ANO Noteikumi Nr. 155 – Vienoti noteikumi par transportlīdzekļu apstiprināšanu attiecībā uz kiberdrošību un kiberdrošības pārvaldības sistēmu [2021/387]

Spēkā stāšanās datums: 2021. gada 22. janvāris

Šis dokuments ir domāts tikai kā dokumentēšanas rīks. Autentiski un juridiski saistoši dokumenti ir:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 un

— ECE/TRANS/WP.29/2020/97

SATURS

1. DARBĪBAS JOMA

1.1. Šos noteikumus attiecībā uz kiberdrošību piemēro M un N kategorijas transportlīdzekļiem.

Šos noteikumus piemēro arī O kategorijas transportlīdzekļiem, ja tie aprīkoti ar vismaz vienu elektroniskās vadības ierīci.

1.2. Šos noteikumus piemēro arī L_6 un L_7 kategorijas transportlīdzekļiem, ja tie aprīkoti ar 3. un augstāka līmeņa automatizētas vadīšanas funkcijām, kā noteikts "WP.29 atsauces dokumentā ar automatizētās vadīšanas definīcijām un ANO noteikumu par automatizētiem transportlīdzekļiem izstrādes vispārīgajos principos" (ECE/TRANS/WP.29/1140).

1.3. Šie noteikumi neskar citus ANO noteikumus, reģionālos vai nacionālos tiesību aktus, kas reglamentē pilnvaroto pušu piekļuvi transportlīdzeklim, tā datiem, funkcijām un resursiem, un šādas piekļuves nosacījumus. Tie neskar arī nacionālo un reģionālo tiesību aktu piemērošanu attiecībā uz privātumu un fizisko personu aizsardzību saistībā ar viņu persondatu apstrādi.

1.4. Šie noteikumi neskar citus ANO noteikumus, nacionālos vai reģionālos tiesību aktus, kas reglamentē fizisku un digitālu maiņas daļu un sastāvdaļu izstrādi un uzstādīšanu/sistēmas integrāciju attiecībā uz kiberdrošību.

2. DEFINĪCIJAS

Šajā regulā piemēro šādas definīcijas:

2.1. "transportlīdzekļa tips" ir transportlīdzekļi, kas neatšķiras vismaz šādos būtiskos aspektos:

a) ražotāja noteiktais transportlīdzekļa tipa apzīmējums;

b) elektriskās/elektroniskās arhitektūras un ārējo saskarņu būtiskie aspekti attiecībā uz kiberdrošību;

2.2. "kiberdrošība" ir stāvoklis, kurā ceļu transportlīdzekļi un to funkcijas ir aizsargātas pret kiberdraudiem elektriskām vai elektroniskām sastāvdaļām;

2.3. "kiberdrošības pārvaldības sistēma (CSMS)" ir sistemātiska, riskos balstīta pieeja, kas apraksta organizatoriskus procesus, pienākumus un pārvaldību, lai novērstu risku, kas saistīts ar kiberdraudiem transportlīdzekļiem, un pasargātu tos no kiberuzbrukumiem;

2.4. "sistēma" ir sastāvdaļu un/vai apakšsistēmu kopums, kas īsteno kādu funkciju vai funkcijas;

2.5. "izstrādes fāze" ir laikposms pirms transportlīdzekļa tipam piešķir tipa apstiprinājumu;

2.6. "ražošanas fāze" attiecas uz transportlīdzekļa tipa ražošanas laikposmu;

2.7. "pēcražošanas fāze" attiecas uz laikposmu no transportlīdzekļa tipa ražošanas izbeigšanas līdz visu transportlīdzekļa tipa transportlīdzekļu nolietošanai. Transportlīdzekļi, kas ietver konkrētu transportlīdzekļa tipu, šīs fāzes laikā tiks ekspluatēti, bet tie vairs netiks ražoti. Fāze beidzas, kad vairs nav konkrētā transportlīdzekļa tipa neviena ekspluatējama transportlīdzekļa;

2.8. "mazināšana" ir risku mazinošs pasākums;

2.9. "risks" ir potenciāls, ka dotais apdraudējums izmantos transportlīdzekļa ievainojamību un tādējādi nodarīs kaitējumu organizācijai vai personai;

2.10. "riska novērtējums" ir vispārīgs process, kurā konstatē, atpazīst un apraksta riskus (risku identificēšana), lai izprastu riska raksturu un noteiktu riska līmeni (riska analīze), un kurā riska analīzes rezultātus salīdzina ar riska kritērijiem, lai noteiktu, vai risks un/vai tā apmērs ir pieņemams vai pieļaujams (riska izvērtējums);

2.11. "riska pārvaldība" ir koordinētas darbības, lai virzītu un vadītu organizāciju attiecībā uz risku;

2.12. "apdraudējums" ir nevēlama incidenta, kas var radīt kaitējumu sistēmai, organizācijai vai indivīdam, potenciālais cēlonis;

2.13. "ievainojamība" ir lietas vai mazināšanas vājā vieta, ko var izmantot viens vai vairāki apdraudējumi.

3. APSTIPRINĀJUMA PIETEIKUMS

3.1. Transportlīdzekļa tipa apstiprinājuma pieteikumu attiecībā uz kiberdrošību iesniedz transportlīdzekļa ražotājs vai tā pienācīgi pilnvarots pārstāvis.

3.2. Pieteikumam pievieno turpmāk minētos dokumentus trijos eksemplāros un šādas ziņas:

3.2.1. transportlīdzekļa tipa apraksts attiecībā uz šo noteikumu 1. pielikumā norādītajiem elementiem;

3.2.2. ja ir norādīts, ka uz šādu informāciju attiecas intelektuālā īpašuma tiesības, vai ka tā ir ražotāja vai viņa piegādātāju specifiska zinātība, ražotājs vai viņa piegādātāji sniedz pietiekamu informāciju, kas ļauj pienācīgi veikt šajos noteikumos minētās pārbaudes. Šādu informāciju apstrādā konfidenciāli;

3.2.3. *CSMS* atbilstības sertifikātu saskaņā ar šo noteikumu 6. punktu.

3.3. Dokumentāciju dara pieejamu divās daļās:

a) formālā dokumentācijas pakete apstiprināšanai, kas satur 1. pielikumā norādīto materiālu, kuru iesniedz apstiprinātājai iestādei vai tās tehniskajam dienestam tipa apstiprinājuma pieteikuma iesniegšanas laikā. Apstiprinātāja iestāde vai tās tehniskais dienests izmanto šo dokumentācijas paketi kā pamata atsauci apstiprināšanas procesā. Apstiprinātāja iestāde vai tās tehniskais dienests nodrošina to, ka šī dokumentācijas pakete ir pieejama vismaz 10 gadus, ko skaita no laika, kad pilnībā izbeigta transportlīdzekļa tipa ražošana;

b) papildu materiāls, kas attiecas uz šo noteikumu prasībām – ražotājs to drīkst paturēt, bet dara pieejamu inspicēšanai tipa apstiprināšanas laikā. Ražotājs nodrošina, ka jebkāds materiāls, kas darīts pieejams inspicēšanai tipa apstiprināšanas laikā, paliek pieejams vismaz 10 gadus, ko skaita no laika, kad pilnībā izbeigta transportlīdzekļa tipa ražošana.

4. MARĶĒJUMS

4.1. Uz katra transportlīdzekļa, kas atbilst saskaņā ar šiem noteikumiem apstiprinātam transportlīdzekļa tipam, skaidri redzamā un viegli pieejamā vietā, kas norādīta apstiprinājuma veidlapā, liek starptautisku apstiprinājuma marķējuma zīmi, ko veido:

4.1.1. aplis, kas aptver burtu "E", kam seko tās valsts pazīšanas numurs, kura piešķīrusi apstiprinājumu;

4.1.2. pa labi no 4.1.1. punktā noteiktā apļa – šo noteikumu numurs, aiz tā burts "R", domuzīme un apstiprinājuma numurs.

4.2. Ja transportlīdzeklis atbilst transportlīdzekļa tipam, kas apstiprināts saskaņā ar vienu vai vairākiem citiem noteikumiem, kuri pievienoti Nolīgumam kā pielikumi, tad valstī, kas piešķīrusi apstiprinājumu saskaņā ar šiem noteikumiem, 4.1.1. punktā noteikto simbolu neatkārto; šādā gadījumā noteikumu un apstiprinājuma numurus un visus papildu simbolus no noteikumiem, saskaņā ar kuriem piešķirts apstiprinājums valstī, kas piešķīrusi apstiprinājumu saskaņā ar šiem noteikumiem, novieto vertikālās slejās pa labi no 4.1.1. punktā noteiktā simbola.

4.3. Apstiprinājuma marķējuma zīmei ir jābūt skaidri salasāmai un neizdzēšamai.

4.4. Apstiprinājuma marķējuma zīmi liek uz ražotāja piestiprinātās transportlīdzekļa datu plāksnītes vai tās tuvumā.

4.5. Apstiprinājuma marķējuma zīmes izkārtojuma paraugi doti šo noteikumu 3. pielikumā.

5. APSTIPRINĀJUMS

5.1. Apstiprinātājas iestādes attiecīgi piešķir tipa apstiprinājumu attiecībā uz kiberdrošību tikai tiem transportlīdzekļa tipiem, kas atbilst šo noteikumu prasībām.

5.1.1. Apstiprinātāja iestāde vai tehniskais dienests dokumentu pārbaudes ceļā verificē, ka transportlīdzekļa ražotājs ir veicis nepieciešamos pasākumus saistībā ar transportlīdzekļa tipu, lai:

a) piegāžu ķēdē vāktu un verificētu šajos noteikumos prasīto informāciju, lai pierādītu, ka ar piegādātājiem saistītie riski ir identificēti un tiek pārvaldīti;

b) dokumentētu riska novērtējumu (veiktu izstrādes fāzē vai retrospektīvi), testa rezultātus un mazināšanas, kas piemērotas transportlīdzekļa tipam, tostarp konstrukcijas informāciju, kas apliecina riska novērtējumu;

c) īstenotu pienācīgus kiberdrošības pasākumus transportlīdzekļa tipa konstrukcijā;

d) konstatētu iespējamus uzbrukumus kiberdrošībai un reaģētu uz tiem;

e) reģistrētu datus, veicinot kiberuzbrukumu konstatēšanu, un nodrošinātu datu kriminālistikas spējas, padarot iespējamu kiberuzbrukumu mēģinājumu vai sekmīgu kiberuzbrukumu analīzi.

5.1.2. Apstiprinātāja iestāde vai tehniskais dienests, testējot transportlīdzekļa tipa transportlīdzekli, verificē, ka transportlīdzekļa ražotājs ir īstenojis tā dokumentētos kiberdrošības pasākumus. Testus, ņemot paraugus, veic apstiprinātāja iestāde vai tehniskais dienests pats, vai sadarbībā ar transportlīdzekļa ražotāju. Paraugu ņemšanai ir jābūt koncentrētai uz, taču ne aprobežotai ar, riskiem, kas riska novērtēšanas laikā novērtēti kā augsti.

5.1.3. Apstiprinātāja iestāde vai tehniskais dienests atsakās piešķirt tipa apstiprinājumu attiecībā uz kiberdrošību, ja transportlīdzekļa ražotājs nav izpildījis vienu vai vairākas prasības, kas minētas 7.3. punktā, proti:

a) transportlīdzekļa ražotājs nav veicis 7.3.3. punktā minēto izsmeļošo riska novērtējumu; tostarp, kad ražotājs nav apsvēris visus riskus saistībā ar 5. pielikuma A daļā minētajiem apdraudējumiem;

b) transportlīdzekļa ražotājs nav aizsargājis transportlīdzekļa tipu pret riskiem, kas identificēti transportlīdzekļa ražotāja riska novērtējumā, vai nav tikušas īstenotas samērīgas mazināšanas, kā tas prasīts 7. punktā;

c) transportlīdzekļa ražotājs nav ieviesis piemērotus un samērīgus pasākumus, lai transportlīdzekļa tipā droši iekļautu atvēlētas vides (ja tādas ir nodrošinātas), kur uzglabā un darbina pēcpārdošanas tirgū esošu programmatūru, pakalpojumus, lietotnes vai datus;

d) transportlīdzekļa ražotājs pirms apstiprināšanas nav veicis atbilstīgu un pietiekamu testēšanu, lai verificētu īstenoto drošības pasākumu efektivitāti.

5.1.4. Apstiprinātāja iestāde atsakās piešķirt tipa apstiprinājumu attiecībā uz kiberdrošību arī tad, ja apstiprinātāja iestāde vai tehniskais dienests nav saņēmis no transportlīdzekļa ražotāja pietiekamu informāciju, lai novērtētu transportlīdzekļa tipa kiberdrošību.

5.2. Paziņojumu par transportlīdzekļa tipa apstiprinājumu, apstiprinājuma paplašinājumu vai atteikumu atbilstīgi šiem noteikumiem nosūta šos noteikumus piemērojošajām 1958. gada Nolīguma pusēm, izmantojot šo noteikumu 2. pielikumā dotajam paraugam atbilstošu veidlapu.

5.3. Apstiprinātājas iestādes nevienam tipam nepiešķir tipa apstiprinājumu, nepārliecinājušās, ka ražotājs ir ieviesis apmierinošus pasākumus un procedūras, lai pienācīgi pārvaldītu kiberdrošības aspektus, kā noteikts šajos noteikumos.

5.3.1. Apstiprinātāja iestāde un tās tehniskie dienesti papildus 1958. gada Nolīguma 2. pielikumā noteiktajiem kritērijiem nodrošina, ka tai(-iem) ir:

a) kompetents personāls ar pienācīgām kiberdrošības prasmēm un specifiskām autotransporta jomas riska novērtēšanas zināšanām ([1]),

b) īstenotas procedūras vienotai izvērtēšanai saskaņā ar šiem noteikumiem.

([1]) Piem., ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

5.3.2. Katra šos noteikumus piemērojošā Nolīguma puse ar tās apstiprinātājas iestādes starpniecību apziņo un informē pārējo šos ANO noteikumus piemērojošo Nolīguma pušu apstiprinātājas iestādes par metodi un kritērijiem, kas paziņojošajai iestādei kalpojuši par pamatu, lai novērtētu saskaņā ar šiem noteikumiem, un, jo īpaši, ar 5.1., 7.2. un 7.3. punktu, veikto pasākumu piemērotību.

Šo informāciju kopīgo: a) tikai pirms pirmo reizi piešķirt apstiprinājumu atbilstīgi šiem noteikumiem un b) ikreiz, kad tiek atjaunināta novērtēšanas metode vai kritēriji.

Šo informāciju ir paredzēts kopīgot, lai apkopotu un analizētu labāko praksi un lai nodrošinātu, ka visas apstiprinātājas iestādes, kas piemēro šos noteikumus, tos piemērotu vienveidīgi.

5.3.3. Angļu valodā sniegtu informāciju, kas minēta 5.3.2. punktā, savlaicīgi un ne vēlāk kā 14 dienas pirms apstiprinājuma piešķiršanas pirmo reizi atbilstoši attiecīgajām novērtēšanas metodēm un kritērijiem augšupielādē drošajā interneta datubāzē "DETA" ([2]), ko izveidojusi Apvienoto Nāciju Organizācijas Eiropas Ekonomikas komisija. Informācijai ir jābūt pietiekamai, lai saprastu, kādu minimālo veiktspējas līmeni apstiprinātāja iestāde ir pieņēmusi attiecībā uz katru konkrēto prasību, kas minēta 5.3.2. punktā, kā arī procesus un pasākumus, ko tā piemēro, lai verificētu, ka šie minimālie veiktspējas līmeņi ir ievēroti ([3]).

5.3.4. Apstiprinātājas iestādes, kas saņem 5.3.2. punktā minēto informāciju, drīkst paziņojošajai apstiprinātājai iestādei iesniegt komentārus, augšupielādējot tos *DETA* 14 dienu laikā pēc paziņošanas dienas.

5.3.5. Ja piešķirošajai apstiprinātājai iestādei nav iespējams ņemt vērā saskaņā ar 5.3.4. punktu saņemtos komentārus, apstiprinātāja iestāde, kas nosūtījusi komentārus, un piešķirošā apstiprinātāja iestāde meklē turpmākus skaidrojumus saskaņā ar 1958. gada nolīguma 6. pielikumu. Transportlīdzekļu noteikumu harmonizācijas Pasaules foruma (WP.29) attiecīgā darba grupa ([4]), kas nodarbojas ar šiem noteikumiem, vienojas par novērtēšanas metožu un kritēriju vienotu interpretāciju ([5]). Šai vienotajai interpretācijai ir jābūt īstenotai, un visām apstiprinātājām iestādēm ir attiecīgi jāizdod tipa apstiprinājumi atbilstīgi šiem noteikumiem.

5.3.6. Katra apstiprinātāja iestāde, kas piešķir tipa apstiprinājumu atbilstīgi šiem noteikumiem, informē citas apstiprinātājas iestādes par piešķirto apstiprinājumu. Apstiprinātāja iestāde 14 dienu laikā pēc apstiprinājuma piešķiršanas dienas *DETA* angļu valodā augšupielādē tipa apstiprinājumu kopā ar papildinošo dokumentāciju ([6]).

5.3.7. Nolīguma puses drīkst pētīt apstiprinājumus, kas piešķirti, pamatojoties uz informāciju, kura augšupielādēta saskaņā ar 5.3.6. punktu. Nolīguma pušu jebkādu atšķirīgu viedokļu gadījumā tos risina saskaņā ar 1958. gada Nolīguma 6. pielikumu un 10. pantu. Nolīguma puses informē par 1958. gada Nolīguma 6. pielikuma izpratnē atšķirīgajām interpretācijām arī Transportlīdzekļu noteikumu harmonizācijas Pasaules foruma (WP.29) attiecīgo darba grupu. Attiecīgā darba grupa atbalsta atšķirīgo viedokļu noregulēšanu un saistībā ar to drīkst konsultēties ar WP.29, ja tas vajadzīgs.

5.4. Šo noteikumu 7.2. punkta vajadzībām ražotājs nodrošina, ka tiek ieviesti šo noteikumu aptvertie kiberdrošības aspekti.

([2]) https://www.unece.org/trans/main/wp29/datasharing.html

([3]) Norādes par augšupielādējamo detalizēto informāciju (piem., metode, kritēriji, veiktspējas līmenis) un tās formātu sniedz interpretācijas dokumentā, ko Kiberdrošības un bezvadu sakaru darba grupa gatavo *GRVA* septītajai sesijai.

([4]) Automatizēto/autonomo un satīkloto transportlīdzekļu darba grupa (*GRVA*).

([5]) Šo interpretāciju atspoguļo interpretācijas dokumentā, kas minēts 5.3.3. punkta zemsvītras piezīmē.

([6]) Turpmāku informāciju par prasību minimumu dokumentācijas paketei izstrādās *GRVA* tās septītajā sesijā.

6. KIBERDROŠĪBAS PĀRVALDĪBAS SISTĒMAS ATBILSTĪBAS SERTIFIKĀTS

6.1. Nolīguma puses norīko apstiprinātāju iestādi veikt ražotāja novērtēšanu un izdot *CSMS* atbilstības sertifikātu.

6.2. Kiberdrošības pārvaldības sistēmas atbilstības sertifikāta pieteikumu iesniedz transportlīdzekļa ražotājs vai tā pienācīgi pilnvarots pārstāvis.

6.3. Tam pievieno turpmāk minētos dokumentus trijos eksemplāros un šādas ziņas:

6.3.1. kiberdrošības pārvaldības sistēmu aprakstošus dokumentus;

6.3.2. parakstītu deklarāciju, kas atbilst 1. pielikuma 1. papildinājumā dotajam paraugam.

6.4. Novērtēšanas kontekstā ražotājs, izmantojot 1. pielikuma 1. papildinājumā doto paraugu, deklarē un pierāda apstiprinātājai iestādei vai tās tehniskajam dienestam, ka tā rīcībā ir procesi, kas nepieciešami, lai izpildītu visas šo noteikumu kiberdrošības prasības.

6.5. Kad šī novērtēšana ir sekmīgi pabeigta un no ražotāja ir saņemta parakstīta deklarācija, kas atbilst 1. pielikuma 1. papildinājumā dotajam paraugam, ražotājam piešķir sertifikātu ar nosaukumu "*CSMS* atbilstības sertifikāts", kā aprakstīts šo noteikumu 4. pielikumā (turpmāk tekstā "*CSMS* atbilstības sertifikāts").

6.6. Apstiprinātāja iestāde vai tās tehniskais dienests *CSMS* atbilstības sertifikātam izmanto šo noteikumu 4. pielikumā doto paraugu.

6.7. *CSMS* atbilstības sertifikāts saglabā derīgumu ne ilgāk kā trīs gadus no sertifikāta izsniegšanas dienas, ja tas netiek anulēts.

6.8. Apstiprinātāja iestāde, kas piešķīrusi *CSMS* atbilstības sertifikātu, drīkst jebkurā laikā pārliecināties, ka tam noteiktās prasības joprojām tiek izpildītas. Apstiprinātāja iestāde anulē *CSMS* atbilstības sertifikātu, ja šajos noteikumos noteiktas prasības vairs netiek izpildītas.

6.9. Ražotājs informē apstiprinātāju iestādi vai tās tehnisko dienestu par jebkādām izmaiņām, kas ietekmēs *CSMS* atbilstības sertifikāta atbilstību. Apspriedusies ar ražotāju, apstiprinātāja iestāde vai tās tehniskais dienests pieņem lēmumu par jaunu pārbaužu nepieciešamību.

6.10. Ražotājs savlaicīgi iesniedz pieteikumu jaunam *CSMS* atbilstības sertifikātam vai tā termiņa pagarināšanai, ļaujot apstiprinātājai iestādei pabeigt novērtēšanu pirms *CSMS* atbilstības sertifikāta derīguma termiņa beigām. Pozitīva novērtējuma gadījumā apstiprinātāja iestāde izdod jaunu *CSMS* atbilstības sertifikātu vai pagarina tā derīguma termiņu uz turpmāko trīs gadu periodu. Apstiprinātāja iestāde pārliecinās, ka *CSMS* joprojām atbilst šo noteikumu prasībām. Apstiprinātāja iestāde izdod jaunu sertifikātu gadījumos, kad par izmaiņām ir paziņots apstiprinātājai iestādei vai tās tehniskajam dienestam un izmaiņas ir atkārtoti pozitīvi novērtētas.

6.11. Ražotāja *CSMS* atbilstības sertifikāta derīguma termiņa izbeigšanos vai anulēšanu attiecībā uz transportlīdzekļa tipiem, uz kuriem attiecas dotā *CSMS*, uzskata par apstiprinātās lietas pārveidojumu, kā minēts 8. punktā, kas var ietvert apstiprinājuma anulēšanu, ja apstiprinājuma piešķiršanas nosacījumi vairs nav izpildīti.

7. SPECIFIKĀCIJAS

7.1. Vispārīgas specifikācijas

7.1.1. Šo noteikumu prasības neierobežo citu ANO noteikumu nosacījumus vai prasības.

7.2. Prasības kiberdrošības pārvaldības sistēmai

7.2.1. Novērtēšanas nolūkā apstiprinātāja iestāde vai tās tehniskais dienests pārliecinās, ka transportlīdzekļa ražotājam ir kiberdrošības pārvaldības sistēma, un verificē tās atbilstību šiem noteikumiem.

7.2.2. Kiberdrošības pārvaldības sistēmai jāaptver šādi aspekti.

7.2.2.1. Transportlīdzekļa ražotājam ir jāpierāda apstiprinātājai iestādei vai tehniskajam dienestam, ka tā kiberdrošības pārvaldības sistēmu piemēro šādām fāzēm:

a) izstrādes fāze;

b) ražošanas fāze:

c) pēcražošanas fāze.

7.2.2.2. Transportlīdzekļa ražotājs pierāda, ka tā kiberdrošības pārvaldības sistēmas drošības nodrošināšanas procesi ir pienācīgi ņemti vērā, tostarp riski un mazināšanas, kā uzskaitīts 5. pielikumā. Proti:

a) procesi ražotāja organizācijā, lai pārvaldītu kiberdrošību;

b) procesi, lai identificētu riskus, kādiem pakļauti transportlīdzekļa tipi. Šajos procesos ņem vērā 5. pielikuma A daļā minētos apdraudējumus un citus attiecīgus apdraudējumus;

c) procesi identificēto risku novērtēšanai, kategorizēšanai un apstrādei;

d) esošie procesi, lai pārliecinātos, ka identificētie riski tiek pienācīgi pārvaldīti;

e) procesi transportlīdzekļa tipa kiberdrošības testēšanai;

f) procesi riska novērtējuma aktualizēšanas nodrošināšanai;

g) procesi, lai pārraudzītu, konstatētu kiberuzbrukumus, kiberdraudus transportlīdzekļa tipiem un to ievainojamības un attiecīgi reaģētu, un procesi, lai novērtētu, vai īstenotie kiberdrošības pasākumi joprojām ir efektīvi jaunu, identificētu kiberdraudu un ievainojamību kontekstā;

h) procesi, lai nodrošinātu pienācīgus datus kiberuzbrukumu mēģinājumu vai sekmīgu kiberuzbrukumu analīzes atbalstam.

7.2.2.3. Transportlīdzekļa ražotājs pierāda, ka kiberdrošības pārvaldības sistēmas procesi nodrošinās to, ka, pamatojoties uz 7.2.2.2. punkta c) apakšpunktā un 7.2.2.2. punkta g) apakšpunktā minēto kategorizāciju, kiberdraudi un ievainojamības, kas prasa transportlīdzekļa ražotāja reakciju, tiks mazinātas saprātīgā termiņā.

7.2.2.4. Transportlīdzekļa ražotājs pierāda, ka kiberdrošības pārvaldības sistēmas procesi nodrošinās to, ka 7.2.2.2. punkta g) apakšpunktā minētā pārraudzība ir nepārtraukta. Tas:

a) ietver pārraudzībā transportlīdzekļus pēc pirmās reģistrācijas;

b) ietver spēju analizēt un atklāt kiberdraudus, ievainojamības un kiberuzbrukumus, izmantojot transportlīdzekļa datus un transportlīdzekļa žurnāldatus. Šai spējai jāievēro 1.3. punkts un vieglo automobiļu īpašnieku vai vadītāju tiesības uz privātumu, īpaši attiecībā uz piekrišanu.

7.2.2.5. Transportlīdzekļa ražotājam tiek prasīts pierādīt, kā kiberdrošības pārvaldības sistēma pārvaldīs atkarības, kādas varētu rasties no nolīgtajiem piegādātājiem, pakalpojumu sniedzējiem vai ražotāja apakšorganizācijām saistībā ar 7.2.2.2. punkta prasībām.

7.3. Prasības transportlīdzekļu tipiem

7.3.1. Ražotājam ir jābūt derīgam kiberdrošības pārvaldības sistēmas atbilstības sertifikātam, kas attiecas uz apstiprināmo transportlīdzekļa tipu.

Tomēr attiecībā uz tipa apstiprinājumiem pirms 2024. gada 1. jūlija transportlīdzekļa ražotājs pierāda, ka kiberdrošība tikusi pienācīgi ņemta vērā dotā transportlīdzekļa tipa izstrādes fāzē, ja transportlīdzekļa ražotājs var pierādīt, ka transportlīdzekļa tips nevarēja tikt izstrādāts atbilstoši *CSMS*.

7.3.2. Transportlīdzekļa ražotājs identificē un pārvalda ar piegādātāju saistītos riskus attiecībā uz apstiprināmo transportlīdzekļa tipu.

7.3.3. Transportlīdzekļa ražotājs identificē transportlīdzekļa tipa kritiskos elementus un veic transportlīdzekļa tipa izsmeļošu riska novērtējumu, un pienācīgi apstrādā/pārvalda identificētos riskus. Riska novērtējumā ņem vērā transportlīdzekļa tipa atsevišķos elementus un to mijiedarbību. Riska novērtējumā ņem vērā arī mijiedarbību ar jebkādām ārējām sistēmām. Novērtējot riskus, transportlīdzekļa ražotājs ņem vērā riskus, kas saistīti ar visiem 5. pielikuma A daļā minētajiem apdraudējumiem, kā arī jebkādus citus attiecīgos riskus.

7.3.4. Transportlīdzekļa ražotājs aizsargā transportlīdzekļa tipu pret riskiem, kas identificēti transportlīdzekļa ražotāja riska novērtējumā. Transportlīdzekļa tipa aizsargāšanai īsteno samērīgas mazināšanas. Īstenotajām mazināšanām ir jāietver visas 5. pielikuma B un C daļā minētās mazināšanas, kas attiecas uz identificētajiem riskiem. Tomēr, ja 5. pielikuma B un C daļā minētā mazināšana nav būtiska vai nav pietiekama attiecībā uz identificēto risku, transportlīdzekļa ražotājs nodrošina citas, piemērotas mazināšanas īstenošanu.

Jo īpaši attiecībā uz tipa apstiprinājumiem pirms 2024. gada 1. jūlija transportlīdzekļa ražotājs nodrošina citas mazināšanas īstenošanu, ja 5. pielikuma B un C daļā minētā mazināšana nav tehniski iespējama. Ražotājs apstiprinātājai iestādei iesniedz attiecīgu tehniskās iespējamības novērtējumu.

7.3.5. Transportlīdzekļa ražotājs ievieš piemērotus un samērīgus pasākumus, lai transportlīdzekļa tipā droši iekļautu atvēlētas vides (ja tādas ir nodrošinātas), kur uzglabā un darbina pēcpārdošanas tirgū esošu programmatūru, pakalpojumus, lietotnes vai datus.

7.3.6. Transportlīdzekļa ražotājs pirms tipa apstiprināšanas veic atbilstīgu un pietiekamu testēšanu, lai verificētu īstenoto drošības pasākumu efektivitāti.

7.3.7. Transportlīdzekļa ražotājs attiecībā uz transportlīdzekļa tipu īsteno pasākumus, lai:

a) konstatētu un nepieļautu kiberuzbrukumus dotā transportlīdzekļa tipa transportlīdzekļiem;

b) atbalstītu transportlīdzekļa ražotāja pārraudzības spēju attiecībā uz tādu apdraudējumu, ievainojamību un kiberuzbrukumu konstatēšanu, kas saistīti ar doto transportlīdzekļa tipu;

c) nodrošinātu datu kriminālistikas spējas, padarot iespējamu kiberuzbrukumu mēģinājumu vai sekmīgu kiberuzbrukumu analīzi.

7.3.8. Šo noteikumu vajadzībām izmantotajiem kriptogrāfiskajiem moduļiem jāatbilst vispārpieņemtiem standartiem. Ja kriptogrāfiskie moduļi neatbilst vispārpieņemtiem standartiem, transportlīdzekļa ražotājam ir jāpamato to izmantošana.

7.4. Ziņošanas noteikumi

7.4.1. Vismaz reizi gadā vai attiecīgā gadījumā biežāk transportlīdzekļa ražotājs ziņo apstiprinātājai iestādei vai tehniskajam dienestam par to pārraudzības darbību rezultātiem, kuras noteiktas 7.2.2.2. punkta g) apakšpunktā, iekļaujot attiecīgu informāciju par jauniem kiberuzbrukumiem. Transportlīdzekļa ražotājs arī ziņo un apstiprina apstiprinātājai iestādei vai tehniskajam dienestam, ka tā transportlīdzekļa tipiem īstenotās, ar kiberdrošību saistītās mazināšanas joprojām ir efektīvas, kā arī veiktās papildu darbības.

7.4.2. Apstiprinātāja iestāde vai tehniskais dienests verificē sniegto informāciju un nepieciešamības gadījumā pieprasa transportlīdzekļa ražotājam novērst konstatēto neefektivitāti.

Ja ziņojums vai atbilde nav pietiekama, apstiprinātāja iestāde drīkst nolemt anulēt *CSMS* atbilstoši 6.8. punktam.

8. TRANSPORTLĪDZEKĻA TIPA PĀRVEIDOJUMS UN TIPA APSTIPRINĀJUMA PAPLAŠINĀŠANA

8.1. Par jebkādu transportlīdzekļa tipa pārveidojumu, kas ietekmē tā tehnisko veiktspēju attiecībā uz kiberdrošību un/vai šajos noteikumos prasīto dokumentāciju, ziņo apstiprinātājai iestādei, kas apstiprinājusi transportlīdzekļa tipu. Apstiprinātāja iestāde tad drīkst vai nu:

8.1.1. uzskatīt, ka veiktie pārveidojumi joprojām atbilst esošā tipa apstiprinājuma prasībām un dokumentācijai, vai

8.1.2. uzsākt nepieciešamo papildu novērtēšanu atbilstīgi 5. punktam un attiecīgā gadījumā pieprasīt jaunu testa ziņojumu no tehniskā dienesta, kas ir atbildīgs par testu veikšanu.

8.1.3. Par apstiprinājuma apliecināšanu, paplašināšanu vai atteikumu, norādot izmaiņas, paziņo, izmantojot šo noteikumu 2. pielikumā dotajam paraugam atbilstošu paziņojuma veidlapu. Apstiprinājuma paplašinājumu piešķirošā apstiprinātāja iestāde piešķir šādam paplašinājumam sērijas numuru un par to informē pārējās šos noteikumus piemērojošās 1958. gada Nolīguma puses, izmantojot šo noteikumu 2. pielikumā dotajam paraugam atbilstošu paziņojuma veidlapu.

9. RAŽOŠANAS ATBILSTĪBA

9.1. Ražošanas atbilstības procedūrām ir jāatbilst 1958. gada nolīguma 1. pielikumā (E/ECE/TRANS/505/Rev.3) noteiktajām, ievērojot šādas prasības.

9.1.1. Apstiprinājuma turētājam jānodrošina, ka ražošanas atbilstības testu rezultāti tiek reģistrēti un ka pievienotie dokumenti paliek pieejami laikposmā, par kādu vienojas ar apstiprinātāju iestādi vai tās tehnisko dienestu. Šis laikposms nedrīkst pārsniegt 10 gadus, ko skaita no laika, kad ražošana ir pilnībā izbeigta.

9.1.2. Tipa apstiprinājumu piešķīrusī apstiprinātāja iestāde drīkst jebkurā laikā verificēt atbilstības kontroles metodes, ko piemēro katrā ražotnē. Šādu verifikāciju normāls biežums ir reize trīs gados.

10. SANKCIJAS PAR RAŽOŠANAS NEATBILSTĪBU

10.1. Atbilstīgi šiem noteikumiem piešķirto transportlīdzekļa tipa apstiprinājumu drīkst anulēt, ja nav izpildītas šajos noteikumos noteiktās prasības vai ja parauga transportlīdzekļi neatbilst šo noteikumu prasībām.

10.2. Ja apstiprinātāja iestāde anulē tās iepriekš piešķirtu apstiprinājumu, tā nekavējoties par to informē pārējās šos noteikumus piemērojošās Nolīguma puses, izmantojot šo noteikumu 2. pielikumā dotajam paraugam atbilstošu paziņojuma veidlapu.

11. RAŽOŠANAS PILNĪGA IZBEIGŠANA

11.1. Ja apstiprinājuma turētājs pilnīgi izbeidz atbilstīgi šiem noteikumiem apstiprināta transportlīdzekļa tipa ražošanu, viņam par to jāinformē iestāde, kas apstiprinājumu piešķīrusi. Saņēmusi attiecīgu paziņojumu, šī iestāde par to informē citas šos noteikumus piemērojošās Nolīguma puses, izmantojot apstiprinājuma veidlapas kopiju, kuras beigās lieliem burtiem rakstīts, parakstīts un datēts paziņojums "RAŽOŠANA IZBEIGTA" ("*PRODUCTION DISCONTINUED*").

12. PAR APSTIPRINĀŠANAS TESTU VEIKŠANU ATBILDĪGO TEHNISKO DIENESTU UN TIPA APSTIPRINĀTĀJU IESTĀŽU NOSAUKUMI UN ADRESES

12.1. Nolīguma puses, kas piemēro šos noteikumus, paziņo Apvienoto Nāciju Organizācijas Sekretariātam to tehnisko dienestu nosaukumus un adreses, kas ir atbildīgi par apstiprināšanas testu veikšanu, un to tipa apstiprinātāju iestāžu nosaukumu un adresi, kuras piešķir apstiprinājumu un kurām jānosūta veidlapas, kas apliecina citās valstīs izdotu apstiprinājumu vai apstiprinājuma paplašināšanu, atteikumu vai anulēšanu.

1. PIELIKUMS

Informācijas dokuments

Turpmāk norādīto informāciju attiecīgā gadījumā iesniedz trīs eksemplāros kopā ar satura rādītāju. Jebkādiem rasējumiem jābūt pienācīgā mērogā un pietiekami detalizētiem, A4 izmēra vai salocītiem līdz A4 formātam. Fotoattēliem, ja tādi ir, jābūt pietiekami detalizētiem.

1. Marka (ražotāja tirdzniecības nosaukums): .....

2. Tips un vispārīgs komercapraksts(-i): .....

3. Tipa identifikācijas līdzekļi, ja marķēti uz transportlīdzekļa: .....

4. Šā marķējuma atrašanās vieta: .....

5. Transportlīdzekļa kategorija(-as): .....

6. Ražotāja/ ražotāja pārstāvja nosaukums un adrese: .....

7. Montāžas rūpnīcas(-u) nosaukums(-i) un adrese(s): .....

8. Reprezentējoša transportlīdzekļa fotogrāfija(-s) un/vai rasējums(-i): .....

9. Kiberdrošība

9.1. Transportlīdzekļa tipa vispārīgi konstrukcijas raksturlielumi, tostarp:

a) transportlīdzekļa sistēmas, kas saistītas ar transportlīdzekļa tipa kiberdrošību;

b) šo sistēmu sastāvdaļas, kas saistītas ar kiberdrošību;

c) šo sistēmu mijiedarbība ar citām transportlīdzekļa tipa sistēmām un ārējām saskarnēm.

9.2. Transportlīdzekļa tipa shematisks attēlojums

9.3. *CSMS* atbilstības sertifikāta numurs: .....

9.4. Dokumenti par apstiprināmo transportlīdzekļa tipu, kas apraksta tā riska novērtējuma iznākumu un identificētos riskus: .....

9.5. Dokumenti par apstiprināmo transportlīdzekļa tipu, kas apraksta uzskaitītajās sistēmās vai attiecībā uz transportlīdzekļa tipu īstenotās mazināšanas un kā tās ietekmē norādītos riskus: .....

9.6. Dokumenti par apstiprināmo transportlīdzekļa tipu, kas apraksta, kā tiek aizsargātas pēcpārdošanas tirgū esošajām programmatūrām, pakalpojumiem, lietotnēm vai datiem atvēlētās vides; .....

9.7. Dokumenti par apstiprināmo transportlīdzekļa tipu, kas apraksta, kādi testi izmantoti, lai verificētu transportlīdzekļa tipa un tā sistēmu kiberdrošību, un šo testu iznākums: .....

9.8. Piegādes ķēdes apraksts ar apsvērumiem attiecībā uz kiberdrošību: .....

1. pielikuma 1. papildinājums

Ražotāja deklarācijas par *CSMS* atbilstību paraugs

Ražotāja deklarācija par kiberdrošības pārvaldības sistēmas atbilstību prasībām

Ražotāja nosaukums: .....

Ražotāja adrese: .....

..... (*Ražotāja nosaukums*) apliecina, ka procesi, kas nepieciešami, lai izpildītu ANO Noteikumu Nr. 155 7.2. punktā noteiktās prasības kiberdrošības pārvaldības sistēmai, ir ieviesti un tiks uzturēti. ....

Izdota: ..... (*vieta*)

Datums: .....

Parakstītāja vārds, uzvārds: .....

Parakstītāja amats: .....

.....

(*Ražotāja pārstāvja zīmogs un paraksts*)

2. PIELIKUMS

Paziņojums

(Maksimālais formāts: A4 (210 × 297 mm))

Izdevējs: Iestādes nosaukums:
.....
.....
.....

par (2) apstiprinājuma piešķiršanu,
apstiprinājuma paplašināšanu,
apstiprinājuma anulēšanu, sākot ar dd/mm/gggg,
apstiprinājuma atteikšanu,
ražošanas pilnīgu izbeigšanu

transportlīdzekļa tipam atbilstīgi ANO Noteikumiem Nr. 155

Apstiprinājuma Nr.: .....

Paplašinājuma Nr.: .....

Paplašinājuma iemesls: .....

1. Marka (ražotāja tirdzniecības nosaukums): .....

2. Tips un vispārīgs(-i) komercapraksts(-i): .....

3. Tipa identifikācijas līdzekļi, ja marķēti uz transportlīdzekļa: .....

3.1. Šā marķējuma atrašanās vieta: .....

4. Transportlīdzekļa kategorija(-as): .....

5. Ražotāja/ ražotāja pārstāvja nosaukums un adrese: .....

6. Montāžas rūpnīcas(-u) nosaukums(-i) un adrese(-es): .....

7. Kiberdrošības pārvaldības sistēmas atbilstības sertifikāta numurs: .....

8. Par testu veikšanu atbildīgais tehniskais dienests: .....

9. Testa ziņojuma datums: .....

10. Testa ziņojuma numurs: .....

11. Piezīmes: (ja ir). .....

12. Vieta: .....

13. Datums: .....

14. Paraksts: .....

15. Apstiprinātājai iestādei iesniegtās informācijas paketes, kuru var saņemt pēc pieprasījuma, satura rādītājs dots pielikumā.

([1]) Tās valsts pazīšanas numurs, kas piešķīrusi/paplašinājusi/atteikusi/anulējusi apstiprinājumu (apstiprinājuma prasības skatīt noteikumos).:

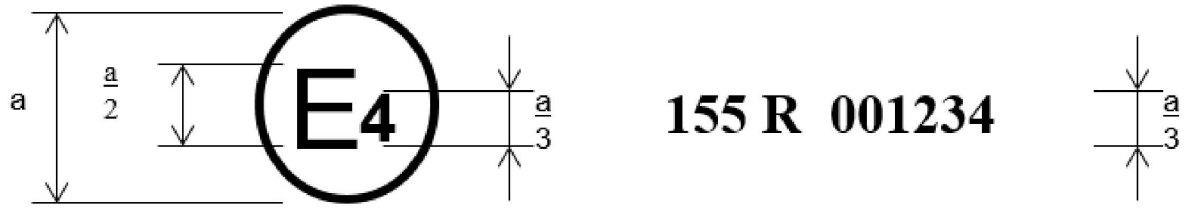
([2]) Nevajadzīgo svītrot.

3. PIELIKUMS

Apstiprinājuma marķējuma zīmes izkārtojums

A PARAUGS

(Skatīt šo noteikumu 4.2. punktu)



a = min. 8 mm

Šāda apstiprinājuma marķējuma zīme uz transportlīdzekļa rāda, ka attiecīgais ceļa transportlīdzekļa tips ir apstiprināts Nīderlandē (E4) atbilstīgi Noteikumiem Nr. 155, un apstiprinājuma numurs ir 001234. Pirmie divi apstiprinājuma numura cipari norāda, ka apstiprinājums piešķirts saskaņā ar šo noteikumu prasībām to sākotnējā redakcijā (00).

4. PIELIKUMS

CSMS atbilstības sertifikāta paraugs

Kiberdrošības pārvaldības sistēmas atbilstības sertifikāts

ANO Noteikumiem Nr. 155

Sertifikāta numurs [*atsauces numurs*]

[……. *Apstiprinātāja iestāde*]

apliecina, ka

ražotājs: ……

Ražotāja adrese: ……

atbilst Noteikumu Nr. 155 7.2. punkta noteikumiem.

Pārbaudes veica: [datums] ……

(apstiprinātājas iestādes vai tehniskā dienesta nosaukums un adrese): ……

Ziņojuma numurs: ……

Sertifikāts ir derīgs līdz [……*datums*].

Izdots [……*vieta*]

[……*datums*]

[……*paraksts*]

Pievienotie dokumenti: ražotāja sagatavots kiberdrošības pārvaldības sistēmas apraksts.

5. PIELIKUMS

Apdraudējumu un attiecīgo mazināšanu uzskaitījums

1. Šis pielikums sastāv no trim daļām. Šī pielikuma A daļā ir aprakstīti pamatdati par apdraudējumiem, ievainojamībām un uzbrukumu metodēm. Šī pielikuma B daļā aprakstītas apdraudējumu mazināšanas, kas paredzētas transportlīdzekļu tipiem. Šī pielikuma C daļā aprakstītas apdraudējumu mazināšanas, kas paredzētas vietām ārpus transportlīdzekļiem, piem., *IT* aizmugursistēmām.

2. A daļu, B daļu un C daļu ņem vērā riska novērtēšanā un mazināšanās, ko īsteno ražotājs.

3. Augsta līmeņa ievainojamības un to attiecīgie piemēri ir indeksēti A daļā. Uz to pašu indeksējumu izdarītas atsauces B un C daļas tabulās, lai sasaistītu katru uzbrukumu/ievainojamību ar atbilstošo mazināšanu sarakstu.

4. Apdraudējumu analīzē ņem vērā arī uzbrukumu iespējamo ietekmi. Tā varētu palīdzēt noskaidrot riska nopietnību un identificēt papildu riskus. Uzbrukuma iespējamā ietekme var ietvert:

   a) skartā transportlīdzekļa drošu darbību;

   b) transportlīdzekļa funkciju darbības apturēšanu;

   c) izmaiņas programmatūrā, izmainītu veiktspēju;

   d) programmatūras darbības izmaiņas, bet bez sekām attiecībā uz darbību;

   e) datu integritātes pārkāpumu;

   f) datu konfidencialitātes pārkāpumu;

   g) datu pieejamības zudumu;

   h) citu ietekmi, tostarp krimināltiesisku.

A daļa. Ievainojamības vai uzbrukuma metode saistībā ar apdraudējumiem

1. Apdraudējumu un ar tiem saistīto ievainojamību vai uzbrukuma metožu augsta līmeņa apraksti uzskaitīti A1. tabulā.

A1. tabula

Ar apdraudējumiem saistīto ievainojamību vai uzbrukuma metožu uzskaitījums

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
4.3.1. Apdraudējumi attiecībā uz aizmugurserveriem, kas saistīti ar transportlīdzekļiem ekspluatācijā	1.	Aizmugurserverus izmanto uzbrukumam transportlīdzeklim vai datu iegūšanai	1.1.	Darbinieku pilnvaru ļaunprātīga izmantošana (uzbrukums no iekšienes)
			1.2.	Nesankcionēta piekļuve serverim caur internetu (ko iespējo, piemēram, slepenpiekļuve, sistēmas programmatūras nelabotas ievainojamības, *SQL* uzbrukumi vai citi līdzekļi)
			1.3.	Nesankcionēta fiziska piekļuve serverim (kas notiek, piemēram, USB zibatmiņām vai citiem datu nesējiem savienojoties ar serveri)
	2.	Pārtraukumi aizmugurservera pakalpojumos, ietekmējot transportlīdzekļa darbību	2.1.	Uzbrukums aizmugurserverim aptur tā darbību, piemēram, neļauj tam mijiedarboties ar transportlīdzekļiem un nodrošināt nepieciešamos pakalpojumus

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
	3.	Ar transportlīdzekli saistītie dati aizmugurserverī pazūd vai notiek iejaukšanās tajos ("datu drošības pārkāpums")	3.1.	Darbinieku pilnvaru ļaunprātīga izmantošana (uzbrukums no iekšienes)
			3.2.	Informācijas zudums mākonī. Sensitīvus datus var pazaudēt uzbrukumu vai negadījumu dēļ, kad datus glabā trešās puses mākoņdatošanas pakalpojumu sniedzēji
			3.3.	Nesankcionēta piekļuve serverim caur internetu (ko iespējo, piemēram, slepenpiekļuve, sistēmas programmatūras nelabotas ievainojamības, *SQL* uzbrukumi vai citi līdzekļi)
			3.4.	Nesankcionēta fiziska piekļuve serverim (kas notiek, piemēram, USB zibatmiņām vai citiem datu nesējiem savienojoties ar serveri)
			3.5.	Informācijas drošības pārkāpums, netīši kopīgojot datus (piem., administratora kļūdas)
4.3.2. Transportlīdzekļa apdraudējumi attiecībā uz to saziņas kanāliem	4.	Transportlīdzekļa saņemto ziņojumu vai datu viltošana	4.1.	Ziņojumu viltošana, uzdodoties par citu (piem., 802.11p V2X sasaistes laikā kolonnā, *GNSS* paziņojumi u.t.t.)
			4.2.	*Sybil* uzbrukums (lai mānītu citus transportlīdzekļus, ka uz ceļa ir daudz transportlīdzekļu)
	5.	Sakaru kanāli, ko izmanto transportlīdzeklī esošo kodu/datu neatļautu manipulāciju, dzēšanas vai citu sagrozījumu veikšanai	5.1.	Sakaru kanāli pieļauj koda injicēšanu, piemēram, neatļauti pārveidotu programmatūras bināro kodu var injicēt sakaru plūsmā
			5.2.	Sakaru kanāli pieļauj transportlīdzeklī esošo datu/kodu manipulācijas
			5.3.	Sakaru kanāli pieļauj transportlīdzeklī esošo datu/kodu pārrakstīšanu
			5.4.	Sakaru kanāli pieļauj transportlīdzeklī esošo datu/kodu dzēšanu
			5.5.	Sakaru kanāli pieļauj datu/kodu ievadīšanu transportlīdzeklī (datu rakstīšanas kods)
	6.	Sakaru kanāli pieļauj neuzticamu/nedrošu ziņojumu pieņemšanu vai ir neaizsargāti pret sesiju pārņemšanu/atkārtošanas uzbrukumiem	6.1.	Informācijas pieņemšana no neuzticama vai nedroša avota
			6.2.	Pārtvērējuzbrukums/ sesijas pārņemšana
			6.3.	Atkārtošanas uzbrukums, piemēram, uzbrukums sakaru vārtejai ļauj uzbrucējam pazemināt *ECU* programmatūru vai vārtejas aparātprogrammatūru

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
	7.	Informācija var tikt viegli atklāta. Piemēram, veicot sakaru noklausīšanos vai atļaujot nesankcionētu piekļuvi sensitīvām datnēm vai mapēm	7.1.	Informācijas pārtveršana / traucējumu raidīšana / sakaru pārraudzīšana
			7.2.	Nesankcionētas piekļuves iegūšana datnēm vai datiem
	8.	Pakalpojumatteices uzbrukums pa sakaru kanāliem, lai traucētu transportlīdzekļa funkcijas	8.1.	Liela daudzuma drazu datu sūtīšana uz transportlīdzekļa informācijas sistēmu, lai tā nespētu normāli sniegt pakalpojumus
			8.2.	Melnā cauruma uzbrukums; lai traucētu sakarus starp transportlīdzekļiem, uzbrucējs spēj bloķēt ziņojumus starp transportlīdzekļiem
	9.	Nepriviliģēts lietotājs var iegūt priviliģētu piekļuvi transportlīdzekļa sistēmām	9.1.	Nepriviliģēts lietotājs var iegūt priviliģētu piekļuvi, piem., ar superlietotāja tiesībām
	10.	Sakaru līdzeklī iegulti vīrusi spēj inficēt transportlīdzekļa sistēmas	10.1.	Sakaru līdzeklī iegults vīruss inficē transportlīdzekļa sistēmas
	11.	Transportlīdzekļa saņemtajiem vai tā robežās pārraidītajiem ziņojumiem (piemēram, X2V vai diagnostikas ziņojumi) ir ļaunprātīgs saturs	11.1.	Ļaunprātīgi iekšējie (piem., *CAN*) ziņojumi
			11.2.	Ļaunprātīgi V2X ziņojumi, piem., no infrastruktūras transportlīdzeklim vai ziņojumi transportlīdzeklis-transportlīdzeklis (piem., *CAM*, *DENM*)
			11.3.	Ļaunprātīgi diagnostikas ziņojumi
			11.4.	Ļaunprātīgi īpašniekziņojumi (piem., tādi, ko parasti sūta *OEM* vai sastāvdaļas/ sistēmas/funkcijas piegādātājs)
4.3.3. Transportlīdzekļa apdraudējumi attiecībā uz atjaunināšanas procedūrām	12.	Atjaunināšanas procedūru nepareiza izmantošana vai iejaukšanās tajās	12.1.	Iejaukšanās programmatūras atjaunināšanas procedūrās, ko veic pa bezvadu kanālu. Tas ietver sistēmas atjaunināšanas programmas vai aparātprogrammatūras fabricēšanu
			12.2.	Iejaukšanās lokālās/fiziskās programmatūras atjaunināšanas procedūrās. Tas ietver sistēmas atjaunināšanas programmas vai aparātprogrammatūras fabricēšanu
			12.3.	Programmatūrā veikta neatļauta iejaukšanās pirms atjaunināšanas procesa (un tādēļ tā ir bojāta), lai gan atjaunināšanas process ir neskarts

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
			12.4.	Iejaukšanās programmatūras nodrošinātāja kriptogrāfiskajās atslēgās, lai atļautu nederīgu atjaunināšanu
	13.	Ir iespējams liegt leģitīmus atjauninājumus	13.1.	Pakalpojumatteices uzbrukums atjaunināšanas serverim vai tīklam, lai nepieļautu kritiski svarīgu programmatūras atjauninājumu uzsākšanu un/vai atbloķētu klientam specifiskas funkcijas
4.3.4. Transportlīdzekļa apdraudējumi attiecībā uz netīšām cilvēka darbībām, kas veicina kiberuzbrukumu	15.	Leģitīmi operatori var veikt darbības, kas neapzināti veicinātu kiberuzbrukumu	15.1.	Nevainīgs cietušais (piem., īpašnieks, operators vai uzturēšanas inženieris) ar viltu iesaistīts darbības veikšanā, lai neapzināti ielādētu ļaunprogrammatūru vai pieļautu uzbrukumu
			15.2.	Netiek izpildītas definētas drošības procedūras
4.3.5. Transportlīdzekļa apdraudējumi attiecībā uz to ārējo savienojamību un savienojumiem	16.	Neatļauta iejaukšanās transportlīdzekļa funkciju savienojamībā iespējo kiberuzbrukumu, tas var ietvert telemātiku; sistēmas, kas pieļauj attālinātas darbības; un sistēmas, kas izmanto maza darbības attāluma bezvadu sakarus	16.1.	Neatļauta iejaukšanās funkcijās, kas konstruētas tādu sistēmu attālinātai darbināšanai kā tālvadības atslēga, imobilaizers un ielas uzlāde
			16.2.	Neatļauta iejaukšanās transportlīdzekļa telemātikā (piem., neatļauta iejaukšanās jutīgu kravu temperatūras mērīšanā, kravas nodalījuma durvju attālināta atslēgšana)
			16.3.	Iejaukšanās maza darbības attāluma bezvadu sistēmās vai sensoros
	17.	Mitināta trešo pušu programmatūra, piem., izklaides lietojumprogrammas, tiek izmantotas kā līdzeklis uzbrukšanai transportlīdzekļa sistēmām	17.1.	Bojātas lietojumprogrammas vai lietotnes ar sliktu programmatūras drošību izmantotas kā metode uzbrukšanai transportlīdzekļa sistēmām
	18.	Ārējām saskarnēm, piem., *USB* pieslēgvietām, *OBD* pieslēgvietai, pieslēgtas ierīces izmantotas kā līdzeklis uzbrukšanai transportlīdzekļa sistēmām	18.1.	Tādas ārējās saskarnes kā *USB* vai citas pieslēgvietas izmantotas par uzbrukuma punktu, piemēram, injicējot kodu
			18.2.	Ar vīrusu inficēti datu nesēji pieslēgti transportlīdzekļa sistēmai
			18.3.	Diagnostikas piekļuve (piem., sargspraudņi *OBD* pieslēgvietā) izmantoti uzbrukuma atvieglošanai, piem., lai neatļauti iejauktos transportlīdzekļa parametros (tieši vai netieši)
4.3.6. Transportlīdzekļa datu/koda apdraudējumi	19.	Transportlīdzekļa datu/koda izgūšana	19.1.	Ar autortiesībām aizsargātas vai īpašnieka programmatūras izgūšana no transportlīdzekļu sistēmām (izstrādājuma pirātisms)
			19.2.	Nesankcionēta piekļuve īpašnieka tādai privātuma informācijai kā personas identitāte, informācija par norēķinu kontu, adrešu grāmatas informācija, informācija par atrašanās vietu, transportlīdzekļa elektroniskā ID u.t.t.
			19.3.	Kriptogrāfisko atslēgu izgūšana

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
	20.	Neatļauta iejaukšanās transportlīdzekļa datos/kodā	20.1.	Prettiesiskas/neatļautas izmaiņas transportlīdzekļa elektroniskajā ID
			20.2.	Krāpšanās ar identitāti. Piemēram, ja lietotājs vēlas parādīt citu identitāti, sazinoties ar nodevu iekasēšanas sistēmām, ražotāja aizmugurserveri
			20.3.	Darbība pārraudzības sistēmu (piem., tādu ziņojumu kā *ODR* izsekotāja dati vai braucienu skaits uzlaušana/ neatļauta iejaukšanās tajos/ bloķēšana) apiešanai
			20.4.	Manipulācijas ar datiem, lai falsificētu transportlīdzekļa braukšanas datus (piem., nobraukumu, braukšanas ātrumu, braukšanas norādījumus u.t.t.)
			20.5.	Neatļautas izmaiņas sistēmas diagnostikas datos
	21.	Datu/koda dzēšana	21.1.	Sistēmas notikumu ierakstu neatļauta dzēšana/manipulācija
	22.	Ļaunprogrammatūras ieviešana	22.2.	Ieviest vai iedarbināt ļaunprogrammatūru
	23.	Jaunas programmatūras ieviešana vai esošās programmatūras pārrakstīšana	23.1.	Transportlīdzekļa vadības sistēmas vai informācijas sistēmas programmatūras fabricēšana
	24.	Sistēmu vai darbības traucējumi	24.1.	Pakalpojumatteici, piemēram, var izraisīt iekšējā tīklā, pārslogojot *CAN* kopni vai izraisot kļūdas *ECU* ar lielu ziņojumapmaiņas apjomu
	25.	Manipulācijas ar transportlīdzekļa parametriem	25.1.	Nesankcionēta piekļuve vai transportlīdzekļa tādu galveno funkciju konfigurācijas parametru falsificēšana kā bremžu dati, drošības spilvena lietojuma robežnosacījumi utt.
			25.2.	Nesankcionēta piekļuve vai tādu uzlādes parametru falsificēšana kā uzlādes spriegums, uzlādes jauda, akumulatoru baterijas temperatūra utt.
4.3.7. Potenciālās ievainojamības, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas	26.	Var notikt iejaukšanās kriptogrāfijas tehnoloģijās vai tās ir nepietiekami lietotas	26.1.	Īsu šifrēšanas atslēgu un ilgstoša derīguma apvienojums ļauj uzbrucējam uzlauzt šifrēšanu
			26.2.	Kriptogrāfisko algoritmu nepietiekama izmantošana sensitīvu sistēmu aizsardzībai
			26.3.	Jau novecojušu vai drīzumā jau novecojušu kriptogrāfisko algoritmu izmantošana

Ievainojamības/apdraudējuma augsta līmeņa un apakšlīmeņa apraksti			Ievainojamības vai uzbrukuma metodes piemērs	
	27.	Var notikt iejaukšanās daļās vai krājumos, kas ļauj uzbrukt transportlīdzekļiem	27.1.	Aparatūra vai programmatūra izstrādāta tā, ka pieļauj uzbrukumu vai neatbilst konstrukcijas kritērijiem uzbrukuma apturēšanai
	28.	Aparatūras vai programmatūras izstrāde pieļauj ievainojamības	28.1.	Programmatūras kļūdas. Programmatūras kļūdas varētu būt pamats iespējamām izmantojamām ievainojamībām. Tas ir īpaši aktuāli, ja programmatūra nav testēta, lai pārliecinātos par jau zināmu nepilnīgu kodu/kļūdu esību un mazinātu nezināmu nepilnīgu kodu/defektu esības risku
			28.2.	Izstrādātāja atgādinājumu (piem., atkļūdošanas pieslēgvietas, *JTAG* pieslēgvietas, mikroprocesori, izstrādes sertifikāti, izstrādātāja paroles) izmantošana var ļaut piekļūt *ECU* vai ļaut uzbrucējiem iegūt lielākas privilēģijas
	29.	Tīkla izveidojums ievieš ievainojamības	29.1.	Atstāti atvērti lieki interneta porti, nodrošinot piekļuvi tīkla sistēmām
			29.2.	Apiet tīkla nodalījumu, lai pārņemtu vadību. Konkrēts piemērs ir neaizsargātu vārteju vai tādu piekļuves punktu kā kravas automobiļa-piekabes vārtejas izmantošana, lai apietu aizsardzību un iegūtu piekļuvi citiem tīkla segmentiem nolūkā veikt tādas ļaunprātīgas darbības kā patvaļīga *CAN* kopnes ziņojumu sūtīšana
	31.	Var notikt netīša datu pārsūtīšana	31.1.	Informācijas drošības pārkāpums. Var tikt nopludināti persondati, kad mainās vieglā automobiļa lietotājs (piem., to pārdod vai jauni īrētāji to izmanto kā nomātu transportlīdzekli)
	32.	Uzbrukumu var pieļaut sistēmu fiziska manipulācija	32.1.	Elektroniskās aparatūras manipulācijas, piem., neatļautas elektroniskās aparatūras pievienošana transportlīdzeklim, lai iespējotu pārtvērējuzbrukumu Atļautas elektroniskās aparatūras (piem., sensora) nomaiņa ar neatļautu elektronisko aparatūru Sensora savāktās informācijas manipulēšana (piemēram, izmantojot magnētu, lai neatļauti iejauktos pārnesumkārbai pievienotajā Hola devējā)

B daļa Uz transportlīdzekli mērķēto apdraudējumu mazināšanas

1. Mazināšana attiecībā uz "transportlīdzekļa sakaru kanāliem"

Ar "transportlīdzekļa sakaru kanāliem" saistīto apdraudējumu mazināšanas ir uzskaitītas B1. tabulā.

B1. tabula

Ar "transportlīdzekļa sakaru kanāliem" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Transportlīdzekļa sakaru kanālu" apdraudējumi	Ats.	Mazināšana
4.1.	Ziņojumu viltošana (piem., 802.11p V2X sasaistes laikā kolonnā, *GNSS* paziņojumi u.t.t.), uzdodoties par citu	M10	Transportlīdzeklis verificē saņemto ziņojumu autentiskumu un integritāti
4.2.	*Sybil* uzbrukums (lai mānītu citus transportlīdzekļus, ka uz ceļa ir daudz transportlīdzekļu)	M11	Jāīsteno drošības kontrole attiecībā uz kriptogrāfisko atslēgu glabāšanu (piem., lietot aparatūras drošības moduļus)
5.1.	Sakaru kanāli pieļauj koda injicēšanu transportlīdzeklī glabātajos datos/kodā, piemēram, neatļauti pārveidotu programmatūras bināro kodu var injicēt sakaru plūsmā	M10 M6	Transportlīdzeklis verificē saņemto ziņojumu autentiskumu un integritāti Lai samazinātu risku, sistēmām jāīsteno jau konstrukcijā iekļauti drošības pasākumi
5.2.	Sakaru kanāli pieļauj manipulācijas ar transportlīdzeklī glabātajiem datiem/kodu	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas
5.3.	Sakaru kanāli pieļauj transportlīdzeklī glabāto datu/kodu pārrakstīšanu		
5.4. 21.1.	Sakaru kanāli pieļauj transportlīdzeklī glabāto datu/kodu dzēšanu		
5.5.	Sakaru kanāli pieļauj datu/koda ievadīšanu transportlīdzekļa sistēmās (datu rakstīšanas kods)		
6.1.	Informācijas pieņemšana no neuzticama vai nedroša avota	M10	Transportlīdzeklis verificē saņemto ziņojumu autentiskumu un integritāti
6.2.	Pārtvērējuzbrukums / sesijas pārņemšana	M10	Transportlīdzeklis verificē saņemto ziņojumu autentiskumu un integritāti
6.3.	Atkārtošanas uzbrukums, piemēram, uzbrukums sakaru vārtejai ļauj uzbrucējam pazemināt *ECU* programmatūru vai vārtejas aparātprogrammatūru		
7.1.	Informācijas pārtveršana / traucējumu raidīšana / sakaru pārraudzīšana	M12	Jābūt aizsargātiem konfidenciālajiem datiem, ko pārraida uz transportlīdzekli vai no tā
7.2.	Nesankcionētas piekļuves iegūšana datnēm vai datiem	M8	Sistēmas uzbūvei un piekļuves kontrolei jābūt tādai, lai nepilnvarotiem darbiniekiem nebūtu iespējas piekļūt personas vai sistēmas kritiskiem datiem. Drošības kontroles piemēru var atrast *OWASP*

Atsauce uz A1. tabulu	"Transportlīdzekļa sakaru kanālu" apdraudējumi	Ats.	Mazināšana
8.1.	Liela daudzuma drazu datu sūtīšana uz transportlīdzekļa informācijas sistēmu, lai tā nespētu normāli sniegt pakalpojumus	M13	Jāizmanto pasākumi, lai konstatētu un atgūtos no pakalpojumatteices uzbrukuma
8.2.	Melnā cauruma uzbrukums, sakaru traucējums starp transportlīdzekļiem, bloķējot ziņojumu pārsūtīšanu uz citiem transportlīdzekļiem	M13	Jāizmanto pasākumi, lai konstatētu un atgūtos no pakalpojuma atteikuma uzbrukuma
9.1.	Nepriviliģēts lietotājs var iegūt priviliģētu piekļuvi, piem., ar superlietotāja tiesībām	M9	Jāizmanto pasākumi, lai nepieļautu un konstatētu nesankcionētu piekļuvi
10.1.	Sakaru līdzeklī iegults vīruss inficē transportlīdzekļa sistēmas	M14	Jāapsver pasākumi sistēmu aizsardzībai pret iegultiem vīrusiem/ļaunprogrammatūru
11.1.	Ļaunprātīgi iekšējie (piem., *CAN*) ziņojumi	M15	Jāapsver pasākumi ļaunprātīgu iekšējo ziņojumu vai darbību konstatēšanai
11.2.	Ļaunprātīgi V2X ziņojumi, piem., ziņojumi no infrastruktūras transportlīdzeklim vai ziņojumi transportlīdzeklis-transportlīdzeklis (piem., *CAM*, *DENM*)	M10	Transportlīdzeklis verificē saņemto ziņojumu autentiskumu un integritāti
11.3.	Ļaunprātīgi diagnostikas ziņojumi		
11.4.	Ļaunprātīgi īpašniekziņojumi (piem., tādi, ko parasti sūta *OEM* vai sastāvdaļas/ sistēmas/funkcijas piegādātājs)		

2. Mazināšanas attiecībā uz "atjauninašanas procesu"

Ar "atjauninašanas procesu" saistīto apdraudējumu mazināšanas ir uzskaitītas B2. tabulā.

B2. tabula

Ar "atjauninašanas procesu" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Atjauninašanas procesa" apdraudējumi	Ats.	Mazināšana
12.1.	Iejaukšanās programmatūras atjauninašanas procedūrās, ko veic pa bezvadu kanālu. Tas ietver sistēmas atjauninašanas programmas vai aparātprogrammatūras fabricēšanu	M16	Jāizmanto drošas programmatūras atjauninašanas procedūras
12.2.	Iejaukšanās lokālās/fiziskās atjauninašanas procedūrās. Tas ietver sistēmas atjauninašanas programmas vai aparātprogrammatūras fabricēšanu		
12.3.	Programmatūrā veikta neatļauta iejaukšanās pirms atjauninašanas procesa (un tādēļ tā ir bojāta), lai gan atjauninašanas process ir neskarts		

Atsauce uz A1. tabulu	"Atjaunināšanas procesa" apdraudējumi	Ats.	Mazināšana
12.4.	Iejaukšanās programmatūras nodrošinātāja kriptogrāfiskajās atslēgās, lai atļautu nederīgu atjaunināšanu	M11	Kriptogrāfisko atslēgu glabāšanai jāizmanto drošības kontrole
13.1.	Pakalpojumatteices uzbrukums atjaunināšanas serverim vai tīklam, lai nepieļautu kritiski svarīgu programmatūras atjauninājumu uzsākšanu un/vai atbloķētu klientam specifiskas funkcijas	M3	Drošības kontrole jāpiemēro aizmugursistēmām. Ja aizmugurserveri ir kritiski svarīgi pakalpojuma sniegšanai, ir atkopšanas pasākumi sistēmas darbības pārtraukšanas gadījumā. Drošības kontroles piemēru var atrast *OWASP*

3. Mazināšanas attiecībā uz "kiberuzbrukumu veicinošām netīšām cilvēka darbībām"

Ar "kiberuzbrukumu veicinošām netīšām cilvēka darbībām" saistīto apdraudējumu mazināšanas ir uzskaitītas B3. tabulā.

B3. tabula

Ar "kiberuzbrukumu veicinošām netīšām cilvēka darbībām" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	Apdraudējumi attiecībā uz "netīšām cilvēka darbībām"	Ats.	Mazināšana
15.1.	Nevainīgs cietušais (piem., īpašnieks, operators vai uzturēšanas inženieris) ar viltu iesaistīts darbības veikšanā, lai neapzināti ielādētu ļaunprogrammatūru vai pieļautu uzbrukumu	M18	Jāievieš pasākumi, lai noteiktu un kontrolētu lietotāju lomas un piekļuves pilnvaras, balstoties uz mazākās piekļuves pilnvarojuma principu
15.2.	Netiek izpildītas definētas drošības procedūras	M19	Organizācijām ir jānodrošina tas, ka drošības procedūras ir definētas un izpildītas, tostarp darbību un piekļuves reģistrēšana saistībā ar drošības funkciju pārvaldību

4. Mazināšanas attiecībā uz "ārējo savienojamību un savienojumiem"

Ar "ārējo savienojamību un savienojumiem" saistīto apdraudējumu mazināšanas ir uzskaitītas B4. tabulā.

B4. tabula

Ar "ārējo savienojamību un savienojumiem" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Ārējās savienojamības un savienojumu" apdraudējumi	Ats.	Mazināšana
16.1.	Neatļauta iejaukšanās funkcijās, kas konstruētas tādu transportlīdzekļa sistēmu attālinātai darbināšanai kā tālvadības atslēgā, imobilaizers un ielas uzlāde	M20	Sistēmām ar attālinātu piekļuvi jāpiemēro drošības kontrole
16.2.	Neatļauta iejaukšanās transportlīdzekļa telemātikā (piem., neatļauta iejaukšanās jutīgu kravu temperatūras mērīšanā, kravas nodalījuma durvju attālināta atslēgšana)		

Atsauce uz A1. tabulu	"Ārējās savienojamības un savienojumu" apdraudējumi	Ats.	Mazināšana
16.3.	Iejaukšanās maza darbības attāluma bezvadu sistēmās vai sensoros		
17.1.	Bojātas lietojumprogrammas vai lietotnes ar sliktu programmatūras drošību izmantotas kā metode uzbrukšanai transportlīdzekļa sistēmām	M21	Programmatūra jānovērtē attiecībā uz drošību, jāautentificē un jāaizsargā tās integritāte Jāpiemēro drošības kontrole, lai mazinātu risku no trešo pušu programmatūras puses, kura ir paredzēta vai kuru ir paredzams mitināt transportlīdzeklī
18.1.	Tādas ārējās saskarnes kā *USB* vai citas pieslēgvietas izmantotas par uzbrukuma punktu, piemēram, injicējot kodu	M22	Drošības kontrole jāpiemēro ārējām saskarnēm.
18.2.	Ar vīrusu inficēti datu nesēji savienoti ar transportlīdzekli		
18.3.	Diagnostikas piekļuve (piem., sargspraudņi *OBD* pieslēgvietā) izmantoti uzbrukuma atvieglošanai, piem., lai neatļauti iejauktos transportlīdzekļa parametros (tieši vai netieši)	M22	Drošības kontrole jāpiemēro ārējām saskarnēm.

5. Mazināšanas attiecībā uz "uzbrukuma potenciālajiem mērķiem vai motivācijām"

Ar "uzbrukuma potenciālajiem mērķiem vai motivācijām" saistīto apdraudējumu mazināšanas ir uzskaitītas B5. tabulā.

B5. tabula

Ar "uzbrukuma potenciālajiem mērķiem vai motivācijām" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Uzbrukuma potenciālo mērķu vai motivāciju" apdraudējumi	Ats.	Mazināšana
19.1.	Ar autortiesībām aizsargātas vai īpašnieka programmatūras izgūšana no transportlīdzekļu sistēmām (izstrādājuma pirātisms / zagta programmatūra)	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*
19.2.	Nesankcionēta piekļuve īpašnieka tādai privātuma informācijai kā personas identitāte, informācija par norēķinu kontu, adrešu grāmatas informācija, informācija par atrašanās vietu, transportlīdzekļa elektroniskā ID u.t.t.	M8	Sistēmas uzbūvei un piekļuves kontrolei jābūt tādai, lai nepilnvarotiem darbiniekiem nebūtu iespējas piekļūt personas vai sistēmas kritiskiem datiem. Drošības kontroles piemērus var atrast *OWASP*
19.3.	Kriptogrāfisko atslēgu izgūšana	M11	Jāīsteno drošības kontrole attiecībā uz kriptogrāfisko atslēgu glabāšanu, piem., drošības moduļi
20.1.	Prettiesiskas/neatļautas izmaiņas transportlīdzekļa elektroniskajā ID	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*
20.2.	Krāpšanās ar identitāti. Piemēram, ja lietotājs vēlas parādīt citu identitāti, sazinoties ar nodevu iekasēšanas sistēmām, ražotāja aizmugurserveri		
20.3.	Darbība pārraudzības sistēmu (piem., tādu ziņojumu kā *ODR* izsekotāja dati vai braucienu skaits uzlaušana/ neatļauta iejaukšanās tajos/ bloķēšana) apiešanai	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*.

Atsauce uz A1. tabulu	"Uzbrukuma potenciālo mērķu vai motivāciju" apdraudējumi	Ats.	Mazināšana
20.4.	Manipulācijas ar datiem, lai falsificētu transportlīdzekļa braukšanas datus (piem., nobraukumu, braukšanas ātrumu, braukšanas norādījumus u.t.t.)		Datu manipulāciju uzbrukumu sensoriem vai nosūtītajiem datiem sekas varētu mazināt, veicot dažādu avotu datu korelāciju
20.5.	Neatļautas izmaiņas sistēmas diagnostikas datos		
21.1.	Sistēmas notikumu ierakstu neatļauta dzēšana/manipulācija	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*.
22.2.	Ieviest vai iedarbināt ļaunprogrammatūru	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*.
23.1.	Transportlīdzekļa vadības sistēmas vai informācijas sistēmas programmatūras fabricēšana		
24.1.	Pakalpojumatteici, piemēram, var izraisīt iekšējā tīklā, pārslogojot *CAN* kopni vai izraisot kļūdas *ECU* ar lielu ziņojumapmaiņas apjomu	M13	Jāizmanto pasākumi, lai konstatētu un atgūtos no pakalpojuma atteikuma uzbrukuma
25.1.	Nesankcionēta piekļuve, lai falsificētu tādus transportlīdzekļa galveno funkciju konfigurācijas parametrus kā bremžu dati, drošības spilvena lietojuma robežnosacījumi utt.	M7	Lai aizsargātu sistēmas datus/kodu, piemēro piekļuves kontroles paņēmienus un konstrukcijas. Drošības kontroles piemēru var atrast *OWASP*
25.2.	Nesankcionēta piekļuve, lai falsificētu tādus uzlādes parametrus kā uzlādes spriegums, uzlādes jauda, akumulatoru baterijas temperatūra utt.		

6. "Potenciālo ievainojamību, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas" mazināšanas

Ar "potenciālajām ievainojamībām, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas" saistīto apdraudējumu mazināšanas ir uzskaitītas B6. tabulā.

B6. tabula

Ar "potenciālajām ievainojamībām, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Potenciālo ievainojamību, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas" apdraudējumi	Ats.	Mazināšana
26.1.	Īsu šifrēšanas atslēgu un ilgstoša derīguma apvienojums ļauj uzbrucējam uzlauzt šifrēšanu	M23	Jāievēro kiberdrošības labākā prakse programmatūras un aparatūras izstrādē

Atsauce uz A1. tabulu	"Potenciālo ievainojamību, kuras varētu izmantot, ja tās nav pietiekami aizsargātas vai nostiprinātas" apdraudējumi	Ats.	Mazināšana
26.2.	Kriptogrāfisko algoritmu nepietiekama izmantošana sensitīvu sistēmu aizsardzībai		
26.3.	Novecojušu kriptogrāfisko algoritmu izmantošana		
27.1.	Aparatūra vai programmatūra izstrādāta tā, ka pieļauj uzbrukumu vai neatbilst konstrukcijas kritērijiem uzbrukuma apturēšanai	M23	Jāievēro kiberdrošības labākā prakse programmatūras un aparatūras izstrādē
28.1.	Programmatūras kļūdas varētu būt pamats iespējamām izmantojamām ievainojamībām. Tas ir īpaši aktuāli, ja programmatūra nav testēta, lai pārliecinātos par jau zināmu nepilnīgu kodu/kļūdu esību un mazinātu nezināmu nepilnīgu kodu/defektu esības risku	M23	Jāievēro kiberdrošības labākā prakse programmatūras un aparatūras izstrādē Kiberdrošības testēšana ar pienācīgu tvērumu
28.2.	Izstrādātāja atgādinājumu (piem., atkļūdošanas pieslēgvietas, *JTAG* pieslēgvietas, mikroprocesori, izstrādes sertifikāti, izstrādātāja paroles) izmantošana var atļaut piekļuvi *ECU* vai ļaut uzbrucējiem iegūt lielākas privilēģijas		
29.1.	Atstāti atvērti lieki interneta porti, nodrošinot piekļuvi tīkla sistēmām		
29.2.	Apiet tīkla nodalījumu, lai pārņemtu vadību. Konkrēts piemērs ir neaizsargātu vārteju vai tādu piekļuves punktu kā kravas automobiļa-piekabes vārtejas izmantošana, lai apietu aizsardzību un iegūtu piekļuvi citiem tīkla segmentiem nolūkā veikt tādas ļaunprātīgas darbības kā patvaļīga *CAN* kopnes ziņojumu sūtīšana	M23	Jāievēro kiberdrošības labākā prakse programmatūras un aparatūras izstrādē. Jāievēro kiberdrošības labākā prakse sistēmu konstrukcijā un sistēmas integrēšanā

7. "Transportlīdzekļa datu zudumu / datu drošības pārkāpumu" mazināšanas

Ar "transportlīdzekļa datu zudumu / datu drošības pārkāpumu" saistīto apdraudējumu mazināšanas ir uzskaitītas B7. tabulā.

B7. tabula

Ar "transportlīdzekļa datu zudumu / datu drošības pārkāpumu" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Transportlīdzekļa datu zudumu / datu drošības pārkāpumu" apdraudējumi	Ats.	Mazināšana
31.1.	Informācijas drošības pārkāpums. Var notikt persondatu drošības pārkāpums, kad mainās vieglā automobiļa lietotājs (piem., to pārdod vai jauni īrētāji to izmanto kā nomātu transportlīdzekli)	M24	Uzglabājot persondatus, jāievēro datu integritātes un konfidencialitātes aizsardzības labākā prakse, lai uzglabātu persondatus.

8. "Uzbrukumu pieļaujošas sistēmu fiziskas manipulācijas" mazināšanas

Ar "uzbrukumu pieļaujošām sistēmu fiziskām manipulācijām" saistīto apdraudējumu mazināšanas ir uzskaitītas B8. tabulā.

B8. tabula

Ar "uzbrukumu pieļaujošām sistēmu fiziskām manipulācijām" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Uzbrukumu pieļaujošu sistēmu fizisku manipulāciju" apdraudējumi	Ats.	Mazināšana
32.1.	Manipulācijas ar *OEM* aparatūru, piem., neatļautas aparatūras pievienošana transportlīdzeklim, lai iespējotu pārtvērējuzbrukumu	M9	Jāizmanto pasākumi, lai nepieļautu un konstatētu nesankcionētu piekļuvi

C daļa. Ārpus transportlīdzekļa esošu apdraudējumu mazināšanas

1. Mazināšanas attiecībā uz "aizmugurserveriem"

Ar "aizmugurserveriem" saistīto apdraudējumu mazināšanas ir uzskaitītas C1. tabulā.

C1. tabula

Ar "aizmugurserveriem" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Aizmugurserveru" apdraudējumi	Ats.	Mazināšana
1.1. & 3.1.	Darbinieku pilnvaru ļaunprātīga izmantošana (uzbrukums no iekšienes)	M1	Lai mazinātu uzbrukuma no iekšienes risku, aizmugursistēmām piemēro drošības kontroli
1.2. & 3.3.	Nesankcionēta piekļuve serverim caur internetu (ko iespējo, piemēram, slepenpiekļuve, sistēmas programmatūras nelabotas ievainojamības, *SQL* uzbrukumi vai citi līdzekļi)	M2	Lai mazinātu nesankcionētu piekļuvi, aizmugursistēmām piemēro drošības kontroli Drošības kontroles piemēru var atrast *OWASP*
1.3. & 3.4.	Nesankcionēta fiziska piekļuve serverim (kas notiek, piemēram, *USB* zibatmiņām vai citiem datu nesējiem savienojoties ar serveri)	M8	Sistēmas uzbūvei un piekļuves kontrolei jābūt tādai, lai nepilnvarotiem darbiniekiem nebūtu iespējas piekļūt personas vai sistēmas kritiskiem datiem.
2.1.	Uzbrukums aizmugurserverim aptur tā darbību, piemēram, neļauj tam mijiedarboties ar transportlīdzekļiem un nodrošināt nepieciešamos pakalpojumus	M3	Drošības kontroli piemēro aizmugursistēmām. Ja aizmugurserveri ir kritiski svarīgi pakalpojuma sniegšanai, ir atkopšanas pasākumi sistēmas darbības pārtraukšanas gadījumā. Drošības kontroles piemēru var atrast *OWASP*
3.2.	Informācijas zudums mākonī. Sensitīvus datus var pazaudēt uzbrukumu vai negadījumu dēļ, kad datus glabā trešās puses mākoņdatošanas pakalpojumu sniedzēji	M4	Piemēro drošības kontroli, lai mazinātu ar mākoņdatošanu saistītos riskus. Drošības kontroles piemēru var atrast *OWASP* un norādēs par *NCSC* mākoņdatošanu
3.5.	Informācijas drošības pārkāpums, netīši kopīgojot datus (piem., administratora kļūdas, datu uzglabāšana autoremontdarbnīcu serveros)	M5	Lai nepieļautu datu drošības pārkāpumus, aizmugursistēmām piemēro drošības kontroli Drošības kontroles piemēru var atrast *OWASP*

2. Mazināšanas attiecībā uz "netīšu cilvēka darbību"

Ar "netīšām cilvēka darbībām" saistīto apdraudējumu mazināšanas ir uzskaitītas C2. tabulā.

C2. tabula

Ar "netīšām cilvēka darbībām" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	Apdraudējumi attiecībā uz "netīšām cilvēka darbībām"	Ats.	Mazināšana
15.1.	Nevainīgs cietušais (piem., īpašnieks, operators vai uzturēšanas inženieris) ar viltu iesaistīts darbības veikšanā, lai neapzināti ielādētu ļaunprogrammatūru vai pieļautu uzbrukumu	M18	Jāievieš pasākumi, lai noteiktu un kontrolētu lietotāju lomas un piekļuves pilnvaras, balstoties uz mazākās piekļuves pilnvarojuma principu
15.2.	Netiek izpildītas definētas drošības procedūras	M19	Organizācijām ir jānodrošina tas, ka drošības procedūras ir definētas un izpildītas, tostarp darbību un piekļuves reģistrēšana saistībā ar drošības funkciju pārvaldību

3. "Datu fiziska zuduma" mazināšana

Ar "datu fizisku zudumu" saistīto apdraudējumu mazināšanas ir uzskaitītas C3. tabulā.

C3. tabula

Ar "datu fizisku zudumu" saistīto apdraudējumu mazināšanas

Atsauce uz A1. tabulu	"Datu fiziska zuduma" apdraudējumi	Ats.	Mazināšana
30.1.	Trešās puses radīti zaudējumi Satiksmes negadījuma vai zādzības gadījumā sensitīvi dati var tikt zaudēti vai var notikt iejaukšanās tajos fizisku bojājumu dēļ	M24	Uzglabājot persondatus, jāievēro datu integritātes un konfidencialitātes aizsardzības labākā prakse. Drošības kontroles piemēru var atrast ISO/SC27/WG5.
30.2.	Zudumi *DRM* (digitālā satura tiesību pārvaldība) konfliktu rezultātā. *DRM* problēmu dēļ var tikt dzēsti lietotāja dati		
30.3.	Sensitīvi dati (to integritāte) var tikt zaudēta *IT* komponentu nolietojuma dēļ, izraisot potenciālas pakārtotās problēmas (piemēram, atslēgas pārveidojumu gadījumā)		