Smart Mobility Ronde Tafel Security

Concept jaarplan 2017
Versie 002 – 24 November 2016

Doelstelling

De landelijke ronde tafel Security heeft als doel om de kennis en de ervaring van security-onderwerpen in Smart Mobility-projecten te delen en te ontwikkelen. Dit is een belangrijke pijler voor de realisatie van de ambitie om de inzet van Smart Mobility op het Nederlandse wegennet op te schalen en te versnellen.

De doelstelling van dit jaarplan is om te inventariseren wat de gezamenlijke prioriteiten zijn van de stakeholdes van de ronde tafel en waar de ronde tafel een concrete bijdrage aan gaat leveren. Dit is de basis voor het uitvoeringsplan voor de security tafel in 2017.

Scope

In het kader van de ronde tafels omvat Smart Mobility zowel:

- cooperative driving (C-ITS, via Wifi-P/G5 communicatie)
- connected driving (via cellulaire communicatie of hybride met Wifi-P/G5)
- autonomous driving (al dan niet ondersteund met V2V-communicatie)

Mogelijke activiteiten en resultaten

1. Risico reductie overzichten voor smart mobility projecten

- In 2015 is gestart met het uitvoeren van risico analyses op Smart Mobility-projecten t.b.v. de C-ITS corridor en de A58 Spookfiles. De geïnventariseerde risico's en de bijbehorende mogelijke maatregelen worden gedocumenteerd in zgn. risico-reductie-overzichten (RRO's). Een RRO is een effectieve vorm om risico's en maatregelen te communiceren met betrokkenen en verantwoordelijken.
- De ronde tafel stimuleert het ontwikkelen van RRO's en het delen van RRO's tussen projecten. Dit levert een bijdrage aan de ontwikkeling en verspreiding van kennis tussen Smart Mobility-projecten over de omvang van de risico's en de effectiviteit van mogelijke maatregelen.
- Nieuwe Smart Mobility-projecten worden uitgenodigd om aan de ronde tafel en de RRO's deel te nemen. De ronde tafel kan projecten ondersteunen met het uitvoeren van de risico analyse.

2. Handreiking security t.b.v. smart mobility projecten

- De meeste smart mobility projecten en pilots zijn geen security projecten en hebben een impliciet vertrouwen dat de techniek (en de mensen) onder alle omstandigheden goed en volgens verwachting zullen functioneren. Het besef dat er wel degelijk risico's zijn, zoals hackers en tal van andere eventualiteiten, is latent aanwezig. Er is een toenemende behoefte en noodzaak om op een passende manier security in projecten mee te nemen. De crux is gepaste dosering: niet te veel en niet te weinig, niet te vroeg en niet te laat.
- In november 2015 heeft de Security tafel een korte handreiking ontwikkeld en gepubliceerd voor de gezamenlijke doelgroep van bestuurders, opdrachtgevers en opdrachtnemers van Smart Mobility-systemen. Hierdoor kan het onderwerp security beter worden geborgd in de projecten en de bij de projecten betrokken organisaties. Deze handreiking wordt regelmatig gedownload.
- In het najaar van 2016 heeft de Security tafel een reeks van security-vragen en antwoorden ontwikkeld voor de doelgroep security verantwoordelijken in C-ITS-projecten. Het voorstel is om

de vragen en antwoorden begin 2017 in de vorm van een handreiking beschikbaar te stellen *(mocht dit niet gereed zijn voor eind 2016)*

3. Vraagbaak Security

- Veelvoorkomende security-vragen zijn in het najaar 2016 geinventariseerd door de ronde tafel, voorzien van standaard antwoorden in de vorm van FAQ's en beschikbaar gesteld via de DITCM-site.
- De DITCM-website krijgt een ruimte waar security vragen kunnen worden gesteld en waar die worden beantwoord. Er is een email-adres beschikbaar: security@ditcm.eu
- Ad hoc-vragen zullen door het kernteam van de Security tafel worden behandeld. Na de beoordeling van nieuwe vragen worden die bij de FAQ's opgenomen.

4. PKI (public key infrastructure) voor C-ITS-diensten

- Voor het vertrouwen tussen ITS-stations (V2V en V2I) is door ETSI een PKI infrastructuur met gebruikmaking van digitale certificaten voorgesteld en gespecificeerd. Hiermee is in Nederland de eerste praktische ervaring opgedaan in het project A58 Spookfiles. De PKI-infrastructuur zal worden ingebracht in de (Hybride) testomgeving voor Smart Mobility in Brabant.
- De ronde tafel heeft vanwege enkele geconstateerde tekortkomingen van de C-ITS-standaard in 2016 het IFAL-voorstel ontwikkeld dat een aanvulling is op de standaard. Dit is ingebracht in de internationale werkgroepen Security (C-ITS platform, ETSI, C2C-CC). Begin 2017 wordt een eerste Proof of Concept gepland waarin IFAL in een kleine praktijkopstelling zal worden beproefd.
- Voor de ontwikkeling en toepassing van C-ITS-diensten in Nederland zal een PKI nodig zijn waarin de certificaten van ITS-stations (weginfrastructuur en voertuigen) worden gebruikt en beheerd. In 2016 heeft de security tafel een workshop PKI vertrouwensdiensten georganiseerd voor deelnemers van de ronde tafel en stakeholders. In 2017 zal de roadmap voor de ontwikkeling en uitrol van de PKI voor C-ITS een terugkerend onderwerp zijn aan de ronde tafel.
- De ronde tafel zal in 2017 initiatieven nemen en klankbord zijn voor de ontwikkeling van PKI certificate policies, zowel t.a.v. de verstrekking van certificaten aan C-ITS deelnemers als het operationele gebruik van zgn. pseudoniem certificaten.

5. Security testing, certificering en compliance van ITS-stations

- In Brabant wordt de Hybride test-omgeving voorbereid die vanaf 2017 ten dienste zal staan van Smart Mobility projecten die testcapaciteit en -faciliteiten nodig hebben. Een security-infrastructuur zal daar waarschijnlijk onderdeel van gaan uitmaken, in eerste instantie t.b.v. C-ITS.
- De ronde tafel heeft in 2016 een sessie georganiseerd om als klankbord te fungeren voor het project Hybride testomgeving. In 2017 zal de ronde tafel ook beschikbaar zijn als klankbord.
- Voor ITS-stations, zowel de voertuigen als de wegkant-infrastructuur, bestaan nog geen security standaards om de betrouwbaarheid van het ITS-station te beoordelen en vast te stellen. Binnen UNECE worden op voorstel van Nederland ook stappen gezet in de verbetering van security-eisen in reglementering. Deze ontwikkelingen moeten met elkaar verbonden worden. De rol en de bijdrage van de ronde tafel is nader te bespreken.

6. Coördinatie en Nederlandse bijdrage in internationale security-werkgroepen

- Het C-ITS platform van de EC heeft tot doel de introductie van C-ITS-services te bevorderen. De WG Security van het C-ITS platform heeft in 2016 de certificate policy opgesteld en een eerste concept voor de security policy. Vanuit Nederland is hierin deelgenomen door Connecting Mobility en de voorzitter van de ronde tafel. Hier is het IFAL-voorstel van Nederland ingebracht. De activiteiten in 2017 zullen gericht zijn op het prioriteren van ontbrekende en urgente vertrouwenselementen van het C-ITS ecosysteem, zoals monitoring, handhaving en revocatie.
- In de ETSI Werkgroep Security voor ITS is in 2016 Nederland toegetreden. De focus vanuit Nederland ligt in 2017 op het inpassen van IFAL in de ETSI-standaard alsook de ontwikkeling van de operationele use case policy voor het wisselen van pseudoniem certificaten vanwege privacy-eisen.
- De afstemming van Nederland met de C2C-CC werkgroep Security is in 2016 informeel gestart via enkele vertegenwoordigers van de industrie. Het voorstel is om de Nederlandse inbreng op deze wijze te continueren in 2017 wat betreft de bovenstaande voor Nederland prioritaire acties
- De ronde tafel zal in 2017 net als in 2016 bij elke bijeenkomst terugkoppeling ontvangen van de ontwikkelingen van de C-ITS standaard en policy-documenten. Tevens wordt de ronde tafel, net als in 2016, actieve inbreng gevraagd op specifieke urgente onderwerpen in de ontwikkeling van C-ITS.

7. Cellulaire ITS services versus Cooperative ITS services

- Pilot projecten en use cases maken in toenemende mate gebruik van zowel connected technologie op basis van 2G/ 3G/ 4G/ 5G cellulaire verbindingen als van coöperatieve technologie op basis van G5 Wifi-P verbindingen. De security impact en de security services van het gebruik van cellulaire technologie voor ITS zijn, ook internationaal, nog niet bepaald.
- In het project InterCOR zal Nederland met Frankrijk, UK en België een aantal interoperabele hybride use cases definiëren en vanaf najaar 2017 kleinschalig gaan testen. De ronde tafel Security heeft een rol als klankbord voor de ontwikkeling van het security framework voor InterCOR.
- Het onderwerp Cellulair vs Cooperatief en Hybride zal in 2017 naar behoefte van stakeholders en projecten voor discussie worden geagendeerd aan de ronde tafel.

8. Autonoom vervoer use cases

- De ontwikkeling van autonome voertuigen zal richting coöperatieve diensten gaan vanwege doelstellingen en randvoorwaarden voor efficiënt weggebruik, verkeersveiligheid en efficiënt brandstofgebruik. Bij truck platooning zal een betrouwbaar communicatieprotocol (en standaard) nodig zijn dat gebruikt gaat worden door de deelnemers aan de platoon. Hierbij kan C-ITS gebruikt worden maar ook dit is nog niet bepaald.
- De ontwikkeling van CACC – Cooperative Adaptive Cruise Control – komt primair uit de USA. Er is nog weinig bekend van de communicatie protocollen en de security eisen. Het voorstel is dat deze kennis wordt opgedaan en verspreid via de security tafel.
- De ronde tafel Security wil in 2017 een platform bieden voor belanghebbenden in Truck platooning pilots om het noodzakelijke en gewenste security kader te bespreken.

9. Data protectie en privacy

- In 2017 zullen de ronde tafels Security en Juridische aspecten evenals in 2016 samenwerken op het onderwerp Data protectie i.h.b. Privacy by Design.
- In het voorjaar van 2017 zal een workshop Privacy by Design worden georganiseerd voor een specifieke Smart Mobility use case. Het doel is om via een of meerdere workshops te komen tot een de facto best practice voor opdrachtgevers, opdrachtnemers en dienstaanbieders in Smart Mobility. Dit levert een bijdrage aan het noodzakelijke vertrouwen van burgers en politiek in Nederland in slimme data- en communicatietoepassingen in het verkeer.
- T.b.v. het C-ITS platform werkgroep Privacy is het voorstel vanuit Nederland om een Privacy by Design-casus te ontwikkelen met een of twee automotive fabrikanten voor een of twee compelling C-ITS use cases. Het doel hiervan is om te doen in het kader van het goedkeuringstraject van de Europese DPA's voor V2V- of V2I-toepassingen. De planning is begin 2017.

10. Hackathon ITS-systemen

- De effectiviteit van security maatregelen kan in de praktijk onder nauwe randvoorwaarden goed getest worden door een ingehuurd team van hackers. De security tafel is een goed platform om ervaringen met hacking-opdrachten en de inzichten in kwetsbaarheden in ITS-systemen te delen.
- Daarnaast kan het organiseren van een hackathon een goede bijdrage zijn aan de bewustwording van het belang van security bij stakeholders van ITS-toepassingen.

11. Documentatie

- De DITCM site zal in 2017 net als in 2016 de documentatie van internationale publicaties over security van ITS-systemen faciliteren. De deelnemers van de tafel krijgen toegang tot alle documentatie en kunnen zelf ook documenten, white papers, artikelen en presentaties plaatsen.

12. Risico repository

- Om de toepasbaarheid van de kennis van en de ervaring met risico's en security maatregelen van ITS-systemen te bevorderen en te borgen, is een registratie van risico's noodzakelijk. Het hulpmiddel hiervoor is een register of een repository. Dit is tevens een hulpmiddel om RRO's van projecten en systemen te evalueren en actueel te houden.
- Het voorstel is om in 2017 met Smart Mobility stakeholders te overleggen hoe kennis en informatie uit risico-registers van Smart Mobility projecten kan worden ontsloten wat betreft security-risico's.

13. Communicatie en bewustwording

- In de meeste ITS-projecten wordt pas in een laat stadium aandacht besteed aan de noodzaak van security maatregelen en de risico's als security maatregelen ontbreken of ontoereikend zijn. Naast de praktische instrumenten, zoals de RRO's en Projecthandreikingen, is er meer nodig om opdrachtgevers bewust te maken van de risico's die zij lopen met hun project en de (bestuurlijke) verantwoordelijkheid die zij hebben voor het beheersen van risico's.
- Een informatiecampagne is zeer gewenst om bestuurders en opdrachtgevers te bereiken. Evenzo is bewustwording gewenst en noodzakelijk bij opdrachtnemers en projectuitvoerenden zoals

projectmanagers en systeemarchitecten. Hierbij kan in 2017, net als in 2016, gedacht worden aan publicaties in vakbladen en spreekbeurten.

- Het voorstel is, na een verkenning in 2016 uitgevoerd met communicatie-stakeholders van I&M, om in het voorjaar van 2017 met en voor stakeholders in mobiliteit een workshop "Communicatie over risico's – wat als het fout gaat?" te organiseren. Het voorstel is zowel de leden van ronde tafel Security als van Human Behavior bij deze workshop te betrekken.

14. Monitoring en opsporing van misbruik van C-ITS

- Voor C-ITS is nog geen systeem voorzien dat op een geavanceerde manier ongewenst en onbedoeld gebruik van het G5-radiospectrum en de C-ITS infrastructuur signaleert en rapporteert.
- Om deze ontwikkeling te versnellen wordt in januari 2017 een gezamenlijke sessie georganiseerd met de HSD (Hague Security Delta) en Automotive Campus NL. Het doel is om met strategische partners en stakeholders van de Ronde tafel, HSD en Automotive Campus te verkennen waar synergie is te halen en investeringsmogelijkheden voor de ontwikkeling van een monitoringsysteem voor misbruik ("misbehavior monitoring"). Op basis van de uitkomst van deze sessie zal een nader plan worden gemaakt en worden ingebracht in de internationale gremia voor de ontwikkeling van C-ITS.

15. Security-wetgeving

- Begin 2016 is het wetsvoorstel Computercriminaliteit III aan de ronde tafel besproken vanwege de mogelijke impact van de hack-bevoegdheid van politie in voertuigdevices. De behandeling van het wetsvoorstel zal waarschijnlijk niet voor 2017 zijn.
- In 2016 is in de EU de NIS directive (NIB richtlijn) aangenomen die lidstaten verplicht om uiterlijk begin 2018 security eisen te implementeren in nationale wetgeving voor kritische maatschappelijke processen en sectoren, waaronder mogelijk verkeer en vervoer.
- Het voorstel is om wetgevingstrajecten die impact hebben op de security (eisen) van Smart Mobility door de ronde tafel te laten monitoren en ad hoc te bespreken, dit in samenwerking met de ronde tafel juridische aspecten.