Europeiska unionens officiella tidning

SV
L-serien

2025/5

10.1.2025

Endast Uneces texter i original har bindande folkrättslig verkan. Denna föreskrifts status och ikraftträdandedag bör kontrolleras i den senaste versionen av Uneces statusdokument TRANS/WP.29/343, som finns på https://unece.org/status-1958-agreement-and-annexed-regulations

FN-föreskrift nr 155 – Enhetliga bestämmelser om godkännande av fordon med avseende på cybersäkerhet och ledningssystem för cybersäkerhet [2025/5]

Inbegripet all giltig text till och med:

Supplement 3 till den ursprungliga versionen av föreskriften – dag för ikraftträdande: 10 januari 2025

Detta dokument tillhandahålls endast i informationssyfte. De giltiga och rättsligt bindande texterna är följande:

— ECE/TRANS/WP.29/2020/79 (i dess ändrade lydelse enligt ECE/TRANS/WP.29/2020/94 och ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70

— ECE/TRANS/WP.29/2024/55

INNEHÅLL

Föreskrift

1. Tillämpningsområde
2. Definitioner
3. Ansökan om godkännande
4. Märkning
5. Godkännande
6. Intyg om överensstämmelse för ledningssystem för cybersäkerhet
7. Specifikationer
8. Ändring av fordonstyp och utökning av typgodkännande
9. Produktionsöverensstämmelse
10. Påföljder vid bristande produktionsöverensstämmelse
11. Slutgiltigt upphörande av produktionen
12. Namn på och adress till typgodkännandemyndigheter och de tekniska tjänster som ansvarar för att utföra godkännandeprovningar

Bilagor

1. Informationsdokument
2. Meddelande
3. Godkännandemärkets utformning
4. Mall för intyg om överensstämmelse för ledningssystem för cybersäkerhet
5. Förteckning över hot och motsvarande riskreducerande åtgärder

1. Tillämpningsområde

1.1 Denna föreskrift gäller med avseende på cybersäkerhet för fordon av kategorierna L, M, N och O, om de är utrustade med minst en elektronisk styrenhet.

1.2 Denna föreskrift påverkar inte andra FN-föreskrifter, regional eller nationell lagstiftning som styr behöriga parters tillgång till fordonet, dess data, funktioner och resurser samt villkoren för denna tillgång. Den påverkar inte heller tillämpningen av nationell och regional lagstiftning om integritet och skydd av fysiska personer när det gäller behandling av deras personuppgifter.

1.3 Denna föreskrift påverkar inte andra FN-föreskrifter, regional eller nationell lagstiftning som styr utvecklingen och installationen/integreringen av fysiska och digitala ersättningsdelar och komponenter med avseende på cybersäkerhet.

2. Definitioner

I denna föreskrift gäller följande definitioner:

2.1 *fordonstyp*: fordon som åtminstone i följande väsentliga avseenden inte skiljer sig från varandra:

a) Tillverkarens beteckning för fordonstypen.

b) Grundläggande aspekter av den elektriska/elektroniska konstruktionen och de externa gränssnitten med avseende på cybersäkerhet.

2.2 *cybersäkerhet*: hur vägfordon och deras funktioner skyddas mot cyberhot mot elektriska eller elektroniska komponenter.

2.3 *ledningssystem för cybersäkerhet*: systematisk, riskbaserad metod varigenom organisatoriska processer, ansvar och styrning fastställs för att hantera risker som är förenade med cyberhot mot fordon och skydda dem mot cyberattacker.

2.4 *system*: uppsättning komponenter och/eller undersystem som utför en eller flera funktioner.

2.5 *utvecklingsfas*: perioden innan en fordonstyp typgodkänns.

2.6 *produktionsfas*: längden av produktionen av en fordonstyp.

2.7 *efterproduktionsfas*: perioden då en fordonstyp inte längre produceras fram till slutet av livscykeln för alla fordon av fordonstypen. Fordon som överensstämmer med en viss fordonstyp kommer att vara i bruk under denna period, men inte längre produceras. Fasen tar slut när det inte längre finns några fordon i bruk av en viss fordonstyp.

2.8 *riskreducerande åtgärd*: åtgärd som minskar en risk.

2.9 *risk*: sannolikheten för att ett visst hot kommer att utnyttja ett fordons sårbarheter och därmed skada organisationen eller en enskild person.

2.10 *riskbedömning*: den övergripande processen av att hitta, erkänna och beskriva risker (riskidentifiering), förstå riskens karaktär och bedöma risknivån (riskanalys) samt jämföra resultaten av riskanalysen med riskkriterier för att avgöra om risken och/eller dess omfattning är acceptabel (riskvärdering).

2.11 *riskhantering*: samordnade insatser för att leda och styra en organisation i riskhänseende.

2.12 *hot*: potentiell orsak till en oönskad händelse som kan leda till skador på ett system, en organisation eller en person.

2.13 *sårbarhet*: svaghet hos en tillgång eller en riskreducerande åtgärd som kan utnyttjas genom ett eller flera hot.

3. Ansökan om godkännande

3.1 Ansökan om godkännande av en fordonstyp med avseende på cybersäkerhet ska lämnas in av fordonstillverkaren eller dess behöriga ombud.

3.2 Ansökan ska åtföljas av följande handlingar i tre exemplar och av följande uppgifter:

3.2.1 En beskrivning av fordonstypen med avseende på de uppgifter som anges i bilaga 1 till denna föreskrift.

3.2.2 Om det visar sig att information omfattas av immateriell äganderätt eller utgör tillverkarens eller tillverkarens leverantörers särskilda know-how ska tillverkaren eller leverantörerna tillhandahålla tillräcklig information för att de kontroller som avses i denna föreskrift ska kunna utföras korrekt. Sådan information ska behandlas konfidentiellt.

3.2.3 Intyget om överensstämmelse för ledningssystem för cybersäkerhet enligt punkt 6 i denna föreskrift.

3.3 Denna dokumentation ska bestå av följande två delar:

a) Det formella dokumentationspaketet för godkännandet, som innehåller det material som anges i bilaga 1 som ska lämnas till godkännandemyndigheten eller dess tekniska tjänst i samband med att ansökan om typgodkännande lämnas in. Godkännandemyndigheten eller dess tekniska tjänst kommer att använda detta dokumentationspaket som den grundläggande referensen för godkännandeförfarandet. Godkännandemyndigheten eller dess tekniska tjänst ska säkerställa att detta dokumentationspaket förblir tillgängligt i minst tio år räknat från den dag då produktionen av fordonstypen slutgiltigt upphörde.

b) Ytterligare material som är relevant för kraven i denna föreskrift får förvaras av tillverkaren och ska uppvisas i samband med typgodkännandet. Tillverkaren ska säkerställa att material som uppvisas i samband med typgodkännandet förblir tillgängligt under en period på minst tio år räknat från den dag då produktionen av fordonstypen slutgiltigt upphörde.

4. Märkning

4.1 Varje fordon som överensstämmer med en fordonstyp som godkänts enligt denna föreskrift ska, på en väl synlig och lättillgänglig plats som anges i godkännandeformuläret, vara märkt med ett internationellt godkännandemärke som består av följande.

4.1.1 En cirkel som omger bokstaven E, följd av det särskiljande numret för det land som beviljat godkännandet.

4.1.2 Numret på denna föreskrift följt av bokstaven R, ett bindestreck och godkännandenumret till höger om den cirkel som beskrivs i punkt 4.1.1.

4.2 Om fordonet överensstämmer med en fordonstyp som godkänts enligt en eller flera andra föreskrifter som är fogade till överenskommelsen, i det land som beviljat godkännande enligt den här föreskriften, behöver den symbol som föreskrivs i punkt 4.1.1 ovan inte upprepas. I sådana fall ska såväl föreskrifternas nummer som typgodkännandenummer och tilläggssymbolerna för alla de föreskrifter enligt vilka typgodkännande har beviljats i det land som beviljat typgodkännande enligt den här föreskriften placeras i lodräta kolumner till höger om symbolen som föreskrivs i punkt 4.1.1 ovan.

4.3 Typgodkännandemärket ska vara lätt läsbart och outplånligt.

4.4 Typgodkännandemärket ska placeras på eller nära den fordonsskylt som anbringats av tillverkaren.

4.5 I bilaga 3 till denna föreskrift finns exempel på typgodkännandemärkets utformning.

5. Godkännande

5.1 Godkännandemyndigheter ska endast bevilja typgodkännande med avseende på cybersäkerhet för de fordonstyper som uppfyller kraven i denna föreskrift.

5.1.1 Godkännandemyndigheten eller den tekniska tjänsten ska genom dokumentkontroller kontrollera att fordonstillverkaren har vidtagit de nödvändiga åtgärderna för fordonstypen för att

a) samla in och kontrollera de uppgifter som krävs enligt denna föreskrift genom leveranskedjan för att visa att leverantörsrelaterade risker upptäcks och hanteras,

b) dokumentera riskbedömningen (som görs under utvecklingsfasen eller i efterhand), provningsresultat och riskreducerande åtgärder som tillämpats på fordonstypen, inbegripet konstruktionsinformation som stöder riskbedömningen,

c) vidta lämpliga cybersäkerhetsåtgärder vid konstruktionen av fordonstypen,

d) upptäcka och svara på eventuella cyberattacker,

e) registrera data för att stödja upptäckten av cyberattacker och skapa kapacitet för it-forensik för att möjliggöra analys av misslyckade eller framgångsrika cyberattacker.

5.1.2 Godkännandemyndigheten eller den tekniska tjänsten ska genom att prova ett fordon av fordonstypen kontrollera att fordonstillverkaren har vidtagit de cybersäkerhetsåtgärder som han eller hon har dokumenterat. Godkännandemyndigheten eller den tekniska tjänsten ska, själv eller i samarbete med fordonstillverkaren, utföra provningar genom provtagning. Provtagning ska inriktas på, men inte begränsas till, risker som bedöms som höga under riskbedömningen.

5.1.3 Godkännandemyndigheten eller den tekniska tjänsten ska vägra att bevilja typgodkännandet med avseende på cybersäkerhet om fordonstillverkaren inte har uppfyllt ett eller flera av de krav som avses i punkt 7.3, särskilt följande:

a) Fordonstillverkaren gjorde inte den uttömmande riskbedömning som avses i punkt 7.3.3, inbegripet fall där tillverkaren inte beaktade alla risker med koppling till de hot som avses i del A i bilaga 5.

b) Fordonstillverkaren skyddade inte fordonstypen mot de risker som identifierades i fordonstillverkarens riskbedömning eller vidtog proportionella riskreducerande åtgärder enligt punkt 7.

c) Fordonstillverkaren vidtog inte lämpliga och proportionella åtgärder för att säkerställa särskilda utrymmen i fordonstypen (om detta föreskrivs) för förvaring och körning av programvara, tjänster, applikationer eller data på eftermarknaden.

d) Fordonstillverkaren utförde inte, före godkännandet, lämplig och tillräcklig provning för att kontrollera effektiviteten i de säkerhetsåtgärder som vidtogs.

5.1.4 Den godkännandemyndighet som utför bedömningen ska även vägra att bevilja typgodkännande med avseende på cybersäkerhet när godkännandemyndigheten eller den tekniska tjänsten inte har erhållit tillräcklig information från fordonstillverkaren för att bedöma fordonstypens cybersäkerhet.

5.2 Ett meddelande om beviljat, utökat eller ej beviljat godkännande av en fordonstyp enligt denna föreskrift ska lämnas till de parter i 1958 års överenskommelse som tillämpar denna föreskrift med hjälp av ett formulär som överensstämmer med mallen i bilaga 2 till denna föreskrift.

5.3 Godkännandemyndigheter får inte bevilja typgodkännande utan att kontrollera att tillverkaren har infört tillfredsställande rutiner och förfaranden för att på ett korrekt sätt hantera de cybersäkerhetsaspekter som omfattas av denna föreskrift.

5.3.1 Godkännandemyndigheten och dess tekniska tjänster ska utöver de kriterier som fastställs i bilaga 2 till 1958 års överenskommelse säkerställa att tillverkaren har

a) kompetent personal med lämplig kompetens inom cybersäkerhet och särskilda kunskaper om riskbedömning av fordon ([1]),

b) infört förfaranden för enhetlig utvärdering enligt denna föreskrift.

5.3.2 Varje part i överenskommelsen som tillämpar denna föreskrift ska genom sin godkännandemyndighet meddela och informera andra godkännandemyndigheter hos de parter i överenskommelsen som tillämpar denna FN-föreskrift om den metod och de kriterier som den anmälande myndigheten använder som underlag för att bedöma lämpligheten av de åtgärder som vidtas i enlighet med denna föreskrift, särskilt punkterna 5.1, 7.2 och 7.3

Dessa uppgifter ska delas a) endast innan ett godkännande beviljas för första gången enligt denna föreskrift och b) varje gång som metoden eller kriterierna för bedömningen uppdateras.

Dessa uppgifter är avsedda att delas för insamling och analys av bästa praxis och för att säkerställa att alla godkännandemyndigheter som tillämpar denna föreskrift gör det på ett enhetligt sätt.

5.3.3 De uppgifter som avses i punkt 5.3.2 ska laddas upp på engelska till den säkra onlinedatabasen DETA ([2]), som upprättats av FN:s ekonomiska kommission för Europa, i god dit och senast 14 dagar innan ett godkännande beviljas för första gången enligt metoderna och kriterierna för den aktuella bedömningen. Uppgifterna ska vara tillräckliga för att förstå vilka lägsta prestandanivåer som godkännandemyndigheten antagit för varje särskilt krav som avses i punkt 5.3.2 samt de processer och åtgärder som myndigheten tillämpar för att kontrollera att dessa lägsta prestandanivåer är uppfyllda ([3]).

5.3.4 Godkännandemyndigheter som erhåller de uppgifter som avses i punkt 5.3.2 kan lämna kommentarer till den anmälande godkännandemyndigheten genom att ladda upp dem till DETA senast 14 dagar efter dagen för anmälan.

5.3.5 Om den beviljande godkännandemyndigheten inte kan ta hänsyn till de kommentarer som den fått enligt punkt 5.3.4 ska de godkännandemyndigheter som skickat in kommentarer och den beviljande godkännandemyndigheten begära ytterligare förtydligande enligt bilaga 6 till 1958 års överenskommelse. Den relevanta arbetsgruppen ([4]) under världsforumet för harmonisering av fordonsföreskrifter (WP.29) för denna föreskrift ska komma överens om en gemensam tolkning av metoderna och kriterierna för bedömningen ([5]). Denna gemensamma tolkning ska tillämpas, och alla godkännandemyndigheter ska följaktligen utfärda typgodkännanden enligt denna föreskrift.

([1]) T.ex. ISO 26262-2018, ISO/PAS 21448 eller ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Riktlinjer för de detaljerade uppgifter (t.ex. metod, kriterier, prestandanivå) som ska laddas upp och formatet ska anges i tolkningsdokumentet, som håller på att utarbetas av arbetsgruppen för cybersäkerhet och trådlösa frågor för GRVA:s sjunde möte.
([4]) Arbetsgruppen för automatiska/autonoma och uppkopplade fordon (GRVA).
([5]) Denna tolkning ska framgå i det tolkningsdokument som avses i fotnoten till punkt 5.3.3.

5.3.6 Varje godkännandemyndighet som beviljar ett typgodkännande enligt denna föreskrift ska meddela andra godkännandemyndigheter om det beviljade godkännandet. Godkännandemyndigheten ska ladda upp typgodkännandet och de kompletterande handlingarna på engelska till DETA ([6]) inom 14 dagar från dagen för beviljandet av godkännandet.

5.3.7 Parterna i överenskommelsen får granska de godkännanden som beviljats utifrån den information som laddats upp enligt punkt 5.3.6. Om det råder delade meningar mellan parterna i överenskommelsen ska detta lösas enligt artikel 10 och bilaga 6 till 1958 års överenskommelse. Parterna i överenskommelsen ska även informera den relevanta arbetsgruppen under världsforumet för harmonisering av fordonsföreskrifter (WP.29) om de olika tolkningarna i den mening som avses i bilaga 6 till 1958 års överenskommelse. Den relevanta arbetsgruppen ska stödja lösningen av de delade meningarna och kan vid behov samråda om detta med WP.29.

5.4 Vid tillämpningen av punkt 7.2 i denna föreskrift ska tillverkaren säkerställa att de cybersäkerhetsaspekter som omfattas av denna föreskrift genomförs.

6. Intyg om överensstämmelse för ledningssystem för cybersäkerhet

6.1 Parterna i överenskommelsen ska utse en godkännandemyndighet som ska utföra bedömningen av tillverkaren och utfärda ett intyg om överensstämmelse för ledningssystem för cybersäkerhet.

6.2 En ansökan om ett intyg om överensstämmelse för ledningssystem för cybersäkerhet ska lämnas in av fordonstillverkaren eller dess behöriga ombud.

6.3 Ansökan ska åtföljas av nedanstående handlingar i tre exemplar och av följande uppgifter:

6.3.1 Handlingar som beskriver ledningssystemet för cybersäkerhet.

6.3.2 En undertecknad deklaration på grundval av mallen enligt tillägg 1 till bilaga 1.

6.4 I samband med bedömningen ska tillverkaren intyga att han eller hon använder mallen enligt tillägg 1 till bilaga 1 och övertyga godkännandemyndigheten eller dess tekniska tjänst om att de förfaranden som krävs för att uppfylla alla cybersäkerhetskrav enligt denna föreskrift har införts.

6.5 När denna bedömning har slutförts med ett tillfredsställande resultat och med mottagande av en undertecknad deklaration från tillverkaren enligt den mall som anges i tillägg 1 till bilaga 1 ska ett intyg som kallas intyg om överensstämmelse för ledningssystem för cybersäkerhet (nedan kallat intyg om överensstämmelse), som beskrivs i bilaga 4 till denna föreskrift, utfärdas till tillverkaren.

6.6 Godkännandemyndigheten eller dess tekniska tjänst ska använda den mall som anges i bilaga 4 till denna föreskrift för intyget om överensstämmelse.

6.7 Intyget om överensstämmelse ska vara giltigt högst tre år från det att det utfärdas, såvida det inte återkallas.

6.8 Den godkännandemyndighet som har utfärdat intyget om överensstämmelse får när som helst kontrollera att kraven för det fortfarande är uppfyllda. Godkännandemyndigheten ska återkalla intyget om överenstämmelse om kraven enligt denna föreskrift inte längre är uppfyllda.

([6]) Ytterligare information om minimikraven för dokumentationspaketet kommer att tas fram av GRVA vid dess sjunde möte.

6.9 Tillverkaren ska underrätta godkännandemyndigheten eller dess tekniska tjänst om förändringar som påverkar relevansen av intyget om överensstämmelse. Efter samråd med tillverkaren ska godkännandemyndigheten eller dess tekniska tjänst besluta om nya kontroller är nödvändiga.

6.10 Tillverkaren ska i god tid, så att godkännandemyndigheten har möjlighet att slutföra sin bedömning innan intyget om överensstämmelse löper ut, ansöka om ett nytt eller utökat intyg om överensstämmelse. Godkännandemyndigheten ska, om bedömningen är positiv, utfärda ett nytt intyg om överensstämmelse eller förlänga dess giltighet med ytterligare tre år. Godkännandemyndigheten ska kontrollera att ledningssystemet för cybersäkerhet fortfarande uppfyller kraven i denna föreskrift. Godkännandemyndigheten ska utfärda ett nytt intyg när myndigheten eller dess tekniska tjänst har fått kännedom om förändringar och förändringarna på nytt har bedömts som positiva.

6.11 När tillverkarens intyg om överensstämmelse löper ut eller återkallas ska detta, med hänsyn till de fordonstyper för vilka det berörda ledningssystemet för cybersäkerhet var relevant, betraktas som en ändring av godkännandet enligt punkt 8, vilket kan innebära att godkännandet återkallas om villkoren för beviljande av godkännande inte längre är uppfyllda.

7. Specifikationer

7.1 Allmänna specifikationer

7.1.1 Kraven i denna föreskrift ska inte begränsa bestämmelser eller krav i andra FN-föreskrifter.

7.2 Krav på ledningssystemet för cybersäkerhet

7.2.1 Vid bedömningen ska godkännandemyndigheten eller dess tekniska tjänst kontrollera att fordonstillverkaren har inrättat ett ledningssystem för cybersäkerhet och säkerställa att det uppfyller kraven i denna föreskrift.

7.2.2 Ledningssystemet för cybersäkerhet ska omfatta följande aspekter:

7.2.2.1 Fordonstillverkaren ska för en godkännandemyndighet eller teknisk tjänst visa att ledningssystemet för cybersäkerhet tillämpas i följande faser:

a) Utvecklingsfasen.

b) Produktionsfasen.

c) Efterproduktionsfasen.

7.2.2.2 Fordonstillverkaren ska visa att de förfaranden som används inom ledningssystemet för cybersäkerhet säkerställer att tillräcklig hänsyn tas till säkerhet, inbegripet de risker och riskreducerande åtgärder som anges i bilaga 5. Detta ska innefatta följande:

a) De förfaranden som används inom tillverkarens organisation för att hantera cybersäkerhet.

b) De förfaranden som används för att identifiera risker för fordonstyper. Inom dessa förfaranden ska hoten i del A i bilaga 5 och andra relevanta hot beaktas.

c) De förfaranden som används för bedömningen, klassificeringen och hanteringen av de risker som identifieras.

d) De förfaranden som införts för att kontrollera att de risker som identifieras hanteras på ett lämpligt sätt.

e) De förfaranden som används för att prova en fordonstyps cybersäkerhet.

f) De förfaranden som används för att säkerställa att riskbedömningen uppdateras.

g) De förfaranden som används för att övervaka, upptäcka och svara på cyberattacker, cyberhot och sårbarheter hos fordonstyper och de förfaranden som används för att bedöma huruvida de cybersäkerhetsåtgärder som vidtagits fortfarande är effektiva mot bakgrund av nya cyberhot och sårbarheter som identifierats.

h) De förfaranden som används för att tillhandahålla relevanta data för att stödja analys av misslyckade eller framgångsrika cyberattacker.

7.2.2.3 Fordonstillverkaren ska visa att de förfaranden som används inom ledningssystemet för cybersäkerhet kommer att säkerställa att cyberhot och sårbarheter som kräver åtgärder från fordonstillverkaren minskas inom rimlig tid, utifrån den klassificering som avses i punkt 7.2.2.2 c och 7.2.2.2 g.

7.2.2.4 Fordonstillverkaren ska visa att de förfaranden som används inom ledningssystemet för cybersäkerhet kommer att säkerställa att den övervakning som avses i punkt 7.2.2.2 g sker löpande. Detta ska

a) inbegripa fordon efter den första registreringen i övervakningen,

b) omfatta kapacitet att analysera och upptäcka cyberhot, sårbarheter och cyberattacker från fordonsdata och fordonsloggar. Denna kapacitet ska överensstämma med punkt 1.3 och bilägarnas eller förarnas rätt till integritet, särskilt samtycke.

7.2.2.5 Fordonstillverkaren är skyldig att visa hur ledningssystemet för cybersäkerhet kommer att hantera beroendeförhållanden som kan finnas med kontrakterade leverantörer, tjänsteleverantörer eller tillverkares underorganisationer när det gäller kraven i punkt 7.2.2.2.

7.3 Krav för fordonstyper

7.3.1 Tillverkaren ska ha ett giltigt intyg om överensstämmelse för det ledningssystem för cybersäkerhet som är relevant för den fordonstyp som ska godkännas. För typgodkännanden av fordon av kategorierna M, N och O som utfärdades för första gången före den 1 juli 2024 och för typgodkännanden av fordon av kategori L som utfärdades för första gången före den 1 juli 2029 och för varje utökning av sådana typgodkännanden ska fordonstillverkaren dock, om det kan påvisas att fordonstypen inte kunde utvecklas i överensstämmelse med ledningssystemet för cybersäkerhet, visa att cybersäkerhet beaktades i tillräcklig utsträckning under utvecklingsfasen av fordonstypen i fråga.

7.3.2 Fordonstillverkaren ska, för den fordonstyp som ska godkännas, identifiera och hantera risker kopplade till leverantören.

7.3.3 Fordonstillverkaren ska identifiera de kritiska delarna av fordonstypen och göra en uttömmande riskbedömning av fordonstypen samt på ett lämpligt sätt hantera de risker som identifieras. Vid riskbedömningen ska hänsyn tas till de enskilda delarna av fordonstypen och deras samverkan. Vidare ska hänsyn tas till samverkan med eventuella externa system. När riskerna bedöms ska fordonstillverkaren beakta riskerna kopplade till alla hot som beskrivs i del A i bilaga 5 samt andra relevanta risker.

7.3.4 Fordonstillverkaren ska skydda fordonstypen mot de risker som identifieras vid fordonstillverkarens riskbedömning. Proportionella riskreducerande åtgärder ska vidtas för att skydda fordonstypen. De riskreducerande åtgärder som vidtas ska innefatta alla de riskreducerande åtgärder som beskrivs i delarna B och C i bilaga 5 och som är relevanta för de risker som identifieras. Om en riskreducerande åtgärd som beskrivs i del B eller C i bilaga 5 emellertid inte är relevant eller tillräcklig för den risk som identifieras ska fordonstillverkaren säkerställa att en annan lämplig riskreducerande åtgärd vidtas.

För typgodkännanden av fordon av kategorierna M, N och O som utfärdades för första gången före den 1 juli 2024 och för typgodkännanden av fordon av kategori L som utfärdades för första gången före den 1 juli 2029 och för varje utökning av sådana typgodkännanden ska fordonstillverkaren särskilt säkerställa att en annan lämplig riskreducerande åtgärd vidtas om någon av de riskreducerande åtgärder som avses i del B eller C i bilaga 5 inte är tekniskt genomförbar. Tillverkaren ska överlämna bedömningen av den tekniska genomförbarheten till godkännandemyndigheten.

7.3.5 Fordonstillverkaren ska vidta lämpliga och proportionella åtgärder för att säkerställa särskilda utrymmen i fordonstypen (om detta föreskrivs) för förvaring och körning av programvara, tjänster, applikationer eller data på eftermarknaden.

7.3.6 Fordonstillverkaren ska, före typgodkännandet, utföra lämplig och tillräcklig provning för att kontrollera effektiviteten i de säkerhetsåtgärder som vidtagits.

7.3.7 Fordonstillverkaren ska vidta åtgärder för fordonstypen för att

a) upptäcka och förhindra cyberattacker mot fordon av fordonstypen,

b) stödja fordonstillverkarens övervakningskapacitet när det gäller att upptäcka hot, sårbarheter och cyberattacker som är relevanta för fordonstypen,

c) skapa kapacitet för it-forensik för att möjliggöra analys av misslyckade eller framgångsrika cyberattacker.

7.3.8 Kryptografiska moduler som används vid tillämpningen av denna föreskrift ska vara förenliga med samförstånds-baserade standarder. Om de kryptografiska moduler som används inte är förenliga med de samförståndsbaserade standarderna ska fordonstillverkaren motivera användningen av dem.

7.4 Rapporteringsbestämmelser

7.4.1 Fordonstillverkaren ska minst en gång om året, eller oftare om så är relevant, rapportera om resultatet av sin övervakningsverksamhet, enligt definitionen i punkt 7.2.2.2 g, till godkännandemyndigheten eller den tekniska tjänsten. Rapporteringen ska omfatta relevant information om nya cyberattacker. Fordonstillverkaren ska även rapportera och bekräfta för godkännandemyndigheten eller den tekniska tjänsten att de cybersäkerhetsåtgärder som har vidtagits för tillverkarens fordonstyper fortfarande är effektiva och om ytterligare åtgärder vidtas.

7.4.2 Godkännandemyndigheten eller den tekniska tjänsten ska kontrollera den information som lämnas och vid behov kräva att fordonstillverkaren åtgärdar eventuell ineffektivitet som upptäcks.

Om rapporteringen eller åtgärderna är otillräckliga kan godkännandemyndigheten besluta att återkalla intyget om överensstämmelse i enlighet med punkt 6.8.

8. Ändring av fordonstyp och utökning av typgodkännande

8.1 Alla ändringar av fordonstypen som påverkar dess tekniska prestanda med avseende på cybersäkerhet och/eller dokumentation som krävs enligt denna föreskrift ska meddelas den godkännandemyndighet som godkände fordonstypen. Godkännandemyndigheten kan då antingen

8.1.1 konstatera att de ändringar som gjorts fortfarande uppfyller kraven och överensstämmer med dokumentationen för det befintliga typgodkännandet, eller

8.1.2 inleda en nödvändig kompletterande bedömning enligt punkt 5 och i förekommande fall kräva ytterligare en provningsrapport från den tekniska tjänst som ansvarar för att utföra provningarna.

8.1.3 Beviljat, utökat eller ej beviljat godkännande, med en beskrivning av ändringarna, ska meddelas med hjälp av ett meddelandeformulär som överensstämmer med mallen i bilaga 2 till denna föreskrift. Den godkännandemyndighet som beviljar utökning av typgodkännande ska tilldela varje sådan utökning ett serienummer och underrätta övriga parter i 1958 års överenskommelse som tillämpar denna föreskrift om detta med hjälp av ett meddelandeformulär som överensstämmer med mallen i bilaga 2 till denna föreskrift.

9. Produktionsöverensstämmelse

9.1 Förfarandena för produktionsöverensstämmelse ska motsvara de som anges i bilaga 1 till 1958 års överenskommelse (E/ECE/TRANS/505/Rev.3) med följande krav:

9.1.1 Innehavaren av godkännandet ska säkerställa att resultaten från provningarna avseende produktionsöverensstämmelse dokumenteras och att de bifogade dokumenten finns tillgängliga under en tid som fastställs genom överenskommelse med godkännandemyndigheten eller dess tekniska tjänst. Denna tid ska inte vara längre än tio år räknat från den tidpunkt då produktionen slutgiltigt upphörde.

9.1.2 Den godkännandemyndighet som beviljat typgodkännandet får när som helst granska de metoder för kontroll av överensstämmelse som tillämpas vid varje produktionsanläggning. Sådan granskning ska normalt ske en gång vart tredje år.

10. Påföljder vid bristande produktionsöverensstämmelse

10.1 Godkännande som, enligt denna föreskrift, beviljats med avseende på en fordonstyp kan återkallas om kraven i denna föreskrift inte uppfylls eller om stickprov av fordon inte överensstämmer med kraven i denna föreskrift.

10.2 Om en godkännandemyndighet återkallar ett godkännande som den tidigare har beviljat ska den genast meddela övriga parter i överenskommelsen som tillämpar denna föreskrift detta med hjälp av ett meddelandeformulär som överensstämmer med mallen i bilaga 2 till denna föreskrift.

11. Slutgiltigt upphörande av produktionen

11.1 Om innehavaren av godkännandet helt upphör med produktionen av en fordonstyp som godkänts enligt denna föreskrift, ska denne underrätta den myndighet som beviljat godkännandet. När myndigheten har mottagit det aktuella meddelandet ska den underrätta övriga parter i överenskommelsen som tillämpar denna föreskrift, med hjälp av en kopia av godkännandeformuläret, som i slutet ska vara försett med en underskriven och daterad notering med lydelsen ”SLUTGILTIGT UPPHÖRANDE AV PRODUKTIONEN” skriven med versaler.

12. Namn på och adress till typgodkännandemyndigheter och de tekniska tjänster som ansvarar för att utföra godkännandeprovningar

12.1 De parter i överenskommelsen som tillämpar denna föreskrift ska meddela Förenta nationernas sekretariat namn på och adress till de tekniska tjänster som ansvarar för att utföra godkännandeprovningarna och de typgodkännandemyndigheter som beviljar godkännande och till vilka formulär om beviljat, utökat, ej beviljat eller återkallat godkännande som utfärdats i andra länder ska sändas.

BILAGA 1

Informationsdokument

Följande information ska, om den är tillämplig, lämnas in i tre exemplar tillsammans med en innehållsförteckning. Alla ritningar ska lämnas i lämplig skala och med tillräcklig detaljgrad i formatet A4 eller vikt till formatet A4. Eventuella fotografier ska vara tillräckligt detaljerade.

1. Fabrikat (tillverkarens företagsnamn): .....

2. Typ och handelsbeteckning: .....

3. Typidentifikationsmärkning, om sådan finns på fordonet: .....

4. Märkningens placering:.....

5. Fordonskategorier:.....

6. Namn på och adress till tillverkarnas ombud: .....

7. Namn på och adresser till monteringsanläggningar:.....

8. Fotografier eller ritningar av ett representativt fordon: .....

9. Cybersäkerhet

9.1 Allmänna uppgifter om fordonstypens konstruktion, inbegripet följande:

a) De fordonssystem som är relevanta för fordonstypens cybersäkerhet.

b) De delar av dessa system som är relevanta för cybersäkerhet.

c) Dessa systems samverkan med andra system inom fordonstypen och externa gränssnitt.

9.2 Systembild på fordonstypen:

9.3 Numret på intyget om överensstämmelse för ledningssystem för cybersäkerhet:.....

9.4 Handlingar för den fordonstyp som ska godkännas med uppgift om resultatet av riskbedömningen och de risker som identifierats: .....

9.5 Handlingar för den fordonstyp som ska godkännas med uppgift om de riskreducerande åtgärder som vidtagits för de angivna systemen, eller för fordonstypen, och hur de minskar de fastställda riskerna: .....

9.6 Handlingar för den fordonstyp som ska godkännas med uppgift om skyddet av särskilda utrymmen för programvara, tjänster, appar eller data på eftermarknaden:.....

9.7 Handlingar för den fordonstyp som ska godkännas som beskriver vilka provningar som har gjorts för att kontrollera fordonstypens och dess systems cybersäkerhet och resultatet av dessa provningar: .....

9.8 Beskrivning av hur hänsyn tagits till leveranskedjan med avseende på cybersäkerhet:.....

Bilaga 1 – Tillägg 1

Mall för tillverkarens försäkran om överensstämmelse för ledningssystem för cybersäkerhet

Tillverkarens försäkran om överensstämmelse med kraven för ledningssystem för cybersäkerhet

Tillverkarens namn:……

Tillverkarens adress: ……

…… (*tillverkarens namn*)

intygar att de förfaranden som krävs för att uppfylla kraven för ledningssystem för cybersäkerhet enligt punkt 7.2 i FN-föreskrift nr 155 har inrättats och kommer att upprätthållas.

Utfärdat i …… (ort)

Datum:……

Undertecknarens namn: ……

Undertecknarens befattning:……

(Stämpel och underskrift från tillverkarens ombud)

BILAGA 2

Meddelande

(maximiformat: A4 [210 × 297 mm])



Utfärdat av: Myndighetens namn:
……
……
……

om (2) beviljat godkännande
utökat godkännande
återkallat godkännande med verkan från och med dd/mm/åååå
ej beviljat typgodkännande
slutgiltigt upphörande av produktionen

av en fordonstyp enligt FN-föreskrift nr 155

Godkännande nr: ……

Utökning nr: ……

Skäl till utökningen: ……

1. Fabrikat (tillverkarens företagsnamn): ……

2. Typ och handelsbeteckning: ……

3. Typidentifikationsmärkning, om sådan finns på fordonet: ……

3,1. Märkningens placering: ……

4. Fordonskategorier: ……

5. Namn på och adress till tillverkarnas ombud: ……

6. Namn på och adress till monteringsanläggningar: ……

7. Nummer på intyget om överensstämmelse för ledningssystem för cybersäkerhet: ……

8. Teknisk tjänst som ansvarar för att utföra provningarna: ……

9. Provningsrapportens datum: ……

10. Provningsrapportens nummer: ……

11. Anmärkningar: (om tillämpligt) ……

12. Ort: ……

(1) Särskiljande nummer för det land som beviljat/utökat/ej beviljat/återkallat godkännandet (se bestämmelserna om godkännande i föreskriften).
(2) Stryk det som inte är tillämpligt.

13. Datum: ……

14. Underskrift:……

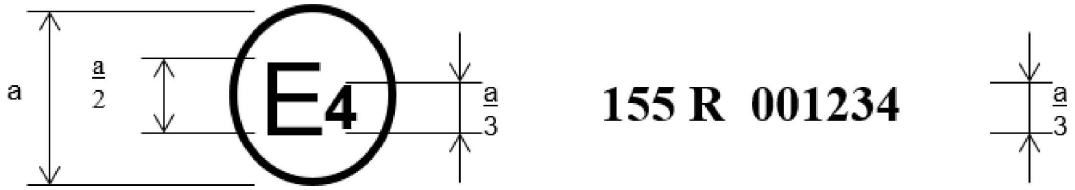
15. Indexet till det informationspaket som har lämnats in till godkännandemyndigheten och som kan fås på begäran bifogas:

BILAGA 3

Godkännandemärkets utformning

MALL A

(se punkt 4.2 i denna föreskrift)



a = 8 mm min.

Ovanstående godkännandemärke på ett fordon visar att fordonstypen har godkänts i Nederländerna (E4) enligt föreskrift nr 155 med godkännandenumret 001234. De två första siffrorna i godkännandenumret anger att godkännandet beviljats enligt kraven i denna föreskrift i dess ursprungliga lydelse (00).

BILAGA 4

MALL FÖR INTYG OM ÖVERENSSTÄMMELSE FÖR LEDNINGSSYSTEM FÖR CYBERSÄKERHET

Intyg om överensstämmelse för ledningssystem för cybersäkerhet

med FN-föreskrift nr 155

Intygsnummer [*referensnummer*]

[*… godkännandemyndigheten*]

intygar att

Tillverkare: ……

Tillverkarens adress: ……

följer bestämmelserna i punkt 7.2 i föreskrift nr 155.

Kontroller har utförts på: ……

av (namn på och adress till godkännandemyndigheten eller den tekniska tjänsten): ……

Rapportens nummer: ……

Detta intyg är giltigt till och med den [……*.datum*]

Utfärdat i [……*ort*]

den [……*.datum*]

[…… *underskrift*]

Bilagor: Tillverkarens beskrivning av ledningssystemet för cybersäkerhet.

BILAGA 5

Förteckning över hot och motsvarande riskreducerande åtgärder

1. Denna bilaga består av tre delar. I del A beskrivs grunden för hot, sårbarheter och attackmetoder. I del B beskrivs åtgärder för att minska hoten avsedda för fordonstyper. I del C beskrivs åtgärder för att minska hoten avsedda för områden utanför fordon, t.ex. backends.

2. Del A, del B och del C ska beaktas vid riskbedömningen och när fordonstillverkarna vidtar riskreducerande åtgärder.

3. Den höga sårbarhetsnivån och motsvarande exempel har indexerats i del A. Det hänvisas till samma indexering i tabellerna i delarna B och C för att koppla varje attack/sårbarhet till en förteckning över motsvarande riskreducerande åtgärder.

4. I hotanalysen ska hänsyn även tas till de potentiella effekterna av attacker. Dessa kan bidra till bedömningen av hur allvarlig en risk är och till identifieringen av ytterligare risker. Potentiella effekter av en attack kan till exempel vara

   a) att säker drift av fordonet påverkas,

   b) att fordonsfunktioner slutar fungera,

   c) att programvara ändras och prestandan förändras,

   d) att programvara ändras men det inte får några operativa effekter,

   e) brott mot dataintegriteten,

   f) brott mot datasekretessen,

   g) förlust av dataåtkomst,

   h) något annat, inbegripet brottslighet.

DEL A.

Sårbarhet eller attackmetod relaterad till hoten

Övergripande beskrivningar av hot och tillhörande sårbarhet eller attackmetod anges i tabell A1.

Tabell A1

Förteckning över sårbarhet eller attackmetod relaterad till hoten

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
4.3.1 Hot med avseende på backendservrar kopplade till fordon i området	1.	Backendservrar används som ett sätt att attackera ett fordon eller hämta data	1.1	Personals missbruk av privilegier (angrepp inifrån)
			1.2	Obehörig internetåtkomst till servern (som möjliggörs genom exempelvis bakdörrar, sårbarheter i opatchad programvara, SQL-attacker eller på andra sätt)
			1.3	Obehörig fysisk tillgång till servern (som genomförs med exempelvis usb-minnen eller andra medier som ansluts till servern)
	2.	Tjänster från backendservern störs och påverkar ett fordons drift	2.1	Attack mot backendservern som gör att den slutar fungera, t.ex. hindrar den att kommunicera med fordon och tillhandahålla tjänster som fordonen är beroende av

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
	3.	Fordonsrelaterade data som lagras på backendservrar försvinner eller skadas (”dataintrång”)	3.1	Personals missbruk av privilegier (angrepp inifrån)
			3.2	Förlust av information i molnet. Känsliga data kan förloras till följd av attacker eller olyckor när data lagras av tredjepartsleverantör av molntjänster
			3.3	Obehörig internetåtkomst till servern (som möjliggörs genom exempelvis bakdörrar, sårbarheter i opatchad programvara, SQL-attacker eller på andra sätt)
			3.4	Obehörig fysisk tillgång till servern (som genomförs med exempelvis usb-minnen eller andra medier som ansluts till servern)
			3.5	Dataintrång genom oavsiktlig datadelning (t.ex. administratörsfel)
4.3.2 Hot mot fordon med avseende på deras kommunikationskanaler	4.	Manipulering av meddelanden eller data som mottas av fordonet	4.1	Manipulering av meddelanden genom att utge sig för att vara någon annan (t.ex. V2X-lägesbild eller meddelanden för samordning av körning eller GNSS-meddelanden)
			4.2	Sybil-attack (för att manipulera andra fordon att tro att det är många fordon på vägen)
	5.	Kommunikationskanaler används för att utföra obehörig manipulation, radering eller andra ändringar av kod/data i fordon	5.1	Kommunikationskanaler som tillåter kodinjektion, t.ex. injektion av en manipulerad binärfil i kommunikationsflödet
			5.2	Kommunikationskanaler som tillåter manipulation av data/kod i fordon
			5.3	Kommunikationskanaler som tillåter överskrivning av data/kod i fordon
			5.4	Kommunikationskanaler som tillåter radering av data/kod i fordon
			5.5	Kommunikationskanaler som tillåter införande av data/kod i fordonet (skriver datakod)
	6.	Kommunikationskanaler tillåter mottagning av osäkra/otillförlitliga meddelanden eller är sårbara för sessionskapning/omtagningsattacker	6.1	Information tas emot från en otillförlitlig eller osäker källa
			6.2	Man-i-mitten-attack/sessionskapning
			6.3	Omtagningsattack, t.ex. en attack mot en nätport som gör att angriparen kan nedgradera en motorstyrenhets programvara eller nätportens fasta programvara
	7.	Information kan enkelt lämnas ut, t.ex. genom att någon tjuvlyssnar på kommunikation eller genom att tillåta obehörig tillgång till känsliga filer eller mappar	7.1	Avlyssning av information/störande strålning/övervakning av kommunikation
			7.2	Obehörig tillgång till filer eller data

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
	8.	Överbelastningsattacker via kommunikationskanaler för att störa fordonsfunktioner	8.1	En stor mängd skräpdata skickas till ett fordons informationssystem så att det inte kan tillhandahålla tjänster på normalt sätt
			8.2	Attack i form av ett svart hål genom att angriparen blockerar meddelanden mellan fordon för att störa kommunikationen mellan dem
	9.	En obehörig användare får åtkomsträtt till fordonssystem	9.1	En obehörig användare får åtkomsträttigheter, t.ex. rootåtkomst
	10.	Virus som är inbyggda i kommunikationsmedier kan infektera fordonssystem	10.1	Virus som är inbyggda i kommunikationsmedier infekterar fordonssystem
	11.	Meddelanden som mottas av fordonet (t.ex. X2V-meddelanden eller diagnosmeddelanden), eller överförs i fordonet, innehåller skadligt innehåll	11.1	Skadliga interna meddelanden (t.ex. CAN-meddelanden)
			11.2	Skadliga V2X-meddelanden, t.ex. mellan infrastruktur och fordon eller mellan två fordon (t.ex. CAM, DENM)
			11.3	Skadliga diagnosmeddelanden
			11.4	Skadliga proprietära meddelanden (t.ex. meddelanden som normalt skickas från OEM-företag eller leverantören av komponenten/systemet/funktionen)
4.3.3 Hot mot fordon med avseende på deras uppdaterings-processer	12.	Missbruk eller röjande av uppdateringsprocesser	12.1	Röjande av trådlösa processer för programvaruuppdatering. Detta inbegriper att fabricera systemets uppdateringsprogram eller fasta programvara
			12.2	Röjande av lokala/fysiska processer för programvaruuppdatering. Detta inbegriper att fabricera systemets uppdateringsprogram eller fasta programvara
			12.3	Programvara som manipuleras före uppdateringsprocessen (och därmed skadas), även om uppdateringsprocessen är intakt
			12.4	Röjande av programvaruleverantörens krypteringsnycklar för att möjliggöra ogiltiga uppdateringar
	13.	Möjlighet att neka legitima uppdateringar	13.1	Överbelastningsattack mot uppdateringsserver eller -nätverk för att förhindra distribution av viktiga programvaruuppdateringar och/eller upplåsning av kundspecifika funktioner
4.3.4 Hot mot fordon med avseende på oavsiktliga mänskliga handlingar som underlättar en cyberattack	15.	Legitima aktörer kan vidta åtgärder som oavsiktligt skulle underlätta en cyberattack	15.1	Ett oskyldigt offer (t.ex. ägare, operatör eller underhållsingenjör) luras att vidta en åtgärd för att oavsiktligt ladda upp sabotageprogram eller möjliggöra en attack
			15.2	Fastställda säkerhetsförfaranden följs inte

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
4.3.5 Hot mot fordon med avseende på deras externa konnektivitet och anslutningar	16.	Manipulation av fordonsfunktioners konnektivitet möjliggör en cyberattack, som kan inbegripa telematik, system som möjliggör fjärrbearbetning och system som använder trådlös korthållskommunikation	16.1	Manipulation av funktioner som är konstruerade för att fjärrstyra system, t.ex. fjärrnycklar, startspärrar och laddstolpar
			16.2	Manipulation av fordonstelematik (t.ex. manipulation av temperaturmätning av känsliga varor, fjärrupplåsning av lastdörrar)
			16.3	Interferens med trådlösa kortdistanssystem eller sensorer
	17.	Inbyggd programvara från tredje part, t.ex. underhållningssystem, används för att attackera fordonssystem	17.1	Förvanskade applikationer, eller applikationer med dålig programvarusäkerhet, som används för att attackera fordonssystem
	18.	Enheter som är anslutna till externa gränssnitt, t.ex. usb-portar och diagnosuttag, används för att attackera fordonssystem	18.1	Externa gränssnitt såsom usb-portar eller andra portar som används som angreppspunkt, t.ex. genom kodinjektion
			18.2	Medier som är infekterade av ett virus och ansluts till ett fordonssystem
			18.3	Diagnostisk åtkomst (t.ex. hårdvarunycklar i diagnosuttag) som används för att underlätta en attack, t.ex. manipulation av fordonsparametrar (direkt eller indirekt)
4.3.6 Hot mot fordonsdata/ fordonskod	19.	Hämtning av fordonsdata/ fordonskod	19.1	Hämtning av upphovsrättsskyddad eller proprietär programvara från fordonssystem (piratkopiering)
			19.2	Obehörig tillgång till ägarens personuppgifter, t.ex. identitet, betalkontoinformation, information om kontakter, platsinformation, fordonets elektroniska identitet etc.
			19.3	Hämtning av krypteringsnycklar
	20.	Manipulation av fordonsdata/ fordonskod	20.1	Olagliga/obehöriga ändringar av fordonets elektroniska identitet
			20.2	Identitetsbedrägeri, t.ex. om en användare vill visa upp en annan identitet vid kommunikation med vägtullsystem eller tillverkares backend
			20.3	Åtgärder för att kringgå övervakningssystem (t.ex. hacka/manipulera/blockera meddelanden såsom data från ODR-spårare eller antal körningar)
			20.4	Manipulation av data för att förfalska ett fordons kördata (t.ex. körsträcka, hastighet, vägvisningar etc.)
			20.5	Obehöriga ändringar av systemets diagnosdata
	21.	Radering av data/kod	21.1	Obehörig radering/manipulation av systemets händelseloggar
	22.	Införande av sabotageprogram	22.2	Införande av skadlig programvara eller skadlig programvaruaktivitet

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
	23.	Införande av ny programvara eller överskrivning av befintlig programvara	23.1	Fabricering av programvara i fordonets styrsystem eller informationssystem
	24.	Störning av system eller drift	24.1	Funktionsförlust, som t.ex. kan utlösas på det interna nätverket genom att översvämma en CAN-buss eller genom att framkalla fel på en motorstyrenhet via en stor mängd meddelanden
	25.	Manipulation av fordonsparametrar	25.1	Obehörig tillgång för att förfalska konfigurationsparametrarna för ett fordons centrala funktioner, t.ex. bromsdata, gräns för utlösning av krockkudde etc.)
			25.2	Obehörig tillgång för att förfalska laddningsparametrarna, t.ex. laddspänning, laddningskraft, batteritemperatur etc.
4.3.7 Potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt	26.	Krypteringsteknik kan skadas eller tillämpas inte i tillräcklig utsträckning	26.1	Kombination av korta krypteringsnycklar och lång giltighetstid som gör det möjligt för angripare att bryta krypteringen
			26.2	Otillräcklig användning av krypteringsalgoritmer för att skydda känsliga system
			26.3	Användning av krypteringsalgoritmer som redan är eller snart kommer att bli föråldrade
	27.	Delar eller leveranser kan skadas för att göra det möjligt för fordon att attackeras	27.1	Maskinvara eller programvara som är konstruerad för att möjliggöra en attack eller inte uppfyller konstruktionskriterierna för att förhindra en attack
	28.	Utveckling av programvara eller maskinvara möjliggör sårbarheter	28.1	Buggar i programvaran. Förekomsten av buggar i programvara kan utgöra en grund för potentiella sårbarheter som kan utnyttjas. Detta gäller särskilt om programvaran inte har provats för att kontrollera att känd dålig kod/buggar inte förekommer och för att minska risken för att okänd dålig kod/buggar ska förekomma
			28.2	Användning av rester från utveckling (t.ex. felsökningsportar, JTAG-portar, mikroprocessorer, utvecklingscertifikat, utvecklarlösenord etc.) som kan ge åtkomst till motorstyrenheter eller göra det möjligt för angripare att få större privilegier
	29.	Nätverkets utformning leder till sårbarheter	29.1	Överflödiga internetportar som lämnas öppna och ger tillträde till nätverk
			29.2	Nätverksseparation kringgås för att få kontroll. Specifika exempel är användningen av oskyddade nätslussar eller accesspunkter (t.ex. nätslussar mellan lastbil och släpvagn) för att kringgå skydd och få tillträde till andra nätverkssegment för att utföra sabotage, t.ex. skicka godtyckliga CAN-bussmeddelanden
	31.	Data kan överföras oavsiktligt	31.1	Dataintrång. Personuppgifter kan läcka när bilen byter användare (t.ex. säljs eller används som hyrbil med nya personer som hyr den)

Övergripande och detaljerade beskrivningar av sårbarhet/hot			Exempel på sårbarhet eller attackmetod	
	32.	Fysisk manipulation av system kan möjliggöra en attack	32.1	Manipulation av elektronisk maskinvara, t.ex. otillåten elektronisk maskinvara som tillförs bilen för att möjliggöra en man-i-mitten-attack Utbyte av tillåten elektronisk maskinvara (t.ex. sensorer) mot otillåten elektronisk maskinvara Manipulation av den information som en sensor samlar in (t.ex. genom natt använda en magnet för att manipulera den halleffektgivare som är ansluten till växellådan)

DEL B.

Riskreducerande åtgärder för hot riktade mot fordon

1. Riskreducerande åtgärder för ”fordons kommunikationskanaler”

Riskreducerande åtgärder för hoten kopplade till ”fordons kommunikationskanaler” anges i tabell B1.

Tabell B1

Riskreducerande åtgärder för hoten kopplade till ”fordons kommunikationskanaler”

Referens i tabell A1	Hot mot ”fordons kommunikationskanaler”	Ref.	Riskreducerande åtgärd
4.1	Manipulering av meddelanden (t.ex. V2X-lägesbild eller meddelanden för samordning av körning eller GNSS-meddelanden) genom att utge sig för att vara någon annan	M10	Fordonet ska kontrollera de meddelanden som det mottar med avseende på äkthet och integritet
4.2	Sybil-attack (för att manipulera andra fordon att tro att det är många fordon på vägen)	M11	Säkerhetskontroller ska genomföras för lagring av krypteringsnycklar (t.ex. användning av säkerhetsmoduler i maskinvara)
5.1	Kommunikationskanaler tillåter kodinjektion i data/kod i fordon, t.ex. injektion av en manipulerad binärfil i kommunikationsflödet	M10 M6	Fordonet ska kontrollera de meddelanden som det mottar med avseende på äkthet och integritet System ska tillämpa utformning för säkerhet för att minimera risker
5.2	Kommunikationskanaler tillåter manipulation av data/kod i fordon	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod
5.3	Kommunikationskanaler tillåter överskrivning av data/kod i fordon		
5.4 21.1	Kommunikationskanaler tillåter radering av data/kod i fordon		
5.5	Kommunikationskanaler tillåter införande av data/kod i fordonssystem (skriver datakod)		

Referens i tabell A1	Hot mot ”fordons kommunikationskanaler”	Ref.	Riskreducerande åtgärd
6.1	Information tas emot från en otillförlitlig eller osäker källa	M10	Fordonet ska kontrollera de meddelanden som det mottar med avseende på äkthet och integritet
6.2	Man-i-mitten-attack/sessionskapning	M10	Fordonet ska kontrollera de meddelanden som det mottar med avseende på äkthet och integritet
6.3	Omtagningsattack, t.ex. en attack mot en nätport som gör att angriparen kan nedgradera en motorstyrenhets programvara eller nätportens fasta programvara		
7.1	Avlyssning av information/störande strålning/övervakning av kommunikation	M12	Konfidentiella data som överförs till eller från fordonet ska skyddas
7.2	Obehörig tillgång till filer eller data	M8	Genom systemets utformning och åtkomstkontroll ska det inte vara möjligt för obehörig personal att få tillgång till personuppgifter eller kritiska systemdata. Exempel på säkerhetskontroller finns i Owasp
8.1	En stor mängd skräpdata skickas till ett fordons informationssystem så att det inte kan tillhandahålla tjänster på normalt sätt	M13	Åtgärder för att upptäcka och återhämta sig från en överbelastningsattack ska vidtas
8.2	Attack i form av ett svart hål, störning av kommunikation mellan fordon genom att blockera överföringen av meddelanden till andra fordon	M13	Åtgärder för att upptäcka och återhämta sig från en överbelastningsattack ska vidtas
9.1	En obehörig användare får åtkomsträttigheter, t.ex. rootåtkomst	M9	Åtgärder för att förhindra och upptäcka obehörig åtkomst ska vidtas
10.1	Virus som är inbyggda i kommunikationsmedier infekterar fordonssystem	M14	Åtgärder för att skydda system mot inbyggda virus/sabotageprogram ska övervägas
11.1	Skadliga interna meddelanden (t.ex. CAN-meddelanden)	M15	Åtgärder för att upptäcka skadliga interna meddelanden eller skadlig intern aktivitet ska övervägas
11.2	Skadliga V2X-meddelanden, t.ex. mellan infrastruktur och fordon eller mellan två fordon (t.ex. CAM, DENM)	M10	Fordonet ska kontrollera de meddelanden som det mottar med avseende på äkthet och integritet
11.3	Skadliga diagnosmeddelanden		
11.4	Skadliga proprietära meddelanden (t.ex. meddelanden som normalt skickas från OEM-företag eller leverantören av komponenten/systemet/funktionen)		

2. Riskreducerande åtgärder för ”processuppdatering”

Riskreducerande åtgärder för hoten kopplade till ”processuppdatering” anges i tabell B2.

Tabell B2

Riskreducerande åtgärder för hoten kopplade till ”processuppdatering”

Referens i tabell A1	Hot mot ”processuppdatering”	Ref.	Riskreducerande åtgärd
12.1	Röjande av trådlösa processer för programvaruuppdatering. Detta inbegriper att fabricera systemets uppdateringsprogram eller fasta programvara	M16	Säkra förfaranden för programvaruuppdatering ska tillämpas
12.2	Röjande av lokala/fysiska processer för programvaruuppdatering. Detta inbegriper att fabricera systemets uppdateringsprogram eller fasta programvara		
12.3	Programvara som manipuleras före uppdateringsprocessen (och därmed skadas), även om uppdateringsprocessen är intakt		
12.4	Röjande av programvaruleverantörens krypteringsnycklar för att möjliggöra ogiltiga uppdateringar	M11	Säkerhetskontroller ska genomföras för lagring av krypteringsnycklar
13.1	Överbelastningsattack mot uppdateringsserver eller -nätverk för att förhindra distribution av viktiga programvaruuppdateringar och/eller upplåsning av kundspecifika funktioner	M3	Säkerhetskontroller ska tillämpas på backendsystem. När backendservrar är nödvändiga för tillhandahållandet av tjänster ska det finnas åtgärder för återhämtning i händelse av systemavbrott. Exempel på säkerhetskontroller finns i Owasp

3. Riskreducerande åtgärderför ”oavsiktliga mänskliga handlingar som underlättar en cyberattack”

Riskreducerande åtgärder för hoten kopplade till ”oavsiktliga mänskliga handlingar som underlättar en cyberattack” anges i tabell B3.

Tabell B3

Riskreducerande åtgärder för hoten kopplade till ”oavsiktliga mänskliga handlingar som underlättar en cyberattack”

Referens i tabell A1	Hot kopplade till ”oavsiktliga mänskliga handlingar”	Ref.	Riskreducerande åtgärd
15.1	Ett oskyldigt offer (t.ex. ägare, operatör eller underhållsingenjör) luras att vidta en åtgärd för att oavsiktligt ladda upp sabotageprogram eller möjliggöra en attack	M18	Åtgärder ska vidtas för att fastställa och kontrollera användarroller och åtkomsträttigheter på grundval av principen för begränsad behörighet

Referens i tabell A1	Hot kopplade till ”oavsiktliga mänskliga handlingar”	Ref.	Riskreducerande åtgärd
15.2	Fastställda säkerhetsförfaranden följs inte	M19	Organisationer ska säkerställa att säkerhetsförfaranden har fastställts och följs, däribland loggning av åtgärder och åtkomst kopplad till förvaltningen av säkerhetsfunktioner

4. Riskreducerande åtgärder för ”extern konnektivitet och anslutningar”

Riskreducerande åtgärder för hoten kopplade till ”extern konnektivitet och anslutningar” anges i tabell B4.

Tabell B4

Riskreducerande åtgärder för hoten kopplade till ”extern konnektivitet och anslutningar”

Referens i tabell A1	Hot mot ”extern konnektivitet och anslutningar”	Ref.	Riskreducerande åtgärd
16.1	Manipulation av funktioner som är konstruerade för att fjärrstyra fordonssystem, t.ex. fjärrnycklar, startspärrar och laddstolpar	M20	Säkerhetskontroller ska tillämpas på system som har fjärråtkomst
16.2	Manipulation av fordonstelematik (t.ex. manipulation av temperaturmätning av känsliga varor, fjärrupplåsning av lastdörrar)		
16.3	Interferens med trådlösa kortdistanssystem eller sensorer		
17.1	Förvanskade applikationer, eller applikationer med dålig programvarusäkerhet, som används för att attackera fordonssystem	M21	Programvara ska bedömas utifrån säkerhet, autentiseras och skyddas med avseende på integritet. Säkerhetskontroller ska tillämpas för att minimera risken från programvara från tredje part som ska eller kan tänkas användas i fordonet
18.1	Externa gränssnitt såsom usb-portar eller andra portar som används som angreppspunkt, t.ex. genom kodinjektion	M22	Säkerhetskontroller ska tillämpas på externa gränssnitt
18.2	Medier som är infekterade av virus och ansluts till fordonet		
18.3	Diagnostisk åtkomst (t.ex. hårdvarunycklar i diagnosuttag) som används för att underlätta en attack, t.ex. manipulation av fordonsparametrar (direkt eller indirekt)	M22	Säkerhetskontroller ska tillämpas på externa gränssnitt

5. Riskreducerande åtgärder för ”potentiella mål eller motiv för en attack”

Riskreducerande åtgärder för hoten kopplade till ”potentiella mål eller motiv för en attack” anges i tabell B5.

Tabell B5

Riskreducerande åtgärder för hoten kopplade till ”potentiella mål eller motiv för en attack”

Referens i tabell A1	Hot mot ”potentiella mål eller motiv för en attack”	Ref.	Riskreducerande åtgärd
19.1	Hämtning av upphovsrättsskyddad eller proprietär programvara från fordonssystem (piratkopiering/stulen programvara)	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp
19.2	Obehörig tillgång till ägarens personuppgifter, t.ex. identitet, betalkontoinformation, information om kontakter, platsinformation, fordonets elektroniska identitet etc.	M8	Genom systemets utformning och åtkomstkontroll ska det inte vara möjligt för obehörig personal att få tillgång till personuppgifter eller kritiska systemdata. Exempel på säkerhetskontroller finns i Owasp
19.3	Hämtning av krypteringsnycklar	M11	Säkerhetskontroller ska genomföras för lagring av krypteringsnycklar, t.ex. säkerhetsmoduler
20.1	Olagliga/obehöriga ändringar av fordonets elektroniska identitet	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp
20.2	Identitetsbedrägeri, t.ex. om en användare vill visa upp en annan identitet vid kommunikation med vägtullsystem eller tillverkares backend		
20.3	Åtgärder för att kringgå övervakningssystem (t.ex. hacka/ manipulera/blockera meddelanden såsom data från ODR-spårare eller antal körningar)	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp. Attacker mot sensorer eller överförda data för att manipulera data kan minskas genom att jämföra data från olika informationskällor
20.4	Manipulation av data för att förfalska ett fordons kördata (t.ex. körsträcka, hastighet, vägvisningar etc.)		
20.5	Obehörig ändring av systemets diagnosdata		
21.1	Obehörig radering/manipulation av systemets händelseloggar	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp.
22.2	Införande av skadlig programvara eller skadlig programvaruaktivitet	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp.
23.1	Fabricering av programvara i fordonets styrsystem eller informationssystem		

Referens i tabell A1	Hot mot ”potentiella mål eller motiv för en attack”	Ref.	Riskreducerande åtgärd
24.1	Funktionsförlust, som t.ex. kan utlösas på det interna nätverket genom att översvämma en CAN-buss eller genom att framkalla fel på en motorstyrenhet via en stor mängd meddelanden	M13	Åtgärder för att upptäcka och återhämta sig från en överbelastningsattack ska vidtas
25.1	Obehörig tillgång för att förfalska konfigurationsparametrarna för ett fordons centrala funktioner, t.ex. bromsdata, gräns för utlösning av krockkudde etc.	M7	Teknik och utformning för åtkomstkontroll ska tillämpas för att skydda systemdata/systemkod. Exempel på säkerhetskontroller finns i Owasp
25.2	Obehörig tillgång för att förfalska laddningsparametrarna, t.ex. laddspänning, laddningskraft, batteritemperatur etc.		

6. Riskreducerande åtgärder för ”potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt”

Riskreducerande åtgärder för hoten kopplade till ”potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt” anges i tabell B6.

Tabell B6

Riskreducerande åtgärder för hoten kopplade till ”potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt”

Referens i tabell A1	Hot mot ”potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt”	Ref.	Riskreducerande åtgärd
26.1	Kombination av korta krypteringsnycklar och lång giltighetstid som gör det möjligt för angripare att bryta krypteringen	M23	Bästa praxis inom cybersäkerhet för utveckling av programvara och maskinvara ska följas
26.2	Otillräcklig användning av krypteringsalgoritmer för att skydda känsliga system		
26.3	Användning av föråldrade krypteringsalgoritmer		
27.1	Maskinvara eller programvara som är konstruerad för att möjliggöra en attack eller inte uppfyller konstruktionskriterierna för att förhindra en attack	M23	Bästa praxis inom cybersäkerhet för utveckling av programvara och maskinvara ska följas
28.1	Förekomsten av buggar i programvara kan utgöra en grund för potentiella sårbarheter som kan utnyttjas. Detta gäller särskilt om programvaran inte har provats för att kontrollera att känd dålig kod/buggar inte förekommer och för att minska risken för att okänd dålig kod/buggar ska förekomma	M23	Bästa praxis inom cybersäkerhet för utveckling av programvara och maskinvara ska följas. Provning av cybersäkerheten med lämplig täckning

Referens i tabell A1	Hot mot ”potentiella sårbarheter som kan utnyttjas om de inte skyddas eller förstärks tillräckligt”	Ref.	Riskreducerande åtgärd
28.2	Användning av rester från utveckling (t.ex. felsökningsportar, JTAG-portar, mikroprocessorer, utvecklingscertifikat, utvecklarlösenord etc.) kan göra det möjligt för angripare att få åtkomst till motorstyrenheter eller få större privilegier		
29.1	Överflödiga internetportar som lämnas öppna och ger tillträde till nätverk		
29.2	Nätverksseparation kringgås för att få kontroll. Specifika exempel är användningen av oskyddade nätslussar eller accesspunkter (t.ex. nätslussar mellan lastbil och släpvagn) för att kringgå skydd och få tillträde till andra nätverkssegment för att utföra sabotage, t.ex. skicka godtyckliga CAN-bussmeddelanden	M23	Bästa praxis inom cybersäkerhet för utveckling av programvara och maskinvara ska följas. Bästa praxis inom cybersäkerhet för systemutformning och systemintegration ska följas

7. Riskreducerande åtgärder för ”dataförlust/dataintrång i fordon”

Riskreducerande åtgärder för hoten kopplade till ”dataförlust/dataintrång i fordon” anges i tabell B7.

Tabell B7

Riskreducerande åtgärder för hoten kopplade till ”dataförlust/dataintrång i fordon”

Referens i tabell A1	Hot mot ”dataförlust/dataintrång i fordon”	Ref.	Riskreducerande åtgärd
31.1	Dataintrång. Intrång i personuppgifter kan ske när bilen byter användare (t.ex. säljs eller används som hyrbil med nya personer som hyr den)	M24	Bästa praxis för skydd av dataintegritet och datasekretess ska följas vid lagring av personuppgifter

8. Riskreducerande åtgärder för ”fysisk manipulation av system kan möjliggöra en attack”

Riskreducerande åtgärder för hoten kopplade till ”fysisk manipulation av system kan möjliggöra en attack” anges i tabell B8.

Tabell B8

Riskreducerande åtgärder för hoten kopplade till ”fysisk manipulation av system kan möjliggöra en attack”

Referens i tabell A1	Hot mot ”fysisk manipulation av system kan möjliggöra en attack”	Ref.	Riskreducerande åtgärd
32.1	Manipulation av maskinvara från OEM-företag, t.ex. otillåten maskinvara som tillförs bilen för att möjliggöra en man-i-mitten-attack	M9	Åtgärder för att förhindra och upptäcka obehörig åtkomst ska vidtas

Del C.

Riskreducerande åtgärder för hot utanför fordon

1. Riskreducerande åtgärder för ”backendservrar”

Riskreducerande åtgärder för hoten kopplade till ”backendservrar” anges i tabell C1.

Tabell C1

Riskreducerande åtgärder för hoten kopplade till ”backendservrar”

Referens i tabell A1	Hot mot ”backendservrar”	Ref.	Riskreducerande åtgärd
1.1 och 3.1	Personals missbruk av privilegier (angrepp inifrån)	M1	Säkerhetskontroller ska tillämpas på backendsystem för att minimera risken för angrepp inifrån
1.2 och 3.3	Obehörig internetåtkomst till servern (som möjliggörs genom exempelvis bakdörrar, sårbarheter i opatchad programvara, SQL-attacker eller på andra sätt)	M2	Säkerhetskontroller ska tillämpas på backendsystem för att minimera risken för obehörig åtkomst. Exempel på säkerhetskontroller finns i Owasp
1.3 och 3.4	Obehörig fysisk tillgång till servern (som genomförs med exempelvis usb-minnen eller andra medier som ansluts till servern)	M8	Genom systemets utformning och åtkomstkontroll ska det inte vara möjligt för obehörig personal att få tillgång till personuppgifter eller kritiska systemdata.
2.1	Attack mot backendservern som gör att den slutar fungera, t.ex. hindrar den att kommunicera med fordon och tillhandahålla tjänster som fordonen är beroende av	M3	Säkerhetskontroller ska tillämpas på backendsystem. När backendservrar är nödvändiga för tillhandahållandet av tjänster ska det finnas åtgärder för återhämtning i händelse av systemavbrott. Exempel på säkerhetskontroller finns i Owasp
3.2	Förlust av information i molnet. Känsliga data kan förloras till följd av attacker eller olyckor när data lagras av tredjepartsleverantör av molntjänster	M4	Säkerhetskontroller ska tillämpas för att minimera risker kopplade till molntjänster. Exempel på säkerhetskontroller finns i Owasp i riktlinjerna för molntjänster från NCSC
3.5	Dataintrång genom oavsiktlig datadelning (t.ex. administratörsfel, lagring av data på servrar i garage)	M5	Säkerhetskontroller ska tillämpas på backendsystem för att förhindra dataintrång. Exempel på säkerhetskontroller finns i Owasp

2. Riskreducerande åtgärder för ”oavsiktliga mänskliga handlingar”

Riskreducerande åtgärder för hoten kopplade till ”oavsiktliga mänskliga handlingar” anges i tabell C2.

Tabell C2

Riskreducerande åtgärder för hoten kopplade till ”oavsiktliga mänskliga handlingar”

Referens i tabell A1	Hot kopplade till ”oavsiktliga mänskliga handlingar”	Ref.	Riskreducerande åtgärd
15.1	Ett oskyldigt offer (t.ex. ägare, operatör eller underhållsingenjör) luras att vidta en åtgärd för att oavsiktligt ladda upp sabotageprogram eller möjliggöra en attack	M18	Åtgärder ska vidtas för att fastställa och kontrollera användarroller och åtkomsträttigheter på grundval av principen för begränsad behörighet
15.2	Fastställda säkerhetsförfaranden följs inte	M19	Organisationer ska säkerställa att säkerhetsförfaranden har fastställts och följs, däribland loggning av åtgärder och åtkomst kopplad till förvaltningen av säkerhetsfunktioner

3. Riskreducerande åtgärder för ”fysisk dataförlust”

Riskreducerande åtgärder för hoten kopplade till ”fysisk dataförlust” anges i tabell C3.

Tabell C3

Riskreducerande åtgärder för hoten kopplade till ”fysisk dataförlust”

Referens i tabell A1	Hot mot ”fysisk dataförlust”	Ref.	Riskreducerande åtgärd
30.1	Skador som orsakas av en tredje part. Känsliga data kan förloras eller skadas på grund av fysiska skador i samband med en trafikolycka eller stöld	M24	Bästa praxis för skydd av dataintegritet och datasekretess ska följas vid lagring av personuppgifter Exempel på säkerhetskontroller finns i ISO/SC27/WG5
30.2	Förlust till följd av DRM-konflikter (förvaltning av digitala rättigheter). Användardata kan raderas på grund av DRM-problem		
30.3	Känsliga data (och dessas integritet) kan förloras på grund av slitage på it-komponenter, vilket kan orsaka dominoeffekter (t.ex. vid stora ändringar)		