Publicatieblad
van de Europese Unie

NL
L-serie

2025/5

10.1.2025

Voor het internationaal publiekrecht hebben alleen de originele VN/ECE-teksten rechtsgevolgen. Voor de status en de datum van inwerkingtreding van dit reglement, zie de recentste versie van VN/ECE-statusdocument TRANS/WP.29/343 op: https://unece.org/status-1958-agreement-and-annexed-regulations

VN-Reglement nr. 155 — Uniforme bepalingen voor de goedkeuring van voertuigen met betrekking tot cyberbeveiliging en het beheersysteem voor cyberbeveiliging [2025/5]

Bevat de volledige geldige tekst tot en met:

Supplement 3 op de oorspronkelijke versie van het reglement – Datum van inwerkingtreding: 10 januari 2025

Dit document dient louter ter informatie. De authentieke en juridisch bindende teksten zijn:

— ECE/TRANS/WP.29/2020/79 (zoals gewijzigd bij ECE/TRANS/WP.29/2020/94 en ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 en

— ECE/TRANS/WP.29/2024/55

INHOUDSOPGAVE

Reglement

1. Toepassingsgebied
2. Definities
3. Goedkeuringsaanvraag
4. Markeringen
5. Goedkeuring
6. Conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging
7. Specificaties
8. Wijziging van het voertuigtype en uitbreiding van de typegoedkeuring
9. Conformiteit van de productie
10. Sancties bij non-conformiteit van de productie
11. Definitieve stopzetting van de productie
12. Naam en adres van de voor de uitvoering van de goedkeuringstest verantwoordelijke technische diensten en van de typegoedkeuringsinstanties

Bijlagen

1 Inlichtingenformulier

2 Mededeling

3 Opstelling van goedkeuringsmerken

4 Model van het conformiteitscertificaat voor het CSMS

5 Lijst van dreigingen en de overeenkomstige mitigatiemaatregelen

1. Toepassingsgebied

1.1. Dit reglement is van toepassing op voertuigen van de categorieën L, M, N en O indien deze zijn uitgerust met ten minste één elektronische regeleenheid.

1.2. Dit reglement doet geen afbreuk aan andere VN-reglementen en regionale of nationale wetgeving betreffende de toegang van gemachtigde partijen tot het voertuig, de gegevens, functies en hulpbronnen ervan, en de voorwaarden van die toegang. Ook doet het geen afbreuk aan de toepassing van nationale en regionale wetgeving inzake privacy en de bescherming van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens.

1.3. Dit reglement doet geen afbreuk aan andere VN-reglementen, nationale of regionale wetgeving betreffende de ontwikkeling en installatie/systeemintegratie van fysieke en digitale vervangingsonderdelen en componenten met betrekking tot cyberbeveiliging.

2. Definities

Voor de toepassing van dit reglement wordt verstaan onder:

2.1. "*voertuigtype*": voertuigen die ten minste op de volgende essentiële punten niet van elkaar verschillen:

a) de aanduiding die de fabrikant voor het voertuigtype gebruikt;

b) essentiële aspecten van de elektrische/elektronische architectuur en externe interfaces met betrekking tot cyberbeveiliging;

2.2. "*cyberbeveiliging*": de omstandigheden waaronder wegvoertuigen en de bijbehorende functies worden beschermd tegen cyberdreigingen voor elektrische of elektronische componenten;

2.3. "*beheersysteem voor cyberbeveiliging* (Cyber Security Management System – *CSMS*)": een systematische, op risico's gebaseerde aanpak waarmee op organisatorisch niveau de processen, verantwoordelijkheden en governance-maatregelen worden vastgesteld om risico's in verband met cyberdreigingen voor voertuigen aan te pakken en voertuigen te beschermen tegen cyberaanvallen;

2.4. "*systeem*": een verzameling componenten en/of subsystemen waarmee een of meer functies worden uitgevoerd;

2.5. "*ontwikkelingsfase*": de periode die voorafgaat aan de goedkeuring van een voertuigtype;

2.6. "*productiefase*": de duur van de productie van een voertuigtype;

2.7. "*post-productiefase*": de periode waarin een voertuigtype niet meer geproduceerd wordt tot het einde van de levensduur van alle voertuigen van dit voertuigtype. Voertuigen die tot een bepaald voertuigtype behoren, zijn tijdens deze fase operationeel, maar worden niet meer geproduceerd. De fase eindigt wanneer er van een bepaald voertuigtype geen voertuigen meer operationeel zijn;

2.8. "*mitigatiemaatregel*": een risicobeperkende maatregel;

2.9. "*risico*": de mogelijkheid dat een bepaalde dreiging de kwetsbaarheden van een voertuig benut en op die manier schade berokkent aan de organisatie of aan een individu;

2.10. "*risicobeoordeling*": het volledige proces van het vinden, herkennen en beschrijven van risico's (risico-identificatie) om inzicht te krijgen in de aard van het risico en het niveau van het risico te bepalen (risicoanalyse), en het vergelijken van de resultaten van de risicoanalyse met risicocriteria om te bepalen of het risico en/of de omvang ervan aanvaardbaar of tolereerbaar is (risico-evaluatie);

2.11. "*risicobeheer*": gecoördineerde activiteiten om een organisatie te besturen en te controleren met betrekking tot risico's;

2.12. "*dreiging*": een mogelijke oorzaak van een ongewenst incident, dat schade kan berokkenen aan een systeem, organisatie of individu;

2.13. "*kwetsbaarheid*": een zwakte van een eigenschap of mitigatiemaatregel die door een of meer dreigingen kan worden benut.

3. Goedkeuringsaanvraag

3.1. De goedkeuringsaanvraag voor een type voertuig wat cyberbeveiliging betreft, moet door de voertuigfabrikant of zijn daartoe gemachtigde vertegenwoordiger worden ingediend.

3.2. De aanvraag gaat vergezeld van de hierna genoemde documenten in drievoud en van de volgende gegevens:

3.2.1. Een beschrijving van het voertuigtype voor wat betreft de in bijlage 1 bedoelde onderdelen.

3.2.2. Wanneer kan worden aangetoond dat informatie door intellectuele-eigendomsrechten wordt beschermd of specifieke kennis van de fabrikant of van zijn leveranciers vormt, verstrekken de fabrikant of zijn leveranciers voldoende informatie zodat de in dit reglement bedoelde controles naar behoren kunnen worden uitgevoerd. Dergelijke informatie moet vertrouwelijk worden behandeld.

3.2.3. Het conformiteitscertificaat voor het CSMS overeenkomstig punt 6 van dit reglement.

3.3. De documentatie moet in twee delen ter beschikking worden gesteld:

a) het formele documentatiepakket voor de goedkeuring, dat het in bijlage 1 gespecificeerde materiaal bevat en dat bij de indiening van de aanvraag om typegoedkeuring aan de goedkeuringsinstantie of haar technische dienst moet worden verstrekt. Dit documentatiepakket wordt door de goedkeuringsinstantie of haar technische dienst gebruikt als basisreferentie voor het goedkeuringsproces. De goedkeuringsinstantie of haar technische dienst zorgt ervoor dat dit documentatiepakket vanaf het moment van definitieve stopzetting van de productie ten minste tien jaar beschikbaar blijft;

b) het aanvullende materiaal met betrekking tot de voorschriften van dit reglement mogen door de fabrikant worden bewaard, maar moeten bij typegoedkeuring beschikbaar worden gesteld voor inspectie. De fabrikant ziet erop toe dat het materiaal dat bij typegoedkeuring beschikbaar wordt gesteld voor inspectie ten minste tien jaar beschikbaar blijft vanaf het moment dat de productie van het voertuigtype definitief wordt stopgezet.

4. Markeringen

4.1. Op elk voertuig dat conform is met een voertuigtype dat krachtens dit reglement is goedgekeurd, wordt op een opvallende en makkelijk bereikbare plaats die op het goedkeuringsformulier is gespecificeerd, een internationaal goedkeuringsmerk aangebracht, dat bestaat uit:

4.1.1. een cirkel met daarin de letter "E", gevolgd door het nummer van het land dat de goedkeuring heeft verleend;

4.1.2. het nummer van dit reglement, gevolgd door de letter "R", een liggend streepje en het goedkeuringsnummer, rechts van de in punt 4.1.1 beschreven cirkel.

4.2. Als het voertuig conform is met een voertuigtype dat op basis van een of meer aan de overeenkomst gehechte reglementen is goedgekeurd in het land dat krachtens dit reglement goedkeuring heeft verleend, hoeft het in punt 4.1.1 bedoelde symbool niet te worden herhaald; in dat geval moeten de reglement- en goedkeuringsnummers en de aanvullende symbolen van alle reglementen op basis waarvan goedkeuring is verleend in het land dat krachtens dit reglement goedkeuring heeft verleend, in verticale kolommen rechts van het in punt 4.1.1 voorgeschreven symbool worden geplaatst.

4.3. Het goedkeuringsmerk moet goed leesbaar en onuitwisbaar zijn.

4.4. Het goedkeuringsmerk wordt op of dicht bij het door de fabrikant bevestigde gegevensplaatje van het voertuig aangebracht.

4.5. In bijlage 3 worden voorbeelden gegeven van de opstelling van het goedkeuringsmerk.

5. Goedkeuring

5.1. De goedkeuringsinstanties verlenen, naar gelang van het geval, alleen typegoedkeuring met betrekking tot cyberbeveiliging aan voertuigen die aan de voorschriften van dit reglement voldoen.

5.1.1. De goedkeuringsinstantie of de technische dienst gaat aan de hand van documentencontroles na of de voertuigfabrikant de voor het voertuigtype relevante noodzakelijke maatregelen heeft genomen om:

a) de in dit reglement vereiste informatie te verzamelen en te verifiëren via de toeleveringsketen, om aan te tonen dat de risico's in verband met leveranciers zijn vastgesteld en beheerd;

b) de risicobeoordeling (uitgevoerd tijdens de ontwikkelingsfase of achteraf), de testresultaten en de voor het voertuigtype uitgevoerde mitigatiemaatregelen te documenteren, met inbegrip van ontwerpinformatie ter ondersteuning van de risicobeoordeling;

c) passende maatregelen inzake cyberbeveiliging in het ontwerp van het voertuigtype op te nemen;

d) mogelijke cyberaanvallen op te sporen en aan te pakken;

e) gegevens te registreren ter ondersteuning van de opsporing van cyberaanvallen, en forensische capaciteit te verstrekken om succesvolle cyberaanvallen of pogingen daartoe te kunnen analyseren.

5.1.2. De goedkeuringsinstantie of de technische dienst verifieert, door middel van een test van het voertuig van het desbetreffende type, of de voertuigfabrikant de gedocumenteerde maatregelen op het gebied van cyberbeveiliging heeft uitgevoerd. De tests worden uitgevoerd door de goedkeuringsinstantie of de technische dienst zelf of in samenwerking met de voertuigfabrikant door middel van steekproeven. De steekproeven worden gericht op, maar niet beperkt tot, de risico's die tijdens de risicobeoordeling als hoog worden beoordeeld.

5.1.3. De goedkeuringsinstantie of de technische dienst weigert de typegoedkeuring met betrekking tot cyberbeveiliging te verlenen wanneer een of meer van de in punt 7.3 genoemde voorschriften niet door de voertuigfabrikant zijn nageleefd, met name in de volgende gevallen:

a) de voertuigfabrikant heeft de in punt 7.3.3 bedoelde uitgebreide risicobeoordeling niet uitgevoerd, of de fabrikant heeft niet alle risico's in verband met de in deel A van bijlage 5 genoemde dreigingen in aanmerking genomen;

b) de voertuigfabrikant heeft het voertuigtype niet tegen de in zijn risicobeoordeling vastgestelde risico's beschermd of geen evenredige mitigatiemaatregelen als vereist in punt 7 uitgevoerd;

c) de voertuigfabrikant heeft geen passende en evenredige maatregelen uitgevoerd om speciale omgevingen (indien die worden geleverd) voor de opslag en uitvoering van aftermarketsoftware, -diensten, -applicaties of -gegevens op het voertuigtype te beveiligen;

d) de voertuigfabrikant heeft voorafgaand aan de goedkeuring geen passende en toereikende tests uitgevoerd om de doeltreffendheid van de uitgevoerde beveiligingsmaatregelen te controleren.

5.1.4. Ook weigert de beoordelende goedkeuringsinstantie typegoedkeuring met betrekking tot cyberbeveiliging te verlenen wanneer de goedkeuringsinstantie of de technische dienst onvoldoende informatie van de voertuigfabrikant heeft ontvangen om de cyberbeveiliging van het voertuigtype te kunnen beoordelen.

5.2. Van de goedkeuring of de uitbreiding of weigering van de goedkeuring van een voertuigtype krachtens dit reglement wordt aan de partijen bij de Overeenkomst van 1958 die dit reglement toepassen, mededeling gedaan door middel van een formulier volgens het model in bijlage 2.

5.3. Goedkeuringsinstanties verlenen geen typegoedkeuring zonder na te gaan of de fabrikant toereikende regelingen en procedures heeft ingevoerd om de aspecten van cyberbeveiliging waarop dit reglement van toepassing is naar behoren te beheren.

5.3.1. In aanvulling op de in bijlage 2 bij de overeenkomst van 1958 vastgestelde criteria, zorgen de goedkeuringsinstantie en haar technische diensten ervoor dat zij:

a) beschikken over bevoegd personeel met passende vaardigheden op het gebied van cyberbeveiliging en specifieke kennis van risicobeoordelingen in de autobranche ([1]);

b) procedures hebben ingesteld voor de uniforme evaluatie overeenkomstig dit reglement.

5.3.2. Elke overeenkomstsluitende partij die dit reglement toepast, stelt via zijn goedkeuringsinstantie andere goedkeuringsinstanties van de overeenkomstsluitende partijen die dit VN-reglement toepassen in kennis van en informeert hen over de methode en de criteria die de kennisgevende goedkeuringsinstantie heeft gebruikt als basis voor het beoordelen van de geschiktheid van de in overeenstemming met dit reglement genomen maatregelen, en met name de punten 5.1, 7.2 en 7.3.

Deze informatie wordt gedeeld: a) alleen voordat voor de eerste keer goedkeuring wordt verleend overeenkomstig dit reglement en b) telkens wanneer de methode of de criteria voor de beoordeling is of zijn geactualiseerd.

Deze informatie is bedoeld om te worden gedeeld met het oog op het verzamelen en analyseren van de beste praktijken en het waarborgen van de geharmoniseerde toepassing van dit reglement door alle goedkeuringsinstanties die dit reglement toepassen.

5.3.3. De in punt 5.3.2 bedoelde informatie wordt tijdig en uiterlijk 14 dagen voordat volgens de desbetreffende beoordelingsmethoden en -criteria voor de eerste keer goedkeuring wordt verleend in de Engelse taal geüpload naar de beveiligde internetgegevensbank DETA ([2]), die is opgezet door de Economische Commissie voor Europa van de Verenigde Naties. Uit de informatie moet duidelijk blijken welke minimale prestatieniveaus de goedkeuringsinstantie voor elk in punt 5.3.2 genoemd voorschrift heeft gehanteerd en welke processen en maatregelen de instantie toepast om na te gaan of aan deze minimale prestatieniveaus wordt voldaan ([3]).

5.3.4. Goedkeuringsinstanties die de in punt 5.3.2 bedoelde informatie ontvangen, kunnen opmerkingen bij de kennisgevende goedkeuringsinstantie indienen door ze uiterlijk 14 dagen na de dag van de kennisgeving naar DETA te uploaden.

5.3.5. Als het voor de verlenende goedkeuringsinstantie niet mogelijk is om rekening te houden met de overeenkomstig punt 5.3.4 ontvangen opmerkingen, verzoeken de goedkeuringsinstanties die de opmerkingen hebben ingediend en de goedkeuringsinstantie die goedkeuring verleent, om nadere inlichtingen, in overeenstemming met bijlage 6 bij de overeenkomst van 1958. De betrokken ondergeschikte werkgroep ([4]) van het Wereldforum voor de harmonisatie van reglementen voor voertuigen (WP.29) komt voor dit reglement een gemeenschappelijke interpretatie van de beoordelingsmethoden en -criteria overeen ([5]). Die gemeenschappelijke interpretatie wordt uitgevoerd, en alle goedkeuringsinstanties geven dienovereenkomstig typegoedkeuringen af krachtens dit reglement.

([1]) Bv. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Richtsnoeren voor de te uploaden gedetailleerde informatie (bv. methode, criteria, prestatieniveau) en het formaat zullen worden gegeven in het interpretatiedocument dat momenteel door de taskforce voor cyberbeveiliging en draadloze kwesties wordt opgesteld voor de zevende bijeenkomst van de GRVA.
([4]) Werkgroep Geautomatiseerde/autonome en communicerende voertuigen (GRVA).
([5]) Deze interpretatie wordt opgenomen in het interpretatiedocument zoals bedoeld in de voetnoot bij punt 5.3.3.

5.3.6. Elke goedkeuringsinstantie die overeenkomstig dit reglement een typegoedkeuring afgeeft, stelt de andere goedkeuringsinstanties van de goedkeuring in kennis. De typegoedkeuring wordt samen met de aanvullende documentatie uiterlijk 14 dagen na de goedkeuring door de goedkeuringsinstantie in de Engelse taal geüpload naar DETA ([6]).

5.3.7. De overeenkomstsluitende partijen kunnen de verleende goedkeuringen onderzoeken op basis van de overeenkomstig punt 5.3.6 geüploade informatie. Eventuele uiteenlopende standpunten tussen de overeenkomstsluitende partijen worden behandeld overeenkomstig artikel 10 van en bijlage 6 bij de overeenkomst van 1958. De overeenkomstsluitende partijen stellen tevens de betrokken ondergeschikte werkgroep van het Wereldforum voor de harmonisatie van reglementen voor voertuigen (WP.29) in kennis van de uiteenlopende standpunten in de zin van bijlage 6 bij de overeenkomst van 1958. De betrokken werkgroep steunt de afhandeling van de uiteenlopende standpunten en pleegt indien nodig overleg hierover met WP.29.

5.4. Voor de toepassing van punt 7.2 van dit reglement ziet de fabrikant erop toe dat de aspecten van cyberbeveiliging waarop dit reglement van toepassing is, worden uitgevoerd.

6. Conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging

6.1. De overeenkomstsluitende partijen wijzen een goedkeuringsinstantie aan voor het uitvoeren van de beoordeling van de fabrikant en het afgeven van een conformiteitscertificaat voor het CSMS.

6.2. Een aanvraag voor een conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging moet door de voertuigfabrikant of zijn daartoe gemachtigde vertegenwoordiger worden ingediend.

6.3. De aanvraag moet vergezeld gaan van de volgende documenten in drievoud:

6.3.1. documenten waarin het beheersysteem voor cyberbeveiliging wordt beschreven;

6.3.2. een ondertekende verklaring volgens het model in aanhangsel 1 van bijlage 1.

6.4. De fabrikant verklaart in de context van de beoordeling dat hij het in aanhangsel 1 van bijlage 1 bedoelde model gebruikt en toont tot voldoening van de goedkeuringsinstantie of haar technische dienst aan dat hij over de noodzakelijke processen beschikt om aan alle voorschriften inzake cyberbeveiliging te voldoen in overeenstemming met dit reglement.

6.5. Wanneer deze beoordeling naar tevredenheid is afgerond en er een ondertekende verklaring van de fabrikant is ontvangen volgens het in aanhangsel 1 van bijlage 1 bedoelde model, wordt er een conformiteitscertificaat voor het CSMS zoals beschreven in bijlage 4 (hierna "conformiteitscertificaat voor het CSMS") aan de fabrikant afgegeven.

6.6. De goedkeuringsinstantie of haar technische dienst gebruikt voor het conformiteitscertificaat voor het CSMS het in bijlage 4 opgenomen model.

6.7. Het conformiteitscertificaat voor het CSMS blijft maximaal drie jaar na de datum van afgifte van het certificaat geldig, tenzij het wordt ingetrokken.

6.8. De goedkeuringsinstantie die het conformiteitscertificaat voor het CSMS heeft verleend, mag te allen tijde controleren of nog steeds aan de bijbehorende voorschriften wordt voldaan. De goedkeuringsinstantie trekt het conformiteitscertificaat voor het CSMS in indien niet langer aan de in dit reglement vastgestelde eisen wordt voldaan.

([6]) De GRVA zal tijdens zijn zevende bijeenkomst verdere informatie over de minimumvereisten voor het documentatiepakket ontwikkelen.

6.9. De fabrikant brengt de goedkeuringsinstantie of haar technische dienst op de hoogte van eventuele veranderingen die van invloed zijn op de relevantie van het conformiteitscertificaat voor het CSMS. Na raadpleging van de fabrikant besluit de goedkeuringsinstantie of haar technische dienst of er nieuwe controles nodig zijn.

6.10. Fabrikanten vragen tijdig een nieuw certificaat of verlenging van het conformiteitscertificaat voor het CSMS aan om de goedkeuringsinstantie in staat te stellen haar beoordeling af te ronden voordat de geldigheidsduur van het conformiteitscertificaat voor het CSMS verstrijkt. Indien de beoordeling een positief resultaat heeft, geeft de goedkeuringsinstantie een nieuw conformiteitscertificaat voor het CSMS af of verlengt zij de geldigheid ervan voor een nieuwe periode van drie jaar. De goedkeuringsinstantie controleert of het CSMS nog steeds aan de voorschriften van dit reglement voldoet. De goedkeuringsinstantie geeft een nieuw certificaat af wanneer wijzigingen onder de aandacht van de goedkeuringsinstantie of haar technische dienst zijn gebracht en de wijzigingen positief zijn herbeoordeeld.

6.11. Het verstrijken van de geldigheidstermijn of het intrekken van het conformiteitscertificaat voor het CSMS wordt met betrekking tot de voertuigtypen waarop het desbetreffende CSMS van toepassing was, beschouwd als wijziging van de goedkeuring, zoals bedoeld in punt 8, hetgeen intrekking van de goedkeuring tot gevolg kan hebben indien niet langer aan de voorwaarden voor goedkeuring wordt voldaan.

7. Specificaties

7.1. Algemene specificaties

7.1.1. De voorschriften van dit reglement vormen geen beperking van bepalingen of voorschriften van andere VN-reglementen.

7.2. Voorschriften voor het beheersysteem voor cyberbeveiliging

7.2.1. De goedkeuringsinstantie of haar technische dienst moet voor de beoordeling verifiëren of de voertuigfabrikant een beheersysteem voor cyberbeveiliging heeft en of het systeem conform dit reglement is.

7.2.2. Het beheersysteem voor cyberbeveiliging bestrijkt de volgende aspecten:

7.2.2.1. De voertuigfabrikant moet aan een goedkeuringsinstantie of technische dienst bewijzen dat zijn beheersysteem voor cyberbeveiliging van toepassing is op de volgende fasen:

a) de ontwikkelingsfase;

b) de productiefase;

c) de post-productiefase.

7.2.2.2. De voertuigfabrikant moet aantonen dat de processen die in het kader van zijn beheersysteem voor cyberbeveiliging worden gebruikt, ervoor zorgen dat naar behoren rekening wordt gehouden met beveiliging, ook met betrekking tot de in bijlage 5 opgesomde risico's en mitigatiemaatregelen. Dit omvat:

a) de processen die binnen de organisatie van de fabrikant worden gebruikt voor het beheren van cyberbeveiliging;

b) de processen die worden gebruikt voor het vaststellen van risico's voor voertuigtypen. Binnen deze processen worden de in deel A van bijlage 5 genoemde dreigingen en andere relevante dreigingen in aanmerking genomen;

c) de processen die worden gebruikt voor het evalueren, categoriseren en behandelen van de vastgestelde risico's;

d) de bestaande processen om na te gaan of de vastgestelde risico's naar behoren worden beheerd;

e) de processen die worden gebruikt om de cyberbeveiliging van een voertuigtype te testen;

f) de processen die worden gebruikt om ervoor te zorgen dat de risicobeoordeling altijd up-to-date is;

g) de processen die worden gebruikt om cyberaanvallen, cyberdreigingen en zwakheden in voertuigtypen te monitoren, op te sporen en aan te pakken en de processen die worden gebruikt om te beoordelen of de uitgevoerde maatregelen inzake cyberbeveiliging nog doeltreffend zijn in het licht van vastgestelde nieuwe cyberdreigingen en zwakheden;

h) de processen die worden gebruikt om relevante gegevens te verstrekken ter ondersteuning van een analyse van succesvolle cyberaanvallen of pogingen daartoe.

7.2.2.3. De voertuigfabrikant moet aantonen dat de processen die in het kader van zijn beheersysteem voor cyberbeveiliging worden gebruikt, er op basis van de in punt 7.2.2.2, c) en g), bedoelde categorisering voor zorgen dat cyberdreigingen en zwakheden die een reactie van de voertuigfabrikant vereisen, binnen een redelijke termijn worden verminderd.

7.2.2.4. De voertuigfabrikant moet aantonen dat de processen die in het kader van zijn beheersysteem voor cyberbeveiliging worden gebruikt, ervoor zorgen dat de in punt 7.2.2.2, g), bedoelde monitoring voortdurend wordt uitgevoerd. Dit zorgt ervoor dat:

a) voertuigen na de eerste registratie in de monitoring worden opgenomen;

b) de capaciteit om cyberdreigingen, zwakheden en cyberaanvallen te detecteren op basis van voertuiggegevens en logbestanden van voertuigen, en die te analyseren, in aanmerking wordt genomen. Deze capaciteit moet voldoen aan punt 1.3 en de privacyrechten van auto-eigenaren of bestuurders in acht nemen, met name wat betreft toestemming.

7.2.2.5. De voertuigfabrikant is verplicht om aan te tonen hoe met zijn beheersysteem voor cyberbeveiliging de eventuele afhankelijkheid van geselecteerde leveranciers, dienstverleners of suborganisaties van de fabrikant wordt beheerd met betrekking tot de voorschriften van punt 7.2.2.2.

7.3. Voorschriften voor voertuigtypen

7.3.1. De fabrikant moet beschikken over een geldig conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging dat relevant is voor het voertuigtype dat wordt goedgekeurd. Echter geldt voor typegoedkeuringen van voertuigen van de categorieën M, N en O die vóór 1 juli 2024 voor het eerst zijn afgegeven, en voor typegoedkeuringen van voertuigen van categorie L die vóór 1 juli 2029 voor het eerst zijn afgegeven, alsmede voor elke uitbreiding daarvan, dat als de voertuigfabrikant kan bewijzen dat het voertuigtype niet in overeenstemming met het beheersysteem voor cyberbeveiliging kan worden ontwikkeld, de voertuigfabrikant moet aantonen dat er tijdens de ontwikkelingsfase van het betrokken voertuigtype voldoende aandacht aan cyberbeveiliging is besteed.

7.3.2. De voertuigfabrikant moet voor het goed te keuren voertuigtype de risico's in verband met leveranciers identificeren en beheren.

7.3.3. De voertuigfabrikant moet de kritieke elementen van het voertuigtype vaststellen, een uitgebreide risicobeoordeling voor het voertuigtype uitvoeren en de vastgestelde risico's op passende wijze aanpakken. De risicobeoordeling moet betrekking hebben op de afzonderlijke elementen van het voertuigtype en de wisselwerkingen daartussen. In de risicobeoordeling moet bovendien rekening worden gehouden met de wisselwerking met eventuele externe systemen. De voertuigfabrikant moet bij het evalueren van de risico's rekening houden met risico's in verband met alle in deel A van bijlage 5 genoemde dreigingen en met alle overige relevante risico's.

7.3.4. De voertuigfabrikant moet het voertuigtype beschermen tegen de in zijn risicobeoordeling vastgestelde risico's. Voor de bescherming van het voertuigtype moeten evenredige mitigatiemaatregelen worden genomen. De uitgevoerde mitigatiemaatregelen moeten alle in bijlage 5, delen B en C, genoemde mitigatiemaatregelen die relevant zijn voor de vastgestelde risico's omvatten. Wanneer een in deel B of C van bijlage 5 genoemde mitigatiemaatregel echter niet relevant of niet toereikend is voor het vastgestelde risico, moet de voertuigfabrikant een andere passende mitigatiemaatregel uitvoeren.

Met name moet de fabrikant ervoor zorgen dat bij typegoedkeuringen van voertuigen van de categorieën M, N en O die vóór 1 juli 2024 voor het eerst zijn afgegeven, en bij typegoedkeuringen van voertuigen van categorie L die vóór 1 juli 2029 voor het eerst zijn afgegeven, en voor elke uitbreiding daarvan, een andere passende mitigatieregel wordt uitgevoerd, indien een mitigatieregel zoals bedoeld in deel B of C van bijlage 5 technisch niet haalbaar is. De fabrikant moet de respectieve beoordeling van de technische uitvoerbaarheid beschikbaar stellen aan de goedkeuringsinstantie.

7.3.5. De voertuigfabrikant moet passende en evenredige maatregelen nemen om speciale omgevingen (indien geleverd) voor de opslag en uitvoering van aftermarketsoftware, -diensten, -applicaties of -gegevens op het voertuigtype te beveiligen.

7.3.6. De voertuigfabrikant moet voorafgaand aan de typegoedkeuring passende en toereikende tests uitvoeren om de doeltreffendheid van de uitgevoerde beveiligingsmaatregelen te controleren.

7.3.7. De voertuigfabrikant moet maatregelen voor het voertuigtype uitvoeren om:

a) tegen voertuigen van het voertuigtype gerichte cyberaanvallen op te sporen en te voorkomen;

b) de monitoringcapaciteit van de voertuigfabrikant met betrekking tot het opsporen van op het voertuigtype gerichte dreigingen, zwakheden en cyberaanvallen te ondersteunen;

c) forensische capaciteit te verstrekken om de analyse van succesvolle cyberaanvallen of pogingen tot cyberaanvallen mogelijk te maken.

7.3.8. Cryptografische modulen die worden gebruikt voor de toepassing van dit reglement moeten overeenstemmen met op consensus gebaseerde normen. Indien de gebruikte cryptografische modulen niet met op consensus gebaseerde normen overeenstemmen, moet de voertuigfabrikant het gebruik ervan rechtvaardigen.

7.4. Bepalingen inzake verslaglegging

7.4.1. De voertuigfabrikant moet minstens eenmaal per jaar, of vaker indien van toepassing, aan de goedkeuringsinstantie of de technische dienst verslag uitbrengen over het resultaat van zijn monitoringactiviteiten, zoals bepaald in punt 7.2.2.2, g), met inbegrip van relevante informatie over nieuwe cyberaanvallen. De voertuigfabrikant moet daarnaast aan de goedkeuringsinstantie of de technische dienst rapporteren en bevestigen dat de voor zijn voertuigtypen uitgevoerde mitigatiemaatregelen inzake cyberbeveiliging nog steeds doeltreffend zijn en of er aanvullende maatregelen zijn getroffen.

7.4.2. De goedkeuringsinstantie of de technische dienst moet de verstrekte informatie verifiëren en de voertuigfabrikant, indien nodig, verzoeken om eventuele vastgestelde ondoeltreffendheden te herstellen.

Indien de verslaglegging of het antwoord ontoereikend is, kan de goedkeuringsinstantie besluiten het CSMS in te trekken overeenkomstig punt 6.8.

8. Wijziging van het voertuigtype en uitbreiding van de typegoedkeuring

8.1. Elke wijziging van het voertuigtype met gevolgen voor de technische prestaties ervan met betrekking tot cyberbeveiliging en/of de bij dit reglement vereiste documentatie wordt meegedeeld aan de goedkeuringsinstantie die het voertuigtype heeft goedgekeurd. De goedkeuringsinstantie kan dan:

8.1.1. oordelen dat de doorgevoerde wijzigingen nog aan de voorschriften en documentatie van de bestaande typegoedkeuring voldoen, of

8.1.2. een noodzakelijke aanvullende beoordeling uitvoeren overeenkomstig punt 5, en indien van toepassing de technische dienst die verantwoordelijk is voor het uitvoeren van de tests om een nieuw testrapport verzoeken.

8.1.3. De bevestiging, uitbreiding of weigering van de goedkeuring, met vermelding van de wijzigingen, wordt meegedeeld door middel van een mededelingenformulier volgens het model in bijlage 2. De goedkeuringsinstantie die de goedkeuring uitbreidt, moet aan die uitbreiding een volgnummer toekennen en de andere partijen bij de overeenkomst van 1958 die dit reglement toepassen daarvan in kennis stellen door middel van een mededelingenformulier volgens het model in bijlage 2.

9. Conformiteit van de productie

9.1. Voor de controle van de conformiteit van de productie gelden de procedures van aanhangsel 1 van de Overeenkomst van 1958 (E/ECE/TRANS/505/Rev.3), met inachtneming van de volgende bepalingen:

9.1.1. de houder van de goedkeuring ziet erop toe dat de resultaten van de tests met betrekking tot de conformiteit van de productie worden geregistreerd en dat de bijgevoegde documenten beschikbaar blijven gedurende een periode die in overleg met de goedkeuringsinstantie of haar technische dienst wordt vastgesteld. Deze periode bedraagt maximaal 10 jaar gerekend vanaf het ogenblik dat de productie definitief is stopgezet;

9.1.2. De goedkeuringsinstantie die de typegoedkeuring heeft verleend, kan te allen tijde in elk productiebedrijf de aldaar toegepaste methoden voor controle van de conformiteit van de productie verifiëren. Die verificaties vinden gewoonlijk om de drie jaar plaats.

10. Sancties bij non-conformiteit van de productie

10.1. De krachtens dit reglement verleende goedkeuring voor een voertuigtype kan worden ingetrokken indien niet aan de voorschriften van dit reglement is voldaan of indien voertuigen uit de steekproef niet aan de voorschriften van dit reglement voldoen.

10.2. Indien een goedkeuringsinstantie een eerder door haar verleende goedkeuring intrekt, stelt zij de overeenkomstsluitende partijen die dit reglement toepassen daarvan onmiddellijk in kennis door middel van een mededelingenformulier volgens het model in bijlage 2.

11. Definitieve stopzetting van de productie

11.1. Indien de houder van de goedkeuring de productie van een krachtens dit reglement goedgekeurd voertuigtype definitief stopzet, stelt hij de instantie die de goedkeuring heeft verleend daarvan in kennis. Zodra deze instantie de kennisgeving heeft ontvangen, stelt zij de andere overeenkomstsluitende partijen die dit reglement toepassen daarvan in kennis door middel van een kopie van het goedkeuringsformulier met aan het einde in hoofdletters de gedateerde en ondertekende vermelding “PRODUCTIE STOPGEZET”.

12. Naam en adres van de voor de uitvoering van de goedkeuringstest verantwoordelijke technische diensten en van de typegoedkeuringsinstanties

12.1. De overeenkomstsluitende partijen die dit reglement toepassen, moeten het secretariaat van de Verenigde Naties de naam en het adres meedelen van de technische diensten die voor de uitvoering van de goedkeuringstests verantwoordelijk zijn, en van de typegoedkeuringsinstanties die goedkeuring verlenen en waaraan de in andere landen afgegeven certificaten betreffende de goedkeuring of de uitbreiding, weigering of intrekking van de goedkeuring moeten worden toegezonden.

BIJLAGE 1

Inlichtingenformulier

De onderstaande gegevens moeten, voor zover van toepassing, in drievoud worden verstrekt en vergezeld gaan van een inhoudsopgave. Eventuele tekeningen moeten op een passende schaal en met voldoende details, in formaat A4 of tot dat formaat gevouwen, worden ingediend. Op eventuele foto's moeten voldoende details te zien zijn.

1. Merk (handelsnaam van de fabrikant):.....

2. Type en algemene handelsbenaming(en):.....

3. Identificatiemerkteken van het type, indien op het voertuig aangebracht:.....

4. Plaats van dat merkteken:.....

5. Voertuigcategorie(ën):.....

6. Naam en adres van de fabrikant/vertegenwoordiger van de fabrikant:.....

7. Naam en adres van de assemblagefabriek(en):.....

8. Foto's en/of tekeningen van een representatief voertuig:.....

9. Cyberbeveiliging

9.1. Algemene bouwwijze van het voertuigtype, met inbegrip van:

a) de voertuigsystemen die relevant zijn voor de cyberbeveiliging van het voertuigtype;

b) de componenten van de systemen die relevant zijn voor de cyberbeveiliging;

c) de wisselwerkingen van die systemen met andere systemen binnen het voertuigtype en met externe systemen.

9.2. Schematische voorstelling van het voertuigtype

9.3. Het nummer van het conformiteitscertificaat voor het CSMS:.....

9.4. Documenten voor het goed te keuren voertuigtype waarin het resultaat van de risicobeoordeling en de vastgestelde risico's worden beschreven:.....

9.5. Documenten voor het goed te keuren voertuigtype waarin de voor de opgesomde systemen of voor het voertuigtype uitgevoerde mitigatiemaatregelen worden beschreven, evenals de manier waarop de genoemde risico's door die maatregelen worden beperkt:.....

9.6. Documenten voor het goed te keuren voertuigtype waarin de bescherming van speciale omgevingen voor aftermarketsoftware, -diensten, -applicaties of -gegevens wordt beschreven:.....

9.7. Documenten voor het goed te keuren voertuigtype waarin wordt beschreven welke tests er zijn uitgevoerd om de cyberbeveiliging van het voertuigtype en de bijbehorende systemen te verifiëren, evenals de resultaten van die tests:.....

9.8. Beschrijving van de wijze waarop de toeleveringsketen in aanmerking is genomen met betrekking tot cyberbeveiliging:.....

Bijlage 1 - Aanhangsel 1

Model van de verklaring van naleving van de fabrikant voor het CSMS

De verklaring van de fabrikant betreffende naleving van de voorschriften voor het beheersysteem voor cyberbeveiliging

Naam van de fabrikant: ……

Adres van de fabrikant: ……

……(*naam van de fabrikant*)

verklaart dat de noodzakelijke processen om aan de voorschriften voor het beheersysteem voor cyberbeveiliging overeenkomstig punt 7.2 van VN-Reglement nr. 155 te voldoen, zijn geïnstalleerd en zullen worden onderhouden.

Gedaan te: …… (*plaats*)

Datum:……

Naam van de ondertekenaar: ……

Functie van de ondertekenaar: ……

(Stempel en handtekening van de vertegenwoordiger van de fabrikant)

BIJLAGE 2

Mededeling

(Maximaal formaat: A4 (210 × 297 mm))



afgegeven door: Naam van de instantie:
……
……
……

Betreffende de (2): goedkeuring
uitbreiding van de goedkeuring
intrekking van de goedkeuring vanaf dd/mm/jjjj
weigering van de goedkeuring
definitieve stopzetting van de productie

van een voertuigtype krachtens VN-Reglement nr. 155.

Goedkeuring nr.:……

Uitbreiding nr.: ……

Reden van de uitbreiding:……

1. Merk (handelsnaam van de fabrikant):……

2. Type en algemene handelsbenaming(en):……

3. Identificatiemerkteken van het type, indien op het voertuig aangebracht:……

3.1. Plaats van dat merkteken:……

4. Voertuigcategorie(ën): ……

5. Naam en adres van de fabrikant/vertegenwoordiger van de fabrikant: ……

6. Naam en adres van de assemblagefabriek(en):……

7. Nummer van het conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging: ……

8. Technische dienst die verantwoordelijk is voor de uitvoering van de tests: ……

9. Datum van het testrapport:……

10. Nummer van het testrapport: ……

11. Opmerkingen: (indien van toepassing) ……

12. Plaats:……

(1) Nummer van het land dat de goedkeuring heeft verleend/uitgebreid/geweigerd/ingetrokken (zie de goedkeuringsbepalingen van het reglement).
(2) Doorhalen wat niet van toepassing is.

13. Datum: ……

14. Handtekening: ……

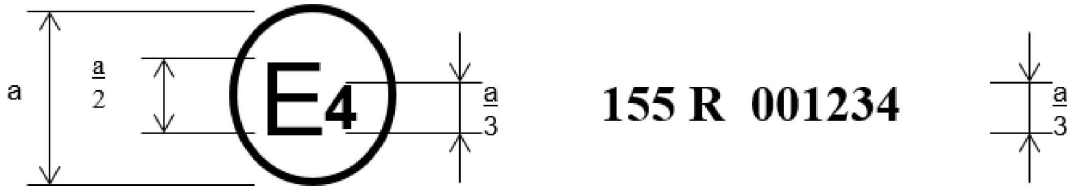
15. De inhoudsopgave van het informatiedossier dat bij de goedkeuringsinstantie is ingediend en dat op verzoek verkrijgbaar is, is bijgevoegd.

BIJLAGE 3

Opstelling van goedkeuringsmerken

MODEL A

(zie punt 4.2 van dit reglement)



a = min. 8 mm

Bovenstaand goedkeuringsmerk, aangebracht op een voertuig, geeft aan dat het wegvoertuigtype in kwestie in Nederland (E4) krachtens Reglement nr. 155 is goedgekeurd onder nummer 001234. De eerste twee cijfers van het goedkeuringsnummer geven aan dat de goedkeuring is verleend volgens de voorschriften van dit reglement in zijn oorspronkelijke vorm (00).

BIJLAGE 4

MODEL VAN HET CONFORMITEITSCERTIFICAAT VOOR HET CSMS

Conformiteitscertificaat voor het beheersysteem voor cyberbeveiliging

met betrekking tot VN-Reglement nr. 155

Certificaatnummer [*referentienummer*]

[……. *goedkeuringsinstantie*]

verklaart dat:

Fabrikant:……

Adres van de fabrikant: ……

voldoet aan de bepalingen van punt 7.2 van Reglement nr. 155

Er werden controles uitgevoerd op:……

door (naam en adres van de goedkeuringsinstantie of de technische dienst): ……

Nummer van het rapport: ……

Het certificaat is geldig tot en met [……*datum*]

Gedaan te […… *plaats*]

Op […… *datum*]

[… *handtekening*] ……

Bijlagen: beschrijving van het beheersysteem voor cyberbeveiliging door de fabrikant.

BIJLAGE 5

Lijst van dreigingen en de overeenkomstige mitigatiemaatregelen

1. Deze bijlage bestaat uit drie delen. In deel A van deze bijlage wordt de referentiesituatie voor dreigingen, kwetsbaarheden en aanvalsmethoden beschreven. In deel B van deze bijlage worden mitigatiemaatregelen voor dreigingen voor voertuigtypen beschreven. In deel C wordt een beschrijving gegeven van de mitigatiemaatregelen voor dreigingen voor gebieden buiten het voertuig, bv. voor IT-backends.

2. Deel A, deel B en deel C worden in aanmerking genomen bij door voertuigfabrikanten uit te voeren risicobeoordelingen en mitigatiemaatregelen.

3. De hoge mate van kwetsbaarheid en de bijbehorende voorbeelden zijn in deel A uitgedrukt in een index. In deel B en deel C wordt verwezen naar dezelfde indexering om elke aanval/kwetsbaarheid te koppelen aan een lijst van overeenkomstige mitigatiemaatregelen.

4. In de dreigingsanalyse wordt ook rekening gehouden met de mogelijke gevolgen van aanvallen. Dit kan helpen de ernst van een risico te bepalen en aanvullende risico's vast te stellen. Mogelijke gevolgen van aanvallen kunnen zijn:

   a) de veilige werking van het voertuig wordt aangetast;

   b) de functies van het voertuig werken niet meer;

   c) software wordt gewijzigd, prestaties nemen af;

   d) software wordt gewijzigd, maar zonder effect op de werking;

   e) inbreuk op de gegevensintegriteit;

   f) schending van de vertrouwelijkheid van gegevens;

   g) verminderde beschikbaarheid van gegevens;

   h) andere, waaronder criminaliteit.

Deel A

Kwetsbaarheid of aanvalsmethode in verband met de dreigingen

Beschrijvingen op hoog niveau van de dreigingen en de daaraan gerelateerde kwetsbaarheid of aanvalsmethode worden gegeven in tabel A1.

Tabel A1

Lijst van kwetsbaarheden of aanvalsmethoden in verband met de dreigingen

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
4.3.1. Dreigingen voor backendservers in verband met voertuigen in het veld	1	Backendservers gebruikt als middel om een voertuig aan te vallen of gegevens op te halen	1.1	Misbruik van rechten door personeel (aanval van binnenuit)
			1.2	Ongeoorloofde internettoegang tot de server (bv. door middel van backdoors, niet-gecorrigeerde kwetsbaarheden in systeemsoftware, SQL-aanvallen of andere middelen)
			1.3	Ongeoorloofde fysieke toegang tot de server (bv. door middel van USB-sticks of andere media die verbinding maken met de server)
	2	Diensten van de backendserver worden onderbroken, met gevolgen voor de werking van een voertuig	2.1	Een aanval op de backendserver zet de werking stop, bijvoorbeeld door te voorkomen dat de server met voertuigen communiceert en diensten levert waarvan deze afhankelijk zijn

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
	3	Op backendservers opgeslagen voertuiggegevens gaan verloren of vallen in verkeerde handen ("gegevenslek")	3.1	Misbruik van rechten door personeel (aanval van binnenuit)
			3.2	Verlies van informatie in de cloud. Gevoelige gegevens kunnen verloren gaan door aanvallen of incidenten wanneer gegevens wordt opgeslagen door externe cloudaanbieders
			3.3	Ongeoorloofde internettoegang tot de server (bv. door middel van backdoors, niet-gecorrigeerde kwetsbaarheden in systeemsoftware, SQL-aanvallen of andere middelen)
			3.4	Ongeoorloofde fysieke toegang tot de server (bv. door middel van USB-sticks of andere media die verbinding maken met de server)
			3.5	Gegevenslek door onbedoeld delen van gegevens (bv. administratieve fouten)
4.3.2 Dreigingen voor voertuigen met betrekking tot hun communicatiekanalen	4	Manipulatie van door het voertuig ontvangen berichten of gegevens	4.1	Manipulatie van berichten door impersonatie (bv. V2X-melding over coöperatief bewustzijn of manoeuvrecoördinatie, GNSS-meldingen enz.)
			4.2	Sybil-aanval (om andere voertuigen te simuleren om te doen alsof er veel andere voertuigen op de weg zijn)
	5	Communicatiekanalen worden gebruikt voor ongeoorloofde manipulatie, verwijdering of andere wijzigingen van de code of gegevens van het voertuig	5.1	Communicatiekanalen staan code-injectie toe; er kan bijvoorbeeld een gemanipuleerde binaire code in de communicatiestroom worden geïnjecteerd
			5.2	Communicatiekanalen staan manipulatie van de gegevens of code van het voertuig toe
			5.3	Communicatiekanalen staan overschrijving van de gegevens of code van het voertuig toe
			5.4	Communicatiekanalen staan uitwissing van de gegevens of code van het voertuig toe
			5.5	Communicatiekanalen staan de invoer van gegevens of de code van het voertuig toe (schrijven van gegevens/code)
	6	Communicatiekanalen staan toe dat onvertrouwde/ onbetrouwbare berichten worden aanvaard of zijn gevoelig voor overneming van sessies/terugspeelaanvallen	6.1	Aanvaarding van informatie uit een onbetrouwbare of onvertrouwde bron
			6.2	Man-in-the-middle-aanval/overneming van sessie
			6.3	Terugspeelaanval, bijvoorbeeld een aanval tegen een communicatiegateway die de aanvaller in staat stelt om software van een ECU of firmware van de gateway te downgraden
	7	Informatie kan eenvoudig openbaar worden gemaakt. Bijvoorbeeld door het afluisteren van communicatie of door ongeoorloofde toegang tot gevoelige bestanden of mappen toe te staan	7.1	Onderschepping van informatie/verstorende straling/monitoring van communicatie
			7.2	Ongeoorloofde toegang tot bestanden of gegevens verkrijgen

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
	8	Denial-of-serviceaanvallen via communicatiekanalen om de voertuigfuncties te verstoren	8.1	Een grote hoeveelheid ongewenste gegevens versturen naar het voertuiginformatiesysteem zodat dit niet op de normale manier kan functioneren
			8.2	Black-hole-aanval, om de communicatie tussen voertuigen te verstoren blokkeert de aanvaller de berichten tussen de voertuigen
	9	Een gebruiker zonder bijzondere rechten kan geprivilegieerde toegang tot voertuigsystemen verkrijgen	9.1	Een gebruiker zonder bijzondere rechten kan geprivilegieerde toegang verkrijgen, zoals root-toegang
	10	Virussen in de communicatiemedia kunnen voertuigsystemen infecteren	10.1	Een virus in de communicatiemedia infecteert voertuigsystemen
	11	Door het voertuig ontvangen berichten (bijvoorbeeld X2V- of diagnoseberichten) of binnen het voertuig doorgegeven berichten bevatten kwaadaardige inhoud	11.1	Kwaadaardige interne (bv. CAN) berichten
			11.2	Kwaadaardige V2X-berichten, bv. berichten van infrastructuur naar het voertuig of tussen voertuigen onderling (bv. CAM, DENM)
			11.3	Kwaadaardige diagnoseberichten
			11.4	Kwaadaardige eigen berichten (bv. die normaal worden verstuurd door OEM of leveranciers van componenten/systemen/functies)
4.3.3. Dreigingen voor voertuigen met betrekking tot hun updateprocedures	12	Misbruik of aantasting van updateprocedures	12.1	Aantasting van draadloze software-updateprocedures. Hiertoe behoort de fabricering van het programma of de firmware voor systeemupdates
			12.2	Aantasting van lokale/fysieke software-updateprocedures. Hiertoe behoort de fabricering van het programma of de firmware voor systeemupdates
			12.3	De software wordt voorafgaand aan het updateproces gemanipuleerd (en raakt daardoor beschadigd), hoewel het updateproces intact is
			12.4	Aantasting van cryptografische sleutels van de softwareleverancier om een ongeldige update mogelijk te maken
	13	Het is mogelijk om legitieme updates te weigeren	13.1	Denial-of-serviceaanval tegen de updateserver of het updatenetwerk om de uitvoering van kritieke software-updates tegen te houden en/of klantspecifieke functies te ontgrendelen
4.3.4. Dreigingen voor voertuigen betreffende onbedoelde menselijke handelingen die een cyberaanval mogelijk maken	15	Legitieme actoren kunnen handelingen uitvoeren die onbewust een cyberaanval zouden vergemakkelijken	15.1	Een onschuldig slachtoffer (bv. eigenaar, gebruiker of onderhoudsmedewerker) wordt er middels een list toe verleid een handeling uit te voeren om onbedoeld malware te downloaden of een aanval mogelijk te maken
			15.2	Vastgestelde beveiligingsprocedures worden niet gevolgd

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
4.3.5. Dreigingen voor voertuigen met betrekking tot hun externe connectiviteit en verbindingen	16	Manipulatie van de connectiviteit van voertuigfuncties maakt een cyberaanval mogelijk, bijvoorbeeld via telematica, systemen die operaties op afstand mogelijk maken en systemen die gebruik maken van draadloze communicatie over korte afstand	16.1	Manipulatie van functies die bedoeld zijn voor het op afstand bedienen van systemen, zoals een afstandsbediening, startonderbreker of laadpaal
			16.2	Manipulatie van de voertuigtelematica (bv. manipuleren van de temperatuurmeting van kwetsbare goederen, op afstand vergrendelen van vrachtdeuren)
			16.3	Interferentie met draadloze kortbereiksystemen of -sensoren
	17	Gebruik van ingebouwde software van derden, bv. entertainmentapplicaties, om voertuigsystemen aan te vallen	17.1	Gebruik van beschadigde applicaties, of applicaties met slecht beveiligde software, om voertuigsystemen aan te vallen
	18	Gebruik van apparaten die met externe interfaces zijn verbonden, zoals USB- of OBD-poort, om voertuigsystemen aan te vallen	18.1	Externe interfaces zoals USB- of andere poorten die als aanvalspunt worden gebruikt, bijvoorbeeld door middel van code-injectie
			18.2	Met een virus geïnfecteerde media die verbonden zijn met een voertuigsysteem
			18.3	Gebruik van een diagnostische toegang (bv. dongles in OBD-poort) om een aanval mogelijk te maken, bv. manipuleren van voertuigparameters (rechtstreeks of onrechtstreeks)
4.3.6. Dreigingen voor voertuiggege-vens/-code	19	Ophalen van voertuiggegevens/-code	19.1	Ophalen uit voertuigsystemen van software waarop auteursrechten of intellectuele-eigendomsrechten van toepassing zijn (productpiraterij)
			19.2	Ongeoorloofde toegang tot de persoonsgegevens van de eigenaar zoals zijn identiteit, betaalrekening, adressenbestand, locatiegegevens, het elektronische identificatienummer van het voertuig enz.
			19.3	Ophalen van cryptografische sleutels
	20	Manipulatie van voertuiggegevens/-code	20.1	Illegale/ongeoorloofde wijzigingen van het elektronische identificatienummer van het voertuig
			20.2	Identiteitsfraude. Als een gebruiker bijvoorbeeld een andere identiteit wil weergeven bij de communicatie met tolsystemen, backendsysteem van de fabrikant
			20.3	Actie om monitoringsystemen te omzeilen (bv. het hacken/manipuleren/blokkeren van berichten zoals gegevens van ODR Tracker, of het aantal ritten)
			20.4	Gegevensmanipulatie om de rijgegevens van een voertuig te vervalsen (bv. kilometerstand, rijsnelheid, routebeschrijving enz.)
			20.5	Ongeoorloofde wijzigingen aan diagnosegegevens van het systeem
	21	Uitwissing van gegevens/code	21.1	Ongeoorloofde verwijdering/manipulatie van gebeurtenissenlogs van het systeem
	22	Introductie van malware	22.2	Introduceren van kwaadaardige software of kwaadaardige softwareactiviteit

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
	23	Introduceren van nieuwe software of overschrijven van bestaande software	23.1	Productie van software van het voertuigcontrolesysteem of -informatiesysteem
	24	Onderbreking van systemen of operaties	24.1	Denial-of-service, dit kan bijvoorbeeld op het interne netwerk worden geactiveerd door een CAN-bus te overspoelen, of door fouten op een ECU te veroorzaken door grote hoeveelheden berichten te versturen
	25	Manipulatie van voertuigparameters	25.1	Ongeoorloofde toegang om de configuratieparameters van belangrijke voertuigfuncties te vervalsen, zoals remgegevens, de drempelwaarde voor de activering van airbags enz.
			25.2	Ongeoorloofde toegang om de laadparameters te vervalsen, zoals laadspanning, laadvermogen, accutemperatuur enz.
4.3.7. Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt	26	Cryptografische technologieën kunnen beschadigd raken of worden onvoldoende toegepast	26.1	Combinatie van korte cryptografische sleutels met een lange geldigheidsduur stellen de aanvaller in staat de versleuteling te kraken
			26.2	Ontoereikend gebruik van cryptografische algoritmen om gevoelige systemen te beschermen
			26.3	Gebruik van reeds of bijna verouderde cryptografische algoritmen
	27	Onderdelen of leveringen zouden beschadigd kunnen worden om ervoor te zorgen dat voertuigen kunnen worden aangevallen	27.1	Hardware of software die wordt aangepast om een aanval mogelijk te maken of die niet voldoet aan de ontwerpcriteria om een aanval tegen te houden
	28	Het ontwerp van software of hardware is de oorzaak van kwetsbaarheden	28.1	Softwarefouten. De aanwezigheid van softwarefouten kan de oorzaak zijn van kwetsbaarheden die kunnen worden uitgebuit. Dit is met name het geval wanneer software niet getest is om te controleren of er geen bekende verkeerde codes/fouten in zitten en om het risico van onbekende verkeerde codes/fouten te beperken
			28.2	Het gebruik van overblijfselen van de ontwikkelingsfase (bv. debug-poorten, JTAG-poorten, microprocessors, ontwikkelingscertificaten, wachtwoorden van ontwikkelaars, …) kan aanvallers toegang tot ECU's geven of hen in staat stellen hogere rechten te verkrijgen
	29	Het ontwerp van het netwerk zorgt voor kwetsbaarheden	29.1	Overbodige poorten die nog open staan en toegang bieden tot netwerksystemen
			29.2	Netwerkscheiding omzeilen om deze onder controle te krijgen. Een specifiek voorbeeld is het gebruik van onbeschermde gateways of toegangspunten (zoals gateways voor vrachtwagens met aanhangwagen) om beschermingen te omzeilen en toegang te verkrijgen tot andere netwerksegmenten om kwaadaardige handelingen uit te voeren, zoals het versturen van willekeurige berichten via de CAN-bus
	31	Er kan onbedoelde gegevensoverdracht plaatsvinden	31.1	Informatielek. Er kunnen persoonsgegevens worden gelekt wanneer het voertuig van eigenaar wisselt (bv. wanneer het wordt verkocht of als huurauto wordt gebruikt met nieuwe huurders)

Beschrijvingen op hoog en middelhoog niveau van de kwetsbaarheid/dreiging			Voorbeeld van de kwetsbaarheid of aanvalsmethode	
	32	Fysieke manipulatie van systemen kan een aanval mogelijk maken	32.1	De manipulatie van elektronische hardware; er wordt bijvoorbeeld ongeoorloofde elektronische hardware aan een voertuig toegevoegd om een "man-in-the-middle"-aanval mogelijk te maken Het vervangen van toegestane elektrische hardware (bv. sensoren) door ongeoorloofde elektronische hardware Manipulatie van de door een sensor verzamelde informatie (bijvoorbeeld het gebruik van een magneet om de aan de versnellingsbak gekoppelde Hall-effectsensor te manipuleren)

Deel B.

Mitigatiemaatregelen voor de dreigingen voor voertuigen

1. Mitigatiemaatregelen voor "Communicatiekanalen van voertuigen"

De mitigatiemaatregelen voor dreigingen in verband met "Communicatiekanalen van voertuigen" worden vermeld in tabel B1.

Tabel B1

Mitigatiemaatregel voor dreigingen in verband met "Communicatiekanalen van voertuigen"

Referentie tabel A1	Dreigingen voor "Communicatiekanalen van voertuigen"	Ref.	Mitigatiemaatregel
4.1	Manipulatie van berichten door impersonatie (bv. V2X-melding over coöperatief bewustzijn of manoeuvrecoördinatie, GNSS-meldingen enz.)	M10	Het voertuig verifieert de authenticiteit en integriteit van de berichten die het ontvangt
4.2	Sybil-aanval (om andere voertuigen te simuleren om te doen alsof er veel andere voertuigen op de weg zijn)	M11	Er moeten beveiligingscontroles worden uitgevoerd voor het opslaan van cryptografische sleutels (bv. met behulp van hardwarebeveiligingsmodulen)
5.1	Communicatiekanalen staan code-injectie in de gegevens of code van het voertuig toe; er kan bijvoorbeeld een gemanipuleerde binaire code in de communicatiestroom worden geïnjecteerd	M10 M6	Het voertuig verifieert de authenticiteit en integriteit van de berichten die het ontvangt Om de risico's te beperken, moet bij het ontwerp van systemen rekening worden gehouden met beveiliging
5.2	Communicatiekanalen staan manipulatie van de gegevens of code van het voertuig toe	M7	Om de gegevens/code van het systeem te beschermen, moeten er technieken en ontwerpen voor toegangscontrole worden toegepast
5.3	Communicatiekanalen staan overschrijving van de gegevens of code van het voertuig toe		
5.4 21.1	Communicatiekanalen staan uitwissing van de gegevens of code van het voertuig toe		
5.5	Communicatiekanalen staan de invoer van gegevens of code in voertuigsystemen toe (schrijven van gegevens/code)		

Referentie tabel A1	Dreigingen voor "Communicatiekanalen van voertuigen"	Ref.	Mitigatiemaatregel
6.1	Aanvaarding van informatie uit een onbetrouwbare of onvertrouwde bron	M10	Het voertuig verifieert de authenticiteit en integriteit van de berichten die het ontvangt
6.2	Man-in-the-middle-aanval/overneming van sessie	M10	Het voertuig verifieert de authenticiteit en integriteit van de berichten die het ontvangt
6.3	Terugspeelaanval, bijvoorbeeld een aanval tegen een communicatiegateway die de aanvaller in staat stelt om software van een ECU of firmware van de gateway te downgraden		
7.1	Onderschepping van informatie/ verstorende straling/monitoring van communicatie	M12	Vertrouwelijke gegevens die van of naar het voertuig worden gestuurd, worden beveiligd
7.2	Ongeoorloofde toegang tot bestanden of gegevens verkrijgen	M8	Het ontwerp van het systeem en toegangscontrole moeten ervoor zorgen dat onbevoegde personen niet bij persoonsgegevens of kritieke systeemgegevens kunnen komen. Zie OWASP voor een voorbeeld van beveiligingscontroles
8.1	Een grote hoeveelheid ongewenste gegevens versturen naar het voertuiginformatiesysteem zodat dit niet op de normale manier kan functioneren	M13	Er worden maatregelen uitgevoerd om een denial-of-service-aanval te detecteren en ervan te herstellen
8.2	Black-hole-aanval, verstoring van de communicatie tussen voertuigen door overdracht van berichten naar andere voertuigen te blokkeren	M13	Er worden maatregelen uitgevoerd om een denial-of-service-aanval te detecteren en ervan te herstellen
9.1	Een gebruiker zonder bijzondere rechten kan geprivilegieerde toegang verkrijgen, zoals root-toegang	M9	Er worden maatregelen toegepast om ongeoorloofde toegang te voorkomen en op te sporen
10.1	Een virus in de communicatiemedia infecteert voertuigsystemen	M14	Er moeten maatregelen om systemen tegen ingebouwde virussen/malware te beschermen, worden overwogen
11.1	Kwaadaardige interne (bv. CAN) berichten	M15	Er moeten maatregelen om kwaadaardige interne berichten of activiteit op te sporen, worden overwogen
11.2	Kwaadaardige V2X-berichten, bv. berichten van infrastructuur naar het voertuig of tussen voertuigen onderling (bv. CAM, DENM)	M10	Het voertuig verifieert de authenticiteit en integriteit van de berichten die het ontvangt
11.3	Kwaadaardige diagnoseberichten		
11.4	Kwaadaardige eigen berichten (bv. die normaal worden verstuurd door OEM of leveranciers van componenten/ systemen/functies)		

2. Mitigatiemaatregelen voor “Updateproces”

De mitigatiemaatregelen voor dreigingen in verband met “Updateproces” worden vermeld in tabel B2.

Tabel B2

Mitigatiemaatregel voor dreigingen in verband met “Updateproces”

Referentie tabel A1	Dreigingen voor “Updateproces”	Ref.	Mitigatiemaatregel
12.1	Aantasting van draadloze software-updateprocedures. Hiertoe behoort de fabricering van het programma of de firmware voor systeemupdates	M16	Er moeten beveiligde procedures voor het updaten van software worden gebruikt
12.2	Aantasting van lokale/fysieke software-updateprocedures. Hiertoe behoort de fabricering van het programma of de firmware voor systeemupdates		
12.3	De software wordt voorafgaand aan het updateproces gemanipuleerd (en raakt daardoor beschadigd), hoewel het updateproces intact is		
12.4	Aantasting van cryptografische sleutels van de softwareleverancier om een ongeldige update mogelijk te maken	M11	Voor het opslaan van cryptografische sleutels worden beveiligingscontroles uitgevoerd
13.1	Denial-of-serviceaanval tegen de updateserver of het updatenetwerk om de uitvoering van kritieke software-updates tegen te houden en/of klantspecifieke functies te ontgrendelen	M3	Er worden beveiligingscontroles uitgevoerd voor backendsystemen. Wanneer backendservers kritiek zijn voor het verlenen van diensten zijn er herstelmaatregelen voor het geval het systeem uitvalt. Zie OWASP voor een voorbeeld van beveiligingscontroles

3. Mitigatiemaatregelen voor “Onbedoelde menselijke handelingen die een cyberaanval mogelijk maken”

De mitigatiemaatregelen voor dreigingen in verband met “Onbedoelde menselijke handelingen die een cyberaanval mogelijk maken” worden vermeld in tabel B3.

Tabel B3

Mitigatiemaatregelen voor dreigingen in verband met “Onbedoelde menselijke handelingen die een cyberaanval mogelijk maken”

Referentie tabel A1	Dreigingen in verband met “Onbedoelde menselijke handelingen”	Ref.	Mitigatiemaatregel
15.1	Een onschuldig slachtoffer (bv. eigenaar, gebruiker of onderhoudsmedewerker) wordt er middels een list toe verleid een handeling uit te voeren om onbedoeld malware te downloaden of een aanval mogelijk te maken	M18	Er moeten maatregelen om gebruikersrollen en toegangsrechten vast te stellen en te controleren, worden uitgevoerd volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend

Referentie tabel A1	Dreigingen in verband met "Onbedoelde menselijke handelingen"	Ref.	Mitigatiemaatregel
15.2	Vastgestelde beveiligingsprocedures worden niet gevolgd	M19	Organisaties zien erop toe dat er beveiligingsprocedures worden vastgesteld en gevolgd, waaronder het bijhouden van handelingen en toegang in verband met het beheer van de beveiligingsfuncties

4. Mitigatiemaatregelen voor "Externe connectiviteit en verbindingen"

De mitigatiemaatregelen voor dreigingen in verband met "Externe connectiviteit en verbindingen" worden vermeld in tabel B4.

Tabel B4

Mitigatiemaatregel voor dreigingen in verband met "Externe connectiviteit en verbindingen"

Referentie tabel A1	Dreigingen voor "Externe connectiviteit en verbindingen"	Ref.	Mitigatiemaatregel
16.1	Manipulatie van functies die bedoeld zijn voor het op afstand bedienen van voertuigsystemen, zoals een sleutel met afstandsbediening, startonderbreker of laadpaal	M20	Er worden beveiligingscontroles uitgevoerd op systemen waartoe op afstand toegang kan worden verkregen
16.2	Manipulatie van de voertuigtelematica (bv. manipuleren van de temperatuurmeting van kwetsbare goederen, op afstand vergrendelen van vrachtdeuren)		
16.3	Interferentie met draadloze kortbereiksystemen of -sensoren		
17.1	Gebruik van beschadigde applicaties, of applicaties met slecht beveiligde software, om voertuigsystemen aan te vallen	M21	Voor softwareprogramma's moet een beveiligingsevaluatie en authenticatie worden uitgevoerd en de integriteit ervan moet worden beschermd. Er moeten beveiligingscontroles worden uitgevoerd om het risico van software van derden die bedoeld is om in het voertuig te worden geïnstalleerd, of dat waarschijnlijk zal worden, tot een minimum te beperken
18.1	Externe interfaces zoals USB- of andere poorten die als aanvalspunt worden gebruikt, bijvoorbeeld door middel van code-injectie	M22	Er worden beveiligingscontroles uitgevoerd voor externe interfaces
18.2	Met virussen geïnfecteerde media die verbonden zijn met het voertuig		
18.3	Gebruik van een diagnostische toegang (bv. dongles in OBD-poort) om een aanval mogelijk te maken, bv. manipuleren van voertuigparameters (rechtstreeks of onrechtstreeks)	M22	Er worden beveiligingscontroles uitgevoerd voor externe interfaces

5. Mitigatiemaatregelen voor “Potentiële doelen van of redenen voor een aanval”

De mitigatiemaatregelen voor dreigingen in verband met “Potentiële doelen van of redenen voor een aanval” worden vermeld in tabel B5.

Tabel B5

Mitigatiemaatregelen voor dreigingen in verband met “Potentiële doelen van of redenen voor een aanval”

Referentie tabel A1	Dreigingen voor “Potentiële doelen van of redenen voor een aanval”	Ref.	Mitigatiemaatregel
19.1	Ophalen uit voertuigsystemen van software waarop auteursrechten of intellectuele-eigendomsrechten van toepassing zijn (productpiraterij/gestolen software)	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles
19.2	Ongeoorloofde toegang tot de persoonsgegevens van de eigenaar zoals zijn identiteit, betaalrekening, adressenbestand, locatiegegevens, het elektronische identificatienummer van het voertuig enz.	M8	Het ontwerp van het systeem en toegangscontrole moeten ervoor zorgen dat onbevoegde personen niet bij persoonsgegevens of kritieke systeemgegevens kunnen komen. Zie OWASP voor een voorbeeld van beveiligingscontroles
19.3	Ophalen van cryptografische sleutels	M11	Er moeten beveiligingscontroles worden uitgevoerd voor het opslaan van cryptografische sleutels, bv. beveiligingsmodulen
20.1	Illegale/ongeoorloofde wijzigingen van het elektronische identificatienummer van het voertuig	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles
20.2	Identiteitsfraude. Als een gebruiker bijvoorbeeld een andere identiteit wil weergeven bij de communicatie met tolsystemen, backendsysteem van de fabrikant		
20.3	Actie om monitoringsystemen te omzeilen (bv. het hacken/manipuleren/blokkeren van berichten zoals gegevens van ODR Tracker, of het aantal ritten)	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles. Aanvallen met gegevensmanipulatie op sensoren of overgedragen gegevens zouden kunnen worden tegengegaan door de gegevens uit verschillende informatiebronnen naast elkaar te leggen
20.4	Gegevensmanipulatie om de rijgegevens van een voertuig te vervalsen (bv. kilometerstand, rijsnelheid, routebeschrijving enz.)		
20.5	Ongeoorloofde wijzigingen aan diagnosegegevens van het systeem		
21.1	Ongeoorloofde verwijdering/manipulatie van gebeurtenissenlogs van het systeem	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles.
22.2	Introduceren van kwaadaardige software of kwaadaardige softwareactiviteit	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles.
23.1	Productie van software van het voertuigcontrolesysteem of -informatiesysteem		

Referentie tabel A1	Dreigingen voor "Potentiële doelen van of redenen voor een aanval"	Ref.	Mitigatiemaatregel
24.1	Denial-of-service, dit kan bijvoorbeeld op het interne netwerk worden geactiveerd door een CAN-bus te overspoelen, of door fouten op een ECU te veroorzaken door grote hoeveelheden berichten te versturen	M13	Er worden maatregelen uitgevoerd om een denial-of-service-aanval te detecteren en ervan te herstellen
25.1	Ongeoorloofde toegang om configuratieparameters van belangrijke voertuigfuncties te vervalsen, zoals remgegevens, de drempelwaarde voor de activering van airbags enz.	M7	Om de gegevens/code van het systeem te beschermen moeten technieken en ontwerpen voor toegangscontrole worden toegepast. Zie OWASP voor een voorbeeld van beveiligingscontroles
25.2	Ongeoorloofde toegang om laadparameters te vervalsen, zoals laadspanning, laadvermogen, accutemperatuur enz.		

6. Mitigatiemaatregelen voor "Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt"

De mitigatiemaatregelen voor dreigingen in verband met "Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt" worden vermeld in tabel B6.

Tabel B6

Mitigatiemaatregelen voor de dreigingen in verband met "Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt"

Referentie tabel A1	Dreigingen voor "Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt"	Ref.	Mitigatiemaatregel
26.1	Combinatie van korte cryptografische sleutels met een lange geldigheidsduur stellen de aanvaller in staat de versleuteling te kraken	M23	De beste praktijken inzake cyberbeveiliging voor de ontwikkeling van software en hardware worden gevolgd
26.2	Ontoereikend gebruik van cryptografische algoritmen om gevoelige systemen te beschermen		
26.3	Gebruik van verouderde cryptografische algoritmen		
27.1	Hardware of software die wordt aangepast om een aanval mogelijk te maken of om niet te voldoen aan de ontwerpcriteria om een aanval tegen te houden	M23	De beste praktijken inzake cyberbeveiliging voor de ontwikkeling van software en hardware worden gevolgd
28.1	De aanwezigheid van softwarefouten kan de oorzaak zijn van kwetsbaarheden die kunnen worden uitgebuit. Dit is met name het geval wanneer software niet getest is om te controleren of er geen bekende verkeerde codes/fouten in zitten en om het risico van onbekende verkeerde codes/fouten te beperken	M23	De beste praktijken inzake cyberbeveiliging voor de ontwikkeling van software en hardware worden gevolgd. De controles met betrekking tot cyberbeveiliging moeten voldoende uitgebreid zijn

Referentie tabel A1	Dreigingen voor "Potentiële kwetsbaarheden die zouden kunnen worden uitgebuit wanneer deze onvoldoende worden beschermd of beperkt"	Ref.	Mitigatiemaatregel
28.2	Het gebruik van overblijfselen van de ontwikkelingsfase (bv. debug-poorten, JTAG-poorten, microprocessors, ontwikkelingscertificaten, wachtwoorden van ontwikkelaars…) kan een aanvallers toegang tot ECU's geven of hen in staat stellen hogere rechten te verkrijgen		
29.1	Overbodige poorten die nog open staan en toegang bieden tot netwerksystemen		
29.2	Netwerkscheiding omzeilen om deze onder controle te krijgen. Een specifiek voorbeeld is het gebruik van onbeschermde gateways of toegangspunten (zoals gateways voor vrachtwagens met aanhangwagen) om beschermingen te omzeilen en toegang te verkrijgen tot andere netwerksegmenten om kwaadaardige handelingen uit te voeren, zoals het versturen van willekeurige berichten via de CAN-bus	M23	De beste praktijken inzake cyberbeveiliging voor de ontwikkeling van software en hardware worden gevolgd. De beste praktijken inzake cyberbeveiliging voor het ontwerp en de integratie van een systeem worden gevolgd

7. Mitigatiemaatregelen voor "Verlies/schending van voertuiggegevens"

De mitigatiemaatregelen voor dreigingen in verband met "Verlies/schending van voertuiggegevens" worden vermeld in tabel B7.

Tabel B7

Mitigatiemaatregelen voor dreigingen in verband met "Verlies/schending van voertuiggegevens"

Referentie tabel A1	Dreigingen voor "Verlies/schending van voertuiggegevens"	Ref.	Mitigatiemaatregel
31.1	Informatielek. Er kunnen persoonsgegevens worden geschonden wanneer het voertuig van eigenaar wisselt (bv. wanneer het wordt verkocht of als huurauto wordt gebruikt door nieuwe huurders)	M24	Voor het opslaan van persoonsgegevens worden de beste praktijken voor de bescherming van de integriteit en vertrouwelijkheid van gegevens gevolgd.

8. Mitigatiemaatregelen voor "Fysieke manipulatie van systemen om een aanval mogelijk te maken"

De mitigatiemaatregelen voor dreigingen in verband met "Fysieke manipulatie van systemen om een aanval mogelijk te maken" worden vermeld in tabel B8.

Tabel B8

Mitigatiemaatregelen voor dreigingen in verband met "Fysieke manipulatie van systemen om een aanval mogelijk te maken"

Referentie tabel A1	Dreigingen voor "Fysieke manipulatie van systemen om een aanval mogelijk te maken"	Ref.	Mitigatiemaatregel
32.1	De manipulatie van OEM-hardware, bijvoorbeeld ongeoorloofde hardware die aan een voertuig is toegevoegd om een "man-in-the-middle"-aanval mogelijk te maken	M9	Er worden maatregelen toegepast om ongeoorloofde toegang te voorkomen en op te sporen

DEEL C.

Mitigatiemaatregelen voor de dreigingen buiten voertuigen

1. Mitigatiemaatregelen voor “Backendservers”

De mitigatiemaatregelen voor dreigingen in verband met “Backendservers” worden vermeld in tabel C1.

Tabel C1

Mitigatiemaatregel voor dreigingen in verband met “Backendservers”

Referentie tabel A1	Dreigingen voor “Backendservers”	Ref.	Mitigatiemaatregel
1.1 & 3.1	Misbruik van rechten door personeel (aanval van binnenuit)	M1	Er worden beveiligingscontroles uitgevoerd op backendsystemen om het risico van aanvallen van binnenuit tot een minimum te beperken
1.2 & 3.3	Ongeoorloofde internettoegang tot de server (bv. door middel van backdoors, niet-gecorrigeerde kwetsbaarheden in systeemsoftware, SQL-aanvallen of andere middelen)	M2	Er worden beveiligingscontroles uitgevoerd op backendsystemen om ongeoorloofde toegang tot een minimum te beperken Zie OWASP voor een voorbeeld van beveiligingscontroles
1.3 & 3.4	Ongeoorloofde fysieke toegang tot de server (bv. door middel van USB-sticks of andere media die verbinding maken met de server)	M8	Het ontwerp van het systeem en toegangscontrole moeten ervoor zorgen dat onbevoegde personen niet bij persoonsgegevens of kritieke systeemgegevens kunnen komen
2.1	Een aanval op de backendserver zet de werking stop, bijvoorbeeld door te voorkomen dat de server met voertuigen communiceert en diensten levert waarvan deze afhankelijk zijn	M3	Er worden beveiligingscontroles uitgevoerd voor backendsystemen. Wanneer backendservers kritiek zijn voor het verlenen van diensten zijn er herstelmaatregelen voor het geval het systeem uitvalt. Zie OWASP voor een voorbeeld van beveiligingscontroles
3.2	Verlies van informatie in de cloud. Gevoelige gegevens kunnen verloren gaan door aanvallen of incidenten wanneer gegevens wordt opgeslagen door externe cloudaanbieders	M4	Er worden beveiligingscontroles uitgevoerd om de risico’s in verband met cloudcomputing tot een minimum te beperken. Zie OWASP en NCSC met richtsnoeren voor cloudcomputing voor een voorbeeld van beveiligingscontroles
3.5	Informatielek door onbedoeld delen van gegevens (bv. administratieve fouten, gegevens opgeslagen op servers in garages)	M5	Er worden beveiligingscontroles uitgevoerd op backendsystemen om gegevenslekken te voorkomen. Zie OWASP voor een voorbeeld van beveiligingscontroles

2. Mitigatiemaatregelen voor “Onbedoelde menselijke handelingen”

De mitigatiemaatregelen voor dreigingen in verband met “Onbedoelde menselijke handelingen” worden vermeld in tabel C2.

Tabel C2

Mitigatiemaatregel voor dreigingen in verband met "Onbedoelde menselijke handelingen"

Referentie tabel A1	Dreigingen in verband met "Onbedoelde menselijke handelingen"	Ref.	Mitigatiemaatregel
15.1	Een onschuldig slachtoffer (bv. eigenaar, gebruiker of onderhoudsmedewerker) wordt er middels een list toe verleid een handeling uit te voeren om onbedoeld malware te downloaden of een aanval mogelijk te maken	M18	Er moeten maatregelen om gebruikersrollen en toegangsrechten vast te stellen en te controleren, worden uitgevoerd volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend
15.2	Vastgestelde beveiligingsprocedures worden niet gevolgd	M19	Organisaties zien erop toe dat er beveiligingsprocedures worden vastgesteld en gevolgd, waaronder het bijhouden van handelingen en toegang in verband met het beheer van de beveiligingsfuncties

3. Mitigatiemaatregelen voor "Fysiek gegevensverlies"

De mitigatiemaatregelen voor dreigingen in verband met "Fysiek gegevensverlies" worden vermeld in tabel C3.

Tabel C3

Mitigatiemaatregelen voor dreigingen in verband met "Fysiek gegevensverlies"

Referentie tabel A1	Dreigingen voor "Fysiek gegevensverlies"	Ref.	Mitigatiemaatregel
30.1	Door derden veroorzaakte schade. Gevoelige gegevens kunnen door materiële schade verloren gaan of beschadigd raken in geval van een verkeersongeval of diefstal	M24	Voor het opslaan van persoonsgegevens worden de beste praktijken voor de bescherming van de integriteit en vertrouwelijkheid van gegevens gevolgd. Zie ISO/SC27/WG5 voor een voorbeeld van beveiligingscontroles
30.2	Verlies als gevolg van conflicten inzake DRM (beheer van digitale rechten). Gebruikersgegevens kunnen worden verwijderd als gevolg van DRM-kwesties		
30.3	Gevoelige gegevens (of de integriteit ervan) kunnen verloren gaan als gevolg van slijtage van IT-componenten, wat een opeenstapeling van problemen kan veroorzaken (bijvoorbeeld bij wijziging van sleutels)		