JT taisyklė Nr. 155. Vienodos nuostatos dėl transporto priemonių patvirtinimo kibernetinio saugumo ir kibernetinio saugumo valdymo sistemos atžvilgiu [2021/387]

Įsigaliojimo data: 2021 m. sausio 22 d.

Šis dokumentas yra skirtas tik informacijai. Autentiški ir teisiškai privalomi tekstai:

— ECE/TRANS/WP.29/2020/79,

— ECE/TRANS/WP.29/2020/94 ir

— ECE/TRANS/WP.29/2020/97.

TURINYS

1. TAIKYMO SRITIS

1.1. Ši taisyklė taikoma M ir N kategorijų transporto priemonių kibernetiniam saugumui.

Ši taisyklė taip pat taikoma O kategorijos transporto priemonėms, jeigu jose įrengtas bent vienas elektroninis valdymo blokas.

1.2. Ši taisyklė taip pat taikoma L_6 ir L_7 kategorijų transporto priemonėms, jeigu jose įrengtos trečio arba aukštesnio lygio automatizuoto vairavimo funkcijos, kaip apibrėžta WP.29 orientaciniame dokumente su automatizuoto vairavimo apibrėžtimis ir Bendruosiuose principuose JT taisyklei dėl automatizuotų automobilių parengti (ECE/TRANS/WP.29/1140).

1.3. Ši taisyklė nedaro poveikio kitoms JT taisyklėms ir regioninės ar nacionalinės teisės aktams, kuriais reglamentuojama įgaliotų šalių prieiga prie transporto priemonės, jos duomenų, funkcijų ir išteklių, taip pat tokios prieigos sąlygos. Taisyklė taip pat neturi poveikio nacionalinės ir regioninės teisės aktų, kuriais reglamentuojamas privatumas ir fizinių asmenų apsauga tvarkant jų asmens duomenis, taikymui.

1.4. Taisyklė neturi poveikio kitoms JT taisyklėms, taip pat nacionalinės ar regioninės teisės aktams, kuriais kibernetinio saugumo požiūriu reglamentuojamas fizinių ir skaitmeninių atsarginių dalių ir komponentų kūrimas ir diegimas arba integravimas į sistemą.

2. APIBRĖŽTYS

Šioje taisyklėje vartojamų terminų apibrėžtys:

2.1. Transporto priemonių tipas – transporto priemonės, nesiskiriančios bent jau šiais esminiais aspektais:

a) gamintojo nurodytu transporto priemonės tipo ženklinimu;

b) esminiais elektros ir elektroninės sistemos sandaros ir išorės sąsajų kibernetinio saugumo aspektais.

2.2. Kibernetinis saugumas – būklė, kuriai esant transporto priemonės ir jų funkcijos yra apsaugos nuo kibernetinių grėsmių elektros arba elektroniniams komponentams.

2.3. Kibernetinio saugumo valdymo sistema (CSMS) – sisteminga, rizika grindžiama koncepcija, pagal kurią apibrėžiami organizaciniai procesai, atsakomybės sritys ir valdymas, skirti su grėsmėmis transporto priemonėms susijusiai rizikai valdyti ir transporto priemonėms nuo kibernetinių išpuolių apsaugoti.

2.4. Sistema – tam tikri komponentai ir (arba) posistemės, per kuriuos įdiegiama viena ar kelios funkcijos.

2.5. Kūrimo etapas – etapas, kuriuo transporto priemonės tipas dar nėra patvirtintas.

2.6. Gamybos etapas – tam tikro tipo transporto priemonių gamybos trukmė.

2.7. Pogamybinis etapas – laikotarpis, kuriuo tam tikro tipo transporto priemonės nebegaminamos ir kuris tęsiasi iki visų to tipo transporto priemonių gyvavimo ciklo pabaigos. Tam tikro tipo transporto priemonės šiuo etapu eksploatuojamos, tačiau nebegaminamos. Etapas baigiasi, kai eksploatuojamų konkretaus tipo transporto priemonių nebėra.

2.8. Rizikos mažinimo priemonė – priemonė, kuria mažinama rizika.

2.9. Rizika – galimybė, kad pasinaudojant konkrečia grėsme bus išnaudotos transporto priemonės saugumo spragos ir taip bus padaryta žala organizacijai arba asmeniui.

2.10. Rizikos vertinimas – visas procesas, per kurį surandama, atpažįstama ir aprašoma rizika (rizikos identifikavimas), suvokiamas rizikos pobūdis ir nustatomas rizikos lygis (rizikos analizė), rizikos analizės rezultatai palyginami su rizikos kriterijais ir taip nustatoma, ar rizika ir (arba) jos mastas yra priimtini arba toleruojami (rizikos įvertinimas).

2.11. Rizikos valdymas – koordinuota veikla, kuria siekiama orientuoti ir kontroliuoti organizaciją rizikos požiūriu.

2.12. Grėsmė – galima nepageidaujamo incidento priežastis, galinti nulemti žalą sistemai, organizacijai ar asmeniui.

2.13. Saugumo spraga – turto arba rizikos mažinimo priemonės silpna vieta, kuria gali būti naudojamasi vienos ar daugiau grėsmių atveju.

3. PATVIRTINIMO PARAIŠKA

3.1. Transporto priemonės tipo, atsižvelgiant į kibernetinį saugumą, patvirtinimo paraišką teikia transporto priemonių gamintojas arba jo tinkamai įgaliotas atstovas.

3.2. Kartu su ja pateikiami trys toliau nurodomų dokumentų egzemplioriai ir šie duomenys:

3.2.1. Transporto priemonės tipo aprašymas šios taisyklės 1 priede nurodytais aspektais.

3.2.2. Tais atvejais, kai informacijai taikomos intelektinės nuosavybės teisės arba ji yra susijusi su ypatingomis gamintojo ar jo tiekėjų turimomis žiniomis, gamintojas arba jo tiekėjai turi pateikti užtektinai informacijos, reikalingos siekiant tinkamai atlikti šioje taisyklėje nurodytus patikrinimus. Ši informacija laikoma konfidencialia.

3.2.3. Kibernetinio saugumo valdymo sistemos atitikties sertifikatas pagal šios taisyklės 6 punktą.

3.3. Dokumentai turi būti suskirstyti į dvi dalis:

a) Patvirtinti skirtas oficialus dokumentų rinkinys, kuriame išdėstyta 1 priede nurodyta medžiaga ir kuris tipo patvirtinimo institucijai arba jos techninei tarnybai pateikiamas tuo pačiu metu kaip ir tipo patvirtinimo paraiška. Šį dokumentų rinkinį tipo patvirtinimo institucija arba jos techninė tarnyba naudoja kaip pagrindinę medžiagą, kuria remiamasi atliekant patvirtinimo procesą. Tipo patvirtinimo institucija arba jos techninė tarnyba užtikrina, kad šis dokumentų rinkinys būtų prieinamas bent 10 metų nuo to laiko, kai galutinai baigiamos gaminti atitinkamo tipo transporto priemonės.

b) Gamintojas gali pasilikti su šios taisyklės reikalavimais susijusią papildomą medžiagą, kurią jis tipo patvirtinimo metu padaro prieinamą patikrinti. Gamintojas užtikrina, kad bet kuri medžiaga, kuri tipo patvirtinimo metu buvo padaryta prieinama patikrinti, išliktų prieinama bent 10 metų nuo to laiko, kai galutinai baigiamos gaminti atitinkamo tipo transporto priemonės.

4. ŽENKLINIMAS

4.1. Prie kiekvienos transporto priemonės, atitinkančios pagal šią taisyklę patvirtintą transporto priemonių tipą, aiškiai matomoje ir lengvai prieinamoje vietoje, nurodytoje patvirtinimo formoje, pritvirtinamas tarptautinis patvirtinimo ženklas, kurį sudaro:

4.1.1. apskritimas, kuriame įrašyta raidė E ir tipą patvirtinusios šalies skiriamasis numeris;

4.1.2. į dešinę nuo 4.1.1 punkte nurodyto apskritimo – šios taisyklės numeris, toliau raidė R, brūkšnelis ir patvirtinimo numeris.

4.2. Jeigu transporto priemonė šalyje, patvirtinusioje tipą pagal šią taisyklę, atitinka transporto priemonių tipą, patvirtintą pagal vieną ar kelias kitas prie Susitarimo pridėtas taisykles, minėtame 4.1.1 punkte nurodyto ženklo kartoti nereikia; tokiu atveju taisyklė ir patvirtinimo numeriai, taip pat papildomi visų taisyklių, pagal kurias patvirtinimas suteiktas šalyje, suteikusioje patvirtinimą pagal šią taisyklę, ženklai išdėstomi vertikaliais stulpeliais į dešinę nuo 4.1.1 punkte nustatyto ženklo.

4.3. Patvirtinimo ženklas turi būti aiškiai įskaitomas ir nenutrinamas.

4.4. Patvirtinimo ženklas pateikiamas ant gamintojo pritvirtintos transporto priemonės duomenų plokštelės arba greta jos.

4.5. Šios taisyklės 3 priede pateikiama patvirtinimo ženklų išdėstymo pavyzdžių.

5. PATVIRTINIMAS

5.1. Tipo patvirtinimo institucijos kibernetinio saugumo aspektais atitinkamai suteikia tik šios taisyklės reikalavimus atitinkančių transporto priemonių tipo patvirtinimus.

5.1.1. Tipo patvirtinimo institucija arba techninė tarnyba, atlikdamos dokumentų patikras, patikrina, ar transporto priemonių gamintojas atitinkamo tipo transporto priemonių atžvilgiu ėmėsi reikiamų priemonių siekdamas:

a) surinkti ir patikrinti šioje taisyklėje reikalaujamą visos tiekimo grandinės informaciją ir taip įrodyti, kad su tiekėjais susijusi rizika yra nustatyta ir valdoma;

b) dokumentais įforminti rizikos vertinimą (kūrimo etapu arba atgaline data), bandymų rezultatus ir transporto priemonės tipui taikomas rizikos mažinimo priemones, įskaitant rizikos vertinimui pagrįsti skirtą projektinę informaciją;

c) projektuojant atitinkamo tipo transporto priemones įdiegti tinkamas kibernetinio saugumo priemones;

d) nustatyti galimus išpuolius prieš kibernetinį saugumą ir į juos reaguoti;

e) registruoti duomenis, padedančius nustatyti kibernetinius išpuolius ir numatyti galimybes atsekti duomenis teismo ekspertizės būdu, kad būtų galima išanalizuoti bandymus atlikti kibernetinius išpuolius arba atliktus sėkmingus kibernetinius išpuolius.

5.1.2. Tipo patvirtinimo institucija arba techninė tarnyba, išbandydama atitinkamo tipo transporto priemonę, patikrina, ar transporto priemonių gamintojas įdiegė kibernetinio saugumo priemones, kurias įformino dokumentais. Tipo patvirtinimo institucija arba techninė tarnyba bandymus imties sudarymo būdu atlieka pati arba bendradarbiaudama su transporto priemonių gamintoju. Imtis sudaroma pagrindinį dėmesį skiriant rizikai, kuri atliekant rizikos vertinimą įvertinama kaip didelė, tačiau ne tik jai.

5.1.3. Tipo patvirtinimo institucija arba techninė tarnyba atsisako kibernetinio saugumo atžvilgiu suteikti tipo patvirtinimą, jeigu transporto priemonių gamintojas neįvykdė vieno arba daugiau 7.3 punkte nurodytų reikalavimų, t. y.:

a) transporto priemonių gamintojas neatliko 7.3.3 punkte nurodyto išsamaus rizikos vertinimo; gamintojas, be kita ko, atsižvelgė ne į visas rizikos rūšis, susijusias su 5 priedo A dalyje nurodytomis grėsmėmis;

b) transporto priemonių gamintojas neapsaugojo atitinkamo tipo transporto priemonių nuo rizikos, kuri buvo nustatyta transporto priemonių gamintojui atliekant rizikos vertinimą, arba nebuvo įdiegtos proporcingos rizikos mažinimo priemonės, kaip reikalaujama 7 punkte;

c) transporto priemonių gamintojas neįdiegė tinkamų ir proporcingų priemonių, kuriomis būtų apsaugotos atitinkamo tipo transporto priemonių specialiosios terpės (jeigu jos numatytos), skirtos antrinės rinkos programinei įrangai, tarnyboms, programoms ar duomenims saugoti ir vykdymo komandoms leisti;

d) transporto priemonių gamintojas iki patvirtinimo neatliko tinkamų ir pakankamų bandymų įdiegtų saugumo priemonių veiksmingumui patikrinti.

5.1.4. Vertinimą atliekanti tipo patvirtinimo institucija taip pat atsisako kibernetinio saugumo atžvilgiu suteikti tipo patvirtinimą, jeigu tipo patvirtinimo institucija arba techninė tarnyba iš transporto priemonių gamintojo negavo pakankamai informacijos atitinkamo tipo transporto priemonių kibernetiniam saugumui įvertinti.

5.2. Pranešimas apie patvirtinimą, patvirtinto tipo išplėtimą arba transporto priemonės tipo nepatvirtinimą pagal šią taisyklę perduodamas šią taisyklę taikančioms 1958 m. susitarimo šalims, naudojant šios taisyklės 2 priede pateiktą pavyzdį atitinkantį šabloną.

5.3. Tipo patvirtinimo institucijos nesuteikia tipo patvirtinimo nepatikrinusios, ar gamintojas įdiegė patenkinamą tvarką ir procedūras, kaip tinkamai valdyti šioje taisyklėje reglamentuojamus kibernetinio saugumo aspektus.

5.3.1. Tipo patvirtinimo institucija ir jos techninės tarnybos užtikrina ne tik 1958 m. susitarimo 2 priedėlyje nustatytų kriterijų taikymą, bet ir:

a) kompetentingą personalą, turintį tinkamų įgūdžių kibernetinio saugumo srityje ir specialių automobilių rizikos vertinimo žinių ([1]);

b) įdiegtas vienodo vertinimo pagal šią taisyklę procedūras.

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

5.3.2. Kiekviena šią taisyklę taikanti susitariančioji šalis per savo tipo patvirtinimo instituciją informuoja kitas šią JT taisyklę taikančių susitariančiųjų šalių tipo patvirtinimo institucijas apie metodą ir kriterijus, kuriais vadovaudamasi informaciją teikianti institucija vertina pagal šią taisyklę, ypač pagal jos 5.1, 7.2 ir 7.3 punktus, įdiegtų priemonių tinkamumą.

Šia informacija keičiamasi a) tik iki patvirtinimo suteikimo pirmą kartą pagal šią taisyklę ir b) kiekvieną kartą, kai vertinimo metodas ar kriterijai atnaujinami.

Šia informacija ketinama keistis siekiant surinkti ir išanalizuoti geriausią patirtį ir užtikrinti, kad šią taisyklę vienodai taikytų visos ją taikančios tipo patvirtinimo institucijos.

5.3.3. Tinkamu laiku ir ne vėliau kaip per 14 dienų iki patvirtinimo suteikimo pirmą kartą taikant atitinkamo vertinimo metodus ir kriterijus 5.3.2 punkte nurodyta informacija anglų kalba įkeliama į Jungtinių Tautų Europos ekonomikos komisijos sukurtą saugią internetinę duomenų bazę „DETA“ ([2]). Informacija turi būti pakankama siekiant suprasti, kokį minimalų rezultatų lygį tipo patvirtinimo institucija patvirtino dėl 5.3.2 punkte nurodyto kiekvieno konkretaus reikalavimo ir kokius procesus bei priemones ji taiko siekdama patikrinti, ar šis minimalus rezultatų lygis yra pasiektas ([3]).

5.3.4. 5.3.2 punkte nurodytą informaciją gaunančios tipo patvirtinimo institucijos gali pateikti pastabų informaciją teikiančiai tipo patvirtinimo institucijai, per 14 dienų nuo informacijos gavimo šias pastabas įkeldamos į DETA.

5.3.5. Jeigu tipo patvirtinimo institucija negali atsižvelgti į pastabas, gautas pagal 5.3.4 punktą, pastabas atsiuntusios tipo patvirtinimo institucijos ir patvirtinimą teikianti tipo patvirtinimo institucija stengiasi papildomai išsiaiškinti padėtį pagal 1958 m. susitarimo 6 priedėlį. Pasaulinio forumo transporto priemonių reglamentavimui suderinti (WP.29) atitinkama pavaldžioji darbo grupė ([4]) šios taisyklės klausimais susitaria dėl bendro metodų aiškinimo ir vertinimo kriterijų ([5]). Bendras aiškinimas įgyvendinamas ir visos tipo patvirtinimo institucijos atitinkamai pagal šią taisyklę išduoda tipo patvirtinimus.

5.3.6. Kiekviena tipo patvirtinimą pagal šią taisyklę suteikianti tipo patvirtinimo institucija apie suteiktą patvirtinimą praneša kitoms tipo patvirtinimo institucijoms. Tipo patvirtinimą kartu su papildomais dokumentais tipo patvirtinimo institucija per 14 dienų nuo patvirtinimo suteikimo anglų kalba įkelia į DETA ([6]).

5.3.7. Susitariančiosios šalys suteiktus patvirtinimus gali nagrinėti remdamosi pagal 5.3.6 punktą įkelta informacija. Jeigu susitariančiųjų šalių požiūriai išsiskiria, nesutarimai sprendžiami pagal 1958 m. susitarimo 6 priedėlio 10 straipsnį. Susitariančiosios šalys apie 1958 m. susitarimo 6 priedėlio požiūriu skirtingus aiškinimus taip pat informuoja atitinkamą Pasaulinio forumo transporto priemonių reglamentavimui suderinti (WP.29) pavaldžiąją darbo grupę. Atitinkama darbo grupė padeda išspręsti skirtingų požiūrių klausimą ir šiuo klausimu prireikus gali konsultuotis su WP.29 grupe.

5.4. Šios taisyklės 7.2 punkto tikslu gamintojas užtikrina, kad būtų įgyvendinti šioje taisyklėje reglamentuoti kibernetinio saugumo aspektai.

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

([3]) Išsamios informacijos (pvz., metodo, kriterijų, rezultatų lygio) įkėlimo gairės ir informacijos formatas nurodomi aiškinamajame dokumente, kurį rengia Kibernetinio saugumo ir belaidžio ryšio darbo grupė septintajai darbo grupės dėl automatizuotų / autonominių ir susietųjų transporto priemonių (GRVA) sesijai.

([4]) Darbo grupė dėl automatizuotų / autonominių ir susietųjų transporto priemonių (GRVA).

([5]) Šis aiškinimas išdėstomas aiškinamajame dokumente, nurodytame 5.3.3 punkto išnašoje.

([6]) Papildomą informaciją apie dokumentų rinkiniui taikomus minimalius reikalavimus GRVA parengs per savo septintąją sesiją.

6. KIBERNETINIO SAUGUMO VALDYMO SISTEMOS ATITIKTIES SERTIFIKATAS

6.1. Susitariančiosios šalys paskiria tipo patvirtinimo instituciją, kuri atlieka gamintojo vertinimą ir išduoda kibernetinio saugumo valdymo sistemos atitikties sertifikatą.

6.2. Paraišką kibernetinio saugumo valdymo sistemos atitikties sertifikatui gauti teikia transporto priemonių gamintojas arba jo tinkamai įgaliotas atstovas.

6.3. Kartu su ja pateikiami trys toliau nurodomų dokumentų egzemplioriai ir šie duomenys:

6.3.1. dokumentai, kuriuose aprašoma kibernetinio saugumo valdymo sistema;

6.3.2. pasirašyta deklaracija, kuriai naudojamas 1 priedo 1 priedėlyje apibrėžto pavyzdžio šablonas.

6.4. Kai atliekamas vertinimas, gamintojas, naudodamas 1 priedo 1 priedėlyje apibrėžtą šabloną, deklaruoja ir tipo patvirtinimo institucijai arba jos techninei tarnybai įrodo, kad jis turi įdiegęs reikiamus procesus kibernetinio saugumo reikalavimams pagal šią taisyklę įvykdyti.

6.5. Kai šis vertinimas tinkamai užbaigiamas ir gaunama pagal 1 priedo 1 priedėlyje apibrėžtą šabloną užpildyta ir pasirašyta gamintojo deklaracija, gamintojui suteikiamas šios taisyklės 4 priede aprašytas kibernetinio saugumo valdymo sistemos atitikties sertifikatas (toliau – kibernetinio saugumo valdymo sistemos atitikties sertifikatas).

6.6. Tipo patvirtinimo institucija arba jos techninė tarnyba kibernetinio saugumo valdymo sertifikatą surašo pagal šios taisyklės 4 priede išdėstytą šabloną.

6.7. Kibernetinio saugumo valdymo sistemos atitikties sertifikatas galioja daugiausia trejus metus nuo jo išdavimo datos, nebent jis atšaukiamas.

6.8. Kibernetinio saugumo valdymo sistemos atitikties sertifikatą išdavusi tipo patvirtinimo institucija bet kuriuo metu gali patikrinti, ar reikalavimai sertifikatui gauti tebėra vykdomi. Jeigu šioje taisyklėje nustatyti reikalavimai nebevykdomi, tipo patvirtinimo institucija kibernetinio saugumo valdymo sistemos atitikties sertifikatą atšaukia.

6.9. Gamintojas tipo patvirtinimo instituciją arba jos techninę tarnybą informuoja apie bet kokius pasikeitimus, turėsiančius poveikį kibernetinio saugumo valdymo sistemos atitikties sertifikato aktualumui. Pasikonsultavusi su gamintoju, tipo patvirtinimo institucija arba jos techninė tarnyba sprendžia, ar reikalingi nauji patikrinimai.

6.10. Tinkamu laiku, siekdamas, kad iki kibernetinio saugumo valdymo sistemos atitikties sertifikato galiojimo laikotarpio pabaigos tipo patvirtinimo institucija galėtų užbaigti vertinimą, gamintojas kreipiasi dėl naujo kibernetinio saugumo valdymo sistemos atitikties sertifikato išdavimo arba galiojančio sertifikato pratęsimo. Jeigu vertinimo rezultatai yra teigiami, tipo patvirtinimo institucija išduoda naują kibernetinio saugumo valdymo sistemos atitikties sertifikatą arba pratęsia jo galiojimą dar trejiems metams. Tipo patvirtinimo institucija patikrina, ar kibernetinio saugumo valdymo sistema ir toliau atitinka šios taisyklės reikalavimus. Tipo patvirtinimo institucija naują sertifikatą išduoda tais atvejais, kai tipo patvirtinimo institucijai arba jos techninei tarnybai buvo pranešta apie pasikeitimus ir atlikus naują vertinimą šie pasikeitimai buvo įvertinti teigiamai.

6.11. Gamintojo turimo kibernetinio saugumo valdymo sistemos atitikties sertifikato galiojimo pabaiga arba atšaukimas tų transporto priemonių tipų, kurioms atitinkama kibernetinio saugumo valdymo sistema buvo aktuali, atžvilgiu laikomi patvirtinimo pakeitimu, kaip nurodyta 8 punkte, o tai gali reikšti ir patvirtinimo atšaukimą, jeigu patvirtinimo suteikimo sąlygos nebevykdomos.

7. SPECIFIKACIJOS

7.1. Bendrosios specifikacijos

7.1.1. Šios taisyklės reikalavimais neribojamos kitų JT taisyklių nuostatos ar reikalavimai.

7.2. Kibernetinio saugumo valdymo sistemai taikomi reikalavimai

7.2.1. Atlikdama vertinimą, tipo patvirtinimo institucija arba jos techninė tarnyba patikrina, ar transporto priemonių gamintojas turi kibernetinio saugumo valdymo sistemą, ir patikrina, ar ji atitinka šią taisyklę.

7.2.2. Kibernetinio saugumo valdymo sistema apima toliau nurodytus aspektus.

7.2.2.1. Transporto priemonių gamintojas tipo patvirtinimo institucijai arba techninei tarnybai įrodo, kad jo kibernetinio saugumo valdymo sistema taikoma šiais etapais:

a) kūrimo etapu;

b) gamybos etapu;

c) pogamybiniu etapu.

7.2.2.2. Transporto priemonių gamintojas įrodo, jog jo kibernetinio saugumo valdymo sistemoje naudojamais procesais užtikrinama, kad būtų tinkamai atsižvelgta į saugumą, taip pat į įvairią riziką ir 5 priede išvardytas rizikos mažinimo priemones. Tai apima:

a) gamintojo organizacijoje naudojamus procesus kibernetiniam saugumui valdyti;

b) tam tikrų tipų transporto priemonėms kylančiai rizikai nustatyti taikomus procesus. Vertinant šiuos procesus, atsižvelgiama į 5 priedo A dalyje išvardytas ir kitas aktualias grėsmes;

c) nustatytos rizikos vertinimo, suskirstymo kategorijomis ir mažinimo procesus;

d) procesus, taikomus siekiant patikrinti, ar nustatyta rizika yra tinkamai valdoma;

e) procesus, naudojamus tam tikro tipo transporto priemonių kibernetiniam saugumui išbandyti;

f) procesus, naudojamus siekiant užtikrinti, kad rizikos vertinimas nuolat būtų aktualus;

g) procesus, naudojamus siekiant stebėti ir aptikti tam tikrų tipų transporto priemonėms aktualius kibernetinius išpuolius, kibernetines grėsmes ir saugumo spragas ir į juos reaguoti, taip pat procesus, skirtus įvertinti, ar įdiegtos kibernetinio saugumo priemonės vis dar yra veiksmingos atsižvelgiant į nustatytas naujas kibernetines grėsmes ir saugumo spragas;

h) procesus, kuriuos taikant pateikiami duomenys, aktualūs bandymų atlikti kibernetinius išpuolius arba sėkmingai atliktų kibernetinių išpuolių analizei.

7.2.2.3. Transporto priemonių gamintojas įrodo, jog jo kibernetinio saugumo valdymo sistemoje taikomais procesais užtikrinama, kad, remiantis 7.2.2.2 punkto c ir g papunkčiuose nurodytomis kategorijomis, per pagrįstą laikotarpį būtų sumažintos kibernetinės grėsmės ir panaikintos tos saugumo spragos, kurių sumažinimas ir panaikinimas priklauso nuo transporto priemonių gamintojo atsakomųjų veiksmų.

7.2.2.4. Transporto priemonių gamintojas įrodo, jog jo kibernetinio saugumo valdymo sistemoje naudojamais procesais užtikrinama, kad 7.2.2.2 punkto g papunktyje nurodyta stebėsena būtų nuolatinė. Tai apima:

a) transporto priemonių įtraukimą į stebėseną po pirmosios registracijos;

b) gebėjimą analizuoti ir iš transporto priemonės duomenų bei transporto priemonės žurnalo failų nustatyti kibernetines grėsmes, saugumo spragas ir kibernetinius išpuolius. Šiuo gebėjimu turi būti laikomasi 1.3 punkto ir automobilių savininkų ar vairuotojų teisių į privatumą, ypač susijusių su sutikimu.

7.2.2.5. Transporto priemonių gamintojas privalo įrodyti, kaip jo kibernetinio saugumo valdymo sistema 7.2.2.2 punkto reikalavimų atžvilgiu suvaldys galimą priklausomybę nuo sutartimis susijusių tiekėjų, paslaugų teikėjų ar gamintojui pavaldžių organizacijų.

7.3. Transporto priemonių tipams taikomi reikalavimai

7.3.1. Gamintojas turi galiojantį tvirtinamam transporto priemonės tipui aktualios kibernetinio saugumo valdymo sistemos atitikties sertifikatą.

Tačiau, jeigu transporto priemonės tipas tvirtinamas iki 2024 m. liepos 1 d. ir jeigu transporto priemonių gamintojas gali įrodyti, kad atitinkamo tipo transporto priemonės negalėjo būti kuriamos laikantis kibernetinio saugumo valdymo sistemos, tada transporto priemonių gamintojas įrodo, kad atitinkamo tipo transporto priemonių kūrimo etapu buvo tinkamai atsižvelgta į kibernetinį saugumą.

7.3.2. Transporto priemonių gamintojas tvirtinamo tipo transporto priemonių atžvilgiu nustato ir valdo su tiekėjais susijusią riziką.

7.3.3. Transporto priemonių gamintojas nustato kritinius tam tikro tipo transporto priemonių elementus, atlieka išsamų atitinkamo tipo transporto priemonių rizikos įvertinimą ir tinkamai valdo nustatytų rūšių riziką. Atliekant rizikos vertinimą, atsižvelgiama į individualius atitinkamo tipo transporto priemonių elementus ir jų sąveiką. Be to, atliekant rizikos vertinimą atsižvelgiama į sąveiką su visomis išorės sistemomis. Vertindamas riziką, transporto priemonių gamintojas atsižvelgia į riziką, susijusią su visomis 5 priedo A dalyje nurodytomis grėsmėmis, taip pat į bet kokią kitą aktualią riziką.

7.3.4. Transporto priemonių gamintojas apsaugo atitinkamo tipo transporto priemones nuo rizikos, kuri buvo nustatyta transporto priemonių gamintojui atliekant rizikos vertinimą. Atitinkamo tipo transporto priemonėms apsaugoti įdiegiamos proporcingos rizikos mažinimo priemonės. Įdiegtos rizikos mažinimo priemonės apima visas 5 priedo B ir C dalyse nurodytas rizikos mažinimo priemones, aktualias nustatytai rizikai sumažinti. Tačiau jeigu 5 priedo B arba C dalyje nurodyta rizikos mažinimo priemonė yra neaktuali arba nepakankama nurodytai rizikai sumažinti, transporto priemonių gamintojas užtikrina, kad būtų įdiegta kita tinkama rizikos mažinimo priemonė.

Visų pirma, jeigu tipas tvirtinamas iki 2024 m. liepos 1 d., transporto priemonių gamintojas užtikrina, kad, jeigu 5 priedo B arba C dalyje nurodytos rizikos mažinimo priemonės techniškai neįmanoma įdiegti, būtų įdiegta kita tinkama rizikos mažinimo priemonė. Gamintojas privalo tipo patvirtinimo institucijai pateikti atitinkamą techninių galimybių vertinimą.

7.3.5. Transporto priemonių gamintojas įdiegia tinkamų ir proporcingų priemonių, kuriomis būtų apsaugotos atitinkamo tipo transporto priemonių specialiosios terpės (jeigu jos numatytos), skirtos antrinės rinkos programinei įrangai, tarnyboms, programoms ar duomenims saugoti ir vykdymo komandoms leisti.

7.3.6. Transporto priemonių gamintojas iki patvirtinimo atlieka tinkamus ir pakankamus bandymus įdiegtų saugumo priemonių veiksmingumui patikrinti.

7.3.7. Transporto priemonių gamintojas atitinkamo tipo transporto priemonių atžvilgiu įdiegia priemones, kad galėtų:

a) nustatyti į tam tikro tipo transporto priemones nukreiptus kibernetinius išpuolius ir užkirsti jiems kelią;

b) padidinti savo gebėjimus vykdyti stebėseną ir aptikti atitinkamo tipo transporto priemonėms aktualias grėsmes, saugumo spragas ir kibernetinius išpuolius;

c) numatyti galimybes atsekti duomenis teismo ekspertizės būdu, kad būtų galima išanalizuoti bandymus atlikti kibernetinius išpuolius arba atliktus sėkmingus kibernetinius išpuolius.

7.3.8. Kriptografiniai moduliai, naudojami šiai taisyklei įgyvendinti, atitinka sutartus standartus. Jeigu naudojami kriptografiniai moduliai neatitinka sutartų standartų, tada transporto priemonių gamintojas pagrindžia jų naudojimą.

7.4. Nuostatos dėl ataskaitų teikimo

7.4.1. Transporto priemonių gamintojas bent kartą per metus, o jeigu aktualu – ir dažniau tipo patvirtinimo institucijai arba techninei tarnybai praneša apie savo stebėsenos veiklos rezultatus, kaip apibrėžta 7.2.2.2 punkto g papunktyje, į šią ataskaitą įtraukdamas aktualią informaciją apie naujus kibernetinius išpuolius. Transporto priemonių gamintojas tipo patvirtinimo institucijai arba techninei tarnybai taip pat praneša ir patvirtina, kad jo gaminamų tipų transporto priemonių atžvilgiu įdiegtos rizikos kibernetiniam saugumui mažinimo priemonės tebėra veiksmingos, ir nurodo visus papildomus veiksmus, kurių buvo imtasi.

7.4.2. Tipo patvirtinimo institucija arba techninė tarnyba patikrina pateiktą informaciją ir, jeigu reikia, pareikalauja, kad transporto priemonės gamintojas pašalintų nustatytus veiksmingumo trūkumus.

Jeigu ataskaitos arba reagavimo priemonių nepakanka, tipo patvirtinimo institucija gali nuspręsti pagal 6.8 punktą atšaukti kibernetinio saugumo valdymo sistemos atitikties sertifikatą.

8. TRANSPORTO PRIEMONĖS TIPO PAKEITIMAS IR PATVIRTINTO TIPO IŠPLĖTIMAS

8.1. Apie kiekvieną transporto priemonės tipo pakeitimą, turintį poveikį jos techniniams rezultatams kibernetinio saugumo ir (arba) šioje taisyklėje reikalaujamos dokumentacijos aspektais, pranešama transporto priemonės tipą patvirtinusiai tipo patvirtinimo institucijai. Tuomet ta tipo patvirtinimo institucija gali:

8.1.1. konstatuoti, kad padaryti pakeitimai tebeatitinka galiojančio tipo patvirtinimo reikalavimus ir dokumentaciją arba

8.1.2. atlikti reikiamą papildomą vertinimą pagal 5 punktą ir, kai aktualu, pareikalauti, kad už bandymų atlikimą atsakinga techninė tarnyba pateiktų papildomą bandymų ataskaitą.

8.1.3. Apie paliktą galioti tipo patvirtinimą, tipo išplėtimą arba tipo nepatvirtinimą, nurodant pakeitimus, pranešama šios taisyklės 2 priede pateiktą pavyzdį atitinkančia forma. Patvirtintą tipą išplečianti tipo patvirtinimo institucija suteikia minėto išplėtimo serijos numerį ir praneša apie tai kitoms šią taisyklę taikančioms 1958 m. susitarimo šalims, naudodama šios taisyklės 2 priede pateikto pavyzdžio pranešimo formą.

9. GAMYBOS ATITIKTIS

9.1. Gamybos atitikties procedūros turi atitikti nustatytąsias 1958 m. susitarimo 1 priedėlyje (E/ECE/TRANS/505/Rev.3) ir toliau nurodytus reikalavimus.

9.1.1. Patvirtinimo turėtojas užtikrina, kad gamybos atitikties bandymų rezultatai būtų užregistruoti ir kad pridedami dokumentai tipo patvirtinimo institucijai arba jos techninei tarnybai būtų prieinami susitarimu su ta institucija ar tarnyba nustatytą laikotarpį. Jis negali būti ilgesnis nei 10 metų, skaičiuoti pradedant nuo visiško gamybos nutraukimo pradžios;

9.1.2. Tipo patvirtinimą suteikusi tipo patvirtinimo institucija gali bet kada patikrinti visuose gamybos objektuose taikomus atitikties kontrolės metodus. Paprastai šios patikros atliekamos kartą per trejus metus.

10. SANKCIJOS UŽ GAMYBOS NEATITIKTĮ

10.1. Transporto priemonės tipui pagal šią taisyklę suteiktą patvirtinimą galima atšaukti, jeigu nesilaikoma šioje taisyklėje nustatytų reikalavimų arba jeigu šios taisyklės reikalavimų neatitinka transporto priemonių pavyzdžiai.

10.2. Jeigu tipo patvirtinimo institucija atšaukia savo anksčiau suteiktą patvirtinimą, ji apie tai kitoms šią taisyklę taikančioms susitariančiosioms šalims nedelsdama praneša naudodama šios taisyklės 2 priede pateikto pavyzdžio pranešimo formą.

11. VISIŠKAS GAMYBOS NUTRAUKIMAS

11.1. Visiškai nutraukęs pagal šią taisyklę patvirtinto tipo transporto priemonių gamybą, patvirtinimo turėtojas apie tai informuoja tipą patvirtinusią instituciją. Tokį pranešimą gavusi institucija apie tai praneša kitoms šią taisyklę taikančioms susitariančiosioms šalims, nusiųsdama patvirtinimo formos kopiją, kurios gale didžiosiomis raidėmis įrašomas įrašas „GAMYBA NUTRAUKTA“, kopija pasirašoma ir joje įrašoma data.

12. UŽ PATVIRTINIMO BANDYMĄ ATSAKINGŲ TECHNINIŲ TARNYBŲ IR TIPO PATVIRTINIMO INSTITUCIJŲ PAVADINIMAI BEI ADRESAI

12.1. Šią taisyklę taikančios Susitarimo šalys Jungtinių Tautų sekretoriatui praneša už patvirtinimo bandymus atsakingų techninių tarnybų ir tipo patvirtinimo institucijų, kurios tvirtina tipą ir kurioms turi būti siunčiami pranešimai apie kitose šalyse patvirtintą tipą, patvirtinto tipo išplėtimą, tipo nepatvirtinimą ar patvirtinimo atšaukimą, pavadinimus ir adresus.

1 PRIEDAS

Informacinis dokumentas

Toliau nurodyta informacija, jei taikoma, pateikiama trimis egzemplioriais (taip pat turi būti pateiktas jos turinys). Brėžiniai turi būti atitinkamo mastelio ir pakankamai išsamūs ir pateikiami A4 formato lapuose arba A4 formato aplanke. Jeigu pateikiamos nuotraukos, jos turi būti pakankamai aiškios.

1. Markė (gamintojo prekės pavadinimas): .....

2. Tipas ir bendras (-i) komercinis (-iai) aprašas (-ai): .....

3. Tipo identifikavimas, jei pažymėtas ant transporto priemonės: .....

4. Tokio ženklo vieta: .....

5. Transporto priemonės kategorija (-os): .....

6. Gamintojo / gamintojo atstovo pavadinimas ir adresas: .....

7. Surinkimo gamyklos (-ų) pavadinimas (-ai) ir adresas (-ai): .....

8. Tipinės transporto priemonės nuotrauka (-os) ir (arba) brėžinys (-iai): .....

9. Kibernetinis saugumas

9.1. Bendrosios atitinkamo tipo transporto priemonių konstrukcijos savybės, t. y., be kita ko:

a) transporto priemonės sistemos, aktualios atitinkamo tipo transporto priemonių kibernetiniam saugumui;

b) kibernetiniam saugumui aktualūs tų sistemų komponentai;

c) tų sistemų sąveika su kitomis atitinkamo tipo transporto priemonių sistemomis ir išorės sąsajomis.

9.2. Transporto priemonės tipo scheminis išdėstymas

9.3. Kibernetinio saugumo valdymo sistemos atitikties sertifikato numeris: .....

9.4. Tvirtinamo transporto priemonės tipo dokumentai, kuriuose aprašomi jos rizikos vertinimo rezultatai ir nustatytų rūšių rizika: .....

9.5 Tvirtinamo transporto priemonės tipo dokumentai, kuriuose aprašomos išvardytose sistemose arba atitinkamo tipo transporto priemonėse įdiegtos rizikos mažinimo priemonės ir kaip jomis sumažinama nurodyta rizika: .....

9.6. Tvirtinamo transporto priemonės tipo dokumentai, kuriuose aprašoma specialiųjų terpių, skirtų antrinės rinkos programinei įrangai, tarnyboms, programoms ar duomenims, apsauga: .....

9.7. Tvirtinamo transporto priemonės tipo dokumentai, kuriuose aprašoma, kokiais bandymais buvo tikrinamas atitinkamo tipo transporto priemonių ir jų sistemų kibernetinis saugumas ir kokie tų bandymų rezultatai: .....

9.8. Aprašymas, kaip kibernetinio saugumo požiūriu buvo atsižvelgta į tiekimo grandinę: .....

1 priedo 1 priedėlis

Gamintojo deklaracijos, kad kibernetinio saugumo valdymo sistema atitinka reikalavimus, pavyzdys

Gamintojo deklaracija, kad kibernetinio saugumo valdymo sistema atitinka reikalavimus

Gamintojo pavadinimas: .....

Gamintojo adresas: .....

..... (*Gamintojo pavadinimas*) patvirtina, kad yra įdiegti ir bus išlaikomi procesai, atitinkantys JT taisyklės Nr. 155 7.2 punkte nustatytus kibernetinio saugumo valdymo sistemai taikomus reikalavimus. .....

Vieta: ..... (*vieta*)

Data: .....

Pasirašančio asmens vardas ir pavardė: .....

Pasirašančio asmens pareigos: .....

.....

(*Gamintojo atstovo antspaudas ir parašas*)

2 PRIEDAS

Pranešimas

(Maksimalus formatas: A4 (210 × 297 mm)

Pateikė: Administracijos pavadinimas:
.....
.....
.....

Dėl transporto priemonės tipo ([2])
Patvirtinimo
patvirtinto tipo išplėtimo
tipo patvirtinimo atšaukimo nuo dd/mm/mmmm
nepatvirtinimo
visiško gamybos nutraukimo

remiantis JT taisykle Nr. 155

Patvirtinimo Nr.: .....

Išplėtimo Nr.: .....

Išplėtimo motyvas: .....

1. Markė (gamintojo prekės pavadinimas): .....

2. Tipas ir bendras (-i) komercinis (-iai) aprašymas (-ai) .....

3. Tipo identifikavimas, jei pažymėtas ant transporto priemonės: .....

3.1. Tokio ženklo vieta: .....

4. Transporto priemonės kategorija (-os): .....

5. Gamintojo / gamintojo atstovo pavadinimas ir adresas: .....

6. Gamyklos (-ų) pavadinimas (-ai) ir adresas (-ai): .....

7. Kibernetinio saugumo valdymo sistemos atitikties sertifikato numeris: .....

8. Už patvirtinimo bandymus atsakinga techninė tarnyba: .....

9. Bandymų ataskaitos data: .....

10. Bandymų ataskaitos numeris: .....

11. Pastabos: (jeigu yra) .....

12. Vieta: .....

13. Data: .....

14. Parašas: .....

15. Pridedama patvirtinimo institucijai pateikto informacinio paketo, kurį galima gauti pateikus prašymą, informacinė rodyklė:

([1]) Tipą patvirtinusios / patvirtintą tipą išplėtusios / tipo nepatvirtinusios / tipo patvirtinimą atšaukusios (žr. patvirtinimo nuostatas šioje taisyklėje) šalies skiriamasis numeris.

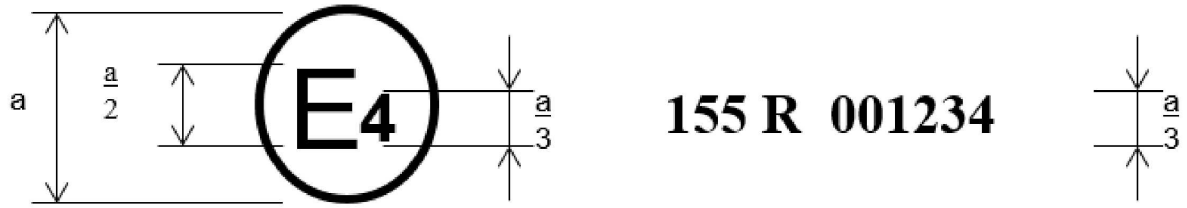
([2]) Išbraukti, kas netaikoma.:

3 PRIEDAS

Patvirtinimo ženklo išdėstymas

A MODELIS

(Žr. šios taisyklės 4.2 punktą)



a ≥ 8 mm

Pateiktas prie transporto priemonės tvirtinamas patvirtinimo ženklas rodo, kad atitinkamas kelių transporto priemonės tipas patvirtintas Nyderlanduose (E4) pagal Taisyklę Nr. 155; patvirtinimo numeris – 001234. Pirmieji du patvirtinimo numerio skaitmenys rodo, kad patvirtinimas buvo suteiktas pagal šios taisyklės pradinės redakcijos (00) reikalavimus.

4 PRIEDAS

Kibernetinio saugumo valdymo sistemos atitikties sertifikato pavyzdys

Kibernetinio saugumo valdymo sistemos atitikties sertifikatas

pagal JT taisyklę Nr. 155

Sertifikato numeris [*Numeris*]

[……. *Tipo patvirtinimo institucija*]

patvirtina, kad

gamintojas: ……

Gamintojo adresas: ……

atitinka taisyklės Nr. 155 7.2 punkto nuostatas.

Patikrinimas atliktas (data): ……

patikrinimą atliko (tipo patvirtinimo institucijos arba techninės tarnybos pavadinimas ir adresas): ……

Ataskaitos numeris: ……

Sertifikatas galioja iki [……*Data*]

Išduota [……*Vieta*]

[……*Data*]

[……*Parašas*]

Priedai: gamintojo kibernetinio saugumo valdymo sistemos aprašymas.

5 PRIEDAS

Grėsmių ir atitinkamų rizikos mažinimo priemonių sąrašas

1. Šį priedą sudaro trys dalys. Šio priedo A dalyje aprašomas grėsmių, saugumo spragų ir išpuolių metodų atskaitos scenarijus. Šio priedo B dalyje aprašomos atitinkamų tipų transporto priemonėms kylančių grėsmių mažinimo priemonės. C dalyje aprašomos už transporto priemonės ribų esančiose srityse, pvz., IT vidinio programavimo sistemose, kylančių grėsmių mažinimo priemonės.

2. Į A, B ir C dalis atsižvelgiama atliekant rizikos vertinimą ir parenkant rizikos mažinimo priemones, kurias turi įdiegti transporto priemonių gamintojai.

3. Aukšto lygio saugumo spragų ir atitinkamų jų pavyzdžių rodyklė sudaryta A dalyje. Ta pačia rodykle remiamasi B ir C dalyse pateiktose lentelėse, siekiant kiekvieną išpuolį ar saugumo spragą susieti su atitinkamų rizikos mažinimo priemonių sąrašu.

4. Grėsmių analizėje taip pat atsižvelgiama į galimus išpuolių padarinius. Jie gal padėti nustatyti rizikos lygį ir papildomų rūšių riziką. Išpuolių padariniai, be kita ko, gali būti šie:

   a) pablogėjusi transporto priemonės naudojimo sauga;

   b) nustojusios veikti transporto priemonės funkcijos;

   c) pakeista programinė įranga, pakitę eksploataciniai rezultatai;

   d) pakeista programinė įranga be eksploatacinių padarinių;

   e) pažeistas duomenų vientisumas;

   f) pažeistas duomenų konfidencialumas;

   g) duomenys tapę neprieinami;

   h) kiti, įskaitant nusikalstamumą.

A dalis. Su grėsmėmis susijusios saugumo spragos ar išpuolio metodas

1. Aukšto lygio grėsmių ir atitinkamų saugumo spragų ar išpuolio metodo aprašymai išvardyti lentelėje A1.

Lentelė A1

Su grėsmėmis susijusių saugumo spragų ar išpuolio metodų sąrašas

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
4.3.1. Grėsmės su eksploatuojamomis transporto priemonėmis susijusiems duomenų saugyklos serveriams	1	Duomenų saugyklos serveriai naudojami kaip priemonė išpuoliui prieš transporto priemonę įvykdyti arba duomenims išgauti	1.1	Privilegijomis piktnaudžiauja darbuotojai (vidaus subjektų išpuolis)
			1.2	Neleistina prieiga internetu prie serverio (jai sudaromos sąlygos, pavyzdžiui, pasitelkiant užpakalines duris, nepašalintas sistemos programinės įrangos saugumo spragas, SQL išpuolius arba kitas priemones)
			1.3	Neleistina fizinė prieiga prie serverio (pavyzdžiui, pasitelkiant USB laikmenas ar kitas prie serverio prijungiamas laikmenas)
	2	Sutrikdomos paslaugos iš duomenų saugyklos serverio ir tai turi poveikį transporto priemonės eksploatacijai	2.1	Dėl išpuolio prieš duomenų saugyklos serverį jis nustoja veikti, pavyzdžiui, dėl išpuolio serveris negali sąveikauti su transporto priemonėmis ir teikti paslaugų, nuo kurių priklauso transporto priemonių veikimas

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
	3	Duomenų saugyklos serveriuose laikomi su transporto priemonėmis susiję duomenys prarandami arba pažeidžiami („duomenų saugumo pažeidimas“)	3.1	Privilegijomis piktnaudžiauja darbuotojai (vidaus subjektų išpuolis)
			3.2	Prarandama informacija debesijoje. Neskelbtini duomenys gali būti prarasti dėl išpuolių arba avarijų, kai duomenis saugo debesijos paslaugas teikiančios trečiosios šalys
			3.3	Neleistina prieiga internetu prie serverio (jai sudaromos sąlygos, pavyzdžiui, pasitelkiant užpakalines duris, nepašalintas sistemos programinės įrangos saugumo spragas, SQL išpuolius arba kitas priemones)
			3.4	Neleistina fizinė prieiga prie serverio (pavyzdžiui, pasitelkiant USB laikmenas ar kitas prie serverio prijungiamas laikmenas)
			3.5	Informacijos saugumo pažeidimas netyčia išplatinant duomenis (pvz., administratoriaus klaidos)
4.3.2. Grėsmės transporto priemonėms dėl jų ryšių kanalų	4	Transporto priemonės gaunamų pranešimų arba duomenų klastojimas	4.1	Pranešimų klastojimas imitacijos būdu (pvz., 802.11p V2X per važiavimą vilkstine, GNSS pranešimai ir kt.)
			4.2	Sibilės išpuolis (siekiant imituoti kitas transporto priemones, tarsi kelyje yra daug transporto priemonių)
	5	Ryšių kanalais atliekamas neleistinas manipuliavimas transporto priemonės turimu kodu / duomenimis, jų ištrynimas ar kiti pakeitimai	5.1	Ryšių kanaluose palikta galimybė įterpti kodą, pavyzdžiui, į ryšio duomenų srautą gali būti įterpiamas pakeistas programinės įrangos dvejetainis kodas
			5.2	Ryšių kanaluose palikta galimybė manipuliuoti transporto priemonės turimais duomenimis / kodu
			5.3	Ryšių kanaluose palikta galimybė ant viršaus perrašyti transporto priemonės turimus duomenis / kodą
			5.4	Ryšių kanaluose palikta galimybė ištrinti transporto priemonės turimus duomenis / kodą
			5.5	Ryšių kanaluose palikta galimybė įrašyti duomenis / kodą į transporto priemonę (įrašyti duomenų kodą)
	6	Ryšių kanaluose palikta galimybė priimti nepatikimais laikomus ar nepatikimus pranešimus arba saugumo spraga sesijos užgrobimo arba pakartojimų išpuoliams vykdyti	6.1	Priimama informacija iš nepatikimo arba nepatikimu laikomo šaltinio
			6.2	Komunikacijos perėmimo išpuolis / sesijos užgrobimo išpuolis
			6.3	Pakartojimo išpuolis, pavyzdžiui, išpuolis prieš ryšių tinklų sietuvą, sudaro sąlygas išpuolį vykdančiam asmeniui įdiegti primityvesnį elektroninio valdymo bloko programinės įrangos arba tinklų sietuvo programinės aparatinės įrangos variantą

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
	7	Gali būti lengvai atskleidžiama informacija. Pavyzdžiui, pasiklausomi ryšiai arba yra palikta galimybė neleistinai prisijungti prie neskelbtinų failų arba katalogų	7.1	Informacijos perėmimas / trukdanti spinduliuotė / ryšių stebėsena
			7.2	Įgyjama galimybė neleistinai prisijungti prie failų arba duomenų
	8	Paslaugos trikdymo atakos per ryšių kanalus siekiant sutrikdyti transporto priemonės funkcijas	8.1	Didelio kiekio beprasmių duomenų siuntimas į transporto priemonės informacinę sistemą, kad ji negalėtų įprastu būdu teikti paslaugų
			8.2	Juodosios skylės išpuolis – siekdamas sutrikdyti ryšius tarp transporto priemonių, išpuolį atliekantis asmuo gali blokuoti pranešimus tarp transporto priemonių
	9	Neprivilegijuotas naudotojas gali gauti privilegijuotą prieigą prie transporto priemonės sistemų	9.1	Neprivilegijuotas naudotojas gali gauti privilegijuotą prieigą, pavyzdžiui, prie šakninio katalogo
	10	Ryšių priemonėse integruoti virusai gali užkrėsti transporto priemonių sistemas	10.1	Ryšių priemonėse integruotas virusas užkrečia transporto priemonės sistemas
	11	Transporto priemonės gaunamuose pranešimuose (pavyzdžiui, X2V arba diagnostiniuose pranešimuose) arba jos viduje perduodamuose pranešimuose yra kenkiamojo turinio	11.1	Kenkimo vidaus (pvz., CAN) pranešimai
			11.2	Kenkimo V2X pranešimai, pvz., infrastruktūros pranešimai transporto priemonei arba transporto priemonės pranešimai kitoms transporto priemonėms (pvz., CAM, DENM)
			11.3	Kenkimo diagnostiniai pranešimai
			11.4	Kenkimo nuosavybiniai pranešimai (pvz., pranešimai, paprastai siunčiami iš OEM arba komponentų / sistemos / funkcijos tiekėjo)
4.3.3. Grėsmės transporto priemonėms, susijusios su jų atnaujinimo procedūromis	12	Netinkamas atnaujinimo procedūrų naudojimas arba jų pažeidimas	12.1	Belaidžiu ryšiu atliekamo programinės įrangos atnaujinimo procedūrų pažeidimas. Tai apima sistemos atnaujinimo programos arba programinės aparatinės įrangos sufabrikavimą
			12.2	Vietinio / fizinio programinės įrangos atnaujinimo pažeidimas. Tai apima sistemos atnaujinimo programos arba programinės aparatinės įrangos sufabrikavimą
			12.3	Programinė įranga neleistinai modifikuojama (ir todėl tampa sugadinta) iki atnaujinimo proceso, nors atnaujinimo procesas nepažeidžiamas

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
			12.4	Pažeidžiami programinės įrangos tiekėjo kriptografiniai raktai ir taip paliekama galimybė atlikti klaidingą atnaujinimą
	13	Įmanoma atmesti teisėtus naujinimus.	13.1	Paslaugos trikdymo ataka prieš atnaujinimo serverį arba tinklą, siekiant užkirsti kelią kritinių programinės įrangos naujinių pateikimui ir (arba) konkrečiam klientui skirtų funkcijų atrakinimui
4.3.4. Grėsmės transporto priemonėms, susijusios su netyčiniais žmonių veiksmais, kuriais palengvinamas kibernetinis išpuolis	15	Teisėti subjektai gali imtis veiksmų, kuriais būtų netyčia palengvinamas kibernetinis išpuolis	15.1	Nekaltas nukentėjusysis (pvz., savininkas, operatorius arba techninės priežiūros inžinierius) suklaidinamas, kad imtųsi veiksmų, kuriais netyčia būtų užkrauta kenkimo programinė įranga arba sudarytos sąlygos atlikti išpuolį
			15.2	Nesivadovaujama apibrėžtomis saugumo procedūromis
4.3.5. Grėsmės transporto priemonėms, susijusios su jų išorės jungtimis ir ryšiais	16	Modifikuojant transporto priemonės funkcijų jungtį sudaromos sąlygos atlikti kibernetinį išpuolį, tai gali apimti telematiką; sistemas, kuriomis sudaromos sąlygos nuotolinėms operacijoms; sistemas, naudojančias trumpojo nuotolio bevielius ryšius	16.1	Modifikuojamos funkcijos, skirtos nuotoliniu būdu valdyti sistemas, pvz., nuotolinį raktą, imobilizatorių ir įkrovimo kolonėlę
			16.2	Modifikuojama transporto priemonės telematika (pvz., modifikuojamas jautrių prekių temperatūros matavimas, nuotoliniu būdu atrakinamos krovinių skyriaus durys)
			16.3	Trikdomos trumpojo nuotolio bevielės sistemos ar jutikliai
	17	Priegloboje veikianti trečiųjų šalių programinė įranga, pvz., pramoginės programos, naudojama kaip priemonė išpuoliams prieš transporto priemonės sistemas vykdyti	17.1	Sugadintos programos arba nesaugios programos naudojamos kaip metodas vykdyti išpuolius prieš transporto priemonių sistemas
	18	Prie išorės sąsajų, pvz., USB prievadų, OBD sistemos prievado, prijungti įrenginiai naudojami kaip priemonė išpuoliams prieš transporto priemonių sistemas vykdyti	18.1	Išorės sąsajos, pvz., USB ar kiti prievadai, naudojamos kaip išpuolio taškai, pavyzdžiui, įterpiant kodą
			18.2	Prie transporto priemonės sistemos prijungiama virusu užkrėsta laikmena
			18.3	Išpuolis palengvinamas pasitelkiant diagnostinę prieigą (pvz., raktus OBD prievade), pvz., (tiesiogiai ar netiesiogiai) modifikuojami transporto priemonės parametrai
4.3.6. Grėsmės transporto priemonės duomenims / kodui	19	Transporto priemonės duomenų / kodo išgavimas	19.1	Autorių teisių saugomos arba nuosavybinės programinės įrangos išgavimas iš transporto priemonės sistemų (produkto piratavimas)
			19.2	Neleistina prieiga prie privačios savininko informacijos, pvz., asmens tapatybės, mokėjimo sąskaitos informacijos, adresų knygos informacijos, vietovės informacijos, transporto priemonės elektroninio ID ir kt.
			19.3	Kriptografinių raktų išgavimas

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
	20	Transporto priemonės duomenų / kodo modifikavimas	20.1	Neteisėti / neleistini transporto priemonės elektroninio ID pakeitimai
			20.2	Tapatybės klastojimas. Pavyzdžiui, jeigu naudotojas, palaikydamas ryšį su muitinės sistemomis ar gamintojo duomenų saugyklos serveriu, nori rodyti kitą tapatybę
			20.3	Veiksmai, kuriais apeinamos stebėjimo sistemos (pvz., įsilaužimas / neteisėtas įrangos keitimas / pranešimų, pvz., ODR seklio duomenų arba paleidimų skaičiaus, blokavimas)
			20.4	Duomenų modifikavimas, siekiant suklastoti transporto priemonės vairavimo duomenis (pvz., ridą, važiavimo greitį, važiavimo kryptis ir kt.)
			20.5	Neleistini sistemos diagnostinių duomenų pakeitimai
	21	Duomenų / kodo ištrynimas	21.1	Neleistinas sistemos įvykių žurnalų ištrynimas / modifikavimas
	22	Kenkimo programinės įrangos įdiegimas	22.2	Įdiegiama kenkimo programinė įranga arba programinė įranga atlieka kenkimo veiklą
	23	Naujos programinės įrangos įdiegimas arba perrašymas ant esamos programinės įrangos	23.1	Transporto priemonės valdymo sistemos arba informacinės sistemos programinės įrangos sufabrikavimas
	24	Sistemų ar operacijų trikdymas	24.1	Paslaugos trikdymas – pavyzdžiui, vidaus tinkle jį gali sukelti CAN magistralės užtvindymas arba trikčių sukėlimas elektroniniame valdymo bloke, siunčiant daug pranešimų
	25	Transporto priemonės parametrų modifikavimas	25.1	Neleistina prieiga siekiant suklastoti svarbiausių transporto priemonės funkcijų, pvz., stabdžių duomenų, oro pagalvės panaudojimo ribos ir kt., konfigūracijos parametrus.
			25.2	Neleistina prieiga siekiant suklastoti įkrovimo parametrus, pvz., įkrovimo įtampą, įkrovimo galią, akumuliatoriaus temperatūrą ir kt.
4.3.7. Galimos saugumo spragos, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis	26	Kriptografinės technologijos gali būti neteisėtai užvaldytos arba yra netinkamai taikomos	26.1	Trumpų šifravimo raktų ir ilgo galiojimo laikotarpio derinys sudaro sąlygas išpuolį vykdančiam asmeniui nulaužti šifravimą
			26.2	Kriptografiniai algoritmai nepakankamai naudojami jautrioms sistemoms apsaugoti
			26.3	Naudojami kriptografiniai algoritmai, kurie jau yra pasenę arba greitai pasens

Aukšto lygio ir žemesnio lygio saugumo spragų / grėsmių aprašymai			Saugumo spragos ar išpuolio metodo pavyzdys	
	27	Sugadinamos dalys arba tiekiami komponentai, kad būtų galima įvykdyti išpuolį prieš transporto priemones	27.1	Aparatinė ar programinė įranga suprojektuota taip, kad sudaro sąlygas įvykdyti išpuolį, arba neatitinka projektinių kriterijų išpuoliui sustabdyti
	28	Programinė įranga arba aparatinė įranga kuriama paliekant galimybę atsirasti saugumo spragoms	28.1	Programinės įrangos defektai. Programinės įrangos defektų buvimas gali būti išnaudotinų saugumo spragų pagrindas. Tuo labiau, jeigu programinė įranga nebuvo išbandyta siekiant patikrinti, ar nėra žinomo blogo kodo ar defektų ir sumažinti nežinomo blogo kodo ar defektų buvimo riziką.
			28.2	Naudojant produkto kūrimo likučius (pvz., defektų šalinimo prievadus, JTAG prievadus, mikroprocesorius, kūrimo sertifikatus, kūrėjų slaptažodžius, …) galima sudaryti sąlygas gauti prieigą prie elektroninių valdymo blokų ar sudaryti sąlygas išpuolius vykdantiems asmenims gauti aukštesnio lygio privilegijas
	29	Saugumo spragos atsiranda projektuojant tinklą	29.1	Paliekama per daug atvirų interneto prievadų, suteikiant prieigą prie tinklo sistemų
			29.2	Siekiant užvaldyti, apeinamas tinklo atskyrimas. Konkretus pavyzdys – neapsaugotų tinklų sietuvų arba prieigos taškų (pvz., sunkvežimio sietuvo su priekaba) naudojimas siekiant apeiti apsaugos priemones ir gauti prieigą prie kitų tinklo segmentų, kad būtų galima atlikti kenkimo veiksmus, pvz., siųsti savavališkus CAN magistralės pranešimus
	31	Gali įvykti netyčinis duomenų perdavimas	31.1	Informacijos pažeidimas. Keičiantis automobilio naudotojui (pvz., parduodant automobilį arba automobilį išnuomojus naujam nuomininkui) gali būti nutekinami asmens duomenys
	32	Sąlygos išpuoliui gali būti sudaromos fiziškai modifikuojant sistemas	32.1	Modifikuojama elektroninė aparatinė įranga, pvz., į transporto priemonę įmontuojama neleistina elektroninė aparatinė įranga ir taip sudaromos sąlygos komunikacijos perėmimo išpuoliui Autorizuota elektroninė aparatinė įranga (pvz., jutikliai) pakeičiama įmontuojant neautorizuotą elektroninę aparatinę įrangą Modifikuojama jutiklio renkama informacija (pavyzdžiui, naudojant magnetą neteisėtai pakeičiama prie pavarų dėžės prijungto Holo efekto jutiklio informacija)

B dalis. Transporto priemonėms galinčių kilti grėsmių mažinimo priemonės

1. Grėsmių „transporto priemonės ryšių kanalams“ mažinimo priemonės

Su transporto priemonės ryšių kanalais susijusių grėsmių mažinimo priemonės išvardytos lentelėje B1.

Lentelė B1

Su transporto priemonės ryšių kanalais susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Grėsmės „transporto priemonės ryšių kanalams“	Nuoroda:	Rizikos mažinimo priemonė
4.1	Pranešimų klastojimas imitacijos būdu (pvz., 802.11p V2X per važiavimą vilkstine, GNSS pranešimai ir kt.)	M10	Transporto priemonė patikrina savo gaunamų pranešimų autentiškumą ir vientisumą
4.2	Sibilės išpuolis (siekiant imituoti kitas transporto priemones, tarsi kelyje yra daug transporto priemonių)	M11	Įdiegiamos saugumo kontrolės priemonės kriptografiniams raktams saugoti (pvz., naudojami aparatinės įrangos saugumo moduliai)
5.1	Ryšių kanaluose palikta galimybė į transporto priemonės turimus duomenis / kodą įterpti kitą kodą, pavyzdžiui, į ryšio duomenų srautą gali būti įterpiamas pakeistas programinės įrangos dvejetainis kodas	M10 M6	Transporto priemonė patikrina savo gaunamų pranešimų autentiškumą ir vientisumą Rizikai sumažinti sistemose turi būti užtikrinamas saugumo aspektų integravimas projektavimo metu
5.2	Ryšių kanaluose palikta galimybė modifikuoti transporto priemonės turimus duomenis / kodą	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai
5.3	Ryšių kanaluose palikta galimybė ant viršaus perrašyti transporto priemonės turimus duomenis / kodą		
5.4 21.1	Ryšių kanaluose palikta galimybė ištrinti transporto priemonės turimus duomenis / kodą		
5.5	Ryšių kanaluose palikta galimybė įrašyti duomenis / kodą į transporto priemonės sistemas (įrašyti duomenų kodą)		
6.1	Priimama informacija iš nepatikimo arba nepatikimu laikomo šaltinio	M10	Transporto priemonė patikrina savo gaunamų pranešimų autentiškumą ir vientisumą
6.2	Komunikacijos perėmimo išpuolis / sesijos užgrobimo išpuolis	M10	Transporto priemonė patikrina savo gaunamų pranešimų autentiškumą ir vientisumą
6.3	Pakartojimo išpuolis, pavyzdžiui, išpuolis prieš ryšių tinklų sietuvą, sudaro sąlygas išpuolį vykdančiam asmeniui įdiegti primityvesnį elektroninio valdymo bloko programinės įrangos arba tinklų sietuvo programinės aparatinės įrangos variantą		
7.1	Informacijos perėmimas / trukdanti spinduliuotė / ryšių stebėsena	M12	Apsaugomi į transporto priemonę ar iš jos perduodami konfidencialūs duomenys
7.2	Įgyjama galimybė neleistinai prisijungti prie failų arba duomenų	M8	Pagal sistemos projektą ir vykdant prieigos kontrolę neįgaliotiems darbuotojams neturėtų būti įmanoma prisijungti prie asmens duomenų arba kritinių sistemos duomenų. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.

Lentelės A1 nuoroda	Grėsmės „transporto priemonės ryšių kanalams“	Nuoroda:	Rizikos mažinimo priemonė
8.1	Didelio kiekio beprasmių duomenų siuntimas į transporto priemonės informacinę sistemą, kad ji negalėtų įprastu būdu teikti paslaugų	M13	Taikomos paslaugos trikdymo atakos aptikimo ir neutralizavimo priemonės
8.2	Juodosios skylės išpuolis, ryšių tarp transporto priemonių sutrikdymas blokuojant pranešimų perdavimą kitoms transporto priemonėms	M13	Taikomos paslaugos trikdymo atakos aptikimo ir neutralizavimo priemonės
9.1	Neprivilegijuotas naudotojas gali gauti privilegijuotą prieigą, pavyzdžiui, prie šakninio katalogo	M9	Taikomos neteisėtos prieigos prevencijos ir aptikimo priemonės
10.1	Ryšių priemonėse integruotas virusas užkrečia transporto priemonės sistemas	M14	Reikėtų apsvarstyti sistemų apsaugos nuo integruotų virusų ir (arba) kenkimo programinės įrangos priemones
11.1	Kenkimo vidaus (pvz., CAN) pranešimai	M15	Reikėtų apsvarstyti kenkimo vidaus pranešimų ar veiklos nustatymo priemones
11.2	Kenkimo V2X pranešimai, pvz., infrastruktūros pranešimai transporto priemonei arba transporto priemonės pranešimai kitoms transporto priemonėms (pvz., CAM, DENM)	M10	Transporto priemonė patikrina savo gaunamų pranešimų autentiškumą ir vientisumą
11.3	Kenkimo diagnostiniai pranešimai		
11.4	Kenkimo nuosavybiniai pranešimai (pvz., pranešimai, paprastai siunčiami iš OEM arba komponentų / sistemos / funkcijos tiekėjo)		

2. „Atnaujinimo procesui“ kylančios rizikos mažinimo priemonės

Su „atnaujinimo procesu “ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B2.

Lentelė B2

Su „atnaujinimo procesu “ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	„Atnaujinimo procesui“ kylančios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
12.1	Belaidžiu ryšiu atliekamo programinės įrangos atnaujinimo procedūrų pažeidimas. Tai apima sistemos atnaujinimo programos arba programinės aparatinės įrangos sufabrikavimą	M16	Taikomos saugios programinės įrangos atnaujinimo procedūros
12.2	Vietinio / fizinio programinės įrangos atnaujinimo pažeidimas. Tai apima sistemos atnaujinimo programos arba programinės aparatinės įrangos sufabrikavimą		
12.3	Programinė įranga neleistinai modifikuojama (ir todėl tampa sugadinta) iki atnaujinimo proceso, nors atnaujinimo procesas nepažeidžiamas		

Lentelės A1 nuoroda	„Atnaujinimo procesui“ kylančios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
12.4	Pažeidžiami programinės įrangos tiekėjo kriptografiniai raktai ir taip paliekama galimybė atlikti klaidingą atnaujinimą	M11	Įdiegiamos saugumo kontrolės priemonės kriptografiniams raktams saugoti
13.1	Paslaugos trikdymo ataka prieš atnaujinimo serverį arba tinklą, siekiant užkirsti kelią kritinių programinės įrangos naujinių pateikimui ir (arba) konkrečiam klientui skirtų funkcijų atrakinimui	M3	Taikomos duomenų saugyklos serverių sistemų saugumo kontrolės priemonės. Kai duomenų saugyklos serveriai turi kritinę reikšmę paslaugų teikimui, sistemos atjungimo atveju taikomos atkūrimo priemonės. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.

3. Netyčinių žmonių veiksmų, kuriais palengvinamas kibernetinis išpuolis, rizikos mažinimo priemonės

Su „netyčiniais žmonių veiksmais, kuriais palengvinamas kibernetinis išpuolis“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B3.

Lentelė B3

Grėsmių transporto priemonėms, susijusių su netyčiniais žmonių veiksmais, kuriais palengvinamas kibernetinis išpuolis, mažinimo priemonės

Lentelės A1 nuoroda	Su netyčiniais žmonių veiksmais susijusios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
15.1	Nekaltas nukentėjusysis (pvz., savininkas, operatorius arba techninės priežiūros inžinierius) suklaidinamas, kad imtųsi veiksmų, kuriais netyčia būtų užkrauta kenkimo programinė įranga arba sudarytos sąlygos atlikti išpuolį	M18	Remiantis mažiausios prieigos privilegijos principu, įdiegiamos naudotojų vaidmenų ir prieigos privilegijų apibrėžimo ir kontrolės priemonės
15.2	Nesivadovaujama apibrėžtomis saugumo procedūromis	M19	Organizacijos užtikrina, kad būtų apibrėžtos ir vykdomos saugumo procedūros, t. y., be kita ko, registruojami veiksmai ir prieigos atvejai, susiję su saugumo funkcijų valdymu

4. „Išorės jungčių ir ryšių“ rizikos mažinimo priemonės

Su „išorės jungtimis ir ryšiais“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B4.

Lentelė B4

Su „išorės jungtimis ir ryšiais“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Grėsmės „išorės jungtims ir ryšiams“	Nuoroda:	Rizikos mažinimo priemonė
16.1	Modifikuojamos funkcijos, skirtos nuotoliniu būdu valdyti transporto priemonės sistemas, pvz., nuotolinį raktą, imobilizatorių ir įkrovimo kolonėlę	M20	Taikomos nuotolinę prieigą turinčių sistemų saugumo kontrolės priemonės.
16.2	Modifikuojama transporto priemonės telematika (pvz., modifikuojamas jautrių prekių temperatūros matavimas, nuotoliniu būdu atrakinamos krovinių skyriaus durys)		

Lentelės A1 nuoroda	Grėsmės „išorės jungtims ir ryšiams“	Nuoroda:	Rizikos mažinimo priemonė
16.3	Trikdomos trumpojo nuotolio bevielės sistemos ar jutikliai		
17.1	Sugadintos programos arba nesaugios programos naudojamos kaip metodas vykdyti išpuolius prieš transporto priemonių sistemas	M21	Įvertinamas programinės įrangos saugumas, patvirtinamas jos autentiškumas ir apsaugomas jos vientisumas. Siekiant kuo labiau sumažinti transporto priemonės priegloboje skirtos laikyti arba joje numatomos laikyti trečiųjų šalių programinės įrangos keliamą riziką, taikomos saugumo kontrolės priemonės
18.1	Išorės sąsajos, pvz., USB ar kiti prievadai, naudojamos kaip išpuolio taškai, pavyzdžiui, įterpiant kodą	M22	Taikomos išorės sąsajų saugumo kontrolės priemonės.
18.2	Prie transporto priemonės prijungiama virusais užkrėsta laikmena		
18.3	Išpuolis palengvinamas pasitelkiant diagnostinę prieigą (pvz., raktus OBD prievade), pvz., (tiesiogiai ar netiesiogiai) modifikuojami transporto priemonės parametrai	M22	Taikomos išorės sąsajų saugumo kontrolės priemonės.

5. „Galimų išpuolio taikinių arba motyvacijos“ rizikos mažinimo priemonės

Su „galimais išpuolio taikiniais arba motyvacija“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B5.

Lentelė B5

Su „galimais išpuolio taikiniais arba motyvacija“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Su „galimais išpuolio taikiniais arba motyvacija“ susijusios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
19.1	Autorių teisių saugomos arba nuosavybinės programinės įrangos išgavimas iš transporto priemonės sistemų (produkto piratavimas / vogta programinė įranga)	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
19.2	Neleistina prieiga prie privačios savininko informacijos, pvz., asmens tapatybės, mokėjimo sąskaitos informacijos, adresų knygos informacijos, vietovės informacijos, transporto priemonės elektroninio ID ir kt.	M8	Pagal sistemos projektą ir vykdant prieigos kontrolę neįgaliotiems darbuotojams neturėtų būti įmanoma prisijungti prie asmens duomenų arba kritinių sistemos duomenų. Saugumo kontrolės pavyzdžių galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
19.3	Kriptografinių raktų išgavimas	M11	Įdiegiamos saugumo kontrolės priemonės kriptografiniams raktams saugoti (pvz., saugumo moduliai)
20.1	Neteisėti / neleistini transporto priemonės elektroninio ID pakeitimai	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
20.2	Tapatybės klastojimas. Pavyzdžiui, jeigu naudotojas, palaikydamas ryšį su muitinės sistemomis ar gamintojo duomenų saugyklos serveriu, nori rodyti kitą tapatybę		
20.3	Veiksmai, kuriais apeinamos stebėjimo sistemos (pvz., įsilaužimas / neteisėtas įrangos keitimas / pranešimų, pvz., ODR seklio duomenų arba paleidimų skaičiaus, blokavimas)	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.

Lentelės A1 nuoroda	Su „galimais išpuolio taikiniais arba motyvacija“ susijusios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
20.4	Duomenų modifikavimas, siekiant suklastoti transporto priemonės vairavimo duomenis (pvz., ridą, važiavimo greitį, važiavimo kryptis ir kt.)		Jutiklių duomenų arba perduodamų duomenų modifikavimo išpuolių riziką būtų galima sumažinti sugretinant duomenis iš skirtingų informacijos šaltinių
20.5	Neleistini sistemos diagnostinių duomenų pakeitimai		
21.1	Neleistinas sistemos įvykių žurnalų ištrynimas / modifikavimas	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
22.2	Įdiegiama kenkimo programinė įranga arba programinė įranga atlieka kenkimo veiklą	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
23.1	Transporto priemonės valdymo sistemos arba informacinės sistemos programinės įrangos sufabrikavimas		
24.1	Paslaugos trikdymas – pavyzdžiui, vidaus tinkle jį gali sukelti CAN magistralės užtvindymas arba trikčių sukėlimas elektroniniame valdymo bloke, siunčiant daug pranešimų	M13	Taikomos paslaugos trikdymo atakos aptikimo ir neutralizavimo priemonės
25.1	Neleistina prieiga siekiant suklastoti svarbiausių transporto priemonės funkcijų, pvz., stabdžių duomenų, oro pagalvės panaudojimo ribos ir kt., konfigūracijos parametrus.	M7	Sistemos duomenims / kodui apsaugoti taikomi prieigos kontrolės metodai ir projektai. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
25.2	Neleistina prieiga siekiant suklastoti įkrovimo parametrus, pvz., įkrovimo įtampą, įkrovimo galią, akumuliatoriaus temperatūrą ir kt.		

6. Galimų saugumo spragų, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis, rizikos mažinimo priemonės

Su „saugumo spragomis, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis,“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B6.

Lentelė B6

Su „saugumo spragomis, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis“, susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Galimų saugumo spragų, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis, keliamos grėsmės	Nuoroda:	Rizikos mažinimo priemonė
26.1	Trumpų šifravimo raktų ir ilgo galiojimo laikotarpio derinys sudaro sąlygas išpuolį vykdančiam asmeniui nulaužti šifravimą	M23	Vadovaujamasi programinės ir aparatinės įrangos kūrimo kibernetinio saugumo geriausia patirtimi

Lentelės A1 nuoroda	Galimų saugumo spragų, kurios galėtų būti išnaudojamos, jeigu nebūtų pakankamai apsaugotos arba nebūtų sumažintas pažeidžiamų vietų kiekis, keliamos grėsmės	Nuoroda:	Rizikos mažinimo priemonė
26.2	Kriptografiniai algoritmai nepakankamai naudojami jautrioms sistemoms apsaugoti		
26.3	Naudojami pasenę kriptografiniai algoritmai		
27.1	Aparatinė ar programinė įranga suprojektuota taip, kad sudaro sąlygas įvykdyti išpuolį, arba neatitinka projektinių kriterijų išpuoliui sustabdyti	M23	Vadovaujamasi programinės ir aparatinės įrangos kūrimo kibernetinio saugumo geriausia patirtimi
28.1	Programinės įrangos defektų buvimas gali būti išnaudotinų saugumo spragų pagrindas. Tuo labiau, jeigu programinė įranga nebuvo išbandyta siekiant patikrinti, ar nėra žinomo blogo kodo ar defektų ir sumažinti nežinomo blogo kodo ar defektų buvimo riziką.	M23	Vadovaujamasi programinės ir aparatinės įrangos kūrimo kibernetinio saugumo geriausia patirtimi Vykdomi pakankamos aprėpties kibernetinio saugumo bandymai
28.2	Naudojant produkto kūrimo likučius (pvz., defektų šalinimo prievadus, JTAG prievadus, mikroprocesorius, kūrimo sertifikatus, kūrėjų slaptažodžius, …) galima sudaryti sąlygas išpuolius vykdantiems asmenims gauti prieigą prie elektroninių valdymo blokų arba aukštesnio lygio privilegijas		
29.1	Paliekama per daug atvirų interneto prievadų, suteikiant prieigą prie tinklo sistemų		
29.2	Siekiant užvaldyti, apeinamas tinklo atskyrimas. Konkretus pavyzdys – neapsaugotų tinklų sietuvų arba prieigos taškų (pvz., sunkvežimio sietuvo su priekaba) naudojimas siekiant apeiti apsaugos priemones ir gauti prieigą prie kitų tinklo segmentų, kad būtų galima atlikti kenkimo veiksmus, pvz., siųsti savavališkus CAN magistralės pranešimus	M23	Vadovaujamasi programinės ir aparatinės įrangos kūrimo kibernetinio saugumo geriausia patirtimi Vadovaujamasi sistemos projektavimo ir sistemos integravimo geriausia patirtimi

7. „Transporto priemonės duomenų praradimo / duomenų pažeidimo“ rizikos mažinimo priemonės

Su „transporto priemonės duomenų praradimu / duomenų pažeidimu“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B7.

Lentelė B7

Su „transporto priemonės duomenų praradimu / duomenų pažeidimu“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	„Transporto priemonės duomenų praradimo / duomenų pažeidimo“ keliamos grėsmės	Nuoroda:	Rizikos mažinimo priemonė
31.1	Informacijos pažeidimas. Keičiantis automobilio naudotojui (pvz., parduodant automobilį arba automobilį išnuomojus naujam nuomininkui) gali būti pažeidžiami asmens duomenys	M24	Saugant asmens duomenis laikomasi duomenų vientisumo ir konfidencialumo apsaugos geriausios patirties.

8. „Sąlygų išpuoliui sudarymo fiziškai modifikuojant sistemas“ rizikos mažinimo priemonės

Su „Sąlygų išpuoliui sudarymu fiziškai modifikuojant sistemas“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje B8.

Lentelė B8

Su „Sąlygų išpuoliui sudarymu fiziškai modifikuojant sistemas“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	„Sąlygų išpuoliui sudarymo fiziškai modifikuojant sistemas“ grėsmių mažinimo priemonės	Nuoroda:	Rizikos mažinimo priemonė
32.1	Modifikuojama OEM aparatinė įranga, pvz., į transporto priemonę įmontuojama neleistina aparatinė įranga ir taip sudaromos sąlygos komunikacijos perėmimo išpuoliui	M9	Taikomos neteisėtos prieigos prevencijos ir aptikimo priemonės

C dalis. Ne transporto priemonėje kylančių grėsmių mažinimo priemonės

1. „Duomenų saugyklos serverių“ rizikos mažinimo priemonės

Su „duomenų saugyklos serveriais“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje C1.

Lentelė C1

Su „duomenų saugyklos serveriais“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Grėsmės „duomenų saugyklos serveriams“	Nuoroda:	Rizikos mažinimo priemonė
1.1 ir 3.1	Privilegijomis piktnaudžiauja darbuotojai (vidaus subjektų išpuolis)	M1	Siekiant kuo labiau sumažinti vidaus subjektų išpuolio riziką, taikomos duomenų saugyklos sistemų saugumo kontrolės priemonės
1.2 ir 3.3	Neleistina prieiga internetu prie serverio (jai sudaromos sąlygos pasitelkiant užpakalines duris, nepašalintas sistemos programinės įrangos saugumo spragas, SQL išpuolius arba kitas priemones)	M2	Siekiant kuo labiau sumažinti neleistinos prieigos galimybes, taikomos duomenų saugyklos sistemų saugumo kontrolės priemonės Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
1.3 ir 3.4	Neleistina fizinė prieiga prie serverio (pavyzdžiui, pasitelkiant USB laikmenas ar kitas prie serverio prijungiamas laikmenas)	M8	Pagal sistemos projektą ir vykdant prieigos kontrolę neįgaliotiems darbuotojams neturėtų būti įmanoma prisijungti prie asmens duomenų arba kritinių sistemos duomenų.
2.1	Dėl išpuolio prieš duomenų saugyklos serverį jis nustoja veikti, pavyzdžiui, dėl išpuolio serveris negali sąveikauti su transporto priemonėmis ir teikti paslaugų, nuo kurių priklauso transporto priemonių veikimas	M3	Taikomos duomenų saugyklos serverių sistemų saugumo kontrolės priemonės. Kai duomenų saugyklos serveriai turi kritinę reikšmę paslaugų teikimui, sistemos atjungimo atveju taikomos atkūrimo priemonės. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.
3.2	Prarandama informacija debesijoje. Neskelbtini duomenys gali būti prarasti dėl išpuolių arba avarijų, kai duomenis saugo debesijos paslaugas teikiančios trečiosios šalys	M4	Siekiant sumažinti su debesijos kompiuterija susijusią riziką, taikomos saugumo kontrolės priemonės Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) ir Nacionalinio kibernetinio saugumo centro (NCSC) debesijos kompiuterijos gairėse.
3.5	Informacijos saugumo pažeidimas netyčia išplatinant duomenis (pvz., administratoriaus klaidos, duomenų saugojimas garažuose esančiuose serveriuose)	M5	Siekiant užkirsti kelią duomenų saugumo pažeidimams, taikomos duomenų saugyklos sistemų saugumo kontrolės priemonės. Saugumo kontrolės priemonių pavyzdį galima rasti Atvirųjų internetinių taikomųjų programų saugumo projekto (OWASP) medžiagoje.

2. „Netyčinių žmonių veiksmų“ rizikos mažinimo priemonės

Su „netyčiniais žmonių veiksmais“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje C2.

Lentelė C2

Su „netyčiniais žmonių veiksmais“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	Su netyčiniais žmonių veiksmais susijusios grėsmės	Nuoroda:	Rizikos mažinimo priemonė
15.1	Nekaltas nukentėjusysis (pvz., savininkas, operatorius arba techninės priežiūros inžinierius) suklaidinamas, kad imtųsi veiksmų, kuriais netyčia būtų užkrauta kenkimo programinė įranga arba sudarytos sąlygos atlikti išpuolį	M18	Remiantis mažiausios prieigos privilegijos principu, įdiegiamos naudotojų vaidmenų ir prieigos privilegijų apibrėžimo ir kontrolės priemonės
15.2	Nesivadovaujama apibrėžtomis saugumo procedūromis	M19	Organizacijos užtikrina, kad būtų apibrėžtos ir vykdomos saugumo procedūros, t. y., be kita ko, registruojami veiksmai ir prieigos atvejai, susiję su saugumo funkcijų valdymu

3. „Fizinio duomenų praradimo“ rizikos mažinimo priemonės

Su „fiziniu duomenų praradimu“ susijusių grėsmių mažinimo priemonės išvardytos lentelėje C3.

Lentelė C3

Su „fiziniu duomenų praradimu“ susijusių grėsmių mažinimo priemonės

Lentelės A1 nuoroda	„Fizinio duomenų praradimo“ grėsmių mažinimo priemonės	Nuoroda:	Rizikos mažinimo priemonė
30.1	Žalą padaro trečioji šalis. Neskelbtini duomenys gali būti prarasti arba neteisėtai atskleisti dėl fizinės žalos eismo avarijų ar vagystės atveju	M24	Saugant asmens duomenis laikomasi duomenų vientisumo ir konfidencialumo apsaugos geriausios patirties. Saugumo kontrolės priemonių pavyzdį galima rasti ISO/SC27/WG5 medžiagoje
30.2	Praradimas dėl DRM (skaitmeninių teisių valdymo) konfliktų. Dėl DRM problemų gali būti ištrinti vartotojų duomenys		
30.3	Neskelbtini duomenys gali būti prarasti arba jų vientisumas gali būti pažeistas dėl IT komponentų nusidėvėjimo, galinčio sukelti kaskadinių problemų (pavyzdžiui, kai pakeičiami raktai)		