Randvoorwaarden en gedeelde voorzieningen voor C-ITS

Een C-ITS-onderzoeksproject is nog relatief eenvoudig op te zetten: enkele basale data- en communicatievoorzieningen zijn vaak afdoende. Maar belanden we eenmaal in de fase van opschalen en uitrollen, dan kan van 'basaal' geen sprake meer zijn. Van data-uitwisseling tot governance – alles moet professioneel zijn georganiseerd en aan strenge kwaliteitseisen voldoen.

Voor een geslaagde uitrol van een C-ITS-dienst is het allereerst zaak om aan te haken bij *standaarden*, zowel qua interfacing als berichttypes. Standaarden zorgen voor een bredere adoptie, een betere werking en ze verkleinen bovendien de kans op een 'vendor lock-in'. Wat de berichten betreft zijn met name DATEX II en ETSI-standaarden als DENM en IVI relevant. DATEX II wordt vooral gebruikt voor het uitwisselen van real-time en semi-statische data, tussen bijvoorbeeld verkeerscentrales. De ETSI-standaarden richten zich meer op real-time communicatie waarbij zeer lage latency cruciaal is.

Waar geen bestaande standaarden zijn, bieden *standaardisatiecomités* een oplossing. Die zijn er op nationaal niveau, zoals in Nederland het NEN. Ook zijn er een aantal organisaties die *de facto* standaarden ontwikkelen: CROW, BISON, DVM-Exchange. Maar de echte afspraken komen natuurlijk van de internationale comités, zoals in Europa de CEN/TC 278.

Interessant is dat belanghebbenden als autoconstructeurs, navigatieproviders en onderzoekers vaak proactief toetreden tot die standaardisatiecomités. Dat gebeurt dan bijvoorbeeld in de context van een onderzoeksproject, waarin samenwerkingspartners nieuwe concepten ontwikkelen die mogelijk een uitbreiding of aanpassing van een standaard vereisen. Je kunt dan maar beter alvast aan tafel zitten bij zo'n comité, is de gedachte.

Data-uitwisseling

Al die C-ITS-data en -berichten moeten we vervolgens ook snel en betrouwbaar zien uit te wisselen binnen het mobiliteitsecosysteem. Dat vraagt om *uitwisselingsplatforms* van hoge kwaliteit met dito beschikbaarheid en inclusief kwaliteitsmonitoring. Zulke platforms zijn typisch voorzieningen die je centraal wil regelen. Voor elke C-ITS-dienst of -onderdeel separate voorzieningen treffen, werkt immers kostenverhogend. Aparte silo's hebben ook vaak verschillende kwaliteitskenmerken – en dat kan in de keten tot (kwaliteits)problemen leiden.

Zo'n breed uitwisselingsplatform moet een zekere neutraliteit hebben. Ook is belangrijk dat het eventuele businessmodel van het platform transparant is. Marktpartijen zullen namelijk niet graag data delen met platformen van concurrenten. Overheden willen weer zekerheid dat hun data niet voor oneigenlijke doelen wordt gebruikt.

Governance

Een derde 'voorziening' is een goede *governancestructuur*. C-ITS is nog volop in ontwikkeling en dat gaat vanzelf gepaard met vragen en dilemma's. Wie levert welke data aan? Wie neemt daarin het voortouw? Wie betaalt wat? Enzovoort. De belangen van publieke partijen enerzijds en private partijen anderzijds willen hierbij nog wel eens uiteenlopen. Door gezamenlijk geschikte 'spelregels' te bepalen, bijvoorbeeld over standaarden, toegang, rollen en rechten, kunnen die vragen ordentelijk worden beantwoord. Bij voorkeur zijn alle stakeholders in de governance vertegenwoordigd, zodat een goede belangenafweging kan plaatsvinden en het draagvlak voor data-uitwisseling groot blijft. In Nederland hebben we Mogin voor (onder meer) de governance van weggerelateerde data.

Zulke organen bepalen bijvoorbeeld welke partijen data mogen inbrengen en welke partijen onder welke condities toegang krijgen tot die data.

Security

Als het gaat om het professioneel organiseren van een C-ITS-dienst, dan is *security* natuurlijk een absoluut vereiste. Voor security in de meer brede zin – van ontwikkeling tot beheer – zijn er nog geen harde internationale standaarden ontwikkeld. Voorlopig moeten we dus uitgaan van nationale afspraken, voor zover die voor C-ITS relevant zijn. In Nederland heeft het Nationaal Cyber Security Centrum goede algemene security-adviezen opgesteld.
Verder is een ISO27001-certificering een minimale eis voor de technische partijen die actief zijn in de keten van C-ITS. (Nederlandse) overheden zullen moeten voldoen aan de BIO, Baseline Informatiebeveiliging Overheid. Ook regelmatige penetratietesten zijn van groot belang.

Dat er nog geen 'ketendekkende' internationale veiligheidsstandaarden zijn, wil natuurlijk niet zeggen dat er geen aandacht voor is. Het Europese automotive onderzoeksproject SECREDAS draait bijvoorbeeld geheel om security. Zeventig organisaties werken hierin samen om de voertuigen veiliger te maken (als in: minder vatbaar voor hacking) en er is daarbij aandacht voor de héle communicatieketen, essentieel voor C-ITS-toepassingen. Dit project geeft specifieke input aan bestaande standaardisatieorganisaties.

In Europa is verder voor de identificatie en authenticatie van het berichtenverkeer het European Union C-ITS Security Credential Management System uitgewerkt, met onder meer het C-ITS Point of Contact (CPOC) Protocol.
En aangaande authenticatie en encryptie is er veel vastgelegd binnen het Europese project C-Roads. Daarbij wordt onderscheid gemaakt tussen de opzet bij directe communicatie (directe verbinding tussen voertuig en wegkant) en de cellulaire opzet (communicatie via een cloudplatform). In Nederland wordt met name de cellulaire opzet gebruikt. Ook autofabrikanten, die zich eerst vooral op kortere-afstandscommunicatie (DSRC in ITS-G5) richtten, testen nu met het cellulaire 5G.

Privacy

Bij C-ITS-diensten worden vrijwel altijd locatiegegevens uitgewisseld, dus ook *privacy* verdient (professionele) aandacht. Een verdere uitdieping van alle privacyaspecten valt buiten de reikwijdte van dit artikel, maar laten we het erop houden dat het zeker de moeite loont om aan te sluiten bij bestaande ketens waar de privacyaspecten door specialisten beoordeeld en georganiseerd kunnen worden. Belangrijke organen in dit verband zijn de Autoriteit Persoonsgegevens in Nederland en de Gegevensbeschermingsautoriteit van België. Zij vertalen de Europese algemene verordening rond het recht op privacy naar nationaal niveau en bepalen aan welke voorwaarden je moet voldoen om toch bepaalde persoonlijke data te kunnen verzamelen. Denk aan het recht om vergeten te worden, al je data op te vragen, niet geïdentificeerd te kunnen worden enzovoort.

Conclusie

Het devies is om voor C-ITS-diensten gebruik te maken van professionele platformen waar kwaliteit, neutraliteit, governance, security en privacy geborgd zijn. Geen sinecure voor wegbeheerders die overwegen zelf aan de slag te gaan, maar in Nederland zijn er gelukkig al de nodige voorzieningen waar provincies en gemeentes gebruik van kunnen maken. Op het vlak van data en data-uitwisseling is er bijvoorbeeld het Urban Data Access Platform, UDAP, bedoeld voor *low latency* real-time data die beschikbaar moeten zijn binnen (milli)seconden. In Nederland stelt daarnaast het NDW Open Data Portal 'gewone latency' real-time data (over reistijden en files bijvoorbeeld) en statische data beschikbaar en is er Melvin voor informatie over wegwerkzaamheden. Deze platformen maken onderdeel uit van het Nationaal Toegangspunt Mobiliteitsdata en vallen, via het NDW, onder toezicht van de verzamelde wegbeheerders.

In België zijn de gewestelijke overheden hard aan het werk om soortgelijke voorzieningen op te zetten. Een voorbeeld hierin is de uitrol van het Mobilidata-platform. Mobilidata wil innovatieve verkeersoplossingen realiseren om zo het verkeer vlotter, duurzamer en veiliger te maken voor elke weggebruiker. Een centrale component is om in eerste instantie alle wegkantinformatie te gebruiken, en aansluitend alle mobiele informatie, zoals de communicatie tussen voertuigen en infrastructuur. Hiermee kan het verkeer gerichter gemanaged worden, met bijvoorbeeld time-to-green-diensten, dynamische snelheidsbeperkingen, doortochten van prioritaire voertuigen enzovoort.

Die platformen zijn belangrijk voor het opschalen en uitrollen, maar ze zijn net zo interessant voor kleinschalige pilots. UDAP biedt bijvoorbeeld de mogelijkheid om voor pilots en/of specifieke use cases data afgeschermd uit te wisselen via een apart datadomein. Rondom deze platformen bestaat ook al een levendige community van bedrijven die de nodige deskundigheid hebben opgebouwd aangaande C-ITS-diensten en data-uitwisseling. De basis is er dus – met alle mogelijkheden voor een efficiënt gebruik van bestaande voorzieningen en deskundigheid. ●

Meer informatie

- **ETSI** etsi.org/committee/its
- **DATEXII** datex2.eu
- **CEN/TC 278** itsstandards.eu
- **Mogin** mogin.ndw.nu
- **CPOC** cpoc.jrc.ec.europa.eu
- **Nationaal Cyber Security Centrum** ncsc.nl
- **BIO** bio-overheid.nl
- **SECREDAS** secredas-project.eu
- **C-Roads** c-roads.eu
- **UDAP** talking-traffic.com/nl/urban-data-access-platform
- **NDW Open Data** opendata.ndw.nu
- **Melvin** melvin.ndw.nu/public
- **Mobilidata** mobilidata.be

De auteurs
Menno Malta *is CEO van Monotch.*
Dr. Sven Maerivoet *is senior onderzoeker bij Transport & Mobility Leuven*