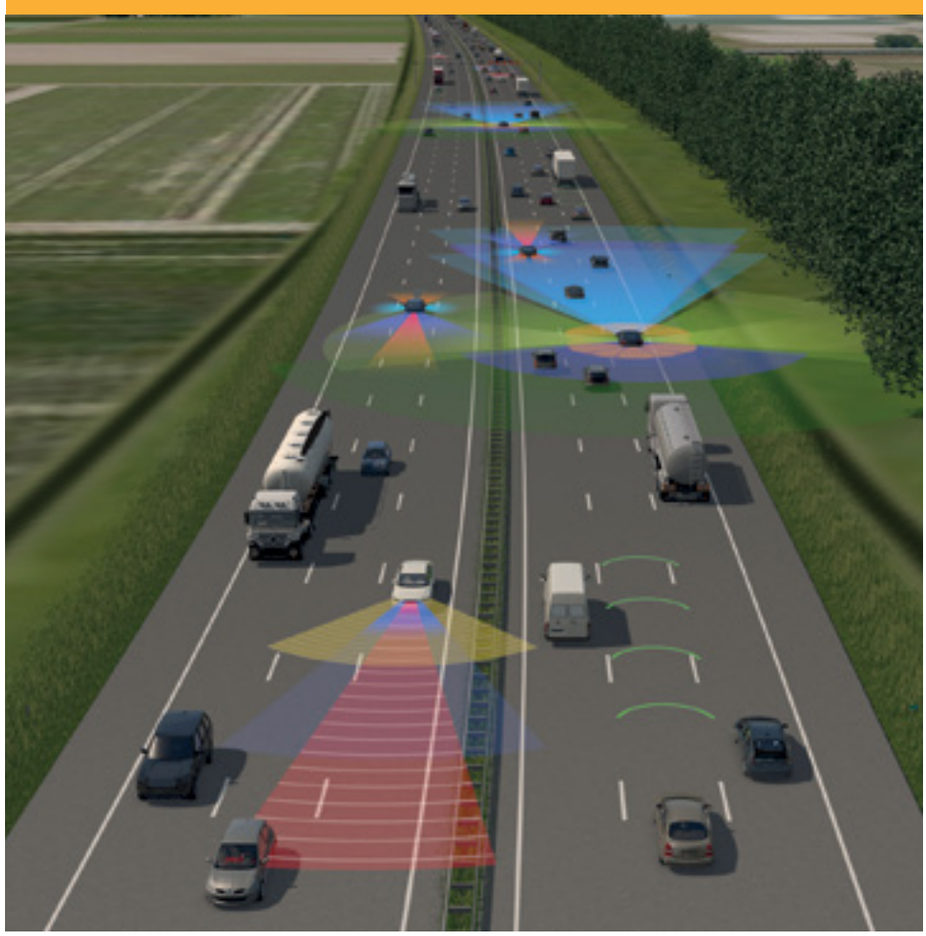
ONDERZOEKSRAAD VOOR VEILIGHEID

Wie stuurt?

Verkeersveiligheid en automatisering in het wegverkeer



Wie stuurt?

Verkeersveiligheid en automatisering in het wegverkeer

Den Haag, november 2019

Foto cover: Onderzoeksraad voor Veiligheid

De rapporten van de Onderzoeksraad voor Veiligheid zijn openbaar en te vinden op onderzoeksraad.nl.

De Onderzoeksraad voor Veiligheid

Als zich een ongeval of ramp voordoet, onderzoekt de Onderzoeksraad voor Veiligheid hoe dat heeft kunnen gebeuren, met als doel daar lessen uit te trekken. Op die manier draagt de Onderzoeksraad bij aan het verbeteren van de veiligheid in Nederland. De Raad is onafhankelijk en besluit zelf welke voorvallen hij onderzoekt. Daarbij richt de Raad zich in het bijzonder op situaties waarin mensen voor hun veiligheid afhankelijk zijn van derden, bijvoorbeeld van de overheid of bedrijven. In een aantal gevallen is de Raad verplicht onderzoek te doen. De onderzoeken gaan niet in op schuld of aansprakelijkheid.

Onderzoeksraad

Voorzitter: ir. J.R.V.A. Dijsselbloem
prof. dr. ir. M.B.A. van Asselt
prof. dr. mr. S. Zouridis

Secretaris-directeur: mr. C.A.J.F. Verheij

Bezoekadres: Lange Voorhout 9
2514 EA Den Haag

Postadres: Postbus 95404
2509 CK Den Haag

Telefoon: 070 333 7000

Website: onderzoeksraad.nl
E-mail: info@onderzoeksraad.nl

INHOUD

Veiligere auto's door innovatie

De geschiedenis van de auto is er een van technologische innovatie. Auto's zijn daardoor in de loop der tijd steeds betrouwbaarder, comfortabeler en veiliger geworden. Mede dankzij technologische vernieuwingen zoals de kreukelzone en de airbag is de verkeersveiligheid sinds de jaren zeventig drastisch verbeterd. De laatste jaren stagneert de verbetering van de verkeersveiligheid: jaarlijks vallen er in Nederland meer dan 600 verkeersdoden en ongeveer 21.000 zwaargewonden. Tegenover deze zorgwekkende situatie staat de ambitie van de overheid – nationaal en Europees – van 'nul doden' in het wegverkeer in het jaar 2050, te beginnen met een daling naar maximaal 500 doden in 2020. De verwachting is dat innovatie – meer specifiek automatisering – hier opnieuw aan kan bijdragen, door de toepassing van rijhulpsystemen (kortweg ADAS) zoals een noodremsysteem en adaptieve cruise control.

Fundamentele karakterverandering van de auto

Het is van belang te beseffen dat auto's met ADAS die nu nieuw op de weg komen, technisch onvergelijkbaar zijn met hun voorgangers van enkele decennia geleden. Nieuwe auto's kunnen nu al veel handelingen van de bestuurder overnemen: sturen, remmen, gas geven. En deze handelingen verrichten de ADAS op basis van eigen waarnemingen en eigen beslissingen, vastgelegd in algoritmes. Dergelijke voertuigen zijn voorzien van zoveel hardware en software dat ze inmiddels rijdende computers zijn. Dit heeft ingrijpende consequenties voor bestuurders, andere weggebruikers en de infrastructuur. Het impliceert in feite een fundamentele karakterverandering van de auto: een transformatie die, zoals iedere innovatie, naast vooruitgang ook nieuwe veiligheidsrisico's met zich meebrengt.

Autorijden wordt makkelijker en moeilijker tegelijkertijd

Door automatisering worden relatief makkelijke taken uit handen genomen en op een constant en hoger veiligheidsniveau uitgevoerd. De moeilijke taken (vooralsnog te complex om te automatiseren) blijven over voor de mens. Automatisering verandert de menselijke taak doordat de automobilist 'continu alert' moet blijven voor het geval de computer het niet meer weet of verkeerd ingrijpt. Dit is extra moeilijk doordat automatisering de alertheid juist verlaagt. De bestuurder moet in luttele secondes beseffen dat ingrijpen nodig is en vervolgens ook adequaat reageren. In het wegverkeer is immers weinig marge. Dit leidt tot de paradoxale situatie dat ADAS die bedoeld waren om de automobilist te ontlasten, de taak op dit punt juist verzwaren.

Zelfrijdende auto is verre toekomst

Als het gaat over automatisering van auto's gaat het vaak over het toekomstbeeld van de zelfrijdende auto, waar de bestuurder overbodig is geworden. De auto rijdt terwijl de inzittenden zich met iets anders bezighouden. Deze verre toekomst spreekt tot de verbeelding van beleidsmakers, technici, stedelijke planners en filosofen. Zo ver is het echter nog lang niet. Zeker in de bebouwde kom, waar auto's en kwetsbare verkeersdeelnemers elkaar ontmoeten, is een toekomst met volledig zelfrijdende auto's nog ver weg, als het ooit zo ver komt.

Aandacht nodig voor de huidige hybride situatie

We bevinden ons nu en de komende jaren in een hybride situatie, waarin zowel de machine als de mens sturen. Deze combinatie is risicovol vanwege de toegenomen interactie tussen mens en voertuig, die bovendien per type ADAS kan verschillen en in de tijd kan veranderen door updates van de software. In een auto voorzien van ADAS is de bestuurder niet meer continu actief aan het rijden, maar heeft hij meer de rol van 'procesbewaker'. Soms verrast het systeem de bestuurder met ingrepen of juist het uitblijven van ingrepen. 'Wie stuurt?' is dan letterlijk een vraag van levensbelang.

Op weg naar maatschappelijk verantwoord innoveren

Auto-industrie, overheden en experts gaan 'fast forward' naar de verre toekomst van de zelfrijdende auto. Om grip te krijgen op de huidige hybride situatie is het noodzakelijk dat de autobranche een omslag maakt naar maatschappelijk verantwoord innoveren. Centraal moet staan dat innovatie de verkeersveiligheid aantoonbaar verbetert. Dit betekent dat fabrikanten risico's inventariseren van nieuwe innovaties en dat zij daar open over zijn. Daarbij moeten fabrikanten meer oog krijgen voor de rol van de mens en de wisselwerking tussen mens en machine. Verder dient het lerend vermogen van de sector te worden verbeterd door te leren van incidenten en ongevallen en door ervaringen van gebruikers actief te betrekken in de verdere ontwikkeling. De Onderzoeksraad is er niet gerust op dat alle fabrikanten uit eigen beweging deze omslag zullen maken en acht het van belang dat er wetgeving komt om maatschappelijk verantwoord innoveren in de praktijk te verankeren. Van belang is dat niet alleen fabrikanten aan zet zijn, maar dat ook de overheid zich bezint op haar eigen rol en de publieke belangen waarborgt die in het geding zijn bij automatisering in het wegverkeer.

Voortrekkersrol Nederland

Nederland is goed gepositioneerd om een voortrekkersrol te spelen als het gaat om innovatie in het wegverkeer. In internationale gremia is Nederland een actief pleitbezorger van innovatie in het algemeen en maatschappelijk verantwoord innoveren in het bijzonder. Het past Nederland dan ook om in internationaal verband te pleiten voor regelgeving voor maatschappelijk verantwoord innoveren in de auto-industrie. Op deze wijze kan de potentiële bijdrage van innovatie aan de verkeersveiligheid ten volle worden benut, op weg naar nul verkeersdoden in 2050.

SAMENVATTING

Advanced Driver Assistance Systems (ADAS) zijn rijhulpsystemen die de bestuurder ondersteunen bij het uitvoeren van de primaire rijtaak. ADAS nemen de omgeving waar door middel van sensoren en kunnen de besturing van de snelheid of rijrichting overnemen onder verantwoordelijkheid van de persoon aan het stuur. Dergelijke systemen kunnen de bestuurder ook waarschuwen in door het systeem als gevaarlijk ingeschatte situaties.

Automatisering in het wegverkeer kan bijdragen aan vergroting van de verkeersveiligheid maar gaat ook gepaard met nieuwe verkeersveiligheidsrisico's. Op basis van onderzoek van ongevallen, bestudering van literatuur en gesprekken met experts identificeert de Onderzoeksraad voor Veiligheid een aantal soorten nieuwe risico's, die nog niet voldoende onderkend en beheerst worden. ADAS zijn nog niet volwassen als ze op de markt komen. Dit betekent dat ze nog verder doorontwikkeld worden na toelating op de openbare weg. Samen met het kennisgebrek van bestuurders, ontstaan situaties waarin bestuurders niet begrijpen waarom de auto op een bepaalde manier reageert of juist niet reageert. Daarnaast vervullen bestuurders in auto's met ADAS een andere rol dan in conventionele auto's, namelijk de rol van operator. Het takenpakket dat bij deze rol hoort, heeft als risico dat bestuurders minder alert zijn en te laat reageren. Automatisering maakt minder alert. Tegelijkertijd is juridisch gezien de bestuurder verantwoordelijk en aansprakelijk, ook als de auto ingrijpt en/of als de bestuurder in de veronderstelling verkeert dat de auto zelf rijdt. Dat wringt en daar ontstaan risico's.

De voortschrijdende automatisering betekent ook dat auto's met ADAS steeds meer rijdende computers zijn geworden. Daarmee worden ook de risico's die horen bij computers steeds meer in auto's met ADAS geïntroduceerd. Het gaat hierbij om cybersecurityrisico's en om het risico dat noodzakelijke veiligheidsupdates uitblijven. Ook kunnen updates juist een risico vormen, als deze de functionaliteit van de ADAS en daarmee het rijgedrag van de auto veranderen zonder dat de bestuurder zich dat realiseert.

Maatschappelijk verantwoord innoveren

De Onderzoeksraad hanteert bij alle onderzoeken een referentiekader. Dit kader schetst de normen waaraan de betrokken partijen zouden moeten voldoen om veiligheidsrisico's op een bepaald terrein te beheersen. Dit referentiekader gaat in essentie over maatschappelijk verantwoord innoveren.

Om te komen tot maatschappelijk verantwoord innoveren, is het nodig om vanaf het begin van de ontwerpfase rekening te houden met de veiligheid. Bovendien is het noodzakelijk om niet alleen naar de veiligheid van de technologische innovatie op zichzelf te kijken maar ook naar de combinatie met de gebruiker. Voorkomen moet worden dat innoveren wordt gezien als een louter technologisch vraagstuk: de menselijke kant is zeker zo belangrijk.

Dit betekent ook dat fabrikanten van een nieuwe technologie een verantwoordelijkheid hebben ten opzichte van gebruikers om deze voor te lichten over de risico's. Nieuwe risico's moeten vooraf worden ingeschat en zoveel mogelijk worden gemitigeerd. Veilig innoveren vormt een gradueel proces met voortdurende sturing op basis van monitoring en evaluatie. Fabrikanten moeten laten zien dat zij veilig innoveren (transparantie) en gegevens over ongevallen moeten beschikbaar zijn. De overheid moet (voor)bereid zijn in te grijpen wanneer het gebruik van een nieuwe technologie per saldo onveiligheid introduceert.

Met behulp van dit kader heeft de Onderzoeksraad knelpunten geïdentificeerd op gebied van ontwerp, beleid, regulering en toezicht, beschikbare gegevens en lerend vermogen.

Ontwerp
Fabrikanten introduceren nieuwe systemen omdat de techniek het mogelijk maakt en om hun auto's aantrekkelijker te maken voor de klant. Verkeersveiligheid is niet vanaf het begin van het ontwerpproces het uitgangspunt en er wordt te weinig rekening gehouden met de automobilist die de innovatie moet gebruiken. Ook worden voertuigen nu niet zo ontworpen dat de veiligheid gedurende de levensduur behouden blijft. Kennisuitwisseling en transparantie zijn binnen de sector niet gebruikelijk.

Beleid
Het Nederlandse en Europese beleid is gericht op het stimuleren en verplicht stellen van ADAS. De ambitie om het aantal verkeersslachtoffers terug te dringen ligt hieraan ten grondslag. Er is echter geen uitgewerkte visie op het gewenste veiligheidsniveau in relatie tot de gewenste mate en richting van innovatie. Er vinden geen systematische risicoanalyses plaats en er is niet uitgewerkt hoe de risico's gemitigeerd kunnen worden of wat er nodig is om tot mitigerende maatregelen te komen. Verder is het beleid te weinig gericht op de huidige generatie systemen en gaat de overheidsaandacht vooral uit naar de verre toekomst waarin voertuigen wellicht volledig autonoom kunnen opereren. De huidige maatregelen van het ministerie van IenW om de kennisachterstand bij bestuurders in te halen zijn een stap in de goede richting maar wel vrijblijvend.

Regulering en toezicht
In veel domeinen is de wetgeving volgend op maatschappelijke ontwikkelingen. In die zin is het niet verwonderlijk dat de technologische veranderingen in de auto-industrie sneller gaan dan de regulering ervan. Er is echter meer aan de hand dan alleen een probleem van fasering. Op diverse aspecten van veiligheid – bijvoorbeeld opleiding van gebruikers en human factors – blijven de regels achter, omdat fabrikanten en overheid hier ook minder aandacht voor hebben. De regelgeving is nog niet toegespitst op het gegeven dat auto's na toelating op de openbare weg veranderen door updates. Daarnaast bepaalt de voertuigregelgeving wel dat nieuwe systemen het verkeer 'niet onveiliger' mogen maken, maar niet hoe het veiligheidsniveau van ADAS of andere innovaties kan worden beoordeeld. Daardoor is er geen toezicht op de wijze waarop fabrikanten risico's inschatten en scenario's overwegen, worden systemen toegelaten waarvan onbekend is wat het effect is op de verkeersveiligheid en wordt ook niet systematisch gemonitord wat de effecten zijn van deze innovatie.

Black box
ADAS vormen op allerlei niveaus een 'black box'. De politie kan de gegevens na een ongeval vaak niet uitlezen en verder is überhaupt onbekend in welke auto's welke ADAS precies aanwezig zijn en of de systemen al dan niet actief waren. Evenmin is voor alle typen ADAS inzichtelijk welk effect ze hebben op de verkeersveiligheid. Het ontbreekt aan een goede monitoring en evaluatie na introductie van deze nieuwe technologieën. Monitoring van ongevallen met ADAS zou kunnen worden ingepast in het reguliere ongevallenonderzoek. Een positieve ontwikkeling in dit kader is dat de SWOV in opdracht van Rijkswaterstaat sinds kort de dodelijke ongevallen op rijkswegen onderzoekt. Dit biedt een basis voor onderzoek naar de rol van ADAS in het ontstaan van dodelijke ongevallen, waarmee het lerend vermogen wordt versterkt.

Lerend vermogen
Fabrikanten doen niet systematisch onderzoek naar ongevallen waardoor zij niet optimaal kunnen leren van eventuele tekortkomingen aan hun producten. Het ongevalsonderzoek dat wordt gedaan, vindt versnipperd plaats. Een deel van de risico's van ADAS komt pas aan het licht in de praktijk, ongeacht hoe zorgvuldig er vooraf wordt ontworpen en getest. Het functioneren van de praktijk als 'living lab' is onvermijdelijk verbonden aan iedere innovatie, maar de innovatie moet wel verantwoord gebeuren. Het is daarbij zaak om als industrie de lessen uit ongevallen en bijna-ongevallen zo breed mogelijk te onderzoeken en daar als auto-industrie gezamenlijk van te leren.

Effect op verkeersveiligheid onzeker
Zowel de Nederlandse regering als de Europese Commissie streven naar nul verkeersdoden in 2050. Om dit ambitieuze doel te halen, is veel hoop gevestigd op technologische ontwikkelingen en automatisering van de auto in het bijzonder. Er ontstaan echter ook nieuwe risico's met de introductie en het gebruik van ADAS, die nog onvoldoende onderkend, gemonitord en beheerst worden. In potentie kunnen ADAS een positieve invloed hebben op de verkeersveiligheid, maar de waarborgen om die potentie ook echt te benutten ontbreken nog.

AANBEVELINGEN

Aan de autofabrikanten en de koepelorganisaties OICA en ACEA:

1. Toon aan dat de ontwikkeling en introductie van ADAS plaatsvindt volgens de principes van maatschappelijk verantwoord innoveren.

Aan de BOVAG en RAI Vereniging:

2. Zorg ervoor dat BOVAG-leden klanten uitgebreid instrueren over de mogelijkheden en beperkingen van hun auto met ADAS. En zorg dat BOVAG-leden daartoe in staat worden gesteld.

Aan de minister van Infrastructuur en Waterstaat:

3. Neem initiatief om binnen de UNECE *human factors* en maatschappelijk verantwoord innoveren op de agenda te krijgen.

4. Steun de initiatieven van Euro NCAP om *human factors* en consumenteninformatie over ADAS onderdeel te laten zijn van de veiligheidsbeoordeling van auto's (Euro NCAP sterren).

5. Verbeter de mogelijkheden om te leren van verkeersongevallen in het algemeen en de rol van ADAS in het bijzonder en tref maatregelen ten behoeve van de verkeersveiligheid op basis van de onderzoeksresultaten.

6. Kaart bij de Europese Commissie aan dat de voertuigregelgeving aan moet sluiten bij de huidige generatie ADAS (SAE level 2 en lager). Daarbij moet de verantwoordelijkheid om aan te tonen dat nieuwe ADAS de veiligheid verbeteren bij de fabrikanten komen te liggen. Verder moet aandacht besteed worden aan eisen op het gebied van human factors, opleiding van gebruikers, toegankelijkheid van data uit ADAS na ongevallen en ongevalsonderzoek door fabrikanten.

ir. J.R.V.A. Dijsselbloem
Voorzitter van de Onderzoeksraad

mr. C.A.J.F. Verheij
Secretaris-directeur

LIJST VAN AFKORTINGEN

AAA	*American Automobile Association*
ABS	*Anti-lock Braking System* (Antiblokkeersysteem)
ACC	*Adaptive CruiseControl*
ACSF	*Automatically Commanded Steering Functions*
ACEA	*European Automobile Manufacturers' Association*
ADAS	*Advanced Driver Assistance System(s)*
ADASS	*Advanced Driver Assistance Steering Systems*
AEBS	*Advanced Emergency Braking System, ook wel Autonomous Emergency Braking System of Automatic Emergency Braking System* genoemd
AI	*Artificial Intelligence*; kunstmatige intelligentie
ANWB	Nederlandse organisatie voor verkeer en toerisme
APK	Algemene Periodieke Keuring
ASS	*Autonomous Steering Systems*
Auto-ISAC	*Automotive Information Sharing & Analysis Center*
AVG	Algemene Verordening Gegevensbescherming
CBR	Centraal Bureau (voor de Afgifte van) Rijvaardigheidsbewijzen
CC	*Cruise control*
CIECA	*International Commission for Driver Testing*
CSF	*Corrective Steering Functions*
CSMS	*Cyber Security Management System*
CS/OTA	*Cyber Security / Over The Air (updates / communication)*
DL	*Deep Learning*
DSSAD	*Data Storage System for Automated Driving*
ECU	*Electronic Control Unit*
EDR	*Event Data Recorder*
ENISA	*European Union Agency for Cybersecurity*
ESC	*Electronic Stability Control*
ETSC	*European Transport Safety Council*
Euro NCAP	*European New Car Assessment Programme*
EVA	*Equality for Vehicle Advancement*
FCW	*Forward Collision Warning*
FOT	*Field Operational Test*
GRVA	UNECE Werkgroep *'Automated/Autonomous and Connected Vehicles'*
GSR	*General Safety Regulation*
HMI	*Human Machine Interaction*

IenW	(Ministerie van) Infrastructuur en Waterstaat
ISA	*Intelligent Speed Assistance of Intelligent Speed Adaptation*
ISO	*International Organization for Standardization*
LDA	*Lane Departure Avoidance*, ook wel gebruikt voor *Lane Departure Alert of Lane Departure Assistance*
LDW	*Lane Departure Warning*
LKA	*Lane Keeping Assist*
LKS	*Lane Keeping System*
ML	*Machine Learning*
NHTSA	*National Highway Traffic Safety Administration*
NTSB	*National Transportation Safety Board*
OEDR	*Object and Event Detection and Response*
OTA	*Over-The-Air (communicate of update)*
RDW	Dienst Wegverkeer (voorheen Rijksdienst voor het Wegverkeer)
RWS	Rijkswaterstaat
SAE	*Society of Automotive Engineers*
SWOV	Stichting Wetenschappelijk Onderzoek Verkeersveiligheid
TACC	*Traffic Aware Cruise Control*, een andere naam voor ACC
TCU	*Telematics Control Unit*
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
UNECE	*United Nations Economic Commission for Europe*
V2I	*Vehicle to Infrastructure (communication)*
V2V	*Vehicle to Vehicle (communication)*
V2X	*Vehicle to everything (communication)*
VDLF	*Vehicle Drivers' License Framework*
VSSF	*Vehicle Safety and Security Framework*

1 INLEIDING

1.1 Verkeersveiligheid en automatisering

Sinds de jaren zeventig is de verkeersveiligheid in Nederland aanmerkelijk verbeterd. De laatste jaren is het verkeer echter niet veiliger geworden. Zo vallen er sinds 2010 jaarlijks gemiddeld ruim 600 verkeersdoden en ongeveer 21.000 ernstig gewonden en in 2018 vielen zelfs 678 doden in het verkeer: het hoogste aantal sinds 2009.[1] Dit in weerwil van het feit dat zowel de Nederlandse regering als de Europese Commissie streven naar nul verkeersdoden in 2050.[2, 3] Automatisering wordt daarbij gezien als een van de middelen om de verkeersveiligheid te verbeteren.[4, 5] EU-lidstaten, de Europese Commissie en de auto-industrie zetten ook vol in op de ontwikkeling van geautomatiseerde voertuigen.[6] De eerste stap bestaande uit de introductie van rijhulpsystemen (*Advanced Driver Assistance Systems*, kortweg ADAS) laat een stormachtige groei zien. Tegelijkertijd kunnen er met de introductie en het gebruik van een nieuwe technologie ook nieuwe risico's ontstaan. Inmiddels hebben zich verschillende ongevallen op de openbare weg voorgedaan waarbij ADAS een rol speelden. Deze ongevallen tonen aan dat risico's die zijn ontstaan door automatisering zich ook al in de praktijk manifesteren.

Gegeven deze ontwikkelingen staan autofabrikanten samen met de andere betrokken partijen voor de taak om kansen zo goed mogelijk te benutten en risico's te minimaliseren, zodat innovatie daadwerkelijk bijdraagt aan de veiligheid in het wegverkeer. Automatisering in het wegverkeer raakt ook de regulerende en toezichthoudende rol van de overheid en vraagt om een andere invulling van deze rollen. De vraag is in hoeverre partijen die verantwoordelijk zijn voor de veiligheid op de openbare weg voldoende aandacht hebben voor de nieuwe risico's van de introductie en het gebruik van ADAS. Een kenmerk van de huidige generatie technologie is dat systemen doorontwikkelen, ook in voertuigen die al op de weg zijn. Deze dynamiek is een karakteristiek onderdeel van de ICT, die steeds meer toepassing vindt binnen de voertuigtechniek. De zorg hierbij is dat partijen onvoldoende oog hebben voor fundamentele karakterveranderingen van voertuigen (en het wegverkeer) waardoor bestaande wet- en regelgeving de veiligheid onvoldoende waarborgt.

1 SWOV, *Factsheet Verkeersdoden in Nederland*, 2019.
2 Ministerie van IenW et al., Veilig van deur tot deur; *Het Strategisch Plan Verkeersveiligheid 2030: Een gezamenlijke visie op aanpak verkeersveiligheidsbeleid*, 2018.
3 Europese Commissie, *Annex 1: Strategic Action Plan on Road Safety*, in Europe on the move; Sustainable Mobility for Europe: safe, connected and clean, 2018.
4 ETSC, *Prioritising the safety potential of automated driving in Europe*, 2016.
5 Minister van Infrastructuur en Milieu, *Kamerbrief 31305 Mobiliteitsbeleid*, 2014.
6 EU-lidstaten, *Declaration of Amsterdam; Cooperation in the field of connected and automated driving*, 2016.

Technische ingrepen hebben in het recente verleden fors bijgedragen aan de vermindering van het aantal verkeersslachtoffers. Bekende voorbeelden zijn autogordels, kreukelzones, kooiconstructies, airbags, antiblokkeersysteem (ABS) en elektronische stabiliteitscontrole (ESC). De eerste vier zijn vormen van passieve veiligheid, waardoor inzittenden van auto's beter beschermd zijn tegen de gevolgen van een ongeval. Maatregelen op het gebied van passieve veiligheid zijn volgens de autofabrikanten vrijwel uitontwikkeld. Deze lijn verder ontwikkelen zou leiden tot zwaardere auto's met weliswaar een betere bescherming van de inzittenden van de auto's maar met negatieve gevolgen voor de verkeersveiligheid van kwetsbare verkeersdeelnemers en hogere emissies. ABS en ESC zijn vormen van actieve veiligheid waardoor ingegrepen wordt in de besturing van de auto met als doel ongelukken te voorkomen of minder ernstig te laten zijn. De autofabrikanten zien nog wel ruimte in verdere ontwikkeling van de actieve veiligheid door bestuurders met ADAS te ondersteunen. Maatregelen op het gebied van passieve veiligheid hadden puur betrekking op de auto, waar veel maatregelen op het gebied van actieve veiligheid ook een duidelijke interactie met de bestuurder en de infrastructuur vertonen. Actieve veiligheid bevorderen door middel van ADAS vraagt daarom om een nieuwe aanpak.

1.2 Doel en onderzoeksvragen

De Onderzoeksraad voor Veiligheid beoogt bij te dragen aan het vergroten van de veiligheid in Nederland in een steeds veranderende omgeving. De Raad wil daarom inspelen op nieuwe veiligheidsvraagstukken zoals die zich voordoen bij de automatisering in het wegverkeer. Het doel van dit onderzoek is het verbeteren van de verkeersveiligheid. Dit doen we door partijen die zorg kunnen en moeten dragen voor veiligheid op de weg inzicht te geven in de manier waarop zij nieuwe risico's als gevolg van de introductie van ADAS inventariseren en beheersen. Gegeven dit doel staan de volgende vragen centraal in dit onderzoek.

Onderzoeksvragen

- Hoe beheersen de gebruikers, auto-industrie, branchepartijen en de overheid de risico's verbonden aan de introductie en het gebruik van rijhulpsystemen (ADAS)?
- In hoeverre zijn er verbeteringen in de risicobeheersing mogelijk?

De focus van het onderzoek ligt op de beheersing van de risico's van de introductie en het gebruik van voertuigen met ADAS door fabrikanten, toeleveranciers, importeurs, dealers, toezichthouders, wetgevers, belangenorganisaties, etc. Het gaat dus om de *beheersing* van de risico's en minder om de risico's zelf. De in dit rapport genoemde risico's dienen vooral als voorbeelden om te laten zien hoe partijen hiermee omgaan. Het rapport geeft geen overzicht van alle risico's. Dit is van belang omdat het veld volop in ontwikkeling is. Daarom komen er gaandeweg nieuwe risico's aan het licht die eerst nog niet bekend waren.

1.3 Werkwijze

Het in dit rapport beschreven onderzoek bestond uit vier fases. Na een verkennende fase (fase 1) is onderzocht welke nieuwe soorten veiligheidsrisico's er zijn en hoe die beheerst worden (fase 2, eerste onderzoeksvraag). Daarvoor zijn zes ongevallen onderzocht, heeft een groot aantal interviews plaatsgevonden, zijn er gesprekken met experts gevoerd, en is er literatuuronderzoek gedaan. Omdat het een themaonderzoek betreft, zijn de beschreven risico's breder dan de risico's gevonden in de ongevallen. De ongevallen dienen als illustratie bij de beschreven risico's en vormen geen overzicht van welke soorten ongevallen met ADAS er zoal plaatsvinden. De nadruk van het onderzoek lag hierbij op de vraag hoe partijen die risico's beheersen. Het onderzoek is geen risico-inventarisatie. Bovendien zullen er op korte termijn altijd weer nieuwe risico's ontstaan omdat de ontwikkelingen voortschrijden.

Bij de meeste beschreven ongevallen waren auto's van het merk Tesla betrokken. Dat wordt verklaard doordat Tesla vooroploopt bij de introductie van ADAS en deze ook standaard in iedere auto inbouwt. Bij ongevallen met Tesla's wordt in de praktijk eerder een verband gelegd met ADAS dan bij ongevallen met andere merken auto's, waardoor deze laatste minder vaak gemeld worden bij de Onderzoeksraad. De in dit rapport beschreven ongevallen zijn dan ook geen representatieve steekproef voor de ongevallen waarbij ADAS een rol speelt.

Om de tweede onderzoeksvraag te beantwoorden, is een referentiekader opgesteld (fase 3) en is met behulp van het referentiekader vastgesteld waar de knelpunten zitten in een veilige introductie en gebruik van ADAS (fase 4).

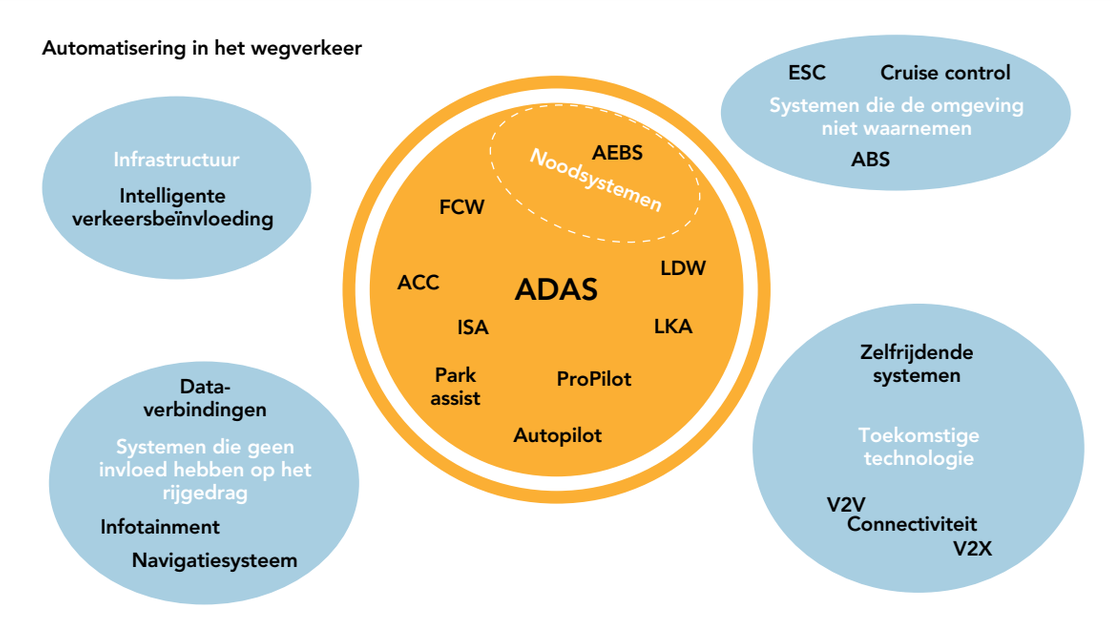
Meer informatie over de werkwijze is te vinden in bijlage A, de onderzoeksverantwoording.

1.4 Afbakening en definities

Deze paragraaf definieert enkele kernbegrippen in dit onderzoek, waarmee tevens de afbakening van het onderzoeksobject helderder wordt.

Automatisering in het wegverkeer is een breed begrip, waar veel ontwikkelingen onder geschaard kunnen worden, zie Figuur 1. Het kan zowel het voertuig als de infrastructuur betreffen. Dit onderzoek focust op automatisering van de primaire rijtaak.

Automatisering van de primaire rijtaak
De primaire rijtaak is de longitudinale en laterale besturing van het voertuig (sturen, gas geven en remmen). Bij (gedeeltelijke) automatisering van de primaire rijtaak wordt de bestuurder ondersteund in het uitvoeren van de rijtaak of wordt de rijtaak (tijdelijk) helemaal overgenomen.



Figuur 1: De focus van het onderzoek ligt op de huidige generatie ADAS (oranje cirkel). Andere onderdelen van automatisering in het wegverkeer blijven buiten beschouwing in dit rapport.

ADAS

Met behulp van geautomatiseerde systemen kan het voertuig op basis van waarnemingen van de omgeving de bestuurder ondersteunen bij het uitvoeren van de rijtaak – door de bestuurder van informatie te voorzien en te waarschuwen bij gevaarlijke situaties – en de besturing van de snelheid en/of rijrichting overnemen. Deze geautomatiseerde systemen worden rijhulpsystemen, ook wel ADAS genoemd. Een voorbeeld van een ADAS is rijstrookassistentie – of Lane Keeping Assist (LKA)[7]. Dit is bedoeld om tegen te gaan dat het voertuig onbedoeld de rijstrook verlaat en kan automatisch ingrijpen met een stuurcorrectie. Dit wordt ook wel Lane Departure Avoidance (LDA) genoemd. Een verdergaande vorm van rijstrookassistentie is Lane Centering, waarbij de auto continu in het midden van de rijstrook wordt gehouden. Lane Departure Warning (LDW) grijpt niet in maar waarschuwt de bestuurder wanneer de auto de rijstrook onbedoeld dreigt te verlaten. Een ander voorbeeld zijn noodremsystemen, die geïntroduceerd werden rond 2010. Een Advanced Emergency Braking System (AEBS) kan tijdelijk de besturing van het voertuig overnemen om het voertuig te laten remmen wanneer een botsing dreigt met bijvoorbeeld een voorligger, fietser, voetganger of een ander object. Forward Collision Warning (FCW) is de alleen waarschuwende variant hiervan.

7 Er zijn verschillende soorten rijstrookassistentie systemen op de markt. Er zijn veel verschillende namen en classificeringen (zie box over verscheidenheid ADAS in paragraaf 3.3, bijlagen D.4 en E.4), waardoor het niet altijd duidelijk is om welk systeem het gaat. Daarom worden in dit rapport deze systemen allemaal geschaard onder de naam rijstrookassistentie (LKA).

Definitie ADAS
Advanced Driver Assistance Systems (ADAS) zijn rijhulpsystemen die de bestuurder ondersteunen bij het uitvoeren van de primaire rijtaak. Deze systemen nemen de omgeving waar door middel van sensoren en kunnen de besturing van de snelheid en/of rijrichting overnemen onder verantwoordelijkheid van de persoon aan het stuur. Dergelijke systemen kunnen de bestuurder ook waarschuwen in door het systeem als gevaarlijk ingeschatte situaties.

De Onderzoeksraad stelt met deze definitie de bestuurder centraal en hanteert hiermee een op hoofdlijnen vergelijkbare definitie als de ADAS Alliantie[8] en een andere definitie dan de European Automobile Manufacturers' Association (ACEA) en de Society of Automotive Engineers (SAE).[9, 10, 11] Systemen zoals ABS en gewone cruisecontrol vallen niet onder deze definitie van ADAS en vallen daardoor buiten de scope van het onderzoek; deze systemen nemen hun omgeving niet waar door middel van sensoren.

Er bestaan op dit moment nog geen volledig zelfrijdende auto's die op de openbare weg zijn toegelaten. De huidige ADAS die fabrikanten overigens onder verschillende namen aanbieden, bestaan vooral uit een combinatie van adaptive cruisecontrol (ACC)[12], rijstrookassistentie (LKA) en een noodremsysteem (AEBS). Op bepaalde wegen en onder bepaalde omstandigheden kan de auto hierdoor zelf sturen, remmen en gas geven, maar de bestuurder moet alert blijven om waar nodig de besturing over te nemen.

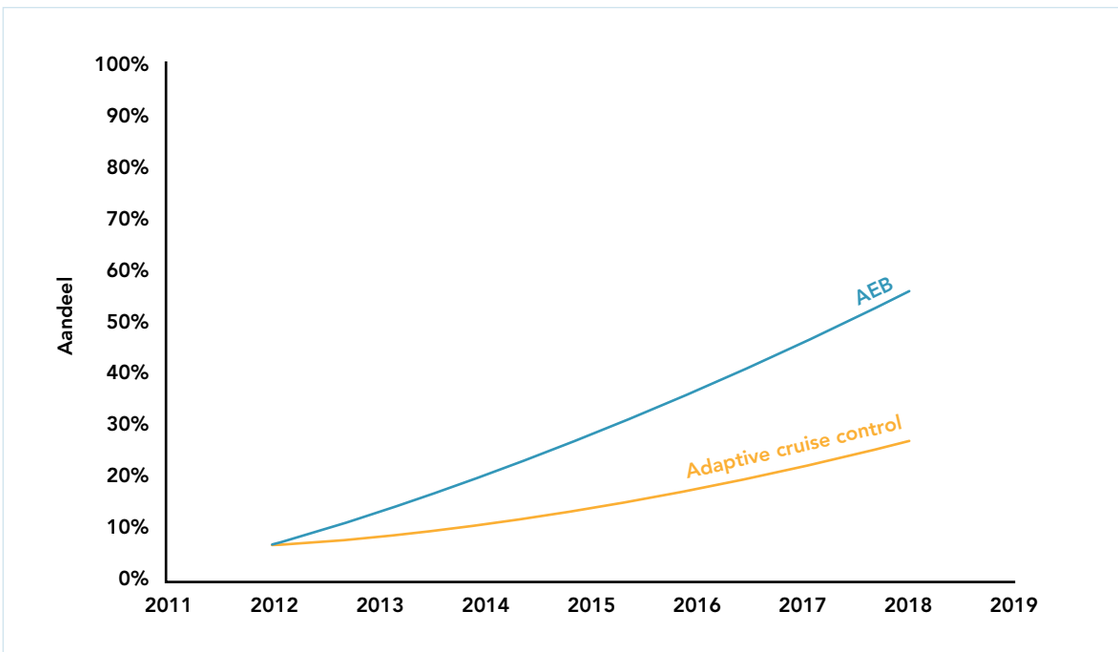
Er zijn voortdurend nieuwe systemen in ontwikkeling zoals evasive steering (een noodsysteem dat een uitwijkmanoeuvre kan maken). Bij toekomstige systemen speelt informatie-uitwisseling met bijvoorbeeld de infrastructuur en met andere voertuigen (zogenaamde connectiviteit) een steeds grotere rol. Deze toekomstige systemen vallen buiten de scope van het onderzoek.

Tabel 1 geeft een overzicht van standaard met ADAS uitgeruste modellen van diverse automerken. Dit is waarschijnlijk een onvolledige momentopname, maar dient vooral als illustratie van de brede toepassing van ADAS. Het marktaandeel van ADAS is met name de afgelopen drie jaar sterk gestegen, zie Figuur 2.[13]

8 ADAS Alliantie, *ADAS Convenant*, 2019.
9 ADAS Alliantie, *Website ADAS Alliantie*, https://www.adasalliantie.nl, geraadpleegd op 23 augustus, 2019.
10 Knapp et al., *Code of Practice for the Design and Evaluation of ADAS*, 2009.
11 SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report*, 2014.
12 Ook wel traffic aware cruisecontrol (TACC) genoemd.
13 VMS in opdracht van BOVAG, *Het effect van ADAS op schadeherstel, onderhoud en reparatie*, 2019.

Alfa Romeo Stelvio	Honda Civic	Land Rover Discovery	Peugeot 508	Toyota C-HR
Audi A6	Hyundai i30	Lexus ES	Peugeot Rifter	Toyota Yaris
Audi Q3	Hyundai Nexo	Mazda 6	Range Rover Velar	Toyota Corolla
BMW 5 Serie	Hyundai Santa Fe	Mercedes-Benz A-Class	Renault Koleos	Toyota RAV4
BMW X5	Jaguar E-pace	Mercedes-Benz C-Class	Subaru Impreza	Volvo S60
Citroën Berlingo	Jaguar F-pace	Mercedes-Benz X-Class	Subaru XV	Volvo S90
DS 7 Crossback	Jaguar I-pace	Mitsubishi Eclipse Cross	Suzuki Jimny	Volvo V60
Ford Focus	Jeep Compass	Nissan Leaf	Tesla Model 3	Volvo V90
Ford Mustang	Kia Stinger	Opel Combo	Tesla Model S	Volvo XC40
Ford Tourneo Connect		Opel/Vauxhall Ampera-e	Tesla Model X	Volvo XC60
		Opel/Vauxhall Insignia		VW Arteon
				VW Touareg
				VW T-Roc

Tabel 1: Overzicht van auto's die standaard zijn uitgerust met ADAS (momentopname april 2019).



Figuur 2: Aanwezigheid van twee soorten ADAS in nieuw verkochte auto's. (Bron gegevens: BOVAG)

Cybersecurity

Met de introductie van ADAS worden ook risico's geïntroduceerd op het raakvlak van digitale ontwikkelingen met het traditionele terrein van het 'fysieke' wegverkeer. Digitale veiligheid wordt daarbij steeds belangrijker voor het waarborgen van de fysieke veiligheid. De auto verandert als het ware in een rijdende computer, waardoor problemen die voorheen typisch waren voor de IT-sector ook in het wegverkeer opkomen. Daarnaast groeit het aantal aanvalsmogelijkheden van een auto doordat deze over steeds meer digitale verbindingen beschikt. Deze twee ontwikkelingen samen introduceren cybersecurityrisico's in auto's.

Definitie cybersecurity

Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie[14]. Tevens kan vervolgschade ontstaan in de fysieke wereld, bijvoorbeeld in het wegverkeer.

In dit onderzoek ligt de focus van cybersecurity op het misbruik van kwetsbaarheden dat leidt tot risico's voor de fysieke veiligheid.

Privacy

Bij de introductie van ADAS staan – naast de verkeersveiligheid – ook andere maatschappelijke belangen op het spel. In het bijzonder de bescherming van persoonlijke informatie (en daarmee het recht op privacy) kan kwetsbaar zijn als bijvoorbeeld gegevens over rijgedrag breed beschikbaar komen (openbaar dan wel in handen van derden). Dergelijke vraagstukken vallen echter buiten de scope van dit rapport. Bovendien heeft dit onderwerp in het voorjaar van 2019 zowel Europees als nationaal nadrukkelijk aandacht gekregen. In Europees verband door het aannemen van de General Safety Regulation (GSR) waarin verwezen wordt naar de Algemene Verordening Gegevensbescherming (AVG), en nationaal, door het antwoord van de minister van IenW op vragen van de Tweede Kamer.[15]

14 National Cyber Security Center, *Cybersecuritybeeld Nederland CSBN 2018*, 2018.
15 Minister van Infrastructuur en Waterstaat, *Kamerbrief Beantwoording Kamervragen van de Leden Schonis En Verhoeven (Beiden D66) over Het Artikel 'Wie Temt Het Datamonster in de Auto-Industrie?*, 2019.

1.5 Betrokken partijen

De partijen die betrokken zijn bij de beheersing van de risico's verbonden aan de introductie en het gebruik van ADAS kunnen in drie groepen worden verdeeld:

1. Industrie en branchepartijen
2. Gebruikers
3. Overheid

De industrie bestaat uit autofabrikanten, die eindverantwoordelijk zijn voor het product dat zij op de markt brengen, en hun toeleveranciers. Naast de traditionele autofabrikanten en toeleveranciers zijn er ook nieuwe producenten, zoals Tesla, die meer affiniteit hebben met ICT. Er zijn zowel toeleveranciers die complete systemen maken als bedrijven die zich alleen toeleggen op chips of software. Combinaties komen ook voor. Voor traditionele autofabrikanten geldt dat zij de meeste ADAS doorgaans 'van de plank' kopen of samen met toeleveranciers ontwikkelen, terwijl nieuwe autofabrikanten veel zelf ontwikkelen. Branchepartijen zijn importeurs, dealers en garagebedrijven; via hen komt het product bij de gebruiker en worden systemen onderhouden en gerepareerd.

Iedere burger kan een gebruiker van ADAS zijn. Er is geen aanvullende opleiding voor nodig, waardoor de automobilist in een auto uitgerust met ADAS in zijn rol als operator ongetraind kan functioneren. Bestuurders van conventionele auto's zijn wel getraind en hebben tijdens het rijexamen moeten aantonen dat zij een auto veilig kunnen besturen. Gebruikers van ADAS zijn bovendien niet altijd goed geïnformeerd over de werking ervan.[16] De ANWB is de belangrijkste belangenorganisatie voor gebruikers van ADAS in Nederland. De introductie van ADAS heeft ook invloed op overige verkeersdeelnemers, bestuurders van auto's zonder ADAS en kwetsbare verkeersdeelnemers als fietsers en voetgangers. Ook voor hen ontstaan nieuwe risico's in het verkeer. Omdat verdere automatisering in het wegverkeer een innovatie is met mogelijk ingrijpende gevolgen voor de samenleving, raakt deze vrijwel alle burgers.

De overheid bestaat uit de nationale overheid en de EU, waarbij de EU een belangrijk deel van de invulling van de regelgeving overlaat aan een speciale VN-commissie, de United Nations Economic Commission for Europe (UNECE). Binnen de Nederlandse overheid zijn de uitvoeringsinstanties opgedeeld in de traditionele indeling van het wegverkeer in mens-voertuig-weg. Het CBR beoordeelt de rijvaardigheid van bestuurders. De RDW en zijn zusterorganisaties in Europa beoordelen voertuigen tegen een geharmoniseerde set van eisen, waarvan veiligheid een belangrijk aspect is en laten goedgekeurde voertuigen toe op de openbare weg in heel Europa. De verschillende wegbeheerders zoals Rijkswaterstaat, provincies en gemeenten dragen zorg voor de weginrichting en het onderhoud. Het Ministerie van Infrastructuur en Waterstaat is verantwoordelijk voor beleid en regelgeving voor zover dat niet internationaal is. Dit ministerie is ook verantwoordelijk voor de Nederlandse inbreng in de EU en bij de UNECE. Een groot deel van de voorbereiding hiervan wordt in opdracht van het ministerie uitgevoerd door de RDW.

16 Harms en Dekker, *ADAS: from owner to user; Insights in the conditions for a breakthrough of Advanced Driver Assistance Systems*, 2017.

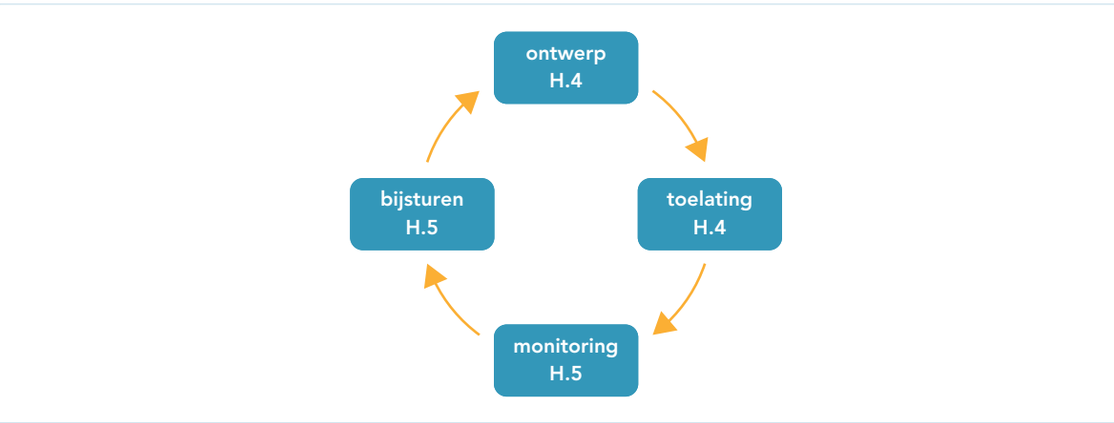
Voertuigveiligheid wordt gestimuleerd door Euro NCAP door inzicht in de veiligheid van auto's te verschaffen met behulp van sterrenratings, waar bepaalde ADAS onderdeel van zijn.

1.6 Leeswijzer

Hoofdstuk 2 geeft weer wat de Onderzoeksraad verwacht van partijen ten aanzien van hun verantwoordelijkheid voor de veilige introductie van nieuwe technologie in het wegverkeer.

De beheersing van veiligheidsrisico's verbonden aan de automatisering in het wegverkeer staat centraal in *hoofdstuk 3*. Dit hoofdstuk geeft een overzicht van thema's waarop risico's zich voordoen en van de mate waarin deze risico's worden onderkend en beheerst. Dit hoofdstuk beschrijft diverse ongevallen ter illustratie.

De risico's van automatisering op de verkeersveiligheid kennen hun oorsprong in knelpunten op stelselniveau. We maken daarbij onderscheid in knelpunten bij ontwerp en toelating van nieuwe ADAS (*hoofdstuk 4*) en knelpunten bij de monitoring en bijsturing (*hoofdstuk 5*).



Figuur 3: De hoofdstukindeling.

Het rapport sluit af met conclusies en aanbevelingen in respectievelijk *hoofdstuk 6* en *7*.

2 REFERENTIEKADER

De Onderzoeksraad hanteert bij alle onderzoeken een referentiekader. Dit kader schetst de normen waaraan de betrokken partijen zouden moeten voldoen om veiligheidsrisico's op een bepaald terrein te beheersen. Door afwijkingen ten opzichte van het referentiekader te identificeren, wordt inzichtelijk waar verbeteringen mogelijk zijn. Het opstellen van het referentiekader voor een veilige introductie van nieuwe technologie en voor cybersecurity was een belangrijk deel van het onderzoek dat de Raad heeft gedaan om tot dit rapport te komen.

2.1 Veilige introductie van nieuwe technologie

Onzekerheid is kenmerkend voor veiligheidsrisico's die gepaard gaan met innovatie en neemt toe naarmate de innovatie radicaler is. Daarom moeten partijen die onzekerheid in al haar verschijningsvormen als uitgangspunt van hun handelen nemen.[17, 18] Dat vereist dat zij niet alleen op basis van empirische gegevens risico's inschatten. Zij dienen ook tot een oordeel te komen over de voorstelbaarheid van scenario's. Zij moeten zich realiseren dat de gekozen set scenario's meestal onvolledig is en dienen ook maatregelen te nemen als risico's nog onvoldoende in beeld zijn (voorzorgsbeginsel).[19]

Veiligheidsprincipes
Veiligheid is een belangrijke maatschappelijke waarde. Literatuur over publieke waarden en ethiek bij innoveren en kunstmatige intelligentie ligt daarom aan de basis van de veiligheidsprincipes voor de introductie van nieuwe technologie die de Onderzoeksraad heeft opgesteld.[20, 21, 22, 23, 24, 25, 26] Deze veiligheidsprincipes zijn generiek voor innoveren en worden in hoofdstuk 4 en 5 specifiek toegepast op de introductie van ADAS.

1. Nieuwe technologieën moeten de veiligheid aantoonbaar verbeteren en zeker niet verslechteren. Dit moet het geval zijn gedurende de gehele levensduur van een product.

17 WRR, *Onzekere Veiligheid: Verantwoordelijkheden rond Fysieke Veiligheid*, 2008.
18 Onderzoeksraad voor Veiligheid, *Opkomende Voedselveiligheidsrisico's*, 2019.
19 Onderzoeksraad voor Veiligheid, *MH17 crash*, 2015.
20 Floridi et al., *An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, Minds and Machines 28, nummer 4, 2018.
21 Van de Poel, *An Ethical Framework for Evaluating Experimental Technology*, Science and Engineering Ethics 22, nummer 3, 14 juni, 2016.
22 Future of Life Institute, *AI Principles*, https://futureoflife.org/ai-principles/?cn-reloaded=1, geraadpleegd op 7 januari, 2019.
23 PBL, *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning*, 2017.
24 Santoni de Sio, *Ethics and Self-Driving Cars; A White Paper on Responsible Innovation in Automated Driving Systems*, nummer oktober, 2016.
25 Rathenau Instituut, *Mensenrechten in het Robottijdperk*, 2017.
26 Von Schomberg, *A vision of Responsible Research and Innovation*, in Responsible Innovation, bewerkt door M. Heintz and J Bessant R. Owen Londen: John Wiley, 2013.

2. Voor een veilig ontwerp van een nieuwe technologie is het vooral in relatie tot verkeersveiligheid nodig:
   - vanaf het begin van de ontwerpfase rekening te houden met de veiligheid (*safety by design*);
   - dat de technologie op een veilige manier uitschakelt wanneer de techniek faalt (*failsafe*);
   - niet alleen naar de veiligheid van de technologische innovatie op zichzelf te kijken maar ook naar de combinatie met de gebruiker (*foolproof design*[27]). Dit is een standaardterm in veilig ontwerpen en betekent dat het ontwerp bestand is tegen (onbedoeld) foutief of ondeskundig gebruik;
   - te kunnen verklaren hoe een systeem tot bepaalde besluiten of acties komt, waardoor het gedrag van het systeem voor de mens begrijpelijk en voorspelbaar is (uitlegbaarheid);
   - duidelijkheid te geven onder welke voorwaarden en omstandigheden een systeem de controle heeft en wanneer de gebruiker; dit moet niet alleen duidelijk zijn voor de gebruiker maar ook tot op zekere hoogte beïnvloedbaar (autonomie).

3. Producenten dienen inzicht te bieden in de technologie, zodat anderen (gebruikers, de overheid) zich er een oordeel over kunnen vormen (transparantie). Daarnaast moeten empirische gegevens over de gevolgen voor de veiligheid openbaar en toegankelijk zijn, zodat nagegaan kan worden of en hoe de innovatie negatieve gevolgen heeft voor de veiligheid. Ook voor cybersecurity is transparantie over dreigingsrisico's en incidenten van belang (zie paragraaf 2.2).

4. Het is van belang erop toe te zien dat verschillende toekomstscenario's en risico's worden onderzocht en gewogen. Tijdens het gebruik van de nieuwe technologie moet worden gemonitord wat nieuwe risico's zijn en moeten zo nodig mitigerende maatregelen worden genomen op operationeel, tactisch en strategisch niveau.

5. Introductie van nieuwe technologie in het wegverkeer moet een beheerst proces zijn met voortdurende bijsturing op basis van monitoring en evaluatie. Het opschalen kan een graduele opschaling van een bepaalde techniek zijn of een graduele verruiming van de gebruiksvoorwaarden.

6. De overheid moet bereid zijn in te grijpen en het gebruik van een nieuwe technologie (tijdelijk) te stoppen of aan te laten passen wanneer deze onveiligheid introduceert. Daar moet van tevoren over zijn nagedacht, bijvoorbeeld door criteria en procesafspraken over de beoordeling van risico's op te stellen.

7. De overheid moet kwetsbare groepen of groepen die zich de nieuwe technologie niet kunnen veroorloven beschermen.

8. Wet- en regelgeving moeten zijn afgestemd op de rijpheid van de technologie en de snelheid waarmee deze zich verder ontwikkelt:

27 Onderzoeksraad voor Veiligheid, *Koolmonoxide: Onderschat en onbegrepen gevaar*, 2015.

- Al langer toegepaste, in de praktijk bewezen en doorontwikkelde technologieën kunnen, liefst na een breed gedragen proces van harmonisatie en standaardisatie, worden vastgelegd in voorschriften. De manier waarop getoetst kan worden of aan deze regels is voldaan, is in dat geval helder omschreven.
- Regelgeving in de vorm van prestatie-eisen past bij technologie die nog in ontwikkeling is. Dergelijke performance-based regelgeving schrijft het niveau van de prestatie en de daarbij behorende beproevingsmethode voor.
- Als de technologie snel verandert en minder rijp is, is kwalitatieve, functionele en liefst adaptieve regelgeving het meest passend. Dat geldt nog sterker als de technologie ook tijdens het gebruik nog wordt aangepast. Daarbij vindt toetsing meer op procesniveau plaats en ligt de verantwoordelijkheid voor het aantonen van de deugdelijkheid en veiligheid meer bij de producent en minder bij toetsingsinstanties.

Maatschappelijke inbedding en verantwoordelijkheden partijen

Maatschappelijk verantwoord innoveren[28] kan worden gekarakteriseerd als een evenwicht tussen inspanningen om de positieve bijdragen van de technologie te maximaliseren en de negatieve gevolgen ervan te minimaliseren.[29] Belangrijk hierbij is de gedeelde verantwoordelijkheid voor de maatschappelijke inbedding tussen innovatoren, fabrikanten, overheid en (andere) maatschappelijke actoren (zoals vertegenwoordigers van de gebruikers). Voorkómen moet worden dat innoveren wordt gezien als een louter technologisch vraagstuk. Dit pleit voor breder overleg, ook met niet direct betrokken partijen.

Gedeelde verantwoordelijkheid voor veiligheid is onderdeel van maatschappelijk verantwoord innoveren. Een transparant, interactief proces waarbij alle actoren op elkaar reageren is nodig voor de ontwikkeling van veilige nieuwe technologieën. Het interactieve proces is noodzakelijk om vast te stellen wat de veiligheidsdoelen zijn, om de verwachtingen te managen en om ontwerpen aan te passen zodat deze aansluiten bij de veiligheidsbehoeften vanuit de maatschappij. *Technology assessments* en risicobeoordelingen vormen daar een onderdeel van.[30, 31]

Fabrikanten zijn hoofdverantwoordelijk voor een veilig ontwerp van een nieuwe technologie. Toeleveranciers moeten een belangrijke bijdrage hieraan leveren, omdat zij een groot deel van de innovatieve techniek ontwikkelen. Voorwaarde om dit goed in te vullen is dat zij informatie verkrijgen over het gebruik van de systemen en welke risico's er in de praktijk optreden. Hiervoor moeten fabrikanten de communicatie binnen de leveringsketen faciliteren en actief inzetten op het verzamelen van praktijkervaringen met de nieuwe technologie bij consumenten. Mogelijk moeten verkopers en importeurs hierbij een rol spelen. Door de productverantwoordelijkheid zijn fabrikanten ook verantwoordelijk voor het interactieve proces waarbij alle actoren op gelijkwaardige wijze op elkaar reageren.

28 In het Engels aangeduid als Responsible Research and Innovation (RRI) is een belangrijk onderdeel van Horizon 2020, Europees kaderprogramma om onderzoek en innovatie te stimuleren.
29 Rip, *The Past and Future of RRI*, Life Sciences, Society and Policy 10, nummer 1, 2014.
30 van Wezel et al., *Risk Analysis and Technology Assessment in Support of Technology Development: Putting Responsible Innovation in Practice in a Case Study for Nanotechnology*, Integrated Environmental Assessment and Management 14, nummer 1, 2018.
31 Borup et al., *The Sociology of Expectations in Science and Technology*, Technology Analysis and Strategic Management 18, 2006.

De overheid dient in een vroeg stadium na te denken over welke rollen zij speelt of wil spelen bij innovatieve ontwikkelingen (bijvoorbeeld gebruiker, opdrachtgever, financier, regelgever, toezichthouder en bewaker van publieke belangen) en (mogelijke) risico's die zij daarbij tegenkomt.[32] Zonder overheidsbemoeienis kunnen nieuwe technologische ontwikkelingen negatieve gevolgen krijgen voor belangrijke publieke waarden.[33] Van de overheid mag dan ook verwacht worden dat zij zich inspant om zowel de kansen als de risico's van innovaties goed in beeld te krijgen en te houden, om ze vervolgens te delen met partijen die in staat zijn mitigerende maatregelen te nemen.

Gebruikers kampen bij innovatieve technologieën vaak met een kennisachterstand, zeker wanneer het geen professionele gebruikers betreft maar burgers zonder specifieke opleiding. Van een fabrikant mag verwacht worden dat hij afnemers en gebruikers voorlicht over de risico's van een nieuwe technologie en de mogelijke mitigerende maatregelen die een gebruiker kan nemen. Andersom is het van belang dat gebruikers(collectieven) de risico's die hun opvallen melden aan fabrikanten en/of de overheid; die laatsten moeten daar dan wel de mogelijkheid voor bieden.

2.2 Cybersecurity

Bijzonder aan de (deels) geautomatiseerde auto is dat het bij veiligheid niet alleen over safetyrisico's gaat maar ook over securityrisico's. Cybersecurity kan namelijk impact hebben op de fysieke veiligheid. Bij een *cyber physical system*, zoals de (deels) geautomatiseerde auto, zijn digitale en fysieke systemen met elkaar verknoopt en vormen cybersecurityrisico's ook risico's voor de fysieke veiligheid.[34] Bij kritieke veiligheidssystemen is beheersing van de cybersecurityrisico's noodzakelijk voor de veiligheid.[35]

De mitigatie van safety- en securityrisico's vergt een verschillende aanpak. Safetyrisico's ontstaan door externe factoren die onbedoelde schade veroorzaken. Deze risico's kunnen worden beheerst door de juiste eisen op te stellen, die aangepast kunnen worden bij nieuw inzicht, maar in essentie redelijk constant zijn. Bij securityrisico's kunnen ook zulke eisen opgesteld worden, maar er moet daarnaast rekening gehouden worden met opzet. Hiervoor is kennis nodig over de intentie en kunde van dreigingsactoren, hun technieken en de kennis over zwakheden van het systeem die misbruikt kunnen worden (kwetsbaarheden). Deze variabelen zullen in de tijd veranderen, waardoor het inschatten van cybersecurityrisico's een momentopname is. Wanneer een auto een aantal jaar oud is kunnen de cybersecurityrisico's wezenlijk verschillen van de risico's tijdens het ontwerpen en de productie van de auto. Hierdoor moet cybersecurity een continu proces zijn gedurende de gehele levensduur van de auto. Om met deze dynamische risico's om te gaan zijn specifieke maatregelen en een controlestructuur nodig.

32 Rathenau Instituut, *Met beleid vormgeven aan sociotechnische innovatie*, 2016.
33 PBL, *Mobiliteit En Elektriciteit in Het Digitale Tijdperk. Publieke Waarden Onder Spanning*, 2017.
34 British Standards Institution, *Connected automotive ecosystems – Impact of security on safety – Code of practice*, vol. PAS 11281, 2018.
35 Bloomfield et al., *Security-informed safety: integrating security within the safety demonstration of a smart device*, 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, 2017.

Daarnaast moet ervan worden uitgegaan dat ieder computersysteem te hacken is mits er genoeg moeite in gestoken wordt door de aanvaller.

Verschillende instanties hebben gedocumenteerd hoe cybersecurity geregeld zou moeten zijn voor IT-systemen in het algemeen en voor IT in voertuigen in het bijzonder.[36, 37, 38, 39, 40, 41, 42] Op basis hiervan zijn acht cybersecurityprincipes voor autofabrikanten en hun toeleveranciers opgesteld op drie gebieden:[43, 44]

Beheersstructuur:

1. Binnen een organisatie is de directie verantwoordelijk voor de cybersecurity. Dat betekent dat de directie betrokken is en stuurt op cybersecurity. Bovendien promoot de directie het belang van cybersecurity voor de organisatie en wordt helder gecommuniceerd wat dit betekent voor de werkwijze.
2. Fabrikanten, inclusief onderaannemers, toeleveranciers en potentiële derde partijen, werken samen om de cybersecurity van het systeem te verbeteren.
3. Cybersecurityrisico's worden op passende en proportionele wijze beoordeeld en beheerst, inclusief de risico's voortkomend uit de toeleveringsketen. Hierbij moet rekening worden gehouden met de intentie en kunde van de dreigingsactoren.

Ontwerp:

4. Het systeem is ontworpen om bestand te zijn tegen aanvallen en op de juiste manier te reageren wanneer afweermechanismen of sensoren uitvallen (*failsafe*).
5. Systemen zijn ontworpen met behulp van een *defense-in-depth*-benadering[45]. *Security-by-obscurity*[46] kan niet worden getolereerd.
6. De opslag en het verzenden van gegevens zijn veilig en kunnen worden beheerst.

Levensduur:

7. De softwarebeveiliging wordt gedurende de hele levensduur van de auto bijgehouden.
8. Fabrikanten zorgen dat nazorg en incidentrespons beschikbaar zijn, zodat ontstane kwetsbaarheden gedurende de hele levensduur zo snel mogelijk opgelost worden en auto's veilig blijven.

Transparantie en samenwerking

Transparantie en samenwerking tussen autofabrikanten, onderaannemers en toeleveranciers, zijn noodzakelijk om kwetsbaarheden, incidenten en dreigingsinformatie te delen. En daarmee te werken volgens bovenstaande principes.

36 ISO en IEC, *ISO/IEC 15408-1:2009*, ISO, 2009.
37 ISO, *The ISO/IEC 27000 family of standards helps organizations keep information assets secure.*, https://www.iso.org/isoiec-27001-information-security.html, geraadpleegd op 23 augustus, 2019.
38 NIST, *NIST Special Publication 800-Series*, https://csrc.nist.gov/publications/sp800, geraadpleegd op 24 januari, 2019.
39 SAE International, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061*, 2016.
40 SAE International, *Requirements for Hardware-Protected Security for Ground Vehicle Applications - J3101*, 2012.
41 NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, 2018.
42 Daarnaast is de ISO/SAE 21434 - Automotive Cybersecurity Standard in ontwikkeling.
43 GOV.UK, *The key principles of vehicle cyber security for connected and automated vehicles*, Gov.Uk, 2017.
44 British Standards Institution, *The fundamental principles of automotive cyber security*, vol. PAS 1885, 2018.
45 Een beveiligingsstrategie waarbij meerdere verdedigingslagen in en rond het te beveiligen systeem zijn aangebracht. Het falen van één verdedigingslaag wordt daardoor opgevangen door de volgende laag.
46 Security die rust op de onbekendheid met de gebruikte elektronica door een potentiële aanvaller.

Openheid richting toezichthouders en wetgevers is nodig om hun inzicht te geven in aantallen en type incidenten die met cybersecurity te maken hebben. Hiermee kunnen zij regelgeving, toezicht en handhaving gefundeerd aanpassen, mocht dit nodig zijn.

Voor de eigenaar van de auto moet het duidelijk zijn wat hij kan verwachten van de software-ondersteuning en de cybersecuritymaatregelen die vanuit de fabrikant gedurende de levensduur van het voertuig worden geleverd. Ook moet duidelijk zijn voor de eigenaar van de auto of hij ook eigenaar is van de daarin aanwezige software. Voor leasemaatschappijen en vlootbeheerders is transparantie in cybersecurity gerelateerde onderwerpen belangrijk zodat zij hun eigen risicoafweging kunnen maken.

Hoofdpunten

Voor een veilig ontwerp van een nieuwe technologie is het nodig om vanaf het begin van de ontwerpfase rekening te houden met de veiligheid en om niet alleen naar de veiligheid van de technologische innovatie op zichzelf te kijken maar ook naar de combinatie met de gebruiker. Voorkómen moet worden dat innoveren wordt gezien als een louter technologisch vraagstuk. Ook hebben fabrikanten een verantwoordelijkheid naar gebruikers om deze voor te lichten over de risico's van een nieuwe technologie.

Nieuwe risico's moeten vooraf worden ingeschat en zoveel mogelijk gemitigeerd. Veilig innoveren vormt een gradueel proces met voortdurende sturing op basis van monitoring en evaluatie. Fabrikanten moeten laten zien dat zij veilig innoveren (transparantie) en gegevens over ongevallen moeten beschikbaar zijn.

De overheid moet (voor)bereid zijn in te grijpen wanneer het gebruik van een nieuwe technologie onveiligheid introduceert.

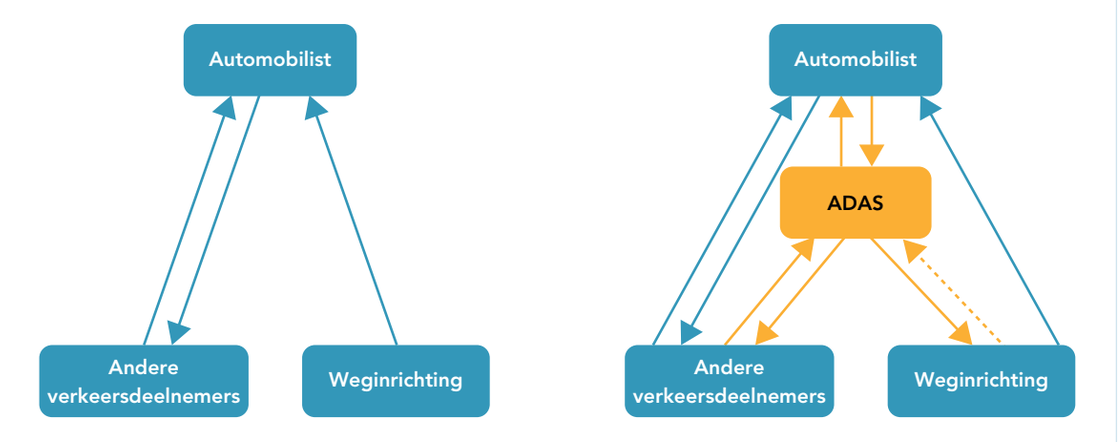
Beheersing van de cybersecurityrisico's is noodzakelijk voor de veiligheid wanneer fysieke en digitale systemen met elkaar verknoopt zijn.

3 BEHEERSING VEILIGHEIDSRISICO'S

De introductie en het gebruik van ADAS veranderen de auto en het wegverkeer. Hierdoor kunnen nieuwe soorten veiligheidsrisico's ontstaan. Risico's zijn inherent aan innovatie, maar dienen wel beheerst te worden. Dit hoofdstuk beschrijft hoe verschillende soorten risico's op dit moment door de betrokken partijen beheerst worden.

Fundamentele karakterverandering van de auto

Technologische ontwikkelingen in (deels) geautomatiseerde voertuigen zorgen ervoor dat een deel van de beslissingen in het verkeer wordt genomen door technologie. Hierdoor ontstaan er nieuwe interacties tussen computer, bestuurder, en andere weggebruikers, zie Figuur 4. De rol en de taken van automobilisten veranderen wezenlijk met de toepassing van ADAS in voertuigen. De automobilist wordt meer een operator dan een directe bestuurder en heeft te maken met veel meer interacties dan in een niet geautomatiseerde auto. Deze verschuiving van rol en taken is groter naarmate de auto van meer en complexere ADAS is voorzien.



Figuur 4: Interacties tussen automobilist en zijn omgeving wanneer hij rijdt in een conventionele auto (linker plaatje) of een auto met ADAS (rechts).

Risicoclusters

Automatisering in het wegverkeer gaat gepaard met de introductie van nieuwe verkeersveiligheidsrisico's. Op basis van onderzoek van ongevallen, bestudering van literatuur en gesprekken met experts hebben we vijf risicoclusters geïdentificeerd:

- Onvolwassenheid systemen
- Bestuurder als operator
- Interactie tussen voertuig en bestuurder
- Dynamiek van automatisering (updates)
- Cybersecurity

In dit rapport beschrijven we niet alle mogelijke risico's, maar geven we per cluster voorbeelden. Deze voorbeelden worden zo mogelijk concreet gemaakt aan de hand van onderzochte ongevallen, zie tabel 2. Deze ongevallen worden in de hoofdtekst uitgebreid omschreven, omdat het een nieuw soort ongevallen betreft waar veel van te leren valt. Meer informatie waaronder de data uit de onderzochte voertuigen is te vinden in Bijlage C. Vervolgens wordt per risicocategorie ingegaan op de risicobeheersing door partijen.

Ongeval	Omschrijving	Voorbeeld in paragraaf
1	Filestaart aanrijding met een vrachtwagen	3.1
2	Noodremsysteem van vrachtwagen voert noodremming uit	-
3	Botsing personenauto met invoegende vrachtwagen	3.1
4	Personenauto botst op langzaam rijdend verkeer	3.2
5	Personenauto rijdt rechtdoor over rotonde	3.2
6	Frontale botsing tussen twee personenauto's	3.3

Tabel 2: Onderzochte ongevallen.

3.1 Onvolwassenheid systemen

Inleiding

Over het effect van de invoering van nieuwe ADAS op de verkeersveiligheid bestaan hooggespannen verwachtingen.[47, 48, 49, 50] In de communicatie en marketing veranderen deze nu en dan in claims, zie onderstaande kader. Deze verwachtingen zijn gebaseerd op kwalitatieve beschouwingen van mogelijk door ADAS te voorkomen ongevallen in combinatie met ongevalsfrequenties van bepaalde typen ongevallen. Deze verwachtingen kennen tal van randvoorwaarden, waaronder volledige invoering van ADAS in het gehele wagenpark, en houden weinig rekening met het gegeven dat door de invoering van ADAS ook weer nieuwe risico's ontstaan.[51, 52] Daarnaast gaan deze studies ervan uit dat de ADAS onder alle omstandigheden perfect werken.

47 De Minister van Infrastructuur en Milieu, *Kamerbrief 31305 Mobiliteitsbeleid*, 2014.
48 EU-lidstaten, *Declaration of Amsterdam; Cooperation in the Field of Connected and Automated Driving*, 2016.
49 AAA Foundation for Traffic Safety, *Potential Reductions in Crashes , Injuries , and Deaths from Large-Scale Deployment of Advanced Driver Assistance Systems*, 2018.
50 Aon Risk Solutions, *Whitepaper: als de auto autonoom wordt; Verkennende analyse van de verzekeringsmarkt en nieuwe risico's bij zelfrijdende auto's*, 2015.
51 ETSC, *Road Safety Priorities for The EU 2020-2030; Briefing for the European Parliamentary Elections*, 2018.
52 ETSC, *BRIEFING | EU Strategy for Automated Mobility*, 2018.

Veiligheidsclaims autofabrikanten

Nissan legt op zijn website nadrukkelijk het verband tussen het gebruik van ADAS en de veiligheid: "Deze technologieën vormen de basis van het geroemde ProPILOT-systeem van Nissan voor veiliger rijden met meer zelfvertrouwen."[53] In een brochure over de Nissan Leaf staat: "Wij gebruiken onze intelligente rijhulpsystemen om voor u op te letten en te helpen om ongelukken te voorkomen". ACEA, de koepelorganisatie van Europese autofabrikanten, stelt dat actieve veiligheidsmaatregelen in staat zijn om het aantal ongelukken en de gevolgen daarvan terug te brengen.[54]

Probleem

De huidige generatie ADAS neemt soms niet de juiste beslissing[55, 56], omdat de technologie nog niet is uitontwikkeld op het moment dat deze wordt geïntroduceerd. Er is dan sprake van 'onvolwassenheid' van het systeem. Automatisering kan (nog) lang niet alle situaties afdekken die in werkelijkheid mogelijk zijn. Hoewel de huidige ADAS de bestuurder wettelijk gezien alleen ondersteunen, ervaren bestuurders in de praktijk dat de ADAS de besturing nu en dan overnemen (zie verder paragraaf 3.2 en 3.3). Bestuurders ervaren soms dat de auto een verkeerde beslissing neemt.

Filestaart aanrijding met Volvo vrachtwagen

Op 27 maart 2017 vond een kop-staartbotsing plaats op de A29 nabij Den Bommel (Goeree-Overflakkee). Hierbij is een vrachtwagen, van het merk Volvo en uit het bouwjaar 2016, achterop een stilstaande trekker met dieplader gereden. De Volvo was voorzien van een in 2015 verplicht gesteld noodremsysteem[57], het zogenaamde Advanced Emergency Braking System (AEBS).

Bij dit ongeval zou AEBS in de Volvo ervoor gezorgd moeten hebben dat deze vrachtwagen tijdig zou remmen, maar dat gebeurde niet. De chauffeur heeft ook geen remming ingezet. Analyse van de tachograafgegevens heeft aangetoond dat de vrachtwagen ongeremd achterop de stilstaande vrachtwagen met dieplader is gebotst met 83 km/uur. Als gevolg van de impact is de laadbak van het chassis van de vrachtwagen losgekomen en, vanaf de achterkant, tegen de cabine gebotst. Daarbij is de cabine van de vrachtwagen geplet tussen de laadbak en de bulldozer op de stilstaande dieplader. De bestuurder van de vrachtwagen is om het leven gekomen.

53 Nissan, *Nissan LEAF - Elektrische auto - Elektrische voertuigen*, 2019.
54 ACEA, *ACEA Position Paper; General Safety Regulation Revision Brussel*, 2018.
55 Gorter en Klem, *Markering en Rijtaakondersteunende Systemen*, Amersfoort: Royal Haskoning DHV in opdracht van de provincie Utrecht, 2016.
56 Eykholt et al., *Robust Physical-World Attacks on Deep Learning Visual Classification*, in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition IEEE, 2018.
57 Verordening (EU) No 347/2012 van de Commissie, 16 april 2012, tot de uitvoering van verordening (EG) 661/2009 van het Europees Parlement en de Raad betreffende typegoedkeuringsvoorschriften voor bepaalde categorieën motorvoertuigen wat geavanceerde noodsystemen betreft. Deze verplichting geldt alleen voor vrachtwagens geproduceerd na de ingangsdatum.

Figuur 5: Luchtfoto van het ongeval op de A29. De Volvo vrachtwagen (wit) is achterop een dieplader met bulldozer gebotst. (Bron: Politie)

Volgens de fabrikant van de vrachtwagen heeft het camerasysteem de dieplader hoogstwaarschijnlijk niet herkend. Het AEBS herkent alleen de achterzijde van veel voorkomende voertuigen, zie bijlage C.2.1 voor de technische details. Een dieplader met daarop een bulldozer komt niet veel voor.

De generatie noodremsystemen die gebruikt werd in deze vrachtwagen slaat bij plotseling spanningsverlies geen gegevens op over het functioneren van het systeem, daarom zijn er geen gegevens beschikbaar van het moment van het ongeval.

Onvolwassenheid AEBS

Het ongeval met de Volvo vrachtwagen laat zien dat AEBS niet in alle gevallen werkt. Ondanks dat AEBS in 2015 verplicht is gesteld voor nieuwe vrachtwagens is er nog een aantal scenario's waarin de huidige generatie noodremsystemen problemen heeft met het detecteren van andere weggebruikers.[58] Ook blijkt dat AEBS in verschillende merken vrachtwagens en personenauto's tijdelijke verkeersmaatregelen (bijvoorbeeld een pijlwagen bij wegwerkzaamheden) niet of nauwelijks detecteren.[59] Dit kan aanleiding geven tot gevaarlijke situaties bij verkeersmaatregelen die worden toegepast bij wegwerkzaamheden en incidenten.

In de toelatingsprocedure voor voertuigen met AEBS wordt de automatische remfunctie getest in drie situaties: nadering stilstaande personenauto, inlopen op langzaam rijdende personenauto en rijden achter een plotseling remmende personenauto[60]. Het functioneren van AEBS bij andere (stationaire) objecten, zoals pijlwagens, is geen onderdeel van de toelatingsprocedure.

58 Klem et al., *AEBS en vrachtwagens; Praktijktest herkenbaarheid vrachtwagens voor Advanced Emergency Braking System Royal Haskoning DHV*, 2017.

59 Van Hattem, Klem, en Gorter, *AEBS en verkeersmaatregelen; Praktijktest zichtbaarheid verkeersmaatregelen voor Autonomous Emergency Braking Systems*, vol. BF1326 Amersfoort: Royal Haskoning DHV, 2017.

60 Verordening (EU) 2015/562 van de Commissie van 8 april 2015 tot wijziging van Verordening (EU) nr. 347/2012 tot uitvoering van Verordening (EG) nr. 661/2009 van het Europees Parlement en de Raad betreffende typegoedkeuringsvoorschriften voor bepaalde categorieën motorvoertuigen wat geavanceerde noodsystemen betreft.

Botsing met invoegende vrachtwagen

Op 11 april 2017 reed een Tesla Model S op de A1 bij Bathmen – een snelweg met twee rijstroken in iedere richting – met geactiveerd Autopilot systeem (combinatie van adaptive cruisecontrol en rijstrookassistentie[61]). Het voertuig reed op de linker rijstrook met hoge snelheid; de ACC was door de bestuurder ingesteld op een snelheid van 150 km/uur.

Op de rechter rijstrook reed een aantal vrachtwagens 'in colonne' achter elkaar. Een van deze vrachtwagens moest plots uitwijken naar de linker rijstrook vanwege een invoegend voertuig. De vrachtwagen wisselde van de rechter naar de linker rijstrook. Op dat moment was de Tesla de colonne met vrachtwagens met hoge snelheid aan het inhalen.

Figuur 6: De Tesla zoals deze tot stilstand kwam onder de oplegger van de vrachtwagen. (Bron: Hof van Twente fotografie)

Onvolwassenheid adaptive cruisecontrol

De bestuurder van de Tesla had niet gezien dat de vrachtwagen van rijstrook was gewisseld; ten tijde van de rijstrookwisseling keek de bestuurder van de Tesla kort in zijn achteruitkijkspiegel. Voordat de Tesla in botsing kwam met de vrachtwagen, nam de snelheid nog af tot ongeveer 128 km/uur doordat Autopilot een voorganger detecteerde en remde – de truck reed toen met een snelheid van 98 km/uur. Met deze snelheid raakte de Tesla de achterkant van de oplegger. De bestuurder van de Tesla raakte niet gewond.

De desbetreffende Tesla was voorzien van een noodrem- en waarschuwingssysteem. Beide systemen traden echter pas zeer kort voor de impact in werking. Te kort om de bestuurder nog in te laten grijpen en de snelheid voldoende te reduceren.

61 Tesla noemt deze systemen TACC en Autosteer.

De fabrikant heeft verklaard dat de versie van het noodrem- en waarschuwingssysteem in de Tesla (2014) goed werkt bij voertuigen recht voor de Tesla, maar nog niet goed in staat is om tijdig voertuigen te detecteren die van rijstrook wisselen. Zowel de initiële remming door Autopilot alsook het activeren van het noodrem- en waarschuwingssysteem werkten zoals ontworpen.

Euro NCAP heeft rijhulpsystemen (combinaties van ACC en LKA, bij sommige merken wel Autopilot of Propilot genoemd) in combinatie met de werking van noodremsystemen in tien verschillende merken auto's getest om consumenten een realistisch beeld te geven van de mogelijkheden van de huidige ADAS.[62] Uit de tests bleek dat de ACC van alle merken moeite heeft met anticiperen op in- en uitvoegend verkeer, omdat de systemen alleen de achterzijde van andere voertuigen herkennen. Een voertuig schuin van achteren wordt niet herkend. Dit gebeurde ook bij het hierboven beschreven ongeval. In andere situaties, zoals het inrijden op een stilstaande file, presteerden de ACC van verschillende merken uiteenlopend. Waar de ene auto met behulp van de ACC rustig afremde voor een file, ging bij de andere auto het noodremsysteem in werking en bij enkele auto's gebeurde zelfs dat niet.

Andere voorbeelden van onvolwassenheid
De huidige beschikbare technologieën voor ADAS bestaande uit een combinatie van ACC, LKA en AEBS zijn in feite uitsluitend bedoeld voor gebruik op wegen met duidelijk gemarkeerde rijstroken, zoals snelwegen. Voorwaarde is wel dat er op de snelweg geen werkzaamheden, ongevallen of andere verstoringen zijn. Deze systemen kunnen echter ook worden ingeschakeld op wegsoorten waarvoor ze volgens de fabrikant niet zijn bedoeld en waarvoor ze niet geschikt zijn.[63] De Autopilot van Tesla houdt bijvoorbeeld geen rekening met rotondes, verkeerslichten, verkeersborden en voorrangssituaties, maar Autosteer kan wel worden geactiveerd op iedere weg, waar de rijstrook voldoende wordt herkend of het systeem denkt deze voldoende te herkennen. Volgens Tesla zijn bestuurders op de hoogte van deze beperkingen en rijden ze graag met de Autopilot geactiveerd waar het maar enigszins mogelijk is.[64] Ook andere fabrikanten hebben geen locatiebeperking (zogeheten *geo-fencing*) ingesteld voor het gebruik van ADAS. Zo stelt bijvoorbeeld Volvo Cars dat Pilot Assist vooral bedoeld is om te gebruiken op wegen buiten de bebouwde kom, maar dit systeem is ook te activeren binnen de bebouwde kom. Hetzelfde geldt voor bijvoorbeeld ProPilot van Nissan. Naast de onduidelijkheid over het toepassingsgebied verrassen deze systemen de bestuurders soms met onverwachte en oncomfortabele acties, zoals plotseling hard remmen zonder duidelijke aanleiding, een uitvoegstrook nemen die de bestuurder niet bedoelt en een bocht uitschieten die scherper is dan waar het systeem voor is geprogrammeerd.

Onderkenning en beheersing van het risico onvolwassenheid
Zoals hierboven uiteengezet, zijn verschillende ADAS nog niet volwassen, waardoor ze niet in alle situaties goed werken en er ongevallen kunnen ontstaan. Het 'leren' tijdens het gebruik is een veel voorkomend kenmerk van de systemen die nu gebruikt worden,

62 Euro NCAP, *2018 Geautomatiseerde Rijsystemen*, 2018.
63 Mits binnen het operationeel ontwerpdomein.
64 Randvoorwaarde is dat er belijning aanwezig is.

omdat in eerste instantie slechts met een beperkt aantal situaties rekening wordt gehouden. Met geautomatiseerde beslisregels wordt een beslissing genomen op basis van een grote hoeveelheid gegevens, zoals sensordata afkomstig van camera's of radar. Door middel van updates kunnen nieuwe beslisregels in ADAS geladen worden. Een voorbeeld van technologische ontwikkeling is de uitbreiding van een detectiesysteem, dat eerst alleen auto's herkende naar een systeem dat ook voetgangers herkent.

Het introduceren van onvolwassen systemen op de weg wordt gezien als een noodzakelijke stap om deze systemen verder te ontwikkelen. Dit hoeft op zichzelf geen probleem te zijn, maar dat is het wel wanneer er te weinig rekening is gehouden met de principes voor veilig innoveren (zie paragraaf 2.1). Zo moeten bestuurders voldoende toegerust zijn om dergelijke geautomatiseerde systemen te doorgronden en hiermee om te gaan (zie paragraaf 3.2 en 3.3), maar bestuurders onderkennen de risico's verbonden aan onvolwassen systemen nog onvoldoende.

Beheersing van deze nieuwe risico's door autofabrikanten vindt plaats op verschillende manieren. Er zijn fabrikanten die systemen voortdurend modificeren en er zijn fabrikanten die alleen nieuwe voertuigen voorzien van updates. Een voorbeeld van een autofabrikant die systemen voortdurend modificeert is Tesla. Tesla stelt dat goed omgaan met zich nog ontwikkelende technologie alleen verantwoord kan als er een kanaal wordt gecreëerd om bestaande systemen regelmatig te updaten. Tesla gebruikt hiervoor 'Over The Air' (OTA) updates, zie verder paragraaf 3.4. Daarnaast sturen Tesla's regelmatig informatie naar de fabrikant, bijvoorbeeld over gevaarlijke situaties en onverwachte ingrepen van het Autopilot systeem. Naast het testen van nieuwe softwareversies binnen een selecte testgroep nodigt Tesla zijn klanten uit om feedback te geven over klachten, ervaringen en bijzonderheden. Deze feedback van auto's en bestuurders gebruikt Tesla dan weer om de systemen verder te ontwikkelen. Om de systemen volwassen te laten worden functioneert de praktijk als 'living lab'. Ook kan risicobeheersing bestaan uit het uitgebreider testen door fabrikanten van hun systemen voordat deze op de markt komen. Daimler laat bijvoorbeeld systemen eerst op verschillende continenten door een groep niet-technische medewerkers testen, doet meerdere circuittesten en voert daarnaast rijsimulatortesten met verschillende testpersonen uit.[65]

Het is niet transparant of en hoe fabrikanten hun product verbeteren op basis van welke informatie, zoals ongevalsinformatie. Fabrikanten zijn niet verplicht om ongevalsdata te verzamelen en te analyseren. Zij vullen het leren van ongevallen op hun eigen manier in. Volvo Cars heeft begin 2019 zijn resultaten van meer dan vijftig jaar ongevallenonderzoek online gezet in zijn E.V.A. (Equality for Vehicle Advancement) initiatief. Deze database bevat informatie over de toedracht van ongevallen inclusief eventueel daarbij betrokken geautomatiseerde systemen. Tesla brengt sinds 2018 per kwartaal een Vehicle Safety Report uit.[66] Deze zijn nog summier, maar Tesla heeft plannen om deze uit te breiden. Andere autofabrikanten rapporteren alleen intern over ongevallen en de veiligheidsprestaties van hun ADAS. De in interviews gegeven overweging van deze

65 Veel van deze procedures zijn intern en dus specifiek voor de fabrikant, maar zijn wel afgeleid van ISO 26262 – een internationale norm voor de functionele veiligheid van elektronische systemen in voertuigen.

66 Tesla, *Q3 2018 Vehicle Safety Report*, https://www.tesla.com/nl_NL/blog/q3-2018-vehicle-safety-report, geraadpleegd op 12 december, 2018.

fabrikanten is dat andere fabrikanten weinig baat hebben bij deze gegevens, omdat ongevallen met andere merken niet vergelijkbaar zijn aangezien deze voertuigen over andere systemen/modules beschikken. We sluiten echter niet uit dat concurrentieoverwegingen ook een rol spelen bij deze terughoudendheid.

Euro NCAP weegt AEBS mee in de veiligheidsbeoordeling ook al werkt het nog niet in alle omstandigheden goed. De reden hiervoor is dat voldoende is aangetoond dat het de veiligheid verbetert. Adaptive cruisecontrol wordt nog niet meegewogen in de veiligheidsbeoordeling, omdat bij Euro NCAP nog onduidelijkheid bestaat over wat de beperkingen en de veiligheidsvoordelen hiervan zijn, zie Bijlage D.

Beheersing risico's door toezicht en wetgeving
ACC wordt breed toegepast in de huidige generatie auto's. Hiervoor gelden geen toelatingseisen.[67] Deze systemen worden door de verschillende toelatingsautoriteiten in Europa niet als onveilig beschouwd en daarom toegelaten (zie schema in Bijlage E), terwijl niet duidelijk is hoe de balans voor de veiligheid uitvalt. Ook voor AEBS in personenauto's is nog geen regelgeving. Voor AEBS in vrachtwagens is deze er wel en deze heeft specifiek als doel het voorkómen van filestaartaanrijdingen waarbij een vrachtwagen achterop een personenauto rijdt.

67 Er is wel een ISO norm: 15622 over de performance requirements.

Deelconclusies

De huidige generatie ADAS is nog niet in alle opzichten volwassen. Ook systemen waarvan bekend is dat ze de verkeersveiligheid verbeteren, zoals AEBS, kunnen verder geperfectioneerd worden. Van andere systemen, zoals ACC, is nog niet duidelijk hoe de voor- en nadelen tegen elkaar afwegen in de praktijk. Desondanks gelden er geen toelatingseisen voor ACC.

De prestaties van soortgelijke ADAS kunnen per merk aanzienlijk verschillen. Systemen herkennen niet alle typen voertuigen of objecten, hebben moeite met in- en uitvoegend verkeer en noodremsystemen remmen niet voor alle typen voertuigen. Dit heeft tot ongevallen geleid.

Systemen zijn niet ontworpen om te gebruiken op elk type weg maar hebben geen locatiebeperking.

Automobilisten zijn onvoldoende bekend met de werking en de beperkingen van de systemen en vertrouwen er desondanks op.

Voor een deel van de huidige soorten ADAS bestaat regelgeving, voor een ander deel ontbreekt deze.

Doorontwikkelen van systemen tijdens het gebruik is inherent aan de huidige generatie technologie. Sommige fabrikanten passen ADAS tijdens de levensduur van de auto aan, terwijl andere dit alleen doen voor nieuw geproduceerde auto's. Het is niet transparant of en hoe fabrikanten hun product verbeteren op basis van monitoring en evaluatie.

Fabrikanten zijn niet verplicht om te leren van ongevallen en vullen dit op hun eigen manier in. De meeste fabrikanten delen de resultaten van ongevallenonderzoek niet met elkaar. Op dit gebied zijn de eerste stappen genomen door Volvo Cars en Tesla.

3.2 Bestuurder als operator

Inleiding
De rol en de taken van automobilisten veranderen met de toepassing van ADAS in voertuigen. De automobilist wordt meer een operator, dat wil zeggen een bewaker van het rijproces, dan een directe bestuurder.[68] Als operator houdt de automobilist in de gaten of zijn met ADAS uitgeruste auto de rijtaken goed uitvoert en grijpt zo nodig in. In sommige gevallen krijgt de automobilist een waarschuwing van zijn auto, wanneer menselijk ingrijpen noodzakelijk is of wanneer het systeem niet overtuigd is van voldoende alertheid van de bestuurder. De automobilist moet vervolgens adequaat reageren, bijvoorbeeld met een stuurcorrectie of door te remmen.[69]

De veranderende rol van de bestuurder speelt bij systemen die gedurende langere tijd een gedeelte van de rijtaak overnemen, zoals *adaptive cruisecontrol* en rijstrookassistentie. Deze veranderende rol speelt niet bij noodsystemen, zoals AEBS.

Naast de verandering van rol is er nog een grote verandering voor de bestuurder, namelijk de toegenomen interactie met het voertuig. Deze interactie brengt ook risico's met zich en deze worden besproken in paragraaf 3.3.

Tesla met Autopilot botst op langzaam rijdend verkeer
Op 25 augustus 2016 reed de bestuurder van een Tesla Model S met geactiveerde Autopilot-functie op de A4 nabij Leiden. Autopilot is een combinatie van *lane keeping assist* en *adaptive cruisecontrol*. Er was sprake van langzaam rijdend verkeer. Matrixborden boven de weg toonden een snelheidslimiet van 50 km/uur. De ACC (door Tesla TACC genoemd) was door de bestuurder ingesteld op een snelheid van 130 km/uur en op de kortste volgafstand.

Figuur 7: Tesla Model S met een snelheid van 58 km/u op zijn voorganger gebotst. (Bron: 112regioleiden.nl)

68 Van Nes en Duivenvoorden, *Veilig naar het verkeer van de toekomst; Nieuwe mogelijkheden, risico's en onderzoeksagenda voor de verkeersveiligheid bij automatisering van het verkeerssysteem*, R-2017-2 Den Haag: Stichting Wetenschappelijk Onderzoek Verkeersveiligheid SWOV, 2017.
69 Kyriakidisa et al., *A Human Factors Perspective on Automated Driving*, Theoretical Issues in Ergonomics Science 18, nummer 1, 2017.

De bestuurder van de Tesla had gemerkt dat het systeem die middag meerdere malen correct tot lage snelheid had afgeremd. Ongeveer vijf minuten voor de botsing werd de bestuurder van de Tesla gewaarschuwd door het *Forward Collision Warning* (FCW) systeem voor een mogelijke botsing met een (andere) voorligger. Direct daaropvolgend werd een remming ingezet door de bestuurder. Hierna heeft hij het Autopilot systeem weer geactiveerd.

Voor een periode van ongeveer vijf minuten voorafgaand aan de botsing was het Autopilot systeem geactiveerd en uit een van de geregistreerde parameters bleek dat de bestuurder zijn handen gedurende deze periode niet aan het stuur had. Er is geen waarschuwing afgegeven door het FCW systeem.

Vlak voor het moment van impact reed de Tesla met een snelheid van ongeveer 67 km/uur. Op 0,5 tot 1,5 seconde voor het bereiken van de voorgaande auto die was gestopt voor een file – op een afstand van 19 meter – begon de bestuurder van de Tesla met remmen. Hij kon hiermee echter niet voorkomen dat de Tesla op zijn voorganger botste waardoor er vervolgens meerdere kop-staartbotsingen tussen vijf andere auto's ontstonden. Hierbij raakte niemand gewond.

Ondanks dat Autopilot was geactiveerd, heeft er geen vorm van snelheidsreductie door het systeem plaatsgevonden. Ook zijn er geen waarschuwingen afgegeven. Wanneer alleen de remweg van de voorganger meegenomen wordt, kan gesteld worden dat de reactietijd van de bestuurder goed was. Een bestuurder wordt echter geacht om veel verder vooruit te kijken dan alleen de voorgaande auto. Uit het onderzoek blijkt dat het aannemelijk is dat de bestuurder deze informatie gemist heeft door de lage taakbelasting of afleiding als gevolg daarvan.

Uit dit ongeval blijkt dat de bestuurder veel vertrouwen had in de Autopilot. Hij had een hoge snelheid ingesteld en hij had gekozen voor een korte volgtijd. Dit vertrouwen werd versterkt doordat het *Forward Collision Warning* systeem hem kort voor het ongeval nog een keer tijdig gewaarschuwd had. Zijn alertheid op het moment dat zijn voorganger ging remmen heeft er aan bijgedragen dat het ongeval niet ernstiger is afgelopen, maar hij heeft niet voldoende geanticipeerd op zijn voorliggers.

Inmiddels heeft Tesla in een update het hands-on detectie interval omlaag gebracht naar 15 seconden. Als de bestuurder zijn handen langer dan deze tijd niet aan het stuur heeft gehad, geeft het systeem een waarschuwing af. Met het omlaag brengen van deze tijdspanne voldoet Tesla aan de UNECE toelatingseisen in R79.03. Ook heeft Tesla later de '*3 strikes you're out*' regel geïntroduceerd, waardoor de bestuurder het voertuig stil moet zetten om Autopilot opnieuw te gebruiken nadat het systeem drie keer heeft gedetecteerd dat de bestuurder zijn handen langer dan 15 seconden niet aan het stuur had.

Langere reactietijden en verminderde alertheid
Het bewaken van het rijproces, zoals het geval is bij rijden met ACC in combinatie met LKA, leidt tot gevaren die bij het zelf actief besturen van de auto niet optreden. Rijprocesbewaking leidt namelijk tot langere reactietijden (tot soms meer dan zes seconden[70, 71, 72, 73] in plaats van circa twee seconden) en het vaker missen van informatie.[74] Daarnaast bestaat het risico op sneller afgeleid raken en verminderde alertheid.

Waymo (dochteronderneming van Google) besloot in oktober 2017 zelfs om te stoppen met het ontwikkelen van systemen die menselijk ingrijpen vergen, omdat er gevaarlijke situaties ontstonden bij testen. De getrainde bestuurders van testvoertuigen waren behoorlijk afgeleid: ze werkten hun make-up bij, keken op hun telefoon of vielen zelfs in slaap.[75]

Uit onderzoek blijkt dat 29% van ADAS-gebruikers op zijn minst af en toe het gevoel hebben zich met andere zaken bezig te kunnen houden dan met het besturen van de auto als zij gebruikmaken van de *adaptive cruisecontrol*.[76] De gevaren van langere reactietijden en het missen van informatie worden versterkt doordat een deel van de bestuurders van geautomatiseerde auto's geneigd is om te vertrouwen op de automatisering, terwijl deze niet in alle situaties goed werkt (zie paragraaf 3.1).

Gebruikers geven aan dat ADAS de rijtaak verlichten, waardoor ze ontspannener rijden. Een enkeling geeft aan dat het daardoor veiliger wordt. Het is echter niet wetenschappelijk vastgesteld of de huidige generatie ADAS leidt tot een lagere mentale taakbelasting.[77] Een bestuurder in een auto met huidige generatie ADAS moet meer verschillende *taken* (in het bijzonder monitoring) uitvoeren dan in een auto zonder ADAS.[78] In de rol van operator moet de automobilist steeds meer informatie checken en bijvoorbeeld de snelheid handmatig in het systeem aanpassen in plaats van door het gaspedaal los te laten of te remmen. Dit telkens checken van de status van het systeem kan ook een risico vormen, doordat het de ogen van de automobilist van de weg haalt.

70 Vlakveld et al., *An empirical exploration of the impact of transition of control on situation awareness for potential hazards; An experiment about the hazard perception capabilities of drivers after interruption in a video-based scanning task*. SWOV, 2015.
71 Endsley en Kaber, *Level of Automation Effects on Performance, Situation Awareness and Workload in a Dynamic Control Task.*, Ergonomics 42, nummer 3, 1999.
72 Wright et al., *Experienced drivers are quicker to achieve situation awareness than inexperienced drivers in situations of transfer of control within Level 3 autonomous environment.*, in Proceedings of the Human Factor and Ergonomics Society 2016 Annual Meeting, vol. 60, 2016.
73 Zhang et al., *Determinants of Take-over Time from Automated Driving: A Meta-Analysis of 129 Studies*, Transportation Research Part F: Traffic Psychology and Behaviour 64, 2019.
74 Vlakveld et al., *Situation awareness increases when drivers have more time to take over the wheel in a Level 3 automated car: A simulator study*, Transportation Research Part F: Traffic Psychology and Behaviour, 2018.
75 Dave, *Google ditched autopilot driving feature after test user napped behind wheel, bewerkt door Sam Holmes Atwater*, California, USA: Reuters, 2017.
76 AAA Foundation for Traffic Safety, *Vehicle Owners' Experiences with and Reactions to Advanced Driver Assistance Systems*, 2018.
77 Zhang et al., *Determinants of Take-over Time from Automated Driving: A Meta-Analysis of 129 Studies*, Transportation Research Part F: Traffic Psychology and Behaviour, 2019.
78 Kyriakidisa et al., *A Human Factors Perspective on Automated Driving, Theoretical Issues in Ergonomics Science*, nummer 1, 2017.

Onderkenning en beheersing van het risico van verminderde alertheid
Fabrikanten kennen het risico dat bestuurders niet alert zijn terwijl zij rijhulpsystemen gebruiken. Soms noemen zij dit 'verkeerd gebruik' van de systemen in plaats van een logisch gevolg van de lage taakbelasting. Fabrikanten proberen deze risico's te mitigeren, bijvoorbeeld door systemen die alertheid meten. Dat vindt bijvoorbeeld plaats door te monitoren of de bestuurder zijn handen aan het stuur houdt en hem middels licht- en/of geluidssignalen te waarschuwen als hij langer dan een bepaalde periode zijn handen niet aan het stuur houdt. Dit is echter geen directe meting van de alertheid maar een gemakkelijker te operationaliseren meting van een mogelijk met alertheid samenhangende gedragscomponent. Renault heeft een andere weg gekozen en een systeem op de markt gebracht dat vermoeidheid detecteert op basis van rijgedrag. Voor dergelijke systemen bestaat nog geen wet- en regelgeving vanuit EC of UNECE. De nieuwe General Safety Regulation (GSR) (zie bijlage E) stelt onder meer de invoering van systemen voor vermoeidheids- en aandachtswaarschuwing en geavanceerde afleidingswaarschuwing verplicht. Aan deze systemen zijn door de EU globale randvoorwaarden gesteld op het gebied van techniek en bescherming van de privacy.

Tesla rijdt over middeneiland rotonde
Op 1 juli 2016, vroeg in de middag, reed een Tesla Model S met hoge snelheid recht over het middeneiland van een rotonde. Aan de andere kant van de rotonde botste de Tesla tegen een paal waarna hij tot stilstand kwam. De bestuurder heeft bij het ongeval zware verwondingen opgelopen.

Ten tijde van het ongeval reed de Tesla op de N57 met Autopilot geactiveerd (ACC en LKA). Een tijdreeksregistratie afkomstig uit het voertuig heeft aangetoond dat het voertuig bij het naderen van de rotonde met een constante snelheid van ongeveer 84 km/uur reed. In ongeveer 3 seconden daarna nam de snelheid af tot 10 km/uur, nog eens 3 seconden later was het voertuig tot stilstand gekomen. Pas tijdens het kruisen van het middeneiland van de rotonde heeft de bestuurder het rempedaal bediend. Het Autopilot systeem heeft geen waarschuwing afgegeven en ook geen vorm van remming toegepast. De bestuurder heeft bij het in gebruik nemen van zijn auto een korte uitleg gehad over de systemen in het voertuig. Ook heeft hij verklaard de meeste informatie over het functioneren van Autopilot uit de handleiding te hebben gehaald. De handleiding vermeldt dat Autosteer bedoeld is voor gebruik op autosnelwegen. Tegelijkertijd geeft de handleiding uitleg over snelheidsbegrenzing bij gebruik van Autosteer binnen de bebouwde kom. Dit impliceert dat het systeem ook daar te gebruiken is. De handleiding geeft overigens geen waarschuwing met betrekking tot rotondes.

De huidige generatie ADAS is ontworpen om gebruikt te worden op wegen waar duidelijke belijning aanwezig is en waar geen andere verstoringen zijn. Deze systemen zijn onder andere niet in staat de auto te besturen in bochten – waarvan de radius onder een bepaalde waarde ligt – en op rotondes. Toch zijn veel van deze ADAS zo ontworpen dat ze te activeren zijn op wegen met scherpe bochten en rotondes. Bij het naderen van zo'n situatie waarschuwt het systeem niet. Het systeem houdt feitelijk alleen de auto binnen de rijstrook en regelt de snelheid die vooraf is ingesteld of zo nodig lager, omdat de voorligger langzamer rijdt. Inmiddels heeft Tesla een update uitgebracht waarmee Autopilot kaartgegevens kan gebruiken om preventief af te remmen en daarmee te

anticiperen op bijvoorbeeld scherpe bochten. Uitgangspunt van het ontwerp van ADAS is dat de bestuurder de controle overneemt, wanneer het systeem de situatie niet meer herkent. Probleem hierbij is dat de automobilist in zijn rol als operator een langere reactietijd heeft en vaker informatie mist dan hij zou doen als bestuurder van een auto zonder ADAS. Hierdoor kan het zijn dat de bestuurder te laat ingrijpt. Dat zien we ook bij dit ongeval waarbij een auto rechtdoor over een rotonde reed.

Figuur 8: Tesla Model S nadat deze tot stilstand is gekomen tegen een paal aan de andere kant van de rotonde. (Bron: Twitter, geplaatst door weginspecteur Jeroen van Rijkswaterstaat)

Kennisgebrek

De veiligheid van ADAS hangt sterk af van hoe ze gebruikt worden. Er bestaan veel misvattingen bij bestuurders over ADAS. Sommigen overschatten de systemen en vertrouwen er te veel op, bijvoorbeeld als de systemen 'auto-pilot' heten[79], maar de bestuurder toch alert moet blijven. Bestuurders weten vaak niet precies welke ADAS in

79 Abraham et al., *What's in a name: Vehicle technology branding and consumer expectations for automation*, AutomotiveUI 2017 - 9th International ACM Conference on Automotive User Interfaces and Interactive Vehicular Applications, Proceedings, September, 2017.

hun auto aanwezig zijn. De functionaliteit hiervan kan per update weer veranderen (zie paragraaf 3.4). Daarnaast kennen niet alle bestuurders de beperkingen van de ADAS in hun auto en is er geen duidelijkheid over waarom bepaalde beslissingen worden genomen door het voertuig. Dit kan leiden tot misverstanden en extra risico's.[80]

Onderkennen en beheersen van het risico kennisgebrek
De helft van de bestuurders gebruikt rijstrookassistentiesystemen zonder enige voorkennis.[81] Een inventarisatie van verschillende online fora en social media laat zien dat bronnen voor informatie meestal zelfstudie en voorlichting door de dealer zijn. Handleidingen zijn in veel gevallen erg lang en worden daarom slecht gelezen. Verder bevatten ze vaak beschrijvingen over de functionaliteit van alle optionele systemen, in plaats van alleen de systemen die daadwerkelijk in het voertuig zitten. Regelmatig bestaan na het lezen van de handleiding nog onduidelijkheden over de omstandigheden waaronder het systeem gebruikt kan worden. Sommige gebruikers ervaren informatievoorziening door middel van een handleiding ook als onvolledig. Onderzoek laat ook zien dat bestuurders de informatie uit handleidingen niet goed toepassen in de praktijk.[82] Daarmee komt instructie over een correcte besturing van een ADAS niet bij de gebruiker terecht.

Sommige fabrikanten vinden voorlichting overbodig, want de bediening moet intuïtief zijn en voor zichzelf spreken. Uitgangspunt daarbij is dat een systeem goed is als een bestuurder het kan gebruiken zonder handleiding. Dit streven wordt niet altijd waargemaakt, want bestuurders lijken niet goed op de hoogte te zijn van de werking en het juiste gebruik van ADAS.[83] Andere fabrikanten vinden dat de gebruiker duidelijke uitleg moet krijgen over de systemen en wat er wel en niet van verwacht mag worden. Zo biedt Volvo Cars kopers van auto's in Nederland een introductiecursus door een gespecialiseerd bedrijf aan. Voor de opleiding van bestuurders is nog geen wetgeving in ontwikkeling (zie paragraaf 4.2.2).

Euro NCAP ontwikkelt testprotocollen om vast te stellen of fabrikanten voldoende duidelijke en niet-misleidende consumenteninformatie verstrekken over ADAS.[84] Daarin moeten onder andere de functionaliteit en de beperkingen van de systemen worden uitgelegd, zodat bestuurders de werking van de systemen begrijpen en de juiste verwachtingen hebben. Deze testresultaten zullen de komende jaren (tot 2025) nog geen invloed hebben op de Euro NCAP sterrenbeoordeling.

Ondanks dat autofabrikanten dealers wel aanmoedigen om klanten te informeren, lijken er geen eisen te zijn vanuit de fabrikanten richting dealers over het voorlichten van klanten over het gebruik van geavanceerde rijhulpsystemen. Bij autodealers waar wel voorlichting wordt gegeven aan de klant blijkt de informatievoorziening vaak incompleet,

80 Carsten and Martens, *How Can Humans Understand Their Automated Cars? HMI Principles, Problems and Solutions*, Cognition, Technology and Work 21, nummer 1, 2019.
81 ANWB, *Verwachtingen werking Lane Assist nog te hoog gespannen; Onderzoek naar rijbaanhulpsysteem in auto's*, 2017.
82 Boelhouwer et al., *Should I Take over? Does System Knowledge Help Drivers in Making Take-over Decisions While Driving a Partially Automated Car?*, Transportation Research Part F: Traffic Psychology and Behaviour 60, 2019.
83 ADAS Alliantie, *ADAS Convenant*, 2019.
84 Euro NCAP, *Euro NCAP 2025 Roadmap: in pursuit of vision zero*, 2017.

zowel bij de aanschaf als bij latere vragen, aangezien de dealers zelf ook niet altijd de juiste informatie hebben. Ook heeft onderzoek aangetoond dat slechts een kwart van de leaserijders instructies over ADAS heeft ontvangen bij de dealer.[85] Dealers en importeurs spelen op dit moment vaak geen rol bij de voorlichting van consumenten. Een belangrijke reden hiervoor is dat zij zelf ook weinig kennis hebben over ADAS in auto's. De BOVAG onderzoekt nog of zijn leden (de dealers) voorlichting als een taak voor zichzelf zien. De RAI-vereniging geeft aan dat niet alleen dealers maar ook importeurs weinig kennis hebben over ADAS in auto's die zij verkopen. Omdat een deel van de fabrikanten er niet voor zorgt dat importeurs, dealers en uiteindelijk de bestuurders voldoende ingelicht zijn, vullen vervolgrijopleidingen deze lacune en trainen ze dealers, importeurs en geïnteresseerde bestuurders. De ANWB ziet het gebrek aan kennis bij bestuurders als een belangrijk risico en geeft algemene voorlichting over ADAS via de website.[86]

De huidige Europese wetgeving voor het rijexamen is strak voorgeschreven. Er is voor lidstaten weinig ruimte om het rijexamen zelf in te vullen. Vanuit het ministerie en CIECA wordt aangedrongen op kaderwetgeving. In de huidige opzet van het rijexamen dat wordt afgenomen door het CBR wordt niet getoetst op een juist gebruik van diverse rijhulpsystemen die aanwezig zijn in het voertuig. Over het algemeen wordt nieuwe technologie pas opgenomen in het rijexamen als deze technologie gemeengoed is. Zo moet pas vanaf 25 maart 2018 een deel van de route tijdens het examen gereden worden met behulp van een navigatiesysteem. Omdat er nog veel verschillen bestaan tussen ADAS kan het CBR het gebruik van ADAS bij het praktijkdeel van het rijexamen nog niet verplichten; wel zou het vragen over ADAS op kunnen nemen in het theoriedeel. Een andere reden is dat veel rijscholen niet beschikken over voertuigen die uitgerust zijn met ADAS en deze voertuigen bijna allemaal automaat zijn, waarmee men dan een automatenrijbewijs krijgt en formeel niet mag rijden in een schakelauto.

Tot voor kort waren alleen duurdere automodellen uitgerust met ADAS. De grote hoeveelheid aan verschillende versies en varianten ADAS vormt een probleem voor de competentieontwikkeling. Examinatoren hebben baat bij uniformiteit; het is lastig om voor elke variant op de hoogte te zijn van de exacte werking en de beperkingen van het systeem. Ook zijn er zorgen over de bekwaamheid van rijinstructeurs op het gebied van ADAS. Samen met de SWOV en andere partijen doet het CBR onderzoek naar de toekomstige invulling van het gebruik van ADAS bij het rijexamen.

In juni 2019 hebben 42 partijen zich verenigd in de ADAS Alliantie en een ADAS Convenant afgesloten (zie paragraaf 4.2.3). Verhogen van de bekendheid van ADAS is één van de pijlers van dit convenant. Een van de maatregelen is een online community (slimonderweg.nl), waar onder andere informatie wordt geboden over de kansen en risico's die ADAS bieden. De website benadrukt vooral dat de zelfrijdende auto nog niet bestaat en dat de bestuurder zelf moet blijven opletten.

85 Harms en Dekker, *ADAS: from owner to user; Insights in the conditions for a breakthrough of Advanced Driver Assistance Systems*, 2017.
86 ANWB, *Welke rijhulpsystemen zijn er?*, 2017.

Deelconclusies
De veranderende rol van de bestuurder naar operator leidt tot langere reactietijden en het missen van informatie. Dit proces wordt versterkt doordat een deel van de bestuurders te veel vertrouwt op ADAS. Deze overschatting van ADAS wordt weer versterkt door de manier waarop autofabrikanten communiceren via advertenties en de media.

Gebruikers hebben beperkt inzicht in de werking van ADAS. De communicatie over de precieze werking en bediening van ADAS blijkt in de praktijk soms niet te voldoen en voorlichting en training blijven vaak achterwege. In het rijexamen wordt niet getoetst op het gebruik van ADAS.

Risico's door ADAS worden gemitigeerd door meer systemen (alertheid- en vermoeidheidsystemen), die ook (nog) niet volwassen zijn.

3.3 Interactie tussen voertuig en bestuurder

Probleem
Hoewel er formeel gezien ook bij de huidige voertuigen met ADAS slechts één bestuurder is, namelijk de automobilist, die volledig verantwoordelijk is voor het gehele rijproces, bestaat in de praktijk de indruk dat er twee bestuurders zijn (menselijke bestuurder en automatisering) als gevolg waarvan nieuwe risico's optreden. Onderzoek in andere context, namelijk arbeidsongevallen, toont aan dat ongevallen zich met name voordoen wanneer meerdere mensen gezamenlijk één proces beheersen of wanneer meerdere mensen deelprocessen beheersen die elkaar beïnvloeden.[87] Problemen doen zich met name voor doordat op de overlappende en grensgebieden er ambiguïteit en conflictsituaties kunnen optreden. Bij voertuigen met ADAS zien we dat terug. Bijvoorbeeld doordat de menselijke bestuurder ervan uitgaat dat de automatisering het proces beheerst of doordat bij de menselijke bestuurder niet duidelijk is wat in de praktijk zijn verantwoordelijkheid is ten opzichte van de automatisering. Het kan ook voorkomen dat de bestuurder niet zeker weet of de ADAS wel of niet is ingeschakeld. Auto's met ingeschakelde ADAS reageren soms anders dan een menselijke bestuurder zou doen. Omgekeerd gaan ADAS ervan uit dat de bestuurder ingrijpt indien nodig (zie ook paragraaf 3.2) soms met en soms zonder waarschuwing. Al met al rijst nu en dan de vraag wie er in de praktijk eigenlijk stuurt.

Dodelijk ongeval met Tesla Model S
Op 30 januari 2019 reed een Tesla Model S op de N277, een provinciale weg in de buurt van Zeeland (Noord-Brabant). Gegevens afkomstig uit het voertuig hebben aangetoond dat het voertuig reed met een snelheid van ongeveer 83 km/uur met ACC geactiveerd.

87 Leplat, *Occupational Accident Research and Systems Approach*, Journal of Occupational Accidents 6, nummer 1–3, 1984.

Om Autopilot te activeren, moet de bestuurder achtereenvolgens ACC en LKA[88] inschakelen. Autopilot werkt alleen op wegen waar duidelijke belijning door het systeem gedetecteerd kan worden. De bestuurder van de Tesla was in de veronderstelling dat het Autopilot systeem geactiveerd was en het voertuig daarmee ook zijn positie in de rijstrook regelde.

Figuur 9: Foto genomen door de camera in de Tesla vlak voor de aanrijding.

Figuur 10: Beide voertuigen na de aanrijding. (Bron: Politie)

88 Tesla gebruikt de termen TACC en Autosteer voor ACC en LKA.

Toen de bestuurder van de Tesla zijn aandacht naar eigen zeggen kort op het scherm in de middenconsole richtte, merkte hij dat het voertuig op de andere rijstrook terecht was gekomen en een tegenligger naderde. De Tesla kwam in botsing met de Nissan. Als gevolg van de botsing overleed de bestuurder van de Nissan; de bestuurder van de Tesla raakte niet gewond.

Uit gegevens afkomstig uit het voertuig is gebleken dat *Autosteer* (LKA) niet geactiveerd was. De handen van de bestuurder waren voor een periode van 9 seconden voorafgaand aan de botsing niet aan het stuur gedetecteerd. Circa 23 seconden voor het moment van impact bewoog de bestuurder twee keer snel achter elkaar het schakelpookje van het Autopilot systeem omhoog. Bij de eerste keer omhoog bewegen werd de TACC snelheid ingesteld op de momentane snelheid, bij de tweede keer werd de ingestelde snelheid verhoogd naar 85 km/uur. De bestuurder heeft zich vergist. Twee keer omhoog met het pookje lijkt erg op twee keer naar je toe trekken (zie blauw kader). De weergave op het scherm verschilt in kleur, namelijk een grijs of blauw wiel rechts boven snelheid. Ook krijgt de bestuurder bij het activeren van Autosteer een geluidssignaal te horen.

De Tesla was wel voorzien van een noodremsysteem maar dit werkt bij de huidige generatie niet bij botsingen met tegenliggers.

Besturing Tesla Autopilot
Het activeren van Tesla Autopilot werkt door middel van een schakelpookje aan de linker achterzijde van het stuur. Autopilot bestaat uit een combinatie van TACC en Autosteer. TACC kan op twee manieren ingeschakeld worden. Door het naar boven of onderen bewegen van het schakelpookje wordt de momentane snelheid ingesteld. Bij het naar de bestuurder toe bewegen van de schakelaar wordt de snelheidslimiet of de huidige snelheid aangehouden. TACC kan alleen worden ingeschakeld als het systeem beschikbaar is, te zien aan het grijze snelheidsmeterpictogram op het instrumentenpaneel.

Indien Autosteer beschikbaar is – het display laat dan een grijs Autosteer-pictogram zien – kan dit geactiveerd worden door het schakelpookje nogmaals naar de bestuurder toe te bewegen. Dit moet gebeuren kort na het activeren van TACC. Na het activeren van Autosteer krijgt de bestuurder een geluidssignaal te horen en wordt het Autosteer-pictogram blauw. Het meermaals omhoog of omlaag bewegen van het pookje zorgt ervoor dat de ingestelde snelheid van TACC aangepast wordt – Autosteer wordt dan niet geactiveerd.

Figuur 11: (a) Als Autosteer beschikbaar is wordt op het instrumentenpaneel een grijs Autosteer-pictogram weergegeven, (b) na het activeren wordt het pictogram blauw. (Bron: Tesla Model S gebruikershandleiding[89])

Onduidelijkheid over wie controle heeft
De bestuurder betrokken bij de frontale aanrijding dacht dat hij Autosteer had aangezet, terwijl dat niet het geval was. Door deze vergissing had hij minder aandacht op de weg. Bij veel merken zijn er verschillende toestanden mogelijk en zijn de verschillen in bediening en de (audio)visuele terugkoppeling subtiel waardoor een vergissing snel gemaakt wordt.

In gevaarlijke situaties waarin de mens de besturing moet overnemen is het belangrijk dat dit duidelijk is voor de bestuurder, omdat anders een bestuurder niet of pas te laat de controle kan overnemen. Daarnaast is het belangrijk dat het systeem op een veilige manier uitschakelt, wanneer de mens de feitelijke besturing niet op tijd overneemt of onvoldoende alert is. In de praktijk ervaren bestuurders bij verschillende merken dat in veelvoorkomende situaties – zoals bij het naderen van een rotonde of bij het naderen van een (te) scherpe bocht – het systeem te laat of niet waarschuwt om de feitelijke besturing over te dragen aan de bestuurder. Onvoldoende alerte bestuurders kunnen hierdoor extra in de problemen komen.

Geen foolproof ontwerp
Het ontwerp was niet *foolproof* genoeg, omdat een bedieningsfout van de bestuurder heeft kunnen leiden tot een ernstig ongeval. Hierbij speelde ook dat de bestuurder niet zag dat de auto niet deed wat hij verwachtte, omdat hij was afgeleid door het scherm in zijn auto. Afleiding komt meer voor wanneer gebruik wordt gemaakt van ADAS, zie paragraaf 3.2.

89 Tesla, *Tesla Model S gebruikershandleiding*, 2018.

Een rijhulpsysteem kan een voertuig besturen onder een aantal voorwaarden. Zo moet het systeem bijvoorbeeld in staat zijn om lijnen op het wegdek te detecteren, werkt het alleen boven of onder een bepaalde snelheid en kan het systeem alleen werken vanaf een bepaalde bochtradius. Dit laatste hangt vaak ook nog weer van de snelheid af, waardoor de bestuurder op basis van een eerdere ervaring kan denken dat het systeem een scherpe bocht goed aan kan, maar dat vervolgens toch niet blijkt te kunnen. Dit kan bijvoorbeeld als hij bij de eerdere ervaring de bocht met een lagere snelheid nam, omdat er een auto voor hem reed en het systeem de snelheid verlaagde ten opzichte van de ingestelde snelheid. Daarnaast spelen omstandigheden, zoals het weer en de lichtinval, soms een rol. Niet alle situaties kunnen van tevoren in kaart gebracht worden, maar zelfs bij veelvoorkomende situaties – zoals het naderen van een rotonde, of het nemen van een te scherpe bocht – is er niet goed nagedacht over de manier waarop een rijhulpsysteem zichzelf uitschakelt en de bestuurder volledige controle over het voertuig moet overnemen. Dit kan resulteren in onveilige situaties.

Onderkennen en beheersen risico's
Volgens autofabrikanten is bij de huidige generatie ADAS volstrekt duidelijk dat de mens altijd alert moet zijn. Juridisch gezien is het bij de huidige generatie ADAS helder wie er verantwoordelijk is. ADAS assisteert of ondersteunt de menselijke bestuurder in zijn rijtaak. De bestuurder moet formeel het voertuig besturen en is dus altijd verantwoordelijk. Tegelijkertijd is de bestuurder daar onvoldoende voor geëquipeerd. De systemen wekken bij sommige menselijke bestuurders namelijk andere verwachtingen (zie paragraaf 3.2), terwijl deze systemen nog niet volwassen zijn (zie paragraaf 3.1). Deze verwachtingen worden mede gevoed door de media en de marketinginformatie van fabrikanten. Daarnaast weten bestuurders soms niet wat de status (aan/uit) van hun systeem is. Dit heeft te maken met onduidelijkheden in de bediening, terugkoppeling (bijvoorbeeld de statusindicatie op het dashboard) en de grote verscheidenheid aan ADAS (zie kader). Fabrikanten onderkennen het risico dat veroorzaakt wordt door de onduidelijkheid over wie er stuurt. Zij proberen dit risico te beheersen door terug te grijpen op het aansprakelijkheidsprincipe en disclaimers te tonen in plaats van te kijken naar de veiligheid van systemen in combinatie met de mensen die de systemen gebruiken.

De grote variatie in ADAS draagt bij aan de onduidelijkheid over de status van het systeem. Partners van de ADAS alliantie (zie paragraaf 4.2.3) gaan voorstellen doen aan de RDW (voor Europese regelgeving) en Euro NCAP (richting fabrikanten) ten behoeve van het ontwikkelen van generieke namen voor typen ADAS, generieke symbolen en, waar mogelijk, een gestandaardiseerde werking van de ADAS. De verantwoordelijkheid voor het toepassen hiervan ligt bij de fabrikanten, want er is op dit moment geen verplichting. Fabrikanten werken nu niet samen om dit te verbeteren. Een uitzondering hierop vormen de samenwerkingsverbanden tussen Daimler en BMW[90] en tussen

90 Daimler, *BMW and Daimler. Plan to headquarter joint venture in Berlin*, https://www.daimler.com/innovation/case/shared-services/jv-daimler-and-bmw.html, geraadpleegd op 22 augustus 2019.

Volkswagen en Ford[91], die samenwerken aan de ontwikkeling van ADAS en zelfrijdende auto's. Een tweede uitzondering vormen ADAS die tijdelijk de stuurfunctie overnemen van de bestuurder. Hier heeft de UNECE in Reglement R.79 een aantal geharmoniseerde eisen aan gesteld (zie Bijlage E4).

Verscheidenheid ADAS
Er zijn verschillen tussen ADAS van verschillende merken en types, maar ook tussen softwareversies. Deze ADAS werken en reageren allemaal net anders en hebben allemaal een eigen operationeel domein (bijvoorbeeld tot welke snelheid ze kunnen werken). Fabrikanten gebruiken deze systemen om zich te onderscheiden van andere merken en gebruiken daarom eigen namen voor de systemen. Zo heeft een onderzoek van de Amerikaanse automobiel vereniging (AAA)[92] aangetoond dat er wel 19 verschillende namen bestaan voor rijstrookassistentie, zoals: active lane assist (Audi), active steering assist (Mercedes-Benz), lane assist (Seat), lane keeping alert (Ford) en intelligent lane intervention (Nissan). Ook maakt rijstrookassistentie vaak weer deel uit van systemen die besturing over de rijrichting en snelheid over kunnen nemen, zoals: Autopilot (Tesla), Pilot Assist (Volvo) en ProPILOT (Nissan). Hetzelfde zien we terug bij andere ADAS.

Mens-machine interactie vormt geen expliciet onderdeel van de voertuigregelgeving en typegoedkeuring. Voor zover dit wordt meegenomen vormt het een integraal onderdeel van de technische voorschriften. Bij de UNECE zijn er geen nieuwe wettelijke eisen op gebied van mens-machine interactie in ontwikkeling voor ADAS van SAE level 1 en 2 (de huidige generatie ADAS). Deze zijn wel in voorbereiding voor ADAS van SAE level 3 en hoger. IenW heeft de Nederlandse inbreng bij WP.29 van de UNECE (voertuigeisen, zie Bijlage E) gemandateerd aan de RDW. Ondanks aanzetten kennis te ontwikkelen, heeft de RDW beperkte kennis op het gebied van mens-machine interactie. Als gevolg daarvan is de Nederlandse inbreng bij de UNECE op dit gebied ook beperkt. Ook de EC heeft geen verzoek gedaan om hier eisen voor te ontwikkelen.

Verder gaan overheden ervan uit dat wetgeving op gebied van HMI (*Human Machine Interaction*) minder belangrijk is voor de huidige generatie ADAS, omdat de bestuurder aansprakelijk is (zie verder paragraaf 4.2.2). Juridisch gezien assisteren ADAS de menselijke bestuurder slechts in zijn rijtaak. Maar in de praktijk nemen ADAS het rijden volledig over onder bepaalde omstandigheden. Systemen kunnen zelf gasgeven, sturen en remmen, totdat ze in een situatie komen waar ze niet voor ontworpen zijn. Dit betekent dat wetgeving op gebied van HMI ook van belang is voor de huidige generatie ADAS.

91 Volkswagen, Ford – *Volkswagen expand their global collaboration to advance autonomous driving, electrification and better serve customers*, https://www.volkswagen-newsroom.com/en/press-releases/ford-volkswagen-expand-their-global-collaboration-to-advance-autonomous-driving-electrification-and-better-serve-customers-5188, geraadpleegd op 22 augustus 2019.
92 AAA, *Advanced Driver Assistance Technology Names*, 2019.

De UNECE[93] geeft aan dat op gebied van human factors en ADAS nog veel onderzoek nodig is, want er zijn alleen globale overwegingen. Gesteld wordt dat de bestuurder van een auto met ADAS optimaal functioneert als hij:

- '*in the loop*' is en niet '*out of the loop*';
- een gemiddelde mentale werkbelasting heeft;
- tijdens de gehele autorit een goed situationeel bewustzijn heeft;
- passend vertrouwen heeft in het rijhulpsysteem;
- geen negatieve gedragsaanpassingen als gevolg van het rijhulpsysteem vertoont.

Om deze algemene uitgangspunten te concretiseren, beveelt de UNECE aan op de volgende punten nader onderzoek te doen:

- Methoden om situationeel bewustzijn tijdens autorijden te meten, te begrijpen hoe het varieert, te schatten wat het voorkeursniveau is en hoe dit kan worden vastgehouden.
- Methoden om mentale onderbelasting en overbelasting te meten, een te grote afhankelijkheid van ADAS bij bestuurders te voorkomen en negatieve gedragsaanpassing van bestuurders aan ADAS te voorkomen.
- Het verkennen van manieren om de verantwoordelijkheid van bestuurders waar te kunnen maken bij toenemend niveau van automatisering in de auto.

Om meer te leren over human factors en ADAS is de eerste *naturalistic driving study* (5 merken, 20 proefpersonen) sinds drie jaar gaande in Nederland. Deze wordt in opdracht van het ministerie van IenW, de RDW en RWS uitgevoerd door TNO in samenwerking met de SWOV. De eerste fase van dit onderzoek, voornamelijk dataverzameling is afgerond. IenW bekijkt of er vervolgonderzoek nodig is en zo ja met welke vraagstelling. In de Verenigde Staten is ook een grote *naturalistic driving study* gaande.[94] De eerste resultaten van deze studie laten zien dat Tesla Autopilot wordt gebruikt in een derde van de gereden afstand en dat bestuurders relatief alert blijven.[95] Een mogelijke verklaring hiervoor is dat Autopilot nog niet perfect is en dat bestuurders gemiddeld iedere 16 km ingrijpen. Dit zou kunnen betekenen dat naarmate systemen beter worden, bestuurders minder alert zijn.

Het bestaan van mens-machine interactie risico's is bekend bij IenW en de EC. Zo worden risico's op dit gebied als uitdaging bij het ontwikkelen van automatisch rijden gezien[96]. Zoals iedere innovatie, kent de huidige generatie ADAS voor- en nadelen. Deze voor- en nadelen moeten tegen elkaar worden afgewogen, waarbij de balans van deze winst- en verliesrekening door moet slaan richting de voordelen. Het voordeel is dat het door de ADAS ondersteunde of overgenomen deel van de rijtaak op een constant en hoog veiligheidsniveau wordt uitgevoerd. Een nadeel is dat men er voetstoots van uitgaat dat

93 Appendix bij Annex 5 van de UN R.E.3
94 Fridman et al., *MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction With Automation*, IEEE Access 7, 2019.
95 Fridman et al., *Human Side of Tesla Autopilot: Exploration of Functional Vigilance in Real-World Human-Machine Collaboration*, 2019.
96 High Level Group on the Competiteness and Sustainable Growth of the Automotive Industry in European Union, Gear 2030, 2017.

de bestuurder in kan grijpen wanneer een systeem niet functioneert. In dergelijke omstandigheden geldt de menselijke bestuurder als veiligheidsbarrière. Ongevallen en onderzoek laten zien dat de mens als barrière niet werkt wanneer deze afgeleid is. Het leidt ook tot de paradoxale situatie dat de bestuurder in laatste instantie de veiligheid moet garanderen terwijl zijn rol door automatisering juist kleiner zou zijn geworden mede in het belang van de veiligheid. Als de mens in bepaalde omstandigheden inderdaad de belangrijkste "veiligheidsbarrière" zou zijn, is het bovendien des te frappanter dat de vraag hoe mens en machine zich tot elkaar verhouden nauwelijks wordt betrokken bij de introductie en toelating. Vooral ook omdat het door zijn rol als operator (paragraaf 3.2) juist lastiger geworden is om adequaat te reageren.

Deelconclusies

Het is voor bestuurders soms onduidelijk wie de controle heeft. Dit kan leiden tot ongevallen mede doordat het ontwerp van de systemen niet *foolproof* is en vergissingen van de gebruiker niet altijd opvangt, voorkomt of beperkt. Dit leidt tot de paradoxale situatie dat de technologie het rijgedrag veiliger moet maken, maar dat de bestuurder als ultiem verantwoordelijke soms in een moeilijkere positie is gebracht.

Vaak wordt er door fabrikanten en overheden teruggegrepen op het aansprakelijkheidsprincipe (bestuurder als barrière) in plaats van te kijken naar de veiligheid van systemen in combinatie met de mensen die de systemen gebruiken. Mens-machine interactie vormt geen expliciet onderdeel van de regels voor typegoedkeuring.

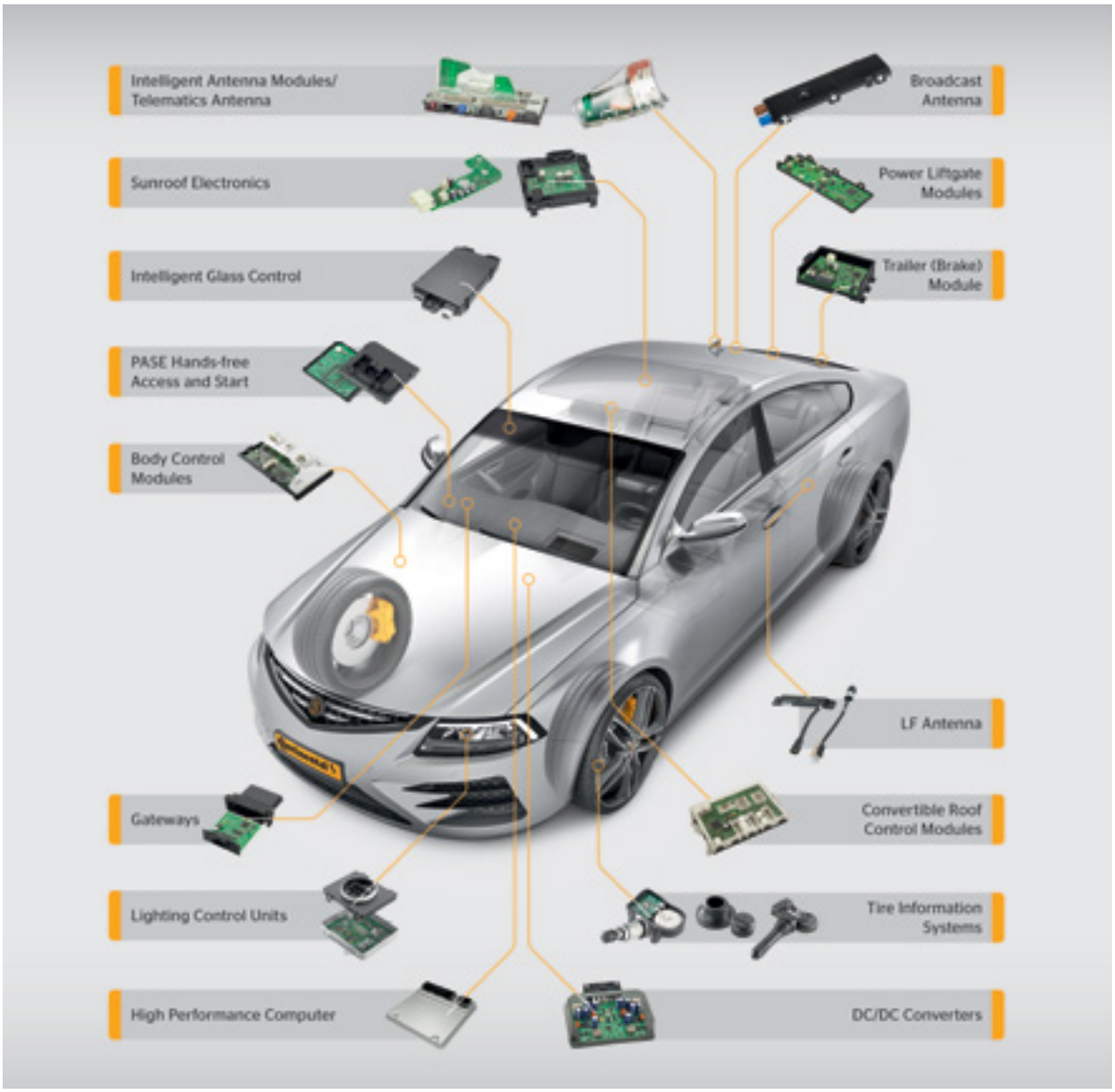
Er is meer (wetenschappelijk) onderzoek naar human factors en ADAS in de praktijk nodig, bijvoorbeeld door *naturalistic driving studies* uit te voeren.

3.4 Dynamiek van automatisering

Inleiding

Digitalisering in de auto kent een vrij lange voorgeschiedenis. In 1977 werd de ECU[97] (Electronic Control Unit, zie Figuur 12) en daarmee software in de auto geïntroduceerd. Sindsdien is de hoeveelheid software sterk gegroeid (zie Figuur 13) door automatisering zoals ADAS, maar ook ten behoeve van navigatie en infotainment. ADAS nemen hun omgeving waar door middel van sensoren. Deze sensoren genereren grote hoeveelheden data die door computersystemen in de auto verwerkt worden. Op basis van algoritmes bepaalt het computersysteem hoe het de bestuurder ondersteunt bij de rijtaak. Dan gaat het bijvoorbeeld om het activeren van de rem of het genereren van een waarschuwing.

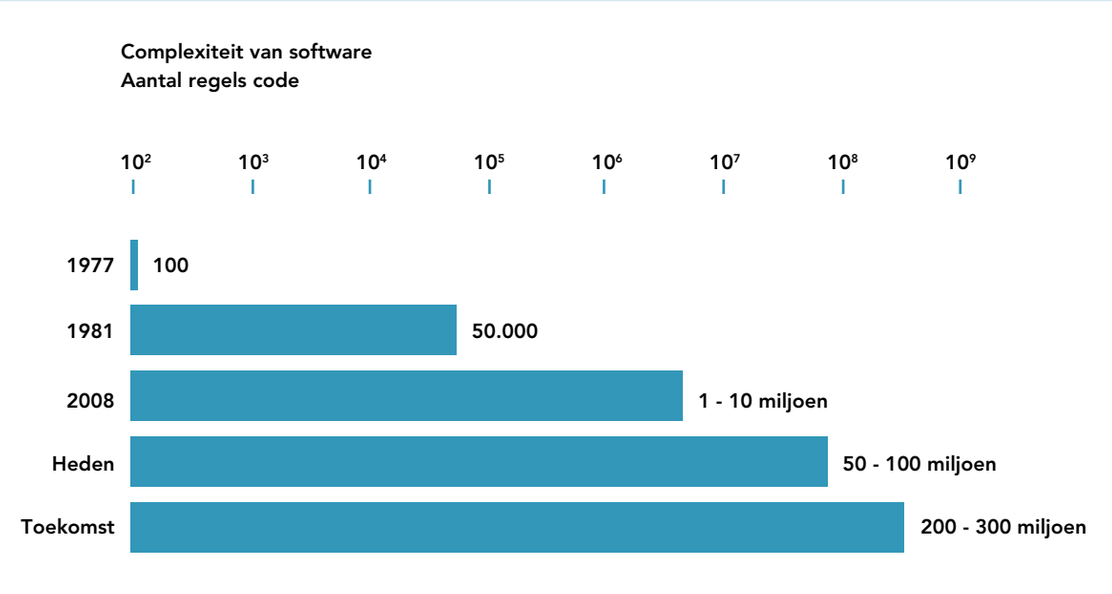
97 Een ECU is een soort mini-computer die als besturingseenheid terug is te vinden in diverse systemen binnen een voertuig. Ze worden onder anderen gebruikt voor het aansturen van de klimaatregeling, infotainmentsysteem en geavanceerde rijtaakondersteunende systemen.



Figuur 12: Verschillende Electronic Control Units (ECU) in de auto. (Bron: Continental[98])

Met de komst van hedendaagse ADAS heeft de hoeveelheid software in een modern voertuig een grote vlucht genomen, zie Figuur 13. Ter vergelijking: de hoeveelheid software die tegenwoordig in een moderne auto te vinden is, is groter dan die in een Boeing 787 passagiersvliegtuig of een F-35 straaljager[99, 100]. Met de komst van *connected cars* –voertuigen die onderling kunnen communiceren en informatie kunnen uitwisselen met de infrastructuur – is te verwachten dat de hoeveelheid en complexiteit van software in een voertuig alleen maar verder zullen groeien.

98 Folda, *From requirement to standard security test; A brief introduction to the world of security testing*, Vector cybersecurity symposium 2019, 2019.
99 McCandless, Doughty-White, and Quick, Million Lines of Code, https://informationisbeautiful.net/visualizations/million-lines-of-code/, geraadpleegd op 10 juli, 2019.
100 Charette, *This Car Runs on Code*, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, geraadpleegd op 21 augustus, 2019.



Figuur 13: Ontwikkeling van de hoeveelheid software in auto's. (Bron: gebaseerd op gegevens uit C't magazine[101])

De ontwikkeling van een nieuw model auto is traditioneel een lang proces. Het duurt vaak meerdere jaren voordat een nieuw model van de productieband afrolt. Softwareontwikkeling daarentegen is meestal een iteratief ontwikkelproces waarbij de ontwerp-, assemblage-, test- en uitrolfase elkaar afwisselen en deels parallel lopen. In de auto-industrie zijn deze twee werelden samengekomen. Enerzijds is er de wereld van de statisch-mechanische auto, die na productie, los van een aantal kleine wijzigingen, geen grote veranderingen meer ondergaat. Anderzijds is er de wereld van de rijdende computer, waar door middel van software-updates gedurende de gebruiksfase grote veranderingen kunnen worden doorgevoerd ten aanzien van de aanwezige functionaliteiten en daarmee in het rijgedrag. De transformatie naar de rijdende computer heeft ook gevolgen voor de auto-industrie. Volkswagen werkt op dit moment met zeventig verschillende besturingssystemen die draaien met software van bijna tweehonderd verschillende leveranciers en onderneemt initiatieven om dit landschap te versimpelen.[102]

Waar softwarecode wordt geschreven, worden ook fouten gemaakt. Om deze fouten te minimaliseren wordt er binnen de auto-industrie gebruikgemaakt van normen om veilig te programmeren.[103] De ISO-norm[104] geeft aan dat bij veiligheidskritische software hier extra aandacht aan besteed moet worden. Fabrikanten geven aan deze norm te volgen. Toch is het onvermijdelijk dat software bij introductie nog fouten (*bugs*) en kwetsbaarheden bevat. Wanneer bugs of kwetsbaarheden na introductie van de auto ontdekt worden en impact hebben op het goed functioneren of de veiligheid van de auto,

101 C't Magazine, *Connected cars in de fout bij cybersecurity*, 2016.
102 *Volkswagen, Volkswagen start Car.Software met 5.000 in-house ontwikkelaars*, https://www.volkswagen.nl/nieuws/volkswagen-start-carsoftware-met-5000-in-house-ontwikkelaars/, geraadpleegd op 10 juli 2019.
103 British Standards Institution, *Connected automotive ecosystems – Impact of security on safety – Code of practice*, 2018.
104 ISO, *ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level Gene*, 2018.

moeten deze zo spoedig mogelijk opgelost worden. Voorwaarde voor het gemakkelijk kunnen updaten van software is dat de auto beschikt over een Over-The-Air (OTA)[105] updatemechanisme. Dit is nu alleen bij de nieuwste en duurdere modellen het geval, maar wordt steeds meer toegepast. Het grootste gedeelte van de huidige auto's heeft geen OTA updatemechanisme en in deze auto's kan software alleen worden geüpdatet bij een dealer of garagebedrijf. Dit is een kostbaar proces en zal in de praktijk alleen gebeuren als het nodig is om aan de productverantwoordelijkheid[106] te voldoen of om nieuwe functionaliteit toe te voegen.

Probleem
Er zijn mogelijk risico's verbonden aan het veranderen van de software of het uitblijven van aanpassingen aan de software.

Het uitblijven van noodzakelijke updates is een mogelijk risico bij oudere auto's. De dynamiek van software-updates is van belang voor het repareren van bugs en voor het blijvend goed functioneren van de auto. De huidige auto's gaan ruim 20 jaar mee, terwijl computersystemen en consumentenelektronica meestal maximaal 5 jaar ondersteund worden door fabrikanten.[107] Het is onduidelijk of soft- en hardware van auto's de hele levensduur van de auto ondersteund worden. Wanneer dat niet het geval is, wordt ADAS software van oudere auto's niet meer aangepast en worden eventuele bugs niet meer verholpen.

Een veranderende mens-machine interactie is een risico, wanneer updates worden gebruikt om nieuwe functionaliteiten te introduceren of om bestaande ADAS aan te passen. Het rijgedrag van de auto zal hierdoor veranderen, met als risico dat de auto anders reageert dan een bestuurder verwacht en/of gewend is. Dit speelt mogelijk sterker bij OTA updates dan bij door de dealer uitgevoerde updates, waar de dealer de gelegenheid heeft de automobilist te informeren over de wijzigingen. Bestuurders worden hierover vaak beperkt geïnformeerd, terwijl een goede voorlichting aan de bestuurder essentieel is, wanneer het rijgedrag van een auto verandert door een software-update. Informeren gebeurt nu bijvoorbeeld in de vorm van een pop-up op het dashboard. Dit is geen goede manier om bestuurders te informeren over een verandering in het rijgedrag, omdat de pop-up verschijnt als iemand op het punt van vertrek staat. Bovendien wordt vaak weergeven welke functionaliteit verandert, maar niet wat dit voor een gevolg heeft voor het uitvoeren van de rijtaak. Daarnaast is de rijtaak een ingesleten patroon van mens-machine interactie, waardoor een bestuurder mogelijk niet goed reageert, ook al is deze ingelicht over veranderingen in het rijgedrag van de auto.

Door OTA te gebruiken voor updates – wat meerdere voordelen heeft – worden nieuwe cybersecurityrisico's geïntroduceerd (zie paragraaf 3.5).

105 OTA refereert naar het proces om op afstand software of configuratie instellingen op elektronische apparaten aan te kunnen passen.
106 In lijn met R79, Annex 6, UNECE 1958 agreement waarin staat aangegeven dat software veilig moet zijn.
107 Een voorbeeld hiervan is de software van smart-TV's. Bron: Van der Staak, *Verdwijnende apps op smart-tv's*, 2018.

Onderkenning en beheersing risico's
Om de computersystemen in moderne auto's te onderhouden, zijn regelmatige updates nodig. Tesla is een voorbeeld van een fabrikant die intensief gebruikmaakt van OTA. In een Tesla heeft de bestuurder de keuze om te bepalen wanneer en waar updates geïnstalleerd worden. Na de installatie ontvangt de bestuurder een overzicht van wijzigingen aan het systeem op het dashboard waarin alle wijzigingen in de functionaliteit of mogelijkheden van de systemen op het voertuig worden beschreven. Ook is het mogelijk voor de bestuurder om een notificatie te ontvangen op de mobiele telefoon, zodat de bestuurder weet wanneer een update heeft plaatsgevonden. De meeste auto's die zich nu op de weg bevinden, beschikken niet over een OTA systeem. Fabrikanten waren tot nu toe nog terughoudend met OTA, omdat het nieuwe technologie betreft en implementatie hiervan kosten met zich meebrengt. Het oplossen van softwarefouten is voor auto's zonder OTA een relatief lang en kostbaar traject, omdat dit bij de dealer moet gebeuren. Voor een bestuurder is het onduidelijk of hij de laatste versie op zijn auto heeft, als hij niet regelmatig naar de dealer gaat. Daarnaast is het voor de bestuurder niet altijd duidelijk welke fouten zijn opgelost in een bepaalde softwareversie. Toezichthouders en opsporingsinstanties hebben geen inzicht of auto's wel de laatste versie hebben geïnstalleerd. Het is daarom ook onbekend voor welk deel van de auto's dit het geval is en hoe groot dit probleem is.

Fabrikanten geven gebruikers geen duidelijkheid over de levensduur van hun product, daarom is niet bekend hoelang ze computersystemen in verschillende merken en typen actief blijven ondersteunen.

Voor de dynamiek van software-updates, die mogelijk invloed hebben op het rijgedrag, is nog geen regelgeving beschikbaar en er is dus geen toezicht. Er zijn evenmin specifieke vereisten aan het onderhouden van software in ADAS. Wel moet in algemene zin worden voldaan aan de zorgplicht door de fabrikanten en moet de auto veilig blijven.[108] Regelgeving voor software en software updates is in ontwikkeling (zie paragraaf 4.2.2).

De grenzen waarbinnen software van ADAS mag veranderen tijdens de levensduur van de auto zijn evenmin vastgesteld. Veranderingen van de software die invloed hebben op de emissie van de auto staan onder verscherpt toezicht sinds het bekend worden van het emissieschandaal in 2015 (zie onderstaande box).

Emissieschandaal
Software is dynamisch en bepaalt (mede) het gedrag van de auto. Een bekend voorbeeld in het recente verleden is het emissieschandaal rond het verbrandingsgedrag van dieselmotoren. De boordcomputer herkende dat er een emissietest werd uitgevoerd en veranderde de werking van de motor, zodat deze binnen de gestelde emissienomen bleef tijdens deze test. Wereldwijd zijn miljoenen auto's van verschillende merken teruggeroepen om deze "sjoemelsoftware" te laten vervangen, zodat de auto ook tijdens het rijden aan de gestelde normen voldeed.[109]

108 Verordening (EU) 2018/858, artikel 14.
109 Teffer, Dieselgate. *Hoe de Industrie Sjoemelde En Europa Faalde*, 2017.

De RDW heeft met een individuele fabrikant afspraken gemaakt over de grenzen waarbinnen software van bestaande auto's mag veranderen voordat voertuigen die reeds van een kenteken zijn voorzien opnieuw een typekeuring moeten ondergaan om de toelating te continueren, zie onderstaande box. Dit is een tijdelijke en informele afspraak in een specifiek geval en geen algemene oplossing, bijvoorbeeld omdat niet duidelijk is wat er gebeurt als de fabrikant het betreffende model uit productie neemt en de in gebruik zijnde auto's een update nodig hebben.

Gentlemen's agreement
Om de risico's die horen bij het dynamische karakter van software-updates enigszins te beheersen, heeft de RDW afspraken gemaakt met een autofabrikant over het updaten van software in voertuigen van deze fabrikant. De updates die reeds in gebruik genomen voertuigen ontvangen, zijn gelijk aan de updates die zijn toegepast in nieuw gefabriceerde voertuigen. Het idee hierachter is dat nieuw gefabriceerde voertuigen bij oplevering aan de toelatingseisen moeten voldoen en daarmee dus ook de reeds in gebruik genomen voertuigen aan deze eisen voldoen.

Deelconclusies
Software bepaalt (mede) het rijgedrag van de auto. Het is nodig om software tijdens de levensduur van een auto te kunnen updaten, met name voor het corrigeren van fouten in de software. ADAS kunnen tijdens hun levensduur worden verbeterd met behulp van een software update als er nieuwe inzichten of betere modellen zijn ontwikkeld.

Veiligheidsrisico's kunnen zowel ontstaan wanneer noodzakelijke veiligheidsupdates uitblijven als wanneer er updates worden uitgevoerd die de functionaliteit veranderen.

Er is geen verplichting voor de autofabrikanten om fouten in software op te lossen gedurende de levensduur van de auto. Wel moet er voldaan worden aan de zorgplicht door de fabrikanten en moet de auto veilig blijven. Veel bestaande automodellen beschikken niet over de juiste techniek in de vorm van OTA om op een efficiënte manier software updates uit te voeren.

Er bestaat nog nauwelijks regelgeving op het gebied van software in ADAS. Daardoor is toezicht op de dynamiek van deze automatisering niet mogelijk.

3.5 Cybersecurity

ADAS bestaan uit sensoren en computersystemen die zich in de auto bevinden. In de afgelopen jaren maakte de automatisering een stormachtige ontwikkeling door, waardoor de hoeveelheid soft- en hardware in auto's met ADAS exponentieel is toegenomen ten opzichte van conventionele auto's. Daarmee worden ook de risico's die horen bij computers steeds meer in auto's met ADAS geïntroduceerd.

Probleem
De komst van geavanceerde ADAS in voertuigen brengt risico's met zich mee op het gebied van cybersecurity. De hedendaagse auto die is uitgerust met ADAS beschikt onder andere over meer externe verbindingen (een groter aanvalsoppervlak) en heeft hiermee dus meer digitale ingangen die beveiligd moeten worden tegen opzettelijk misbruik.[110] Ook hebben ADAS gezorgd voor een directere link tussen de computersystemen in de auto en de besturing van het voertuig. Met digitale toegang tot de ADAS kan de auto, in ieder geval in theorie, op afstand bestuurd worden. Dat betekent dat een kwaadwillende die het lukt om deze toegang te krijgen, op afstand een auto of meerdere auto's bijvoorbeeld kan laten remmen, sturen of gasgeven of de remmen uitschakelen, met potentiële gevolgen voor de verkeersveiligheid.

De verbinding die moderne auto's met computersystemen van de fabrikant hebben voor updates van software, file-informatie, onderhoudsberichten en informatie zorgt ervoor dat ook deze systemen een belangrijke rol hebben in de cybersecurity van de auto's. Bij het compromitteren van deze systemen kan een aanvaller digitale toegang krijgen tot veel auto's tegelijkertijd zonder fysiek aanwezig te hoeven zijn in de buurt van de auto's.

Ethische hacks
Verschillende onderzoeken (ethische hacks[111]) hebben aangetoond dat systemen in voertuigen die zich al op de openbare weg bevinden gehackt kunnen worden; ze bevatten kwetsbaarheden die misbruikt kunnen worden waardoor de verkeersveiligheid in het geding komt.

In 2014 toonden Amerikaanse onderzoekers als eerste aan dat zij in staat waren om op afstand in te breken op het computersysteem van een Jeep Cherokee en een Toyota Prius.[112, 113, 114] Vervolgens bleken zij in staat om de controle over te nemen van een aantal ADAS en zo het rijgedrag van de auto te beïnvloeden. Bij de aanvallen die de onderzoekers uitvoerden op de Jeep Cherokee, konden zij de bestuurders en inzittenden

110 Voorbeelden hiervan zijn verbindingen met computersystemen van de fabrikant, wifi in de auto en bluetooth koppelingen.
111 Bij een ethische hack worden beveiligingssystemen van computers en netwerken getest met als doel fouten en veiligheidslekken op te sporen in de systemen en netwerken om deze daarna te melden aan de bedrijven of instanties.
112 Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, geraadpleegd op 17 augustus, 2018.
113 Greenberg, *Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video) Forbes*, https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#38c3a6b1228c, geraadpleegd op 23 augustus, 2018.
114 Greenberg, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/, geraadpleegd op 23 augustus, 2018.

van de auto's ernstig in gevaar brengen. Zo was het bijvoorbeeld mogelijk om de motor of de remmen uit te schakelen en de stand van het stuur aan te passen om zo invloed uit te oefenen op de rijrichting. Als reactie op deze hack besloot Jeep om 1,4 miljoen auto's terug te roepen om de kwetsbaarheden te verhelpen.[115] De terugroepactie bestond uit het toesturen van een USB-stick naar de eigenaren van de auto's, waarmee deze zelf de auto moesten updaten. Hierdoor is niet geborgd of alle auto's tijdig zijn geüpdatet.

Figuur 14: Tijdens het experiment met de Jeep Cherokee werd onder andere het remsysteem uitgeschakeld waardoor de bestuurder niet meer kon remmen en het voertuig in een greppel eindigde (Bron: Wired).

In 2016 voerden Chinese onderzoekers van Keen Security Lab (onderdeel van Tencent, een Chinees internetbedrijf) een ethische hack uit op alle toen bestaande modellen van Tesla. Het bleek mogelijk om op afstand verschillende onderdelen van de Tesla's aan te sturen en te beïnvloeden, zoals de zijspiegels inklappen of de achterbak openen tijdens het rijden. Ook was het mogelijk de remmen te activeren en stuurbekrachtiging en ABS uit te schakelen.[116] Tesla heeft binnen enkele dagen deze kwetsbaarheden met een OTA update verholpen. Dit is bevestigd door de onderzoekers van Keen Security Lab.

Meer recent, tot februari 2018, heeft Keen Security Lab een jaar onderzoek gedaan naar de beveiliging van auto's van BMW, waarbij verschillende kwetsbaarheden zijn gevonden. De bevindingen zijn gepubliceerd en gepresenteerd op de Blackhat USA security conferentie, nadat deze eerst aan BMW gerapporteerd zijn en BMW mitigerende maatregelen genomen heeft.[117, 118] De gevonden kwetsbaarheden maakten verschillende aanvalsscenario's mogelijk. Het bleek mogelijk om via een gesimuleerd mobiel netwerk

115 Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/, geraadpleegd op 17 augustus, 2018.
116 Nie, Liu, en Du, *Free-fall: Hacking Tesla from wireless to CAN bus*, in Blackhat, vol. Briefings USA, 2017.
117 Tencent, *Experimental Security Assessment of BMW Cars: A Summary Report*, 2018.
118 Cai et al., *0-days & Mitigations : Roadways to Exploit and Secure Connected BMW Cars*, White Paper Blackhat USA 2019 Conference, 2019.

toegang te krijgen tot de Telematics Control Unit (TCU)[119]. Ook was het mogelijk om digitale toegang tot het infotainment systeem te krijgen via lokale toegang tot de auto of het overnemen van de communicatie van de auto met de "ConnectedDrive" dienst van BMW. Wanneer een aanvaller op één van deze manieren digitale toegang had gekregen tot de auto, kon hij ondanks de aanwezigheid van domeinisolatie berichten versturen naar afgeschermde ECU's waardoor specifieke functies van de auto bediend konden worden. Ook was het mogelijk om via een SMS uit een eigen gesimuleerd mobiel netwerk de BMW Remote Services te misleiden, waarmee de deuren geopend kunnen worden of de climate control bediend wordt. BMW heeft de toegang via een gesimuleerd mobiel netwerk direct na het ontvangen van de ontdekte problemen opgelost via een OTA update in de getroffen automodellen. Vervolgens zijn de kwetsbaarheden in de auto's en de problemen in de servers waarmee de auto's verbinding maken opgelost. De openheid van BMW over dit incident en het delen van ervaringen hierover is een positief voorbeeld binnen de auto-industrie.

Geen ongevallen bekend

Tot nu toe zijn er geen ongevallen bekend waarbij cybersecurity een rol heeft gespeeld. Dat betekent niet dat uitgesloten kan worden dat deze hebben plaatsgevonden. Security-onderzoekers uit verschillende landen zijn in staat gebleken om auto's van buitenaf te hacken en daarbij ook het rijgedrag van de auto te beïnvloeden. Hiermee is aangetoond dat het mogelijk is. Er wordt echter niet voldoende informatie opgeslagen in auto's of datacentra van de fabrikanten waarmee achteraf onderzocht kan worden of een cybersecurity incident ten grondslag ligt aan een ongeval. Ook wordt hier niet actief op gemonitord. Op deze manier blijft het onduidelijk of cybersecurity een rol heeft gespeeld bij het ontstaan van een ongeval.

Ook in de in ontwikkeling zijnde eisen voor een Event Data Recorder (EDR), zie ook paragraaf 5.2.2, zijn geen eisen opgenomen met betrekking tot het opslaan van data die inzicht kunnen geven in mogelijke cybersecurity incidenten.

Onderkenning en risicobeheersing

Zowel overheden als fabrikanten en toeleveranciers hebben de afgelopen jaren meer aandacht gekregen voor cybersecurity. De auto-industrie heeft normen ontwikkeld waar een groot deel van de fabrikanten en toeleveranciers al aan voldoen en de overige zich aan conformeren. Zo heeft de SAE (Society of Automotive Engineers) in 2016 een handboek uitgebracht als hulpmiddel voor organisaties binnen de sector om cybersecuritybedreigingen te identificeren en kwantificeren en hier vanaf de ontwerpfase rekening mee te houden.[120] Deze normen gaan in op de punten uit ons referentiekader (zie paragraaf 2.2). Momenteel werkt de sector aan een ISO/SAE norm voor cybersecurity in de auto-industrie[121] die in 2020 gepubliceerd zal worden.

119 Een TCU is een computersysteem in de auto dat gegevens verzamelt en deze kan delen met de fabrikant of eigenaar. Het gaat bijvoorbeeld om de positie en snelheid van het voertuig.
120 SAE International, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061*, 2016.
121 ISO/SAE 21434 - *Automotive Cybersecurity Engineering Standard* in ontwikkeling.

Naast de industrienormen hebben diverse overheidsinstanties zoals ENISA, NHTSA en de nationale overheid van Groot-Brittannië richtlijnen en best practices gepubliceerd. [122, 123, 124, 125] Ook zijn er verschillende Europese onderzoeksprojecten uitgevoerd op het gebied van security van connected cars.[126] Er bestaat echter nog geen specifieke regelgeving over cybersecurity in en rond auto's (ontwikkelingen in wetgeving worden beschreven in paragraaf 4.2.2). Cybersecurity is nu als guideline beschreven in een appendix bij toelatingseisen.[127]

Voor nieuw te produceren auto's kunnen fabrikanten de nieuwe cybersecurityprincipes standaard in het ontwerpproces meenemen, maar deze zijn niet verplicht. Voor oudere voertuigen die al enkele jaren op de weg rijden is dit niet het geval, omdat deze ontworpen en geproduceerd zijn in een periode dat er minder aandacht was voor cybersecurity. In oudere ECU modellen is het soms niet mogelijk om de software aan te passen door gebrek aan opslagcapaciteit of het afwezig zijn van een update mechanisme.

Oudere modellen auto's zijn niet ontworpen om de softwarebeveiliging gedurende de gehele levensduur bij te kunnen houden. Wanneer het technisch niet mogelijk is om kwetsbaarheden op te lossen, zijn er soms wel mitigerende maatregelen mogelijk, die misbruik van een bepaalde kwetsbaarheid beperken. Dit kan voldoende zijn om de ergste risico's te beperken, maar doordat de kwetsbaarheden blijven bestaan wordt de *defense-in-depth*-benadering (cybersecurityprincipe 5) aangetast.

Binnen de auto-industrie is het ongewoon te publiceren over problemen rondom cybersecurity omdat de veronderstelling is dat openheid hierover juist voor meer veiligheidsproblemen kan zorgen. Als een kwetsbaarheid die nog steeds te misbruiken is publiek wordt, kan dat namelijk grote gevolgen hebben. Door het gebrek aan openheid is onbekend of de kwetsbaarheden die zijn blootgelegd door de ethische hacks uitzonderingen zijn of dat soortgelijke problemen spelen bij meer auto's. Het onderzoeken van auto's door onafhankelijke cybersecurity experts gebeurt een stuk minder dan het hacken van reguliere software systemen, omdat het kostbaarder is, er minder informatie over de hard- en software van de systemen beschikbaar is en er software gebruikt wordt waarvan de broncode meestal niet beschikbaar is. Voor controlerende instanties, vlooteigenaren en individuele autobezitters is er daarom nauwelijks informatie beschikbaar over eventueel aanwezige kwetsbaarheden in de systemen van een bepaald type auto.

122 NHTSA, *A Summary of Cybersecurity Best Practices*, 2014.
123 NHTSA, *Cybersecurity Best Practices for Modern Vehicles*, 2016.
124 ENISA, *Cyber security and resilience of smart cars; Good practices and recommendations*, 2016.
125 British Standards Institution, *The fundamental principles of automotive cyber security. Specification, vol. PAS 1885*, 2018.
126 Bijvoorbeeld https://www.preserve-project.eu/, https://www.evita-project.org/.
127 ECE/TRANS/WP.29/78/Rev.6 Annex 6

Deelconclusies
De introductie van ADAS in voertuigen en de toename van het aantal externe verbindingen brengen risico's met zich mee op het gebied van cybersecurity. Autofabrikanten zijn zich bewust van het belang van cybersecurity en laten dat zien door hun inzet bij het ontwikkelen van normen en *best practices*.

Er zijn geen ongevallen bekend waarbij een gebrek aan cybersecurity een rol heeft gespeeld. Dit betekent niet dat uitgesloten kan worden dat deze plaats hebben gevonden. Er wordt niet voldoende informatie opgeslagen waarmee achteraf onderzocht kan worden of een cybersecurityincident ten grondslag heeft gelegen aan het ontstaan van een ongeval.

Onafhankelijke cybersecuritytests worden niet vaak uitgevoerd, terwijl deze er aan kunnen bijdragen dat de sector beter bestand is tegen cyberaanvallen. Voor controlerende instanties, vlooteigenaren en individuele autobezitters is er nauwelijks informatie beschikbaar over eventuele kwetsbaarheden. Eerder geproduceerde auto's voldoen mogelijk niet aan de huidige cybersecuritynormen waardoor ze een blijvend veiligheidsrisico kunnen vormen. Controle hierop ontbreekt.

3.6 Conclusies

De voortschrijdende automatisering in het wegverkeer gaat vooral uit van de technische mogelijkheden en stelt de bestuurder onvoldoende centraal. Er komen systemen op de markt die nog niet zijn uitontwikkeld en onvolwassen zijn. Fabrikanten en overheden hanteren bij de huidige generatie ADAS (SAE Level 2) als uitgangspunt dat de bestuurder de volledige verantwoordelijkheid draagt en de systemen slechts ondersteunen. Dat betekent dat de bestuurder altijd kan en moet ingrijpen wanneer een systeem niet functioneert. Dit voelt voor de bestuurder in de praktijk echter anders. Hij ervaart dat hij de controle over het rijden met zijn auto en de daarin aanwezige systemen deelt. Bovendien is het voor de mens in de rol van operator juist lastiger geworden om adequaat te reageren dan wanneer de mens zonder ADAS rijdt. Deze systemen zijn onvoldoende afgestemd op de menselijke gebruiker en de mens is niet getraind om met deze systemen om te gaan.

De auto verandert geleidelijk in een rijdende computer. Hierdoor nemen cybersecurityrisico's toe en het is niet bekend in hoeverre fabrikanten deze risico's beheersen. Automatisering is per definitie een dynamisch proces, waarin software in de auto tijdens het gebruik wordt aangepast. Dit kan invloed hebben op het rijgedrag van de auto en daarmee op de verkeersveiligheid. Zowel aan het uitvoeren van updates als aan het uitblijven van noodzakelijke veiligheidsupdates zijn risico's verbonden.

Uit dit onderzoek komt naar voren dat risico's die verbonden zijn aan automatisering in het wegverkeer niet voldoende beheerst worden. Dit roept de vraag op in hoeverre zich op stelselniveau knelpunten voordoen bij de introductie van ADAS (hoofdstuk 4) en de monitoring tijdens het gebruik in de praktijk en de bijsturing (hoofdstuk 5).

4 KNELPUNTEN VOOR EEN VEILIGE INTRODUCTIE VAN ADAS

De introductie van nieuwe ADAS bestaat uit het ontwerp van de systemen en vervolgens de toelating op de openbare weg. In beide fases is de vraag van belang: welke rol speelt veiligheid? Deze vraag is vooral pregnant omdat ADAS juist worden ingezet om het aantal verkeersslachtoffers te verminderen en zeker niet mogen worden ingezet als ze de verkeersveiligheid negatief beïnvloeden. Juist vanuit dit (beleids-)perspectief is het nodig dat verkeersveiligheid een leidend principe is bij ontwerp en toelating. Dit betekent dat nieuwe risico's moeten worden onderkend en herkend en zo veel mogelijk moeten worden beheerst. Nieuwe risico's mogen niet bij voorbaat worden geaccepteerd. Hoofdstuk 3 toont aan dat er verschillende soorten nieuwe risico's ontstaan die niet beheerst worden. Bovendien is onbekend of het effect van verschillende ADAS op de verkeersveiligheid per saldo positief is. In dit hoofdstuk identificeren we belangrijke knelpunten in het maken van een veilig ontwerp (paragraaf 4.1) en in het toezicht hierop in de vorm van toelating (paragraaf 4.2). De principes voor veilige introductie van nieuwe technologie (referentiekader, paragraaf 2.1) en de cybersecurityprincipes (paragraaf 2.2) worden hiervoor gebruikt.

4.1 Ontwerp

4.1.1 Innovatie niet gedreven door veiligheid

Veel ADAS zijn ontworpen omdat de (technologische) ontwikkelingen zich voordeden. Vooral door het goedkoper, krachtiger en compacter worden van nieuwe technologie zijn er veel mogelijkheden voor het ontwikkelen van functionaliteiten die tot voor kort niet mogelijk waren. Autofabrikanten en toeleveranciers zien deze mogelijkheden en spelen hier op in met als doel marktwaarde te creëren. Het verbeteren van de veiligheid staat niet altijd centraal bij het ontwikkelen van diverse systemen zoals LKA en ACC en combinaties daarvan zoals Autopilot en ProPilot. Deze systemen dragen bij aan het rijcomfort en de ontwikkeling hiervan is technologiegedreven. Er is daarom niet vanaf het begin rekening gehouden met de veiligheid (veiligheidsprincipe: *safety by design*). Hierin bestaan overigens verschillen tussen autofabrikanten.

4.1.2 Onvoldoende kennisuitwisseling in de leveringsketen

Een beperkt aantal autofabrikanten ontwikkelt systemen geheel binnenshuis. Daarmee zijn er geen afhankelijkheden van externe partijen en is kennis over ADAS geborgd binnen de organisatie. Het overgrote deel van de autofabrikanten laat de ontwikkeling van dergelijke systemen over aan partijen die hierin gespecialiseerd zijn, de zogenoemde *Tier-1 suppliers*.

In de praktijk is het vaak zo dat autofabrikanten – die sensoren, systeemcomponenten en software inkopen van toeleveranciers – voldoende kennis hebben over de werking van deze ADAS ter integratie in hun voertuigen. Men heeft echter minder detailkennis over de werking en beperkingen van de sensorhardware of de softwareversie in de hardware. In veel gevallen is dit uitbesteed aan de leverancier, maar kan onvoorziene gevolgen hebben bij de integratie in hun voertuig (veiligheidsprincipe: transparantie).

4.1.3 Gebruiker staat niet centraal bij het ontwerp

Fabrikanten vinden *failsafe* en *foolproof* design belangrijk en gebruiken deze principes in hun ontwerpproces. Zij vinden het belangrijk dat de systemen intuïtief zijn en dat de gebruiker na een korte periode weet hoe en onder welke omstandigheden de systemen werken. Ook is er aandacht voor het veilig tot stilstand komen van het voertuig wanneer de gebruiker geen input geeft.[128] Het ongevallenonderzoek van de Raad (paragraaf 3.2 en 3.3) illustreert dat aandacht voor de combinatie van techniek en gebruiker nog een knelpunt is. Dit knelpunt is ook bij de autofabrikanten bekend. In hoofdstuk 3 is aangetoond dat de ontwerpen niet altijd *foolproof* zijn. Dat betekent niet dat ervan uitgegaan moet worden dat de bestuurder een '*fool*' zou zijn, maar de bestuurder is wel in veel gevallen ongetraind en niet deskundig op het gebied van ADAS. Er zijn ontwerpen die tot onveilige situaties kunnen leiden, bijvoorbeeld omdat de systemen plotseling uitschakelen of niet werken en de bestuurder niet meer wordt ondersteund, terwijl hij daar wel op rekent. Voorbeelden van mogelijk onveilige situaties zijn scherpe bochten of nadering van een rotonde zonder voorliggers. De ADAS-alliantie stelt dat de bestuurder de controle over het voertuig deelt met het voertuig, terwijl zij aan de andere kant het standpunt hanteren dat de bestuurder verantwoordelijk is.[129] Voor bestuurders is dit een lastige situatie, omdat het voor bestuurders onduidelijk kan zijn wie de controle heeft (veiligheidsprincipe: autonomie).

Ontwerpprincipes

Failsafe, of faalveilig, is een ontwerpprincipe waarbij een systeem op een zodanige manier moet zijn ontworpen dat het, in het geval van het falen van de techniek, op een veilige manier terug moet kunnen vallen op de menselijke bestuurder en niet mag leiden tot een minder veilige werking.

Foolproof ontwerp houdt in dat systemen zo ontworpen zijn dat het niet fout gaat bij ondeskundig of verkeerd gebruik, bijvoorbeeld dat een onjuiste bediening wordt gecorrigeerd.

Duidelijkheid over de controle houdt in dat het voor de gebruiker duidelijk moet zijn onder welke voorwaarden en omstandigheden een systeem de controle heeft en wanneer de gebruiker.

128 Er bestaan tussen autofabrikanten verschillen over hoe veilig tot stilstand komen moet worden ingevuld: op de eigen rijstrook, op de rechter rijstrook, op de vluchtstrook, op de dichtstbijzijnde parkeerplaats. Ook tussen overheidsinstanties verschillen de meningen hierover. Binnen de UNECE wordt hierover gesproken met als uiteindelijk doel om op termijn tot regelgeving te komen.

129 ADAS Alliantie, *ADAS Convenant*, 2019.

Doordat de ontwerpen niet *foolproof* zijn, is voorlichting over de werking nodig. In praktijk wordt de handleiding vaak niet of nauwelijks gelezen. Daarnaast biedt de handleiding onvoldoende duidelijkheid en spelen dealers en importeurs op dit moment vaak geen rol bij de voorlichting van consumenten (zie paragraaf 3.2). Daarmee komt instructie over juist en veilig gebruik van een ADAS niet bij de gebruiker terecht (veiligheidsprincipe: transparantie).

4.1.4 Onbekend of ontwerp secure is

In oudere automodellen is soms sprake van *security-by-obscurity*, waarbij de gedachte is dat een computergestuurd systeem veilig is als de specifieke werking van het systeem geheim blijft. Of dit nu ontstaan is door een bewuste keuze of dat dit het gevolg is van de geslotenheid over specificaties in een concurrerende markt is onduidelijk. Wel heeft het voortbouwen op een bestaande (verouderde) architectuur invloed op het blijven bestaan van deze *security-by-obscurity* in plaats van een gelaagde verdediging (ook wel *defense-in-depth* benadering genoemd). Dit bemoeilijkt het hacken van auto's wel, maar voorkomt het uiteindelijk niet als er voldoende motivatie is voor een hacker. Aan de buitenkant van een auto is niet te zien hoeveel van de security nog rust op de onbekendheid met de gebruikte elektronica door een potentiële aanvaller (*security-by-obscurity*) of het gevolg is van goede beschermingsmaatregelen in de vorm van een gelaagde verdediging. (Cybersecurityprincipes: Ontwerp)

De systemen die invloed kunnen hebben op de cybersecurity van de auto reiken verder dan de fysieke grenzen van de auto. Denk hierbij aan het kaartmateriaal met actuele route-informatie, communicatie tussen voertuigen, communicatie met autofabrikanten voor updates en informatieverzameling, telemetrie-apparaten die na verkoop worden toegevoegd (*after market devices*), de mobiele telefoons die gekoppeld worden aan het entertainmentsysteem van de auto en de apps waarmee de eigenaar gegevens kan inzien van zijn auto en deze kan bedienen via zijn mobiel. Dit zijn allemaal voorbeelden van systemen buiten de auto, die direct invloed kunnen hebben op de cybersecurity van de auto als geheel. Omdat deze systemen door vele auto's gebruikt worden, kan de impact bij misbruik van deze systemen erg groot zijn. Van deze systemen is niet altijd bekend of het ontwerp secure is. Er bestaan op dit moment voor deze aanverwante systemen geen toelatingseisen en evenmin permanente eisen.

4.1.5 Onderhoud gedurende de levensduur

Voor het onderhoud van computersystemen, zoals in moderne auto's, wordt de software aangepast tijdens het gebruik. Deze updates zijn erop gericht bugs en kwetsbaarheden op te lossen, waardoor de veiligheid van het voertuig gedurende de levensduur niet vermindert. Nu is het vaak zo dat updates na een bepaalde tijd niet meer uit worden gebracht. Bij sommige fabrikanten worden er helemaal geen updates uitgebracht voor bestaande voertuigen als er zich geen klachten voordoen. Als er problemen met systemen aan het licht komen, worden bij sommige fabrikanten alleen die specifieke voertuigen van een update voorzien, terwijl in soortgelijke systemen in de gehele vloot mogelijk dezelfde problemen spelen. Een fabrikant (en anders de toezichthouder) onderneemt actie wanneer het nodig is om aan de zorgplicht te voldoen, bijvoorbeeld met een terugroepactie van bepaalde modellen. Specifieke regelgeving is in ontwikkeling (zie paragraaf 4.2.2). Daarnaast zijn er allerlei praktische problemen met het uitvoeren van updates, omdat daar tijdens het ontwerp in het verleden weinig rekening mee is gehouden. (Cybersecurityprincipes: levensduur)

De nieuwste auto's met ADAS beschikken vrijwel allemaal over de mogelijkheid om draadloos te communiceren (OTA) met bijvoorbeeld de autofabrikant, waarmee het updaten van software gemakkelijker is geworden. Daarmee kunnen cybersecuritydreigingen beter beheerst worden. Om de software van oudere auto's te onderhouden die nog niet over OTA beschikken, zal dit dus bij de dealer of garage moeten gebeuren. Verschillende autoleveranciers zijn terughoudend om de software tot de laatste versie bij te werken. Het kost de auto-industrie doorgaans meer moeite om kwetsbaarheden te verhelpen in vergelijking met de IT-sector. Dit komt doordat er hoge eisen gesteld worden aan de functionele veiligheid[130] van de systemen tijdens ontwikkeling, productie en onderhoud. Hierdoor vindt er certificering en validatie plaats voordat een update daadwerkelijk wordt uitgerold. Het vereist een complex proces van registratie, testen en beheer van alle mogelijke hard- en software combinaties om te voorkomen dat met het updaten nieuwe problemen geïntroduceerd worden. Bovendien kunnen bij eenzelfde model auto in de loop der jaren verschillende typen ECU's toegepast zijn waardoor het softwareonderhoud complexer wordt.

Met het laten voortbestaan van kwetsbaarheden wordt de gelaagde beveiliging aangetast, daardoor kan een nieuw ontdekte kwetsbaarheid grotere gevolgen hebben. Het oplossen van alle kwetsbaarheden is mogelijk praktisch niet haalbaar door de kosten en technische beperkingen. Het probleem is dat niet duidelijk is op welke manier fabrikanten hier keuzes in maken en op basis van welke overwegingen. Het is dus ook niet duidelijk of in een bepaald eerder geproduceerd model en type auto bij de fabrikant bekende kwetsbaarheden zitten. Specifieke richtlijnen vanuit overheden hierover zijn er niet.

Deelconclusies

Het ontwerp van ADAS is hoofdzakelijk gedreven door de technologische mogelijkheden. Het ontwerp van verschillende ADAS is daardoor op bepaalde punten niet veilig en geeft voor een gebruiker niet altijd duidelijkheid over wat het systeem kan en doet en wat de rol van de bestuurder is en waarom. Ook is het in de praktijk voor de bestuurder niet altijd duidelijk wie er feitelijk stuurt. Fabrikanten zorgen er onvoldoende voor dat bestuurders goed begrijpen hoe ADAS werken. De bestuurder staat niet altijd voldoende centraal bij het ontwerp van ADAS.

In veel gevallen is het onduidelijk of de software van een bepaald eerder geproduceerd model en type auto up-to-date is en bij de fabrikant bekende kwetsbaarheden bevat.

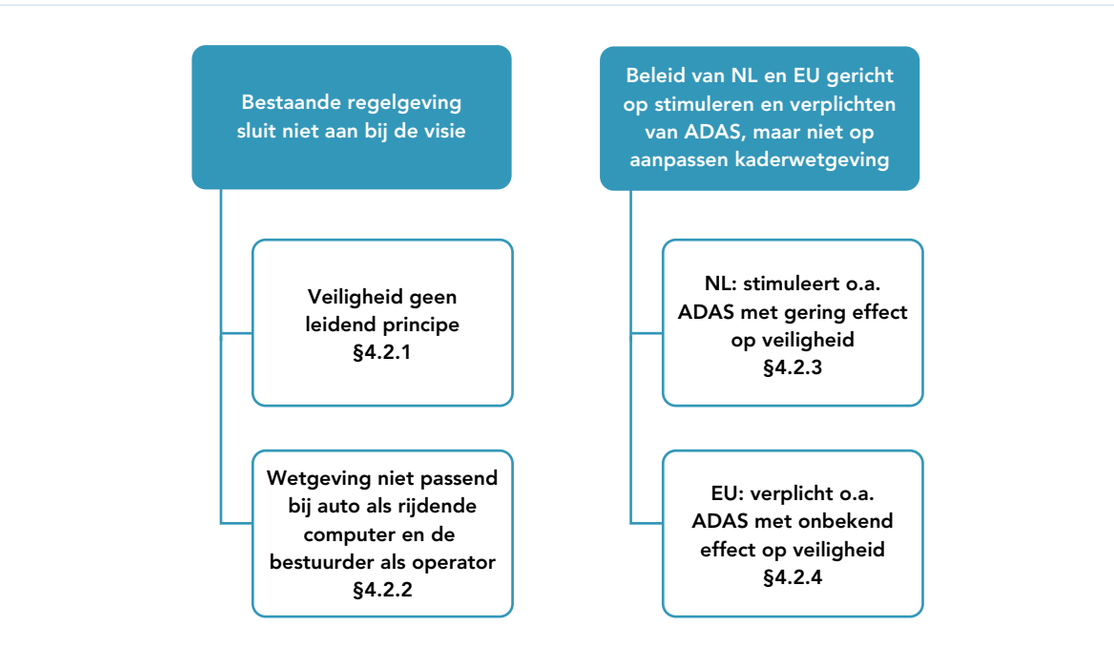
De cybersecurity gedurende de gehele levensduur van de auto is onvoldoende geborgd en afhankelijk van de goede intenties en professionaliteit van de fabrikant.

130 ISO, *ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level*, 2018.

4.2 Toelating en beleid

In de visie van de Nederlandse overheid en de Europese Commissie moeten ADAS een belangrijke bijdrage leveren aan het verlagen van het aantal verkeersslachtoffers, zie paragraaf 1.1. Hiervoor zou veiligheid een leidend principe moeten zijn bij ontwerp en toelating. In deze paragraaf wordt beschreven in hoeverre de bestaande regelgeving voor toelating en het onderliggende beleid van Nederland en de Europese Commissie op het gebied van ADAS aansluiten bij de ambitie de verkeersveiligheid te verhogen.

We laten zien dat de bestaande regelgeving voor toelating niet aansluit bij de visie dat ADAS een belangrijke bijdrage leveren aan het verlagen van het aantal verkeersslachtoffers, omdat verhoging van de veiligheid geen leidend principe is bij toelating (paragraaf 4.2.1) en omdat de wetgeving niet past bij de auto als rijdende computer (paragraaf 4.2.2), want de wetgeving is ontwikkeld voor de 'mechanische' auto. Bovendien zijn het Nederlandse (paragraaf 4.2.3) en Europese beleid (paragraaf 4.2.4) wel gericht op het stimuleren van ADAS, maar niet of nauwelijks op het mitigeren van risico's en het aanpassen van de kaderwetgeving.



Figuur 15: Hoofdstukindeling.

4.2.1 Veiligheid geen leidend principe

Om ADAS een belangrijke bijdrage te laten leveren aan het verlagen van het aantal verkeerslachtoffers, zou verhoging van de veiligheid een leidend principe moeten zijn bij ontwerp en toelating. In de huidige voertuigregelgeving zien we dit uitgangspunt echter niet consequent terug.

Bij toelating van nieuwe ADAS op grond van artikel 20 van Richtlijn 2007/46/EG geldt als voorwaarde om ontheffing te verlenen dat hiermee uitgeruste voertuigen ten minste een even hoog veiligheidsniveau bereiken. Dit is minder ambitieus dan een verhoging van het verkeersveiligheidsniveau.

In de voertuigregelgeving wordt bovendien nergens aangegeven hoe het veiligheidsniveau van een ADAS kan worden beoordeeld. De onduidelijkheid in het beoordelen van het veiligheidsniveau heeft tot gevolg dat fabrikanten geen risico-inschatting en scenario's hoeven aan te leveren (veiligheidsprincipe 4). Ook zijn er vaak geen wetenschappelijk onderbouwde uitspraken over de veiligheid van bepaalde systemen, omdat daarvoor beter verkeersongevallenonderzoek noodzakelijk is en meer inzicht nodig is in de samenwerking tussen ADAS en bestuurder in de praktijk, bijvoorbeeld op basis van *naturalistic driving studies* (zie paragraaf 5.2.2.). Nu wordt bij de beoordeling van nieuwe ADAS vaak gesteld dat het effect op de verkeersveiligheid niet aantoonbaar is. Vervolgens wordt gesteld dat van het nieuwe ADAS niet kan worden gezegd dat het de verkeersveiligheid negatief beïnvloedt. Daarmee voldoet een dergelijk ADAS binnen het huidige kader aan de randvoorwaarde van een ten minste even hoog veiligheidsniveau. Voor ACC zijn bijvoorbeeld geen toelatingseisen gesteld, hetgeen alleen maar impliceert (zie Figuur 38 in Bijlage E) dat er bij de introductie geen expliciete aanwijzingen waren dat het systeem een negatief effect op de verkeersveiligheid heeft.

Specifieke eisen zijn niet voorhanden of niet scherp genoeg. Fabrikanten zijn niet verplicht om zelf een risico-inschatting te maken, terwijl dit wel verplicht is bij experimenten met *automated and connected driving*[131]. Hierdoor wordt niet geborgd dat nieuwe ADAS voldoende getoetst zijn op de risico's en bijdragen aan verhoging van de verkeersveiligheid en bestaat het gevaar dat ambitieuze beleidsintenties niet verder komen dan goede bedoelingen.

4.2.2 Wetgeving niet passend bij auto als rijdende computer

De huidige voertuigregelgeving bestaat uit kaderwetgeving en uitgebreide technische eisen, zie bijlage E. De kaderwetgeving regelt de uitgebreide eenmalige toetsing (toelating) en de meer globale APK. Deze wetgeving is toegesneden op de 'mechanische' auto maar past minder goed bij de nieuwe ontwikkeling van de auto als 'computer op wielen' en de daaraan gekoppelde ontwikkeling van de bestuurder als operator, omdat:

1. technologische veranderingen op gebied van ICT sneller gaan dan voorheen en het wetgevingstraject daardoor ook meer achterloopt dan voorheen;
2. de wet- en regelgeving tot nu toe gemaakt en toegepast werden door mensen met een achtergrond in de voertuigtechniek;
3. de computer op wielen tijdens de levensduur verandert door updates;
4. slijtage van computeronderdelen niet geleidelijk gaat.

Snelle veranderingen

De internationaal geharmoniseerde technische regelgeving komt tot stand door uitgebreid internationaal overleg tussen overheden, autofabrikanten en andere betrokken partijen in de UNECE. De auto-industrie speelt hierbij een grote rol, doordat zij in veel informele werkgroepen aan tafel zit. Technologische veranderingen op gebied van ICT

131 In het CAD-document (*connected and automated driving*, voorheen CAV) heeft de RDW het proces uitgewerkt voor fabrikanten/onderzoeksinstituten die een ontheffing aanvragen voor een experiment. Het beoordelen van de risicobeoordeling (bijvoorbeeld een FMEA volgens ISO 26262) opgesteld door de aanvrager is een belangrijk onderdeel van de procedure. De risicobeoordeling bevat risico's op voertuig-, weg- en gedragsaspecten en mitigerende maatregelen. De mitigerende maatregelen worden vervolgens onderdeel van de ontheffing.

gaan snel, waardoor het tot voor kort goed functionerende systeem op basis van het bereiken van overeenstemming over technische vereisten niet meer snel genoeg is. Daardoor kan onduidelijkheid ontstaan over welke toelatingseisen gelden voor een nieuw ADAS. Dit bleek een aantal jaar geleden het geval te zijn toen goedkeuringsinstanties in verschillende landen soortgelijke nieuwe ADAS, namelijk een gecombineerd systeem van ACC en LKA, verschillend beoordeelden. In Nederland werd het systeem binnen de bestaande toelatingseisen goedgekeurd, terwijl in Duitsland een Artikel 20 procedure werd gestart, omdat de betreffende goedkeuringsinstantie vond dat het nieuwe systeem niet binnen de bestaande regelgeving paste. Voor LKA zijn pas in oktober 2018 in UN R.79 (zie Bijlage E) toelatingseisen van kracht geworden. Dat was een aantal jaar nadat de eerste LKA-systemen op de markt kwamen in 2014 en bij gebrek aan specifieke regelgeving zonder meer toegelaten waren. In 2018 heeft de EC besloten dat nieuwe ADAS waarvoor nog geen uitgewerkte eisen bestaan, via een Artikel 20 procedure moeten worden beoordeeld.

Artikel 20 procedure
In een artikel 20 procedure kan een nieuwe technologie worden toegelaten via een ontheffing, wanneer deze onverenigbaar is met de bestaande regelgeving. Voorwaarde is dat de fabrikant aantoont dat bij de nieuwe technologie een even hoog veiligheidsbeschermingsniveau wordt gewaarborgd. Een artikel 20 procedure is een opmaat naar regelgeving (via artikel 21). Zie bijlage E voor meer uitleg.

Aandacht vooral op voertuigtechniek
De regelgeving werd tot nu toe gemaakt en toegepast door mensen met een achtergrond in de voertuigtechniek, de mechanische auto. Hierdoor is er minder aandacht voor nieuwe soorten risico's en zijn er nog nauwelijks eisen ontwikkeld op gebied van mens-machine interactie (paragraaf 3.3), software (paragraaf 3.4) en cybersecurity (paragraaf 3.5).

Voor mechanische onderdelen van de auto zijn er gedetailleerde specifieke eisen. Voor software zijn deze er niet, omdat het voor een toezichthouder onmogelijk is om de grote hoeveelheid (steeds veranderende) computercode te controleren. Bovendien kunnen fabrikanten bij een vast testprogramma inspelen op de toelatingstest (zoals gebeurd is bij het emissieschandaal, zie paragraaf 3.4). Toezicht op softwaresystemen is mogelijk door het gedrag van de software te valideren (bijvoorbeeld door computersimulaties en testritten) en door te beoordelen op procesniveau of de ontwikkeling van de software op een juiste manier is gedaan[132]. De RDW stelt dat dit niet nodig is bij de huidige generatie ADAS (tot en met SAE level 2), omdat deze systemen de bestuurder assisteren of ondersteunen en de mens altijd formeel de rijtaak uit zou moeten voeren. Tegelijkertijd is dit niet hoe de gebruikers de systemen ervaren en gebruiken en niet in lijn met hoe dit in de buitenwereld, onder andere door de autofabrikanten en de media wordt gepositioneerd. Daar wordt het beeld gecreëerd dat auto's met de huidige generatie ADAS deels zelfrijdende auto's zijn. Voor mens-machine interactie ontbreken om dezelfde reden eisen. Bovendien is er onvoldoende kennis op dit gebied (zie paragraaf 5.3.2).

132 Voor systemen waarbij de auto de controle van de mens overneemt wordt hier wel wetgeving op ontwikkeld.

Omdat specifieke eisen ontbreken op gebied van software en mens-machine interactie en omdat fabrikanten niet wordt gevraagd om een risico-inschatting (zie paragraaf 4.2.1), worden nieuwe risico's niet voldoende meegewogen in de beslissing om een bepaald voertuig of specifieke ADAS toe te laten.

Veranderingen tijdens de levensduur
Automatiseringssystemen kunnen tijdens de levensduur van de auto regelmatig worden geüpdatet met (gedeeltelijke) verandering van de functionaliteit als mogelijk gevolg, zie paragraaf 3.4. Ook kan een nieuwe functionaliteit worden toegevoegd aan bestaande systemen. Deze updates worden niet standaard vooraf beoordeeld en getoetst door de toezichthouder, want de toelating is eenmalig. Er is geen sprake van een 'continue' of stapsgewijze toelating. Deze wordt binnen de UNECE ontwikkeld voor toekomstige auto's die (tijdelijk) de controle van de bestuurder overnemen (SAE level 3 en hoger). Verder wordt wetgeving ontwikkeld op het gebied van software updates (zie verder hieronder).

Abrupt prestatieverlies
Digitale onderdelen en systemen gaan niet geleidelijk, als gevolg van (mechanische) slijtage, minder presteren, maar doen dit in de meeste gevallen abrupt, zonder vooraf te waarschuwen. Bij een periodieke keuring (APK) komen daardoor geen problemen met digitale onderdelen aan het licht, daarom is een periodieke keuring niet geschikt voor digitale onderdelen. Een vorm van continue monitoring zou geschikter zijn voor een rijdende computer dan een APK. De RDW spreekt in zijn Jaarverslag[133] in dit kader over omvorming van de APK naar Algemene Permanente Keuring.

Ontwikkelingen op gebied van wetgeving
De spanning tussen de bestaande op de mechanische auto toegesneden regelgeving en de nieuwe vragen en risico's die gepaard gaan met de ontwikkeling van de auto richting een computer op wielen wordt onderkend door de RDW en de UNECE. De RDW werkt aan de ontwikkeling van het VSSF (Vehicle Safety & Security Framework) en het VDLF (Vehicle Drivers' License Framework). In UNECE-verband wordt er zowel gewerkt aan regelgeving voor auto's die de controle van de bestuurder (tijdelijk) kunnen overnemen en aan regelgeving op gebied van software-updates en cybersecurity voor alle nieuwe auto's.

Binnen de *Informal Working Group on Functional Requirements for Automated and Autonomous Vehicles* (FRAV) is een roadmap[134] opgesteld met daarin een visie op veiligheid: geautomatiseerde of autonome voertuigsystemen mogen in hun geautomatiseerde modus geen verkeersongevallen veroorzaken die leiden tot letsel of overlijden die redelijkerwijs te voorzien en te voorkomen zijn. Gebaseerd op deze visie is een aantal onderwerpen geïdentificeerd waarop regelgeving ontwikkeld moet worden. Het gaat hierbij om functionele eisen (zoals die ook voor andere auto-onderdelen bestaan), validatie (nieuwe testmethoden, zoals ook binnen het VDLF ontwikkeld worden) en kwaliteitsborging (inclusief cybersecurity) zoals binnen het ICT-domein gebruikelijk is die gericht is op het proces van ontwerpen, produceren, toetsen, monitoren en updaten (zoals in het VSSF).

133 RDW, Jaarverslag 2018, 2019.
134 UNECE, *ECE/TRANS/WP.29/2019/34, Framework document on automated/autonomous vehicles*, 2019.

De roadmap beschrijft een aantal onderwerpen die de basis kunnen vormen voor toekomstige wetgeving. Een groot deel van de onderwerpen is echter niet alleen relevant voor toekomstige systemen, maar ook voor huidige systemen, bijvoorbeeld mens-machine interface (HMI), validatie op systeemveiligheid (inclusief een gevarenanalyse en een risicoassessment), dataopslag (EDR en DSSAD). Voor validatiemethoden en voor dataopslag zijn al informele werkgroepen opgericht maar voor HMI niet. En van het onderwerp voorlichting en training voor gebruikers is zelfs bepaald dat dit geen prioriteit heeft binnen WP.29. Hoewel de wetgeving niet meer past, is er dus voor de huidige generatie ADAS (nog) geen nieuwe wetgeving in ontwikkeling op UNECE niveau voor HMI en voor validatie (een reeks van testen door de fabrikant in simulatoren, op testbanen en door gespecialiseerde testrijders in de praktijk).

De informele werkgroep CS/OTA heeft een voorstel voor een *regulation* op het gebied van cybersecurity opgesteld dat in november 2019 in WP.29 besproken wordt. De RDW is een voortrekker in deze werkgroep. De ontwikkeling van het VSSF heeft hier aan bijgedragen. Het voorstel houdt in dat fabrikanten verplicht zijn een gecertificeerd cyber security management systeem (CSMS) te hebben op het moment van toelating. Het CSMS moet rekening houden de gehele levensduur van een auto. Verder moeten fabrikanten aantonen dat zij de cybersecurity risico's van het betreffende model geëvalueerd hebben en voldoende mitigerende maatregelen hebben genomen. Het voorstel schrijft niet precies voor hoe dit te doen, maar verwijst naar actuele normen, omdat dit aan verandering onderhevig is. Verder heeft de informele werkgroep CS/OTA een voorstel voor een *regulation* op gebied van software updates opgesteld dat ook in november 2019 in WP.29 besproken wordt. Dit voorstel behelst dat software versies identificeerbaar zijn en dat veranderingen aan software via updates bijgehouden moeten worden in een gecertificeerd Software Update Management Systeem.

Op EU-niveau is er geen ontwikkeling gaande om de kaderwetgeving aan te passen, terwijl deze niet meer past bij de huidige generatie auto's met ADAS. Verder zijn er op EU-niveau wel ontwikkelingen op het gebied van cybersecurity wetgeving, die in de toekomst wellicht de autobranche gaat raken. Zo is er de Netwerk en Informatie Systemen richtlijn (Richtlijn (EU) 2016/1148) die eisen aan clouddienstverleners stellen en de opvolger van de Cyber Security Act (Verordening (EU) 2019/881) waar het cybersecurity certificeringskader voor ICT-producten, diensten en processen wordt beschreven.

4.2.3 Nederlands beleid

Stimuleren van ADAS
Binnen het Nederlandse beleid is er veel aandacht voor de zelfrijdende auto. Het (verre) toekomstbeeld van een auto die overal of op bepaalde locaties volledig automatisch rijdt (SAE levels 4 en 5; zie Bijlage D.4) wordt door het Ministerie van IenW als zeer aantrekkelijk ervaren, vanwege de vele potentiële voordelen op het gebied van verkeersveiligheid, milieu (uitstoot) en doorstroming. Dit was ook de reden om in 2014 met een stuurgroep Zelfrijdende Auto te starten. Daarnaast speelden ook economische voordelen mee. De aandacht van de stuurgroep is sterk toekomstgericht. Er is binnen deze stuurgroep weinig aandacht voor ADAS; de focus ligt op volledig of onder voorwaarden automatisch rijden.

Eén van de maatregelen in het Actieplan Verkeersveiligheid[135] uit 2018 is gericht op het, onder voorwaarden, stimuleren van het veilig gebruik van ADAS, zie paragraaf 1.1. Sindsdien houdt een kleinere groep IenW-medewerkers zich bezig met de ontwikkeling van ADAS onder de paraplu van het ADAS Convenant, dat in juni 2019 is afgesloten.[136] In het ADAS Convenant is afgesproken om ADAS te stimuleren die een positief effect hebben op een of meer van de beleidsprioriteiten verkeersveiligheid, milieu of doorstroming en tegelijkertijd geen negatief effect hebben op de verkeersveiligheid. Het convenant is ondertekend door leden van de zogenoemde ADAS Alliantie, die bestaat uit 42 partijen die ieder een eigen ADAS Uitvoeringsplan hebben opgesteld.

Een belangrijke pijler van het ADAS Convenant is het verhogen van de bekendheid van ADAS en daarmee kennisgebrek bij bestuurders aanpakken. Er wordt ingezet op het informeren van zowel bestuurders als van personen werkzaam in de autobranche. Zo gaat IenW samen met BOVAG/RAI autoverkopers informeren en hebben IenW, ANWB, RAI Vereniging, Provincie Noord-Holland en CBR de website slimonderweg.nl opgezet om bestuurders te informeren. Deze maatregelen zijn vrijblijvend en borgen niet dat het kennisgebrek bij alle gebruikers aangepakt wordt.

In opdracht van IenW heeft de SWOV de veiligheidseffecten van ADAS in kaart gebracht op basis van verschillende buitenlandse onderzoeken, waarbij een aantal aannamen gemaakt is omdat er niet altijd voldoende onderzoek voorhanden was.[137] Uit deze literatuurstudie komt naar voren dat drie van de veertien onderzochte systemen een groot positief effect op de verkeersveiligheid hebben. Het gaat hierbij om de combinatie van FCW en AEB, ISA dat ingrijpt wanneer de geldende maximumsnelheid wordt overschreden en een alcoholslot (Tabel 3). Van de door de Onderzoeksraad onderzochte systemen LKA en autopilot is het effect op de veiligheid onbekend en van ACC geven verschillende onderzoeken tegenstrijdige resultaten. De partijen in het ADAS Convenant gaan die systemen promoten waarvan de SWOV heeft aangegeven dat deze bij de huidige stand van de techniek al gepromoot kunnen worden. IenW onderzoekt de mogelijkheden tot financiële ondersteuning van dergelijke ADAS. Het gaat voornamelijk om systemen die waarschuwen of ingrijpen bij kritieke situaties. LKA, autopilot en ACC worden (nu) niet geadviseerd door de SWOV. Bij sommige systemen, zoals FCW, waren er grote verschillen in effectiviteit tussen verschillende modellen en merken auto's. Dit kan te maken hebben met de onvolwassenheid van de systemen of de mens-machine interactie.

Inzicht in de risico's

Door het werk van de Stuurgroep zelfrijdende auto, de experimenten met *connected and automated driving* (bijvoorbeeld *platooning* experimenten waarbij personenauto's of vrachtwagens in een 'treintje' rijden) en de contacten met de RDW heeft het ministerie van IenW inzicht gekregen in de risico's die verbonden zijn aan de huidige en toekomstige

135 Ministerie van Infrastructuur en Waterstaat, Landelijk Actieplan Verkeersveiligheid 2019-2021: *Veilig van deur tot deur Den Haag*, 2018.
136 ADAS Alliantie, *ADAS Convenant*, 2019.
137 SWOV, *Veiligheidseffecten van rijtaakondersteunende systemen; Bijlage bij het convenant van de ADAS Alliantie*, 2019.

ADAS. In de kamerbrief over Smart Mobility[138] worden verschillende soorten risico's genoemd. Er zijn echter geen risicoanalyses voor bestaande ADAS uitgevoerd of toekomstscenario's opgesteld, terwijl voor experimenten met *automated and connected driving* wel risicoanalyses plaatsvinden (zie paragraaf 4.2.1). De risico's van de huidige ADAS worden beperkt gemonitord (zie paragraaf 5.3.2). Ook heeft het ministerie van IenW niet uitgewerkt hoe de risico's gemitigeerd kunnen worden of wat er nodig is om tot mitigerende maatregelen te komen. Het ministerie van IenW gaat ervan uit dat de risico's vanzelf af zullen nemen wanneer de technologische ontwikkelingen voortschrijden, zie box hieronder. Daarnaast neemt men op het ministerie aan dat door het strenger worden van de eisen voor bestaande ADAS veel risico's beheerst worden.

Uit het Strategisch Plan Verkeersveiligheid

"Niet alleen de voertuigen veranderen, maar ook de wijze van verkeersmanagement. De toenemende connectiviteit maakt het mogelijk om verkeersdeelnemers op steeds slimmere manieren te sturen in hun verplaatsingsgedrag. De ontwikkelingen in automatisering en connectiviteit zorgen er bovendien voor dat steeds meer data over infrastructuur en voertuigen beschikbaar zijn. Op basis daarvan kunnen overheden hun verkeersveiligheidsbeleid beter vormgeven. Ook biedt automatisering nieuwe kansen voor (digitale vormen van) handhaving. Innovaties bieden nieuwe mogelijkheden, maar leiden ook tot nieuwe vragen over verkeersveiligheidsbeleid. Omdat de ontwikkelingen zo snel gaan, zijn voortdurend aanpassingen nodig. Dit vraagt een visie van overheden op de gewenste mate van innovatie en hoe om te gaan met nieuwe ontwikkelingen."

De overheid schetst een beeld van heel snelle, autonome, technologische ontwikkelingen. Tegelijk geeft het Strategisch Plan Verkeersveiligheid het belang aan van ingrijpen, wanneer de risico's zich anders dan gewenst ontwikkelen. Daarvoor is het echter noodzakelijk dat er een visie is op het gewenste veiligheidsniveau in relatie tot de gewenste mate en richting van innovatie, dat er systematische risicoanalyses plaatsvinden en dat de invloed van ADAS op de verkeersveiligheid gemonitord wordt. Aan geen van deze voorwaarden wordt echter voldaan.

138 De Minister van Infrastructuur en Waterstaat, *Kamerbrief 205325 Smart Mobility Dutch Reality*, 2018.

Systeem	Informeren/ Waarschuwen/ Overnemen/ Ingrijpen	Accuraatheid	Gedrags-aanpassing	Effect op verkeers-veiligheid[139]	Timing van promotie[140]	GSR
Longitudinale controle (snelheid)						
Forward Collision Warning	Waarschuwen	Redelijk	Gering	+/-	Nu	
Autonomous Emergency Braking	Ingrijpen	Redelijk	Gering	+	Nu	Ja
Combinatie van FCW en AEB	Waarschuwen/ Ingrijpen	Redelijk	Gering	++	Nu	
Voetganger- en Fietser-detectie	Waarschuwen	Vermoedelijk nog onvoldoende	Onbekend	Onbekend	Potentieel	Ja
Adaptive Cruisecontrol	Overnemen	Redelijk	Tegen-strijdige resultaten	Tegen-strijdige resultaten	Geen	
Intelligent Speed Adaptation	Informeren/ Waarschuwen/ Overnemen	Goed	Gering	+/- + ++[141]	Nu	Ja Alleen infor-merend
Noodstop-signaal	Waarschuwen[142]					Ja
Laterale controle (sturen en intentie tot koersverandering)						
Lane Departure Warning	Waarschuwen	Redelijk	Gering	+/-	Nu	
Lane Keeping System	Overnemen	Redelijk	Onbekend	Onbekend	Potentieel	Ja
Dodehoek-verklikker	Waarschuwen	Redelijk	Gering	+/-	Nu	
Gecombineerde longitudinale en laterale controle						
Autopilot	Overnemen	Redelijk	Groot	Onbekend	Potentieel	

139 gering +/-, redelijk +, groot ++

140 Nu = kan bij huidige stand van de techniek al gepromoot worden; Potentieel = effect op de verkeersveiligheid in de praktijk is onbekend, maar kan bij gebleken effectiviteit een grote bijdrage leveren aan de verkeersveiligheid en kan vervolgens ook gepromoot worden; Geen = promotie heeft geen prioriteit, omdat het veiligheidseffect (in de praktijk nog onbekend) als tamelijk laag wordt ingeschat.

141 Afhankelijk of de ISA informerend, waarschuwend of in meer of mindere mate ingrijpend is.

142 Valt enigszins buiten de definitie van ADAS, omdat het niet de bestuurder ondersteunt maar zijn omgeving informeert. Wel opgenomen, omdat de GSR het noodstopsignaal verplicht stelt.

Systeem	Informeren/ Waarschuwen/ Overnemen/ Ingrijpen	Accuraatheid	Gedrags-aanpassing	Effect op verkeers-veiligheid[139]	Timing van promotie[140]	GSR
Monitoren staat van de bestuurder						
Vermoeid-heids-detector	Waarschuwen	Vermoedelijk nog onvoldoende	Onbekend	Onbekend	Potentieel	Ja
Afleidings-detector	Waarschuwen	Onvoldoende	Onbekend	Onbekend	Potentieel	Ja
Alcoholslot	Ingrijpen	Goed	Geen	++	Nu	Ja[143]
Ondersteuning bij bijzondere manoeuvres						
Achteruitrij-camera	Waarschuwen	Redelijk	Gering	+/-	Nu	
Ongevalsgegevens						
Gegevens-recorder voor ongevallen[144]	Informeren					Ja

Tabel 3: Overzicht van ADAS en globale indicatie van het effect op de verkeersveiligheid volgens SWOV. Daarnaast is aangegeven welke ADAS volgens het ADAS Convenant worden gepromoot. In de laatste kolom zijn de maatregelen vanuit de GSR aangegeven.

4.2.4 EU-beleid

De nieuwe General Safety Regulation is door het Europees Parlement aangenomen in april 2019 en treedt in werking in 2022. Deze GSR zou moeten bijdragen aan de vermindering van het aantal verkeersdoden ('Vision Zero') en stelt voor verschillende soorten motorvoertuigen extra systemen verplicht. Voor personenauto's gaat het onder meer om ISA (Intelligent Speed Assistant), AEBS (Advanced Emergency Braking System), voetganger- en fietserdetectie (noodremsysteem), een waarschuwingssysteem voor bestuurders die slaperig of afgeleid worden, achteruitrijbeveiliging met camera of sensoren, EDR (Event Data Recorder; een soort 'zwarte doos' voor motorvoertuigen) en LKA (Lane Keeping Assist), zie Tabel 3. Specifieke invulling van de eisen aan deze systemen moet nog plaatsvinden in de UNECE.

Bij het bereiken van overeenstemming over de GSR meldt de EC een groot vertrouwen te hebben in technische maatregelen als remedie tegen onveiligheid in het wegverkeer.[145]

143 De GSR stelt alleen de ondersteuning van de installatie van een alcoholslot verplicht, niet het alcoholslot zelf. Dit komt neer op het aanbrengen van een gestandaardiseerde interface die de montage van een aftermarket alcoholslot in een voertuig vergemakkelijkt.
144 Deze gegevensrecorder (EDR) is geen ADAS, maar wordt wel verplicht gesteld in de GSR.
145 Europese Commissie, *Persbericht Verkeersveiligheid: Commissie Verheugd over Akkoord over Nieuwe EU-Regels Om Levens Te Helpen Redden*, https://europa.eu/rapid/press-release_IP-19-1793_nl.htm, geraadpleegd op 23 augustus, 2019.

Dit vertrouwen volgt uit de redenering dat 90% van de verkeersslachtoffers toe te schrijven is aan menselijke fouten en dat dit percentage zal dalen als machines de plaats innemen van de mens. In deze redenering wordt echter voorbijgegaan aan het gegeven dat menselijke fouten ook gemaakt kunnen worden bij het ontwerpen en programmeren van nieuwe technologieën (onvolwassen systemen) en aan het gegeven dat de mens ook verantwoordelijk is voor het voorkómen van ongevallen. Verder blijft de bestuurder in veel gevallen als veiligheidsbarrière fungeren ook als de bestuurder dat niet beseft (zie hoofdstuk 3).

Er bestaan opmerkelijke verschillen tussen de systemen die de Nederlandse overheid wil stimuleren (ADAS Convenant) en de systemen die verplicht worden volgens de GSR.

- Het ADAS Convenant promoot nu alleen ADAS die volgens de SWOV een positief effect op de verkeersveiligheid hebben, waar de GSR invoering van een aantal ADAS verplicht stelt, waarvan het effect op de verkeersveiligheid volgens de SWOV onbekend is.
- Het ADAS Convenant promoot alle drie de ISA varianten (systemen die adviseren over snelheid, die waarschuwen over snelheidsoverschrijdingen, die die snelheid begrenzen), maar verwacht het grootste positieve effect op de verkeersveiligheid van de variant die in meer of mindere mate ingrijpend is, terwijl de GSR invoering van de informerende variant van ISA verplicht stelt. Deze heeft volgens de SWOV slechts een gering effect op de verkeersveiligheid.
- De GSR stelt systemen voor vermoeidheids- en aandachtswaarschuwing verplicht evenals geavanceerde systemen voor afleidingswaarschuwing. Het ADAS Convenant acht de tijd hiervoor nog niet rijp, omdat het effect van deze systemen op de verkeersveiligheid (volgens de SWOV) onbekend is. De GSR kiest nadrukkelijk voor invoering van mitigerende maatregelen om het risico van gedragsadaptatie te beheersen en stapelt daarmee systeem op systeem, hetgeen leidt tot een toename van complexiteit, die op gespannen voet staat met de veiligheid.
- De GSR promoot voetganger- en fietserdetectie, terwijl het ADAS Convenant de tijd hiervoor nog niet rijp acht, omdat het effect van deze systemen op de verkeersveiligheid (volgens de SWOV) onbekend is. Opmerkelijk is dat mede door de inspanning van Nederland herkenning van fietsen en voetgangers door AEBS is opgenomen in de nieuwe GSR. Uit de eerste testen blijkt echter dat het systeem vaak niet goed functioneert.[146, 147]

146 Charlebois, Meloche, en Burns, *Detection of Cyclist and Pedestrians Around Heavy Commercial Vehicles*, in 26th International Technical Conference and Exhibition on the Enhanced Safety of Vehicles (ESV) Eindhoven, 2019.
147 AAA, *Automatic emergency braking with pedestrian detection*, 2019.

Deelconclusies
De beleidsambitie om alleen ADAS toe te laten die de verkeersveiligheid wetenschappelijk aantoonbaar verbeteren komt niet terug in de voertuigregelgeving, die uitgaat van een ten minste even hoog veiligheidsniveau. Er is onduidelijkheid in het beoordelen van het veiligheidsniveau, hetgeen tot gevolg heeft dat fabrikanten geen risico-inschatting en scenario's hoeven aan te leveren en dat er niet geborgd is dat er geen systemen worden toegelaten die een negatief effect hebben op de verkeersveiligheid.

De spanning tussen de bestaande op de mechanische auto toegesneden regelgeving en de nieuwe risico's die gepaard gaan met de ontwikkeling van de auto richting een computer op wielen, waardoor de rol van de bestuurder steeds meer opschuift naar die van operator en de mens-machine-interactie belangrijker wordt, wordt onderkend door de Nederlandse overheid, maar heeft nog niet tot aanpassing van de voertuigregelgeving geleid. Ontwikkelingen op gebied van wetgeving vinden hoofdzakelijk plaats voor voertuigen die de controle (tijdelijk) van de bestuurder overnemen, terwijl de wetgeving ook niet meer past voor systemen die de bestuurder assisteren of ondersteunen.

Het ministerie van IenW is op het gebied van automatisering in het wegverkeer meer met de verre toekomst bezig dan met het heden en de nabije toekomst. Binnen IenW bestaat de veronderstelling dat de grootschalige introductie van ADAS op termijn en per saldo tot minder verkeersslachtoffers zal leiden. Deze veronderstelling wordt door het ontbreken van een visie op het gewenste veiligheidsniveau en het ontbreken van systematische risicoanalyses nauwelijks onderbouwd.

In het in juni 2019 afgesloten ADAS Convenant is afgesproken om ADAS te stimuleren die geen negatief effect hebben op de verkeersveiligheid en een positief effect op verkeersveiligheid, milieu of doorstroming. Vrijblijvende voorlichting aan bestuurders is een belangrijk onderdeel van de uitvoeringsplannen die onder het convenant vallen. De nieuwe *General Safety Regulation* stelt per 2022 een aantal ADAS verplicht waarvan nog niet wetenschappelijk onderbouwd is wat het effect op de verkeersveiligheid is.

4.3 Conclusies

Het is inherent aan innovatie dat er systemen op de markt komen die nog niet volledig uitontwikkeld zijn. Juist bij informatie-gestuurde systemen kan alleen in de praktijk blijken wat nodig is om systemen helemaal volwassen te laten worden. Dit betekent dat ADAS op de openbare weg verder ontwikkeld worden. Deze realiteit is vanuit veiligheidsperspectief niet wenselijk. Tegelijkertijd kan innovatie ook ingezet worden om de veiligheid te verbeteren wanneer verbetering van de veiligheid een vereiste is bij de ontwikkeling van nieuwe systemen. Het is daarom van groot belang dat er maatschappelijk verantwoord geïnnoveerd wordt. Daarvoor zou een aantal veiligheidsprincipes moeten worden gerespecteerd bij ontwerp, toelating en beleid (zie het referentiekader in Hoofdstuk 2). De Raad concludeert dat hier nog winst te behalen is.

Ontwerp
Fabrikanten richten zich in het ontwerp meer op de technische functionaliteit dan op verhoging van de verkeersveiligheid. Zo zien we dat de veiligheidsprincipes *safety by design, foolproof* ontwerp, *secure* ontwerp en duidelijkheid wie de controle heeft niet gerespecteerd worden. Verder wordt cybersecurity gedurende de gehele levensduur onvoldoende geborgd en is er een gebrek aan transparantie binnen de leveringsketen en naar de consument.

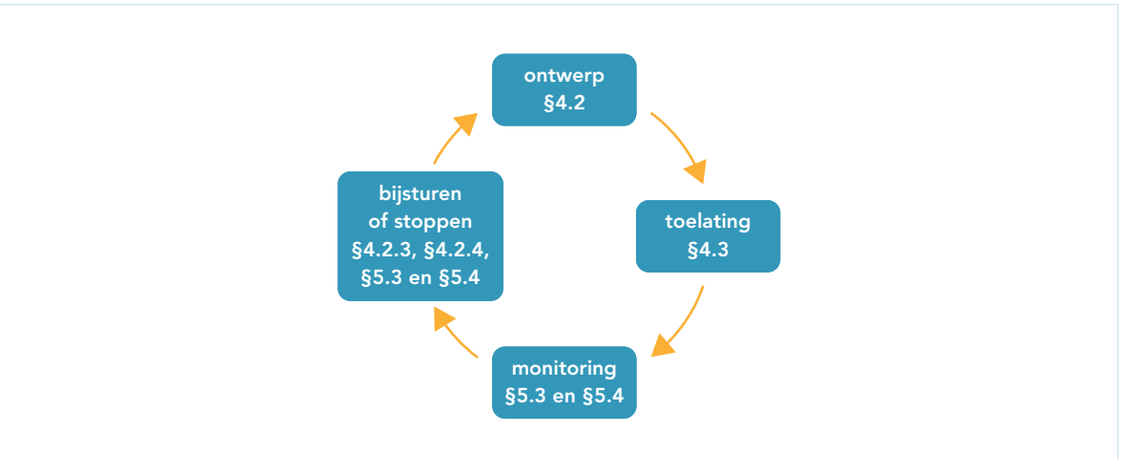
Toelating
De bestaande regelgeving voor toelating sluit onvoldoende aan bij het principe dat innovatie de veiligheid moet verbeteren en bij de Nederlandse en Europese beleidsambitie dat ADAS een belangrijke bijdrage leveren aan het verlagen van het aantal verkeersslachtoffers. Redenen hiervoor zijn dat veiligheid geen leidend principe is bij toelating en dat de bestaande wetgeving niet past bij de auto als rijdende computer waarin de bestuurder een operator is en de mens-machine interactie toegenomen is. Ook de macht van de auto-industrie speelt hierbij een rol.

Beleid
Het Nederlandse en Europese beleid is gericht op het stimuleren en verplicht stellen van ADAS. De ambitie om het aantal verkeersslachtoffers terug te dringen ligt hieraan ten grondslag. Er is echter geen uitgewerkte visie op het gewenste veiligheidsniveau in relatie tot de gewenste mate en richting van innovatie. Zo vinden er geen systematische risicoanalyses plaats en is niet uitgewerkt hoe de risico's gemitigeerd kunnen worden of wat er nodig is om tot mitigerende maatregelen te komen. Verder is het beleid te weinig gericht op de huidige generatie systemen en gaat de overheidsaandacht vooral uit naar systemen die in de (verre) toekomst de controle (tijdelijk) kunnen overnemen. De huidige mitigerende maatregelen van IenW om het kennisgebrek bij bestuurders tegen te gaan zijn alle vrijblijvend. Binnen de UNECE is er geen specifieke werkgroep voor regelgeving op gebied van HMI.

5 KNELPUNTEN IN MONITOREN EN BIJSTUREN

5.1 Inleiding

De introductie van nieuwe technologie, zoals ADAS, is altijd met onzekerheid omgeven. Pas wanneer de nieuwe technologie in de praktijk gebruikt wordt ('*living lab*' situatie) zal blijken wat nodig is om de technologie volwassen te laten worden. Daarom is het bij innovatieve technologieën van groot belang om de vinger aan de pols te houden (monitoring) en informatie over het functioneren van de technologie terug te koppelen naar fabrikanten en de overheid (feedback). Hierdoor kunnen op basis van een evaluatie, indien nodig, mitigerende maatregelen worden genomen door de fabrikant of de overheid in de vorm van bijsturen dan wel verbieden (veiligheidsprincipes beheerst proces en ingrijpen door de overheid, referentiekader, paragraaf 2.1). Door monitoren en het nemen van maatregelen is de feedbackloop gesloten, zie Figuur 16.



Figuur 16: Veilige introductie en veilig gebruik van ADAS.

In dit hoofdstuk inventariseren we de knelpunten bij het sluiten van de feedbackloop. Deze knelpunten zijn achtereenvolgens het gebrek aan informatie om te monitoren en bij te sturen (paragraaf 5.2), het lerend vermogen van partijen naar aanleiding van ongevallen en gevaarlijke situaties (paragraaf 5.3) en het leren van cybersecurity incidenten (paragraaf 5.4).

5.2 Gebrek aan gegevens

Het verzamelen van empirische gegevens is essentieel voor het lerend vermogen van het stelsel en voor bijsturen of ingrijpen op basis van monitoring.[148] Bij empirische gegevens gaat het om inzicht in het aantal auto's met ADAS en gegevens over ongevallen, gevaarlijke situaties en het voorkómen van gevaarlijke situaties.

5.2.1 Geen inzicht in aantal auto's met ADAS

Er zijn geen statistieken met gegevens over de aanwezigheid van verschillende ADAS in het Nederlandse wagenpark. De RDW houdt een groot aantal gegevens bij in de kentekenregistratie, maar de aanwezigheid van ADAS vormt daar geen onderdeel van. De reden daarvoor is dat het lastig is om een compleet en goed beeld te geven van de ADAS in een voertuig in slechts enkele parameters. Zo hebben fabrikanten verschillende systemen die op elkaar lijken, maar net anders werken en reageren, zie paragraaf 3.3. Verder maakt het uit welke softwareversie er geïnstalleerd is. Doordat er verschillende softwareversies zijn, is de variatie in systemen groot.

De RDW verkent de mogelijkheid om ADAS op te nemen in het kentekenregister en om gegevens over ADAS in voertuigen te ontsluiten (bijvoorbeeld voor autokopers via de website). Het onderzoek is een eigen initiatief van de RDW, naar aanleiding van discussies met belanghebbenden als RAI Vereniging, BOVAG en ANWB. Vooral voor de handel in tweedehands auto's is het voor kopers en verkopers van belang te weten welke systemen aan boord zijn en wat de specificaties zijn van die systemen.

IenW is als onderdeel van het ADAS Convenant gestart met het monitoren van de penetratiegraad van diverse ADAS in het Nederlandse wagenpark en de bekendheid en het gebruik daarvan onder Nederlandse automobilisten.

5.2.2 Empirische gegevens over ongevallen ontbreken

Empirische gegevens over ongevallen waarbij ADAS een rol hebben gespeeld, zijn vaak niet beschikbaar. Dat ligt allereerst aan het ontwerp van ADAS en de manier waarop data opgeslagen worden. Uit ongevalsonderzoek en gesprekken met experts is gebleken dat de huidige generatie systemen een aantal tekortkomingen heeft voor wat betreft de opslag en verzameling van ongevalsdata:

1. Data worden niet altijd bewaard. Sommige systemen zijn bijvoorbeeld zo ontworpen dat bij een plotselinge stroomonderbreking – als gevolg van een botsing – de gegevens van de laatste seconden niet weggeschreven worden. Ook zijn er gevallen waar helemaal geen data worden opgeslagen over de werking van ADAS, niet tijdens het rijden maar ook niet na ongevallen. Het is ook niet altijd te achterhalen of in een auto aanwezige ADAS ook daadwerkelijk waren ingeschakeld.
2. Data worden in bedrijfseigen formaat opgeslagen. Uitlezen is hierdoor niet mogelijk zonder hulp van de fabrikant.
3. Data worden versleuteld opgeslagen. Uitlezen is dan ook niet mogelijk zonder hulp van de fabrikant.

148 Zie de veiligheidsprincipes uit het referentiekader in paragraaf 2.1.

4. Data worden verspreid opgeslagen over verschillende modules en het is niet altijd duidelijk waar. Doordat ADAS in veel gevallen bij toeleveranciers worden ingekocht, is het in sommige gevallen zelfs voor de autofabrikant niet duidelijk welke informatie waar opgeslagen ligt.

Daarnaast zijn empirische gegevens niet beschikbaar, omdat ongevallen niet geregistreerd worden. Over het algemeen is de registratiegraad laag (circa 30% voor ernstig gewonde verkeersslachtoffers).[149] Van de dodelijke verkeersongevallen worden alleen die op rijkswegen sinds enige tijd systematisch geanalyseerd.[150] Bovendien is de aanwezigheid van ADAS geen kenmerk in de ongevallenregistratie, omdat de aanwezigheid van ADAS in voertuigen niet geregistreerd wordt, zie paragraaf 5.2.1. Verder wordt vaak niet onderzocht of ADAS een ongevalsfactor is. Een reden hiervoor is dat partijen (zoals politie) geen inzicht hebben in de aanwezigheid van ADAS in verschillende voertuigen (merken, typen, softwareversies), zie paragraaf 5.2.1. Bovendien is het bewustzijn niet overal aanwezig dat ADAS in alle moderne auto's aanwezig kunnen zijn en dus een ongevalsfactor kunnen zijn.

Onder andere om ongevalsonderzoek te faciliteren wordt in 2022 verplicht om alle nieuwe auto's te voorzien van een EDR (Event Data Recorder), zie paragraaf 4.2.4. Welke data precies moeten worden opgeslagen, wie gemachtigd is deze data uit te lezen en wie deze data voor onderzoek mag gebruiken is nog onderwerp van besluitvorming in de UNECE en de EC.[151] Dat geldt ook voor de data die in ADAS worden opgeslagen en in principe uitgelezen zouden kunnen worden.[152] EDR's zijn vanwege hun beperkte opslagcapaciteit niet het juiste apparaat voor de opslag van ADAS gerelateerde of cybersecuritygebeurtenissen. Deze gebeurtenissen worden over het algemeen opgeslagen op andere gegevensopslagapparaten.

5.2.3 Empirische gegevens over cybersecurity incidenten ontbreken

We kunnen niet uitsluiten dat er ongevallen plaatsgevonden hebben door misbruik van kwetsbaarheden, omdat huidige auto's niet zijn ingericht om na een ongeluk digitaal te onderzoeken of een ongeluk mogelijk cybersecurity gerelateerd is. Data om vast te stellen of er een aanval heeft plaatsgevonden worden niet specifiek opgeslagen, zie paragraaf 3.5. Hierdoor hebben politie en ongevalsonderzoekers geen mogelijkheid om een cybersecurity incident te herkennen of uit te sluiten, waardoor verder onderzoek uitblijft.

149 SWOV, *Ernstig verkeersgewonden 2017*, 2018.
150 SWOV, *Dodelijke verkeersongevallen op rijkswegen in 2017*, 2019.
151 EU-lidstaten, *Declaration of Amsterdam; Cooperation in the Field of Connected and Automated Driving*, 2016.
152 Europese Commissie, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions; On the road to automated mobility: An EU strategy for mobility of the future*, 2018.

Deelconclusies
Empirische gegevens over ongevallen, gevaarlijke situaties en cybersecurity incidenten met voertuigen met ADAS ontbreken, terwijl deze noodzakelijk zijn voor de feedbackloop. Ook het ontbreken van een registratie van de aanwezige ADAS is een belemmering voor het evalueren van ADAS na introductie.

In de auto worden niet de juiste gegevens opgeslagen om ongevallen en cybersecurity incidenten te onderzoeken.

5.3 Leren van ongevallen en gevaarlijke situaties

5.3.1 Leren van (bijna-)ongevallen door fabrikanten

Fabrikanten leren op verschillende manieren van ongevallen en bijna-ongevallen. Grofweg bestaan er vijf mogelijkheden om informatie te verzamelen:

1. Het verzamelen van data die door de computersystemen in het voertuig worden gegenereerd. Deze data kunnen via een draadloze verbinding met de fabrikant worden gedeeld. Daarmee ontstaat niet alleen de mogelijkheid om in te grijpen – bijvoorbeeld door het uitbrengen van een update om de huidige generatie systemen te verbeteren – maar ook biedt deze informatie de fabrikant inzicht bij het verder verbeteren en veiliger ontwerpen van nieuwe producten. Tesla past deze methode toe om een gesloten feedbackloop te creëren.
2. Het doen van onderzoek ter plaatse door een onderzoeksteam of incidentenresponsteam. Dit onderzoek kan onder andere bestaan uit het verzamelen van gegevens afkomstig uit het voertuig, het vastleggen van sporen en repliceren van de systeemtoestand.
3. Het verzamelen van klachten van automobilisten en vrachtwagenchauffeurs.
4. Het verzamelen van verkoopgegevens van reserveonderdelen zoals voor- en achterbumpers, waarvan aannemelijk is dat deze vaak worden toegepast bij het herstel van voertuigen na een ongeval.
5. Het initiëren of uitvoeren van gericht (wetenschappelijk) onderzoek al dan niet in samenwerking met onderzoeksinstellingen.

Er zijn weinig fabrikanten die deze vijf methoden combineren voor het vormen van een zo compleet mogelijk beeld van wat er zich heeft afgespeeld vlak voor, tijdens en na een (bijna-)ongeval. Daarnaast bieden niet alle fabrikanten goede mogelijkheden voor het ontvangen van feedback van consumenten over bijvoorbeeld het functioneren van ADAS en (bijna-)ongevallen. Een aantal autofabrikanten geeft aan feedback te verzamelen door met klanten in gesprek te gaan en publieke discussies te voeren tijdens, bijvoorbeeld, congressen en auto-evenementen. Toch heeft een analyse van online media aangetoond dat in veel gevallen de gebruiker doorverwezen wordt naar de autodealer als aanspreekpunt. Dit terwijl autodealers niet altijd bekend zijn met alle ADAS in het voertuig en mogelijke problemen eerst bekend moeten zijn bij de autodealer wil deze op zoek gaan naar een oplossing.

Toeleveranciers vormen een belangrijke schakel, omdat fabrikanten ADAS in veel gevallen inkopen bij deze partijen. Net als fabrikanten kunnen toeleveranciers op verschillende manieren leren van ongevallen. Toeleveranciers hebben weinig tot geen contact met eindgebruikers. Zij ontvangen feedback over het functioneren van ADAS dan ook vooral via de autofabrikant. Deze feedback is maar beperkt toepasbaar, omdat de toeleveranciers vaak al bezig zijn met de volgende generatie ADAS wanneer de feedback over het functioneren van de vorige generatie binnenkomt. Net als de autofabrikant doet de toeleverancier in sommige gevallen onderzoek ter plaatse. De toeleverancier doet dit echter niet op eigen initiatief. Als de fabrikant onderzoek doet naar een ongeval, kan deze ervoor kiezen om de toeleverancier te vragen om assistentie, als vermoed wordt dat ADAS een rol hebben gespeeld. In andere gevallen komt de toeleverancier meestal niet in beeld.

Naast het leren van eigen ongevallenonderzoek en informatieverzameling kunnen fabrikanten ook leren van casussen bij branchegenoten. Immers, veel fabrikanten werken met systemen van dezelfde toeleverancier, hebben ADAS met vergelijkbare functionaliteit en lopen bovendien tegen dezelfde technische beperkingen aan van de huidige generatie ADAS, zowel tijdens de ontwerp- als de gebruiksfase. Informatiedeling tussen fabrikanten komt in de praktijk echter nauwelijks voor. Als belangrijkste reden worden concurrentiebelangen en beperkte vergelijkbaarheid van ADAS door onderlinge verschillen in functionaliteit en bediening aangevoerd. Fabrikanten zijn vooral gericht op het verbeteren van het eigen product en hebben minder aandacht voor het verbeteren van de veiligheid van ADAS in het algemeen.

Volvo Cars heeft begin 2019 de geslotenheid van fabrikanten doorbroken door het publiek beschikbaar stellen van zijn database met de resultaten van onderzoeken naar ongevallen waarbij in de loop der jaren meer dan 40.000 auto's betrokken zijn geweest. Volvo Cars noemt dit het E.V.A. (Equality for Vehicle Advancement) initiatief, zie ook paragraaf 3.1.

5.3.2 Leren van ongevallen en gevaarlijke situaties door de overheid

Door de gebrekkige ongevalsregistratie waarin bovendien ontbreekt in welke auto's ADAS aanwezig zijn (paragraaf 5.2.2) heeft het ministerie van IenW geen inzicht in hoeveel ongevallen er gebeuren waarbij auto's met ADAS betrokken zijn. Invoering van de AVG heeft het ongevallenonderzoek bovendien moeilijker gemaakt.[153]

153 De Minister van Infrastructuur en Waterstaat, *Beantwoording Kamervragen van de leden Dijkstra en Van Gent (VVD) over de berichten "De schrikbarende stijging die niemand kan verklaren" en "Verkeersanalyse provincie nutteloos door Privacywet"*, 2019.

Deelconclusies
Er wordt binnen de branche onvoldoende van (bijna-)ongevallen geleerd op systeemniveau door gebrek aan empirische gegevens en transparantie. Van informatiedeling tussen fabrikanten is nauwelijks sprake; leren vindt alleen plaats binnen een fabrikant en de fabrikant zelf bepaalt de mate waarin geleerd wordt. Hierdoor maakt iedere fabrikant zijn eigen leerproces door. Er zijn geen afspraken en er is geen wettelijke verplichting tot leren van incidenten zoals in de luchtvaart, scheepvaart en BRZO (Besluit risico's zware ongevallen)-bedrijven waar het leren van incidenten en delen van veiligheidsinformatie is geregeld in internationale verdragen.

Het ministerie van IenW kan niet beoordelen wat het effect (positief dan wel negatief) van de introductie van ADAS is op de verkeersveiligheid. Het ontbreekt daarvoor aan de benodigde monitoringsgegevens. Het ministerie van IenW zorgt niet dat het over voldoende empirische gegevens over de veiligheid van ADAS beschikt, terwijl dat noodzakelijk is voor de feedbackloop.

5.4 Leren van cybersecurity incidenten

5.4.1 Geen grootschalige incidenten

De auto-industrie heeft in de praktijk nog niet te maken gehad met een grootschalige cyberdreiging. Wel is er ervaring met het misbruik van bijvoorbeeld de contactloze autosleutel, waarbij dieven de signalen van de sleutel kunnen afvangen en gebruiken om een auto te stelen. Misbruik van deze kwetsbaarheid heeft echter geen impact op de verkeersveiligheid van de auto. Behalve voor autodiefstal is er nog geen praktisch uitvoerbaar verdienmodel gevonden voor het misbruik van kwetsbaarheden. Andere sectoren zijn al veel eerder geconfronteerd met cyberdreigingen, omdat aanvallers geld konden verdienen met digitale aanvallen of hacks. Voorbeelden zijn het kraken van beveiliging van beeldmateriaal bij pay-TV en het misbruiken van internetbankieren. In beide gevallen is er een kat-en-muisspel ontstaan om de criminelen een stapje voor te blijven. Een groot verschil met de auto-industrie is dat in bovenstaande branches het negatieve effect voornamelijk financieel is en geen veiligheidsimpact heeft.

Het vermogen van de auto-industrie om te reageren op digitale aanvallen en de effecten daarvan te minimaliseren is onduidelijk, omdat de auto-industrie nog nauwelijks te maken heeft gehad met een grootschalige cyberdreigingen. Initiatieven zoals de Auto-ISAC dragen wel bij om kennis over deze dreigingen te delen binnen de sector. Tot nog toe zijn veel digitale aanvalsscenario's nog als onwaarschijnlijk ingeschat[154] omdat er geen concrete voorbeelden in de praktijk bekend zijn.[155] (Cybersecurity principes: Controlestructuur)

154 ENISA, *Cyber security and resilience of smart cars; Good practices and recommendations*, 2016.
155 Ook in andere onderzoeken van de Onderzoeksraad is geconstateerd dat bepaalde scenario's onwaarschijnlijk werden geacht, namelijk *MH17 Crash*, 2015 en *Opkomende Voedselveiligheidsrisico's*, 2019

5.4.2 Leren van kwetsbaarheden en incidenten

Er is geen misbruik van kwetsbaarheden bekend dat effect heeft gehad op de veiligheid, maar er zijn – net als in andere computersystemen - wel kwetsbaarheden gevonden (paragraaf 3.6). Deze security-incidenten zijn onderzocht door securityonderzoekers die juist willen helpen om de beveiliging van de auto te verbeteren.

Het verantwoord melden van kwetsbaarheden door securityonderzoekers helpt fabrikanten om hun interne afhandelingsproces van gevonden kwetsbaarheden of misbruik van kwetsbaarheden (incident response) effectief in te richten. Door dit proces in de praktijk toe te passen zal het gehele cybersecurityproces naar een hoger niveau worden gebracht en zal bij incidenten met daadwerkelijk misbruik van kwetsbaarheden sneller gereageerd kunnen worden. In het referentiekader is dit terug te vinden in het belang van samenwerken met derden om de cybersecurity van het systeem te verbeteren. (Cybersecurity principe: Controlestructuur)

De meeste autofabrikanten hebben tegenwoordig een *bug bounty* programma, dat externe hackers de mogelijkheid geeft om geld te verdienen aan een gevonden kwetsbaarheid wanneer ze deze melden volgens de gestelde voorwaarden. General Motors maakt ook gebruik van de expertise van externe securityonderzoekers via het *bug bounty* programma van HackerOne[156] en heeft een securityprogramma waarbij onderzoekers toegang krijgen tot een GM auto. Een ander voorbeeld hierin is Tesla die als eerste fabrikant zijn auto beschikbaar stelde voor een publieke hackerwedstrijd Pwn2Own. Daarmee volgt Tesla het voorbeeld van softwarebedrijven zoals Microsoft en Apple.

Kennis over kwetsbaarheden en het vermogen om deze op te lossen is voornamelijk aanwezig bij de fabrikant en niet bij garagebedrijven of dealers. Deze zijn afhankelijk van de fabrikant en zijn in het algemeen niet in staat zelfstandig cybersecurityonderzoek te doen. Omdat dealers en garages geen rol hebben in de keten op het gebied cybersecurity, ontbreken *checks-and-balances* in de keten en komt een grotere verantwoordelijkheid te liggen bij de fabrikant.

In de statistieken van de *bug bounty* programma's is te vinden dat er vele gerapporteerde kwetsbaarheden zijn opgelost. In de praktijk gaan automerken verschillend om met het oplossen van gevonden kwetsbaarheden zoals in paragraaf 4.2.5 wordt besproken. Bij de meeste merken is onbekend of er kwetsbaarheden zijn of zijn geweest in een specifiek model. Controle hierop ontbreekt.

Onderling delen fabrikanten dreigingen en *best practices* en informatie over hacks en andere incidenten binnen de *automotive information sharing and analysis center* (Auto-ISAC)[157]. De Auto-ISAC is een positief voorbeeld hoe een vaak onderling gesloten auto-industrie samenwerkt op het gebied van cybersecurity.

156 HackerOne, *How GM works with hackers to enhance their security*, 2018.
157 Voor meer informatie, zie https://www.automotiveisac.com/

Deelconclusies
Er is nog geen grootschalig misbruik van kwetsbaarheden in voertuigen geweest waardoor de verkeersveiligheid in gevaar kwam. Cybersecurity zal een belangrijk issue worden als hackers een praktisch toepasbaar verdienmodel vinden. Het is onduidelijk of de branche hierop afdoende zal kunnen reageren.

De kennis over kwetsbaarheden en de keuzes die hierin gemaakt worden (de cybersecurityrisico-inschatting) liggen bij de fabrikant en worden spaarzaam gedeeld met andere ketenpartijen, zoals dealer of garage. Ook de overheid en de gebruikers hebben hier geen inzicht in.

Overzicht bevindingen op gebied van cybersecurity
Het onderwerp cybersecurity komt aan de orde in zowel hoofdstuk 3 als hoofdstuk 4 en hoofdstuk 5. Daarom hebben we de belangrijkste bevindingen op het gebied van cybersecurity hier samengevat.

Cybersecurity heeft de laatste jaren steeds meer de aandacht binnen de auto-industrie. De noodzaak is duidelijk geworden door verschillende gevonden kwetsbaarheden. Fabrikanten moeten afwegen hoeveel zij willen investeren in security om toekomstige dreigingen te kunnen weerstaan. Een complicatie hierbij voor de auto-industrie ten opzichte van andere sectoren, zoals kantoorautomatisering, is de lange ontwikkeltijd, lange levensduur en het complexe stelsel van onderdelen, leveranciers en software. Dit maakt het extra relevant om de cybersecurityprincipes (referentiekader, paragraaf 2.2) overal toe te passen.

Over de cybersecuritymaatregelen die nodig zijn in het ontwerp van de huidige auto en welke cybersecuritymaatregelen er genomen moeten worden voor eerder geproduceerde auto's is nog geen consensus. Normen en *best practices* voor cybersecurity zijn in ontwikkeling. Eisen voor cybersecurity in de vorm van wetgeving zijn in ontwikkeling.

Autofabrikanten hebben moeite om cybersecurity op een juiste en effectieve manier toe te passen. De volgende knelpunten zijn geïdentificeerd rond het onderwerp cybersecurity:

- Het is moeilijk vast te stellen hoeveel van cybersecurity van een auto nog het gevolg is van onbekendheid met de elektronica in het voertuig (*security-by-obscurity* in plaats van *defense-in-depth*).
- In veel gevallen is het onduidelijk of de software van een bepaald eerder geproduceerd model en type auto up-to-date is en bij de fabrikant bekende kwetsbaarheden bevat (gebrek aan transparantie).
- De software van auto's wordt onvoldoende bijgehouden, waardoor de cybersecurity gedurende de gehele levensduur onvoldoende geborgd is.
- Voor systemen die aan de auto gekoppeld zijn, zoals kaartmateriaal en mobiele telefoons, bestaan geen toelatingseisen en evenmin permanente eisen, terwijl deze systemen direct impact hebben op de cybersecurity en dus mogelijk indirect op de veiligheid.
- De huidige auto is niet ingericht om na een ongeluk te kunnen onderzoeken of dit mogelijk cybersecurity gerelateerd is. Door het gebrek aan empirische gegevens kan er onvoldoende van cybersecurity incidenten worden geleerd (gebrek aan openbaarheid en toegankelijkheid).
- Cybersecurity incidenten zullen vaker voorkomen als hackers een praktisch toepasbaar verdienmodel vinden. Het is onduidelijk of de branche hierop afdoende zal kunnen reageren (controlestructuur onbekend).
- De cybersecurityrisico-inschatting wordt nu uitsluitend gemaakt door de autofabrikant; gebruikers en overheden moeten er op vertrouwen dat dit op een juiste manier gebeurt. Dit is strijdig met de in paragraaf 2.1 beschreven veiligheidsprincipes bij de introductie van nieuwe technologie.

5.5 Conclusies

ADAS vormen vooral voor de gebruikers en de overheid op allerlei niveaus een 'black box'. Dit komt de verkeersveiligheid niet ten goede. Er is gebrek aan inzicht in de werking van ADAS en het is niet duidelijk in welke auto's ADAS aanwezig zijn. Evenmin is voor alle typen ADAS inzichtelijk welk effect een bepaalde ADAS heeft op de verkeersveiligheid. Hiermee is niet voldaan aan de veiligheidsprincipes transparantie en uitlegbaarheid die onderdeel vormen van maatschappelijk verantwoord innoveren. Ook ontbreken goede 'poortwachters' bij de introductie van ADAS. En er vinden geen gestructureerde evaluaties plaats naar de reductie van ongevallen die door ADAS gerealiseerd zou moeten worden. Innovatie gaat door zonder bijsturing en zonder de nodige mitigerende maatregelen. Verder is er geen goede monitoring na introductie van deze nieuwe technologieën. Ongevallen met ADAS worden niet gemonitord. Dit alles wordt nog versterkt door de beperkte bereidheid van betrokken partijen om data te delen. Zowel transparantie als de beschikbaarheid van empirische gegevens zijn noodzakelijk voor de overheid in het bijsturen en ingrijpen.

6 CONCLUSIES

Nieuwe risico's
Automatisering in het wegverkeer kan bijdragen aan vergroting van de verkeersveiligheid maar gaat ook gepaard met nieuwe verkeersveiligheidsrisico's. Op basis van onderzoek van ongevallen, bestudering van literatuur en gesprekken met experts identificeert de Onderzoeksraad voor Veiligheid een aantal soorten nieuwe risico's, die nog niet voldoende onderkend en beheerst worden. ADAS zijn nog niet volwassen als ze op de markt komen. Dit betekent dat ze nog verder doorontwikkeld worden na toelating op de openbare weg. Samen met het kennisgebrek van bestuurders, ontstaan situaties waarin bestuurders niet begrijpen waarom de auto op een bepaalde manier reageert of juist niet reageert. Daarnaast vervullen bestuurders in auto's met ADAS een andere rol dan in conventionele auto's, namelijk de rol van operator. Het takenpakket dat bij deze rol hoort, heeft als risico dat bestuurders minder alert zijn en minder snel reageren. Verder betekent de voortschrijdende automatisering dat auto's met ADAS steeds meer een rijdende computer zijn geworden. Daarmee worden ook de risico's die horen bij computers steeds meer in auto's met ADAS geïntroduceerd. Het gaat hierbij om cybersecurityrisico's en om het risico dat noodzakelijke veiligheidsupdates uitblijven. Ook kunnen updates juist een risico vormen, als deze de functionaliteit van de ADAS en daarmee het rijgedrag van de auto veranderen zonder dat de bestuurder zich dat realiseert.

Bestuurder staat niet centraal
ADAS zijn vaak niet volwassen. In combinatie met ongetrainde bestuurders leidt dit ertoe dat de bestuurder in een auto met ADAS ervaart dat het systeem de besturing van de auto regelmatig overneemt. Soms verrast het systeem de bestuurder met ingrepen of het uitblijven van ingrepen. 'Wie stuurt?' is dan letterlijk een vraag van levensbelang. Auto-industrie en overheden vinden deze vraag in de huidige generatie ADAS echter irrelevant. Zij houden zich bij de traditionele, juridische benadering dat de bestuurder aansprakelijk is, terwijl deze onvoldoende geëquipeerd is om de ADAS met dit besef te gebruiken. In hun marketing en voorlichting versterken autofabrikanten de indruk dat ADAS vooral de veiligheid en het gemak van de automobilist zouden dienen, zonder te wijzen op de nieuwe veiligheidsrisico's die gepaard gaan met automatisering.

Veiligheid niet centraal bij het ontwerp
Automatisering in auto's wordt gedreven door de technologische mogelijkheden. Zeker voor ADAS die gericht zijn op het vergroten van het rijcomfort vormen deze het uitganspunt bij de ontwikkeling binnen de onvoldoende geoperationaliseerde randvoorwaarde dat de veiligheid er niet op achteruit mag gaan. De gebruiker staat niet centraal bij het ontwerp. Verder wordt bij het ontwerp onvoldoende nagedacht over de veiligheid gedurende de levensduur. Zo is cybersecurity gedurende de gehele levensduur onvoldoende gewaarborgd. Vaak is het onbekend of de software van een auto kwetsbaarheden bevat.

Wetgeving niet passend
De technologische veranderingen gaan sneller dan de regulering ervan. Het gevolg is dat de huidige wetgeving niet meer past bij de moderne auto, die als het ware veranderd is in een rijdende computer. Met name op gebied van human factors blijven de regels achter, omdat fabrikanten en overheid hier ook minder aandacht voor hebben. De regelgeving is ook niet toegespitst op het gegeven dat auto's dynamischer worden en na toelating op de openbare weg veranderen door updates. In aanvulling op de traditionele detailregelgeving is er ook wetgeving die een minimaal veiligheidsniveau voorschrijft. Hierin wordt echter nergens aangegeven hoe het veiligheidsniveau van ADAS kan worden beoordeeld. Dat heeft tot gevolg dat er geen toezicht bestaat op de wijze waarop fabrikanten risico's inschatten en scenario's overwegen. Hierdoor worden er systemen toegelaten waarvan onbekend is wat het effect is op de verkeersveiligheid.

Onvoldoende lerend vermogen
Zowel fabrikanten als overheid leren onvoldoende van ongevallen doordat:

- er geen registratie is van welke ADAS zich in welke voertuigen bevinden;
- ongevallen met ADAS niet gemonitord worden;
- de ongevallenregistratie van de politie in het algemeen onvolledig is en dodelijke ongevallen hooguit geteld maar niet geanalyseerd worden;
- de benodigde gegevens niet of moeilijk uit een voertuig te halen zijn;
- er geen gestructureerde evaluatie plaatsvindt naar de reductie van ongevallen die door ADAS gerealiseerd zou moeten worden.

Het is hierdoor onbekend hoeveel ongevallen met ADAS er plaatsvinden en hoeveel er door ADAS worden voorkómen. Fabrikanten leren te weinig van ongevallen met hun eigen merk auto's. Ze onderzoeken een groot deel van de ongevallen niet. Fabrikanten leren niet van elkaar, waardoor het lerend vermogen van de sector beperkt is. Toeleveranciers zijn bijna nooit betrokken bij ongevallenonderzoek ten behoeve van verbetering van de verkeersveiligheid.

Te weinig aandacht voor de huidige generatie ADAS
De overheid, in het bijzonder het ministerie van IenW, is meer bezig met de (verre) toekomst van de zelfrijdende auto dan met de introductie en het gebruik van de huidige generatie ADAS. Het ministerie heeft weinig visie op hoe ADAS zouden moeten bijdragen aan het verbeteren van de verkeersveiligheid en voert niet proactief en op een systematische manier risicoanalyses uit. Tegelijkertijd is IenW gestart om ADAS onder voorwaarden te stimuleren, maar de verbetering van verkeersveiligheid is niet noodzakelijk als het effect op één van de drie doelen verkeersveiligheid, milieu of doorstroming maar positief is. Nieuwe regelgeving die in ontwikkeling is bij de UNECE onder meer op het gebied van mens-machine interactie en het beschikbaar maken van data uit ADAS om ongevallen goed te kunnen onderzoeken heeft alleen betrekking op toekomstige systemen die de controle (tijdelijk) van de bestuurder overnemen, terwijl de wetgeving ook niet meer past voor de huidige systemen die de bestuurder assisteren of ondersteunen.

Effect op verkeersveiligheid onzeker

Zowel de Nederlandse regering als de Europese Commissie streven naar nul verkeersdoden in 2050. Om dit ambitieuze doel te halen, is veel hoop gevestigd op technologische ontwikkelingen en automatisering van de auto in het bijzonder. Er ontstaan echter ook nieuwe risico's met de introductie en het gebruik van ADAS, die nog onvoldoende onderkend, gemonitord en beheerst worden. In potentie kunnen ADAS weliswaar een positieve invloed hebben op de verkeersveiligheid maar nu ontbreken de waarborgen om die potentie ook echt ten volle te benutten.

7 AANBEVELINGEN

Aan de autofabrikanten en de koepelorganisaties OICA en ACEA:

1. Toon aan dat de ontwikkeling en introductie van ADAS plaatsvindt volgens de principes van maatschappelijk verantwoord innoveren.

Aan de BOVAG en RAI Vereniging:

2. Zorg ervoor dat BOVAG-leden klanten uitgebreid instrueren over de mogelijkheden en beperkingen van hun auto met ADAS. En zorg dat BOVAG-leden daartoe in staat worden gesteld.

Aan de minister van Infrastructuur en Waterstaat:

3. Neem initiatief om binnen de UNECE *human factors* en maatschappelijk verantwoord innoveren op de agenda te krijgen.

4. Steun de initiatieven van Euro NCAP om *human factors* en consumenteninformatie over ADAS onderdeel te laten zijn van de veiligheidsbeoordeling van auto's (Euro NCAP sterren).

5. Verbeter de mogelijkheden om te leren van verkeersongevallen in het algemeen en de rol van ADAS in het bijzonder en tref maatregelen ten behoeve van de verkeersveiligheid op basis van de onderzoeksresultaten.

6. Kaart bij de Europese Commissie aan dat de voertuigregelgeving aan moet sluiten bij de huidige generatie ADAS (SAE level 2 en lager). Daarbij moet de verantwoordelijkheid om aan te tonen dat nieuwe ADAS de veiligheid verbeteren bij de fabrikanten komen te liggen. Verder moet aandacht besteed worden aan eisen op het gebied van human factors, opleiding van gebruikers, toegankelijkheid van data uit ADAS na ongevallen en ongevalsonderzoek door fabrikanten.

LITERATUURLIJST

AAA, Advanced Driver Assistance Technology Names, 2019, https://newsroom.aaa.com/2019/01/common-naming-for-adas-technology/.

AAA, Automatic emergency braking with pedestrian detection, 2019, https://www.aaa.com/AAA/common/aar/files/Research-Report-Pedestrian-Detection.pdf.

AAA Foundation for Traffic Safety, Potential Reductions in Crashes , Injuries , and Deaths from Large-Scale Deployment of Advanced Driver Assistance Systems, 2018, http://aaafoundation.org/wp-content/uploads/2018/09/18-0567_AAAFTS-ADAS-Potential-Benefits-Brief_v2.pdf.

AAA Foundation for Traffic Safety, Vehicle Owners' Experiences with and Reactions to Advanced Driver Assistance Systems, 2018, https://aaafoundation.org/vehicle-owners-experiences-reactions-advanced-driver-assistance-systems/.

Abraham, H., Seppelt, B., Mehler, B., en Reimer, B., What's in a name: Vehicle technology branding and consumer expectations for automation, AutomotiveUI 2017 - 9th International ACM Conference on Automotive User Interfaces and Interactive Vehicular Applications, Proceedings, nummer September, 2017.

ACEA, ACEA Position Paper; General Safety Regulation Revision. Brussel, 2018.

ADAS Alliantie, ADAS Convenant, 2019.

ADAS Alliantie, Website ADAS Alliantie, https://www.adasalliantie.nl. Geraadpleegd op 23 augustus, 2019.

Alvarez, S., Safety Benefit Assessment, Vehicle Trial Safety and Crash Analysis of Automated Driving: A Systems Theoretic Approach. PSL Research University, 2017, https://pastel.archives-ouvertes.fr/tel-01767563.

ANWB, Verwachtingen Werking Lane Assist Nog Te Hoog Gespannen; Onderzoek Naar Rijbaanhulpsysteem in Auto's, 2017, https://www.anwb.nl/auto/zelfrijdende-auto/rijbaan-hulp-lane-assist-onderzoek.

ANWB, Welke Rijhulpsystemen Zijn Er?, 2017, https://www.anwb.nl/auto/zelfrijdende-auto/andere-systemen.

Aon Risk Solutions, Whitepaper: Als de Auto Autonoom Wordt; Verkennende Analyse van de Verzekeringsmarkt En Nieuwe Risico's Bij Zelfrijdende Auto's, 2015.

BCG, A Roadmap to Safer Driving through Advanced Driver Assistance Systems, 2015.

Bloomfield, R., Butler, E., Guerra, S., en Netkachova, K., Security-Informed Safety: Integrating Security within the Safety Demonstration of a Smart Device, 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, 2017, http://openaccess.city.ac.uk/17724/1/pp9v01n_npic_cyber_smarts.pdf.

Boelhouwer, A., Beukel, A.P. van den, Voort, M.C. van der, en Martens, M.H., Should I Take over? Does System Knowledge Help Drivers in Making Take-over Decisions While Driving a Partially Automated Car?, Transportation Research Part F: Traffic Psychology and Behaviour 60, nummer december, 2019: 669–684, https://doi.org/10.1016/j.trf.2018.11.016.

Borup, M., Brown, N., Konrad, K., and Lente, H. van, The Sociology of Expectations in Science and Technology , Technology Analysis and Strategic Management 18, 2006: 285–298.

British Standards Institution, Connected Automotive Ecosystems – Impact of Security on Safety – Code of Practice, Vol. PAS 11281, 2018.

British Standards Institution, The Fundamental Principles of Automotive Cyber Security. Specification, Vol. PAS 1885, 2018, https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114.

British Standards Institution, The Fundamental Principles of Automotive Cyber Security, Vol. PAS 1885, 2018, https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114.

C't Magazine, Connected Cars in de Fout Bij Cybersecurity, 2016, https://www.ct.nl/achtergrond/connected-cars-fout-cybersecurity/.

Cai, Z., Wang, A., Zhang, W., Gruffke, M., en Schweppe, H., 0-Days & Mitigations : Roadways to Exploit and Secure Connected BMW Cars, White Paper Blackhat USA 2019 Conference, 2019: 1–37.

CAR, Technology Roadmaps: Intelligent Mobility Technology, Materials and Manufacturing Processes, and Light Duty Vehicle Propulsion, 2017, https://doi.org/10.1044/leader.ppl.22062017.20.

Carsten, O., en Martens, M.H., How Can Humans Understand Their Automated Cars? HMI Principles, Problems and Solutions, Cognition, Technology and Work 21, nummer 1, 2019: 3–20, https://doi.org/10.1007/s10111-018-0484-0.

Charette, R.N., This Car Runs on Code, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code. Geraadpleegd op 21 augustus, 2019.

Charlebois, D., Meloche, E., en Burns, P., Detection of Cyclist and Pedestrians Around Heavy Commercial Vehicles, In 26th International Technical Conference and Exhibition on the Enhanced Safety of Vehicles (ESV). Eindhoven: Transport Canada, 2019.

Daimler, BMW en Daimler. Plan to Headquarter Joint Venture in Berlin, https://www.daimler.com/innovation/case/shared-services/jv-daimler-and-bmw.html. Geraadpleegd op 22 augustus, 2019.

Dave, P., Google Ditched Autopilot Driving Feature after Test User Napped behind Wheel, Edited by Sam Holmes. Atwater, California, USA: Reuters, 2017.

Electrek.co, Tesla Increases Autopilot 2.0 Speed Limits with Latest Update, https://electrek.co/2017/03/08/tesla-autopilot-2-0-speed-limit-update/. Geraadpleegd op 21 mei, 2018.

Electrek.co, Tesla Releases New Update to Enable Full Speed Automatic Emergency Braking for Autopilot 2.5 and More, https://electrek.co/2017/10/22/tesla-update-full-speed-automatic-emergency-braking-autopilot-2-5/. Geraadpleegd op 7 augustus, 2018.

Endsley, M.R., en Kaber, D.B., Level of Automation Effects on Performance, Situation Awareness and Workload in a Dynamic Control Task., Ergonomics 42, nummer 3, 1999: 462–492.

ENISA, Cyber Security and Resilience of Smart Cars; Good Practices and Recommendations, 2016.

ETSC, BRIEFING | EU Strategy for Automated Mobility, 2018.

ETSC, Prioritising the Safety Potential of Automated Driving in Europe, 2016.

ETSC, Road Safety Priorities for The EU 2020-2030; Briefing for the European Parliamentary Elections, 2018, http://etsc.eu/wp-content/uploads/2015_lux_pres_briefing_final.pdf.

EU-lidstaten, Declaration of Amsterdam; Cooperation in the Field of Connected and Automated Driving, 2016.

Euro NCAP, Euro NCAP 2025 Roadmap: in pursuit of vision zero, 2017

Euro NCAP, 2018 Geautomatiseerde Rijsystemen, 2018, https://www.euroncap.com/nl/veiligheid-voertuig/veiligheidscampagnes/2018-geautomatiseerde-rijsystemen/.

Europese Commissie, Annex 1: Strategic Action Plan on Road Safety, In Europe on the Move; Sustainable Mobility for Europe: Safe, Connected and Clean, 2018.

Europese Commissie, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions; On the Road to Automated Mobility: An EU Strategy for Mobility of the Future, 2018.

Europese Commissie, Persbericht Verkeersveiligheid: Commissie Verheugd over Akkoord over Nieuwe EU-Regels Om Levens Te Helpen Redden, https://europa.eu/rapid/press-release_IP-19-1793_nl.htm. Geraadpleegd op 23 augustus, 2019.

Eykholt, K., Evtimov, I., Fernandes, E., Kohno, T., Li, B., Prakash, A., Rahmati, A., en Song, D., Robust Physical-World Attacks on Deep Learning Visual Classification, CVPR, nummer 2018, 2017, https://arxiv.org/pdf/1707.08945.pdf.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., en Luetge, C., An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines 28, number 4, 2018: 689–707, https://doi.org/10.31235/OSF.IO/2HFSC.

Folda, C., From Requirement to Standard Security Test; A Brief Introduction to the World of Security Testing, Vector Cybersecurity Symposium 2019, 2019, https://assets.vector.com/cms/content/events/2019/vSES19/vSES19_08_Folda_Continental.pdf.

Fridman, L., Brown, D. Glazer, M. Angell, W., Dodd, S., Jenik, B., Terwilliger, J., Patsekin, A., Kindelsberger, J., Ding, L., Seaman, S., Mehler, A., Sipperley, A., Pettinato, A., Seppelt, B.D., Angell, L., Mehler, B., en Reimer B., MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction With Automation, IEEE Access 7, 2019

Future of Life Institute, AI Principles, https://futureoflife.org/ai-principles/?cn-reloaded=1. Geraadpleegd op 7 januari, 2019.

Gorter, M., en Klem, E., Markering En Rijtaakondersteunende Systemen. Amersfoort: Royal Haskoning DHV in opdracht van de provincie Utrecht, 2016.

GOV.UK, The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles, Gov.Uk, 2017, https://doi.org/10.1016/j.molcel.2010.01.018.

Greenberg, A., After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/. Geraadpleegd op 17 augustus, 2018.

Greenberg, A., Hackers Remotely Kill a Jeep on the Highway—With Me in It, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Geraadpleegd op 17 augustus, 2018.

Greenberg, A., Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video). Forbes, https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video. Geraadpeegd op 23 augustus, 2018.

Greenberg, A., The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. Wired, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. Geraadpleegd op 23 augustus, 2018.

HackerOne, How GM Works with Hackers to Enhance Their Security, 2018.

Harms, I.M., en Dekker, G.-M., ADAS: From Owner to User; Insights in the Conditions for a Breakthrough of Advanced Driver Assistance Systems, 2017.

Hattem, J. Van, Klem, E., en Gorter, M., AEBS En Verkeersmaatregelen; Praktijktest Zichtbaarheid Verkeersmaatregelen Voor Autonomous Emergency Braking Systems, Amersfoort: Royal Haskoning DHV, 2017.

High Level Group on the Competiteness and Sustainable Growth of the Automotive Industry in European Union, Gear 2030, 2017.

Iriondo, R., Differences Between AI and Machine Learning, and Why It Matters, https://medium.com/datadriveninvestor/differences-between-ai-and-machine-learning-and-why-it-matters-1255b182fc6. Geraadpleegd op 23 augustus, 2019.

ISO, ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level. Gene, 2018.

ISO, The ISO/IEC 27000 Family of Standards Helps Organizations Keep Information Assets Secure., https://www.iso.org/isoiec-27001-information-security.html. Geraadpleegd op 23 augustus, 2019.

ISO, en IEC, ISO/IEC 15408-1:2009, ISO, 2009.

Jong, R. De, Kool, L., en Est, R. Van, Zo Brengen We AI in de Praktijk Vanuit Europese Waarden, 2019, https://www.rathenau.nl/sites/default/files/inline-files/Zo brengen we AI in de praktijk vanuit Europese waarden - Roos de Jong%2C Linda Kool en Rinie van Est_0.pdf.

Klem, E., Barten, N., Droogsma, J., Gorter, M., en Huisman, M., AEBS En Vrachtwagens; Praktijktest Herkenbaarheid Vrachtwagens Voor Advanced Emergency Braking System. Royal Haskoning DHV, 2017.

Knapp, A., Neumann, M., Brockmann, M., Walz, R., en Winkle, T., Code of Practice for the Design and Evaluation of ADAS, 2009, https://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf.

Kyriakidisa, M., Winter, J.C.F. de, Stanton, N., Bellet, T., Arem, B. van, Brookhuis, K., en Martens, M.H., A Human Factors Perspective on Automated Driving, Theoretical Issues in Ergonomics Science 18, nummer 1, 2017: 1–27, https://doi.org/http://dx.doi.org/10.1080/1463922X.2017.1293187.

Leplat, J., Occupational Accident Research and Systems Approach, Journal of Occupational Accidents 6, nummer 1–3, 1984: 77–89.

McCandless, D., Doughty-White, P., en Quick, M., Million Lines of Code, https://informationisbeautiful.net/visualizations/million-lines-of-code/. Geraadpleegd op 10 juli, 2019.

McKinsey&Company, Rethinking Car Software and Electronics Architecture, 2018: 1–15.

Michigan Tech Research Institute, Benchmarking Sensors for Vehicle Computer Vision Systems, https://mtri.org/automotivebenchmark.html. Geraadpleegd op 28 augustus, 2019.

Minister van Infrastructuur en Milieu, Kamerbrief 31305 Mobiliteitsbeleid, 2014.

Minister van Infrastructuur en Waterstaat, Beantwoording Kamervragen van de Leden Dijkstra En Van Gent (VVD) over de Berichten "De Schrikbarende Stijging Die Niemand Kan Verklaren" En "Verkeersanalyse Provincie Nutteloos Door Privacywet," 2019.

Minister van Infrastructuur en Waterstaat, Kamerbrief 205325 Smart Mobility Dutch Reality, 2018.

Minister van Infrastructuur en Waterstaat, Kamerbrief Beantwoording Kamervragen van de Leden Schonis En Verhoeven (Beiden D66) over Het Artikel 'Wie Temt Het Datamonster in de Auto-Industrie?, 2019.

Ministerie van Infrastructuur en Waterstaat, Ministerie van Justitie en Veiligheid, IPO, VNG, Vervoerregio Amsterdam, en Metropoolregio Rotterdam Den Haag, Veilig van Deur Tot Deur Veilig van Deur Tot Deur; Het Strategisch Plan Verkeersveiligheid 2030: Een Gezamenlijke Visie Op Aanpak Verkeersveiligheidsbeleid, 2018.

Ministerie van Infrastructuur en Waterstaat, Landelijk Actieplan Verkeersveiligheid 2019-2021: Veilig van Deur Tot Deur. Den Haag, 2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/12/05/bijlage-2-landelijk-actieplan-verkeersveiligheid-2019-2021.

National Cyber Security Center, Cybersecuritybeeld Nederland CSBN 2018, 2018.

National Instruments, Building Flexible, Cost-Effective ECU Test Systems, 2019, https://www.ni.com/nl-nl/innovations/white-papers/06/building-flexible--cost-effective-ecu-test-systems.html.

Nes, C.N. Van, en Duivenvoorden, C.W.A.E., Veilig Naar Het Verkeer van de Toekomst; Nieuwe Mogelijkheden, Risico's En Onderzoeksagenda Voor de Verkeersveiligheid Bij Automatisering van Het Verkeerssysteem, R-2017-2. Den Haag: SWOV, 2017.

NHTSA, A Summary of Cybersecurity Best Practices, 2014.

NHTSA, Cybersecurity Best Practices for Modern Vehicles, 2016, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.

Nick Davis, Automotive Electronics: What Are They, and How Do They Differ from "Normal" Electronics? - Power Electronics, https://www.powerelectronicsnews.com/technology/automotive-electronics-what-are-they-and-how-do-they-differ-from-normal-electronics. Geraadpleegd op 23 augustus, 2019.

Nie, S., Liu, L., en Du, Y., Free-Fall: Hacking Tesla from Wireless to CAN Bus, In Blackhat, Vol. Briefings. USA, 2017, https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

Nissan, Nissan LEAF - Elektrische Auto - Elektrische Voertuigen, 2019, https://www.nissan.nl/voertuigen/nieuw/leaf.html.

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018, https://doi.org/10.6028/NIST.CSWP.04162018.

NIST, NIST Special Publication 800-Series, https://csrc.nist.gov/publications/sp800. Geraadpleegd op 24 januari, 2019.

NTSB, Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck - Highway Accident Report, 2017, https://doi.org/10.1093/jicru/ndl025.

NTSB, Preliminary Report: Highway HWY18FH011, 2018, 4, https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18FH011-preliminary.pdf.

NTSB, Preliminary Report - Highway - HWY18MH010. Washington D.C., 2018, https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.

Onderzoeksraad voor Veiligheid, Koolmonoxide: Onderschat en onbegrepen gevaar, 2015.

Onderzoeksraad voor Veiligheid, MH17 Crash, 2015.

Onderzoeksraad voor Veiligheid, Opkomende Voedselveiligheidsrisico' s, 2019.

PBL, Mobiliteit En Elektriciteit in Het Digitale Tijdperk. Publieke Waarden Onder Spanning, 2017.

Poel, I. van de, An Ethical Framework for Evaluating Experimental Technology, Science and Engineering Ethics 22, nummer 3, 2016: 667–686, https://doi.org/10.1007/s11948-015-9724-3.

Rathenau Instituut, Met Beleid Vormgeven Aan Sociotechnische Innovatie, 2016.

Rathenau Instituut, Mensenrechten in Het Robottijdperk, 2017.

RDW, Jaarverslag 2018, 2019.

Rip, A., The Past and Future of RRI, Life Sciences, Society and Policy 10, nummer 1, 2014: 17, https://doi.org/10.1186/s40504-014-0017-4.

Russel, S., en Norvig, P., Artificial Intelligence – A Modern Approach, 2010, https://doi.org/10.1017/S0269888900007724.

SAE International, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061, 2016.

SAE International, Requirements for Hardware-Protected Security for Ground Vehicle Applications - J3101, 2012, https://www.sae.org/standards/content/j3101/.

SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report, 2014.

Santoni de Sio, F., Ethics and Self-Driving Cars; A White Paper on Responsible Innovation in Automated Driving Systems, nummer oktober, 2016.

Schomberg, R. von, A Vision of Responsible Research and Innovation, In Responsible Innovation, edited by M. Heintz and J Bessant R. Owen. Londen: John Wiley, 2013.

Staak, B. Van der, Verdwijnende Apps Op Smart-Tv's, 2018, https://www.consumentenbond.nl/tv/honderden-meldingen-over-verdwijnende-apps-op-smart-tvs.

SWOV, Dodelijke Verkeersongevallen Op Rijkswegen in 2017, 2019.

SWOV, Ernstig Verkeersgewonden 2017, 2018, https://www.swov.nl/publicatie/ernstig-verkeersgewonden-2017.

SWOV, Factsheet Verkeersdoden in Nederland, 2019.

SWOV, Veiligheidseffecten van Rijtaakondersteunende Systemen; Bijlage Bij Het Convenant van de ADAS Alliantie, 2019.

Teffer, P., Dieselgate. Hoe de Industrie Sjoemelde En Europa Faalde, 2017.

Tencent, Experimental Security Assessment of BMW Cars: A Summary Report, 2018.

Tesla, Q3 2018 Vehicle Safety Report, https://www.tesla.com/nl_NL/blog/q3-2018-vehicle-safety-report. Geraadpleegd op 12 december, 2018.

Tesla, Tesla Model S Gebruikershandleiding, 2018, https://www.tesla.com/sites/default/files/model_s_owners_manual_europe_nl_nl.pdf.

Tricentis, AI Approaches Compared: Rule-Based Testing vs. Learning, https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/. Geraadpleegd op 23 augustus, 2019.

UNECE, ECE/TRANS/WP.29/2019/34, Framework Document on Automated/Autonomous Vehicles, 2019.

UNECE, ECE/TRANS/WP.29/78/Rev.6, Consolidated Resolution on the Construction of Vehicles (R.E.3), Revision 6, 2017, https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r6e.pdf.

UNECE, ECE/TRANS/WP.29/GRVA/2019/2, Proposal for a Recommendation on Cyber Security, 2019, http://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf.

UNECE, Proposal for Amendments to ECE/TRANS/WP.29/2019/34; Framework Document on Automated/Autonomous Vehicles (Levels 3 and Higher), 2019.

UNECE, World Forum For Harmonization of Vehicle Regulations (WP.29); How It Works, How to Join It, 2019, http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29wgs/wp29gen/wp29pub/WP29-BlueBook-4thEdition2019-Web.pdf.

Vetzo, M.J., Gerards, J.H., en Nehmelman, R., Algoritmes En Grondrechten, 2018.

Vlakveld, W., Vissers, L., Hulleman, K., en Nes, N. van, An Empirical Exploration of the Impact of Transition of Control on Situation Awareness for Potential Hazards; An Experiment about the Hazard Perception Capabilities of Drivers after Interruption in a Video-Based Scanning Task. The Hague: SWOV, 2015.

Vlakveld, W., Nes, N. van, Bruin, J. De, Vissers, L., and Kroft, M. van der, Situation Awareness Increases When Drivers Have More Time to Take over the Wheel in a Level 3 Automated Car: A Simulator Study, Transportation Research Part F: Traffic Psychology and Behaviour, 2018, https://doi.org/10.1016/j.trf.2018.07.025.

VMS in opdracht van BOVAG, Het Effect van ADAS Op Schadeherstel , Onderhoud En Reparatie, 2019.

Volkswagen, Ford – Volkswagen Expand Their Global Collaboration to Advance Autonomous Driving, Electrification and Better Serve Customers, https://www.volkswagen-newsroom.com/en/press-releases/ford-volkswagen-expand-their-global-collaboration-to-advance-autonomous-driving-electrification-and-better-serve-customers-5188. Geraadpleegd op 22 augustus, 2019.

Volkswagen, Volkswagen Start Car.Software Met 5.000 in-House Ontwikkelaars, 2019, https://www.volkswagen.nl/nieuws/volkswagen-start-carsoftware-met-5000-in-house-ontwikkelaars/.

Weiss, S.M., en Indurkhya, N., Rule-Based Machine Learning Methods for Functional Prediction, Journal of Artificial Intelligence Research 3 (1995): 383–403, https://arxiv.org/pdf/cs/9512107.pdf.

Wezel, A.P. van, Lente, H. van, Sandt, J.J. van de, Bouwmeester, H., Vandeberg, R.L., en Sips, A.J., Risk Analysis and Technology Assessment in Support of Technology Development: Putting Responsible Innovation in Practice in a Case Study for Nanotechnology, Integrated Environmental Assessment and Management 14, nummer 1, 2018: 9–16, https://doi.org/10.1002/ieam.1989.

Wright, T.J., Samuel, S., Borowsky, A., Zilberstein, S., en Fisher, D.L., Experienced Drivers Are Quicker to Achieve Situation Awareness than Inexperienced Drivers in Situations of Transfer of Control within Level 3 Autonomous Environment., In Proceedings of the Human Factor and Ergonomics Society 2016 Annual Meeting, 60:270–273, 2016.

WRR, Onzekere Veiligheid: Verantwoordelijkheden Rond Fysieke Veiligheid, 2008.

Zhang, B., Winter, J. de, Varotto, S., Happee, R., en Martens, M., Determinants of Take-over Time from Automated Driving: A Meta-Analysis of 129 Studies, Transportation Research Part F: Traffic Psychology and Behaviour 64, 2019: 285–307, https://doi.org/10.1016/j.trf.2019.04.020.

ONDERZOEKSVERANTWOORDING

Deze bijlage beschrijft het onderzoeksproces op hoofdlijnen, de belangrijkste kwaliteitstoetsen en de projectorganisatie.

A.1 Doel, onderzoeksvragen en fasering van het onderzoek

Het doel van het onderzoek was het verbeteren van de verkeersveiligheid. Dit hebben we gedaan door partijen die zorg kunnen en moeten dragen voor veiligheid op de weg inzicht te geven in de manier waarop zij nieuwe risico's als gevolg van de introductie van ADAS inventariseren en beheersen. Gegeven dit doel stonden de volgende hoofdvragen centraal in dit onderzoek.

- Hoe beheersen de gebruikers, de auto-industrie, branchepartijen en de overheid de risico's verbonden aan de introductie en het gebruik van rijhulpsystemen (ADAS)?
- In hoeverre zijn er verbeteringen in de risicobeheersing mogelijk?

De focus van het onderzoek lag op de beheersing van de risico's van de introductie en het gebruik van (deels) geautomatiseerde voertuigen door fabrikanten, toeleveranciers, importeurs, dealers, toezichthouders, wetgevers, belangenorganisaties, etc. Het ging dus om de beheersing van de risico's en minder om de risico's zelf.

Uitwerking van de hoofdvragen in subvragen
Om de eerste hoofdvraag te beantwoorden, onderzochten we de huidige situatie en de manier waarop nieuwe risico's nu beheerst worden door partijen binnen het stelsel. Dat deden we op basis van de onderstaande vragen.

1. Hoe ziet het systeem van partijen die zorg kunnen of moeten dragen voor de veiligheid bij de introductie en het gebruik van ADAS er uit?
   a. Welke partijen zijn waarvoor verantwoordelijk? Wat is hun samenhang? Welke bestaande wet- en regelgeving is relevant?
   b. Wat is hun huidige werkwijze en taakopvatting?
   c. Wat is de historische achtergrond van deze verdeling van taken en verantwoordelijkheden?

2. Hoe brengen partijen risico's in kaart? En hoe spelen zij daarbij in op risico's die zich nog niet gemanifesteerd hebben?
   a. Hoe worden fundamentele karakterveranderingen van voertuigen binnen het systeem gedetecteerd?
   b. Hoe monitoren partijen (mogelijke) risico's?
   c. Welke soorten risico's worden in kaart gebracht ?
   d. Welk detailniveau?
   e. Inschatten ernst of grootte van de risico's?
3. Hoe beheersen partijen risico's?
4. Wat zijn volgens de Onderzoeksraad de uitgangspunten waar de branche en het systeem van regulering en toezicht aan moeten voldoen vanuit veiligheidsperspectief?
5. In hoeverre worden de risico's afdoende beheerst?
6. Zien partijen mogelijkheden om risico's beter te beheersen aan de hand van het door de Raad opgestelde referentiekader?

Fasering
Het onderzoek bestond uit vier fases.

Fase 1:	oriëntatie en achtergrond
Fase 2:	de huidige situatie: beantwoording van de onderzoeksvragen 1 t/m 3
Fase 3:	het referentiekader: beantwoording van de onderzoeksvraag 4
Fase 4:	Confrontatie bevindingen met referentiekader: onderzoeksvragen 5 en 6

Fase 1: De fase van oriëntatie en achtergrond betrof het in beeld krijgen van de sector (invloed en belangen) en het aanscherpen van de onderzoeksvragen. Dit was een iteratief proces dat tegelijkertijd plaatsvond. Daarnaast werden reeds bekende nieuwe risico's (literatuur en zorgen van partijen) globaal geïnventariseerd en werd een aantal ongevallen onderzocht. Ook de resultaten van onderzoek naar buitenlandse ongevallen (Tesla en Uber door NTSB) werden samengevat. In fase 1 werden enkele voorbeelden geselecteerd die gebruikt konden worden om de partijen te bevragen op hun huidige wijze van risicobeheersing. De fasen 2 t/m 4 liepen in elkaar over waarbij fase 2 en fase 3 gedeeltelijk parallel liepen.

A.2 Gegevensverzameling

Om de onderzoeksvragen gedurende de verschillende fases te kunnen beantwoorden zijn gegevens uit verschillende bronnen verzameld. Hieronder worden de belangrijkste informatiebronnen beschreven.

A.2.1 Interviews

Tabel 4 geeft een alfabetisch overzicht van de partijen die geïnterviewd zijn. Om kwaliteitsredenen worden interviews door de Onderzoeksraad altijd uitgevoerd door twee onderzoekers. Vooraf worden op basis van de onderzoeksvragen en naar aanleiding van de uitkomsten van de analyse (zie kopje "Analyse") in teamverband de onderwerpen voor het interview opgesteld. Van het interview werd een verslag gemaakt dat ter verificatie werd voorgelegd aan de geïnterviewde partijen.

Gedurende het onderzoek bleek het lastig om private partijen in het stelsel, zoals autofabrikanten, te spreken. De bereidheid van deze partijen om mee te werken aan het onderzoek was beperkt.

Organisatie	Organisatie
Agentschap Telecom	NTSB
ANWB	NXP
AON	Planbureau voor de Leefomgeving (PBL)
BOVAG	Politie (VOA)
CBR	PON
Computest	RAI-vereniging
Continental	Rathenau instituut
Cruise automation	Riscure
Daimler	RLI
DITSS	RDW
ENISA	RWS
ETSC	SWOV
Euro NCAP	Tesla
Europese Commissie, DG GROW, Unit C.4	TNO
Science and Technology, Maastricht University	Verbond van Verzekeraars
Ministerie van IenW	Volvo Cars
NFI	Volvo Trucks
NHTSA	Waag
Nissan	

Tabel 4: Overzicht van de organisaties waarmee interviews zijn gehouden en/of gesprekken zijn gevoerd.

A.2.2 Documenten

Een groot aantal documenten is geraadpleegd voor het onderzoek. Het betreft openbare wetenschappelijke artikelen/proefschriften over ADAS, wet- en regelgeving, tweede kamerstukken, ministeriële brieven, rapporten, krantenartikelen en interne/vertrouwelijke documenten van partijen die geïnterviewd zijn.

A.2.3 Werkbezoeken

Om als onderzoeksteam ervaring op te doen met het onderwerp is een praktijkmiddag georganiseerd waarbij is gereden met van diverse ADAS voorziene auto's van Tesla, Volvo en Nissan.

A.2.4 Conferenties en bijeenkomsten

Verder is relevante informatie vergaard door conferenties en bijeenkomsten bij te wonen. Het gaat om de onderstaande conferenties:

- EVU Haarlem 2017 (European Association for Accident Research)
- AEBS testdag, Lelystad, december 2017
- Humanist conference Den Haag 2018
- ADAS Congres Rosmalen 2018
- Bijeenkomst Scandinavische Onderzoeksraden 2019
- ESV2019 (International Conference on the Enhanced Safety of Vehicles) Eindhoven

A.2.5 Onderzoek van ongevallen met auto's met ADAS

Ter beantwoording van de onderzoeksvragen zijn tevens negen ongevallen met ADAS betrokkenheid onderzocht. Gegevens die hiervoor werden verzameld betroffen onder andere digitale tachograafgegevens en data/logbestanden van datarecorders. Zoals in het rapport beschreven was het niet eenvoudig om de benodigde digitale informatie uit de datarecorders van de auto te halen (versleuteling, geen of gebrekkige opslag EDR, geen logging) na een ongeval.

De Onderzoeksraad heeft bij het ongevallenonderzoek niet alleen gekeken naar de rol van ADAS bij het ontstaan of het beperken van de ernst van een ongeval, maar heeft ook andere factoren onderzocht die mogelijk hebben bijgedragen aan de totstandkoming van het ongeval, zoals de toestand van de bestuurder, het gebruik van de mobiele telefoon, weersomstandigheden en de toestand van de weg. Deze factoren worden niet uitgebreid beschreven in het rapport. Bij een deel van de onderzochte voorvallen bleken ADAS geen belangrijke rol te hebben gespeeld; deze voorvallen zijn opgenomen in bijlage C.3.

A.3 Analyse

A.3.1 CAST en CASCAD

Voor het analyseren van de gegevens is gebruikgemaakt van CAST (*Causal Analysis using* STAMP). Het betreft een methode gebaseerd op systeemtheorie (circulaire causaliteit - *feedback & control* – in plaats van het traditionele lineair causale model). Ongevallen/ onveiligheid vinden volgens STAMP plaats wanneer externe verstoringen, falende componenten of disfunctionele interacties tussen componenten niet worden beheerst door het hiërarchische stelsel van partijen (*control structure*). Veiligheid wordt aldus

gezien als een controleprobleem dat moet worden beheerst door een hiërarchisch stelsel van partijen (*control structure*) middels het opleggen en doorvoeren van '*safety constraints*'. Hiervoor hebben partijen uit het stelsel feedback nodig over het te beheersen proces. Voor de analyse van de voorvallen is een specifieke versie van CAST gebruikt die ontwikkeld is voor het analyseren van verkeersongevallen met geautomatiseerde voertuigen. Deze analysemethode heet CASCAD (*Causal Analysis using STAMP for Connected and Automated Driving*[158]). CAST is gebruikt om te analyseren hoe partijen in het stelsel veiligheidsrisico's rondom automatisering in het wegverkeer beheersen.

A.3.2 Analysesessies

De CAST/CASCAD analyse vond voor een deel plaats middels teamsessies. Deze teamsessies werden ook gebruikt om gegevens die door de verschillende teamleden verzameld waren gedurende de verschillende fases van het onderzoek op een systematische wijze te delen, te verrijken en te duiden. In totaal zijn zes analysesessies met het onderzoeksteam gehouden.

A.3.3 Stakeholderanalyse

Om zicht te krijgen op het belang bij het onderwerp en de beïnvloedingsmogelijkheden van partijen zijn door de afdeling communicatie twee stakeholderanalyses gehouden. Deze analyse vond in twee stappen plaats: 1) inventarisatie van stakeholders, 2) voor iedere stakeholder inschatten wat zijn belang is bij het onderwerp en in hoeverre hij het onderwerp kan beïnvloeden. Concreet is de uitkomst een overzicht waarin partijen ingedeeld worden op een matrix van veel/weinig invloed, positieve/negatieve houding en groot/beperkt belang. Door deze drie factoren op verschillende manieren met elkaar te combineren, kreeg het team inzicht in welke partijen voor- of tegenstander zijn, of ze belang hebben bij het onderzoek en welke partijen een essentiële rol hebben in de sector. Dit hielp de onderzoekers mede bij het bepalen van de volgorde en vorm van gesprekken en interviews.

A.3.4 Social media analyse

Er is een *social media* analyse uitgevoerd om het element 'gebruikersmeningen' toe te voegen aan het onderzoek. Vier onderzoeksvragen, één algemene en drie specifieke, zijn hiervoor opgesteld:

1. Wat vinden gebruikers van voertuigen met een vorm van ADAS over de aanwezigheid van deze technologie in hun auto?
2. Hoe ervaren gebruikers van voertuigen met een vorm van ADAS de voorlichting over de technologie bij de aanschaf van een nieuwe of tweedehands auto?
3. In welke mate melden gebruikers van voertuigen met een vorm van ADAS risico's of problemen met de technologie aan de fabrikant, en hoe reageert die op deze meldingen?
4. Hebben gebruikers van voertuigen met een vorm van ADAS ervaringen met ongevallen die nog niet in ons rapport staan?

158 Alvarez, *Safety benefit assessment, vehicle trial safety and crash analysis of automated driving: a Systems Theoretic approach* PSL Research University, 2017.

Eerst is een overzicht gemaakt van gebruikersgroepen en relevante sociale media, waarna data zijn verzameld van discussiewebsites. Dat betreffen 61 discussietopics, veelal van autoforums. Deze data zijn verwerkt op basis van kwalitatieve thematische analyse.

A.3.5 Vergelijking met de burgerluchtvaart

Bij de discussie over de invoering van ADAS in auto's wordt vaak de parallel getrokken met de invoering van geautomatiseerde systemen, zoals de automatische piloot, in de burgerluchtvaart. Wij hebben deze mogelijke parallel geanalyseerd en kwamen daarbij dusdanig grote verschillen tussen de commerciële burgerluchtvaart en het wegverkeer tegen dat we deze analyse niet in het rapport hebben opgenomen. De belangrijkste verschillen zijn:

- Piloten zijn veel beter geïnformeerd over en opgeleid en getoetst in de werking van de geautomatiseerde systemen dan automobilisten. Piloten worden getraind in hun rol als operator, automobilisten niet.
- Geautomatiseerde systemen in de luchtvaart worden beter getest en gevalideerd dan ADAS in auto's voordat ze in de praktijk worden toegepast.
- Bij het ontwerp van geautomatiseerde systemen in de luchtvaart wordt nadrukkelijk rekening gehouden met human factors, mens-machine interactie; in het wegverkeer nauwelijks.
- In de luchtvaart is een systeem van risicomanagement en terugkoppeling van ervaringen in werking dat leren van incidenten structureel ondersteunt; in het wegverkeer niet.
- Binnen de luchtvaart bestaat consensus over het grote belang van veiligheid dat commerciële belangen van individuele fabrikanten overstijgt, waar in de automobielsector commerciële belangen het lijken te winnen van de verkeersveiligheid.
- Het wegverkeer is complexer dan het luchtverkeer door verschillen in het aantal en de heterogeniteit van de verkeersdeelnemers.
- De maatschappelijke impact van luchtvaartongevallen met dodelijke slachtoffers is vele malen groter dan de impact van verkeersongevallen met dodelijke slachtoffers.

Dit alles betekent niet dat nieuwe automatiseringssystemen in de burgerluchtvaart altijd feilloos werken, maar wel dat problemen eerder worden opgemerkt en dat er maatregelen worden getroffen als er ondanks alle voorzorgsmaatregelen toch problemen optreden in de praktijk. Verder zijn er grote verschillen tussen de burgerluchtvaart waar geselecteerde en getrainde professionals vliegtuigen besturen en het wegverkeer waarin iedereen een auto moet kunnen besturen, waardoor bepaalde maatregelen niet kunnen worden overgenomen in het wegverkeer. Hierdoor hebben we besloten deze analyse geen prominente plek in het rapport te geven. Wel heeft deze verkennende analyse ons geleerd dat veiligheid meer aandacht moet krijgen bij het ontwerp van ADAS, dat automobilisten beter geïnformeerd moeten worden over de in hun auto aanwezige ADAS en dat autofabrikanten en overheden gezamenlijk moeten zorgen voor een goed werkend en transparant systeem om ervaringen in de praktijk terug te koppelen ten behoeve van het ontwerp van nieuwe ADAS en de aanpassing van bestaande ADAS.

A.4 Oordeelsvorming: bevindingen contrasteren met het referentiekader

In dit onderzoek was er veel aandacht voor onderzoeksactiviteiten gericht op het opstellen van het referentiekader. Dit referentiekader moest afgestemd zijn op nieuwe en veranderende risico's van een nieuwe technologie zoals ADAS (Hoofdstuk 2 geeft een uitgebreide beschrijving van het referentiekader). Het algemene referentiekader van de Raad, gebaseerd op de VMS-gedachte (zie paragraaf A.4.1) bood weliswaar een goede basis maar was niet voldoende flexibel. Het was nodig om vast te stellen aan welke uitgangspunten het systeem dat moet zorgdragen voor de veiligheid dient te voldoen om klaar te zijn voor de huidige en toekomstige technologische ontwikkelingen. Om het referentiekader op te kunnen stellen zijn literatuur en interviews gebruikt als gegevensbronnen. Daarnaast is in teamsessies gestructureerd nagedacht over welke principes in het referentiekader thuishoorden. Het team heeft met de betrokken partijen gekeken naar de verschillen tussen de huidige situatie en de gewenste situatie (beschreven in het referentiekader). Hiermee werd de tweede hoofdvraag beantwoord.

A.4.1 Algemene principes voor veiligheidsmanagement

Het algemene referentiekader van de Onderzoeksraad bestaat uit vijf principes waaraan partijen invulling aan zouden moeten geven om de veiligheid te beheersen. Deze principes zijn gebaseerd op (inter)nationale wet- en regelgeving en breed geaccepteerde en geïmplementeerde normen. Het betreft de volgende principes:

1. Inzicht in risico's als basis voor veiligheidsaanpak:
   Startpunt voor het bereiken van de vereiste veiligheid is:
   - een verkenning van het systeem;
   - gevolgd door een inventarisatie van de bijbehorende risico's.
2. Aantoonbare en realistische veiligheidsaanpak:
   Ter voorkoming en beheersing van ongewenste gebeurtenissen dient een realistische en praktisch toepasbare veiligheidsaanpak, inclusief de bijbehorende uitgangspunten, vastgelegd te worden. Deze veiligheidsaanpak dient vanuit de top van de organisatie vastgesteld en aangestuurd te worden. Deze veiligheidsaanpak is gebaseerd op:
   - wet- en regelgeving;
   - normen, richtlijnen, '*best practices*' en eigen inzichten en ervaringen van de organisatie en de voor de organisatie specifiek opgestelde veiligheidsdoelstellingen.
3. Uitvoeren en handhaven veiligheidsaanpak:
   Het uitvoeren en handhaven van de veiligheidsaanpak en het beheersen van de geïdentificeerde risico's vindt plaats door:
   - een beschrijving van de wijze waarop de gehanteerde veiligheidsaanpak tot uitvoering wordt gebracht, met aandacht voor de concrete doelstellingen en plannen inclusief de daaruit voortvloeiende preventieve en repressieve maatregelen;
   - een transparante, eenduidige en voor ieder toegankelijke verdeling van verantwoordelijkheden;
   - een duidelijke vastlegging van de vereiste personele inzet en deskundigheid voor de verschillende taken;
   - een duidelijke en actieve centrale coördinatie van veiligheidsactiviteiten.

4. Aanscherping veiligheidsaanpak:
   De veiligheidsaanpak dient continu aangescherpt te worden op basis van:
   - periodiek en in ieder geval bij iedere wijziging van uitgangspunten, uitvoeren van (risico)analyses, observaties, inspecties en audits (proactieve aanpak);
   - een systeem van monitoring en onderzoek van incidenten, bijna-ongevallen en ongevallen, alsmede een analyse daarvan (reactieve aanpak). Op basis hiervan worden evaluaties uitgevoerd en wordt eventueel de veiligheidsaanpak bijgesteld.
5. Sturing, betrokkenheid en communicatie:
   De leiding van de betrokken partijen/organisaties dient:
   - intern zorg te dragen voor duidelijke en realistische verwachtingen ten aanzien van de veiligheidsambitie, zorg te dragen voor een klimaat van continue verbetering van de veiligheid op de werkvloer door in ieder geval het goede voorbeeld te geven en voldoende mensen en middelen hiervoor beschikbaar te stellen;
   - extern duidelijk te communiceren over de algemene werkwijze, wijze van toetsing daarvan, procedures bij afwijkingen etc. op basis van heldere en vastgelegde afspraken met de omgeving.

A.5 Kwaliteitsbeheersing

SWOT-analyse - Om de kwaliteitsrisico's van het project te beheersen is een Strengths, Weaknesses, Opportunities & Threats (SWOT) analyse uitgevoerd. Op basis van deze analyse zijn specifieke maatregelen getroffen om bedreigingen te neutraliseren en kansen te benutten.

Tegendenksessies – op drie momenten gedurende het project hebben medewerkers van de Onderzoeksraad (buiten het onderzoeksteam) tussenproducten met "vreemde ogen" beoordeeld. De uitkomsten van deze tegendenksessies zijn gebruikt om de kwaliteit van het onderzoek te verbeteren.

Begeleidingscommissie - Het onderzoek werd besproken met een begeleidingscommissie. Zie onder kopje Begeleidingscommissie voor de concrete invulling hiervan.

Inzage - Een conceptversie van dit rapport is, conform de Rijkswet Onderzoeksraad voor veiligheid, voorgelegd aan de betrokken organisaties en personen met het verzoek het rapport te controleren op fouten, omissies en onjuistheden en het eventueel te voorzien van commentaar.

Analysemethoden – om de kans te verkleinen onjuiste of irrelevante conclusies te trekken, zijn analysemethodieken (zoals hierboven beschreven) gebruikt.

A.6 Begeleidingscommissie

De Onderzoeksraad heeft voor dit onderzoek een begeleidingscommissie samengesteld. Deze commissie bestaat uit externe leden met voor het onderzoek relevante deskundigheid onder voorzitterschap van een lid van de Onderzoeksraad. De externe leden hebben op persoonlijke titel zitting in de begeleidingscommissie. Gedurende het onderzoek is de commissie twee keer bijeengekomen om met het raadslid en het projectteam van gedachten te wisselen over de opzet en de resultaten van het onderzoek. Daarnaast heeft een schriftelijke consultatieronde plaatsgevonden om tussentijds feedback op te halen. De commissie vervult een adviserende rol binnen het onderzoek. De eindverantwoordelijkheid voor het rapport en de aanbevelingen ligt bij de Onderzoeksraad. De commissie is als volgt samengesteld:

Prof. Dr. Ir. M.B.A. van Asselt	Voorzitter begeleidingscommissie, Raadslid Onderzoeksraad voor Veiligheid.
Prof. Dr. M.H. Martens	Professor of ITS & Human Factors aan de UTwente van januari 2014 tot mei 2019. Sinds juni 2019 hoogleraar TU Eindhoven met als leerstoel Automated Vehicles & Human Interaction. Expert op het gebied van menselijke interactie met intelligente vervoerssystemen. Met een achtergrond in gedragswetenschappen, is zij gespecialiseerd in menselijke reacties op slimme mobiliteitsoplossingen voor in de auto en op de weg. Lid van de wetenschappelijke adviesraad van de SWOV. Zij werkt ook al meer dan 23 jaar bij TNO op dit gebied.
J.G. Hakkenberg MSc	Directeur van de Rijksdienst voor het Wegverkeer (RDW) van september 1995 tot oktober 2014. Hij heeft nu een eigen adviesbureau en zit in de adviesraad van ORMIT (ORMIT verbindt trainees aan organisaties) en BridgeHead (BridgeHead verbindt vragen van de overheid met oplossingen uit de markt). Hij was CFO bij het ministerie van Verkeer en Waterstaat van 1989 tot en met 1995.
Prof. Dr. M.J. van den Hoven	Professor of Ethics and Technology aan de TU Delft. Oprichter en wetenschappelijk directeur van 4TU Centre for Ethics and Technology (2007-2013). In 2009 won hij de World Technology Award voor ethiek en de IFIP-prijs voor ICT en samenleving voor zijn werk in ethiek en ICT. Oprichter en tot 2016 programmaleider van de Nederlandse Onderzoeksraad voor Verantwoorde Innovatie. Lid van het Blockchain Lab van de TU Delft.
Prof. Dr. A.W. Bronkhorst	Principal Scientist bij TNO Defensie en Veiligheid. Hij leidt een groot meerjarig programma over vroeg technologisch onderzoek op het domein van defensie en veiligheid. Dat loopt uiteen van biotechnologie, robotica, informatica, nanotechnologie tot cognitieve wetenschappen.
M.C. Stikker	Internetpionier en oprichter van De Digitale Stad. Directeur en oprichter van het culturele onderzoek- en ontwikkellab Waag, Technology & Society; een instituut dat technologische experimenten initieert. Lid van de Europese Horizon 2020 commissie 'High-level Expert Group for SRIA on innovating Cities' / DGResearch en van AcTI Nederlandse academie technologie & innovatie.
Ir. R.J. Prins	Cybersecurity expert en buitengewoon Raadslid van de Onderzoeksraad voor Veiligheid. Oprichter en eigenaar van Fox-IT (1999-2017). Hij is lid van de Adviesraad van de Kansspelautoriteit en van de Adviescommissie van Fintech & Innovatie (AFM).

A.7 Projectorganisatie

Namens de Onderzoeksraad is voor dit onderzoek prof. dr. ir. M.B.A. van Asselt opgetreden als portefeuillehouder. Het onderzoek is uitgevoerd door het projectteam, dat als volgt was samengesteld:

Dr. A. Umar	Onderzoeksmanager
Dr. ir. E.M Berends	Projectleider
Ir. M.A. van den Hoek	Onderzoeker en dataspecialist
F. van Leusden - Tamsma MSc	Digitaal onderzoeker
Drs. J.D. Romkes	Externe onderzoeker (specialist cybersecurity)
Dr. W.M.M. Heijnen	Senior onderzoeker
Drs. E. Mol	Adviseur onderzoek en ontwikkeling
Dr. E.M. de Croon	Adviseur methoden (CASCAD/STAMP)
Drs. M. Amelink	Extern onderzoeker
C. Dielen MSc	Extern onderzoeker
Mr. drs. D.C. Ipenburg	Secretaris
S. Sewnath	Projectassistent
J. Demir	Projectassistent

REACTIES CONCEPTRAPPORT

Een conceptversie (zonder beschouwing en aanbevelingen) van dit rapport is, conform de Rijkswet Onderzoeksraad voor veiligheid, voorgelegd aan betrokkenen ter beoordeling op feitelijke onjuistheden en onduidelijkheden.

Het conceptrapport is voorgelegd aan de volgende partijen:

- Minister van Infrastructuur en Waterstaat
- RDW
- Tesla, Inc.
- Volvo Trucks
- DAF Trucks N.V.

De ontvangen reacties zijn in de volgende twee categorieën te verdelen:

- Correcties van feitelijke onjuistheden, aanvullingen op detailniveau, en redactioneel commentaar heeft de Onderzoeksraad (voor zover juist en relevant) overgenomen. De betreffende tekstdelen zijn in het eindrapport aangepast. Deze reacties zijn niet afzonderlijk vermeld.
- De reacties die niet zijn overgenomen, zijn voorzien van een motivering van de Onderzoeksraad waarom deze niet zijn overgenomen. Deze reacties zijn opgenomen in een tabel die te vinden is op de website van de Onderzoeksraad voor Veiligheid (www.onderzoeksraad.nl).

ONGEVALLEN

C.1 Inleiding

Ongevallen met auto's uitgerust met ADAS waarbij het rijhulpsysteem mogelijk een rol heeft gespeeld bij de totstandkoming van het ongeval, zijn mede aanleiding geweest voor de Raad om een onderzoek te starten naar automatisering in het wegverkeer. Om te onderzoeken of en hoe ADAS inderdaad een rol kunnen spelen in het ontstaan van verkeersongevallen, heeft de Onderzoeksraad een aantal ongevallen onderzocht in de periode 2016 - 2019. Deze ongevallen worden samen met een aantal ongevallen in de VS die uitvoerig zijn onderzocht door de National Transportation Safety Board (NTSB) beschreven in deze bijlage.

C.2 Ongevallen in Nederland

In deze paragraaf presenteren we een aantal ongevallen die plaats hebben gevonden in Nederland in de periode 2016 – 2019. Bij elk van deze ongevallen was er betrokkenheid van een geavanceerd rijhulpsysteem (ADAS). Het onderzoek naar deze ongevallen is voor een groot deel gebaseerd op informatie verzameld door ongevalsanalisten van de politie. Merk op dat de ongevallen niet representatief zijn voor alle ongevallen met ADAS.

Ongeval	Omschrijving	Voorbeeld in paragraaf
1	Filestaart aanrijding met een vrachtwagen	3.1
2	Noodremsysteem van vrachtwagen voert noodremming uit	-
3	Botsing personenauto met invoegende vrachtwagen	3.1
4	Personenauto botst op langzaam rijdend verkeer	3.2
5	Personenauto rijdt rechtdoor over rotonde	3.2
6	Frontale botsing tussen twee personenauto's	3.3

Tabel 5: Onderzochte ongevallen.

C.2.1 Filestaart aanrijding met Volvo vrachtwagen

Op 27 maart 2017 vond een kop-staartbotsing plaats op de A29 nabij Den Bommel (Goeree-Overflakkee). Hierbij is een vrachtwagen, van het merk Volvo en uit het bouwjaar 2016, achterop een stilstaande vrachtwagen met dieplader gereden. De Volvo was voorzien van een in 2015 verplicht gesteld noodremsysteem, het zogenaamde *Advanced Emergency Braking System* (AEBS).[159] Bij dit ongeval zou AEBS in de Volvo ervoor gezorgd moeten hebben dat deze vrachtwagen tijdig zou remmen, maar dat gebeurde niet. Analyse van de tachograafgegevens heeft aangetoond dat de vrachtwagen ongeremd achterop de stilstaande vrachtwagen met dieplader is gebotst met 83 km/uur.

Automatic Emergency Braking System

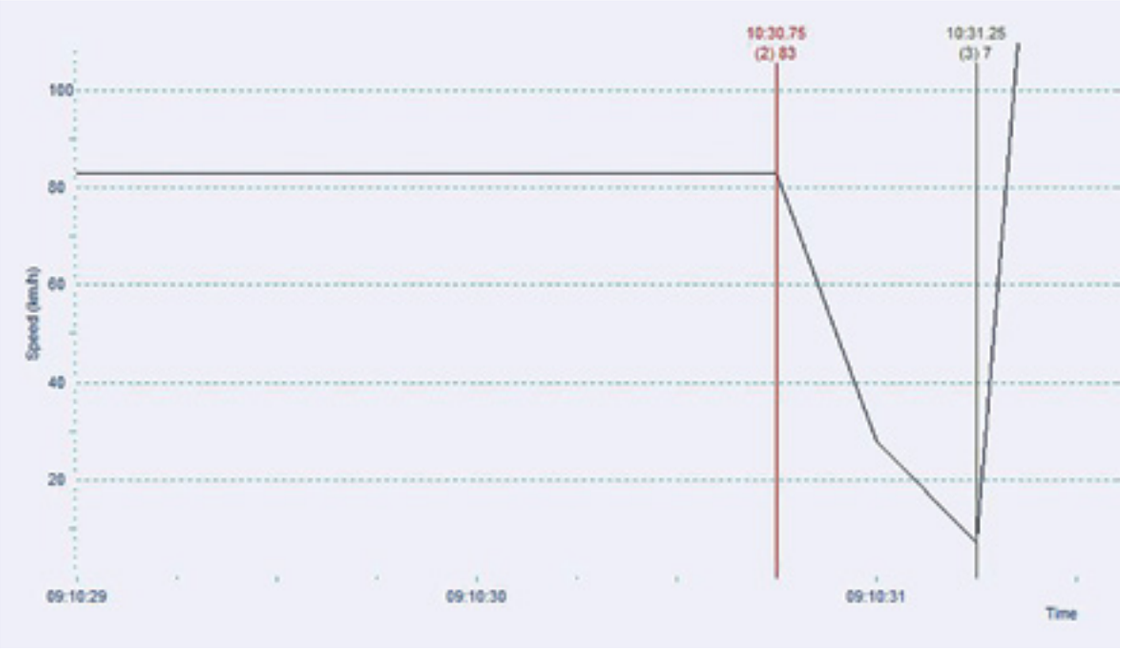
AEBS is bedoeld om bij een dreigende botsing automatisch te remmen. De sensoren van het systeem meten continu of er in een noodgeval voldoende afstand is om een aanrijding met de voorligger te voorkomen. Wanneer een kritieke limiet wordt overschreden, geeft het systeem een audiovisuele waarschuwing. Hierin zijn verschillende niveaus van waarschuwingen mogelijk. Als de chauffeur hier niet direct op reageert, treedt AEBS in werking. De vrachtwagen zal dan – met maximale remkracht – proberen zo veel als mogelijk te remmen om een aanrijding te voorkomen of de gevolgen ervan te beperken.

Figuur 17: Luchtfoto van het ongeval op de A29. De Volvo vrachtwagen (wit) is achterop een dieplader met bulldozer gebotst. (Bron: politie)

De bestuurder van de Volvo vrachtwagen is bij deze aanrijding om het leven gekomen en de schade was enorm. Op de overzichtsfoto, zie Figuur 17, is goed te zien dat de Volvo vrachtwagen (wit) bovenop de stilstaande dieplader met daarop een bulldozer is gereden. In eerste instantie is de cabine van de vrachtwagen in contact gekomen met de oplader. Als gevolg van de impact is vervolgens de laadbak van het chassis losgekomen en, vanaf de achterkant, tegen de cabine gebotst. Daarbij is de cabine van de vrachtwagen geplet tussen de laadbak en de bulldozer op de stilstaande dieplader.

159 Verordening (EU) No 347/2012 van de Commissie, 16 april 2012, tot de uitvoering van verordening (EG) 661/2009 van het Europees Parlement en de Raad betreffende typegoedkeuringsvoorschriften voor bepaalde categorieën motorvoertuigen wat geavanceerde noodsystemen betreft. Deze verplichting geldt alleen voor vrachtwagens geproduceerd na de ingangsdatum.

Onderzoek van de tachograafgegevens door de politie heeft aangetoond dat, gedurende een periode van 7 minuten en 12 seconden voorafgaand aan het ongeval, de vrachtwagen reed met een constante snelheid van 83 km/uur (zie Figuur 18). In een tijdsbestek van 0,50 sec. vertraagde de Volvo van 83 km/uur naar 7 km/uur. De chauffeur van de Volvo heeft niet geremd en is met volle snelheid achterop een stilstaande dieplader gereden bij daglicht en voldoende zicht. De Onderzoeksraad heeft niet kunnen vaststellen waarom de chauffeur niet remde.

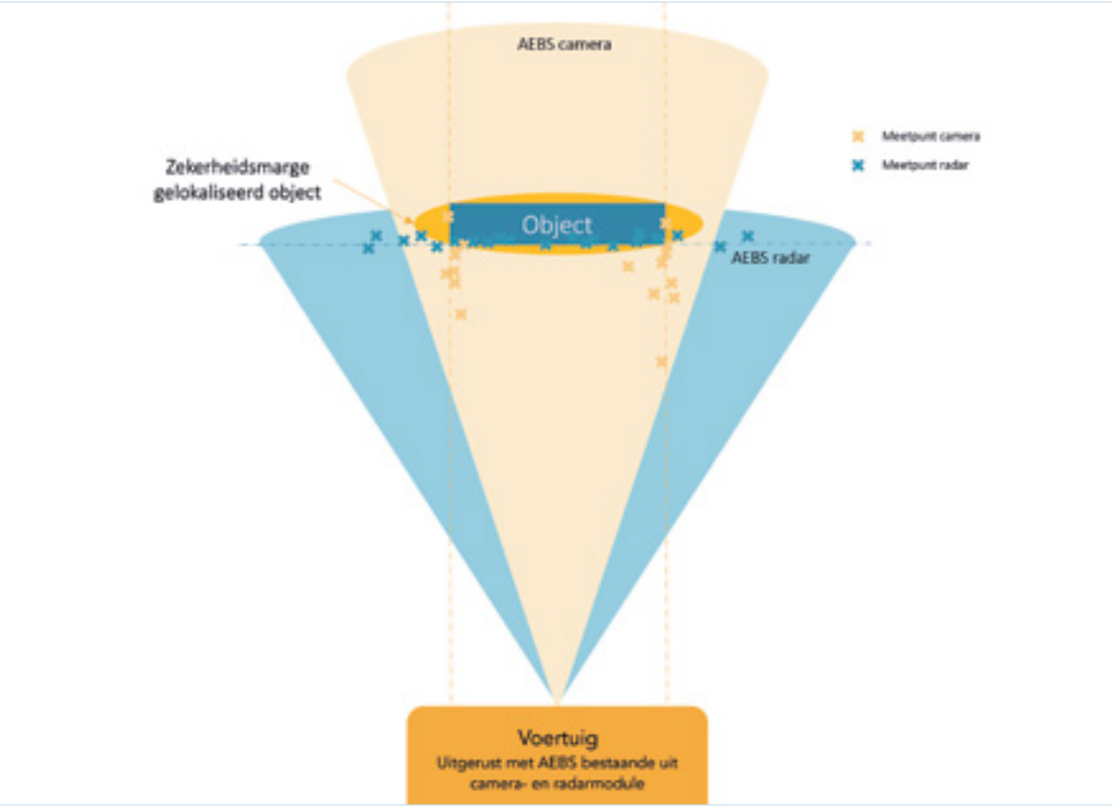


Figuur 18: Snelheidsregistratie afkomstig uit de tachograaf van de vrachtwagen. (Bron: Proces verbaal opgemaakt door de politie)

De werking van het AEB systeem is onderzocht, want een ingeschakeld en goed functionerend AEBS zou de noodremfunctie moeten hebben geactiveerd. Het zou echter ook zo kunnen zijn dat het AEBS – een verplicht gesteld systeem – uitgeschakeld was door de bestuurder. De Onderzoeksraad heeft niet kunnen vaststellen of de AEBS aanstond, omdat de wijze waarop de data worden opgeslagen in dit type vrachtwagen zo is ontworpen dat data alleen worden opgeslagen als de vrachtwagen op de normale wijze wordt uitgezet. Wanneer de stroom plotseling uitvalt, zoals bij dit ongeval, is het systeem niet in staat de data tijdig weg te schrijven naar het permanente geheugen.

Technici van Volvo hebben verklaard – op basis van kennis over de werking van het camerasysteem – dat het camerasysteem deze dieplader met lading hoogstwaarschijnlijk niet heeft herkend. Volvo koopt het camerasysteem in bij een toeleverancier en kent alleen de principes waarop voertuigen herkend worden die zich voor de vrachtwagen – waar het systeem is ingebouwd – bevinden. De huidige generatie camerasystemen detecteert bijvoorbeeld een voertuig door te kijken naar de plaatsing van de as en wielen van het voertuig met inachtneming van de vorm. Afwijkende vormen (zoals een dieplader met bulldozer, pijlwagen) zullen niet altijd worden gedetecteerd.

Locatiebepaling object door AEBS
In de regel is elk voertuig dat is voorzien van een AEB systeem uitgerust met een camera- en radarmodule. Door middel van *sensorfusie* – een techniek die de computer in staat stelt om informatie afkomstig van meerdere sensoren te combineren – bepaalt de computer de afstand van het voertuig tot het object. De radarmodule voorziet daarbij het systeem van nauwkeurigheid met betrekking tot de richting van het object. De cameramodule is nauwkeurig in het bepalen van de afstand tussen het voertuig en het object. In Figuur 19 is schematisch weergegeven hoe de waarnemingen van beide modules samen tot een locatiebepaling komen. Indien – na lokalisatie – het object zich binnen een vooraf gedefinieerde afstand (afhankelijk van de snelheid van het voertuig) bevindt, treedt een noodremming in werking.



Figuur 19: Detectie van een object in de rijrichting van een voertuig uitgerust met AEBS door middel van de camera- en radarmodule.

C.2.2 Noodremsysteem van vrachtwagen voert noodremming uit
Op 29 maart 2018 vond er een kop-staartaanrijding plaats tussen twee vrachtwagens, een bestelbus en een personenwagen, waarbij de achterste trekker-opleggercombinatie een DAF XF betrof uit bouwjaar 2018. Dit voertuig was – zoals regelgeving voor voertuigen met een brutomassa van meer dan 3,5 ton voorschrijft – voorzien van een automatisch noodremsysteem (AEBS).

Na een aanrijding tussen een personenwagen en een vrachtwagen (zie Figuur 20 (a)) – deze waren inmiddels tot stilstand gekomen op rijbaan 2 – waren een bestelbus (blauw) en de eerder genoemde DAF vrachtwagen achterop de stilstaande combinatie gebotst (zie Figuur 20 (b)). De chauffeur van de vrachtwagen heeft verklaard dat de bestelbus kort voor het ongeval voor hem op diens rijstrook had ingevoegd en dat de DAF vervolgens een noodremming heeft ingezet. Ondanks de zware schade aan de overige voertuigen is de achteropkomende DAF redelijk intact gebleven. Twee inzittenden van de andere voertuigen zijn met spoed naar het ziekenhuis gebracht.

De digitale tachograafgegevens zijn door de politie in beslag genomen en geanalyseerd. Hieruit kan echter niet worden opgemaakt of de bestuurder of het AEB systeem een remming heeft ingezet. De radarmodule is door de fabrikant en/of toeleverancier onderzocht. Dit onderzoek heeft aangetoond dat op tijdstip 12:12:27 het AEB systeem een ingreep heeft geïnitieerd. De truck reed op dat moment met een snelheid van 76 km/uur. Hierna werd ook het rempedaal bediend door de bestuurder van de truck. Ondanks dat de afstand om nog tot stilstand te komen – in combinatie met de snelheid van het voertuig – te klein was, heeft activatie van het noodremsysteem mogelijk erger voorkomen.

(a) In eerste instantie kwam de voorste vrachtwagen (ook DAF, kleur zilver) in botsing met de personenwagen (Seat, kleur zilver).

(b) De bestelbus (blauw) kwam vervolgens in botsing met de stilstaande vrachtwagen en werd geplet door de daarop volgende vrachtwagen (DAF, kleur wit).

Figuur 20: Twee DAF trucks, een personenwagen en een bestelbus betrokken bij een kop-staartbotsing. De DAF truck met de witte cabine was uitgerust met een AEB systeem. (Bron: Politie)

C.2.3 Botsing met invoegende vrachtwagen

Op 11 april 2017 is een Tesla Model S op de A1 bij Bathmen – een snelweg met dubbele rijstrook - achterop een vrachtwagen gebotst. De Tesla reed op de linker rijstrook met hoge snelheid; de Autopilot[160] functie was geactiveerd. De vrachtwagen reed op de rechter rijstrook. Kort voor de aanrijding wisselde de vrachtwagen van rijstrook, omdat er een andere vrachtwagen invoegde. Het remsysteem van de Tesla werd niet geactiveerd door het Autopilot systeem of de bestuurder. Wel lijkt het voertuig kort voor de impact gas terug te hebben genomen, hierdoor schoof de Tesla met een enigszins gereduceerde snelheid onder de vrachtwagen en werd een paar honderd meter meegesleurd. Er raakte niemand gewond bij dit ongeval.

160 Voor meer informatie over de functionaliteiten van de Autopilot, zie https://www.tesla.com/nl_NL/autopilot. Over het algemeen spreekt men van activatie van Autopilot als zowel Autosteer als TACC zijn geactiveerd. Die definitie wordt in deze bijlage aangehouden.

Figuur 21: Tesla Model S ongeremd achterop van baan wisselende vrachtwagen gereden met een snelheid van ongeveer 127 km/uur.

In Figuur 22 a tot en met f is een tijdreeksregistratie van een aantal parameters afkomstig van de Tesla logbestanden weergegeven. Zoals af te leiden uit Figuur 22 a en b reed het voertuig vlak voor het ongeval (07:43:00) met een snelheid van ongeveer 150 km/uur; de Autopilotfunctie was daarbij geactiveerd (TACC[161] en Autosteer[162]; de gerapporteerde toestand was *active nominal*). De cruisesnelheid was al geruime tijd ingesteld op 145 km/uur en werd vlak voor het ongeval (07:43:17) door de bestuurder verhoogd naar 150 km/uur (Figuur 22 e).

Om 07:43:43 – kort nadat de vrachtwagen naar de linker rijstrook was gewisseld en voor de Tesla invoegde – kwam de Tesla in aanraking met de vrachtwagen. Tot het moment van impact was het Autopilot systeem geactiveerd. Wel was de snelheid van de Tesla al enigszins teruggelopen naar ongeveer 130 km/uur. Dit is volgens Tesla het gevolg van het terugnemen van het gaspedaal en een initiële afremming door het TACC systeem omdat deze een voorganger detecteerde. Met een snelheid van 127 km/uur schoof de Tesla onder de vrachtwagen. Ogenblikkelijk werd het remsysteem geactiveerd door de bestuurder (zie Figuur 22 d) – hiermee werd ook het Autopilot systeem gedeactiveerd. Na de impact kwam de Tesla onder de vrachtwagen vast te zitten en werd enkele honderden meters meegesleurd. Om 07:44:00 kwamen beide voertuigen tot stilstand.

Ten tijde van de aanrijding rapporteerde het Autopilot systeem "*hands required and detected*" – de bestuurder lijkt zijn handen aan het stuur te hebben gehad. Aan instellingen op het display van de Tesla valt af te leiden dat het FCW en AEB systeem waarschijnlijk aan hebben gestaan. Echter, AEBS is pas in een latere softwareversie (2.5)

161 Benaming van Tesla voor hun variant van adaptive cruisecontrol.
162 Autosteer is een actieve vorm van lane keeping assist en regelt de plaats van de auto op de weg.

geactiveerd voor hoge snelheden (van 50 – 90 mijl/uur of 80 – 145 km/uur) en het voertuig lijkt dus met een impactsnelheid van 127 km/uur buiten het operationele domein van het voertuigspecifieke AEBS te zijn.

ACC systemen kunnen moeite hebben met anticiperen op rijstrookwisselingen. Volgens Tesla heeft het TACC systeem wel een voorganger gedetecteerd en ook een initiële afremming ingezet. Waarom het systeem niet heeft geprobeerd meer/krachtiger af te remmen is onduidelijk. Zowel de initiële remming door Autopilot alsook het activeren van het noodrem- en waarschuwingssysteem werkten zoals ontworpen

De datastructuur van de Tesla in kwestie wijkt af van de datastructuur bij eerdere onderzochte Tesla voertuigen. Een aantal parameters is niet opgenomen in de log-bestanden of is van locatie verwisseld (o.a. afstand tot voorganger, snelheid voorganger, uitslag gaspedaal). Zoals eerder vermeld is het mogelijk om de manier waarop data opgeslagen worden door een over-the-air software-update te veranderen.

Door een software-update zijn op eenvoudige wijze wijzigingen aan te brengen in het functioneren van systemen die controle uitvoeren over het systeem. Zo is in softwareversie 2.0 de snelheidslimiet van TACC gewijzigd en in 2.5 een noodremfunctie toegevoegd die werkt bij snelheden boven de 80 km/uur (tot 145 km/uur).[163, 164] Deze software-updates – en daarmee ook het toevoegen of veranderen van functionaliteiten – gebeuren als het voertuig voor langere tijd stil staat. In een Tesla heeft de bestuurder de keuze om te bepalen wanneer en waar updates geïnstalleerd worden. Na de installatie ontvangt de bestuurder een overzicht van wijzigingen aan het systeem op het dashboard waarin alle wijzigingen in de functionaliteit of mogelijkheden van de systemen op het voertuig worden beschreven. Ook is het mogelijk voor de bestuurder om een notificatie te ontvangen op de mobiele telefoon, zodat de bestuurder weet wanneer een update heeft plaatsgevonden.

163 Electrek.co, *Tesla increases Autopilot 2.0 speed limits with latest update*, https://electrek.co/2017/03/08/tesla-autopilot-2-0-speed-limit-update/, geraadpleegd op 21 mei 2018.

164 Electrek.co, *Tesla releases new update to enable full speed automatic emergency braking for Autopilot 2.5 and more*, https://electrek.co/2017/10/22/tesla-update-full-speed-automatic-emergency-braking-autopilot-2-5/, geraadpleegd op 7 augustus 2018.

(a) snelheid van het voertuig

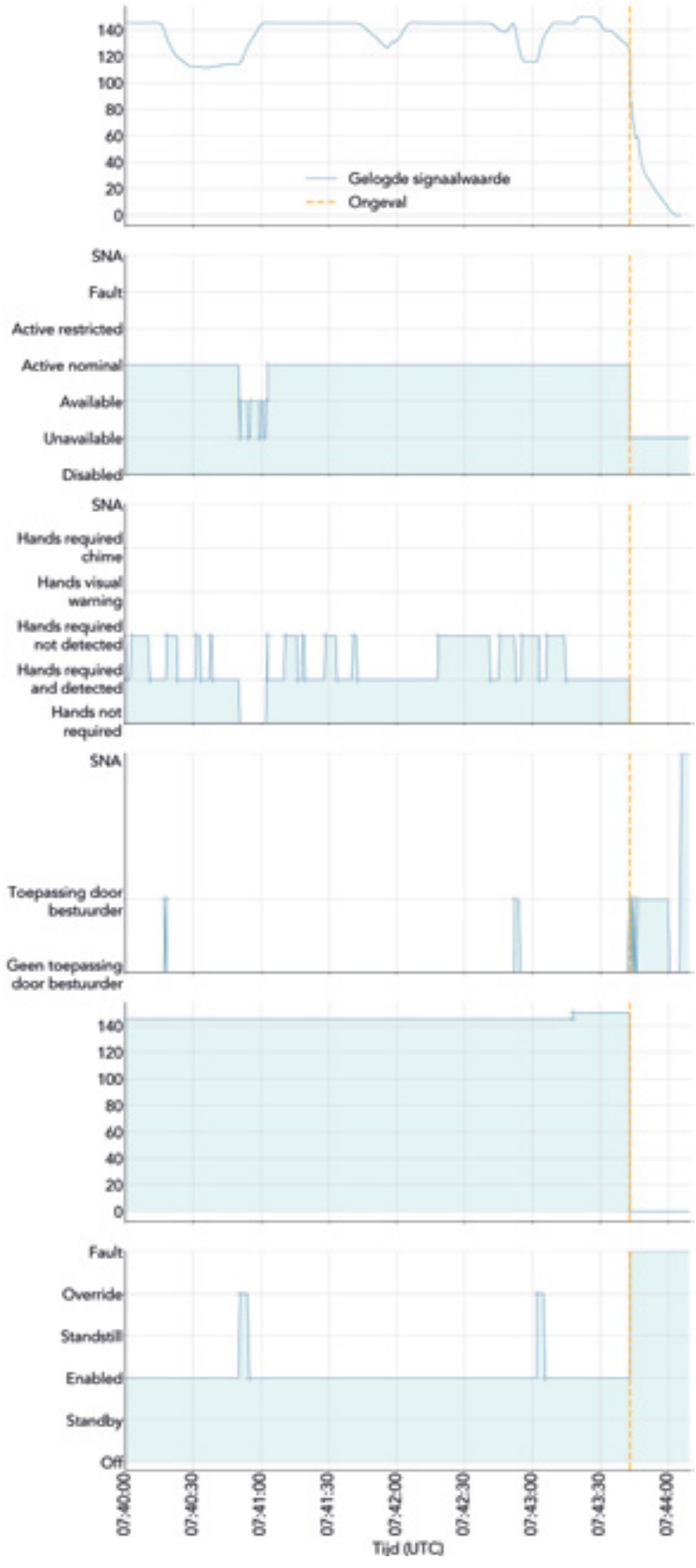
(b) Toestand van het Autopilot systeem

(c) Autopilot hands on toestand

(d) Toepassing van remming door bestuurder

(e) Ingestelde snelheid TACC systeem

(f) Toestand TACC systeem



Figuur 22: Tijdreeksregistratie van een aantal parameters afkomstig van de logbestanden uit het voertuig (Tesla Model S, Bathmen).

C.2.4 Personenauto met Autopilot botst op langzaam rijdend verkeer

Op 25 augustus 2016 vond er een kettingbotsing plaats op de A4 bij Leiden, waarbij zes personenauto's betrokken waren. Vijf van de betrokken auto's waren gestopt voor een file. Een Tesla Model S reed tegen deze vijf auto's. De Tesla was uitgerust met het Autopilot systeem. Ten tijde van het voorval was dit systeem geactiveerd.

Figuur 23: Tesla Model S met een snelheid van 58 km/u op zijn voorganger gebotst (Bron: 112regioleiden.nl).

Als gevolg van de botsing tussen de Tesla en zijn voorganger ontstonden er meerdere kop-staartbotsingen tussen de overige vijf auto's. Geen van de betrokkenen heeft letsel opgelopen.

De matrixborden gaven '50' aan en het was duidelijk dat het langzaam rijdend verkeer was. De bestuurder had gemerkt dat het systeem die middag meerdere malen correct tot lage snelheid had afgeremd. Analyse van Tesla toont aan dat het Autopilot systeem en het TACC systeem (Figuur 24 b en g) dat gedurende 20 minuten voorafgaand aan de botsing de snelheid van de auto verkeersafhankelijk werd geregeld door TACC en dat ongeveer vijf minuten voor de botsing de bestuurder audiovisueel werd gewaarschuwd door het Forward Collision Warning System (FCW systeem)[165] voor een mogelijke botsing met een (andere) voorligger. Direct daaropvolgend werd een remming ingezet door de bestuurder en werd het Autopilot systeem gedeactiveerd (zie Figuur 24 d; 13:12:09). Hierna heeft hij het Autopilot systeem weer geactiveerd. De bestuurder vertrouwde op de Autopilot functie van de Tesla. Autopilot was geactiveerd en de TACC-snelheid stond ingesteld op 130 km/uur en de kortste volgafstand was ingesteld. Dit vertrouwen werd versterkt doordat het *Forward Collision Warning* systeem hem kort voor het ongeval nog een keer tijdig gewaarschuwd had.

165 Alle Tesla's zijn uitgerust met een Forward Collision Warning systeem. Dit systeem staat los van het Autopilot systeem en waarschuwt de bestuurder – zowel auditief als visueel – in het geval van een naderende botsing. Er zijn verschillende waarschuwingsniveaus (bijvoorbeeld eerst een visuele waarschuwing, daarna een geluidswaarschuwing). Het FCW heeft alleen de mogelijkheid om te waarschuwen en kan niet het remsysteem aansturen.

Uit de parameters afkomstig van de logbestanden van het voertuig (Figuur 24) valt af te leiden dat het voertuig vlak voor het moment van impact (13:17:07) reed met een snelheid van ongeveer 67 km/uur. Op 0,5 tot 1,5 seconde voor het bereiken van de file – op een afstand van om en nabij 18 meter van zijn voorganger – begon de bestuurder van de Tesla met remmen (13:17:10). Dit was onvoldoende om het voertuig op tijd tot stilstand te brengen. De Tesla botste op zijn voorganger met ongeveer 58 km/uur. De bestuurder zette 0,5 tot 1,5 seconde na het begin van de remming van zijn voorganger zelf een remming in. Wanneer alleen de remweg van de voorganger meegenomen wordt, kan gesteld worden dat dit duidt op een alerte reactie van de bestuurder. Een bestuurder wordt echter geacht om veel verder vooruit te kijken dan alleen de voorgaande auto. Uit het onderzoek blijkt dat het aannemelijk is dat de bestuurder deze informatie gemist heeft door de lage taakbelasting.

Uit Figuur 24 b valt af te leiden dat ten tijde van het voorval het Autopilot geactiveerd was in de modus *active nominal* – Autopilot maakt in deze modus gebruik van Autosteer en TACC. Dit wordt bevestigd door de toestand van het snelheidsregelsysteem, deze was *enabled* en stond ingesteld op een snelheid van 130 km/uur (zie Figuur 24 f en g). Verder blijkt uit de hands-on toestand parameter dat het systeem gedurende een periode van ongeveer vijf minuten – tijdens deze periode was Autopilot geactiveerd – geen handen aan het stuur heeft gedetecteerd (zie Figuur 24 b en c). Er is geen FCW waarschuwing afgegeven.

Ondanks dat het Autopilot systeem geactiveerd was, heeft het systeem geen actie ondernomen om afstand tot zijn voorganger te houden. Ongeveer één seconde voor het in contact komen met zijn voorganger heeft de bestuurder van de Tesla het rempedaal bediend. Zeer korte tijd hiervoor remde het voertuig regeneratief af; dit is een lichte remming om kinetische energie terug te geleiden naar de batterij en staat verder los van de noodremming.

Verder blijkt uit de *hands-on* toestand dat het systeem gedurende een periode van ongeveer vijf minuten – tijdens deze periode was Autopilot geactiveerd – geen handen aan het stuur heeft gedetecteerd. Er is geen waarschuwing afgegeven.

(a) snelheid van het voertuig

(b) Toestand van het Autopilot systeem

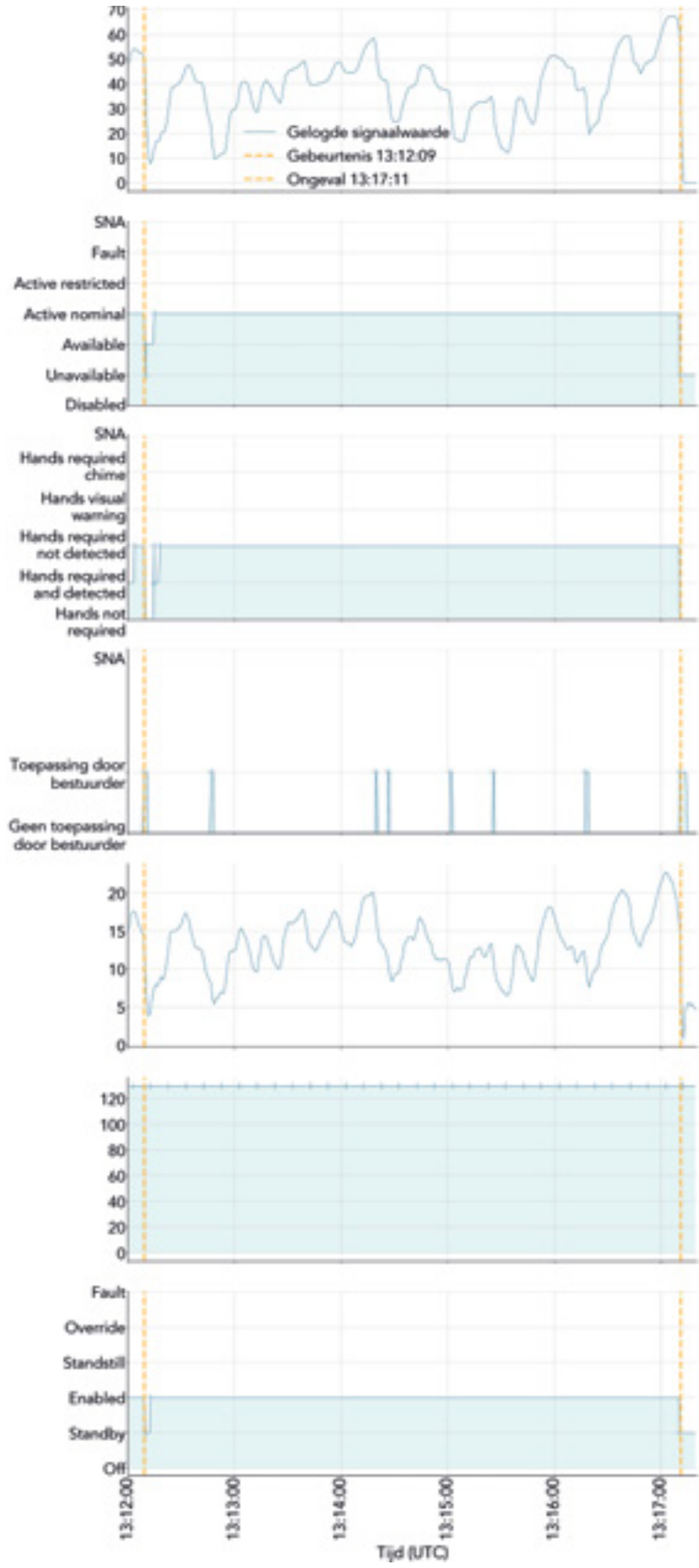
(c) Autopilot hands on toestand

(d) Toepassing van remming door bestuurder

(e) Gemeten afstand van voertuig tot voorganger

(f) Ingestelde snelheid TACC systeem

(g) Toestand TACC systeem



Figuur 24: Tijdreeksregistratie van een aantal parameters afkomstig van de logbestanden uit het voertuig (Tesla Model S, Leiden).

Data zijn op een bedrijfseigen manier weggeschreven: alleen de fabrikant heeft de exacte sleutel om de data te ontcijferen. Inspanningen van diverse instanties hebben geleid tot het ontcijferen van een klein gedeelte van de parameters. Echter, bij een software-update[166] kan de sleutel weer veranderen. De hoeveelheid werk voor het achterhalen van de datastructuur en de diversiteit aan manieren waarop data zijn weggeschreven maken het onmogelijk voor derde partijen om eenvoudig inzicht in de data te krijgen.

C.2.5 Personenauto rijdt rechtdoor over rotonde

Op 1 juli 2016, vroeg in de middag, is een Tesla Model S met hoge snelheid recht over het middeneiland van een rotonde gereden op de N57. Aan de andere kant van de rotonde is de Tesla tegen een paal gebotst en daarbij tot stilstand gekomen. De bestuurder heeft bij het ongeval zware verwondingen opgelopen. Ten tijde van het ongeval was het rustig op de N57; er reed geen voertuig voor de Tesla.

Figuur 25: Tesla Model S nadat deze tot stilstand is gekomen tegen een paal aan de andere kant van de rotonde. (Bron: Twitter, geplaatst door weginspecteur Jeroen van Rijkswaterstaat)

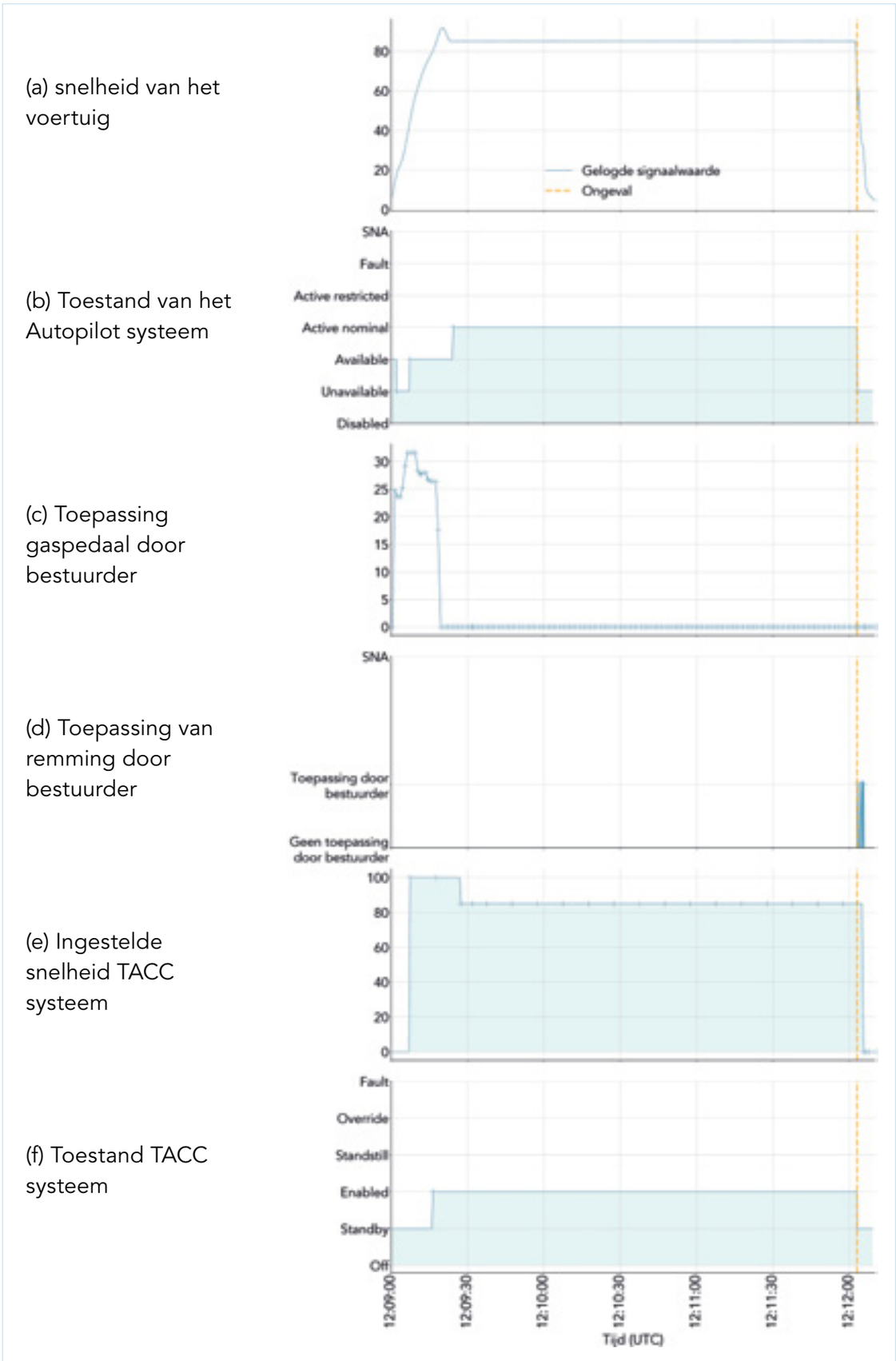
Tijdreeksregistraties van een aantal parameters afkomstig van de logbestanden van het voertuig zijn weergegeven in Figuur 26. Uit deze informatie bleek dat het voertuig bij het naderen van de rotonde met een constante snelheid van ongeveer 84 km/uur reed. Het voertuig had deze snelheid al gedurende een periode van ongeveer 3 minuten. Om 12:12:03 nam de snelheid in ongeveer 3 seconden af naar 10 km/uur waarna het voertuig na nog eens 3 seconden tot stilstand kwam.

166 Tesla krijgt regelmatig software-updates over-the-air (via het mobiele netwerk).

Het Autopilot systeem rapporteerde "*Active Nominal*" als toestand: het Autopilot was geactiveerd voorafgaand aan het ongeval. Uit Figuur 26 e en f valt af te leiden dat de toestand van TACC normaal was en het systeem ingesteld was op een cruise snelheid van 85 km/uur. Ook aan de hand van Figuur 26 c is te zien dat het Autopilot systeem aan heeft gestaan; de bestuurder heeft in een periode van ongeveer 3 minuten voorafgaand aan het ongeval het gaspedaal niet bediend. Het rempedaal (Figuur 26 d) werd in die periode ook niet bediend. Na het oprijden van het middeneiland van de rotonde – nog voordat het voertuig tot stilstand kwam – heeft de bestuurder nog wel geprobeerd om het voertuig af te remmen.

Tijdens het naderen van de rotonde heeft het FCW niet gewaarschuwd, ook heeft het noodremsysteem niet ingegrepen (loggegevens). Ook de bestuurder verklaart dat hij geen waarschuwing van het systeem heeft ontvangen. Het is mogelijk om Autosteer te gebruiken op wegen waarvoor het eigenlijk niet ontworpen is.

De bestuurder heeft verklaard de meeste informatie over het functioneren van Autopilot uit de handleiding te hebben gehaald. Ook heeft hij bij het in gebruik nemen van zijn auto een korte uitleg gehad over de systemen in het voertuig.



Figuur 26: Tijdreeksregistratie van een aantal parameters afkomstig van de logbestanden uit het voertuig (Tesla Model S, Ouddorp).

C.2.6 Frontale botsing tussen twee personenauto's

Op 30 januari 2019 reed een Tesla Model S op de N277, een provinciale weg in de buurt van Zeeland (Noord-Brabant). Het voertuig was uitgerust met Autopilot en een noodremsysteem.

Om Autopilot te activeren moet de bestuurder achtereenvolgens *traffic aware cruise control* (TACC) en Autosteer inschakelen. Dit gaat door middel van een schakelpookje aan de linker achterzijde van het stuur. Autosteer werkt alleen op wegen waar duidelijke belijning door het systeem gedetecteerd kan worden. Als Autosteer beschikbaar is wordt een grijs icoon weergegeven op het dashboard. Na activatie door middel van het schakelpookje is een blauw icoon te zien naast de snelheid (zie Figuur 27).

Besturing Tesla Autopilot

Het activeren van Tesla Autopilot werkt door middel van een schakelpookje aan de linker achterzijde van het stuur. Autopilot bestaat uit een combinatie van TACC en Autosteer. TACC kan op twee manieren ingeschakeld worden. Door het naar boven of onderen bewegen van het schakelpookje wordt de momentane snelheid ingesteld. Bij het naar de bestuurder toe bewegen van de schakelaar wordt de de snelheidslimiet of de huidige snelheid aangehouden. TACC kan alleen worden ingeschakeld als het systeem beschikbaar is, te zien aan het grijze snelheidsmeterpictogram op het instrumentenpaneel.

Indien Autosteer beschikbaar is – het display laat dan een grijs Autosteer-pictogram zien – kan dit geactiveerd worden door het schakelpookje nogmaals naar de bestuurder toe te bewegen. Dit moet gebeuren kort na het activeren van TACC. Na het activeren van Autosteer krijgt de bestuurder een geluidssignaal te horen en wordt het Autosteer-pictogram blauw. Het meermaals omhoog of omlaag bewegen van het pookje zorgt ervoor dat de ingestelde snelheid van TACC aangepast wordt – Autosteer wordt dan niet geactiveerd.

Figuur 27: (a) Als Autopilot beschikbaar is wordt op het instrumentenpaneel een grijs Autosteer-icoon weergegeven, (b) na het activeren wordt het icoon blauw. (Bron: Tesla Model S gebruikershandleiding[167])

Figuur 28: (a) foto genomen door de camera in de Tesla vlak voor de aanrijding, (b) de restanten van beide voertuigen na de aanrijding (Bron: Politie).

Gegevens afkomstig uit het voertuig (zie tijdreeksregistraties in Figuur 29 a tot en met f) hebben aangetoond dat het voertuig reed met een snelheid van ongeveer 83 km/uur met TACC geactiveerd. Autosteer was niet actief. Circa 23 seconden voor het moment van impact beweegt de bestuurder twee keer snel na elkaar het schakelpookje van het Autopilot systeem omhoog. Bij de eerste keer omhoog bewegen wordt de TACC snelheid ingesteld op de momentane snelheid. Bij de tweede keer wordt de ingestelde snelheid verhoogd naar 85 km/uur. Autosteer werd niet ingeschakeld. Uit een verklaring van de bestuurder is gebleken dat hij dacht dat Autopilot, en daarmee TACC en Autosteer – door hem waren geactiveerd. De activatie van TACC en daarbij een verhoging van de snelheid (twee keer het pookje omhoog bewegen) lijkt erg op het activeren van TACC en Autosteer (twee keer naar de bestuurder toe bewegen). Mogelijk dacht de bestuurder dat hij Autosteer had geactiveerd.

167 Tesla, *Tesla Model S gebruikershandleiding*, 2018.

Toen de bestuurder zijn aandacht kort op het scherm in de middenconsole richtte, merkte de bestuurder dat het voertuig op een andere rijstrook terechtkwam en een tegenligger naderde. De Tesla kwam in botsing met de tegenliggende Nissan. Gegevens laten zien dat de bestuurder zijn handen toen voor een periode van ongeveer 9 seconden niet aan het stuur heeft gehad – het systeem waarschuwde ook niet omdat Autosteer niet geactiveerd was.[168] Als gevolg van de botsing kwam de bestuurder van de Nissan om het leven; de bestuurder van de Tesla kwam met de schrik vrij. Er heeft geen activatie van het AEBS plaatsgevonden, ook was er geen FCW waarschuwing. De huidige generatie van dergelijke systemen is niet gemaakt om naderende botsingen met tegenliggers te detecteren.

168 In het geval Autopilot wel ingeschakeld was, had het systeem bij een snelheid van 83 km/uur elke 40 seconden een hands-on detectie uitgevoerd. Variabelen die onmiddellijk aanleiding geven tot een waarschuwing zijn onder meer: geen geldige rijstrooklijnen gedetecteerd, ongebruikelijke rijstrooklijnen, een mogelijk dreigende botsing met een object in de rijrichting.

(a) snelheid van het voertuig

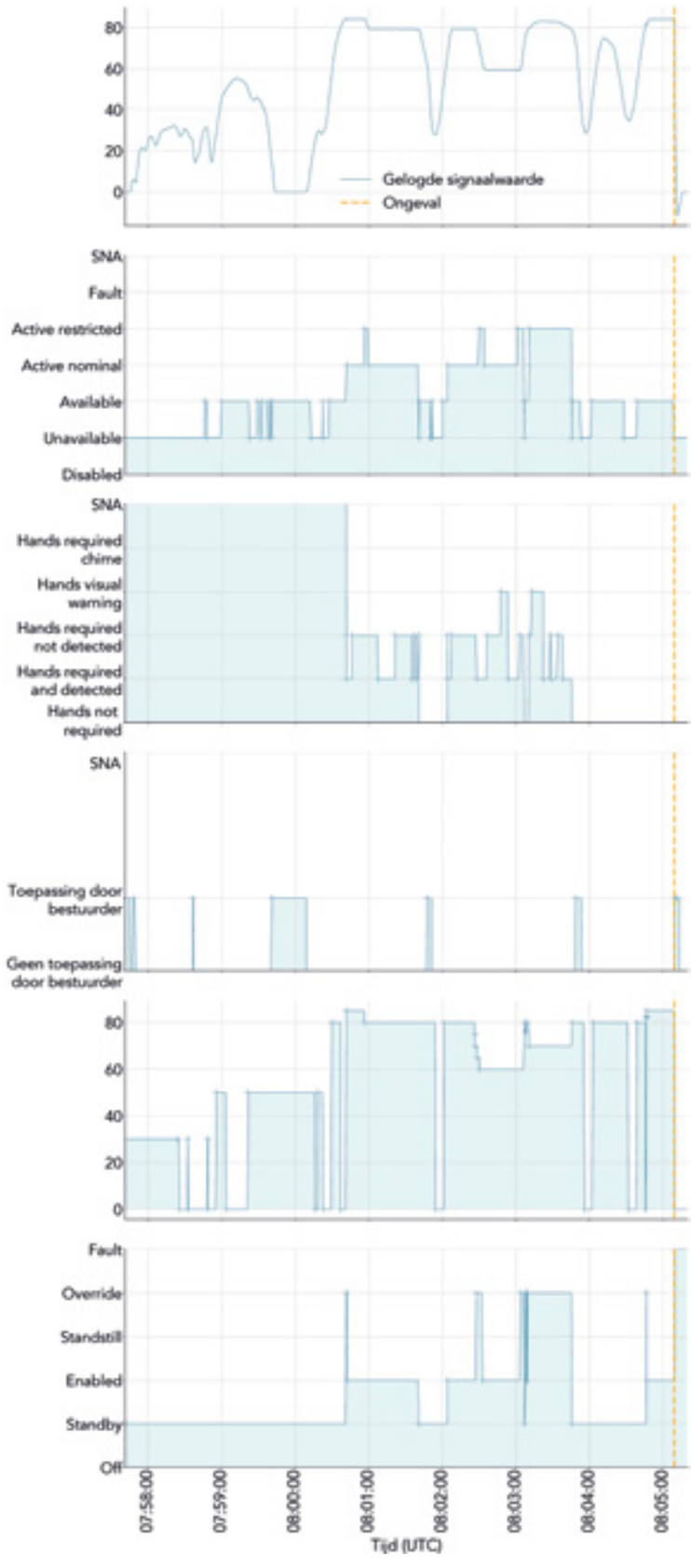
(b) Toestand van het Autopilot systeem

(c) Autopilot hands on toestand

(d) Toepassing van remming door bestuurder

(e) Ingestelde snelheid TACC systeem

(f) Toestand TACC systeem



Figuur 29: Tijdreeksregistratie van een aantal parameters afkomstig van de logbestanden uit het voertuig (Tesla Model S, Zeeland).

C.2.7 Aanrijdingen met een personenauto waarbij ADAS geen rol speelden

De Onderzoeksraad heeft verscheidene ongevallen met personenauto's onderzocht. Echter, bij een groot deel van die ongevallen speelde ADAS geen rol omdat deze systemen uitgeschakeld waren. Hieronder een overzicht van deze onderzochte ongevallen.

15 maart 2015	Woonwijk in Wormerveer De bestuurder wilde wegrijden uit een parkeervak toen de Tesla opeens vooruit schoot en daarbij een paar paaltjes ramde en een fietser raakte. De bestuurder had de indruk dat de Tesla op hol sloeg. Onderzoek wees uit dat de bestuurder het gaspedaal ingedrukt hield. Het betrof dus een bedieningsfout. Daarbij moet wel aangemerkt worden dat een Tesla veel meer vermogen heeft dan de gemiddelde benzine- of dieselauto.
7 september 2016	Provinciale weg in Baarn Tesla met hoge snelheid frontaal tegen boom. Bestuurder op slag dood. Deel accupakket losgeraakt en na enige tijd spontaan in brand gevlogen. Bestuurder pas na meerdere uren door brandweer geborgen. Volgens Tesla was de botssnelheid ca. 155 km/uur en (dus) was Autopilot niet in bedrijf[169].
20 juli 2017	A35 bij Hengelo Tesla X achterop een file gereden. Hij botste met circa 130 km/uur en zonder te remmen tegen de achterzijde van een Mercedes. De Mercedes werd met kracht vooruit geduwd waardoor deze tegen de achterzijde van een Volvo botste, die ook vooruit werd geduwd. Daardoor botste de Volvo tegen een Volkswagen. Autopilot stond niet aan. De mogelijke rol van mens-machine interactie bij de totstandkoming van dit ongeval (bijvoorbeeld de bestuurder dacht dat de systemen aanstonden en vertrouwde er op) is niet verder onderzocht.
27 februari 2019	Provinciale weg bij Vogelenzang Een Jaguar I-Pace, uitgerust met o.a. adaptive cruisecontrol, lane keeping assist en een noodremsysteem, botste op een BMW die in zuidelijke richting reed en af wilde slaan om een inrit in te gaan. EDR gegevens hebben aangetoond dat de Jaguar reed met een gemiddelde snelheid van 120 km/uur, een ernstige overschrijding van de geldende maximumsnelheid (50 km/uur). Dergelijke snelheden liggen buiten het operationele domein van het noodremsysteem. Detectie van voertuigen werkt met deze versie van het noodremsysteem tot 80 km/uur. Bovendien is het met deze versie niet mogelijk tegenliggers te detecteren.

169 Pas in een latere softwareversie is de snelheidslimiet voor Autopilot omhoog gegaan naar 145 km/uur.

C.3 Ongevallen in de VS

C.3.1 Tesla botst op afslaande vrachtwagen, Florida, USA

Op 7 mei 2016 botste een Tesla S tegen de zijkant van de oplegger van een vrachtwagen combinatie bestaande uit een trekker met oplegger. Dit ongeval is uitgebreid onderzocht door de NTSB.[170]

De Tesla reed op US Highway 27A met 120 km/uur, terwijl de vrachtwagen die uit de tegenovergestelde richting als de Tesla kwam linksaf sloeg naar een onverharde zijstraat. De Tesla raakte de rechterkant van de oplegger, ging onder de oplegger door en raakte vervolgens van de weg. Bij de botsing met de onderkant van de oplegger scheurde het dak van de auto. De bestuurder van de Tesla overleed bij het ongeval.

Figuur 30: Tesla Model S na de botsing met de vrachtwagen. (Bron: Florida Highway Patrol)

Bevindingen:

- De zichtafstand was voldoende voor zowel de vrachtwagenchauffeur als de automobilist om tijdig te reageren en het ongeval te voorkomen. Het is niet duidelijk geworden waarom ze niet alert waren.
- Waarschijnlijk overschatte de bestuurder van de Tesla de betrouwbaarheid van de automatisering en begreep hij de beperkingen van de systemen niet.
- Beperkingen van het systeem. Uit gegevens uit de Tesla bleek ook dat Autopilot 11 km voor de botsing ingeschakeld was. Deze niveau 2 automatiseringstechnologie kan kruisend verkeer niet betrouwbaar identificeren om er op te reageren.
- Beperkingen van het systeem. De auto was uitgerust met een automatisch noodremsysteem (AEBS), dat is ontworpen om automatisch de remmen aan te zetten om de ernst van de impact te verminderen of te helpen bij het voorkomen van frontale en kop-staart botsingen. Het systeem is niet ontworpen om kruisende voertuigen te detecteren.

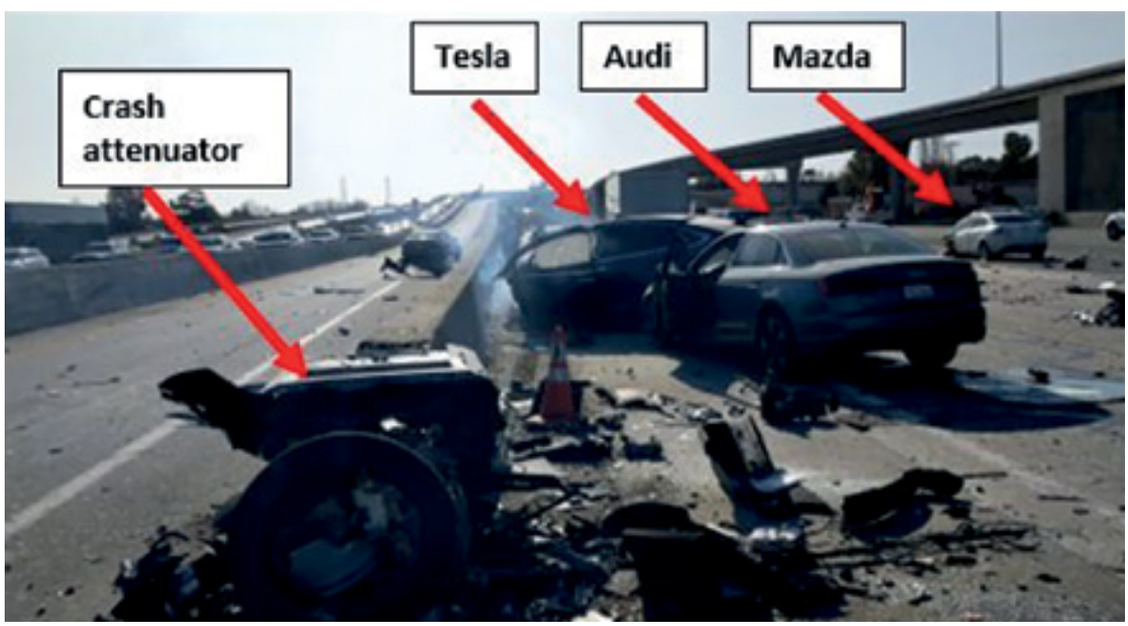
170 NTSB, *Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck*, Highway Accident Report, 2017.

C.3.2 Tesla botst op middenbarrière, Californië, USA

Op 23 maart 2018 botste een Tesla X op een middenbarrière tussen de hoofdrijbaan en de afslag. Dit ongeval wordt momenteel onderzocht door de NTSB.[171]

De bestuurder had de Autopilotfuncties ingeschakeld toen hij de afslag naar US Highway 85 naderde. Dit is een afslag naar links. De Tesla begon naar links te sturen toen de bestuurder het verdrijvingsvlak naderde. Vervolgens botste de Tesla op de middenbarrière waarvan de botsabsorber[172] ontbrak door een eerdere botsing. De Tesla tolde om zijn as en raakte daarbij twee andere voertuigen. Vervolgens vloog de Tesla in brand waarbij de bestuurder dodelijk gewond raakte. De bestuurder van een van de twee andere auto's raakte lichtgewond.

(a) Plaats van het ongeval.



(b) Overblijfselen van diverse voertuigen waaronder de Tesla.

171 NTSB, *Preliminary Report: Highway HWY18FH011*, 2018.
172 Ook rimpelbuisobstakelbeveiliging genoemd.

(c) Botsabsorber in normale situatie en een dag voor de fatale crash.

Figuur 31: Crash van Tesla Model X met middenbarrière op snelweg. (Bron: NTSB rapport)

Bevindingen:

- De bestuurder van de Tesla remde niet en stuurde niet bij.
- 6 Seconden voor de botsing had de bestuurder voor het laatst zijn handen aan het stuur.
- 3 Seconden voor de botsing versnelde de Tesla van 100 km/uur naar 114 km/uur. De auto remde niet voor de botsing en week niet uit voor de barrière.
- Beperkingen van het systeem: waarschijnlijk heeft Autopilot moeite gehad met het herkennen en volgen van de belijning op de weg. Het Autopilot systeem heeft een verminderd situationeel bewustzijn in vergelijking met de menselijke bestuurder.
- De bestuurder had eerder al geklaagd bij de dealer dat de auto in de Autopilot op dit punt op de snelweg uitweek naar links.[173] Toch was hij niet alert en greep hij niet in.
- Een andere Tesla met de Autopilotfunctie ingeschakeld heeft kort na het incident een video gemaakt waarop het lijkt dat ook zijn Tesla uitwijkt naar links op het bewuste punt.[174] Er is nog een video van een Tesla die met de Autopilot ingeschakeld recht op een middenbarrière inrijdt.[175]

C.3.3 Uber zelfrijdende auto rijdt voetganger aan, Arizona, USA

Op 18 maart 2018 botste een Uber testvoertuig in het donker op een overstekende voetganger. Het Uber voertuig, een aangepaste Volvo V90 uitgerust met een geïntegreerd zelfrijdend systeem (testversie richting SAE level 3) bestaande uit aantal sensoren en computerunits, reed in de zelfrijdende modus over een doorgaande weg met middenberm met circa 70 km/uur. In het Uber testvoertuig zat een operator die als taken had het zelfrijdende systeem en verkeer te monitoren, en indien nodig in te grijpen. De voetganger met een fiets aan de hand stak over vanaf de begroeide middenberm. De voetganger overleed bij dit ongeval.

173 Abc7news, *I-TEAM EXCLUSIVE: Victim who dies in Tesla crash had complained about Autopilot*, http://abc7news.com/automotive/i-team-exclusive-victim-who-died-in-tesla-crash-had-complained-about-autopilot/3275600/, geraadpleegd op 27 mei 2018.

174 Youtube, *Tesla Autopilot 2 Almost Crashes Into Barrier (ala Deadly Mountain View crash)*, https://www.youtube.com/watch?v=TIUU1xNqI8w, geraadpleegd op 20 mei 2018.

175 Youtube, *This is what may have happened in the recent Tesla Autopilot Crash*, https://www.youtube.com/watch?v=6QCF8tVqM3I, geraadpleegd op 20 mei 2018.

De NTSB is een onderzoek gestart naar dit ongeval, hiervan is reeds een voortijdig rapport verschenen.[176]

Figuur 32: Ongeval met een Volvo V90 van Uber die uitgerust was met een zelfrijdend systeem. Links: de ongevalslocatie met daarin aangegeven de route van de Uber (groen) en de voetganger (oranje). Rechts: de Uber na het ongeval met schade aan de rechter voorzijde. (Bron NTSB)

Bevindingen:

- Het was donker en de voetganger droeg donkere kleding en de fiets had geen zijreflectoren.
- De operator had een dubbele taak, namelijk op de weg letten en op het diagnostische scherm onder het dashboard.
- De operator keek niet op de weg ten tijde van het ongeval. Het is nog niet bekend wat zij wel deed.
- De sensoren detecteerden de voetganger 6 seconden voor de botsing, maar het zelfrijdende systeem ondernam geen actie. Mogelijk omdat het systeem moeite had met de classificatie: is het object een persoon, voertuig, stationair, etc.?
- Het Volvo collision avoidance system[177] (CAS) was uitgeschakeld. Naast het Volvo systeem was het voertuig uitgerust met een op maat gemaakt zelfrijdend systeem van Uber. Het Uber system was ook uitgerust met een FCW systeem; dit systeem (dat niet in staat is te remmen en slechts waarschuwt) stelde vast dat op 1,3 seconde voor de botsing een noodremming noodzakelijk was. De remming is echter niet ingezet omdat de noodremfunctionaliteit van Volvo softwarematig was uitgeschakeld.

176 NTSB, *Preliminary Report - Highway - HWY18MH010*, 2018.
177 CAS verschilt van FCW: FCW waarschuwt alleen terwijl CAS in staat is het remsysteem (of in sommige gevallen ook de stuurinrichting) te activeren. In feite is CAS dus FCW gecombineerd met AEBS.

ADAS

D.1 Historie digitalisering en automatisering in auto's

De steeds verdergaande digitalisering van de auto heeft het mogelijk gemaakt dat steeds meer automatiseringstoepassingen in de auto geïntroduceerd zijn.

Digitalisering
De digitalisering van auto's kent een lange voorgeschiedenis. Eind jaren zestig werden de eerste computers in de auto geïnstalleerd om het ontbrandingsproces efficiënter te maken. Hiervoor werden kleine computersystemen op basis van een microprocessor gebruikt die Electronic Control Units (ECU) worden genoemd.[178] De eerste ECU's voor elektronische benzine-injectie worden al sinds 1968 gebruikt. Later werden ECU's ook voor andere toepassingen gemaakt. Voorbeelden van ECU's zijn: *Transmission control, Seat Position Control, Electric Power Steering, Adaptive Front Lighting, Airbag Deployment, Telematic Control Unit* (TCU), *Brake Control Module* (BCM), ABS of ESC. Deze microcomputers in auto's hebben nieuwe functionaliteiten mogelijk gemaakt die extra comfort bieden voor de bestuurder of taken van de bestuurder kunnen overnemen. Moderne auto's hebben meer dan honderd geschakelde ECU's.[179]

Figuur 33: Een ECU.

178 Nick Davis, *Automotive electronics: What are they, and how do they differ from "normal" electronics?* - Power Electronics, https://www.powerelectronicsnews.com/technology/automotive-electronics-what-are-they-and-how-do-they-differ-from-normal-electronics, geraadpleegd op 23 augustus 2019.
179 National Instruments, *Building Flexible, Cost-Effective ECU Test Systems*, 2019.

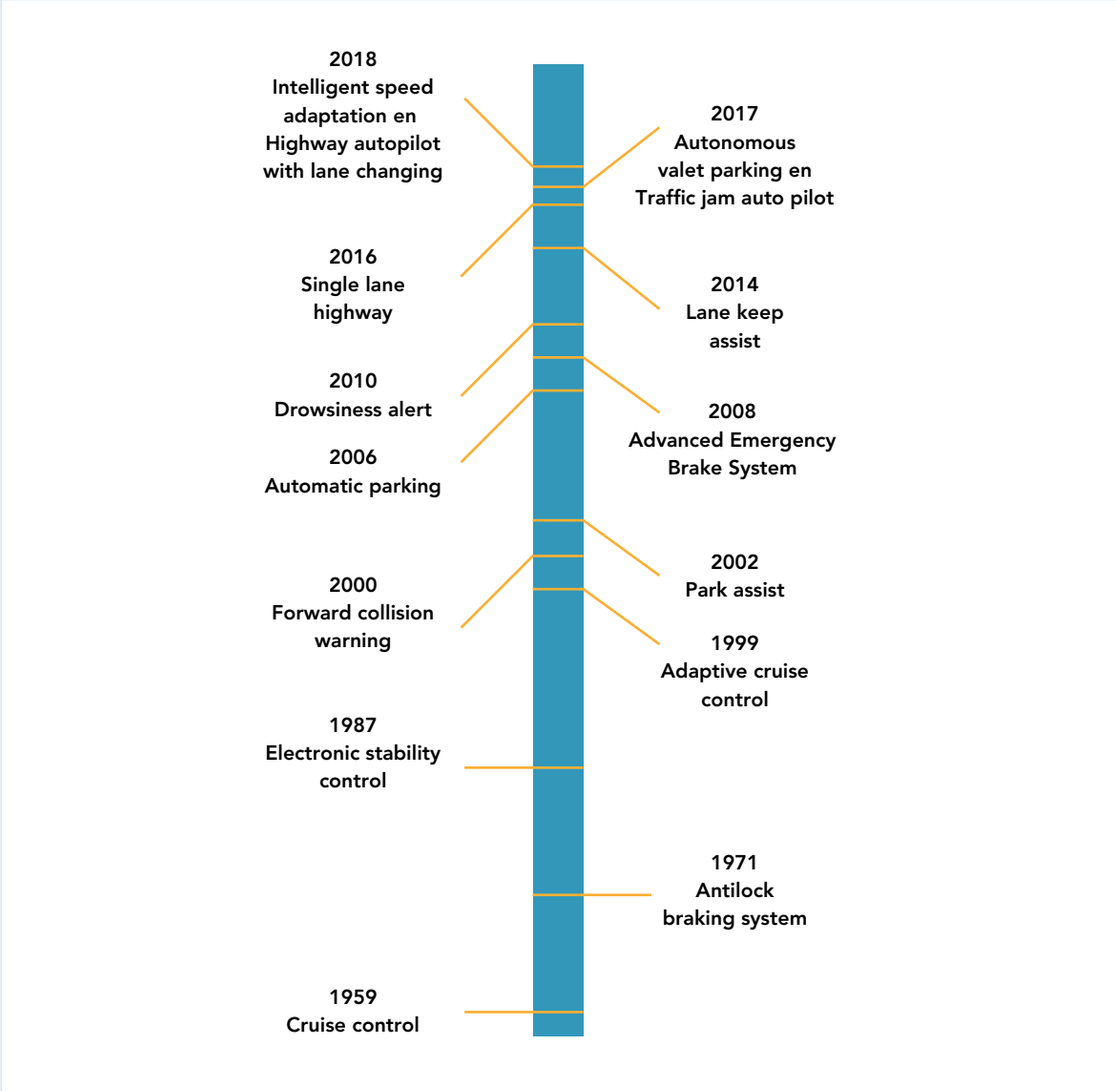
Met de toename van ECU's in de auto is ook de hoeveelheid software sterk toegenomen. In 2015 zou een moderne auto al tien miljoen regels code bevatten.[180] De flexibiliteit van software ten opzichte van hardware geeft veel nieuwe mogelijkheden om toepassingen voor de auto te ontwikkelen, maar heeft ook zijn eigen uitdagingen met bugs, kwetsbaarheden en updates.

In de klassieke aanpak door de auto-industrie wordt voor elke nieuwe functie een nieuwe ECU ontwikkeld. Momenteel is er in het ontwerp van nieuwe auto's een verschuiving te zien naar het gebruik van een centraal computersysteem met meer rekenkracht dat informatie ontvangt vanuit veel verschillende sensoren.[181] Dit is nodig voor de grote hoeveelheid data die verwerkt wordt en de rekenkracht die hierbij nodig is in het toepassen van ADAS en zelfrijdende oplossingen. Verder zorgt het samenvoegen van meerdere losse computer modules (de ecu's) er voor dat de auto als geheel beter te beheersen is en dat er gemakkelijker standaardisatie plaats kan vinden op hardware en software gebied. De auto is zich aan het ontwikkelen van een mechanisch voortuig met verschillende computersystemen aan boord tot een datacentrum op wielen.

Automatisering
Automatisering ondersteunt de automobilist bij het uitvoeren van de rijtaak. Dit kan door de bestuurder van informatie te voorzien en te waarschuwen bij gevaarlijke situaties en door bepaalde taken over te nemen.

De automatisering van de rijtaak is begonnen met de introductie van cruisecontrol (CC) in 1959. Al was deze eerste automatiseringstoepassing mechanisch geïmplementeerd, het aantal auto's met CC nam pas echt toe toen deze met een ECU werden aangestuurd (sinds eind jaren tachtig). Sindsdien zijn er steeds nieuwe mogelijkheden om de primaire rijtaak van de bestuurder over te nemen bijgekomen. De digitalisering van de auto heeft deze automatisering mogelijk gemaakt. Figuur 34 geeft een overzicht wanneer specifieke automatiseringsfuncties geïntroduceerd zijn.[182, 183] De meer recente functies worden vaak aangeduid als *Advanced Driving Assistance Systems* (ADAS).

180 McCandless, Doughty-White, en Quick, *Million Lines of Code*, https://informationisbeautiful.net/visualizations/million-lines-of-code/, geraadpleegd op 10 juli 2019.
181 McKinsey&Company, *Rethinking car software and electronics architecture*, 2018.
182 BCG, *A roadmap to safer driving through advanced driver assistance systems*, 2015.
183 CAR, *Technology roadmaps: Intelligent mobility technology, Materials and manufacturing processes, and Light duty vehicle propulsion*, 2017.



Figuur 34: Tijdlijn van automatisering van voertuigen.

D.2 Wat zijn ADAS?

Er bestaat geen eenduidige definitie van Advanced Driver Assistance Systems (ADAS). Soms worden alle technieken bedoeld waarmee de bestuurder ondersteund wordt bij het rijden. Cruisecontrol en ABS vallen er dan ook onder. In andere gevallen wordt de nadruk gelegd op "Advanced" en vallen alleen de complexere systemen zoals Lane Changing Assistance onder ADAS. Het verschil hangt vaak samen met het gehanteerde referentiekader:

- De bestuurder wordt centraal gesteld en men kijkt naar de mate waarin het systeem de bestuurder ondersteunt.
- De techniek wordt centraal gesteld en men kijkt naar de mate waarin het systeem autonoom kan besturen.

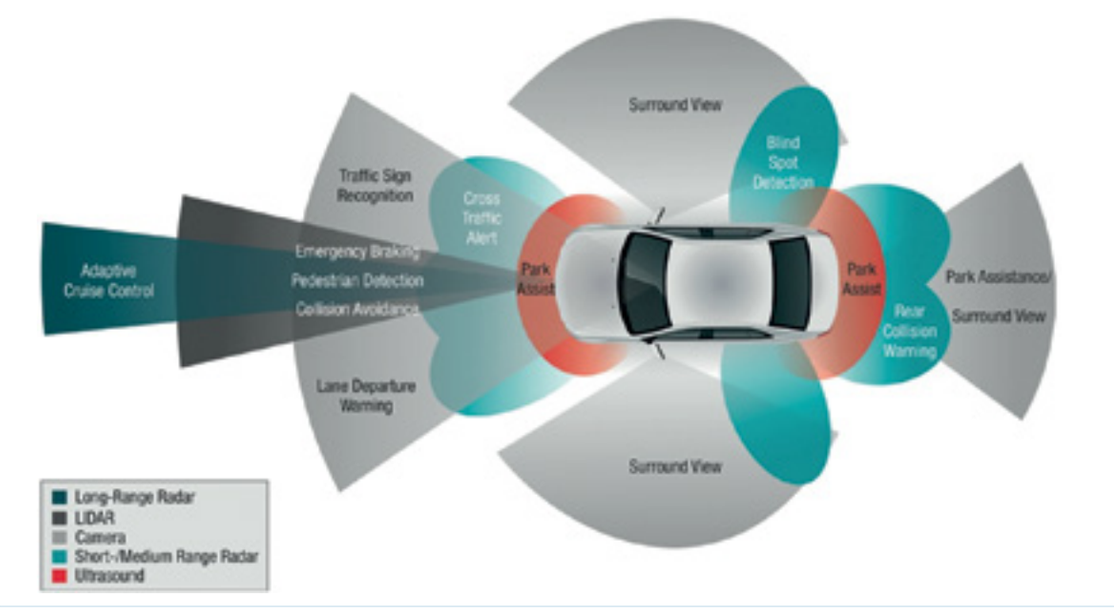
De ADAS Alliantie noemt drie kenmerken van ADAS[184]:

- De bestuurder draagt de volledige verantwoordelijkheid , maar deelt de controle met het voertuig.
- Het voertuig en de bestuurder delen het detecteren van en reageren op objecten en gebeurtenissen (Object and Event Detection en Response (OEDR)).
- De bestuurder mag geen secundaire taken uitvoeren, anders dan die zijn toegestaan tijdens normaal rijden.

De Onderzoeksraad hanteert de volgende definitie:

Definitie ADAS
Advanced Driver Assistance Systems (ADAS) zijn rijhulpsystemen die de bestuurder ondersteunen bij het uitvoeren van de primaire rijtaak. Deze systemen nemen de omgeving waar door middel van sensoren en kunnen de besturing van de snelheid en/of rijrichting overnemen onder verantwoordelijkheid van de persoon aan het stuur. Dergelijke systemen kunnen de bestuurder ook waarschuwen in door het systeem als gevaarlijk ingeschatte situaties.

De Onderzoeksraad stelt met deze definitie de bestuurder centraal en hanteert hiermee een bredere definitie dan de ACEA[185] en de SAE.[186]



Figuur 35: Sensoren van geautomatiseerde auto.[187]

184 ADAS Alliantie, *ADAS Convenant*, 2019.
185 Knapp et al., *Code of Practice for the Design and Evaluation of ADAS*, 2009.
186 SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report*, 2014.
187 Michigan Tech Research Institute, *Benchmarking Sensors for Vehicle Computer Vision Systems*, https://mtri.org/automotivebenchmark.html, geraadpleegd 28 augustus 2019.

Een belangrijk kenmerk van ADAS is dat ze gebruikmaken van sensoren om de omgeving van de auto waar te nemen. Op basis van de data afkomstig uit de sensoren kunnen de ADAS beslissingen nemen. Er zijn verschillende soorten sensoren, elk met specifieke eigenschappen zoals radar, lidar en camera systemen die voor verschillende toepassingen gebruikt kunnen worden, zie Figuur 35. Zo werkt radar goed voor lange afstanden en is radar minder goed in richting inschatten. Radar wordt daarom toegepast in adaptive cruisecontrol, waarbij de voorganger op grote afstand gedetecteerd moet worden. In sommige gevallen wordt informatie van meerdere sensoren gecombineerd om zo tot een nauwkeuriger beeld te komen. Dan spreekt men van *sensor fusion*.

Een overzicht van verschillende soorten ADAS met korte beschrijving is te vinden in onderstaande tabel (Tabel 6). We gebruiken de Engelstalige benaming voor deze systemen omdat verschillende termen al ingeburgerd zijn en vertaling naar het Nederlands verwarring zou kunnen opleveren.

ADAS	Afkorting	Beschrijving
Adaptive Cruisecontrol	ACC	Systeem dat de snelheid van de auto aanpast aan de voorganger. Ook wel Intelligent Adaptive Cruisecontrol.
Lane Keeping Assistant	LKA	Ondersteunt de bestuurder om de auto binnen de rijstrook te houden.
Lane Departure Warning	LDW	Waarschuwt de bestuurder als de auto uit de rijstrook dreigt te gaan.
Forward Collision Warning	FCW	Waarschuwt de bestuurder als een voorwaartse aanrijding dreigt.
Intelligent Speed Adaptation	ISA	Past de snelheid van de auto aan op basis van informatie van de specifieke weg (ontvangen signaal of waargenomen op borden).
Automatic Parking		Voertuig parkeert zichzelf op lage snelheid in na bevestiging van bestuurder.
Drowsiness alert		Waarschuwt de bestuurder als deze niet voldoende aandacht heeft voor het uitvoeren van de rijtaak.
Single Lane Highway	LKA+ACC	Combinatie van LKA en ACC waardoor de auto zelfstandig binnen dezelfde rijstrook kan blijven rijden.
Advanced Emergency Brake System	AEBS	Noodremsysteem bij dreigende aanrijding.

Tabel 6: Verschillende ADAS beschreven.

De bovenstaande tabel zou kunnen doen vermoeden dat ADAS een eenduidige taxonomie heeft, maar dit is in de praktijk niet het geval. ADAS worden vaak gebruikt door marketing van verschillende automerken om de auto meer onderscheidend te maken. Hierdoor kan het zo zijn dat voor dezelfde functionaliteit verschillende benamingen gebruikt worden. Zo heeft Nissan Pro pilot, Tesla Autopilot en Volvo Pro pilot die dezelfde functionaliteit bieden.

D.3 Artificial intelligence

Bij de nieuwste ADAS en het ontwikkelen van autonome functies wordt steeds meer gebruik gemaakt van *Artificial Intelligence* (AI).[188, 189, 190, 191, 192] Het gaat hierbij vooral om het verwerken en interpreteren van sensordata. AI systemen kunnen complexe taken uitvoeren zonder menselijke controle of begeleiding. AI richt zich op systemen die autonoom opereren, reageren op hun omgeving op basis van sensordata, zichzelf kunnen verbeteren en aanpassen aan veranderingen. Deze systemen bestaan uit verschillende technologieën die er samen voor zorgen dat in een bepaalde context een zekere mate van intelligent gedrag vertoond wordt.

Binnen AI systemen is er het onderscheid tussen systemen waarbij de mens alle situaties in kaart heeft gebracht en daarbij beslisregels heeft opgesteld (*rule-based* AI) en zelflerende systemen die in staat zijn om te leren op basis van eerdere ervaringen of simulaties (*machine learning*)

Rule-based AI
Bij *rule-based AI* wordt een beslisboom met instructies gemaakt waarmee het systeem in specifieke situaties min of meer zelfstandig een bepaald doel kan bereiken. Het is gebaseerd op een vooraf gedefinieerd statisch model van de omgeving. Voor veel huidige ADAS wordt een beslisboom gebruikt. Echter wordt dit niet altijd AI genoemd.

Machine learning
Machine Learning (ML) is een lerend systeem gebaseerd op algoritmes die in staat zijn om te leren op basis van eerdere ervaringen. Zo ontstaat een adaptief systeem dat zijn parameters kan aanpassen afhankelijk van externe input. Er zijn ML systemen die eenmalig getraind zijn met een specifieke dataset en systemen die continu bijleren. Voor verschillende ADAS-toepassingen wordt gebruik gemaakt van Machine Learning. Een voorbeeld hiervan is de objectdetectie die nodig is bij 'Single lane highway'-ondersteuning.

Verbeteren van rule-based systemen
ADAS moeten omgaan met veel verschillende verkeerssituaties. Daarom liggen complexe algoritmes ten grondslag aan de beslissingen die het systeem neemt. Het kost veel moeite om deze systemen te ontwikkelen en verbeteren bij *rule-based* systemen. Een manier om dit op te lossen is om gebruik te maken van *rule-based machine learning*.[193] Hierbij wordt op de achtergrond "meegekeken" door het systeem om nieuwe handige regels te ontdekken die weer toegevoegd kunnen worden aan de beslisboom.

188 Russel en Norvig, *Artificial Intelligence – A modern approach,Artificial Intelligence – A modern approach*, 2010.
189 Vetzo, Gerards, en Nehmelman, *Algoritmes en grondrechten,Algoritmes en grondrechten*, 2018.
190 De Jong, Kool, en Van Est, *Zo brengen we AI in de praktijk vanuit Europese waarden*, 2019.
191 Tricentis, *AI Approaches Compared: Rule-Based Testing vs. Learning*, https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/, geraadpleegd op 23 augustus 2019.
192 Iriondo, *Differences Between AI and Machine Learning, and Why it Matters*, https://medium.com/datadriveninvestor/differences-between-ai-and-machine-learning-and-why-it-matters-1255b182fc6, geraadpleegd op 23 augustus 2019.
193 Weiss en Indurkhya, *Rule-based Machine Learning Methods for Functional Prediction*, Journal of Artificial Intelligence Research 3, 1995.

Deze nieuwe beslisregels kunnen dan voor implementatie in productie, uitgebreid getest en geverifieerd worden. Door niet de data van één auto te gebruiken, maar de geaggregeerde data van alle auto's. kan een beter lerend systeem gemaakt worden.

Nieuwe ontwikkelingen
Deep Learning (DL) is een geavanceerde vorm van ML en maakt gebruik van kunstmatige neurale netwerken. Deep Learning is nog niet aanwezig in moderne auto's. Dit zijn grotere modellen bestaande uit meerdere lagen die gelijkenissen hebben met de werking van neuronen in de hersenen. Het op een correcte manier trainen van een DL model met de juiste input data en het uitgebreid verifiëren van de uiteindelijke prestaties van het model is een essentiële stap om tot de gewenste kwaliteit van het model te komen. Om uiteindelijk een effectief model te maken zijn heel veel data nodig. *Deep Learning*-technieken zijn essentieel voor zelfrijdende voertuigen. Door de beschikbaarheid van de enorme hoeveelheid data uit sensoren en de benodigde rekenkracht worden er grote stappen gemaakt in de ontwikkeling naar een autonoom opererend voertuig.

D.4 Classificatie automatisering

Zoals eerder beschreven zijn er verschillende definities van ADAS en wordt er verschillend aangekeken tegen de automatisering. Dit resulteert erin dat de systemen op verschillende manieren geclassificeerd worden. De meest bekende indeling van automatisering van de auto is ontwikkeld door de Society of Automotive Engineers en vastgelegd in het document SAE-J3016[194]. Daarnaast is er de formele wettelijke indeling van de UNECE. Verder is de indeling van Euro NCAP van belang, omdat deze onderscheid maakt tussen veiligheidssystemen en overige systemen.

194 SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report*, 2014.

	Level 0 Geen automatisering rijtaak	Level 1 Ondersteuning bestuurder	Level 2 Gedeeltelijke automatisering	Level 3 Voorwaardelijke automatisering	Level 4 Hoge mate van automatisering	Level 5 Volledige automatisering
Wie bestuurt het voertuig?	De mens bestuurt het voertuig (bepaalt richting en snelheid); als er gebruik wordt gemaakt van automatisering moet de mens in staat zijn in te grijpen. De mens monitort de verkeerssituatie en kan daarvoor hulpmiddelen gebruiken.			De mens moet stand-by staan om besturing van de automatisering over te nemen als deze daar om vraagt.	De automatisering bestuurt het voertuig, de menselijke bestuurder is niet meer nodig.	
Wat doen deze systemen?	Automatisering kan waarschuwingen geven bij gevaarlijke situaties en tijdelijk ingrijpen, bijvoorbeeld bij een dreigende botsing met een andere weggebruiker of object.	Besturing over de richting of snelheid kan overgenomen worden door automatisering in het voertuig. De mens monitort de verkeerssituatie en kan daarvoor hulpmiddelen gebruiken.	Besturing over de richting en snelheid kan (tegelijkertijd) overgenomen worden door automatisering in het voertuig. De mens monitort de verkeerssituatie en kan daarvoor hulpmiddelen gebruiken.	Automatisering heeft onder bepaalde omstandigheden (bijvoorbeeld op snelwegen en/of tijdens het rijden in een file) volledige besturing over het voertuig. Level 3 werkt niet in alle situaties.	Automatisering heeft onder de meeste omstandigheden volledige besturing over het voertuig. Level 4 werkt nog niet in alle situaties (bijvoorbeeld alleen in bepaalde regio's).	Automatisering heeft onder alle omstandigheden volledige besturing over het voertuig.
Voorbeelden	Automatic Emergency Braking System (AEBS) Lane Departure Warning (LDW), Front Collision Warning (FCW) ABS, ESC, traction control	Adaptive Cruisecontrol (ACC), Lane Keeping Assist (LKA), Park Assist (PA)	ACC gecombineerd met LKA, bijvoorbeeld Tesla Autopilot, Nissan ProPilot, Volvo Pilot Assist			Volledig automatisch voertuig

Tabel 7: SAE levels van automatisering in het wegverkeer. In het oranje gearceerde vlak de systemen waarop de primaire focus ligt in dit onderzoek.

SAE levels
De automatisering van de auto is door de SAE ingedeeld in vijf categorieën. Een overzicht hiervan is te vinden in Tabel 7. Kort beschreven zijn deze als volgt in te delen:

- Bij level 1 en 2 maakt de bestuurder de tactische keuzes, maar neemt het systeem gradueel de operationele taak over en heeft de bestuurder nu eens de rol van operator, die klaar moet staan om de besturing over te nemen als het systeem er niet uitkomt of een fout maakt, en dan weer de vertrouwde rol van handmatige bestuurder.
- Bij level 3 is de bestuurder volledig operator geworden.
- Bij level 4 en 5 heeft de bestuurder geen rol meer in de besturing van het voertuig. Voor level 4 is dit in een beperkte omgeving en voor level 5 overal.

De scope van ADAS in dit onderzoeksrapport komt in ieder geval overeen met de SAE levels 1 en 2. Ook level 3 systemen vallen volgens onze ADAS definitie binnen het onderzoek, maar hiervan zijn op dit moment nog weinig tot geen voorbeelden in het verkeer aanwezig. Van de SAE level 0 systemen valt de AEBS ook binnen de scope van dit onderzoek, maar andere (nood)systemen in level 0 niet.

UNECE
In de UN regulation No. 79 zijn de belangrijkste termen en categorieën gedefinieerd rond het automatiseren van de rijtaak. De automatiseringssystemen in de auto wordt hier op een veel technischere manier ingedeeld dan in de SAE levels. Er is alleen een classificatie voor systemen die invloed hebben op sturen, omdat er voor ADAS die de snelheid van het voertuig continu beïnvloeden op dit moment nog geen specifieke eisen zijn. In bijlage E.4 wordt deze classificatie beschreven.

Euro NCAP
Euro NCAP is een instituut dat de veiligheid beoordeelt van auto's in kritieke situaties zoals bescherming van inzittenden bij een botsing. Euro NCAP maakt onderscheid tussen veiligheidssystemen en overige systemen. Veiligheidssystemen worden meegenomen in het sterrenbeoordelingssysteem als onderdeel van de *safety assist* systemen. Het gaat hierbij om drie verschillende soorten ADAS, namelijk:

- *AEB Interurban* (bij hogere snelheid ook wel AEBS),
- *Lane Support* (systemen die waarschuwen of ingrijpen bij het verlaten van de rijstrook en blindspotmonitoring systemen) en
- *Speed Assist* (systemen die waarschuwen voor snelheidsoverschrijdingen, systemen die de maximale snelheid weergeven en sytemen die de snelheid begrenzen).

Daarnaast worden andere veiligheidssystemen meegewogen die niets met automatisering te maken hebben, zoals gordelverklikkers. Er word dus niet gekeken naar het automatiseringsniveau van de rijtaak, maar alleen of een bepaald type systeem bewezen veiligheidswinst oplevert.

Sterrensysteem
Het sterrensysteem van Euro NCAP geeft een beoordeling over de extra veiligheidsmaatregelen die een auto boven op de al verplichte maatregelen heeft genomen. Hierbij wordt gekeken naar de bescherming van de volwassen bestuurder, van inzittende kinderen, van kwetsbare weggebruikers zoals voetgangers en naar de al genoemde *safety assist* systemen. De *safety assist* systemen bestaan uit rijhulpsystemen die de bestuurder helpen om veilig te rijden.

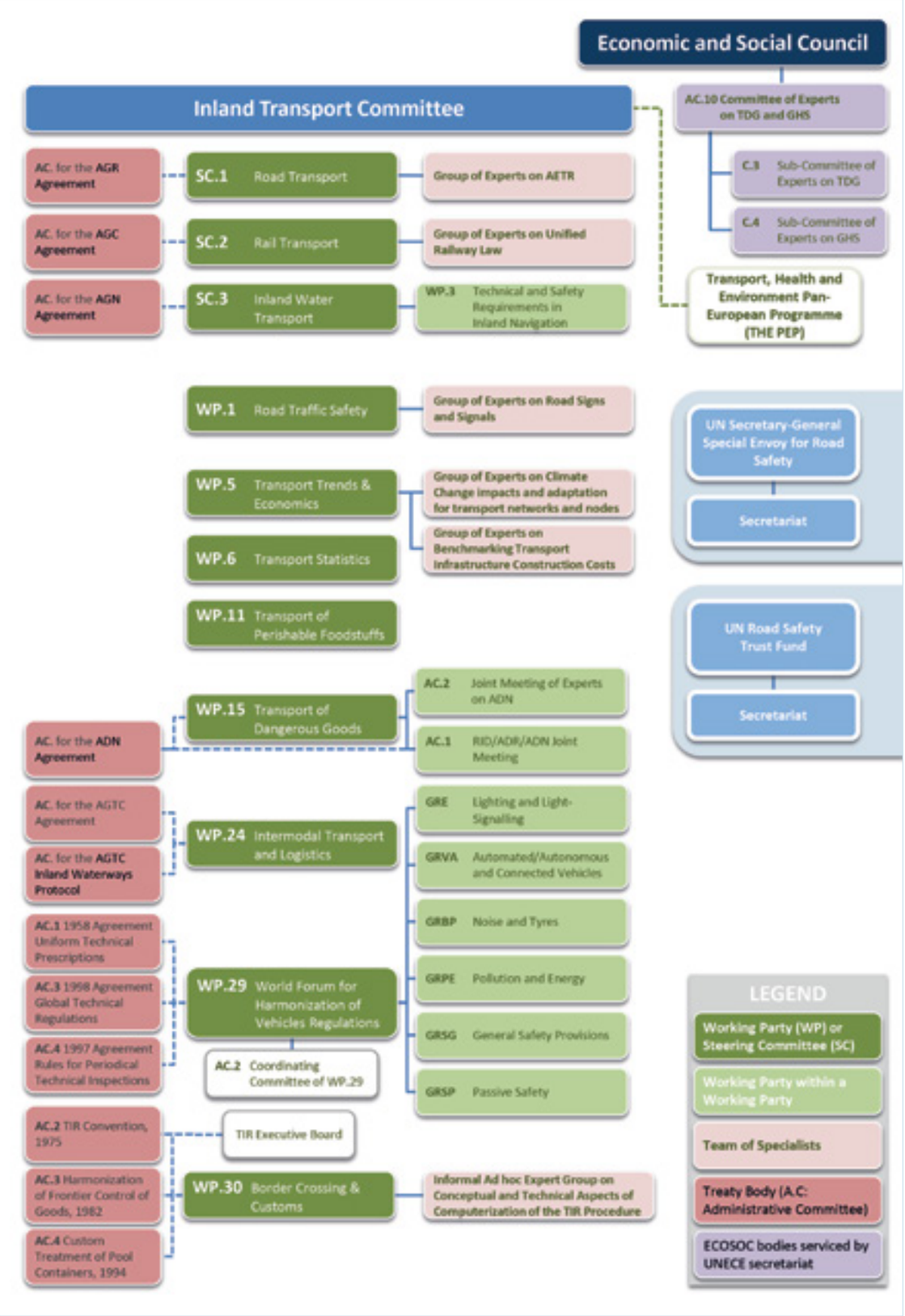
REGELGEVING

E.1 Inleiding

Voertuigen die in Nederland op de openbare weg rijden, moeten voldoen aan bepaalde eisen. Deze eisen verschillen per type voertuig. In het kader van dit onderzoek beperken we ons in de eerste plaats tot eisen die gesteld worden aan motorvoertuigen en in het bijzonder tot eisen aan seriematig geproduceerde personenauto's. In de tweede plaats beperken we ons tot eisen met een directe relatie tot de verkeersveiligheid. Dat betekent dat we bijvoorbeeld geen aandacht besteden aan de regelgeving op het gebied van geluid en emissies en evenmin ingaan op verschillen tussen elektrische personenauto's en personenauto's met een verbrandingsmotor. De nadruk ligt op actieve veiligheid (bijvoorbeeld via systemen als ABS en diverse ADAS) en niet op passieve veiligheid (bijvoorbeeld door middel van autogordels, hoofdsteunen, airbags en kreukelzones).

E.2 Totstandkoming regelgeving

Autofabrikanten komen uit verschillende landen en continenten en produceren en concurreren op een internationale markt. Fabrikanten hebben er groot belang bij dat voor zoveel mogelijk landen dezelfde regels en technische normen gelden. Binnen de interne markt van de Europese Unie is dat al een gegeven. Zo mogen in Nederland toegelaten auto's rijden in andere Europese lidstaten en vice versa. De Nederlandse voertuigregelgeving is Europees geharmoniseerd voor de meeste motorvoertuigen waaronder personenauto's en vrachtwagens. Voorstellen voor EU-wetgeving worden voorbereid en ingediend door de Europese Commissie en vastgesteld door de lidstaten, verenigd in de Europese Raad van ministers en het Europees Parlement. De EU-wetgeving valt uiteen in twee categorieën: verordeningen, die rechtstreeks en onmiddellijk kracht van wet hebben in alle EU-lidstaten en richtlijnen, die door de lidstaten moeten worden geïmplementeerd in nationale wet- en regelgeving. De EU-richtlijnen en verordeningen bevatten op veel onderdelen internationale reglementen, met name op het gebied van technische eisen. Die zijn vastgesteld in de UNECE (United Nations Economic Commission for Europe) in Genève. Het belangrijkste doel van de UNECE is het bevorderen van pan-Europese economische integratie. Doordat de besluitvorming binnen de UNECE gericht is op het bereiken van consensus wordt hier uitgebreid op verschillende niveaus overlegd. De UNECE behartigt meer onderwerpen dan alleen transport, maar die blijven in het kader van dit onderzoek buiten beschouwing. Figuur 36 geeft een overzicht van de UNECE organisatie op het gebied van transport.



Figuur 36: Organisatie van UNECE op het gebied van transport. (Bron: UNECE)

Bij de UNECE zijn ook niet-Europese landen met een belangrijke auto-industrie aangesloten, zoals de Verenigde Staten, Japan en Zuid-Korea. De UNECE is daarmee een mondiaal platform op het gebied van technische voertuigregelgeving. In het samenspel tussen Brussel (Europese Commissie) en Genève (UNECE) wordt het initiatief voor nieuwe regelgeving nu eens in Brussel genomen en dan weer in Genève. Europese wetgeving wordt voorbereid door de EC en vastgesteld door de Europese Raad en het Europees Parlement. De EU is lid van de UNECE en de Europese Commissie stemt mede namens de EU-lidstaten binnen de UNECE over nieuwe reglementen of aanpassing van bestaande reglementen, waarbij het EU-standpunt vooraf in Brussel is afgestemd met de EU-lidstaten. Deze afstemming vindt plaats in diverse commissies en werkgroepen binnen zowel de Europese Commissie als de Europese Raad. De in Genève mede door de EU aangenomen reglementen zijn verplichtend voor alle lidstaten van de EU.

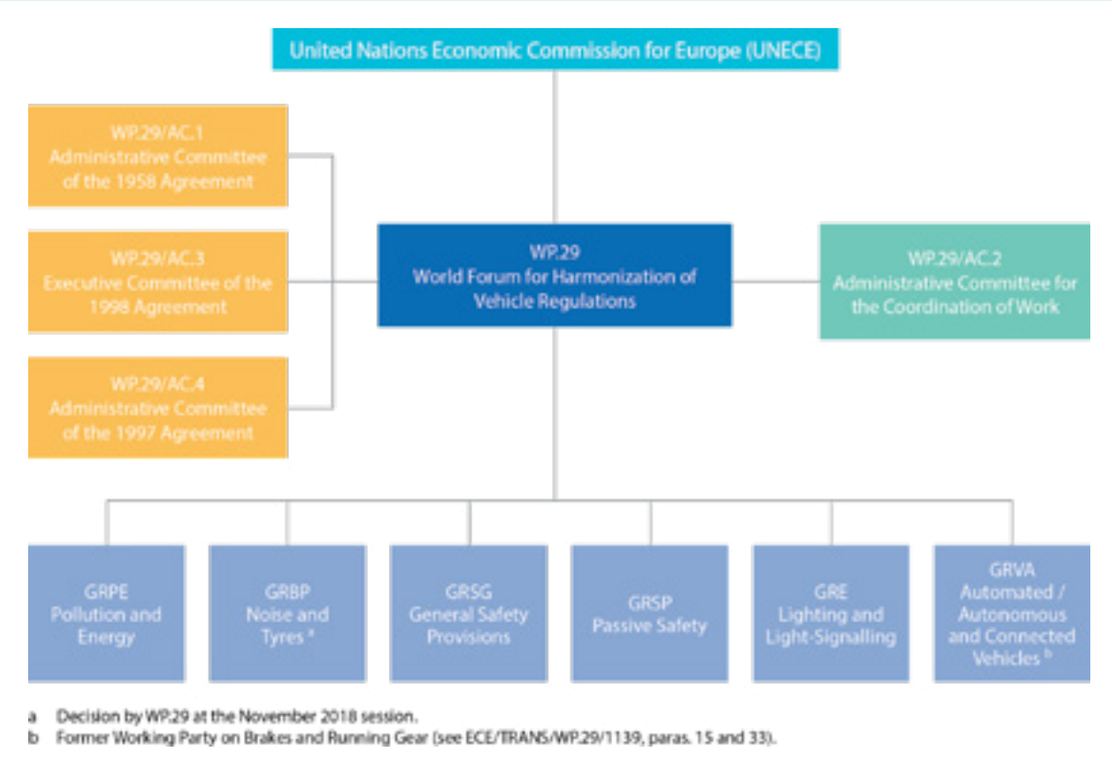
Binnen de UNECE zijn voor dit onderzoek twee zogenoemde *Working Parties* belangrijk:

- WP.1 '*Global Forum for Road Traffic Safety*'. Deze *Working Party* richt zich op verbetering van de verkeersveiligheid en beschouwt daarbij de drie bepalende aspecten: voertuig, gedrag van de verkeersdeelnemers en infrastructuur in hun onderlinge samenhang.
- WP.29 '*World Forum for Harmonization of Vehicle Regulations*'. Het '*Blue Book*'[195] geeft een overzicht van de werkwijze van deze Working Party, die gericht is op het opstellen van breed gedragen en breed toepasbare technische reglementen voor voertuigen. Hier liggen drie verdragen aan ten grondslag, waar hier niet verder op wordt ingegaan. Onder WP.29 zijn zes werkgroepen actief in verschillende domeinen, waarbij voor dit onderzoek de GRVA, de werkgroep over '*Automated/Autonomous and Connected Vehicles*' de belangrijkste is. Deze werkgroep bereidt de reglementen op het gebied van ADAS voor en brengt deze ter besluitvorming in WP.29. Onder de GRVA hangen nog weer informele werkgroepen voor specifieke typen of onderdelen van ADAS. Figuur 37 geeft de organisatie van WP.29 op hoofdlijnen schematisch weer.

In WP.1 en WP.29 hebben alleen (vertegenwoordigers van) de aangesloten landen zitting. Een medewerker van het ministerie van Infrastructuur en Waterstaat vertegenwoordigt Nederland in WP.1; in WP.29 heeft het ministerie van I&W een medewerker van RDW gemandateerd om Nederland te vertegenwoordigen. De RDW en het ministerie van I&W stemmen regelmatig af over UNECE. De aangesloten landen stemmen en beslissen over de voorgestelde reglementen (*UN Regulations, UN Global Technical Regulations en UN Rules* afhankelijk van het verdrag waaronder de regelgeving valt), die worden voorbereid door de onder deze *Working Parties* hangende werkgroepen, waar ook vertegenwoordigers van autofabrikanten, toeleveranciers, belangengroeperingen en goedkeuringsinstanties zoals de RDW deel van uitmaken. Het doel van dit overleg is het bereiken van overeenstemming over technische vereisten waarbij (uiteenlopende) politieke en economische belangen een belangrijke rol spelen. De richtlijnen stellen minimumeisen op het gebied van verkeersveiligheid. Deze mogen door individuele lidstaten niet worden verzwaard. Wel staat het autofabrikanten vrij om veiligere auto's te maken dan wettelijk vereist.

195 UNECE, *World Forum For Harmonization of Vehicle Regulations (WP.29); How it works, how to join it*, 2019.

Op dit aspect kunnen autofabrikanten zich van elkaar onderscheiden en elkaar beconcurreren. Euro NCAP (zie bijlage D) beoordeelt op basis van tests een aantal bovenwettelijke veiligheidsmaatregelen in auto's en classificeert deze volgens een sterrensysteem. Sinds kort wordt ook een beperkt aantal ADAS in deze tests en classificatie betrokken. Van dit sterrensysteem gaat een stimulerende werking uit op autofabrikanten om extra maatregelen te nemen om de actieve en passieve veiligheid van hun auto's te verbeteren. Als veel autofabrikanten een bepaalde extra maatregel hebben genomen, wordt deze vaak door UNECE en EU in de regelgeving opgenomen.



Figuur 37: Organisatie UNECE WP.29. (Bron: UNECE)

E.3 Soorten eisen aan personenauto's

Seriematig geproduceerde personenauto's die gebruikmaken van de openbare weg moeten aan drie soorten eisen voldoen: toelatingseisen, permanente eisen en gebruikseisen.

De **toelatingseisen** worden getoetst door middel van een typekeuring in een van de EU-lidstaten. Deze wordt uitgevoerd door een geautoriseerd Europees testlaboratorium. Dit soort keuringen kan zowel op voertuigen als op systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, worden uitgevoerd. Typegoedkeuring in één EU-lidstaat leidt tot toelating in de gehele EU. Een eenmaal verkregen goedkeuring blijft van kracht ook indien toelatingseisen later worden veranderd of aangescherpt. Dit betekent dat eenmaal toegelaten voertuigen niet gewijzigd hoeven te worden om aan nieuwe regels te voldoen. Wel kan het zijn dat nieuw geproduceerde auto's van een bepaald type op een gegeven moment aan aangescherpte

eisen moeten voldoen. De toelatingseisen en de manier waarop deze worden getoetst zijn opgenomen in de Europese Richtlijn 2007/46/EG, die de basis vormt van de Nederlandse Regeling voertuigen, waarvan op 20 mei 2018 een nieuwe versie van kracht is geworden. De Regeling voertuigen geeft uitvoering aan de hoofdstukken III en VI van de Wegenverkeerswet 1994. Voor typegoedkeuring wordt in de Regeling voertuigen direct verwezen naar richtlijn 2007/46/EG. Deze richtlijn bevat gedetailleerde voorschriften om te borgen dat typekeuringen in verschillende landen tot hetzelfde resultaat leiden. Een deel van de voorschriften is opgenomen in de Richtlijn, een ander deel verwijst naar UNECE reglementen, die bij verdrag bindend zijn voor de EU en haar lidstaten. In Artikel 34 'VN/ECE-reglementen die deel uitmaken van de EG-typegoedkeuring' van Richtlijn 2007/46/EG is dit expliciet vastgelegd. Voor de 'traditioneel' in auto's aanwezige, grotendeels mechanische delen en systemen zijn deze voorschriften descriptief en kwantitatief. Voor ADAS zijn ze kwalitatief en functioneel of ontbreken ze. Hier komen we in een volgende paragraaf op terug.

De Europese wet- en regelgeving op het gebied van toelatingseisen van voertuigen wordt ongeveer eens per tien jaar vernieuwd. Zo staat de opvolger van Richtlijn 2007/46/EG al klaar in de vorm van Verordening (EU) 2018/858 die met ingang van 1 september 2020 in werking zal treden. In zo'n periode van ongeveer tien jaar is het wel nodig om aanvullingen te maken op de geldende regelgeving, bijvoorbeeld om in te spelen op nieuwe technische ontwikkelingen. Hier komen we in een volgende paragraaf op terug. In april 2019 hebben de Europese Raad en het Europees Parlement bovendien de General Safety Regulation (GSR) aangenomen, waarin aanvullende eisen op het gebied van voertuigregelgeving vanuit het oogpunt van verkeersveiligheid zijn opgenomen. Deze wordt in een volgende paragraaf nader toegelicht.

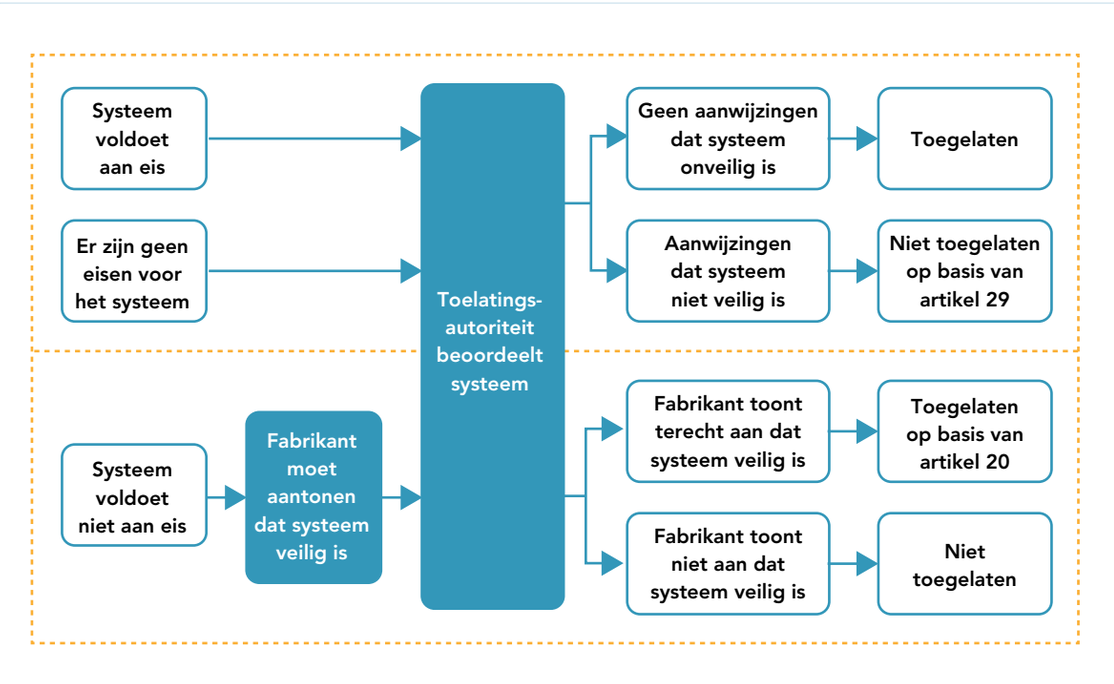
Permanente eisen zijn eisen waaraan het voertuig bij gebruik op de weg dient te voldoen. Het zwaartepunt ligt bij verkeersveiligheidsaspecten, zoals de goede werking van verlichting, remmen, stuurinrichting en banden. Deze worden gecontroleerd door de politie en tijdens de APK. Dergelijke controles moeten snel kunnen worden uitgevoerd zonder demontage of een rijproef. De permanente eisen zijn dan ook veel minder uitgebreid dan de toelatingseisen. De permanente eisen en de wijze van keuren zijn duidelijk en limitatief vermeld in de Regeling voertuigen en zijn gebaseerd op Richtlijn 2014/45/EU. Ze bevatten nauwelijks bepalingen over ADAS; als er al iets staat, heeft het betrekking op de goede werking van waarschuwingssignalen en controlelampjes om de bestuurder te informeren.

Gebruikseisen hebben betrekking op het praktisch handelen, zoals het koppelen van aanhangwagens en het meenemen van passagiers, en zijn in het kader van dit onderzoek niet relevant.

E.4 Bestaande Europese toelatingseisen voor ADAS

De Regeling voertuigen verwijst voor de toelatingseisen die gesteld worden aan seriematig vervaardigde personenauto's en onderdelen daarvan één op één naar Richtlijn 2007/46/EG. Deze richtlijn bevat gedetailleerde toelatingseisen voor motorvoertuigen als geheel maar ook voor systemen, onderdelen of technische eenheden die binnen motorvoertuigen worden toegepast. EU-typegoedkeuring gaat over voertuigen zoals ze door de fabrikant geleverd worden. Nieuwe personenauto's bevatten vaak systemen, onderdelen en technische eenheden die al eerder zijn toegepast, vaak in meerdere merken en/of types. Voor deze delen kunnen deeltypegoedkeuringen worden aangevraagd, die weer als bouwstenen gebruikt kunnen worden bij de aanvraag van de typegoedkeuring van een nieuwe auto. Richtlijn 2007/46/EG bevatte op het moment van invoering echter nog geen toelatingseisen aan ADAS.

Anticiperen op innovaties bij het toelatingsproces
Richtlijn 2007/46/EG regelt hoe delen waarvoor geen toelatingseisen zijn opgenomen op hoofdlijnen moeten worden beoordeeld om voor een deeltypegoedkeuring in aanmerking te komen. Hiervoor zijn twee artikelen van de Richtlijn leidend, zie Figuur 38.



Figuur 38: Stroomschema voor behandeling van een aanvraag voor typegoedkeuring.

Artikel 20 'Ontheffingen voor nieuwe technologieën of nieuwe concepten' in Hoofdstuk VIII 'Nieuwe technologieën of concepten die onverenigbaar zijn met de bijzondere richtlijnen' biedt fabrikanten de mogelijkheid om een EG-typegoedkeuring aan te vragen voor een systeem, onderdeel of technische eenheid waarin technologieën of concepten zijn toegepast die onverenigbaar zijn met de bestaande regelgeving. Een dergelijke aanvraag kan in een lidstaat naar keuze worden ingediend. Bij verlening van de vergunning voor toelating (in eerste instantie alleen in de betreffende lidstaat) van een voertuigtype waarop de gevraagde ontheffing betrekking heeft, dient de lidstaat de EC en de overige lidstaten te informeren over:

a. de redenen waarom de desbetreffende technologieën of concepten tot gevolg hebben dat het systeem, het onderdeel of de technische eenheid onverenigbaar is met de voorschriften;
b. een beschrijving van de desbetreffende veiligheids- en milieuoverwegingen en van de genomen maatregelen;
c. een beschrijving van de tests en de resultaten ervan, waaruit blijkt dat in vergelijking met de voorschriften waarvan ontheffing wordt aangevraagd, ten minste een even hoog veiligheids- en milieubeschermingsniveau wordt gewaarborgd.

Artikel 20 regelt voorts hoe de voorlopige toelating in één lidstaat kan worden uitgebreid naar een in alle lidstaten geldende EG-typegoedkeuring. Artikel 21 regelt vervolgens hoe de bestaande regelgeving (op zogenoemde niet-essentiële onderdelen) moet worden aangepast, ook ingeval het een UNECE reglement betreft.

Artikel 29 'Voertuigen, systemen, onderdelen of technische eenheden die aan deze richtlijn voldoen' in Hoofdstuk XII 'Vrijwaringsclausules' biedt lidstaten de mogelijkheid om nieuwe voertuigen, systemen, onderdelen of technische eenheden, ook al voldoen zij aan de toepasselijke voorschriften of zijn zij naar behoren gemerkt, gedurende maximaal zes maanden te weigeren deze voertuigen te registreren of de verkoop of het in verkeer brengen van deze voertuigen, systemen, onderdelen of technische eenheden op zijn grondgebied toe te staan, ingeval zij naar het oordeel van de lidstaat een ernstig gevaar betekenen voor de verkeersveiligheid dan wel het milieu of de volksgezondheid ernstig schaden. In voorkomende gevallen dient de lidstaat de fabrikant, de overige lidstaten en de EC onmiddellijk daarover te informeren met opgave van de redenen voor zijn besluit. In het bijzonder moet hierbij worden vermeld of het besluit het gevolg is van:

- tekortkomingen in de betrokken regelgevingen, of
- onjuiste toepassing van de betrokken voorschriften.

Artikel 29 regelt voorts welke maatregelen de EC vervolgens moet nemen.

UNECE Reglementen voor ADAS

Binnen UNECE zijn drie documenten belangrijk voor de regelgeving ten aanzien van ADAS in personenauto's:

1. UN Regulation No.79, Addendum 78, Revision 4 '*Uniform provisions concerning the approval of vehicles with regard to steering equipment*' met ingangsdatum 18 oktober 2018 (verder aangeduid als UN R.79). Dit reglement behandelt ADAS die tijdelijk de stuurfunctie overnemen van de bestuurder. Deze worden Advanced Driver Assistance Steering Systems (ADASS) genoemd. De bestuurder kan ADASS altijd overrulen. Het reglement kijkt ook vooruit naar de toekomst met het oog op de mogelijkheid van zelfrijdende auto's zonder aanwezigheid van een bestuurder. De daarvoor benodigde systemen worden Autonomous Steering Systems (ASS) genoemd. Al worden ASS gedefinieerd in UN R.79, het is het op dit moment nog niet toegestaan om de autonome variant toe te laten op de weg en er zijn dus ook geen verdere technische eisen voor beschreven. Binnen ADASS maakt UN R.79 onderscheid tussen Automatically Commanded Steering Functions (ACSF)[196] en Corrective Steering Functions (CSF)[197]. ACSF zijn comfortsystemen die de bestuurder ondersteunen bij zijn primaire rijtaak. Het document verdeelt de ACSF onder in zes categorieën afhankelijk van hun functie (zie Tabel 8).

Categorie	Omschrijving
A	Een functie die werkt met een snelheid van niet meer dan 10 km/uur om de bestuurder bij te staan, op verzoek, bij manoeuvres bij lage snelheid of bij parkeeroperaties.
B1	Een functie die de bestuurder helpt het voertuig binnen de gekozen rijstrook te houden door de zijwaartse beweging van het voertuig te beïnvloeden.
B2	Een functie die wordt geïnitieerd / geactiveerd door de bestuurder en die het voertuig binnen zijn rijstrook houdt door de zijwaartse beweging van het voertuig gedurende lange perioden te beïnvloeden zonder verdere opdracht of bevestiging van de bestuurder.
C	Een functie die een enkele manoeuvre kan uitvoeren (bijvoorbeeld verandering van rijstrook) op bevel van de bestuurder.
D	Een functie die de mogelijkheid van een enkele manoeuvre (bijvoorbeeld verandering van rijstrook) kan aangeven, maar die functie alleen uitvoert na een bevestiging door de bestuurder.
E	Een functie die door de bestuurder wordt geactiveerd en die continu de mogelijkheid van een manoeuvre (bijvoorbeeld rijstrookverandering) kan bepalen en deze manoeuvres gedurende langere perioden kan voltooien zonder verdere opdracht of bevestiging van de bestuurder.

Tabel 8 - Categorieën ACSF volgens UN R.79.

196 Voorbeelden van ACSF zijn Lane Change Assist (Categorie C) , High way pilot (Categorie E) of ParkAssist (Categorie A).
197 Een voorbeeld van CSF is LDA (Lane Departure Avoidance).

Voor de ACSF categorieën A, B1 en C zijn al technische eisen opgesteld; voor B2, D en E moet dit nog worden gedaan. De bestuurder heeft de keuze om ACSF te gebruiken of niet en kan tijdens het rijden van keuze veranderen.
CSF zijn noodsystemen, die ingrijpen bij incidentele onverwachte veranderingen van de zijwaartse koers van de auto. Deze systemen zijn op de achtergrond altijd actief en grijpen incidenteel en kortdurend in (net zoals ABS en ESC). In het geval dat een CSF ingrijpt, moet een verklikkerlichtje gaan branden. Als een ingreep meer dan tien seconden duurt, moet als waarschuwing een geluidsignaal worden gegeven. Dit geluidsignaal stopt pas als de bestuurder zelf gaat sturen.

2. UN Reglement No. 130 'Uniforme voorschriften voor de goedkeuring van voertuigen wat het waarschuwingssysteem voor het onbedoeld verlaten van de rijstrook (LDWS) betreft' met 9 juli 2013 als datum van inwerkingtreding. LDWS geeft alleen een waarschuwing en grijpt niet in, wat een CSF wel doet.
3. Annex 6 '*Guideline on cybersecurity and data protection*' van de *Consolidated Resolution on the Construction of Vehicles* (R.E.3)[198] geeft een algemene richtlijn voor maatregelen ter waarborging van cybersecurity en gegevensbescherming van auto's met ADAS. Deze richtlijn verwijst naar goeddeels in andere branches ontwikkelde en toegepaste normen op het gebied van informatiebeveiliging (ISO 27000 serie), cybersecurity (ISO/IEC 15408) en de veiligheid van elektrische en elektronische systemen. Binnen WP.29 wordt gewerkt aan nieuwe voorstellen[199] op het gebied van cybersecurity en over-the-air (OTA) communicatie tussen (ADAS in) auto's en autofabrikanten bijvoorbeeld ten behoeve van het updaten van ADAS.

Binnen UNECE wordt door informele werkgroepen onder de GRVA gewerkt aan onder meer de voorbereiding van regulering op het gebied van EDR/DSSAD (*Event Data Recorder en Data Storage System for Automated Driving*)en AEBS voor personenauto's. Hierbij ligt de nadruk op systemen van SAE level 3 en hoger. In de 'roadmap' van WP.29 staan ook onderwerpen, die later nog ter hand moeten worden genomen, zoals de opleiding van bestuurders en de manier waarop voertuigen met ADAS gedurende hun levensduur moeten worden onderhouden en gekeurd.

198 UNECE, *ECE/TRANS/WP.29/78/Rev.6, Consolidated Resolution on the Construction of Vehicles (R.E.3)*, Revision 6, 2017.
199 UNECE, *ECE/TRANS/WP.29/GRVA/2019/2, Proposal for a Recommendation on Cyber Security*, 2019.

ONDERZOEKSRAAD
VOOR VEILIGHEID

Bezoekadres
Lange Voorhout 9
2514 EA Den Haag
T 070 333 70 00
F 070 333 70 77

Postadres
Postbus 95404
2509 CK Den Haag

www.onderzoeksraad.nl