Leading partners in Smart Mobility

DITCM Innovations

Smart Mobility ronde tafel Security

JAARPLAN 2016

GJA
DITCM INNOVATIONS | WWW.DITCM.EU
JAARPLAN 2016

Smart Mobility ronde tafel Security

Doelstelling

De landelijke ronde tafel Security heeft als doel om de kennis en de ervaring van security-onderwerpen in C-ITS-projecten te delen en te ontwikkelen. Dit is een belangrijke pijler voor de realisatie van de ambitie om de inzet van C-ITS 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 opdrachtgevers en deelnemers aan de tafel en waar de tafel een concrete bijdrage aan gaat leveren. Dit is de basis voor het uitvoeringsplan voor de security tafel in 2016.

Scope

In het kader van de security tafel is C-ITS niet beperkt tot cooperative driving. Ook connected driving, autonomous driving en combinaties zijn onderwerp van Smart mobility en worden in deze tafel besproken.

Mogelijke activiteiten en resultaten

1. Risico reductie overzichten voor smart mobility projecten

- In 2015 is gestart met het uitvoeren van risico analyses op C-ITS projecten t.b.v. de C-ITS corridor en de A58 Spookfiles. Voor IVRI wordt begin 2016 een risico analyse gepland.
- 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 tafel stimuleert het ontwikkelen en delen van RRO's tussen projecten. Dit levert een bijdrage aan de ontwikkeling en verspreiding van kennis tussen C-ITS-projecten over de omvang van de risico's en de effectiviteit van mogelijke maatregelen in C-ITS.
- Nieuwe C-ITS- en mobiliteits-projecten worden uitgenodigd om aan de security tafel en de RRO's deel te nemen. De security 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.
- Het gaat om een scala aan onderwerpen als planning en timing van security maatregelen, uitvoering van risico analyses, omvang van security maatregelen, rollen en verantwoordelijk-

heden van opdrachtgever en opdrachtnemer, het meenemen van security in het programma van eisen, beveiliging van persoonsgegevens (privacy), communicatie over security en regie.

- In november 2015 heeft de Security tafel een korte handreiking ontwikkeld en gepubliceerd voor de gezamenlijke doelgroep van bestuurders, opdrachtgevers en opdrachtnemers van ITS-systemen. Hierdoor kan het onderwerp security beter worden geborgd in de projecten en de bij de projecten betrokken organisaties.
- Het plan is om in 2016 een handreiking op te stellen en uit te brengen voor de doelgroep security verantwoordelijken in ITS-projecten. De handreiking zal praktisch zijn en best practices bevatten die aanbevolen worden om in ITS-projecten toe te passen.

3. Vraagbaak Security

- De DITCM-website krijgt een ruimte waar security vragen kunnen worden gesteld en waar die worden beantwoord.
- Veelvoorkomende vragen worden voorzien van standaard antwoorden in de vorm van FAQ's.
- 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.
- In het C-ITS platform WG 5 van de EC is in 2015 een voorstel voorbereid voor de inrichting van het trust model voor de PKI. Het voorstel wordt volgens planning begin 2016 afgerond.
- 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. Hiertoe zijn op dit moment geen activiteiten gepland. Te bespreken zijn de mogelijke road map voor de totstandkoming van een PKI voor C-ITS-diensten, de bijdrage die de tafel daar aan kan leveren en de timing.

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

- 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 ISO wordt hier aan gewerkt net als in WG5 van het C-ITS platform van de EC.
- 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 tafel is nader te bespreken.

6. Coördinatie van de Nederlandse bijdrage in WG5

- Het C-ITS platform van de EC heeft tot doel de introductie van C-ITS-services te bevorderen. De industrie neemt actief deel in dit platform. WG5 is de security werkgroep. Vanuit Nederland is hierin deelgenomen door Connecting Mobility, RWS en RDW.
- WG5 heeft de volgende voorstellen uitgewerkt die allen begin 2016 zullen worden afgerond.
    - PKI trust model
    - revocatie van certificaten

- crypto agility
- certificering en compliance

- In 2016 zal WG5 wellicht opgaan in de op te richten organisatie voor E-SCMS (European C-ITS Security Credential Management System).
- Het voorstel is om de Nederlandse inbreng te structureren via de security tafel. Te bespreken is hoe dit in 2016 te organiseren.

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 cellulaire verbindingen als van coöperatieve technologie op basis van G5 Wifi-P verbindingen. De security impact van het gebruik van cellulaire technologie voor ITS is nog niet bekend.
- Zowel op het gebied van risico-analyses als security standaarden is nader inzicht gewenst. Een relevante bron is het Converge project in Duitsland. In Nederland heeft TNO een eerste onderzoek uitgevoerd naar de impact van cellulaire technologie op alle aspecten van ITS.
- Dit onderwerp kan op korte termijn voor discussie worden geagendeerd aan de security tafel.

8. Autonoom vervoer use cases

- De ontwikkeling van autonome voertuigen gaat richting coöperatieve diensten vanwege doelstellingen en randvoorwaarden voor efficiënt weggebruik, verkeersveiligheid en efficiënt brandstofgebruik.
- 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.
- Voor autonoom vervoer gaan in 2016 in Nederland de eerste pilots plaatsvinden zoals de Truck Platooning challenge. De security tafel biedt een platform om de doelstelling van de pilot en het noodzakelijke security kader te bespreken.

9. Data protectie en privacy

- Anticiperend op de privacy impact van C-ITS diensten zijn bij de ontwikkeling van C-ITS standaards zowel de principes van privacy by design als security by design toegepast. Een resultante hiervan is de grote hoeveelheid en de snelle roulatie van digitale certificaten.
- Voor de toekomstige praktijk van C-ITS-diensten is er behoefte aan richtlijnen voor het gebruik van deze certificaten. Het gaat hierbij allereerst om inzicht in de keuzes en impact van diverse gebruiksscenario's en de verwerking en opslag van C-ITS-berichten.
- Het voorstel is om in 2016 onderzoek te laten uitvoeren naar verschillende scenario's van het gebruik van deze certificaten.
- De security tafel en de juridische tafel zullen in 2016 structureel samenwerken op het onderwerp privacy en data protectie. Speerpunt van de samenwerking is de bevordering van de toepassing van privacy by design en security by design binnen ITS-projecten.

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 gaat 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.
- Eind 2014 is een nederlandse White paper opgesteld en gepubliceerd over Cyber security en Privacy aspecten in Cooperative en Connected mobility.
- Het voorstel is om het White paper in 2016 te herzien en te actualiseren vanwege nieuwe ontwikkelingen en use cases. Dan wordt het een actueel overzicht van de kennis- en onderzoeksagenda gekoppeld aan de documentatie op de DITCM-site.

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.

13. Communicatie en bewustwording

- In de meeste ITS-projecten wordt in een te laat stadium aandacht besteed aan de noodzaak van security maatregelen en de risico's als security maatregelen ontbreken. 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. Het voorstel is om in het voorjaar van 2016 een plan op te stellen om bestuurders en opdrachtgevers te gaan bereiken. Evenzo is bewustwording gewenst en noodzakelijk bij opdrachtnemers en projectuitvoerenden zoals projectmanagers en systeemarchitecten.
- Het voorstel is om de bewustwordingscampagnes te koppelen aan het gereed komen en het publiceren van de eerder genoemde Security- handreikingen en andere opleveringen van de Security tafel. Hierbij kan gedacht worden aan publicaties in vakbladen en spreekbeurten.