočijo stranska vrata, nepopravljene ranljive točke v programski opremi sistema, napadi SQL ali druga sredstva).
			1.3	Nepooblaščen fizični dostop do strežnika (npr. prek ključa USB ali drugega medija, ki se poveže s strežnikom).
	2.	Motene so storitve zalednega strežnika, kar vpliva na delovanje vozila.	2.1	Napad na zaledni strežnik ustavi njegovo delovanje, mu na primer prepreči interakcijo z vozili in zagotavljanje storitev, od katerih so vozila odvisna.

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
	3.	Podatki v zvezi z vozilom na zalednih strežnikih so izgubljeni ali ogroženi (v nadaljnjem besedilu: kršitev varnosti podatkov).	3.1	Zloraba privilegijev s strani osebja (notranji napad).
			3.2	Izguba informacij v oblaku. Če podatke hranijo neodvisni ponudniki storitev v oblaku, se lahko zaradi napadov ali nesreč izgubijo občutljivi podatki.
			3.3	Nepooblaščen internetni dostop do strežnika (ki ga npr. omogočijo stranska vrata, nepopravljene ranljive točke v programski opremi sistema, napadi SQL ali druga sredstva).
			3.4	Nepooblaščen fizični dostop do strežnika (npr. prek ključa USB ali drugega medija, ki se poveže s strežnikom).
			3.5	Kršitev varnosti informacij z nenamerno izmenjavo podatkov (npr. napake skrbnika).
4.3.2 Grožnje vozilom v zvezi z njihovimi komunikacijskimi kanali	4.	Zakrinkanje sporočil ali podatkov, ki jih prejme vozilo.	4.1	Zakrinkanje sporočil s poosebljanjem (npr. sporočil V2X sodelovalne izmenjave podatkov ali usklajevanja manevrov, sporočil GNSS).
			4.2	Napad, pri katerem vsiljivec ustvari lažne identitete več vozil (s čimer druga vozila zavaja, da je na cesti veliko vozil; t. i. Sybil attack).
	5.	Komunikacijski kanali, ki se uporabljajo za nepooblaščeno manipulacijo s kodo/podatki v vozilu ali njihovo brisanje ali druge spremembe.	5.1	Komunikacijski kanali dovoljujejo vrivanje kode, na primer v komunikacijski tok se lahko vrine spremenjena strojna koda programske opreme.
			5.2	Komunikacijski kanali omogočajo manipulacijo s podatki/kodo v vozilu.
			5.3	Komunikacijski kanali omogočajo prepis podatkov/kode v vozilu.
			5.4	Komunikacijski kanali omogočajo brisanje podatkov/kode v vozilu.
			5.5	Komunikacijski kanali omogočajo vnos podatkov/kode v vozilo (pisanje podatkovne kode).
	6.	Komunikacijski kanali omogočajo sprejemanje sporočil, ki niso zaupanja vredna / so nezanesljiva ali pa so ranljiva za napade, katerih cilj je ugrabitev/ponavljanje seje.	6.1	Sprejemanje informacij iz nezanesljivega vira ali vira, ki ni vreden zaupanja.
			6.2	Napad s posrednikom/ugrabitev seje.
			6.3	Napad s ponavljanjem, na primer napad na komunikacijski vmesnik, napadalcu omogoča, da poslabša učinkovitost programske opreme elektronske krmilne enote ali vdelane programske opreme vmesnika.
	7.	Informacije je mogoče zlahka razkriti. Na primer s prisluškovanjem komunikacijam ali z omogočanjem nepooblaščenega dostopa do občutljivih datotek ali map.	7.1	Prestrezanje informacij/moteče sevanje/spremljanje komunikacij.
			7.2	Nepooblaščen dostop do datotek ali podatkov.

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
	8.	Napadi z zavrnitvijo storitve prek komunikacijskih kanalov zaradi motenj v delovanju vozila.	8.1	Pošiljanje velike količine odpadnih podatkov informacijskemu sistemu vozila, tako da ne more zagotavljati storitev kot običajno.
			8.2	Napad s črno luknjo, pri katerem lahko napadalec, da bi motil komunikacijo z vozili, blokira sporočila med vozili.
	9.	Nepooblaščen uporabnik lahko pridobi pooblaščen dostop do sistemov v vozilu.	9.1	Nepooblaščen uporabnik lahko pridobi pooblaščen dostop, na primer dostop do korenske mape.
	10.	Virusi, vdelani v komunikacijska sredstva, lahko okužijo sisteme v vozilu.	10.1	Virus, vdelan v komunikacijska sredstva, okuži sisteme v vozilu.
	11.	Sporočila, ki jih prejema vozilo (npr. sporočila X2V ali diagnostična sporočila) ali se znotraj njega prenašajo, vsebujejo zlonamerno vsebino.	11.1	Zlonamerna notranja sporočila (npr. CAN).
			11.2	Zlonamerna sporočila V2X, na primer sporočila infrastrukture vozilu ali sporočila vozila vozilu (npr. CAM, DENM).
			11.3	Zlonamerna diagnostična sporočila.
			11.4	Zlonamerna lastniška sporočila (npr. tista, ki jih običajno pošlje proizvajalec originalne opreme ali dobavitelj sestavnega dela/sistema/funkcije).
4.3.3 Grožnje vozilom v zvezi z njihovimi postopki posodobitve	12.	Zloraba ali ogrožanje varnosti postopkov posodobitve.	12.1	Ogrožanje varnosti postopkov brezžične posodobitve programske opreme. To vključuje ponarejanje programa za posodobitev sistema ali vdelane programske opreme.
			12.2	Ogrožanje varnosti lokalnih/fizičnih postopkov posodobitve programske opreme. To vključuje ponarejanje programa za posodobitev sistema ali vdelane programske opreme.
			12.3	S programsko opremo se pred postopkom posodobitve manipulira (in je zato poškodovana), čeprav je postopek posodobitve nedotaknjen.
			12.4	Ogrožanje varnosti kriptografskih ključev ponudnika programske opreme, da se omogoči neveljavna posodobitev.
	13.	Zavrniti je mogoče zakonite posodobitve.	13.1	Napad z zavrnitvijo storitve proti strežniku ali omrežju za posodobitev, da se prepreči uvajanje kritičnih posodobitev programske opreme in/ali odklenejo funkcije, specifične za stranke.
4.3.4 Grožnje vozilom v zvezi z nenamernimi človeškimi dejanji, ki olajšajo kibernetski napad	15.	Zakoniti akterji lahko sprejmejo ukrepe, ki bi nenamerno olajšali kibernetski napad.	15.1	Nedolžna žrtev (npr. lastnik, operater ali inženir za vzdrževanje) je zavedena, da sprejme ukrep, s katerim nenamerno naloži zlonamerno programsko opremo ali omogoči napad.
			15.2	Opredeljeni varnostni postopki se ne upoštevajo.

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
4.3.5 Grožnje vozilom v zvezi z njihovo zunanjo povezljivostjo in povezavami	16.	Manipulacija s povezljivostjo funkcij vozila omogoča kibernetski napad, kar lahko vključuje telematiko, sisteme, ki omogočajo delovanje na daljavo, in sisteme, ki uporabljajo brezžične komunikacije kratkega dosega.	16.1	Manipulacija s funkcijami za daljinsko upravljanje sistemov, kot so daljinski ključ, naprava za imobilizacijo in polnilnica.
			16.2	Manipulacija s telematiko vozila (npr. manipulacija z merjenjem temperature občutljivega blaga, odklepanje vrat prtljažnika na daljavo).
			16.3	Motenje delovanja brezžičnih sistemov ali senzorjev kratkega dosega.
	17.	Gostujoča programska oprema tretjih oseb, npr. aplikacije za prosti čas, se uporabi kot sredstvo za napade na sisteme vozila.	17.1	Poškodovane aplikacije ali aplikacije s slabo varnostjo programske opreme, ki se uporabijo kot sredstvo za napade na sisteme vozila.
	18.	Naprave, povezane z zunanjimi vmesniki, na primer vrata USB, vrata OBD, se uporabijo kot sredstvo za napade na sisteme vozila.	18.1	Zunanji vmesniki, kot so vrata USB ali druga vrata, se uporabijo kot točka napada, na primer z vrivanjem kode.
			18.2	Mediji, okuženi z virusom, se povežejo s sistemom vozila.
			18.3	Diagnostični dostop (npr. zaščitni ključi za vrata OBD), uporabljen za olajšanje napada, na primer manipulacije s parametri vozila (neposredno ali posredno).
4.3.6 Grožnje podatkom/ kodi vozila	19.	Pridobivanje podatkov/kode vozila.	19.1	Pridobivanje avtorske ali lastniške programske opreme iz sistemov vozila (piratstvo izdelkov).
			19.2	Nepooblaščen dostop do zasebnih podatkov lastnika, kot so osebna identiteta, podatki o plačilnem računu, podatki iz imenika, podatki o lokaciji, elektronska identifikacija vozila itd.
			19.3	Pridobivanje kriptografskih ključev.
	20.	Manipulacija s podatki/kodo vozila.	20.1	Nezakonite/nepooblaščene spremembe elektronske identifikacije vozila.
			20.2	Identitetna prevara. Če na primer uporabnik želi prikazati drugo identiteto pri komunikaciji s sistemi cestninjenja ali zalednim sistemom proizvajalca.
			20.3	Ukrepi za izogibanje nadzornim sistemom (npr. vdiranje/spreminjanje/blokiranje sporočil, kot so podatki sledilnika snemalnika operativnih podatkov ali število zagonov).
			20.4	Manipulacija s podatki za ponarejanje podatkov iz vozila o vožnji (npr. kilometrina, hitrost vožnje, navodila za vožnjo.).
			20.5	Nepooblaščene spremembe diagnostičnih podatkov sistema.
	21.	Izbris podatkov/kode.	21.1	Nepooblaščeno brisanje/manipulacija dnevnikov sistemskih dogodkov.
	22.	Uvedba zlonamerne programske opreme.	22.2	Uvedba zlonamerne programske opreme ali dejavnost zlonamerne programske opreme.

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
	23.	Uvedba nove programske opreme ali prepisovanje obstoječe programske opreme.	23.1	Ponarejanje programske opreme nadzornega sistema ali informacijskega sistema vozila.
	24.	Motenje sistemov ali operacij.	24.1	Zavrnitev storitve, kar se lahko na primer sproži na notranjem omrežju s preplavljanjem področnega krmilnega omrežja ali spodbujanjem napak na elektronski krmilni enoti s pogostim pošiljanjem sporočil.
	25.	Manipulacija s parametri vozila.	25.1	Nepooblaščen dostop za ponarejanje konfiguracijskih parametrov ključnih funkcij vozila, kot so podatki o zavorah, prag sprožitve zračne blazine.
			25.2	Nepooblaščen dostop za ponarejanje parametrov polnjenja, kot so napetost polnjenja, moč polnjenja, temperatura akumulatorja.
4.3.7 Potencialne ranljive točke, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene	26.	Ogrožena je lahko varnost kriptografskih tehnologij ali pa se te tehnologije nezadostno uporabljajo.	26.1	Kombinacija kratkih šifrirnih ključev in dolgega obdobja veljavnosti napadalcu omogoča, da dešifrira šifriranje.
			26.2	Nezadostna uporaba kriptografskih algoritmov za zaščito občutljivih sistemov.
			26.3	Uporaba že zastarelih ali kmalu zastarelih kriptografskih algoritmov.
	27.	Ogrožena bi lahko bila varnost delov ali zaloge, kar bi omogočilo napad na vozila.	27.1	Strojna ali programska oprema, ki je zasnovana tako, da omogoča napad, ali ki ne izpolnjuje meril glede zasnove za zaustavitev napada.
	28.	Razvoj programske ali strojne opreme omogoča ranljive točke.	28.1	Napake programske opreme. Prisotnost napak v programski opremi je lahko osnova za ranljive točke, ki jih je morda mogoče izkoristiti. To velja zlasti, če programska oprema ni bila preizkušena, s čimer bi se preverilo, da znana slaba koda/napake niso prisotne, in zmanjšalo tveganje prisotnosti neznanih slabih kod/napak.
			28.2	Uporaba preostalih elementov pri razvoju (npr. vrata za odpravljanje napak, vrata JTAG, mikroprocesorji, razvojni certifikati, gesla za razvijalce ...) lahko omogoči dostop do elektronskih krmilnih enot ali napadalcem omogoči, da pridobijo večje pravice.
	29.	Zaradi zasnove omrežja so prisotne ranljive točke.	29.1	Odvečna internetna vrata ostanejo odprta in omogočajo dostop do omrežnih sistemov.
			29.2	Zaobide se ločitev omrežja, da se pridobi nadzor. Konkreten primer je uporaba nezaščitenih prehodov ali točk dostopa (kot so prehodi med tovornjakom in prikolico), da se zaobidejo zaščite in pridobi dostop do drugih segmentov omrežja ter izvedejo zlonamerna dejanja, kot je pošiljanje poljubnih sporočil področnega krmilnega omrežja.
	31.	Pride lahko do nenamernega prenosa podatkov.	31.1	Kršitev varnosti informacij. Osebni podatki lahko uhajajo, ko avto zamenja uporabnika (npr. se proda ali se uporablja kot vozilo za najem in so najemniki novi).

Podroben in nadalje razčlenjen opis ranljive točke/grožnje			Primer ranljive točke ali metode napada	
	32.	Fizična manipulacija s sistemi lahko omogoči napad.	32.1	Manipulacija z elektronsko strojno opremo, v vozilo se na primer doda nepooblaščena elektronska strojna oprema, ki omogoča napad s posrednikom. Zamenjava pooblaščene elektronske strojne opreme (npr. senzorjev) z nepooblaščeno elektronsko strojno opremo. Manipulacija z informacijami, ki jih zbere senzor (npr. z magnetom za poseg v Hallov senzor, priključen na menjalnik).

DEL B

Blažitveni ukrepi za grožnje, namenjeni za vozila

1. Blažitveni ukrepi za „komunikacijske kanale vozila“

Blažitveni ukrepi za grožnje, povezane s „komunikacijskimi kanali vozila“, so navedeni v preglednici B1.

Preglednica B1

Blažitveni ukrepi za grožnje, povezane s „komunikacijskimi kanali vozila“

Sklic na preglednico A1	Grožnje, povezane s „komunikacijskimi kanali vozila“	Sklic	Blažitveni ukrep
4.1	Zakrinkanje sporočil (npr. sporočil V2X sodelovalne izmenjave podatkov ali usklajevanja manevrov, sporočil GNSS) s poosebljanjem.	M10	Vozilo preveri pristnost in celovitost prejetih sporočil.
4.2	Napad, pri katerem vsiljivec ustvari lažne identitete več vozil (s čimer druga vozila zavaja, da je na cesti veliko vozil; t. i. Sybil attack).	M11	Pri shranjevanju kriptografskih ključev se izvaja varnostni nadzor (npr. uporaba varnostnih modulov strojne opreme).
5.1	Komunikacijski kanali dovoljujejo vrivanje kode v podatke/kodo v vozilu, na primer v komunikacijski tok se lahko vrine spremenjena binarna vrednost programske opreme.	M10 M6	Vozilo preveri pristnost in celovitost prejetih sporočil. Sistemi izvajajo vgrajeno varnost, da minimizirajo tveganja.
5.2	Komunikacijski kanali omogočajo manipulacijo s podatki/kodo v vozilu.	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom.
5.3	Komunikacijski kanali omogočajo prepis podatkov/kode v vozilu.		
5.4 21.1	Komunikacijski kanali omogočajo brisanje podatkov/kode v vozilu.		
5.5	Komunikacijski kanali omogočajo vnos podatkov/kode v sisteme vozila (pisanje podatkovne kode).		

Sklic na preglednico A1	Grožnje, povezane s „komunikacijskimi kanali vozila“	Sklic	Blažitveni ukrep
6.1	Sprejemanje informacij iz nezanesljivega vira ali vira, ki ni vreden zaupanja.	M10	Vozilo preveri pristnost in celovitost prejetih sporočil.
6.2	Napad s posrednikom/ugrabitev seje.	M10	Vozilo preveri pristnost in celovitost prejetih sporočil.
6.3	Napad s ponavljanjem, na primer napad na komunikacijski vmesnik, napadalcu omogoča, da poslabša učinkovitost programske opreme elektronske krmilne enote ali vdelane programske opreme vmesnika.		
7.1	Prestrezanje informacij/moteče sevanje/spremljanje komunikacij.	M12	Zaščitijo se zaupni podatki, ki se prenašajo v vozilo ali iz njega.
7.2	Nepooblaščen dostop do datotek ali podatkov.	M8	Z zasnovo sistema in nadzorom nad dostopom bi se moral nepooblaščenemu osebju preprečiti dostop do osebnih podatkov ali podatkov, kritičnih za sistem. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
8.1	Pošiljanje velike količine odpadnih podatkov informacijskemu sistemu vozila, tako da ne more zagotavljati storitev kot običajno.	M13	Izvesti bi bilo treba ukrepe za odkrivanje napada z zavrnitvijo storitve in okrevanje po njem.
8.2	Napad s črno luknjo, tj. motenje komunikacije med vozili z blokiranjem prenosa sporočil drugim vozilom.	M13	Izvesti bi bilo treba ukrepe za odkrivanje napada z zavrnitvijo storitve in okrevanje po njem.
9.1	Nepooblaščen uporabnik lahko pridobi pooblaščen dostop, na primer dostop do korenske mape.	M9	Izvesti bi bilo treba ukrepe za preprečevanje in odkrivanje nepooblaščenega dostopa.
10.1	Virus, vdelan v komunikacijska sredstva, okuži sisteme v vozilu.	M14	Proučiti bi bilo treba ukrepe za zaščito sistemov pred vdelanimi virusi/zlonamerno programsko opremo.
11.1	Zlonamerna notranja sporočila (npr. CAN).	M15	Proučiti bi bilo treba ukrepe za odkrivanje zlonamernih notranjih sporočil ali dejavnosti.
11.2	Zlonamerna sporočila V2X, na primer sporočila infrastrukture vozilu ali sporočila vozila vozilu (npr. CAM, DENM).	M10	Vozilo preveri pristnost in celovitost prejetih sporočil.
11.3	Zlonamerna diagnostična sporočila.		
11.4	Zlonamerna lastniška sporočila (npr. tista, ki jih običajno pošlje proizvajalec originalne opreme ali dobavitelj sestavnega dela/sistema/funkcije).		

2. Blažitveni ukrepi za „postopek posodobitve“

Blažitveni ukrepi za grožnje, povezane s „postopkom posodobitve“, so navedeni v preglednici B2.

Preglednica B2

Blažitveni ukrepi za grožnje, povezane s „postopkom posodobitve“

Sklic na preglednico A1	Grožnje, povezane s „postopkom posodobitve“	Sklic	Blažitveni ukrep
12.1	Ogrožanje varnosti postopkov brezžične posodobitve programske opreme. To vključuje ponarejanje programa za posodobitev sistema ali vdelane programske opreme.	M16	Uporabijo se varni postopki posodobitve programske opreme.
12.2	Ogrožanje varnosti lokalnih/fizičnih postopkov posodobitve programske opreme. To vključuje ponarejanje programa za posodobitev sistema ali vdelane programske opreme.		
12.3	S programsko opremo se pred postopkom posodobitve manipulira (in je zato poškodovana), čeprav je postopek posodobitve nedotaknjen.		
12.4	Ogrožanje varnosti kriptografskih ključev ponudnika programske opreme, da se omogoči neveljavna posodobitev.	M11	Pri shranjevanju kriptografskih ključev se izvaja varnostni nadzor.
13.1	Napad z zavrnitvijo storitve proti strežniku ali omrežju za posodobitev, da se prepreči uvajanje kritičnih posodobitev programske opreme in/ali odklenejo funkcije, specifične za stranke.	M3	Za zaledne sisteme se uporablja varnostni nadzor. Kadar so zaledni strežniki ključnega pomena za zagotavljanje storitev, so vzpostavljeni obnovitveni ukrepi v primeru izpada sistema. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).

3. Blažitveni ukrepi za „nenamerna človeška dejanja, ki olajšajo kibernetski napad“

Blažitveni ukrepi za grožnje, povezane s „nenamernimi človeškimi dejanji, ki olajšajo kibernetski napad“, so navedeni v preglednici B3.

Preglednica B3

Blažitveni ukrepi za grožnje, povezane z „nenamernimi človeškimi dejanji, ki olajšajo kibernetski napad“

Sklic na preglednico A1	Grožnje, povezane z „nenamernimi človeškimi dejanji“	Sklic	Blažitveni ukrep
15.1	Nedolžna žrtev (npr. lastnik, operater ali inženir za vzdrževanje) je zavedena, da sprejme ukrep, s katerim nenamerno naloži zlonamerno programsko opremo ali omogoči napad.	M18	Izvedejo se ukrepi za opredelitev vlog uporabnikov in njihovih pravic dostopa ter nadzor nad njimi na podlagi načela najmanjše pravice do dostopa.

Sklic na preglednico A1	Grožnje, povezane z „nenamernimi človeškimi dejanji“	Sklic	Blažitveni ukrep
15.2	Opredeljeni varnostni postopki se ne upoštevajo.	M19	Organizacije zagotovijo, da se opredelijo in upoštevajo varnostni postopki, vključno z beleženjem dejanj in dostopom, povezanim z upravljanjem varnostnih funkcij.

4. Blažitveni ukrepi za „zunanjo povezljivost in povezave“

Blažitveni ukrepi za grožnje, povezane z „zunanjo povezljivostjo in povezavami“, so navedeni v preglednici B4.

Preglednica B4

Blažitveni ukrepi za grožnje, povezane z „zunanjo povezljivostjo in povezavami“

Sklic na preglednico A1	Grožnje, povezane z „zunanjo povezljivostjo in povezavami“	Sklic	Blažitveni ukrep
16.1	Manipulacija s funkcijami za daljinsko upravljanje sistemov v vozilu, kot so daljinski ključ, naprava za imobilizacijo in polnilnica.	M20	Nad sistemi, ki imajo oddaljen dostop, se izvaja varnostni nadzor.
16.2	Manipulacija s telematiko vozila (npr. manipulacija z merjenjem temperature občutljivega blaga, odklepanje vrat prtljažnika na daljavo).		
16.3	Motenje delovanja brezžičnih sistemov ali senzorjev kratkega dosega.		
17.1	Poškodovane aplikacije ali aplikacije s slabo varnostjo programske opreme, ki se uporabijo kot sredstvo za napade na sisteme vozila.	M21	Oceni se varnost programske opreme, potrdi se njena pristnost in zaščiti njena celovitost. Uporabi se varnostni nadzor, da se zmanjša tveganje zaradi programske opreme tretje osebe, za katero se načrtuje ali predvideva, da bo nameščena v vozilu.
18.1	Zunanji vmesniki, kot so vrata USB ali druga vrata, se uporabijo kot točka napada, na primer z vrivanjem kode.	M22	Za zunanje vmesnike se uporablja varnostni nadzor.
18.2	Mediji, okuženi z virusi, so povezani z vozilom.		
18.3	Diagnostični dostop (npr. zaščitni ključi za vrata OBD), uporabljen za olajšanje napada, na primer manipulacije s parametri vozila (neposredno ali posredno).	M22	Za zunanje vmesnike se uporablja varnostni nadzor.

5. Blažitveni ukrepi za „potencialne tarče napada ali motivacijo za napad“

Blažitveni ukrepi za grožnje, povezane s „potencialnimi tarčami napada ali motivacijo za napad“, so navedeni v preglednici B5.

Preglednica B5

Blažitveni ukrepi za grožnje, povezane s „potencialnimi tarčami napada ali motivacijo za napad“

Sklic na preglednico A1	Grožnje, povezane s „potencialnimi tarčami napada ali motivacijo za napad“	Sklic	Blažitveni ukrep
19.1	Pridobivanje avtorske ali lastniške programske opreme iz sistemov vozila (piratstvo izdelkov / ukradena programska oprema).	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
19.2	Nepooblaščen dostop do zasebnih podatkov lastnika, kot so osebna identiteta, podatki o plačilnem računu, podatki iz imenika, podatki o lokaciji, elektronska identifikacija vozila itd.	M8	Z zasnovo sistema in nadzorom nad dostopom bi se moral nepooblaščenemu osebju preprečiti dostop do osebnih podatkov ali podatkov, kritičnih za sistem. Za primere varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
19.3	Pridobivanje kriptografskih ključev.	M11	Pri shranjevanju kriptografskih ključev se izvaja varnostni nadzor, na primer varnostni moduli.
20.1	Nezakonite/nepooblaščene spremembe elektronske identifikacije vozila.	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
20.2	Identitetna prevara. Če na primer uporabnik želi prikazati drugo identiteto pri komunikaciji s sistemi cestninjenja ali zalednim sistemom proizvajalca.		
20.3	Ukrepi za izogibanje nadzornim sistemom (npr. vdiranje/spreminjanje/blokiranje sporočil, kot so podatki sledilnika snemalnika operativnih podatkov ali število zagonov).	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP). Napadi z manipulacijo s podatki na senzorje ali prenesene podatke se lahko ublažijo s korelacijo podatkov iz različnih virov informacij.
20.4	Manipulacija s podatki za ponarejanje podatkov iz vozila o vožnji (npr. kilometrina, hitrost vožnje, navodila za vožnjo.).		
20.5	Nepooblaščene spremembe diagnostičnih podatkov sistema.		
21.1	Nepooblaščeno brisanje/manipulacija dnevnikov sistemskih dogodkov.	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
22.2	Uvedba zlonamerne programske opreme ali dejavnost zlonamerne programske opreme.	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
23.1	Ponarejanje programske opreme nadzornega sistema ali informacijskega sistema vozila.		

Sklic na preglednico A1	Grožnje, povezane s „potencialnimi tarčami napada ali motivacijo za napad“	Sklic	Blažitveni ukrep
24.1	Zavrnitev storitve, kar se lahko na primer sproži na notranjem omrežju s preplavljanjem področnega krmilnega omrežja ali spodbujanjem napak na elektronski krmilni enoti s pogostim pošiljanjem sporočil.	M13	Izvesti bi bilo treba ukrepe za odkrivanje napada z zavrnitvijo storitve in okrevanje po njem.
25.1	Nepooblaščen dostop za ponarejanje konfiguracijskih parametrov ključnih funkcij vozila, kot so podatki o zavorah, prag sprožitve zračne blazine.	M7	Za zaščito sistemskih podatkov/kode se uporabljajo tehnike in zasnove za nadzor nad dostopom. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
25.2	Nepooblaščen dostop za ponarejanje parametrov polnjenja, kot so napetost polnjenja, moč polnjenja, temperatura akumulatorja.		

6. Blažitveni ukrepi za „potencialne ranljive točke, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene“

Blažitveni ukrepi za grožnje, povezane s „potencialnimi ranljivimi točkami, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene“, so navedeni v preglednici B6

Preglednica B6

Blažitveni ukrepi za grožnje, povezane s „potencialnimi ranljivimi točkami, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene“

Sklic na preglednico A1	Grožnje, povezane s „potencialnimi ranljivimi točkami, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene“	Sklic	Blažitveni ukrep
26.1	Kombinacija kratkih šifrirnih ključev in dolgega obdobja veljavnosti napadalcu omogoča, da dešifrira šifriranje.	M23	Upoštevajo se dobre prakse kibernetske varnosti za razvoj programske in strojne opreme.
26.2	Nezadostna uporaba kriptografskih algoritmov za zaščito občutljivih sistemov.		
26.3	Uporaba zastarelih kriptografskih algoritmov.		
27.1	Strojna ali programska oprema, ki je zasnovana tako, da omogoča napad, ali ki ne izpolnjuje meril glede zasnove za zaustavitev napada.	M23	Upoštevajo se dobre prakse kibernetske varnosti za razvoj programske in strojne opreme.
28.1	Prisotnost napak v programski opremi je lahko osnova za ranljive točke, ki jih je morda mogoče izkoristiti. To velja zlasti, če programska oprema ni bila preizkušena, s čimer bi se preverilo, da znana slaba koda/napake niso prisotne, in zmanjšalo tveganje prisotnosti neznanih slabih kod/napak.	M23	Upoštevajo se dobre prakse kibernetske varnosti za razvoj programske in strojne opreme. Preizkušanje kibernetske varnosti z zadostno pokritostjo.

Sklic na preglednico A1	Grožnje, povezane s „potencialnimi ranljivimi točkami, ki bi se lahko izkoristile, če niso dovolj zaščitene ali okrepljene“	Sklic	Blažitveni ukrep
28.2	Uporaba ostalih elementov pri razvoju (npr. vrata za odpravljanje napak, vrata JTAG, mikroprocesorji, razvojni certifikati, gesla za razvijalce ...) lahko napadalcu omogoči dostop do elektronskih krmilnih enot ali pridobitev večjih pravic.		
29.1	Odvečna internetna vrata ostanejo odprta in omogočajo dostop do omrežnih sistemov.		
29.2	Zaobide se ločitev omrežja, da se pridobi nadzor. Konkreten primer je uporaba nezaščitenih prehodov ali točk dostopa (kot so prehodi med tovornjakom in prikolico), da se zaobidejo zaščite in pridobi dostop do drugih segmentov omrežja ter izvedejo zlonamerna dejanja, kot je pošiljanje poljubnih sporočil področnega krmilnega omrežja.	M23	Upoštevajo se dobre prakse kibernetske varnosti za razvoj programske in strojne opreme. Upoštevajo se dobre prakse kibernetske varnosti za zasnovo sistema in vključevanje sistema.

7. Blažitveni ukrepi za „izgubo podatkov/kršitev varnosti podatkov iz vozila“.

Blažitveni ukrepi za grožnje, povezane z „izgubo podatkov/kršitvijo varnosti podatkov iz vozila“, so navedeni v preglednici B7.

Preglednica B7

Blažitveni ukrepi za grožnje, povezane z „izgubo podatkov/kršitvijo varnosti podatkov iz vozila“

Sklic na preglednico A1	Grožnje, povezane z „izgubo podatkov/kršitvijo varnosti podatkov iz vozila“	Sklic	Blažitveni ukrep
31.1	Kršitev varnosti informacij. Varnost osebnih podatkov je lahko kršena, ko avto zamenja uporabnika (npr. se proda ali se uporablja kot vozilo za najem, pri čemer so najemniki novi).	M24	Pri shranjevanju osebnih podatkov se upoštevajo dobre prakse za zaščito celovitosti in zaupnosti podatkov.

8. Blažitveni ukrepi za „fizično manipulacijo s sistemi, da se omogoči napad“

Blažitveni ukrepi za grožnje, povezane s „fizično manipulacijo s sistemi, da se omogoči napad“, so navedeni v preglednici B8.

Preglednica B8

Blažitveni ukrepi za grožnje, povezane s „fizično manipulacijo s sistemi, da se omogoči napad“

Sklic na preglednico A1	Grožnje, povezane s „fizično manipulacijo s sistemi, da se omogoči napad“	Sklic	Blažitveni ukrep
32.1	Manipulacija s strojno opremo proizvajalca originalne opreme, v vozilo se na primer doda nepooblaščena strojna oprema, ki omogoča napad s posrednikom.	M9	Izvesti bi bilo treba ukrepe za preprečevanje in odkrivanje nepooblaščenega dostopa.

DEL C

Blažitveni ukrepi za grožnje zunaj vozil

1. Blažitveni ukrepi za „zaledne strežnike“

Blažitveni ukrepi za grožnje, povezane z „zalednimi strežniki“, so navedeni v preglednici C1.

Preglednica C1

Blažitveni ukrepi za grožnje, povezane z „zalednimi strežniki“

Sklic na preglednico A1	Grožnje, povezane z „zalednimi strežniki“	Sklic	Blažitveni ukrep
1.1 in 3.1	Zloraba privilegijev s strani osebja (notranji napad).	M1	Za zaledne sisteme se uporabi varnostni nadzor, da se zmanjša tveganje notranjega napada.
1.2 in 3.3	Nepooblaščen internetni dostop do strežnika (ki ga npr. omogočijo stranska vrata, nepopravljene ranljive točke v programski opremi sistema, napadi SQL ali druga sredstva).	M2	Za zaledne sisteme se uporabi varnostni nadzor, da se zmanjša tveganje nepooblaščenega dostopa. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
1.3 in 3.4	Nepooblaščen fizični dostop do strežnika (npr. prek ključa USB ali drugega medija, ki se poveže s strežnikom).	M8	Z zasnovo sistema in nadzorom nad dostopom bi se moral nepooblaščenemu osebju preprečiti dostop do osebnih podatkov ali podatkov, kritičnih za sistem.
2.1	Napad na zaledni strežnik ustavi njegovo delovanje, mu na primer prepreči interakcijo z vozili in zagotavljanje storitev, od katerih so vozila odvisna.	M3	Za zaledne sisteme se uporablja varnostni nadzor. Kadar so zaledni strežniki ključnega pomena za zagotavljanje storitev, so vzpostavljeni obnovitveni ukrepi v primeru izpada sistema. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).
3.2	Izguba informacij v oblaku. Če podatke hranijo neodvisni ponudniki storitev v oblaku, se lahko zaradi napadov ali nesreč izgubijo občutljivi podatki.	M4	Za zmanjšanje tveganj, povezanih z računalništvom v oblaku, se uporabi varnostni nadzor. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP) in smernice NCSC o računalništvu v oblaku.
3.5	Kršitev varnosti informacij z nenamerno izmenjavo podatkov (npr. napake skrbnika, shranjevanje podatkov na strežnikih v garažah).	M5	Za zaledne sisteme se uporabi varnostni nadzor, da se preprečijo kršitve varnosti podatkov. Za primer varnostnega nadzora glej projekt o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).

2. Blažitveni ukrepi za „nenamerna človeška dejanja“

Blažitveni ukrepi za grožnje, povezane z „nenamernimi človeškimi dejanji“, so navedeni v preglednici C2.

Preglednica C2

Blažitveni ukrepi za grožnje, povezane z „nenamernimi človeškimi dejanji“

Sklic na preglednico A1	Grožnje, povezane z „nenamernimi človeškimi dejanji“	Sklic	Blažitveni ukrep
15.1	Nedolžna žrtev (npr. lastnik, operater ali inženir za vzdrževanje) je zavedena, da sprejme ukrep, s katerim nenamerno naloži zlonamerno programsko opremo ali omogoči napad.	M18	Izvedejo se ukrepi za opredelitev vlog uporabnikov in njihovih pravic dostopa ter nadzor nad njimi na podlagi načela najmanjše pravice do dostopa.
15.2	Opredeljeni varnostni postopki se ne upoštevajo.	M19	Organizacije zagotovijo, da se opredelijo in upoštevajo varnostni postopki, vključno z beleženjem dejanj in dostopom, povezanim z upravljanjem varnostnih funkcij.

3. Blažitveni ukrepi za „fizično izgubo podatkov“

Blažitveni ukrepi za grožnje, povezane s „fizično izgubo podatkov“, so navedeni v preglednici C3.

Preglednica C3

Blažitveni ukrepi za grožnje, povezane s „fizično izgubo podatkov“

Sklic na preglednico A1	Grožnje, povezane s „fizično izgubo podatkov“	Sklic	Blažitveni ukrep
30.1	Škoda, ki jo povzroči tretja oseba. Občutljivi podatki se lahko izgubijo ali so ogroženi zaradi fizične škode v primeru prometne nesreče ali kraje.	M24	Pri shranjevanju osebnih podatkov se upoštevajo dobre prakse za zaščito celovitosti in zaupnosti podatkov. Za primer varnostnega nadzora glej standard ISO/SC27/WG5.
30.2	Izguba zaradi sporov glede upravljanja digitalnih pravic. Uporabniški podatki se lahko izbrišejo zaradi težav z upravljanjem digitalnih pravic.		
30.3	Občutljivi podatki (ali njihova celovitost) se lahko izgubijo zaradi obrabe komponent IT, kar povzroči morebitne kaskadne težave (kot v primeru spremembe ključa).		