Lichtkogel | 2016 | nr 1

> Robots in de openbare ruimte

> Trendwatch

Trenddossier van en voor professionals in Bereikbaarheid, Veiligheid en Leefbaarheid

INTERVIEW

Verkeersveiligheid, cybersecurity en aansprakelijkheid

Overzien we de risico's?

Door Ingrid Zeegers

Ze zeggen dat negentig procent van de verkeersongelukken wordt veroorzaakt door menselijk falen. Autonome voertuigen moeten zulke fouten voorkomen. Maar wat als er juist nieuwe risico's ontstaan? Hoe zit het met de verkeersveiligheid, cybersecurity en aansprakelijkheid? Wat maakt autonoom verkeer veilig? Drie experts aan het woord.

Verkeersveiligheid

Welke verkeersrisico's kunnen ontstaan door autonome voertuigen?

Hoogleraar Verkeersveiligheid Marjan Hagenzieker (TU Delft): "Het is de bedoeling dat autonome auto's het verkeer veiliger maken. Die winst komt er in de toekomst ook wel, maar het zal veel langer duren dan de mediahype nu suggereert. Er moeten nogal wat issues worden opgelost. De belangrijkste onzekere factor is het menselijk gedrag. Sociale interactie is in het verkeer cruciaal. Mensen nemen bijvoorbeeld beslissingen op basis van oogcontact met de andere bestuurder. Maar oogcontact met een persoon in een autonome auto, betekent iets heel anders dan oogcontact met een bestuurder die zelf in control is. De vraag wordt: hoe weet je straks met welk type voertuig je te maken hebt? Is het überhaupt zichtbaar of af te leiden dat het om een robot gaat? In de transitiefase krijgen we te maken met een mix van allerlei soorten voertuigen, van robots tot oldtimers. De vraag is hoe mensen omgaan met die grote variatie in soorten voertuigen op straat. Hoe beïnvloedt dat het gedrag en welke risico's kunnen er ontstaan? Dat moeten we de komende jaren gaan onderzoeken."

Interactie tussen robot en mens

"Meer concreet: het gaat ten eerste om het gedrag van de autonome auto zelf. Hoe communiceert het voertuig met andere verkeersdeelnemers en met voertuigen met andere software? Daarnaast gaat het om het gedrag van de 'bestuurder' van de autonome auto: is het überhaupt mogelijk dat mensen supervisie houden over een autonoom systeem, en tegelijkertijd in staat moeten zijn de rijtaak soms weer over te nemen? Hoe zit het dan met de taakbelasting? Vervolgens gaat het ook om het gedrag van de bestuurder van een gewone auto: hoe reageert die op een autonome auto die ander rijgedrag vertoont? Zal de bestuurder van een gewone auto bijvoorbeeld het bumperkleven van autonome voertuigen imiteren? Ten slotte gaat het om de interactie tussen robots en andere verkeersdeelnemers, zoals fietsers en voetgangers: nemen mensen meer risico omdat ze verwachten dat de robot toch wel stopt, of zijn ze juist voorzichtiger – wellicht té voorzichtig? Deze vragen nemen we mee in wetenschappelijk onderzoek, maar ook in de praktijktests die de komende jaren op de openbare weg zullen worden uitgevoerd."

Marjan Hagenzieker

Contact
e m.p.hagenzieker@tudelft.nl

Marjan Hagenzieker is gedragswetenschapper en als hoogleraar Verkeersveiligheid verbonden aan de TU Delft, faculteit CiTG, afdeling Transport & Planning. Daarnaast is ze wetenschappelijk adviseur bij SWOV (Stichting Wetenschappelijk Onderzoek Verkeersveiligheid).

Cyberveiligheid

Met welke risico's rond cybersecurity hebben autonome voertuigen te maken?

Cybersecurityspecialist Eric Luiijf (TNO): "Bij cybersecurity denken mensen vaak aan hackers, creatieve geesten die het leuk vinden om in te breken in een verkeerssysteem. Cyberrisico's gaan veel verder dan dat. Het gaat om onbewuste onveiligheid van ons allemaal. Het gaat om onze eigen cyberhygiëne. Stel, je brengt je autonome voertuig voor onderhoud naar de garage: wie controleert dan of de laptop van de monteur virusvrij is? Het gaat ook om techniek en software. ICT zit verstopt in de hele keten. Software heeft updates nodig. Wie is verantwoordelijk voor het onderhoud van de informatiebeveiliging? Daar denken fabrikanten meestal niet over na. En hoe rol je nieuwe softwareversies uit over heel veel autonome voertuigen tegelijk, terwijl er in het totale verkeerssysteem ook nog oude softwareversies operationeel zijn? Een voorbeeld. Laatst besloot een autofabrikant om 1,4 miljoen auto's terug te roepen naar de garage voor nieuwe software. Dat kan de leverancier eenmalig doen, maar niet zeven keer per jaar, en ook niet gedurende de >

jarenlange levenscyclus van het voertuig. Met andere woorden: als cybersecurity niet van meet af aan meegenomen wordt in het ontwerp van het hele systeem, is het dweilen met de kraan open."

Risico's

"Een complicerende factor in de beveiliging van autonome systemen is de hoge mate van connectiviteit. Alles is met iedereen verbonden. Informatie gaat over en weer via zowel lokale communicatienetwerken, telecomnetwerken als ook het internet. Dat maakt stelselmatige beveiliging van de data ingewikkeld, omdat de beveiligingsvraag besloten ligt in verschillende systemen. Zolang de software van autonome en met het internet verbonden voertuigen niet stelselmatig en op ketenniveau wordt beveiligd, bestaat er een groot onbewust en ongecontroleerd risico op het gebied van cyberveiligheid. En daarmee bestaat er ook een groot risico voor de veiligheid van personen. Dit is een aandachtspunt voor de hele systeemketen rondom autonome voertuigen: van fabrikanten, dealers, wagenparkbeheerders, wegbeheerders en wet- en regelgevers tot aan opleidingen toe."

Eric Luiijf

Contact
eric.luiijf@tno.nl

Eric Luiijf is principal consultant bescherming vitale infrastructuur bij TNO en expert beveiliging procescontrolesystemen en Smart Grids. Auteur van onder andere Cyber Security of Industrial Control Systems (2015).

Aansprakelijkheid

Als het autonome systeem faalt en er gebeuren ongelukken, wie is er dan aansprakelijk?

"Met de komst van automatische systemen ontstaan er nieuwe vragen", vertelt advocaat Anton Ekker (HeidemanBoot). "Zolang de bestuurder nog de uiteindelijke controle blijft houden over het voertuig zal hij op grond van de Wegenverkeerswet in de meeste gevallen aansprakelijk zijn voor de schade als gevolg van een ongeluk. Maar als de fout wordt veroorzaakt door een falend intelligent systeem, zal de bestuurder de claim kunnen doorschuiven naar de producent. Dan komt de productaansprakelijkheid om de hoek kijken. De autofabrikant is dan het logische eerste aanspreekpunt. Daarnaast is het denkbaar dat een fout wordt veroorzaakt door een falend positioneringssysteem of communicatienetwerk. Als de mens helemaal niet meer kán ingrijpen en feitelijk een passagier is, verandert de zaak. Dan is de situatie vergelijkbaar met een taxirit. Een passagier in een taxi is natuurlijk niet aansprakelijk voor schade als gevolg van een ongeluk. Maar de aanbieder van de taxidienst wel. In de toekomst gaan we het autonome voertuig mogelijk als een intelligent agent zien. Dat is een rechtspersoon die qua juridische status vergelijkbaar is met een stichting of een bv. Een intelligent agent is een rechtspersoon die zelf aanspra-

kelijk en ook verzekerbaar kan zijn."
Autonoom vervoer brengt ook nog andere, aanverwante juridische risico's met zich mee, zoals de bescherming van privacygevoelige informatie. Ekker: "Autonome voertuigen zijn nauwkeurig te volgen, niet alleen door de overheid maar ook door andere (commerciële) partijen. Gevleugelde uitspraak: kennis over personen is macht over personen. Op het internet zijn er speciale regels gemaakt voor het gebruik van cookies, zodat mensen zelf kunnen beslissen of ze door de markt gevolgd willen worden. Naar analogie daarvan zou je wellicht ook voor intelligente verkeerssystemen aanvullende regels moeten bedenken die persoonsgebonden informatie beveiligen. De automobilist moet straks zelf kunnen kiezen of hij gebruik wil maken van commerciële aanbiedingen in het voertuig of niet."

Vooruitblik

Wat moeten we nú doen voor een optimale veiligheid in de toekomst?

Nieuwe verkeersrisico's en inherente cybersecurityvraagstukken roepen de vraag op wat er moet gebeuren om autonoom verkeer straks veilig te krijgen.
Verkeersdeskundige Marjan Hagenzieker wijst op het belang van het menselijk gedrag en pleit voor (internationale) eisen aan de rijvaardigheden van de bestuurder: "Die moet niet alleen het voertuig kunnen besturen, maar ook supervisie kunnen houden op zelfrijdende systemen. Dat vraagt andere competenties. Rijopleidingen moeten daarop aangepast worden."
Cybersecurityspecialist Eric Luiijf vindt het hoog tijd voor risicoanalyses op ketenniveau: "Welke onacceptabele risico's ontstaan er als de cybersecurity niet geregeld is? En wie is er eindverantwoordelijk voor de beveiliging van geïntegreerde systemen die afkomstig zijn van vele verschillende partijen?"
Advocaat Anton Ekker: "We moeten nadenken over de vraag hoe gebruikers zeggenschap houden over hun data. En over de kwestie 'medische monitoring in het intelligente voertuig'. Er bestaan allerlei medische apps die scannen hoe het met een persoon gaat. Die komen wellicht ook in de auto terecht. Is de bestuurder wel alert, is hij gestrest, gaat het goed met hem? De vraag is of de bestuurder wel wil dat de auto een medische diagnose van hem stelt. Kortom, veilig autonoom verkeer gaat ook over persoonsbescherming, privacy en profileringsvraagstukken." <

Anton Ekker

Contact
e ekker@heidemanboot.nl

Anton Ekker is advocaat bij HeidemanBoot. Hij is gespecialiseerd in juridische aspecten van ICT, onder andere op vraagstukken rond e-health en kunstmatige intelligentie. Auteur voor onder andere Het Financieele Dagblad (2015).

Dit cahier is een uitgave van
Rijkswaterstaat.
Voor meer informatie kunt u
contact opnemen met de redactie
via lichtkogel@rws.nl

April 2016