2025/5

10.1.2025

Rahvusvahelise avaliku õiguse alusel on õiguslik toime ainult ÜRO Euroopa Majanduskomisjoni originaaltekstidel. Käesoleva eeskirja staatust ja jõustumise kuupäeva tuleb kontrollida ÜRO Euroopa Majanduskomisjoni staatusdokumendi TRANS/WP.29/343 viimasest versioonist, mis on kättesaadav internetis: https://unece.org/status-1958-agreement-and-annexed-regulations.

Ühinenud Rahvaste Organisatsiooni (ÜRO) eeskiri nr 155: ühtsed sätted, mis käsitlevad sõidukite tüübikinnitust seoses küberturvalisuse ja küberturvalisuse haldamise süsteemiga [2025/5]

Sisaldab kogu kehtivat teksti kuni:

eeskirja algversiooni 3. täiendus – jõustumiskuupäev: 10. jaanuar 2025

Käesolev dokument on üksnes dokumenteerimisvahend. Autentsed ja õiguslikult siduvad tekstid on:

— ECE/TRANS/WP.29/2020/79 (nagu seda on muudetud dokumentidega ECE/TRANS/WP.29/2020/94 ja ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54;

— ECE/TRANS/WP.29/2023/70 ja

— ECE/TRANS/WP.29/2024/55.

SISUKORD

Eeskiri

1. Kohaldamisala
2. Mõisted
3. Tüübikinnituse taotlemine
4. Märgistus
5. Tüübikinnitus
6. Küberturvalisuse haldamise süsteemi vastavustunnistus
7. Tehniline kirjeldus
8. Sõidukitüübi muutmine ja tüübikinnituse laiendamine
9. Tootmise nõuetele vastavus
10. Karistused tootmise nõuetele mittevastavuse korral
11. Tootmise lõpetamine
12. Tüübikinnituskatse eest vastutavate tehniliste teenistuste ja tüübikinnitusasutuste nimed ja aadressid

LISAD

1. Teabedokument
2. Teatis
3. Tüübikinnitusmärgi kujundus
4. Küberturvalisuse haldamise süsteemi vastavustunnistuse näidis
5. Ohtude ja leevendusmeetmete loetelu

1. Kohaldamisala

1.1. Eeskirja kohaldatakse vähemalt ühe elektroonilise juhtseadega L, M-, N- ja O-kategooria sõidukite küberturvalisuse suhtes.

1.2. Eeskiri ei piira muude ÜRO eeskirjade, piirkondlike või riiklike õigusaktide kohaldamist, millega reguleeritakse volitatud poolte juurdepääsu sõidukile, selle andmetele, funktsioonidele ja vahenditele ning sellise juurdepääsu tingimusi. Samuti ei piira see eraelu puutumatust ja füüsiliste isikute kaitset käsitlevate riiklike ja piirkondlike õigusaktide kohaldamist nende isikuandmete töötlemisele.

1.3. Eeskiri ei piira seoses küberturvalisusega muude selliste ÜRO eeskirjade ega riiklike või piirkondlike õigusaktide kohaldamist, millega reguleeritakse füüsiliste ja digitaalsete varuosade ja osiste väljatöötamist ja paigaldamist / süsteemi integreerimist.

2. Mõisted

Käesolevas eeskirjas kasutatakse järgmisi mõisteid.

2.1. „Sõidukitüüp“ – sõidukid, mis ei erine üksteisest vähemalt järgmistes tähtsates aspektides:

a) tootja sõidukitüübi tähistus;

b) elektri-/elektroonikasüsteemi arhitektuuri ja välisliideste küberturvalisuse põhiaspektid.

2.2. „Küberturvalisus“ – olek, kus maanteesõidukid ja nende funktsioonid on kaitstud elektriliste või elektrooniliste osiste küberohtude eest.

2.3. „Küberturvalisuse haldamise süsteem“ – süstemaatiline riskipõhine käsitlus, millega määratletakse töökorralduslikud protsessid, ülesanded ja juhtimine, et ohjata sõidukite küberohtudega seotud riske ja kaitsta sõidukeid küberrünnete eest.

2.4. „Süsteem“ – funktsiooni või funktsioone rakendav osiste ja/või allsüsteemide komplekt.

2.5. „Arendusetapp“ – sõidukitüübi kinnitamisele eelnev ajavahemik.

2.6. „Tootmisetapp“ – sõidukitüübi tootmise ajavahemik.

2.7. „Tootmisjärgne etapp“ – ajavahemik sõidukitüübi tootmise lõpetamisest kuni kõigi sõidukitüübi alla kuuluvate sõidukite kasutusea lõpuni. Konkreetse sõidukitüübi alla kuuluvad sõidukid on selles etapis töökorras, kuid nende tootmine on lõpetatud. See etapp lõpeb siis, kui enam ei ole alles ühtegi konkreetse sõidukitüübi alla kuuluvat töökorras sõidukit.

2.8. „Leevendusmeede“ – riski vähendav meede.

2.9. „Risk“ – võimalus, et kindel oht kasutab ära sõiduki turvanõrkusi ja kahjustab seeläbi organisatsiooni või üksikisikut.

2.10. „Riskihindamine“ – protsess, mis hõlmab riskide avastamist, äratundmist ja kirjeldamist (riski tuvastamine) riski olemuse mõistmiseks ja riski taseme kindlaksmääramiseks (riskianalüüs) ning riskianalüüsi tulemuste võrdlemist riskikriteeriumidega, et teha kindlaks, kas risk ja/või selle suurus on vastuvõetav või talutav (riski hindamine).

2.11. „Riskijuhtimine“ – koordineeritud tegevus organisatsiooni riskide juhtimiseks ja kontrollimiseks.

2.12. „Oht“ – soovimatu intsidendi võimalik põhjus, mis võib tekitada kahju süsteemile, organisatsioonile või üksikisikule.

2.13. „Turvanõrkus“ – vara või leevendusmeetme nõrkus, mida võidakse ühe või mitme ohu abil ära kasutada.

3. Tüübikinnituse taotlemine

3.1. Sõiduki tüübikinnituse taotluse seoses küberturvalisusega esitab sõiduki tootja või tema nõuetekohaselt volitatud esindaja.

3.2. Koos taotlusega tuleb esitada järgmised dokumendid kolmes eksemplaris ja järgmised andmed.

3.2.1. Sõidukitüübi kirjeldus seoses käesoleva eeskirja 1. lisas täpsustatud andmetega.

3.2.2. Juhul kui teave on kaitstud intellektuaalomandi õigustega või on tegu tootja või tema tarnijate eriomase oskusteabega, teeb tootja või teevad tema tarnijad kättesaadavaks piisava teabe, mis võimaldab käesolevas eeskirjas osutatud kontrolli nõuetekohast läbiviimist. Sellist teavet käsitletakse konfidentsiaalsena.

3.2.3. Käesoleva eeskirja punktile 6 vastav küberturvalisuse haldamise süsteemi vastavustunnistus.

3.3. Dokumentatsioon tehakse kättesaadavaks kahes osas:

a) tüübikinnituse saamiseks esitatav ametlik dokumendipakett, mis sisaldab 1. lisas loetletud materjale ja esitatakse tüübikinnitusasutusele või selle tehnilisele teenistusele tüübikinnituse taotluse esitamise ajal. Tüübikinnitusasutus või selle tehniline teenistus kasutab seda dokumendipaketti tüübikinnitusmenetluses võrdlusalusena. Tüübikinnitusasutus või selle tehniline teenistus peab tagama, et dokumendipakett jääb kättesaadavaks vähemalt kümneks aastaks alates sõidukitüübi tootmise lõpetamisest;

b) käesoleva eeskirja nõuete täitmiseks vajalikud lisamaterjalid võivad jääda tootja valdusse, kuid need tuleb tüübikinnituse ajal teha kontrollimise tarvis kättesaadavaks. Tootja tagab, et tüübikinnituse ajal kontrollimise tarvis kättesaadavaks tehtud materjalid jäävad kättesaadavaks veel vähemalt kümneks aastaks alates sõidukitüübi tootmise lõpetamisest.

4. Märgistus

4.1. Igale käesoleva eeskirja kohaselt kinnitatud tüübile vastavale sõidukile tuleb kinnitada tüübikinnituse vormil kindlaksmääratud hästi märgatavasse ja kergesti juurdepääsetavasse kohta rahvusvaheline tüübikinnitusmärk, millel on:

4.1.1. ringjoonega ümbritsetud E-täht, millele järgneb tüübikinnituse andnud riigi tunnusnumber;

4.1.2. punktis 4.1.1 kirjeldatud ringist paremal käesoleva eeskirja number, millele järgneb R-täht, mõttekriips ja tüübikinnituse number.

4.2. Kui sõiduk vastab sõidukitüübile, mis on käesolevale eeskirjale vastava tüübikinnituse andnud riigis saanud tüübikinnituse ühe või mitme kokkuleppele lisatud muu eeskirja alusel, ei ole punktis 4.1.1 sätestatud tähist vaja korrata; sel juhul paigutatakse kõikide käesolevale eeskirjale vastava tüübikinnituse andnud riigis tüübikinnituse andmise aluseks olnud eeskirjade numbrid, tüübikinnitusnumbrid ning lisatähised tulpadena punktis 4.1.1 sätestatud tähisest paremale.

4.3. Tüübikinnitusmärk peab olema selgesti loetav ja kustumatu.

4.4. Tüübikinnitusmärk paigutatakse tootja kinnitatud sõiduki andmeplaadile või selle lähedusse.

4.5. Näited tüübikinnitusmärgi kujunduse kohta on esitatud käesoleva eeskirja 3. lisas.

5. Tüübikinnitus

5.1. Tüübikinnitusasutused annavad küberturvalisusega seotud tüübikinnituse ainult käesoleva eeskirja nõuetele vastavatele sõidukitüüpidele.

5.1.1. Tüübikinnitusasutus või tehniline teenistus teeb dokumentide kontrollimisega kindlaks, kas sõiduki tootja on võtnud sõidukitüübile vastavad vajalikud meetmed, et:

a) koguda ja kontrollida käesoleva eeskirjaga nõutavat teavet tarneahelas eesmärgiga näidata, et tarnijatega seotud riske tuvastatakse ja juhitakse;

b) dokumenteerida sõidukitüübile kohaldatud (arendusetapis või tagasiulatuvalt ellu viidav) riskihindamine, katsetulemused ja leevendusmeetmed, sealhulgas riskihindamist toetav konstrueerimisteave;

c) rakendada sõidukitüübi konstrueerimisel asjakohaseid küberturvalisuse meetmeid;

d) tuvastada võimalikud küberründed ja neile reageerida;

e) logida andmeid küberrünnete paremaks tuvastamiseks ja tagada küberkriminalistika võimekus küberründe katsete või õnnestunud küberrünnete analüüsimiseks.

5.1.2. Tüübikinnitusasutus või tehniline teenistus testib vastava tüübi sõidukit, et kontrollida, kas sõiduki tootja on rakendanud oma dokumenteeritud küberturvalisuse meetmeid. Tüübikinnitusasutus või tehniline teenistus teeb valimi põhjal katseid ise või koostöös sõiduki tootjaga. Valimi koostamine peab keskenduma eelkõige riskidele, mida riskihindamises on hinnatud suurteks.

5.1.3. Tüübikinnitusasutus või tehniline teenistus keeldub küberturvalisusega seotud tüübikinnituse andmisest, kui sõiduki tootja ei ole täitnud üht või mitut punktis 7.3 osutatud nõuet, eelkõige:

a) sõiduki tootja ei ole teinud punktis 7.3.3 osutatud põhjalikku riskihindamist, sealhulgas ei ole tootja võtnud arvesse kõiki 5. lisa A osas osutatud ohtudega seotud riske;

b) sõiduki tootja ei ole kaitsnud sõidukitüüpi sõiduki tootja riskihindamises tuvastatud riskide eest või ei ole rakendanud punktis 7 nõutud proportsionaalseid leevendusmeetmeid;

c) sõiduki tootja ei ole kehtestanud asjakohaseid ja proportsionaalseid meetmeid, et kaitsta sõidukitüübi järelturu tarkvara, teenuste, rakenduste või andmete salvestamiseks ja kasutamiseks ettenähtud keskkondi (olemasolu korral);

d) sõiduki tootja ei teinud rakendatud turvameetmete tulemuslikkuse kontrollimiseks enne tüübikinnituse saamist asjakohaseid ega piisavaid katseid.

5.1.4. Hindav tüübikinnitusasutus keeldub küberturvalisusega seotud tüübikinnituse andmisest ka juhul, kui tüübikinnitusasutus või tehniline teenistus ei ole saanud sõiduki tootjalt sõidukitüübi küberturvalisuse hindamiseks piisavalt teavet.

5.2. Teade sõidukitüübile käesoleva eeskirja kohase tüübikinnituse andmise, laiendamise või andmata jätmise kohta edastatakse käesolevat eeskirja kohaldavatele 1958. aasta kokkuleppe osalistele käesoleva eeskirja 2. lisas esitatud näidisele vastaval vormil.

5.3. Tüübikinnitusasutused ei anna tüübikinnitust, kui ei ole kontrollitud, kas tootja on kehtestanud piisava korra ja piisavad menetlused käesolevas eeskirjas kirjeldatud küberturvalisuse aspektide nõuetekohaseks haldamiseks.

5.3.1. Tüübikinnitusasutus ja selle tehnilised teenistused tagavad lisaks 1958. aasta kokkuleppe liites 2 sätestatud kriteeriumidele, et:

a) neil on pädevad töötajad, kellel on asjakohased küberturvalisuse alased oskused ja mootorsõiduki riski hindamise eriteadmised ([1]);

b) nad on rakendanud menetlusi käesoleva eeskirja kohase ühetaolise hindamise tagamiseks.

5.3.2. Iga käesolevat eeskirja kohaldav kokkuleppeosaline teavitab oma tüübikinnitusasutuse kaudu käesolevat ÜRO eeskirja kohaldavate teiste kokkuleppeosaliste tüübikinnitusasutusi meetodist ja kriteeriumidest, millest teavitav asutus lähtub käesoleva eeskirja, eriti selle punktide 5.1, 7.2 ja 7.3 kohaselt võetud meetmete asjakohasuse hindamisel.

Seda teavet jagatakse a) ainult enne esmakordselt käesoleva eeskirja kohase tüübikinnituse andmist ja b) iga kord, kui hindamismeetodit või -kriteeriume ajakohastatakse.

See teave on mõeldud jagamiseks parimate tavade kogumise ja analüüsimise eesmärgil ning selleks, et tagada käesoleva eeskirja ühtlustatud kohaldamine kõigis tüübikinnitusasutustes, kes seda kohaldavad.

5.3.3. Punktis 5.3.2 osutatud teave laaditakse inglise keeles õige aja jooksul ja hiljemalt 14 päeva enne asjaomaste hindamismeetodite ja -kriteeriumide alusel tüübikinnituse andmist Ühinenud Rahvaste Organisatsiooni Euroopa Majanduskomisjoni loodud turvalisse internetipõhisesse andmebaasi DETA ([2]). Teave peab olema piisav, et mõista, millised tulemuslikkuse miinimummäärad on tüübikinnitusasutus punktis 5.3.2 osutatud iga konkreetse nõude puhul vastu võtnud, samuti milliseid protsesse ja meetmeid rakendab asutus nende tulemuslikkuse miinimummäärade täitmise kontrollimiseks ([3]).

5.3.4. Punktis 5.3.2 osutatud teavet vastuvõtvad tüübikinnitusasutused võivad esitada teavitavale tüübikinnitusasutusele märkusi, laadides need andmebaasi DETA 14 päeva jooksul pärast teavitamise kuupäeva.

5.3.5. Kui tüübikinnitust andval asutusel ei ole võimalik arvestada punkti 5.3.4 kohaselt saadud märkusi, paluvad märkused saatnud tüübikinnitusasutused ja tüübikinnitust andev asutus 1958. aasta kokkuleppe liite 6 kohaselt lisaselgitusi. Sõidukeid käsitlevate eeskirjade ühtlustamise ülemaailmse foorumi (WP.29) käesoleva eeskirja kohane asjaomane töörühm ([4]) lepib kokku hindamismeetodite ja -kriteeriumide ühises tõlgenduses ([5]). Ühist tõlgendust rakendatakse ja kõik tüübikinnitusasutused väljastavad käesoleva eeskirja kohaseid tüübikinnitusi vastavalt sellele.

([1]) Nt ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Suunised üleslaaditava üksikasjaliku teabe (nt meetod, kriteeriumid, tulemuslikkuse tase) ja selle vormi kohta esitatakse tõlgendusdokumendis, mille koostab küberturvalisuse ja kaablita side küsimuste rakkerühm automatiseeritud/autonoomsete ja ühendatud sõidukite töörühma (GRVA) seitsmendaks istungiks.
([4]) Automatiseeritud/autonoomsete ja ühendatud sõidukite töörühm (GRVA).
([5]) Tõlgendust käsitletakse punkti 5.3.3 joonealuses märkuses osutatud tõlgendusdokumendis.

5.3.6. Iga tüübikinnitusasutus, kes annab tüübikinnituse vastavalt käesolevale eeskirjale, teavitab antud tüübikinnitusest teisi tüübikinnitusasutusi. Tüübikinnitusasutus laadib ingliskeelse tüübikinnituse koos lisadokumentidega DETA andmebaasi 14 päeva jooksul pärast kinnituse andmise kuupäeva ([6]).

5.3.7. Kokkuleppeosalised võivad uurida punkti 5.3.6 kohaselt üleslaaditud teabe põhjal antud tüübikinnitusi. Kokkuleppeosaliste vaheliste eriarvamuste korral lahendatakse need vastavalt 1958. aasta kokkuleppe artiklile 10 ja liitele 6. Lisaks teatavad kokkuleppeosalised erinevatest tõlgendustest 1958. aasta kokkuleppe liites 6 määratletud tähenduses sõidukeid käsitlevate eeskirjade ühtlustamise ülemaailmse foorumi (WP.29) asjaomasele töörühmale. Asjaomane töörühm toetab lahkarvamuste lahendamist ja võib vajaduse korral selles küsimuses nõu pidada sõidukeid käsitlevate eeskirjade ühtlustamise ülemaailmse foorumiga (WP.29).

5.4. Käesoleva eeskirja punkti 7.2 kohaldamisel tagab tootja eeskirjas käsitletavate küberturvalisusega seotud aspektide rakendamise.

6. Küberturvalisuse haldamise süsteemi vastavustunnistus

6.1. Kokkuleppeosalised nimetavad tüübikinnitusasutuse, mis hindab tootjat ja väljastab küberturvalisuse haldamise süsteemi vastavustunnistuse.

6.2. Küberturvalisuse haldamise süsteemi vastavustunnistuse taotluse esitab sõiduki tootja või tema nõuetekohaselt akrediteeritud esindaja.

6.3. Taotlusele tuleb lisada järgmised dokumendid kolmes eksemplaris ja järgmised andmed:

6.3.1. küberturvalisuse haldamise süsteemi kirjeldavad dokumendid;

6.3.2. allkirjastatud deklaratsioon, mis on koostatud 1. lisa liites 1 määratletud näidise põhjal.

6.4. Kasutades 1. lisa liites 1 määratletud näidist, deklareerib tootja ja tõendab hindamise raames tüübikinnitusasutusele või selle tehnilisele teenistusele, et tal on olemas vajalikud protsessid kõigi käesoleva eeskirja kohaste küberturvalisuse nõuete täitmiseks.

6.5. Kui hindamine on rahuldavalt lõpule viidud ja tootjalt on laekunud 1. lisa liites 1 määratletud näidisele vastav allkirjastatud deklaratsioon, antakse tootjale käesoleva eeskirja 4. lisas kirjeldatud küberturvalisuse haldamise süsteemi vastavustunnistus (edaspidi „küberturvalisuse haldamise süsteemi vastavustunnistus“).

6.6. Tüübikinnitusasutus või selle tehniline teenistus kasutab küberturvalisuse haldamise süsteemi vastavustunnistuse koostamiseks käesoleva eeskirja 4. lisas esitatud näidist.

6.7. Küberturvalisuse haldamise süsteemi vastavustunnistus kehtib kuni kolm aastat tunnistuse väljastamise kuupäevast, välja arvatud selle tühistamise korral.

6.8. Küberturvalisuse haldamise süsteemi vastavustunnistuse andnud tüübikinnitusasutus võib igal ajal kontrollida, kas selle saamise nõuded on jätkuvalt täidetud. Kui käesolevas eeskirjas sätestatud nõudeid enam ei täideta, tühistab tüübikinnitusasutus küberturvalisuse haldamise süsteemi vastavustunnistuse.

([6]) Automatiseeritud/autonoomsete ja ühendatud sõidukite töörühm koostab oma seitsmendal istungil lisateabe dokumendipaketi miinimumnõuete kohta.

6.9. Tootja teavitab tüübikinnitusasutust või selle tehnilist teenistust kõigist muudatustest, mis mõjutavad küberturvalisuse haldamise süsteemi vastavustunnistuse asjakohasust. Pärast tootjaga konsulteerimist otsustab tüübikinnitusasutus või selle tehniline teenistus, kas on vaja uusi kontrolle.

6.10. Tootja taotleb uut küberturvalisuse haldamise süsteemi vastavustunnistust või olemasoleva vastavustunnistuse pikendamist piisavalt aegsasti, et tüübikinnitusasutus saaks viia hindamise lõpule enne küberturvalisuse haldamise süsteemi vastavustunnistuse kehtivusaja lõppu. Positiivse hinnangu korral väljastab tüübikinnitusasutus küberturvalisuse haldamise süsteemi uue vastavustunnistuse või pikendab selle kehtivust veel kolmeks aastaks. Tüübikinnitusasutus kontrollib, kas küberturvalisuse haldamise süsteem vastab jätkuvalt käesoleva eeskirja nõuetele. Tüübikinnitusasutus väljastab uue tunnistuse juhul, kui tüübikinnitusasutuse või selle tehnilise teenistuse tähelepanu on juhitud muudatustele ja need on saanud positiivse hinnangu.

6.11. Seoses sõidukitüüpidega, mille puhul oli küberturvalisuse haldamise süsteem asjakohane, käsitletakse tootja küberturvalisuse haldamise süsteemi vastavustunnistuse kehtivuse lõppemist või tühistamist punktis 8 osutatud tüübikinnituse muutmisena, mis võib hõlmata tüübikinnituse tühistamist, kui tüübikinnituse andmise tingimusi enam ei täideta.

7. Tehniline kirjeldus

7.1. Üldnõuded

7.1.1. Käesoleva eeskirja nõuded ei piira muude ÜRO eeskirjade sätete ega nõuete kohaldamist.

7.2. Küberturvalisuse haldamise süsteemi nõuded

7.2.1. Hindamiseks teeb tüübikinnitusasutus või tema tehniline teenistus kindlaks, kas sõiduki tootjal on küberturvalisuse haldamise süsteem olemas, ja kontrollib selle vastavust käesolevale eeskirjale.

7.2.2. Küberturvalisuse haldamise süsteem hõlmab järgmisi aspekte.

7.2.2.1. Sõiduki tootja tõendab tüübikinnitusasutusele või tehnilisele teenistusele, et tema küberturvalisuse haldamise süsteemi kohaldatakse järgmistes etappides:

a) arendusetapp;

b) tootmisetapp;

c) tootmisjärgne etapp.

7.2.2.2. Sõiduki tootja peab tõendama, et tema küberturvalisuse haldamise süsteemis kasutatavad protsessid tagavad, et turvalisust, sealhulgas 5. lisas loetletud riske ja leevendusmeetmeid võetakse piisavalt arvesse. See hõlmab järgmist:

a) tootja organisatsioonis kasutatavad küberturvalisuse haldamise protsessid;

b) sõidukitüüpide riskide tuvastamiseks kasutatavad protsessid. Nendes protsessides võetakse arvesse 5. lisa A osas loetletud ja muid asjakohaseid ohte;

c) tuvastatud riskide hindamiseks, liigitamiseks ja ohjamiseks kasutatavad protsessid;

d) protsessid tuvastatud riskide nõuetekohase juhtimise tagamiseks;

e) sõidukitüübi küberturvalisuse testimiseks kasutatavad protsessid;

f) riskihindamise ajakohasuse tagamiseks kasutatavad protsessid;

g) küberrünnete, küberohtude ja sõidukitüüpide turvanõrkuste jälgimiseks, avastamiseks ja neile reageerimiseks kasutatavad protsessid ning protsessid, mille abil hinnatakse, kas rakendatud küberturvalisuse meetmed on uute tuvastatud küberohtude ja turvanõrkuste puhul endiselt tõhusad;

h) protsessid, mida kasutatakse, et saada asjakohaseid andmeid, mis toetaksid küberründe katsete või õnnestunud küberrünnete analüüsimist.

7.2.2.3. Sõiduki tootja peab tõendama, et protsesside abil, mida ta küberturvalisuse haldamise süsteemis kasutab, tagatakse punkti 7.2.2.2 alapunktides c ja g osutatud liigitusest lähtuvalt selliste küberohtude ja turvanõrkuste leevendamine mõistliku aja jooksul, millele sõiduki tootja peab reageerima.

7.2.2.4. Sõiduki tootja tõendab, et tema küberturvalisuse haldamise süsteemis kasutatavate protsessidega tagatakse punkti 7.2.2.2 alapunktis g osutatud jälgimise pidevus. See hõlmab:

a) esmakordselt registreeritud sõidukite jälgimist;

b) suutlikkust analüüsida ja tuvastada küberohte, turvanõrkusi ja küberründe sõiduki andmete ja logide järgi. See suutlikkus peab vastama punktile 1.3 ja austama autoomanike või -juhtide eraelu puutumatusega seotud õigusi, eriti selles osas, mis puudutab nõusolekut.

7.2.2.5. Sõiduki tootja peab näitama, kuidas ta seoses punkti 7.2.2.2 nõuetega reguleerib oma küberturvalisuse haldamise süsteemi abil lepinguliste tarnijate, teenuseosutajate või tootja allorganisatsioonide vahelisi võimalikke sõltuvusseoseid.

7.3. Sõidukitüüpidele esitatavad nõuded

7.3.1. Tootjal peab olema kinnitatavale sõidukitüübile vastav kehtiv küberturvalisuse haldamise süsteemi vastavustunnistus. Kui sõiduki tootja suudab M-, N- ja O-kategooria sõidukitele esmakordselt enne 1. juulit 2024 antud tüübikinnituste ja L-kategooria sõidukitele esmakordselt enne 1. juulit 2029 antud tüübikinnituste ja nende tüübikinnituste iga pikendamise puhul tõendada, et sõidukitüübi arendamine ei saanud toimuda vastavalt küberturvalisuse haldamise süsteemile, peab sõiduki tootja tõendama, et küberturvalisust võeti asjaomase sõidukitüübi arendusetapis piisavalt arvesse.

7.3.2. Sõiduki tootja teeb kindlaks kinnitatava sõidukitüübi tarnijatega seotud riskid ja juhib neid.

7.3.3. Sõiduki tootja teeb kindlaks sõidukitüübi kriitiliselt tähtsad elemendid, teeb sõidukitüübi põhjaliku riskihindamise ja ohjab/juhib asjakohaselt tuvastatud riske. Riskihindamises võetakse arvesse sõidukitüübi üksikelemente ja nende koostoimet. Riskihindamises võetakse arvesse ka koostoimet väliste süsteemidega. Riskide hindamisel võtab sõiduki tootja arvesse kõigi 5. lisa A osas osutatud ohtudega seotud riske ja kõiki muid asjakohaseid riske.

7.3.4. Sõiduki tootja kaitseb sõidukitüüpi tootja riskihindamises tuvastatud riskide eest. Sõidukitüübi kaitsmiseks tuleb rakendada proportsionaalseid leevendusmeetmeid. Rakendatavad leevendusmeetmed hõlmavad kõiki 5. lisa B ja C osas osutatud leevendusmeetmeid, mis on tuvastatud riskide puhul asjakohased. Kui 5. lisa B või C osas osutatud leevendusmeede ei ole aga tuvastatud riski puhul asjakohane või piisav, tagab sõiduki tootja, et rakendatakse mõnda muud asjakohast leevendusmeedet.

Eelkõige peab sõiduki tootja M-, N- ja O-kategooria sõidukitele esmakordselt enne 1. juulit 2024 antud tüübikinnituste ja L-kategooria sõidukitele esmakordselt enne 1. juulit 2029 antud tüübikinnituste ja nende tüübikinnituste iga pikendamise puhul tagama mõne muu asjakohase leevendusmeetme rakendamise, kui 5. lisa B või C osas osutatud leevendusmeede ei ole tehniliselt teostatav Vastava tehnilise teostatavuse hinnangu esitab tüübikinnitusasutusele tootja.

7.3.5. Sõiduki tootja võtab asjakohased ja proportsionaalsed meetmed, et kaitsta sõidukitüübi järelturu tarkvara, teenuste, rakenduste või andmete salvestamiseks ja kasutamiseks ettenähtud keskkondi (olemasolu korral).

7.3.6. Enne tüübikinnitust teeb sõiduki tootja asjakohaseid ja piisavaid katseid, et kontrollida rakendatud turvameetmete tulemuslikkust.

7.3.7. Sõiduki tootja rakendab sõidukitüübiga seoses meetmeid, et:

a) tuvastada ja ära hoida küberründed sõidukitüübi sõidukitele;

b) toetada sõiduki tootja jälgimissuutlikkust, et tuvastada selle sõidukitüübiga seotud ohte, turvanõrkusi ja küberründeid;

c) tagada andmeekspertiisi võimekus küberründekatsete või õnnestunud küberrünnete analüüsimiseks.

7.3.8. Käesoleva eeskirja kohaldamisel kasutatavad krüptomoodulid peavad olema kooskõlas kokkulepitud standarditega. Kui kasutatavad krüptomoodulid ei ole kokkulepitud standarditega kooskõlas, peab sõiduki tootja põhjendama nende kasutamist.

7.4. Aruandlussätted

7.4.1. Sõiduki tootja peab vähemalt kord aastas või vajaduse korral sagedamini andma tüübikinnitusasutusele või tehnilisele teenistusele aru punkti 7.2.2.2 alapunktis g määratletud jälgimistegevuse tulemustest, esitades muu hulgas asjakohase teabe uute küberrünnete kohta. Lisaks teatab ja kinnitab sõiduki tootja tüübikinnitusasutusele või tehnilisele teenistusele, et tema sõidukitüüpide suhtes rakendatud küberturvalisuse leevendusmeetmed on jätkuvalt tõhusad, ja nimetab kõik võetud lisameetmed.

7.4.2. Tüübikinnitusasutus või tehniline teenistus kontrollib esitatud teavet ja nõuab vajaduse korral sõiduki tootjalt tuvastatud tagajärjetuse kõrvaldamist.

Kui aruandlus või vastus ei ole piisav, võib tüübikinnitusasutus küberturvalisuse haldamise süsteemi vastavustunnistuse vastavalt punktile 6.8 tühistada.

8. Sõidukitüübi muutmine ja tüübikinnituse laiendamine

8.1. Kõigist sõidukitüübi muudatustest, mis mõjutavad küberturvalisuse tehnilisi näitajaid ja/või käesolevas eeskirjas nõutavaid dokumente, tuleb teavitada sõidukitüübi kinnitanud tüübikinnitusasutust. Seejärel võib tüübikinnitusasutus:

8.1.1. otsustada, et tehtud muudatused vastavad jätkuvalt olemasoleva tüübikinnituse nõuetele ja dokumentidele või

8.1.2. teha punkti 5 kohase vajaliku lisahindamise ja vajaduse korral nõuda katsete tegemise eest vastutavalt tehniliselt teenistuselt täiendavat katsearuannet.

8.1.3. Teatis tüübikinnituse andmise, laiendamise või andmata jätmise kohta, milles märgitakse ära muudatused, edastatakse käesoleva eeskirja 2. lisas esitatud näidisele vastaval vormil. Tüübikinnituse laienduse väljastav tüübikinnitusasutus määrab laiendusele seerianumbri ja teavitab sellest teisi käesolevat eeskirja kohaldavaid 1958. aasta kokkuleppe osalisi, kasutades käesoleva eeskirja 2. lisas esitatud näidisele vastavat teatisevormi.

9. Tootmise nõuetele vastavus

9.1. Tootmise nõuetele vastavuse menetlus peab vastama 1958. aasta kokkuleppe liites 1 sätestatud korrale (E/ECE/TRANS/505/Rev.3) ja järgmistele nõuetele.

9.1.1. Tüübikinnituse omanik peab tagama, et tootmise nõuetele vastavuse katsete tulemused dokumenteeritakse ja lisatud dokumendid jäävad kättesaadavaks tüübikinnitusasutuse või selle tehnilise teenistusega sõlmitud kokkuleppes kindlaks määratud ajavahemikuks. See ajavahemik ei ületa kümmet aastat alates tootmise lõpetamisest.

9.1.2. Tüübikinnituse andnud asutus võib igal ajal kontrollida igas tootmisüksuses kohaldatud nõuetele vastavuse kontrollimeetodeid. Neid kontrolle tehakse tavaliselt kord kolme aasta jooksul.

10. Karistused tootmise nõuetele mittevastavuse korral

10.1. Sõidukitüübile käesoleva eeskirja kohaselt antud tüübikinnituse võib tühistada, kui eeskirjas sätestatud nõuded ei ole täidetud või kui valimi sõidukid ei vasta käesoleva eeskirja nõuetele.

10.2. Kui tüübikinnitusasutus tühistab tüübikinnituse, mille ta on eelnevalt andnud, teatab ta sellest kohe käesolevat eeskirja kohaldavatele kokkuleppeosalistele, kasutades selleks käesoleva eeskirja 2. lisas esitatud näidisele vastavat teatisevormi.

11. Tootmise lõpetamine

11.1. Kui tüübikinnituse omanik lõpetab täielikult käesoleva eeskirja kohase tüübikinnituse saanud sõidukitüübi tootmise, peab ta sellest teatama tüübikinnituse andnud asutusele. Pärast asjaomase teatise saamist teatab asutus sellest teistele käesolevat eeskirja kohaldavatele kokkuleppeosalistele, kasutades selleks tüübikinnituse vormi, mille lõppu on lisatud suurtähtedega kirjutatud märge „TOOTMINE LÕPETATUD“ koos kuupäeva ja allkirjaga.

12. Tüübikinnituskatse eest vastutavate tehniliste teenistuste ja tüübikinnitusasutuste nimed ja aadressid

12.1. Käesolevat eeskirja kohaldavad kokkuleppeosalised edastavad ÜRO sekretariaadile tüübikinnituskatsete eest vastutavate tehniliste teenistuste ja nende tüübikinnitusasutuste nimed ja aadressid, mis annavad tüübikinnitusi ja millele tuleb saata teistes riikides välja antud vormid, mis tõendavad tüübikinnituse andmist, laiendamist, andmata jätmist või tühistamist.

1. LISA

Teabedokument

Vajaduse korral tuleb järgmine teave esitada kolmes eksemplaris koos sisukorraga. Joonised esitatakse sobivas mõõtkavas ja piisavalt üksikasjalikult A4-formaadis või A4-formaadiga kaustas. Kui lisatakse fotod, peavad need olema piisavalt üksikasjalikud.

1. Mark (tootja ärinimi): .....

2. Tüüp ja üldine kaubanduslik kirjeldus (kirjeldused): .....

3. Tüübi identifitseerimisandmed, kui need on märgitud sõidukile: .....

4. Märgistuse asukoht: .....

5. Sõiduki kategooria(d): .....

6. Tootja / tootja esindaja nimi ja aadress: .....

7. Koostetehaste nimed ja aadressid: .....

8. Representatiivsõiduki foto(d) ja/või joonis(ed): .....

9. Küberturvalisus

9.1. Sõidukitüübi ehituse üldandmed, sealhulgas:

a) sõidukitüübi küberturvalisuse seisukohast olulised sõidukisüsteemid;

b) nende süsteemide küberturvalisuse seisukohast tähtsad osised;

c) nende süsteemide koostoime sõidukitüübi muude süsteemide ja välisliidestega.

9.2. Sõidukitüübi skemaatiline esitus

9.3. Küberturvalisuse haldamise süsteemi vastavustunnistuse number: .....

9.4. Kinnitatava sõidukitüübi dokumendid, milles kirjeldatakse selle riskihindamise tulemust ja tuvastatud riske: .....

9.5. Kinnitatava sõidukitüübi dokumendid, milles kirjeldatakse loetletud süsteemides või sõidukitüübi puhul rakendatud leevendusmeetmeid ja seda, kuidas need loetletud riskide puhul aitavad: .....

9.6. Kinnitatava sõidukitüübi dokumendid, milles kirjeldatakse järelturu tarkvarale, teenustele, rakendustele või andmetele ettenähtud keskkondade kaitset: .....

9.7. Kinnitatava sõidukitüübi dokumendid, milles kirjeldatakse katseid, mida on sõidukitüübi ja selle süsteemide küberturvalisuse kontrollimiseks tehtud, ning nende tulemusi: .....

9.8. Küberturvalisusega seoses arvesse võetava tarneahela kirjeldus: .....

1. lisa 1. liide

Tootja küberturvalisuse haldamise süsteemi vastavusdeklaratsiooni näidis

Tootja deklaratsioon küberturvalisuse haldamise süsteemi nõuete täitmise kohta

Tootja nimi: .....

Tootja aadress: .....

.....(*tootja nimi*)

kinnitab, et ÜRO eeskirja nr 155 punktis 7.2 sätestatud küberturvalisuse haldamise süsteemi nõuete täitmiseks vajalikud protsessid on kasutusele võetud ja jäävad kasutusse.

Koht: .....(*koht*)

Kuupäev: .....

Allakirjutaja nimi: .....

Allakirjutaja ametikoht: .....

(tootja esindaja tempel ja allkiri)

2. LISA

Teatis

(Suurim formaat: A4 (210 × 297 mm))



Välja andnud: ametiasutuse nimi:
……
……
……

milles käsitletakse sõidukitüübi ([2])
tüübikinnituse andmist,
tüübikinnituse laiendamist,
tüübikinnituse tühistamist alates pp/kk/aaaa,
tüübikinnituse andmata jätmist või
tootmise lõpetamist

ÜRO eeskirja nr 155 kohaselt

Tüübikinnituse nr: ……

Laienduse nr: ……

Laienduse põhjus: ……

1. Mark (tootja ärinimi): ……

2. Tüüp ja üldine kaubanduslik kirjeldus (kirjeldused): ……

3. Tüübi identifitseerimisandmed, kui need on märgitud sõidukile: ……

3.1. Märgistuse asukoht: ……

4. Sõiduki kategooria(d): ……

5. Tootja / tootja esindaja nimi ja aadress: ……

6. Tootmistehas(t)e nimi (nimed) ja aadress(id): ……

7. Küberturvalisuse haldamise süsteemi vastavustunnistuse number: ……

8. Katsete eest vastutav tehniline teenistus: ……

9. Katsearuande kuupäev: ……

10. Katsearuande number: ……

11. Märkused: (kui neid on) ……

12. Koht: ……

([1]) Tüübikinnituse andnud, seda laiendanud, selle andmata jätnud või selle tühistanud riigi tunnusnumber (vt käesoleva eeskirja sätted tüübikinnituse kohta).
([2]) Mittevajalik maha tõmmata.

13. Kuupäev: .....

14. Allkiri: .....

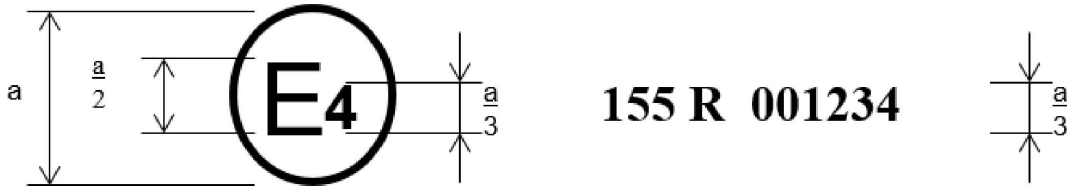
15. Lisatud on loetelu tüübikinnitusasutusele esitatud teabest, mida on võimalik taotluse korral saada.

3. LISA

Tüübikinnitusmärgi kujundus

NÄIDIS A

(vt käesoleva eeskirja punkt 4.2)



a = min 8 mm

Sõidukile kinnitatud eespool kujutatud tüübikinnitusmärk näitab, et asjaomase maanteesõiduki tüüp on saanud tüübikinnituse Madalmaades (E 4) eeskirja nr 155 alusel tüübikinnitusnumbri 001234 all. Tüübikinnitusnumbri kaks esimest numbrit näitavad, et tüübikinnitus on antud vastavalt käesoleva eeskirja originaalversioonile (00).

4. LISA

KÜBERTURVALISUSE HALDAMISE SÜSTEEMI VASTAVUSTUNNISTUSE NÄIDIS

Vastavustunnistus selle kohta, et küberturvalisuse haldamise süsteem on vastavuses

ÜRO eeskirjaga nr 155

Tunnistuse number [*viitenumber*]

[… *tüübikinnitusasutus*]

tõendab, et:

Tootja: ……

Tootja aadress: ……

järgib eeskirja nr 155 punktis 7.2 sätestatud nõudeid.

Kontrolli toimumise kuupäevad: ……

Väljastanud (tüübikinnitusasutuse või tehnilise teenistuse nimi ja aadress): ……

Aruande number: ……

Tunnistus kehtib kuni [……..*kuupäev*]

Koostatud […… *koht*]

[…… *kuupäev*]

[…… *allkiri*]

Lisatud dokumendid: küberturvalisuse haldamise süsteemi tootjapoolne kirjeldus.

5. LISA

Ohtude ja leevendusmeetmete loetelu

1. Käesolev lisa koosneb kolmest osast. A osas kirjeldatakse ohtude, turvanõrkuste ja ründemeetodite baasstsenaariumi. B osas kirjeldatakse sõidukitüüpide vastu suunatud ohtude leevendamiseks kavandatud meetmeid. C osas kirjeldatakse meetmeid, millega leevendada sõidukiväliste valdkondade, nt IT-tagasüsteemide vastu suunatud ohte.

2. A, B ja C osa võetakse arvesse sõidukitootjate riskide hindamisel ja leevendusmeetmete rakendamisel.

3. A osas on indekseeritult esitatud suured turvanõrkused ja nende vastavad näited. Samale indeksile viidatakse B ja C osa tabelites, et siduda iga rünne/turvanõrkus vastavate leevendusmeetmete loeteluga.

4. Ohuanalüüsis käsitletakse ka ründe võimalikku mõju. See võib aidata kindlaks teha riski raskusastet ja tuvastada lisariske. Ründe võimalikud tagajärjed:

   a) sõiduki ohutu käitamine on kahjustatud;

   b) sõiduki funktsioonid enam ei toimi;

   c) muudetakse tarkvara ja jõudlust;

   d) muudetakse tarkvara, kuid see ei mõjuta käitamist;

   e) andmetervikluse rikkumine;

   f) andmete konfidentsiaalsuse rikkumine;

   g) andmete käideldavuse kadu;

   h) muu, sealhulgas kuritegevus.

A OSA

Ohtudega seotud turvanõrkus või ründemeetod

Ohtude ja nendega seotud turvanõrkuste või ründemeetodite üldised kirjeldused on esitatud tabelis A1.

Tabel A1

Ohtudega seotud turvanõrkuste või ründemeetodite loetelu

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
4.3.1. Liiklevate sõidukitega seotud tagaserverite ohud	1	Sõiduki ründeks või andmevarguseks kasutatakse tagaservereid.	1.1	Töötajad kuritarvitavad privileege (siserünne).
			1.2	Volitamata internetijuurdepääs serverile (näiteks tagauste, süsteemitarkvara parandamata turvanõrkuste, SQL-rünnete või muude vahendite abil).
			1.3	Volitamata füüsiline juurdepääs serverile (näiteks mälupulga või muu serveriga ühenduva andmekandja abil).
	2	Tagaserveri teenuste halvang mõjutab sõiduki töövõimet.	2.1	Rünne tagaserverile peatab selle toimimise, näiteks takistab selle suhtlemist sõidukitega ja sõidukitele vajalike teenuste osutamist.

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
	3	Tagaserverites hoitavad sõidukiga seotud andmed kaovad või rikutakse (andmetega seotud rikkumine).	3.1	Töötajad kuritarvitavad privileege (siserünne).
			3.2	Teave kaob pilvest. Tundlikud andmed võivad rünnete või õnnetuste tõttu kaduma minna, kui andmeid talletavad kolmandast isikust pilveteenuse pakkujad.
			3.3	Volitamata internetijuurdepääs serverile (näiteks tagauste, süsteemitarkvara parandamata turvanõrkuste, SQL-rünnete või muude vahendite abil).
			3.4	Volitamata füüsiline juurdepääs serverile (näiteks mälupulga või muu serveriga ühenduva andmekandja abil).
			3.5	Teabega seotud rikkumine andmete tahtmatu jagamise tõttu (nt administraatori vead).
4.3.2. Sõidukite sidekanalitega seotud ohud	4	Sõiduki vastuvõetavate sõnumite või andmete võltsimine.	4.1	Sõnumeid võltsitakse, esinedes kellegi teisena (nt koostoimelise teadlikkuse või manöövrite koordineerimise sõnumid V2X-sides, ülemaailmse satelliitnavigatsioonisüsteemi (GNSS) sõnumid jne).
			4.2	Sibüllrünne (teistele sõidukitele tekitatakse vale mulje, et teel on palju sõidukeid).
	5	Sidekanaleid kasutatakse sõiduki koodi/andmete volituseta muutmiseks või kustutamiseks.	5.1	Sidekanalid võimaldavad koodisüste, näiteks võidakse sidevoogu sisestada urgitud kahendkoodiga täitmisfail.
			5.2	Sidekanalid võimaldavad muuta sõiduki andmeid/koodi.
			5.3	Sidekanalid võimaldavad sõiduki andmeid/koodi üle kirjutada.
			5.4	Sidekanalid võimaldavad sõiduki andmeid/koodi kustutada.
			5.5	Sidekanalid võimaldavad sõidukisse sisestada andmeid/koodi (kirjutada andmeid/koodi).
	6	Sidekanalid võimaldavad ebausaldusväärsete sõnumite vastuvõtmist või on haavatavad seansi kaaperdamise/ taasesitusrünnete suhtes.	6.1	Võetakse vastu ebausaldusväärsest allikast pärit teavet.
			6.2	Vahendusrünne / seansi kaaperdamine.
			6.3	Taasesitusrünne, näiteks rünne sidelüüsi vastu võimaldab ründajal viia elektroonilise juhtseadme tarkvara või lüüsi püsivara üle vanemale versioonile.
	7	Teavet saab hõlpsasti avalikustada, näiteks side pealtkuulamise kaudu või lubades volitamata juurdepääsu tundlikele failidele või kaustadele.	7.1	Infopüük / häiriv kiirgus / side jälgimine.
			7.2	Failidele või andmetele volitamata juurdepääsu saamine.

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
	8	Teenusetõkestusründed sidekanalite kaudu, et halvata sõiduki funktsioone.	8.1	Sõiduki infosüsteemi saadetakse suur hulk andmeprügi, nii et süsteem ei saa funktsioneerida tavapärasel viisil.
			8.2	Musta augu rünne, mille korral ründe toimepanija on võimeline sõidukitevahelise side häirimiseks blokeerima sõidukitevahelised sõnumid.
	9	Privileegideta kasutaja võib saada eelispääsu sõiduki süsteemidele.	9.1	Privileegideta kasutajal on võimalik saada eelispääs, näiteks juurpääs.
	10	Sidekandjate viirused on võimelised nakatama sõiduki süsteeme.	10.1	Sidekandja viirus nakatab sõiduki süsteeme.
	11	Sõiduki vastuvõetud (nt X2V või diagnostikasõnumid) või sõidukis edastatavad sõnumid sisaldavad pahatahtlikku sisu.	11.1	Pahatahtlikud sisesõnumid (nt vallasvõrgust).
			11.2	Pahatahtlikud V2X-sõnumid, näiteks taristult sõidukile või sõidukilt sõidukile edastatavad sõnumid (nt linnakuvõrgusõnum (CAM), detsentraliseeritud keskkonnateate sõnum (DENM)).
			11.3	Pahatahtlikud diagnostikasõnumid.
			11.4	Pahatahtlikud tootja või tarnija sõnumid (nt sellised, mille tavaliselt saadab originaalseadme tootja või osiste/süsteemi/funktsioonide tarnija).
4.3.3. Uuendusprotsessiga seotud ohud sõidukitele	12	Uuendusprotsessi väärkasutatakse või kahjustatakse.	12.1	Rikutakse nn üle-õhu tarkvara uuendusprotsessi. See sisaldab süsteemi võltsuuendusprogrammi või -püsivara loomist.
			12.2	Rikutakse lokaalset/füüsilist tarkvara uuendusprotsessi. See sisaldab süsteemi võltsuuendusprogrammi või -püsivara loomist.
			12.3	Tarkvara muudetakse enne uuendusprotsessi (mistõttu see on rikutud), ehkki uuendusprotsessi ei puututa.
			12.4	Murtakse tarkvara pakkuja krüptovõtmed vigase uuenduse lubamiseks.
	13	Legitiimsetest uuendustest on võimalik keelduda.	13.1	Teenusetõkestusrünne uuendusserveri või -võrgu vastu, et hoida ära kriitiliselt tähtsate tarkvarauuenduste levitamine ja/või kliendispetsiifiliste funktsioonide avamine.
4.3.4. Ohud, mis ähvardavad sõidukit küberrünnet hõlbustava tahtmatu inimtegevuse tõttu	15	Legitiimsete osaliste tegevus võib tahtmatult hõlbustada küberrünnet.	15.1	Süütu ohver (nt omanik, käitaja või hooldusinsener) petetakse tahtmatult alla laadima pahavara või võimaldama rünnet.
			15.2	Kindlaksmääratud turvakorda ei järgita.

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
4.3.5. Välise ühenduvuse ja ühendustega seotud ohud sõidukitele	16	Sõiduki funktsioonide ühenduvuse muutmine võimaldab toime panna küberründe; see võib hõlmata telemaatikat, kaugtoiminguid võimaldavaid süsteeme ja traadita lähitoimesidet kasutavaid süsteeme.	16.1	Muudetakse süsteemide kaugjuhtimise funktsioone, näiteks kaugvõti, kasutustõkis ja kiirlaadimisjaam.
			16.2	Muudetakse sõiduki telemaatikat (nt muudetakse tundlike kaupade temperatuuri mõõtmist, avatakse eemalt pagasiruumi uksed).
			16.3	Häired traadita lähitoimesüsteemides või -andurites.
	17	Sõiduki süsteemide ründamiseks kasutatakse kolmanda isiku hallatavat tarkvara, näiteks meelelahutusrakendusi.	17.1	Sõiduki süsteemide ründamise meetodina kasutatakse rikutud või nõrga tarkvaraturbega rakendusi.
	18	Sõiduki süsteemide ründamiseks kasutatakse välisliidestega ühendatud seadmeid, näiteks USB-porte ja pardadiagnostikaseadme porte.	18.1	Välisliideseid, näiteks USB- või muid porte kasutatakse ründepunktina, näiteks koodisüsti abil.
			18.2	Sõiduki süsteemiga ühendatakse viirusega nakatunud andmekandja.
			18.3	Ründe hõlbustamiseks kasutatakse diagnostilist juurdepääsu (nt pardadiagnostikaseadme pordi lukud), näiteks muudetakse (otseselt või kaudselt) sõiduki parameetreid.
4.3.6. Sõiduki andmeid/ koodi ähvardavad ohud	19	Sõiduki andmete/koodi vargus.	19.1	Sõiduki süsteemidest varastatakse autoriõigusega kaitstud või omandtarkvara (tootepiraatlus).
			19.2	Volitamata juurdepääs omaniku privaatsele teabele, nagu isiku identiteet, arveldusarve, aadressiraamatu ja asukoha teave, sõiduki elektrooniline pass jms.
			19.3	Krüptovõtmete vargus.
	20	Muudetakse sõiduki andmeid/ koodi.	20.1	Ebaseaduslikult/volituseta muudetakse sõiduki elektroonilist passi.
			20.2	Identiteedipettus, näiteks kui kasutaja soovib teemaksusüsteemide või tootja tagaprogrammiga suheldes kasutada kellegi teise identiteeti.
			20.3	Hiilitakse mööda jälgimissüsteemidest (häkitakse/ muudetakse/blokeeritakse sõnumeid, nt nn auto musta kasti (ODR Tracker) andmed või sõitude arv).
			20.4	Muudetakse andmeid sõiduki sõiduandmete (nt läbisõit, sõidukiirus, sõidujuhised) võltsimiseks.
			20.5	Volituseta muudetakse süsteemi diagnostikaandmeid.
	21	Kustutatakse andmed/kood.	21.1	Volituseta kustutatakse süsteemi sündmustelogid või neid muudetakse.
	22	Paigaldatakse pahavara.	22.2	Paigaldatakse pahavara või juurutatakse pahavaralist tegevust.

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
	23	Paigaldatakse uus tarkvara või kirjutatakse üle olemasolev tarkvara.	23.1	Luuakse sõiduki juhtimissüsteemi või infosüsteemi võltstarkvara.
	24	Süsteemi- või operatsioonihäired.	24.1	Teenusetõkestus, mida võib sisevõrgus põhjustada näiteks vallasvõrgu siini üleujutamine või elektroonilise juhtseadme vigade esilekutsumine suure sõnumite hulgaga.
	25	Muudetakse sõiduki parameetreid.	25.1	Volitamata juurdepääs, et võltsida sõiduki põhifunktsioonide konfiguratsiooniparameetreid, nagu piduriandmed, turvapadja kasutuslävi jms.
			25.2	Volitamata juurdepääs, et võltsida laadimisparameetreid, nagu laadimispinge, laadimisvõimsus, aku temperatuur jms.
4.3.7. Võimalikud turvanõrkused, mida saab ära kasutada, kui süsteem ei ole piisavalt kaitstud ega tugevdatud	26	Krüptotehnoloogia võib olla rikutud või seda ei ole piisavalt kasutatud.	26.1	Lühikesed krüpteerimisvõtmed koos pika kehtivusajaga võimaldavad ründajal krüpteeringu murda.
			26.2	Krüptoalgoritmide ebapiisav kasutus, selleks et kaitsta tundlikke süsteeme.
			26.3	Kasutatakse aegunud või peagi aeguvaid krüptoalgoritme.
	27	Sõidukite ründamise eesmärgil võidakse muuta osi või tarvikuid.	27.1	Riist- või tarkvara on paigaldatud ründe võimaldamiseks või riist- või tarkvara ei vasta ründe peatamiseks kavandatud kriteeriumidele.
	28	Tark- või riistvara arendus toob kaasa turvanõrkusi.	28.1	Tarkvara programmivead. Tarkvara programmivead võivad tekitada ärakasutatavaid turvanõrkusi, eriti juhul, kui tarkvara ei ole testitud, et veenduda teadaolevate vigaste koodide või programmivigade puudumises ja vähendada teadmata vigase koodi / vigade riski.
			28.2	Arendusest järelejäänud vahendite (nt veaparanduspordid, JTAG-pordid, mikroprotsessorid, arendussertifikaadid, arendajate paroolid) kasutamine võib anda ründajale juurdepääsu elektroonilistele juhtseadmetele või paremad juurdepääsuõigused.
	29	Võrgu ülesehitus põhjustab turvanõrkusi.	29.1	Avatuks jäetud üleliigsed internetipordid võimaldavad juurdepääsu võrgusüsteemidele.
			29.2	Kontrolli saamiseks hiilitakse mööda võrgu lahususest. Konkreetne näide on kaitsmata lüüside või pääsupunktide (nt veoauto ja haagise lüüside) kasutamine kaitsemeetmetest möödahiilimiseks ja teistele võrgusegmentidele juurdepääsu saamiseks pahatahtliku tegevuse eesmärgil, näiteks omavoliliste vallasvõrgu siini sõnumite saatmiseks.
	31	Võib esineda tahtmatut andmete edastamist.	31.1	Teabega seotud rikkumised. Isikuandmed võivad lekkida, kui auto kasutaja vahetub (nt auto müüakse või seda kasutavad rendisõidukina uued rentijad).

Turvanõrkuse/ohu üldised ja täpsed kirjeldused			Turvanõrkuse või ründemeetodi näide	
	32	Süsteemide füüsiline muutmine võib võimaldada rünnet.	32.1	Muudetakse elektroonilist riistvara, näiteks lisatakse sõidukile volituseta elektroonilist riistvara, et võimaldada vahendusrünnet. Volitatud elektrooniline riistvara (nt andurid) asendatakse volitamata elektroonilise riistvaraga. Muudetakse anduri kogutavat teavet (nt mõjutatakse magneti abil käigukastiga ühendatud Halli efekti sensorit).

B OSA

Sõidukite ohtude leevendamiseks kavandatud meetmed

1. Sõiduki sidekanalitega seotud leevendusmeetmed

Sõiduki sidekanalitega seotud ohte leevendavad meetmed on loetletud tabelis B1.

Tabel B1

Sõiduki sidekanalitega seotud ohte leevendavad meetmed

Viide tabelile A1	Sõiduki sidekanalitega seotud ohud	Viide	Leevendusmeede
4.1	Sõnumeid võltsitakse, esinedes kellegi teisena (nt koostoimelise teadlikkuse või manöövrite koordineerimise sõnumid V2X-sides, ülemaailmse satelliitnavigatsioonisüsteemi (GNSS) sõnumid jne).	M10	Sõiduk kontrollib vastuvõetavate sõnumite autentsust ja terviklust.
4.2	Sibüllrünne (teistele sõidukitele tekitatakse vale mulje, et teel on palju sõidukeid).	M11	Krüptovõtmete salvestamiseks rakendatakse turvameetmeid (nt kasutades riistvara turvamooduleid).
5.1	Sidekanalid võimaldavad koodisüste sõiduki andmetesse/koodi, näiteks võidakse sidevoogu sisestada urgitud kahendkoodiga täitmisfail.	M10 M6	Sõiduk kontrollib vastuvõetavate sõnumite autentsust ja terviklust. Riskide minimeerimiseks rakendavad süsteemid sisseprojekteeritud turvet.
5.2	Sidekanalid võimaldavad muuta sõiduki andmeid/koodi.	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme.
5.3	Sidekanalid võimaldavad sõiduki andmeid/koodi üle kirjutada.		
5.4 21.1	Sidekanalid võimaldavad sõiduki andmeid/koodi kustutada.		
5.5	Sidekanalid võimaldavad sõiduki süsteemidesse sisestada andmeid/koodi (kirjutada andmeid/koodi).		

Viide tabelile A1	Sõiduki sidekanalitega seotud ohud	Viide	Leevendusmeede
6.1	Võetakse vastu ebausaldusväärsest allikast pärit teavet.	M10	Sõiduk kontrollib vastuvõetavate sõnumite autentsust ja terviklust.
6.2	Vahendusrünne / seansi kaaperdamine.	M10	Sõiduk kontrollib vastuvõetavate sõnumite autentsust ja terviklust.
6.3	Taasesitusrünne, näiteks rünne sidelüüsi vastu võimaldab ründajal viia elektroonilise juhtseadme tarkvara või lüüsi püsivara üle vanemale versioonile.		
7.1	Infopüük / häiriv kiirgus / side jälgimine.	M12	Kaitstakse sõidukile või sõidukist edastatud konfidentsiaalseid andmeid.
7.2	Failidele või andmetele volitamata juurdepääsu saamine.	M8	Süsteemi ülesehitus ja juurdepääsu reguleerimine ei tohiks lasta volitamata töötajatel pääseda ligi isikuandmetele ega süsteemi kriitiliselt tähtsatele andmetele. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
8.1	Sõiduki infosüsteemi saadetakse suur hulk andmeprügi, nii et süsteem ei saa funktsioneerida tavapärasel viisil.	M13	Võetakse meetmed teenusetõkestusrünnete avastamiseks ja nendest taastumiseks.
8.2	Musta augu rünne ja sõidukitevaheline side katkeb, sest blokeeritakse sõnumite edastamine teistele sõidukitele.	M13	Võetakse meetmed teenusetõkestusrünnete avastamiseks ja nendest taastumiseks.
9.1	Privileegideta kasutajal on võimalik saada eelispääs, näiteks juurpääs.	M9	Rakendatakse meetmeid volituseta juurdepääsu ärahoidmiseks ja tuvastamiseks.
10.1	Sidekandja viirus nakatab sõiduki süsteeme.	M14	Tuleb kaaluda meetmeid süsteemide kaitsmiseks sardviiruste/-pahavara eest.
11.1	Pahatahtlikud sisesõnumid (nt vallasvõrgust).	M15	Tuleb kaaluda meetmeid pahatahtlike sisesõnumite või pahatahtliku sisetegevuse tuvastamiseks.
11.2	Pahatahtlikud V2X-sõnumid, näiteks taristult sõidukile või sõidukilt sõidukile edastatavad sõnumid (nt linnakuvõrgusõnum (CAM), detsentraliseeritud keskkonnateate sõnum (DENM)).	M10	Sõiduk kontrollib vastuvõetavate sõnumite autentsust ja terviklust.
11.3	Pahatahtlikud diagnostikasõnumid.		
11.4	Pahatahtlikud tootja või tarnija sõnumid (nt sellised, mille tavaliselt saadab originaalseadme tootja või osiste/ süsteemi/funktsioonide tarnija).		

2. Uuendusprotsessidega seotud leevendusmeetmed

Uuendusprotsessidega seotud ohte leevendavad meetmed on loetletud tabelis B2.

Tabel B2

Uuendusprotsessidega seotud ohte leevendavad meetmed

Viide tabelile A1	Uuendusprotsessidega seotud ohud	Viide	Leevendusmeede
12.1	Rikutakse nn üle-õhu tarkvara uuendusprotsessi. See sisaldab süsteemi võltsuuendusprogrammi või -püsivara loomist.	M16	Kasutatakse turvalisi tarkvara uuendamise protsesse.
12.2	Rikutakse lokaalset/füüsilist tarkvara uuendusprotsessi. See sisaldab süsteemi võltsuuendusprogrammi või -püsivara loomist.		
12.3	Tarkvara muudetakse enne uuendusprotsessi (mistõttu see on rikutud), ehkki uuendusprotsessi ei puututa.		
12.4	Murtakse tarkvara pakkuja krüptovõtmed vigase uuenduse lubamiseks.	M11	Krüptovõtmete salvestamiseks rakendatakse turvameetmeid.
13.1	Teenusetõkestusrünne uuendusserveri või -võrgu vastu, et hoida ära kriitiliselt tähtsate tarkvarauuenduste levitamine ja/või kliendispetsiifiliste funktsioonide avamine.	M3	Tagasüsteemidele rakendatakse turvameetmeid. Kui tagaserverid on teenuste osutamiseks kriitiliselt tähtsad, on süsteemiseisaku jaoks olemas taastamismeetmed. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).

3. Küberrünnet hõlbustava tahtmatu inimtegevusega seotud leevendusmeetmed

Küberrünnet hõlbustava tahtmatu inimtegevusega seotud ohte leevendavad meetmed on loetletud tabelis B3.

Tabel B3

Küberrünnet hõlbustava tahtmatu inimtegevusega seotud ohte leevendavad meetmed

Viide tabelile A1	Tahtmatu inimtegevusega seotud ohud	Viide	Leevendusmeede
15.1	Süütu ohver (nt omanik, käitaja või hooldusinsener) petetakse tahtmatult pahavara alla laadima või rünnet võimaldama.	M18	Rakendatakse meetmeid kasutajarollide ja juurdepääsuõiguste määratlemiseks ja kontrollimiseks, tuginedes vähima juurdepääsuõiguse põhimõttele.

Viide tabelile A1	Tahtmatu inimtegevusega seotud ohud	Viide	Leevendusmeede
15.2	Kindlaksmääratud turvakorda ei järgita.	M19	Organisatsioonid tagavad turvanõuete määratlemise ja järgimise, sealhulgas turvafunktsioonide haldamisega seotud toimingute ja juurdepääsu logimise.

4. Välise ühenduvuse ja ühendustega seotud leevendusmeetmed

Välise ühenduvuse ja ühendustega seotud ohte leevendavad meetmed on loetletud tabelis B4.

Tabel B4

Välise ühenduvuse ja ühendustega seotud ohte leevendavad meetmed

Viide tabelile A1	Välise ühenduvuse ja ühendustega seotud ohud	Viide	Leevendusmeede
16.1	Muudetakse sõiduki süsteemide kaugjuhtimise funktsioone, näiteks kaugvõti, kasutustõkis ja kiirlaadimisjaam.	M20	Kaugjuurdepääsuga süsteemide suhtes rakendatakse turvameetmeid.
16.2	Muudetakse sõiduki telemaatikat (nt muudetakse tundlike kaupade temperatuuri mõõtmist, avatakse eemalt pagasiruumi uksed).		
16.3	Häired traadita lähitoimesüsteemides või -andurites.		
17.1	Sõiduki süsteemide ründamise meetodina kasutatakse rikutud või nõrga tarkvaraturbega rakendusi.	M21	Tarkvara turvalisust tuleb hinnata, tarkvara tuleb autentida ja selle terviklus peab olema kaitstud. Sõidukisse paigaldamiseks kavandatud või potentsiaalselt tulevikus paigaldatava kolmandate isikute tarkvara põhjustatava riski minimeerimiseks tuleb rakendada turvameetmeid.
18.1	Välisliideseid, näiteks USB- või muid porte kasutatakse ründepunktina, näiteks koodisüsti abil.	M22	Välisliideste suhtes rakendatakse turvameetmeid.
18.2	Sõidukiga ühendatakse viirusega nakatunud andmekandja.		
18.3	Ründe hõlbustamiseks kasutatakse diagnostilist juurdepääsu (nt pardadiagnostikaseadme pordi lukud), näiteks muudetakse (otseselt või kaudselt) sõiduki parameetreid.	M22	Välisliideste suhtes rakendatakse turvameetmeid.

5. Ründe võimalike sihtmärkide või ajenditega seotud leevendusmeetmed

Ründe võimalike sihtmärkide või ajenditega seotud ohte leevendavad meetmed on loetletud tabelis B5.

Tabel B5

Ründe võimalike sihtmärkide või ajenditega seotud ohte leevendavad meetmed

Viide tabelile A1	Ründe võimalike sihtmärkide või ajenditega seotud ohud	Viide	Leevendusmeede
19.1	Sõiduki süsteemidest varastatakse autoriõigusega kaitstud või omandtarkvara (tootepiraatlus / varastatud tarkvara).	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
19.2	Volitamata juurdepääs omaniku privaatsele teabele, nagu isiku identiteet, arveldusarve, aadressiraamatu ja asukoha teave, sõiduki elektrooniline pass jms.	M8	Süsteemi ülesehitus ja juurdepääsu reguleerimine ei tohiks lasta volitamata töötajatel pääseda ligi isikuandmetele ega süsteemi kriitiliselt tähtsatele andmetele. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
19.3	Krüptovõtmete vargus.	M11	Krüptovõtmete salvestamiseks rakendatakse turvameetmeid, näiteks turvamooduleid.
20.1	Ebaseaduslikult/volituseta muudetakse sõiduki elektroonilist passi.	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
20.2	Identiteedipettus, näiteks kui kasutaja soovib teemaksusüsteemide või tootja tagaprogrammiga suheldes kasutada kellegi teise identiteeti.		
20.3	Hiilitakse mööda jälgimissüsteemidest (häkitakse/muudetakse/blokeeritakse sõnumeid, nt nn auto musta kasti (ODR Tracker) andmed või sõitude arv).	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP). Andurite või edastatud andmete vastu suunatud andmemanipulatsioonirünnakeid saab leevendada eri teabeallikate andmete korreleerimisega.
20.4	Muudetakse andmeid sõiduki sõiduandmete (nt läbisõit, sõidukiirus, sõidujuhised) võltsimiseks.		
20.5	Volituseta muudetakse süsteemi diagnostikaandmeid.		
21.1	Volituseta kustutatakse süsteemi sündmustelogid või neid muudetakse.	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
22.2	Paigaldatakse pahavara või juurutatakse pahavaralist tegevust.	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
23.1	Luuakse sõiduki juhtimissüsteemi või infosüsteemi võltstarkvara.		

Viide tabelile A1	Ründe võimalike sihtmärkide või ajenditega seotud ohud	Viide	Leevendusmeede
24.1	Teenusetõkestus, mida võib sisevõrgus põhjustada näiteks vallasvõrgu siini üleujutamine või elektroonilise juhtseadme vigade esilekutsumine suure sõnumite hulgaga.	M13	Võetakse meetmed teenusetõkestusrünnete avastamiseks ja nendest taastumiseks.
25.1	Volitamata juurdepääs, et võltsida sõiduki põhifunktsioonide konfiguratsiooniparameetreid, nagu piduriandmed, turvapadja kasutuslävi jms.	M7	Süsteemi andmete/koodi kaitsmiseks kasutatakse juurdepääsu reguleerimise meetodeid ja programme. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
25.2	Volitamata juurdepääs, et võltsida laadimisparameetreid, nagu laadimispinge, laadimisvõimsus, aku temperatuur jms.		

6. Leevendusmeetmed võimalikele turvanõrkustele, mida saab ära kasutada, kui süsteemi ei ole piisavalt kaitstud ega tugevdatud

Leevendusmeetmed ohtude vastu, mis on seotud võimalike turvanõrkustega, mida saab ära kasutada, kui süsteem ei ole piisavalt kaitstud ega tugevdatud, on loetletud tabelis B6.

Tabel B6

Leevendusmeetmed ohtude vastu, mis on seotud võimalike turvanõrkustega, mida saab ära kasutada, kui süsteem ei ole piisavalt kaitstud ega tugevdatud

Viide tabelile A1	Ohud seoses võimalike turvanõrkustega, mida saab ära kasutada, kui süsteem ei ole piisavalt kaitstud ega tugevdatud	Viide	Leevendusmeede
26.1	Lühikesed krüpteerimisvõtmed koos pika kehtivusajaga võimaldavad ründajal krüpteeringu murda.	M23	Järgitakse tark- ja riistvaraarenduse küberturvalisuse parimaid tavasid.
26.2	Krüptoalgoritmide ebapiisav kasutus, selleks et kaitsta tundlikke süsteeme.		
26.3	Kasutatakse taunitavaid krüptoalgoritme.		
27.1	Riistvara või tarkvara, mida on ründe võimaldamiseks muudetud või mis ei vasta ründe peatamiseks kavandatud kriteeriumidele	M23	Järgitakse tark- ja riistvaraarenduse küberturvalisuse parimaid tavasid.
28.1	Tarkvara programmivead võivad tekitada ärakasutatavaid turvanõrkusi, Tarkvara programmivead võivad tekitada ärakasutatavaid turvanõrkusi, eriti juhul, kui tarkvara ei ole testitud, et veenduda teadaolevate vigaste koodide või programmivigade puudumises ja vähendada teadmata vigase koodi / vigade riski.	M23	Järgitakse tark- ja riistvaraarenduse küberturvalisuse parimaid tavasid. Küberturvalisuse testimine on piisavalt ulatuslik.

Viide tabelile A1	Ohud seoses võimalike turvanõrkustega, mida saab ära kasutada, kui süsteem ei ole piisavalt kaitstud ega tugevdatud	Viide	Leevendusmeede
28.2	Arendusest järelejäänud vahendite (nt veaparanduspordid, JTAG-pordid, mikroprotsessorid, arendussertifikaadid, arendajate paroolid) kasutamine võib anda ründajale juurdepääsu elektroonilistele juhtseadmetele või paremad juurdepääsuõigused.		
29.1	Avatuks jäetud üleliigsed internetipordid võimaldavad juurdepääsu võrgusüsteemidele.		
29.2	Kontrolli saamiseks hiilitakse mööda võrgu lahususest. Konkreetne näide on kaitsmata lüüside või pääsupunktide (nt veoauto ja haagise lüüside) kasutamine kaitsemeetmetest möödahiilimiseks ja teistele võrgusegmentidele juurdepääsu saamiseks pahatahtliku tegevuse eesmärgil, näiteks omavoliliste vallasvõrgu siini sõnumite saatmiseks.	M23	Järgitakse tark- ja riistvaraarenduse küberturvalisuse parimaid tavasid. Järgitakse süsteemi projekteerimise ja integreerimise küberturvalisuse parimaid tavasid.

7. Sõiduki andmete kadumise/rikkumisega seotud leevendusmeetmed

Sõiduki andmete kadumise/rikkumisega seotud ohte leevendavad meetmed on loetletud tabelis B7.

Tabel B7

Sõiduki andmete kadumise/rikkumisega seotud ohte leevendavad meetmed

Viide tabelile A1	Sõiduki andmete kadumise/rikkumisega seotud ohud	Viide	Leevendusmeede
31.1	Teabega seotud rikkumised. Isikuandmeid võidakse rikkuda, kui auto kasutaja vahetub (nt auto müüakse või seda kasutavad rendisõidukina uued rentijad).	M24	Isikuandmete säilitamisel järgitakse andmete tervikluse ja konfidentsiaalsuse kaitse parimaid tavasid.

8. Leevendusmeetmed, kui tegemist on süsteemide füüsilise muutmisega, et võimaldada ründeid

Leevendusmeetmed ohtude vastu, mis on seotud süsteemide füüsilise muutmisega, et võimaldada ründeid, on loetletud tabelis B8.

Tabel B8

Leevendusmeetmed ohtude vastu, mis on seotud süsteemide füüsilise muutmisega, et võimaldada ründeid

Viide tabelile A1	Ohud, mis on seotud süsteemide füüsilise muutmisega, et võimaldada ründeid	Viide	Leevendusmeede
32.1	Muudetakse originaalseadmete tootja riistvara, näiteks lisatakse sõidukile volituseta riistvara, et võimaldada vahendusrünnet.	M9	Rakendatakse meetmeid volituseta juurdepääsu ärahoidmiseks ja tuvastamiseks.

C OSA

Sõidukiväliste ohtude leevendamise meetmed

1. Tagaserveritega seotud leevendusmeetmed

Tagaserveritega seotud ohtude leevendamise meetmed on loetletud tabelis C1.

Tabel C1

Tagaserveritega seotud ohtude leevendamise meetmed

Viide tabelile A1	Tagaserveritega seotud ohud	Viide	Leevendusmeede
1.1 & 3.1	Töötajad kuritarvitavad privileege (siserünne).	M1	Tagasüsteemidele rakendatakse siseringi rünnete riski vähendamiseks turvameetmeid.
1.2 & 3.3	Volitamata internetijuurdepääs serverile (näiteks tagauste, süsteemitarkvara parandamata turvanõrkuste, SQL-rünnete või muude vahendite abil).	M2	Tagasüsteemidele rakendatakse volituseta juurdepääsu minimeerimiseks turvameetmeid. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
1.3 & 3.4	Volitamata füüsiline juurdepääs serverile (näiteks mälupulga või muu serveriga ühenduva andmekandja abil).	M8	Süsteemi ülesehitus ja juurdepääsu reguleerimine ei tohiks lasta volitamata töötajatel pääseda ligi isikuandmetele ega süsteemi kriitiliselt tähtsatele andmetele.
2.1	Rünne tagaserverile peatab selle toimimise, näiteks takistab selle suhtlemist sõidukitega ja sõidukitele vajalike teenuste osutamist.	M3	Tagasüsteemidele rakendatakse turvameetmeid. Kui tagaserverid on teenuste osutamiseks kriitiliselt tähtsad, on süsteemiseisaku jaoks olemas taastamismeetmed. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).
3.2	Teave kaob pilvest. Tundlikud andmed võivad rünnete või õnnetuste tõttu kaduma minna, kui andmeid talletavad kolmandast isikust pilveteenuse pakkujad.	M4	Pilvandmetöötlusega seotud riskide minimeerimiseks rakendatakse turvameetmeid. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP) ja riikliku küberturvalisuse keskuse (NCSC) pilvandmetöötluse juhendis.
3.5	Teabega seotud rikkumine andmete tahtmatu jagamise tõttu (nt administraatori vead, andmete salvestamine töökodade serveritesse).	M5	Tagasüsteemidele rakendatakse andmetega seotud rikkumiste vältimiseks turvameetmeid. Turvameetmete näited on esitatud avatud veebirakenduste turbe projektis (OWASP).

2. Tahtmatu inimtegevusega seotud leevendusmeetmed

Tahtmatu inimtegevusega seotud ohte leevendavad meetmed on loetletud tabelis C2.

Tabel C2

Tahtmatu inimtegevusega seotud ohte leevendavad meetmed

Viide tabelile A1	Tahtmatu inimtegevusega seotud ohud	Viide	Leevendusmeede
15.1	Süütu ohver (nt omanik, käitaja või hooldusinsener) petetakse tahtmatult pahavara alla laadima või rünnet võimaldama.	M18	Rakendatakse meetmeid kasutajarollide ja juurdepääsuõiguste määratlemiseks ja kontrollimiseks, tuginedes vähima juurdepääsuõiguse põhimõttele.
15.2	Kindlaksmääratud turvakorda ei järgita.	M19	Organisatsioonid tagavad turvanõuete määratlemise ja järgimise, sealhulgas turvafunktsioonide haldamisega seotud toimingute ja juurdepääsu logimise.

3. Füüsilise andmekaoga seotud leevendusmeetmed

Füüsilise andmekaoga seotud ohte leevendavad meetmed on loetletud tabelis C3.

Tabel C3

Füüsilise andmekaoga seotud ohte leevendavad meetmed

Viide tabelile A1	Füüsilise andmekaoga seotud ohud	Viide	Leevendusmeede
30.1	Kolmanda isiku tekitatud kahju. Liiklusõnnetuse või varguse korral võivad tundlikud andmed kaduda või saada füüsiliselt kahjustada.	M24	Isikuandmete säilitamisel järgitakse andmete tervikluse ja konfidentsiaalsuse kaitse parimaid tavasid. Turvameetmete näited on esitatud dokumendis ISO/SC27/WG5.
30.2	Autoriõiguste digitaalkaitse konfliktidest tulenev kahju. Kasutajate andmed võidakse autoriõiguste digitaalkaitse probleemide tõttu kustutada.		
30.3	Tundlikud andmed (ja nende terviklus) võivad IT-osiste kulumise tõttu kaduda, põhjustades võimalikke järjestikuseid probleeme (nt võtme muutmise korral).		