Opdrachtomschrijving werkgroep veiligheid

Versie: 2.1 (uitbreiding scope)

Datum: september 2020

Aanleiding

In het Klimaatakkoord is elektrisch vervoer één van de vier pijlers van het mobiliteitsbeleid. In 2030 zullen naar verwachting alle nieuwe personenauto's zero emissie zijn. Een groot deel hiervan zal bestaan uit batterij-elektrische auto's. Het is de ambitie van de Nationale Agenda Laadinfrastructuur om ervoor te zorgen dat het laden van elektrische voertuigen in Nederland net zo makkelijk is als het laden van een mobiele telefoon. Dit is noodzakelijk om te zorgen dat het voor de consument aantrekkelijk is om nu én in de toekomst elektrisch te rijden en daarbij overal in Nederland op een eenvoudige en een eenduidige manier gebruik te kunnen maken van de laadinfrastructuur.

Veiligheid met rijden en opladen van elektrische auto's is belangrijk om ervoor te zorgen dat er geen belemmeringen ontstaan bij de uitrol. Het gaat daarbij zowel om fysieke veiligheid, zoals voertuigveiligheid, veilig werken met elektrische installaties en brandgevaar, als om digitale veiligheid ofwel cyber security (CS).

De Werkgroep Veiligheid richt zich op zowel fysieke als digitale veiligheid.

De opdracht aan de werkgroep

De werkgroep veiligheid draagt bij aan het faciliteren van een veilig gebruik en veilig opladen van elektrische voertuigen in Nederland waardoor elektrisch vervoer wordt gestimuleerd.

Dit doet de werkgroep aan de hand van de volgende type werkzaamheden:

- het identificeren van risico's op basis van onderzoek en ervaringen in de praktijk;
- inventarisatie van bestaande of aankomende wet- en regelgeving en witte vlekken;
- het opstellen van advies voor aanvullende maatregelen of aanpassing van bestaande normen en/of wet- en regelgeving;
- het zorgen voor de ontwikkeling van noodzakelijke nieuwe kennis en het verspreiden van kennis bij verschillende doelgroepen.

De werkgroep hanteert hierbij de volgende drie uitgangspunten:

1. Samen zorgen we voor een veilige setting zodat iedereen zijn inbreng kan hebben;
2. We delen zo open mogelijk alle relevante informatie en stukken afhankelijk van de grenzen die door de eigen organisatie gesteld worden;
3. Stukken worden niet buiten de werkgroep gedeeld tenzij dit expliciet is afgesproken binnen werkgroep (bijvoorbeeld ter consultatie bij de achterban).

De werkgroep voert voor de fysieke veiligheid en cyber security in ieder geval de volgende acties uit.

Fysieke veiligheid

- Vergaren van kennis (binnen- en buitenland) over de veiligheid m.b.t laadinfra en laadprocessen en de wet- en regelgeving op dit gebied.
- Aanbevelingen doen voor maatregelen om de technische veiligheid van elektrisch laden en rijden verder te borgen.
- Begeleiding van het onderzoeksbureau bij het opstellen van de Factsheet veiligheid elektrisch vervoer en het leveren van input.
- Begeleiding onderzoeksbureaus bij vervolgonderzoek op het gebied van veiligheid wanneer er nog vragen open blijven in de Factsheet en het uitvoeren van andere acties die volgen het de Factsheet.
- (Afstemming van) communicatie over veilig realiseren/ gebruiken en onderhouden van laadinfrastructuur. Hiervoor worden factsheets opgesteld die o.a. via de NAL samenwerkingsregio's, brancheverenigingen, NKL en ElaadNL verspreid zullen worden.
- Leveren van input aan specifieke doelgroepen zoals hulpdienstverleners en veiligheidsadviseurs ten behoeve van risicobeheersing.

Cyber security

- Beschrijving van de CS-risico's in de keten van laden.
- In kaart brengen welke maatregelen genomen moeten worden op het gebied van CS.
- Beschrijving van de manier van borging van deze maatregelen (regelgeving, normen) en waar deze ontbreekt.
- Beschrijving van het gewenste handhavingsproces (testen, certificeren, toezicht).
- Het opstellen van aanbevelingen aan beleidsmakers voor ontbrekende regelgeving in Nederland en eventueel vanuit Brussel.
- Zorgen voor bewustwording bij beleidsmakers, marktpartijen en eindgebruikers. Communicatie richting contractmanagers en bedrijven.

Beoogde producten van de werkgroep Veiligheid

- Een overzicht van beschikbare kennis van onderwerpen binnen elektrisch vervoer ten aanzien van fysieke en digitale veiligheid.
- Factsheets en handreikingen voor verschillende doelgroepen (o.a. gemeenten, bedrijven, consumenten, garagehouders) over veilige installatie en gebruik van laadinfrastructuur.
- Inventarisatie en publicatie van eisen voor laadinfrastructuur, zowel op het gebied van fysieke veiligheid als op het gebied van cyber security.
- Aanbeveling voor borging van deze eisen in beleid, normen, producteisen en wet- en regelgeving.
- Aanbevelingen voor het handhavingsproces, zowel voor fysieke veiligheid als voor cyber security.

Rapportage en verantwoording

De werkgroep adviseert de stuurgroep Nationale Agenda Laadinfrastructuur en het Formule E-Team. Belangrijke producten worden voor akkoord of besluitvorming voorgelegd aan de stuurgroep NAL en het Formule E-Team. Andere producten worden ter informatie gedeeld.

Scope van de opdracht

De focus van de Werkgroep Veiligheid is in eerste instantie gericht op de onderwerpen waar nog kennislacunes zijn of waar veel vragen over zijn bij bedrijven en organisaties die bezig zijn met elektrisch vervoer. Vaak zijn dit veiligheidsaspecten die specifiek zijn voor elektrische voertuigen in vergelijking met conventionele voertuigen.

Scope fysieke veiligheid
Om te bekijken waar de kennislacunes zich bevinden wordt door CE Delft, in opdracht van RVO een factsheet veiligheid elektrisch vervoer opgesteld. Met deze factsheet wordt ook een nadere invulling gegeven aan de scope van de werkgroep. Onder de fysieke veiligheid verstaat de werkgroep de volgende veiligheidsaspecten van elektrisch rijden en laden:

a. Voertuigveiligheid van batterij-elektrische voertuigen
b. Verkeersveiligheid
c. Onderhoud en veiligheid
d. Brandveiligheid, incl afgesloten ruimtes
e. Te water geraking
f. Beschadiging batterij
g. laadinfrastructuur
h. Incident management

a. Voertuigveiligheid van batterij-elektrische voertuigen
Het gaat hierbij vooral om de componenten die specifiek zijn voor elektrische voertuigen, waaronder de batterij en het BMS.

Elektrische voertuigen zijn voertuigen die middels een stekker kunnen worden opgeladen. Het gaat dus zowel om volledig elektrische voertuigen (ook wel batterij-elektrische voertuigen (BEVs)) als plug-in hybride voertuigen (PHEVs). In eerste instantie richt de werkgroep zich op elektrische voertuigen die op kenteken staan/mogen worden gezet, en dus op de openbare weg mogen rijden.
De focus ligt hierbij op elektrische personenauto's, echter indien bevindingen ook relevant zijn voor andere voertuigtypen (denk aan bestelauto's, tweewielers, bussen en vrachtwagens) dan zal de werkgroep zorgen voor agendering bij de betreffende gremia. Brandstofcel-elektrische voertuigen (ook wel waterstofvoertuigen) worden ook als elektrische voertuigen aangemerkt maar vallen buiten de scope van deze werkgroep.

b. Verkeersveiligheid
Het gaat bij verkeersveiligheid om de aspecten die specifiek zijn aan elektrische voertuigen, zoals het ontbreken van geluid en ook de geavanceerde veiligheidssystemen (AVAS) die elektrische auto's vaak hebben en wat een positieve bijdrage levert aan de verkeersveiligheid. Uit de factsheet veiligheid elektrisch vervoer moet blijken of hier nog aandachtspunten liggen voor de werkgroep.

c. Onderhoud en veiligheid
Dit onderwerp is al opgepakt door de branche. Uit de factsheet veiligheid elektrisch vervoer moet blijken of hier nog aandachtspunten liggen voor de werkgroep.

d. Brandveiligheid, inclusief afgesloten ruimtes
Het gaat om specifieke aspecten voor elektrische voertuigen en de bijbehorende laadinfrastructuur. De recente aandacht voor de veiligheid van elektrische auto's en laadinfrastructuur in parkeergarages is onderdeel van de brandveiligheid.

e. Te water geraking
Uit de factsheet veiligheid elektrisch vervoer moet blijken of hier nog aandachtspunten liggen voor de werkgroep.

f. Beschadiging batterij
Uit de factsheet veiligheid elektrisch vervoer moet blijken of hier nog aandachtspunten liggen voor de werkgroep.

g. Laadinfrastructuur
De Werkgroep Veiligheid is gekoppeld aan de NAL en zal daarom veel aandacht besteden aan veiligheidsonderwerpen die met laadinfrastructuur te maken hebben. Veiligheidsaspecten waar de werkgroep zich op richt zijn:

- Veiligheid van de laadinfrastructuur en de achterliggende elektrische (huis)installatie;
- Borging van veiligheid in regelgeving, protocollen, handreikingen e.d.;
- Veiligheid van laden in de gebouwde omgeving.;
- Gebruik van laadinfrastructuur door de EV-rijder en professionals, zoals dealers, monteurs.

Laadinfrastructuur voor elektrische voertuigen kent verschillende typen en verschijningvormen en maakt gebruik van verschillende laadtechnieken.

Type laadinfrastructuur
- Publieke en semi-publieke/private laadpunten.
- Inpandig (o.a. in parkeergarages) en in de buitenlucht.

Verschijningsvormen
- Reguliere laadinfrastructuur (zoals de 'reguliere laadpaal' en snelladers).
- De Verlengd Private Aansluiting d.w.z. een laadpunt in de openbare ruimte dat d.m.v. een ondergrondse kabel wordt aangesloten op de meterkast van een nabije woning of bedrijfspand.
- Andere vormen van laadinfrastructuur (laadlantaarns, Streetplug enz, zie andersladen.nl).
- Zowel 'stekkerladen' als gebruik van alternatieve connectoren bijv. een pantograaf.

Soorten laadtechniek
- De laders van LEV's en andere elektrische twee- en driewielers.
- Gebruik van een 'granny lader' (IEC 61851 mode 2) voor EV's die wordt aangesloten op een normale wandcontactdoos. Soms sluit men deze lader, al dan niet met een verlengsnoer, aan op een inpandige wandcontactdoos waarbij de kabel door de brievenbus of het keukenraam naar buiten wordt gebracht. Buiten loopt de laadkabel soms over het trottoir heen. Soms worden granny laders inpandig gebruikt bijv. in autoshowrooms.
- Normaal (IEC 61851 mode 3) AC-laden.

- DC-snelladen, zowel voor personenauto's als voor heavy duty voertuigen. Het outputvermogen van een DC-lader kan uiteenlopen van 50 tot 600 kW (in de toekomst zullen nog hogere vermogens gebruikt gaan worden).
- Mobiele laadoplossingen, bijvoorbeeld in de bouw of bij evenementen.
- Inductieladen.
- V2G-laders.

h. Incidentmanagement

Bij elk van de genoemde veiligheidsaspecten moet bekeken worden of het incidentmanagement in orde is. Uit de factsheet veiligheid elektrisch vervoer moet blijken of hier nog aandachtspunten liggen voor de werkgroep en waar extra onderzoek nodig is.

Scope cyber security

De scope voor cyber security (CS) betreft de gehele keten van het laden: van de laadpas of -app tot en met de backoffice van de CPO en de interfaces met de partijen die stuursignalen voor smart charging verzenden (zoals netbeheerders, energieleveranciers en beheerders van energiemanagementsystemen).

De hoofddoelstelling op voor CS is: *Het waarborgen van netstabiliteit, toegankelijkheid en bescherming van (persoons-) gegevens door middel van de definitie van Europese (cyber-)security eisen om manipulatie en onrechtmatige toegang tot laadinfrastructuur te voorkomen.*

Specifiek gaat het voor de werkgroep om de volgende CS-aspecten:

- De interface gebruiker-laadpunt (met laadpas of app).
- De interface tussen laadpunt en voertuig (bij gebruik van een laadkabel maar ook van een pantograaf, bij inductieladen enz.).
- Bescherming van het laadpunt tegen indringing.
- De interface tussen laadpunt en back end van de CPO (inclusief de verbinding zelf).
- Voorkomen dat de firmware van een laadpunt tijdens opslag en transport gewijzigd kan worden.
- De toegangsmogelijkheid voor de laadpuntfabrikant ná installatie.
- De interfaces tussen laadpuntexploitanten, mobility service providers en roaming platforms (ook internationaal).
- De interface tussen CPO en netbeheerder (of andere smart charging partij).
- Bescherming tegen indringing van de systemen van laadpuntexploitanten, mobility service providers en andere partijen in de laadketen.

Samenstelling van de werkgroep

De werkgroep bestaat uit een werkgroep gericht op fysieke veiligheid. Daaronder hangt een speciale taakgroep cyber security. Paul Broos (ElaadNL) fungeert als linking pin tussen de taakgroep CS en de werkgroep veiligheid. Zowel de werkgroep als de taakgroep komen maandelijks bijeen om de voortgang te bespreken. Alle informatie over de werkgroep is te vinden op https://agendalaadinfrastructuur.pleio.nl/.

Deelnemers Werkgroep fysieke veiligheid

Stakeholder	Stakeholder vertegenwoordiging
Netbeheerders	ElaadNL
EV sector	Vereniging DOET
Kennisinstelling EV	NKL
Rijksoverheid/ uitvoering	RWS
Rijksoverheid/ ministerie	IenW
Rijksoverheid/ uitvoering	RVO
Gemeenten	Gemeente Rotterdam
Kennisinstelling veiligheid	IFV
Provincies	Provincie Utrecht
Automotive	RAI Vereniging

Deelnemers NAL taakgroep Cyber Security

Stakeholder	Stakeholder vertegenwoordiging
Netbeheerders	ElaadNL
Rijksoverheid	JenV
Rijksoverheid	EZK
Rijksoverheid/ uitvoering	RVO
Europees kennisinstituut	ENCS
Laadpuntfabrikant	Alfen
CPO	Last Mile Solutions
EMSP	Ntb

Planning

Voor de werkgroep is de oplevering van de factsheet met de aanbevelingen in oktober 2020 een belangrijk ijkmoment. Dan kan bepaald worden waar kennislacunes zitten en aanvullend onderzoek nodig is. Ook zal voor specifieke onderwerpen een aantal verdiepende expertsessies georganiseerd worden om meer inzicht te krijgen. De kennis zal gedeeld worden met verschillende doelgroepen in de vorm van Q&A's, factsheets etc.

Veel aandacht gaat op dit moment naar de brandveiligheid van elektrisch laden in parkeergarages. Brandweer Nederland heeft een eerste advies uitgebracht en het IFV heeft op 9 juli 2020 een studie met brandveiligheidsmaatregelen voor parkeergarages uitgebracht. In september wordt naast de

factsheet van de werkgroep een onderzoeksrapport naar een recente brand in een parkeergarage gepubliceerd.

Vanuit de NEN wordt onder de nieuwe integrale norm voor brandveiligheid in ondergrondse parkeergarages na de zomer een werkgroep gestart die zich specifiek richt op alternatief aangedreven vervoer. Het doel is om binnen de integrale norm een specifieke module te maken voor onder meer elektrisch vervoer. De nieuwe norm zal rond 1 januari 2022 gepubliceerd worden. De werkgroep veiligheid zal de ontwikkelingen binnen deze NEN werkgroep volgen en waar nodig input leveren.

Globale planning van de acties en resultaten 2020-2021

Onderstaande planning voor fysieke veiligheid wordt op basis van de aanbevelingen bij de factsheet verder uitgewerkt en verfijnd. Ook wordt een planning voor cyber security opgenomen.

	Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021	Q4 2021
Opdrachtomschrijving definitief maken							
Begeleiding onderzoeksbureau/ leveren kennis en input							
Factsheet EV en veiligheid definitief							
Factsheets en handreikingen voor veilig gebruik laadinfra							
Eisen voor laadinfrastructuur op papier							
Aanbevelingen voor borging							
Beschrijving handhavingsproces							

In onderstaande tabel staat de voorlopige planning van de taakgroep cybersecurity.

Activiteit	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021	Q4 2021
Uitwerking: bescherming tegen indringing van de systemen van CPO's, EMSPs en andere partijen in de laadketen.						
Extern onderzoek geselecteerde onderwerpen						
Bescherming van het laadpunt tegen indringing (praktijkervaringen en evaluatie)						
Papers/handreikingen opstellen						
Adviezen aan MinJenV en EU opstellen						

Bijlage: afspraken in de NAL en het Klimaatakkoord ten aanzien van veiligheid

Fysieke veiligheid
Op het gebied van fysieke veiligheid zijn geen specifieke actiepunten opgenomen in de NAL.

Cyber security
Op het gebied van cyber security zijn wel specifieke actiepunten opgenomen in de NAL:

- Het ministerie van Infrastructuur en Waterstaat zorgt i.s.m. ElaadNL en andere ministeries dat er in 2020 afspraken zijn gemaakt over cyber security voor de laadinfrastructuur . Zo moeten er maatregelen worden genomen en processen ingericht om adequaat te kunnen reageren op mogelijke cyberaanvallen op de laadinfrastructuur.
- Het ministerie van Infrastructuur en Waterstaat neemt het voortouw om voor 2020 afspraken te maken over cyber security voor de laadinfrastructuur.
- De overheid en de marktspelers stimuleren de vorming van een neutraal Europees instituut voor de informatiebeveiliging van de laadinfrastructuur, zoals het European Network for Cyber Security (ENCS).
- Er is behoefte aan een ‘Roadmap cyber security EV’. Daarbij moet er aandacht zijn voor het feit dat indien het door CPO’s beheerde vermogen boven een bepaalde grens komt, het laadpalennetwerk als een vitale infrastructuur beschouwd wordt. Hier wordt de NIB richtlijn (netwerk- en informatieveiligheid richtlijn) van toepassing. Bovendien moeten maatregelen worden genomen en processen ingericht om adequaat te kunnen reageren op mogelijke cyberaanvallen op de laadinfrastructuur.
- Daarnaast zal de Rijksoverheid bezien hoe de uitrol van laadpunten in nieuwe en bestaande gebouwen kan worden vergemakkelijkt … en zal bekijken of kwaliteitseisen gericht op o.a. interoperabiliteit, cybersecurity en smart charging opgenomen kunnen worden.