Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Rapport Rijksinspectie Digitale Infrastructuur

Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen

Colofon

Van	Rijksinspectie Digitale Infrastructuur
Datum	23 mei 2023

Samenvatting

De Rijksinspectie Digitale Infrastructuur (RDI), voorheen Agentschap Telecom, maakt zich ernstige zorgen over een groot deel van de zonnepaneelomvormers dat op de markt wordt gebracht. Dit worden ook wel PV-omvormers genoemd. Omvormers zetten zonne-energie om in elektriciteit die bruikbaar is voor het elektriciteitsnet.

Veel omvormers veroorzaken storing en zijn cyberonveilig. Dit zorgt ervoor dat bijvoorbeeld draadloze apparaten in de buurt niet of slecht werken en zonnepaneelinstallaties kunnen worden gehackt. Om ervoor te zorgen dat iedereen ook in de toekomst probleemloos gebruik kan maken van het radiospectrum en de digitale weerbaarheid van onze energievoorziening is geborgd, treedt de RDI hiertegen op.

Er komen in Nederland steeds meer zonnepaneelinstallaties bij. De RDI startte mede daarom in 2021 een onderzoek om te kijken of omvormers voldoen aan de (toekomstige) wettelijke eisen van de Telecommunicatiewet. Dit onderzoek bestond uit twee delen: de RDI richtte zich op de stoorkans en op de cyberveiligheid. De wettelijke eisen voor cyberveiligheid zijn nog niet actief. Hiervoor werden 9 omvormers onderzocht. Sommige omvormers maken zelf geen verbinding met het internet, maar via een accessoire. Daarom werden ook 5 accessoires onderzocht.

Storing
Uit de resultaten blijkt dat 5 van de 9 omvormers (eventueel in combinatie met een accessoire) storing veroorzaken. Onder andere lucht- en scheepvaart en alledaagse toepassingen zoals radio-omroep, elektrische verkeerspaaltjes en draadloze *tags* kunnen worden verstoord.

Cyberveiligheid
De testen op cyberveiligheid wezen uit dat geen van de 9 onderzochte omvormers voldeed aan de gebruikte norm. Hierdoor zijn zonnepaneelinstallaties bijvoorbeeld eenvoudig te hacken en kunnen deze daarna worden uitgeschakeld of worden deze ingezet voor DDOS-aanvallen. Of kunnen persoons- en gebruiksgegevens worden onderschept.

Administratieve eisen
Geen van de onderzochte producten voldeed aan de administratieve eisen. Deze eisen moeten er onder andere voor zorgen dat fabrikanten van tevoren toetsen of producten voldoen aan de eisen, dat producten traceerbaar zijn en gebruikers de informatie hebben om een product correct te gebruiken. Veel fabrikanten besteden in hun toetsing weinig aandacht aan de omstandigheden waarin een product in de praktijk wordt gebruikt. Fabrikanten zijn verplicht om hun product ook hierop te beoordelen. Anders bestaat het risico dat een product voldoet in een labsituatie, maar in de praktijk stoort.

Wat heeft de RDI gedaan?
Alle fabrikanten ontvingen van de RDI een waarschuwing. De wet verplicht de fabrikanten om per direct passende maatregelen te nemen. Zo wordt voorkomen dat nog meer producten die niet aan de eisen voldoen, op de markt komen. De eisen voor cyberveiligheid zijn pas vanaf 1 augustus 2024 actief. Hiervoor kon de

RDI dus geen waarschuwingen geven. Vanwege de risico's is het toch zaak dat fabrikanten hun apparaten aanpassen.

Hercontroles
De RDI ziet erop toe dat de fabrikanten deze maatregelen nemen. Dit doet zij door over een redelijke termijn hercontroles te doen. Als hieruit blijkt dat de fabrikanten geen passende maatregelen namen of zij opnieuw producten verhandelen die niet voldoen, neemt de RDI handhavende maatregelen. Dit kunnen bijvoorbeeld boetes, verkoopverboden of terugroepacties zijn. Voor cyberveiligheid gebeurt dit vanaf 1 augustus 2024, als de eisen hiervoor gelden.

Wat kan de consument doen?
Fabrikanten zijn ervoor verantwoordelijk dat zij producten verhandelen die voldoen. Maar consumenten kunnen ook zelf problemen signaleren of (gedeeltelijk) oplossen. Zo kan de consument controleren of een product een (juiste) CE-markering heeft. Ook kunnen consumenten alert zijn op storingen van bijvoorbeeld de radio of Wi-Fi. Tot slot kunnen consumenten onder andere sterke wachtwoorden instellen en apparatuur regelmatig updaten, om de cyberveiligheid te verhogen.

Inhoud

1 Inleiding en aanleiding

De Rijksinspectie Digitale Infrastructuur (RDI), voorheen Agentschap Telecom, startte in 2021 een onderzoek naar de mate waarin omvormers voor zonnepanelen (ook wel PV-omvormers genoemd), voldoen aan de (toekomstige) eisen uit Telecommunicatiewet. Dit hoofdstuk plaatst de missie van de RDI, een veilig verbonden Nederland, binnen de context van de energietransitie. In deze context worden ontwikkelingen en uitdagingen geanalyseerd die duidelijk maken waarom een onderzoek naar omvormers noodzakelijk was.

1.1 Een veilig verbonden Nederland

De RDI heeft als missie ervoor te zorgen dat Nederland veilig verbonden is. Dit doet zij op verschillende manieren. De RDI houdt onder andere toezicht op (radio)apparaten die worden verhandeld op de Nederlandse markt. Deze dienen te voldoen aan een aantal eisen. Alleen dan mogen fabrikanten de CE-markering[1] aanbrengen en mogen importeurs en distributeurs apparaten verkopen. Zo moeten deze bijvoorbeeld veilig te gebruiken en storingsvrij[2] zijn. Daarmee wordt de beschikbaarheid en betrouwbaarheid geborgd van de IT- en communicatienetwerken waarvan wij steeds meer afhankelijk zijn.

1.2 Toenemend aantal zonnepaneelinstallaties

Net zoals de rest van de wereld, bevindt Nederland zich in een energietransitie. (Internationale) klimaatdoelen dienen te worden behaald en er wordt vol ingezet op onder andere de verduurzaming van energie. Dit gebeurt bijvoorbeeld in de vorm van zonnepaneelinstallaties. Steeds meer burgers en organisaties kiezen voor deze installaties. De afgelopen jaren is hierdoor het aantal zonnepaneelinstallaties in Nederland explosief toegenomen. In 2015 lagen er ongeveer 1,8 miljoen installaties. Dat aantal groeide naar ruim 5,2 miljoen in 2018, tot 16,3 miljoen in 2021[3].

Een veilig verbonden en tegelijkertijd duurzaam Nederland is essentieel voor een toekomstbestendige samenleving. Daarbij is het van belang dat producten die bijdragen aan verduurzaming, voldoen aan de wettelijke eisen. Producten die aan de wettelijke eisen voldoen, veroorzaken namelijk geen storing. De RDI wil dat de energietransitie slaagt, maar ook dat de benodigde apparatuur veilig en betrouwbaar is.

1.3 Verstoring van radiocommunicatie

Een zonnepaneelinstallatie bestaat naast zonnepanelen uit een omvormer en bekabeling. Soms wordt randapparatuur toegevoegd die de efficiëntie van de installatie verbetert. Deze randapparatuur kan bijvoorbeeld een zonnepaneel in de schaduw beter laten functioneren.

Het elektriciteitsnet maakt gebruik van wisselspanning. Zonnepanelen produceren energie in de vorm van gelijkspanning. Een omvormer zet gelijkspanning om in wisselspanning en pas na het omzetten, is de energie die geleverd wordt door de zonnepanelen bruikbaar voor het elektriciteitsnet.

[1] Met de CE-markering verklaart de fabrikant dat zijn apparaat getoetst is aan alle geldende Europese wet- en regelgeving.
[2] Storingsvrij betekent in dit geval dat apparatuur voldoet aan de eisen voor EMC-storing. De EMC-richtlijn 2014/30/EU en Radioapparatenrichtlijn 2014/53/EU bepalen onder andere dat apparaten het niveau van storing niet mogen overschrijden, waarboven andere apparatuur en toepassingen niet juist functioneren. Zie hoofdstuk 2 voor meer informatie over het wettelijk kader, normen en storingslimieten.
[3] https://klimaatmonitor.databank.nl/dashboard/dashboard/hernieuwbare-energie

Dit omzetten levert altijd 'ongewenste radiofrequenties' op in de omvormers. Deze moeten door juiste filtering 'in' de omvormer worden gehouden. Als dit niet gebeurt, kunnen deze ongewenste frequenties door de kabels en behuizing van de installatie worden uitgestraald. De kabels gedragen zich dan als antennes. Het zijn deze signalen die storen bij gebruikers van het radiospectrum.

In de afgelopen jaren zag de RDI het aantal meldingen van storing door zonnepaneelinstallaties toenemen. Zo ontving de rijksinspectie in de periode 2014-2016 in totaal 21 meldingen. In de periode 2017-2019 waren dit er fors meer: 82 meldingen. Het aantal meldingen liep in de periode 2020-2022 op tot 113 meldingen. Deze toename hangt vermoedelijk samen met het stijgende aantal zonnepaneelinstallaties. De storingen bleken voort te komen uit onjuiste installatie, storende omvormers of storende randapparatuur.

Meldingen worden met name gedaan over storingen op frequenties die omroep, defensie, radiozendamateurs, DAB+ (radio) en het communicatiesysteem voor hulpdiensten (C2000) gebruiken. Naar verwachting zijn de storingen die bij de rijksinspectie bekend zijn, slechts een klein deel van het werkelijke aantal storingen. De gemiddelde burger heeft beperkte tot geen kennis van het radiospectrum. Een burger merkt mogelijk vreemde fenomenen bij draadloze apparaten en toepassingen (bijvoorbeeld slechte Wi-Fi), maar koppelt dit niet snel aan zonnepanelen. Daardoor kan een melding bij de RDI uitblijven.

Naast de eerdergenoemde toepassingen waarover meldingen worden ontvangen, ziet de rijksinspectie de volgende ontwikkelingen:

- Toenemende zorgen over zonnepaneelinstallaties in de buurt van vaarwegen en luchthavens. Scheep- en luchtvaartcommunicatie kan namelijk verstoord worden.
- Storingsproblemen in huis. Door (sterke) stoorsignalen van zonnepanelen kunnen andere elektrische apparaten en installaties beïnvloed worden, zoals kabel-tv, internet, internetrouters en -modems, radio's en PLC-units.
- Naast directe verstoringen van apparaten is ook de verhoging van het algemene onbedoelde storingsniveau (*man-made noise*) een zorg. Als één zonnepaneelinstallatie stoort en dit wordt opgemerkt, is het aannemelijk dat alle soortgelijke installaties storen. Dit verslechtert de bruikbaarheid van de gehele ether.

1.4 Toekomstige wettelijke cybereisen

Vanaf 1 augustus 2024 moeten draadloze, met het internet verbonden apparaten, naast storingsvrij ook cyberveilig zijn. Vanaf dat moment gelden hiervoor wettelijke eisen. De RDI toetst apparaten nu al op cyberveiligheid. Allereerst om voorbereid te zijn op wat er op de samenleving en de RDI als toezichthouder afkomt. Ten tweede om fabrikanten, importeurs en distributeurs te wijzen op deze naderende eisen. Tot slot doet de RDI dit ook om digitale kwetsbaarheden nu al te tackelen.

De energietransitie is verweven met de digitale transitie. Een groot deel van het dagelijks leven is afhankelijk van digitale toepassingen. Energieopwekking via zonnepanelen is tegenwoordig in bijna alle gevallen te monitoren en regelen via het internet, bijvoorbeeld via een app.

Slechte cyberveiligheid van zonnepaneelinstallaties kan nu al (enorme) schade aanrichten. Denk hierbij aan het scenario dat een groot deel van de zonnepaneelinstallaties in Nederland in één keer wordt uitgeschakeld door een hack. Hierdoor ontstaat schade aan het stroomnet. Daardoor is het niet meer bruikbaar

voor huishoudens. De RDI vindt daarom dat zij en marktpartijen niet kunnen wachten tot 2024, maar hier meteen mee aan de slag moeten.

1.5 Focus onderzoek

Naar aanleiding van de bovengenoemde ontwikkelingen, heeft de RDI van juli 2021 tot en met mei 2022 twee aspecten van omvormers onderzocht: het stoorpotentieel en de cyberveiligheid. Het omzetten van de energie door omvormers die geleverd wordt door zonnepanelen in spanning, kan gepaard gaan met storing. Dit blijkt ook uit eerdere onderzoeken van de RDI. Daarnaast wilde de rijksinspectie, met het oog op de toekomstige wet- en regelgeving, de cyberveiligheid van de omvormers onderzoeken. De impact van een cyberprobleem kan namelijk grote gevolgen hebben voor onze maatschappij.

2 Onderzoek

Bij ieder onderzoek dat de RDI start, wordt van tevoren een selectie gemaakt van te onderzoeken producten. Daarnaast worden altijd de administratieve eisen getoetst. In aanvulling daarop, worden op basis van productrisico's de onderdelen bepaald die de rijksinspectie al dan niet technisch onderzoekt. Dit tweede hoofdstuk geeft inzicht in de uitgangspunten en vaststelling van de onderzochte producten en aspecten in dit onderzoek. Inclusief het wettelijk kader dat van toepassing is.

2.1 Selectie producten

2.1.1 Soorten, typen en merken

Omvormers zijn er in allerlei soorten en maten. Voor het onderzoek dat de RDI deed, werden alleen omvormers met een vermogen tot 3,6 kilowatt geselecteerd. Deze zijn bedoeld voor residentiële omgevingen, bijvoorbeeld woonwijken. In deze omgeving worden omvormers dichtbij elkaar geplaatst. Daardoor wordt de kans op storing groter. Daarnaast blijkt uit eerder onderzoek dat de installatiekwaliteit van zonnepaneelinstallaties in residentiële omgevingen divers is. De zonnepaneelinstallaties worden aangelegd door professionals, maar ook door leken.

Bij het selecteren van de merken en typen producten werd een lijst van Netbeheer Nederland gebruikt. Installaties die stroom leveren aan het elektriciteitsnet moeten aan bepaalde Europese eisen voldoen. Netbeheer Nederland houdt een lijst bij van omvormers die hieraan voldoen en op het elektriciteitsnet mogen worden aangesloten.[4]

Van deze lijst werden willekeurig negen verschillende typen omvormers, van acht merken geselecteerd. De steekproef leverde namelijk twee typen omvormers van één merk op. Uit internetonderzoek en de administratie van storingsmeldingen van de rijksinspectie, bleek dat een aantal van de meest verkochte merken omvormers binnen de selectie viel.

Apparatuur werd bij de fabrikant opgevraagd. De fabrikant heeft namelijk de meeste invloed op het voldoen van de omvormers aan de wettelijke eisen. Met alle acht fabrikanten is direct, dan wel via hun Europese vestigingen, contact geweest. Daarbij werden exemplaren van omvormers en accessoires opgevraagd zoals deze ook aan consumenten geleverd worden.

2.1.2 Accessoires

Bijna alle zonnepaneelinstallaties worden bediend en uitgelezen via een internetportaal en/of smartphone-applicatie. Sommige omvormers communiceren draadloos (bijvoorbeeld via Wi-Fi) of bekabeld (via een netwerkkabel). Andere omvormers hebben hiervoor een accessoire nodig. Voor het onderzoeken van de storing, die wordt uitgestraald via kabels, en de cyberveiligheid, moesten de omvormers aangesloten kunnen worden via een netwerkkabel. Van de omvormers waarbij dit niet direct mogelijk was, werd een monitoraccessoire opgevraagd. Dit was het geval bij vijf producten.

[4] https://www.netbeheernederland.nl/nieuws/vanaf-27-april-2021-extra-verplichting-voor-kleinere-opwekinstallaties--1452

2.2 Wettelijk kader

Hierboven wordt onderscheid gemaakt tussen de omvormers die draadloos kunnen communiceren en de omvormers die dit niet kunnen. Ook voor de accessoires geldt dit onderscheid. Dit is belangrijk voor de wetgeving die van toepassing is. Apparaten met draadloze functies worden namelijk radioapparaten genoemd. Denk hierbij aan bijvoorbeeld een afstandsbediening, Wi-Fi of Bluetooth. Deze radioapparaten moeten voldoen aan de Europese Radioapparatenrichtlijn 2014/53/EU.

Elektrische apparaten die niet dit soort draadloze functies hebben, kunnen ook storen of gevoelig zijn voor storing. Voor die aspecten moeten de producten voldoen aan de EMC-richtlijn 2014/30/EU. EMC is de afkorting van elektromagnetische compatibiliteit.

Beide EU-richtlijnen stellen vergelijkbare eisen aan de toegestane mate van storing. Dit worden de essentiële eisen genoemd. Daarnaast bevatten de richtlijnen formele (administratieve) eisen. Dit zijn onder andere regels voor de conformiteitsbeoordeling; de toetsing van het product voordat deze op de markt wordt gebracht. Deze regels zorgen ervoor dat fabrikanten, importeurs en distributeurs de nodige stappen doorlopen om producten op de markt brengen die voldoen aan de essentiële eisen.

Alle eisen uit de Radioapparatenrichtlijn en EMC-richtlijn zijn opgenomen in Nederlandse wetgeving, namelijk de Telecommunicatiewet, het Besluit radioapparaten 2016 en het Besluit elektromagnetische compatibiliteit 2016.

Op dit moment gelden de wettelijke eisen voor cyberveiligheid nog niet. Deze worden vanaf 1 augustus 2024 geactiveerd als essentiële eisen van de Radioapparatenrichtlijn. Strikt genomen is er (nog) geen juridische basis om de naleving op cyberveiligheid te handhaven. De RDI heeft als toekomstig verantwoordelijk toezichthouder wel de vrijheid om cyberaspecten te onderzoeken ter voorbereiding op deze taak.

2.3 Essentiële eisen en normen

De essentiële eisen van de Radioapparatenrichtlijn en EMC-richtlijn zijn leidend tijdens de conformiteitsbeoordeling. Een apparaat moet bijvoorbeeld zo ontworpen zijn dat deze niet stoort en gestoord wordt. Zo'n essentiële eis is alleen niet erg concreet, want hoe wordt bepaald wanneer een apparaat stoort en wanneer niet?

Hiervoor bestaan er normen. Dit zijn door de markt (en soms ook in samenwerking met de overheid) ontwikkelde standaarden die onder andere storingslimieten, meetprocedures en testcondities voorschrijven voor apparatuur en installaties. Bepaalde normen worden bovendien voor specifieke richtlijnen geharmoniseerd door de Europese Commissie.

Normen zijn hulpmiddelen en geven 'slechts' een vermoeden van overeenstemming. Daarbij is dat vermoeden van overeenstemming sterker bij het gebruik van een geharmoniseerde norm. Maar alleen het voldoen aan een geharmoniseerde norm is niet genoeg. Een product kan voldoen aan een (geharmoniseerde) norm, en tegelijkertijd in de praktijk nog steeds storen. Daarmee voldoet deze niet aan de essentiële eisen. De belangrijkste redenen hiervoor zijn dat ieder individueel product verschilt (normen zijn vaak ontworpen voor productgroepen), geen product altijd exact hetzelfde wordt gebruikt en geïnstalleerd, en testen meestal gebeuren in een laboratoriumomgeving.

Een fabrikant moet daarom rekening houden met de praktijksituaties[5] waarin zijn product wordt gebruikt. Van hem wordt verwacht dat hij bij de conformiteitsbeoordeling rekening houden met zowel normen, als praktijkscenario's, die soms niet door de norm worden afgedekt. Dit zijn risico's die moeten worden weggenomen (bijvoorbeeld door een aanvullende test of aanpassingen aan het productontwerp). Dit verwerkt de fabrikant in een risicoanalyse. Als uit dit gehele traject blijkt dat het product in geen geval gebreken heeft, kan overeenstemming met de eisen uit de richtlijnen worden verklaard en mag de CE-markering worden aangebracht.

2.4 Onderzochte aspecten

De RDI doorloopt bij het onderzoeken van producten meestal (onderdelen van) de route die fabrikanten ook moeten volgen voordat zij een product op de markt brengen. Dit betekent dat de rijksinspectie een testprocedure bepaalt, op basis van zowel de meest geschikte geharmoniseerde normen als beoogde praktijksituaties.

2.4.1 EMC

Bij de omvormers is de EMC-emissie onderzocht. Emissie gaat over de mate waarin een apparaat stoort op andere apparaten of toepassingen. Uit de storingsmeldingen die de RDI ontvangt over omvormers, blijkt dat bij omvormers zich vooral problemen met de emissie voordoen.

Tijdens het onderzoek naar de EMC-emissie voerde de rijksinspectie twee verschillende testen uit: een *radiated* emissie-test en een *conducted* emissie-test. *Radiated* emissie heeft betrekking op de storing die een apparaat creëert vanuit de behuizing. Voornamelijk C2000 en radiozendamateurs hebben last van deze soort verstoring. *Conducted* emissie is de storing die een apparaat veroorzaakt via de kabels. De kabels fungeren dan als antenne. De overige storingen die bekend zijn bij de rijksinspectie, worden veelal hierdoor veroorzaakt.

Voor de testen gebruikte de RDI de geharmoniseerde norm EN 55011:2016/A11:2020. Deze omvat *semiconductor converters* en is daarmee een specifieke norm voor apparaten zoals omvormers. Logischerwijs geeft ook het gebruik van een specifieke norm een meer aannemelijk vermoeden van overeenstemming, dan een generieke norm.

De paragrafen 3.1 en 3.2 van de norm beschrijven de limieten voor *radiated* emissie en *conducted* emissie (op de AC-, DC- en LAN-poorten). Op basis van de testresultaten kan worden afgeleid of een product storing veroorzaakt en dus of deze voldoet aan de essentiële eisen.

De omvormers zijn getest op frequenties tot 1 gigahertz. Er zijn namelijk geen meldingen of signalen door de rijksinspectie ontvangen dat zonnepaneelinstallaties of omvormers storen op frequenties boven 1 gigahertz.

2.4.2 Cyberveiligheid

Voor het toetsen van de cyberveiligheid werd de norm ETSI EN 303 645 V2.1.1 gebruikt. Deze norm is op dit moment niet geharmoniseerd, omdat de wettelijke cybereisen nog niet van kracht zijn. De inhoud van deze norm wordt op dit moment wel algemeen beschouwd als de actuele stand der techniek voor cyberveiligheid van slimme apparatuur.

[5] Onder praktijksituaties worden verstaan: alle beoogde en redelijkerwijs voorzienbare gebruikssituaties en -condities waarin een product (mogelijk) gebruikt kan worden.

Uit deze norm werden de volgende onderdelen getest:

- *Universele standaardwachtwoorden* (paragraaf 5.1): de minimale vereisten voor wachtwoorden. Hierbij wordt gekeken naar bijvoorbeeld de mate waarin standaardwachtwoorden worden gebruikt, gebruikers worden gedwongen een uniek en sterk wachtwoord in te stellen bij het eerste gebruik en het aantal inlogpogingen met onjuiste inloggegevens.
- *Rapporteren kwetsbaarheden* (paragraaf 5.2): de mogelijkheid om als gebruiker kwetsbaarheden te rapporteren, zodat deze sneller kunnen worden opgelost.
- *Software updates* (paragraaf 5.3): de vereisten voor softwarebeleid. Denk hierbij onder andere aan de mogelijkheid om updates automatisch en eenvoudig te downloaden.
- *Veilige communicatie* (paragraaf 5.5): de mate waarin een apparaat veilig is verbonden met de '*cloud*'. Is de verbinding bijvoorbeeld versleuteld?
- *Minimaliseren aanvalsoppervlak* (paragraaf 5.6): apparaten en digitale applicaties hebben vaak meerdere 'ingangen' waarmee ongeautoriseerde personen kunnen 'binnenkomen'. Dit onderdeel toetst of al deze (soms onnodige) 'ingangen' zijn afgesloten.
- *Beveiliging van persoonlijke gegevens* (paragraaf 5.8): dit onderdeel heeft (net als de volgende twee onderdelen) raakvlakken met de Algemene verordening gegevensbescherming (AVG). Dit onderdeel toetst of de draadloze communicatie van persoonsgegevens voldoende is beveiligd en of bijvoorbeeld het privacybeleid vermeld welke persoonlijke gegevens voor welk doel worden gebruikt.
- *Verwijderen gebruiksgegevens* (paragraaf 5.11): de mogelijkheid om persoonlijke gegevens eenvoudig te kunnen verwijderen.
- *Gegevensbescherming* (paragraaf 6): ook bij dit onderdeel wordt het privacybeleid beoordeeld. Daarnaast toetst het de mogelijkheden en beperkingen rondom persoons- en gebruiksgegevens. Zoals de mogelijkheid om eerder gegeven toestemming voor de verwerking van gegevens in te trekken, de mate waarin gegevens die zijn opgeslagen in de *cloud* ingezien kunnen worden en de mogelijkheid om gegevens te kunnen verwijderen.

Een deel van de omvormers en accessoires had geen draadloze functie. Deze konden met een netwerkkabel verbonden worden met een applicatie of portaal via het internet. Dat maakt deze apparaten geen radioapparaten. Strikt genomen zijn de toekomstige cybereisen uit de Radioapparatenrichtlijn hierop niet van toepassing.

Alle fabrikanten brengen echter ook andere versies van diezelfde accessoires op de markt, met bijvoorbeeld een Wi-Fi functie. De smartphone-applicatie of het web portaal waarmee verbinding wordt gemaakt, is voor ieder apparaat hetzelfde, zowel draadloos als bekabeld. Daarom is de cyberveiligheidstest relevant voor alle geselecteerde apparaten. Het is van belang voor de digitale infrastructuur dat ook bekabelde, met het internet verbonden apparaten, cyberveilig zijn. Overigens wordt ook voor de cyberveiligheid (van software) van bekabelde apparatuur Europese wetgeving ontwikkeld.

2.4.3 Administratieve eisen

Op administratief vlak worden bij ieder onderzoek door de RDI in ieder geval twee aspecten gecontroleerd. Aan de hand van de documentatie die hoort bij een product, wordt beoordeeld of de fabrikant een volledige en juiste conformiteitsbeoordeling heeft doorlopen. Daarnaast onderzoekt de rijksinspectie of fabrikanten of importeurs voldoen aan hun wettelijke verplichtingen ten aanzien van alle markeringen, gegevens en informatie op en bij een product.

Voor de omvormers en hun accessoires betekent dit dat onderdelen van de technische documentatie (conformiteitsverklaring, testrapporten en risicoanalyse) werden gecontroleerd op volledigheid en juistheid. Verder werden de aanwezigheid en vorm van de CE-markering, de traceerbaarheid (bijvoorbeeld typeaanduiding), de adresgegevens van fabrikant en de gebruiks- en veiligheidsinformatie getoetst.

3 Resultaten en gevolgen

In de volgende fase van het onderzoek beoordeelt en toetst de RDI de apparatuur en bijbehorende documentatie. EMC-metingen en cybertesten worden gedaan in een daarvoor ingericht laboratorium. Dit hoofdstuk beschrijft de onderzoekresultaten en andere bevindingen per getoetst onderdeel.

Op basis van eventuele tekortkomingen intervenieert de RDI om wettelijke overtredingen te beëindigen. De rijksinspectie bepaalt interventies op basis van de mogelijke gevolgen van een non-conformiteit. Dit hoofdstuk gaat ook in op deze mogelijke gevolgen.

3.1 EMC-gedragingen

3.1.1 Resultaten

Zoals eerder beschreven, definieert de gebruikte norm verschillende testen en de daarbij horende limieten. De RDI heeft de omvormers tegen die limieten getoetst. Daar werd bij 5 van de 9 omvormers een hoger storingsniveau gemeten dan de norm voorschrijft. De overschrijdingen werden op meerdere frequenties gezien. Dit betekent dat deze vijf omvormers mogelijk storen op andere apparatuur en toepassingen die gebruikmaken van diezelfde frequenties. De betreffende omvormers voldoen hierdoor niet aan de wettelijke eisen.

Vastgesteld werd dat drie omvormers de limieten overschrijden voor *radiated* emissie. Wat betreft uitstraling door middel van de kabels (*conducted* emissie) bleek dat twee omvormers storen via de poort voor wisselstroom (AC-aansluiting). Via de poort voor gelijkstroom (DC-poort) storen alle vijf non-conforme omvormers. Tot slot bleken twee omvormers storing te kunnen veroorzaken via de netwerkkabel (in combinatie met monitoraccessoire). De metingen aan deze poorten tonen aan dat de opgewekte EMC-storingen het niveau overschrijden, waarboven andere apparaten niet meer kunnen functioneren zoals waarvoor deze bedoeld zijn.

Onderzoek naar de frequenties waarop overschrijdingen werden gemeten en de hoogte van die overschrijdingen, wijst uit dat de omvormers vooral via poorten en bekabeling ernstig storen. Hierdoor kunnen toepassingen volledig plat gelegd worden en is communicatie via die frequenties niet mogelijk. Dit kan tot kritieke situaties leiden. De ernst van de storing via de behuizing is lager.

Het eenvoudig en overzichtelijk duiden van de ernst van EMC-storing is lastig. Dit heeft ermee te maken dat een apparaat (tegelijkertijd) kan storen op meerdere frequenties. Ook de mate waarin er wordt gestoord verschilt per frequentie. Daarnaast zijn sommige stoorsignalen permanent aanwezig. Terwijl andere storingen niet continu optreden. Tot slot is de daadwerkelijke hoeveelheid EMC-storing in de praktijk afhankelijk van meer zaken, zoals de afstand van de stoorbron.

Toch wilde de RDI de ernst van de storende omvormers op een overzichtelijke manier presenteren. Vanuit de resultaten is daarom een vertaalslag gemaakt naar die tabellen die de ernst van de storende omvormers aantonen. Deze tabellen zijn te vinden op de volgende pagina. De tabellen geven weer hoeveel van de onderzochte omvormers storen, welke frequentiegebruikers hierdoor worden beïnvloed en in welke mate de omvormers storen. De mate van storing is gecategoriseerd in drie

niveaus: minimale verstoring, merkbare verstoring en verstoring die communicatie (in potentie) onmogelijk gemaakt.

Een minimale verstoring is een gemeten limietoverschrijding. Daardoor voldoet de omvormer weliswaar niet aan de eisen, maar de gevolgen van de storing zijn beperkt. Onder een merkbare verstoring wordt verstaan een verstoring die regelmatig voorkomt. Deze verstoring is merkbaar, maar radiocommunicatie is nog mogelijk (haperende radio bijvoorbeeld). Tot slot zijn er de omvormers die communicatie (potentieel) onmogelijk maken. Deze leggen (in ongunstige omstandigheden) volledige toepassingen plat. Radiocommunicatie is in dat geval onmogelijk.

Tabel 1
Bevindingen radiated emissie (storing vanuit behuizing apparaat)

Beïnvloede frequentiegebruikers	**Aantal omvormers dat minimaal stoort**	**Aantal omvormers dat merkbare storing veroorzaakt**	**Aantal omvormers dat communicatie (in potentie) onmogelijk maakt**
Radiozendamateurs	1	2	geen
Defensie	geen	2	geen
Omroep (radio en tv)	geen	geen	1
Luchtvaart	1	1	geen

Tabel 2
Bevindingen conducted emissie (storing via kabels)

Beïnvloede frequentiegebruikers	**Aantal omvormers dat minimaal stoort**	**Aantal omvormers dat merkbare storing veroorzaakt**	**Aantal omvormers dat communicatie (in potentie) onmogelijk maakt**
Radiozendamateurs	1	2	2
Defensie	1	1	2
Omroep (radio en tv)	1	1	3
Luchtvaart	1	2	1
Scheepvaart	1	3	1
Radiografische klokken	geen	1	1
Radio-frequency identification (RFID)	1	1	3

Tabel 3
Totaal aantal storende omvormers per radiotoepassing (radiated en conducted emissie samen, waarbij bij overlap van een merk alleen de 'worst-case' is meegerekend)

Beïnvloede frequentiegebruikers	**Aantal omvormers dat minimaal stoort**	**Aantal omvormers dat merkbare storing veroorzaakt**	**Aantal omvormers dat communicatie (in potentie) onmogelijk maakt**
Radiozendamateurs	geen	3	2
Defensie	geen	2	2
Omroep (radio en tv)	1	geen	4
Luchtvaart	1	3	1
Scheepvaart	1	3	1
Radiografische klokken	geen	1	1
Radio-frequency identification (RFID)	1	1	3

3.1.2 Gevolgen

De eventuele gevolgen van de overschrijdingen verschillen per frequentieband en de betreffende frequentiegebruikers. De gevolgen van EMC-verstoring per toepassing op een rij gezet:

- Storing op defensieapparatuur kan in het meest extreme geval de nationale veiligheid in gevaar brengen omdat communicatie via in ieder geval de reguliere kanalen onmogelijk is.
- Lucht- en scheepvaartvoertuigen kunnen onderling niet communiceren waardoor de veiligheid en verkeersdoorstroom in de lucht en op het water in het gedrang komen.
- Burgers kunnen hun favoriete radiozender niet luisteren of tv-zender niet meer bekijken. Ook zijn delen van het frequentiespectrum onbruikbaar, terwijl omroepzenders betalen om hierop te mogen uitzenden.
- Radiografische klokken die continu via radiosignalen gelijk worden gezet, lopen niet meer op tijd.
- Radiozendamateurs kunnen hun hobby niet meer uitoefenen.

RFID (*Radio-frequency identification*) is een radiotechnologie waar steeds meer (moderne) producten en processen mee werken. Dat gaat dan om bijvoorbeeld elektronische sleutels (*tags*), laadpaalpassen, chips in dierenhalsbanden, antidiefstalpoortjes, goederentracering in magazijnen en elektrische verkeerspaaltjes. Bij verstoring op de frequentiebanden waarop RFID werkt, is het niet onwaarschijnlijk dat dit soort scenario's zich voordoen:

- Verkeerspaaltjes gaan niet naar beneden voor bijvoorbeeld ambulances of openbaar vervoer.
- Producten kunnen makkelijker uit winkels worden gestolen doordat antidiefstalpoortjes niet goed werken.
- Kattenluiken gaan niet meer open, vee krijgt geen eten op geplande tijden, koeien worden niet meer gemolken.
- Elektrische auto's kunnen niet meer worden opgeladen met een laadpaalpas.
- Deuren in bijvoorbeeld flats of bedrijfsgebouwen gaan niet meer open na het scannen van een *tag*.
- Actuele voorraad in winkels klopt niet meer.

3.1.3 Kanttekeningen bij testresultaten

In eerste instantie concludeerde de RDI dat 7 van de 9 onderzochte omvormers de storingslimieten uit de norm overschreden. In plaats van de eerdergenoemde vijf non-conforme omvormers. De twee betreffende fabrikanten hadden dezelfde metingen gedaan. Dat leverde andere resultaten op. Voor de RDI was dit een reden om nieuw onderzoek te doen en de eerdere conclusies te heroverwegen.

Uit nader onderzoek bleek dat de eerdere conclusies over beide omvormers inderdaad moesten worden gecorrigeerd door de RDI. Beide omvormers werden opnieuw gemeten. Bij één omvormer bleven tijdens deze hermeting de gemeten waarden onder de limiet. Wat betreft de andere omvormer, stelde de RDI vast dat de gebruikte meetopstelling toch niet geschikt was voor de technische constructie en specificaties van die omvormer. Hoofdstuk 4 geeft een verdere toelichting op het vervolg na de metingen en controles. In paragraaf 4.3 wordt dit nadere onderzoek beschreven.

3.2 Cyberveiligheid

3.2.1 Resultaten

De bevindingen voor cyberveiligheid worden gecategoriseerd per fabrikant in plaats van per onderzocht product. Bij de meeste fabrikanten maken de apparaten gebruik van dezelfde smartphone-applicatie of hetzelfde web portaal. Bij dit onderdeel wordt daarom geschreven over acht fabrikanten.

Geen van de acht fabrikanten voldoet aan de getoetste cyberveiligheidsnorm. De testresultaten van vier fabrikanten zijn volgens de rijksinspectie zelfs zeer kritiek voor de cyberveiligheid van het elektriciteitsnet, woningen en burgers. De onderstaande tabel geeft per getest onderdeel het aantal omvormers weer dat niet voldoet aan de (toekomstige) eisen.

Tabel 4
Bevindingen cyberveiligheid

Getoetst onderdeel	**Aantal fabrikanten dat niet voldoet**
Wachtwoorden	7
Rapporteren kwetsbaarheden	8
Software updates	7
Veilige communicatie	4
Minimaliseren aanvalsoppervlak	3
Beveiliging van persoonlijke data	1
Verwijderen persoonsgegevens	2
Gegevensbescherming	3

3.2.2 Gevolgen

De gevolgen per onderdeel zijn de volgende:

- Doordat het mogelijk is om een zwak wachtwoord in te stellen of apparatuur zelf zwakke standaardwachtwoorden hebben, kunnen inloggegevens eenvoudig achterhaald worden.
- Als het voor gebruikers niet mogelijk is om kwetsbaarheden te rapporteren, blijven deze kwetsbaarheden mogelijk langer bestaan en kunnen kwaadwillende personen hiervan gebruik maken.

- Als er geen updates worden uitgegeven of updates zijn voor gebruikers niet eenvoudig te installeren, is er een aanzienlijke kans dat verouderde (en kwetsbare) softwareversies actief blijven.
- Bij onveilige communicatie kan data van en naar de zonnepaneelinstallatie, zoals gegevens over stroomverbruik en -opbrengst, worden onderschept of gemanipuleerd.
- Bij een onvoldoende minimalisatie van het aanvalsoppervlak kun je op verschillende manieren bij de gegevens en instellingen van een zonnepaneelinstallatie kunnen, waarbij niet al deze 'openingen' beveiligd zijn.
- Als persoonlijke data van gebruikers onvoldoende beveiligd is, kunnen persoonsgegevens worden onderschept of gestolen worden.
- Persoonsgegevens en andere data moeten verwijderd kunnen worden door gebruikers. Als dit niet mogelijk is, kunnen gebruikers hun account niet verwijderen en blijven persoonsgegevens onterecht in het bezit van de leverancier.
- Als een leverancier gebruikers niet informeert over de manier waarop gegevens worden beschermd of waarvoor deze gebruikt worden, kunnen deze gegevens gebruikt worden voor doeleinden waar de gebruiker niets van weet.

Het feit dat veel fabrikanten hun wachtwoordbeleid of updatebeleid niet op orde hebben, kan zeer onwenselijke situaties tot gevolg hebben. Veel apparaten worden één keer geconfigureerd (door een installateur). Daarna worden soms geen updates meer gedaan. Of het updaten van apparatuur is moeilijk voor gebruikers. Hierdoor draait er na een bepaalde periode verouderde software. Terwijl digitale techniek dagelijks door ontwikkelt, waardoor nieuwe kwetsbaarheden ontstaan. Een met het internet verbonden omvormer met zwakke of standaardwachtwoorden, of verouderde software, is kwetsbaar voor kwaadaardige software of personen.

Er zijn scenario's denkbaar dat omvormers (op grote schaal) worden uitgeschakeld. Voor individuele gebruikers wordt hierdoor zonne-energie misgelopen. Voor de gehele samenleving leidt dit ertoe dat het stroomnet wordt gemanipuleerd of er landelijk een (zonne-)energietekort is.

Ook kunnen digitaal kwetsbare omvormers worden ingezet voor een (Distributed) Denial-of-Service-aanval (DDoS-aanval) waardoor websites of andere digitale toepassingen (tijdelijk) onbruikbaar zijn of hier schade aan wordt toegebracht. Overigens heeft de gebruiker in het geval van een DDOS-aanval daar op dat moment geen kennis van.

Tot slot zenden sommige omvormers een continue wifi-hotspot uit. Deze is toegankelijk met een standaardwachtwoord. Dat standaardwachtwoord is in bepaalde gevallen eenvoudig te vinden via het internet (in digitale handleidingen). Op deze manier kunnen personen die fysiek in de buurt zijn van zo'n omvormer, hiermee verbinden en de omvormer uitschakelen, manipuleren of misbruiken.

3.3 Administratieve eisen

3.3.1 Resultaten

Tot slot werden de omvormers getoetst aan de administratieve eisen. Hieruit bleek dat geen van de negen onderzochte omvormers voldeed op dit vlak. Ook de vijf onderzochte accessoires voldeden niet.

De meest voorkomende en impactvolle administratieve tekortkomingen zijn:

- Ontbrekende conformiteitsverklaring (alleen bij accessoires).
- Aantonen van conformiteit op basis van ingetrokken geharmoniseerde normen.
- Overslaan van verplichte onderdelen van geharmoniseerde normen bij de conformiteitsbeoordeling.
- Traceerbaarheid via typenummers en modelnamen van producten niet op orde (bijvoorbeeld op de conformiteitsverklaring of product labels).
- Ontbrekende adresgegevens van vestiging van de fabrikant binnen de EU op product labels.
- Ontbrekende informatie voor de gebruiker.
- Ontbrekende risicoanalyse in de technische documentatie.
- Geen onderzoek naar de conformiteit van bepaalde onderdelen of functionaliteiten van een product (bijvoorbeeld het testen van de DC-poort op EMC-storing).
- Testsituaties die niet overeenkomen met gebruikssituaties (bijvoorbeeld het testen van een monitoraccessoire terwijl deze is aangesloten op een computer of een printplaat, in plaats van een omvormer of iets vergelijkbaars).

3.3.2 Gevolgen

De ernst van de verschillende soort administratieve non-conformiteiten loopt sterk uiteen. Het overslaan van complete stappen uit het conformiteitsbeoordelingsproces brengt logischerwijs grotere risico's met zich mee, dan een omvormer waarvan de conformiteitsverklaring niet de wettelijk voorgeschreven titel heeft. Ten aanzien van bijvoorbeeld dat laatste geval worden dan ook minder ingrijpende maatregelen verwacht.

Er zijn drie soorten gevolgen te onderscheiden. Allereerst duiden de volgende gebreken op het niet, onjuist of onvolledig doorlopen van de conformiteitsbeoordeling:

- het ontbreken van een (correcte) conformiteitsverklaring
- het gebruiken van ingetrokken geharmoniseerde normen
- het overslaan van onderdelen uit normen

Dit vergroot de kans op een omvormer of accessoire die niet voldoet aan de essentiële eisen. De fabrikant heeft dit simpelweg niet (goed genoeg) onderzocht. Het gevolg daarvan is dat het product in gebruik mogelijk onveilig is of stoort.

Ten tweede zijn er veel gebreken gezien in de informatie en gegevens op en bij de producten. De traceerbaarheid van producten is van belang om te borgen dat iedere variant van een product voldoet. Daarnaast is de informatie noodzakelijk bij een ingezette terugroepactie. Ook moeten gebruikers en markttoezichtautoriteiten, zoals de RDI, een contactpunt hebben binnen de Europese Unie. De adresgegevens van dit contactpunt moeten op het apparaat staan. Anders is niet duidelijk waar consumenten en de markttoezichtautoriteiten terecht kunnen met vragen over of problemen met het product.

Tot slot moet de gebruiker informatie hebben over hoe een product gebruikt moet worden. Is deze informatie er niet, dan bestaat de kans dat een product verkeerd wordt gebruikt en daardoor stoort of onveilig is. Bij radioapparaten moeten daarnaast de conformiteitsverklaring en de radio-specificaties worden bijgevoegd. Dit in verband met het gebruik van frequenties waarvoor mogelijk een vergunning nodig is.

3.3.3 Conformiteit in gebruiksomstandigheden

Het ontbreken van een risicoanalyse en testsituaties die niet overeenkomen met gebruikssituaties behoeft expliciete aandacht. Zoals eerder beschreven moet een product voldoen aan de essentiële eisen in alle mogelijke configuraties en beoogde en redelijkerwijs voorzienbare gebruikssituaties. Met andere woorden: een omvormer (en accessoire) moet veilig en storingsvrij zijn in alle instelbare toestanden. Bij bijvoorbeeld maximaal vermogen én in stand-by-toestand.

Ook moet een omvormer storingsvrij zijn in alle verschillende gebruikssituaties die kunnen voorkomen. Denk aan de locatie waar apparaat wordt gebruikt (garage, meterkast of zolder), alle accessoires die men kan aansluiten, of de lengte van kabels naar de zonnepanelen.

Van fabrikanten wordt verwacht dat zij hier voldoende rekening mee houden. In een risicoanalyse moet een fabrikant aandacht besteden aan alle voorzienbare scenario's en risico's bij het gebruik. Om risico's te voorkomen moeten maatregelen worden bedacht en uitgewerkt. Soms volstaat het om een gebruikswaarschuwing op te nemen in de gebruiksinstructies. In andere gevallen is dit niet genoeg. Dan moet het productontwerp bijvoorbeeld worden aangepast.

Voor het testen van het apparaat betekent dit dat de best passende norm moet worden gekozen. In andere gevallen moeten meerdere situaties of configuraties worden onderzocht. Of er moet misschien worden afgeweken van een voorgeschreven testopstelling. Dit om ervoor te zorgen dat conformiteit wordt beoordeeld in omstandigheden die overeenkomen met het daadwerkelijke gebruik.

Geen van de fabrikanten had een (adequate) risicoanalyse voor zijn product(en). Er was slechts één fabrikant die een risicoanalyse aanleverde. De inhoud van deze analyse was echter ontoereikend. Er werd hierin alleen gesteld dat wordt voldaan aan geharmoniseerde normen.

Daarnaast is de conformiteit van bepaalde producten (voornamelijk accessoires) door de fabrikant beoordeeld in omstandigheden die niet representatief zijn voor hetgeen waarvoor het product is bedoeld. Dit heeft als gevolg dat producten weliswaar voldoen in een specifieke situatie of in laboratoriumomstandigheden, maar in de praktijk kunnen deze onveilig zijn en/of storen.

4 Vervolg

Na het onderzoek, analyse en interpretatie van de resultaten, doet de RDI interventies om eventuele overtredingen te beëindigen. Een gesprek met de betreffende marktdeelnemer maakt altijd onderdeel uit van de interventiestrategie. Daarna wordt een waarschuwing gegeven of start er een sanctietraject. Dit hoofdstuk beschrijft het vervolg op de onderzoeksfase en de verdere inzichten die de RDI in deze fase verkreeg.

4.1 Overtredingen

Met het op de markt brengen van de non-conforme omvormers en accessoires overtreden de betrokken fabrikanten de Telecommunicatiewet. Marktdeelnemers, waaronder fabrikanten, zijn vanuit de EMC-richtlijn en Radioapparatenrichtlijn verplicht om passende maatregelen te nemen als apparatuur die zij verhandelen niet voldoet. Denk hierbij aan terugroepacties, het staken van de handel, aanpassingen aan apparatuur, aanvullende testen of het herzien van interne conformiteitsprocessen. Welke maatregelen een fabrikant moet nemen, ligt aan de (ernst van de) tekortkomingen.

Fabrikanten zijn door de RDI in individuele gesprekken gewezen op de geconstateerde overtreding(en) en hun wettelijke verplichtingen. De rijksinspectie verwacht van de fabrikanten dat in ieder geval de handel wordt gestaakt van de apparaten die EMC-technisch niet voldoen. Daarnaast wordt verwacht dat fabrikanten actief storingen oplossen als hiervan melding bij hen of de RDI wordt gedaan.

4.2 Waarschuwingen en hercontroles

Naar aanleiding van dit onderzoek zijn geen boetes opgelegd of andere maatregelen genomen vanuit de RDI. De fabrikanten waren voldoende bereid om te handelen volgens hun verplichtingen en passende maatregelen te nemen. De fabrikanten hebben wel een waarschuwing ontvangen voor het overtreden van de wettelijke eisen.

Over een redelijke termijn doet de rijksinspectie hercontroles bij de betreffende fabrikanten. Als opnieuw blijkt dat fabrikanten hun wettelijke verplichtingen niet nakomen, worden daarvan inspectierapporten opgemaakt. Deze rapporten kunnen leiden tot een boete of andere sanctie, zoals een verkoopverbod of terugroepactie. Dit gebeurt bijvoorbeeld als een fabrikant nog steeds apparaten op de markt brengt die niet voldoen aan de wettelijke eisen. Maar ook wordt tijdens de hercontrole onderzocht of naar aanleiding van dit eerste onderzoek de juiste maatregelen zijn genomen.

Voor cyberveiligheid zijn de wettelijke eisen nog niet geactiveerd. Op dat gebied kan de rijksinspectie geen waarschuwing geven en heeft het geen bevoegdheden om te handhaven. De bevindingen over cyberveiligheid zijn op dit moment een zeer dringend verzoek. Er wordt wel van fabrikanten verwacht dat zij hier actief mee aan de slag gaan, gezien de mogelijke impact van al die kwetsbaarheden.

Vanaf 1 augustus 2024 is de RDI van plan om in ieder geval nog een controle te doen op cyberveiligheid. De rijksinspectie neemt dan wel maatregelen bij tekortkomingen. Dit kunnen boetes, verkoopverboden, terugroepacties of een combinatie van deze maatregelen zijn.

4.3 Nader onderzoek

Zoals in hoofdstuk 3 al werd beschreven, voerde de RDI met twee fabrikanten meer gesprekken, na de bovengenoemde gesprekken. De omvormers van deze fabrikanten werden in eerste instantie non-conform bevonden. Naar aanleiding hiervan deden deze twee fabrikanten dezelfde metingen. Daaruit volgden andere resultaten. Dit was voor de RDI aanleiding om opnieuw onderzoek te doen en de eerdere conclusies en resultaten van de betreffende twee fabrikanten te heroverwegen. Voor een duidelijke en overzichtelijke toelichting, worden deze omvormers aangeduid als omvormer A en omvormer B.

Als onderdeel van dit onderzoek werden vanwege kwaliteitsredenen nog twee omvormers opnieuw onderzocht. In totaal zijn er dus vier omvormers opnieuw onderzocht. Deze omvormers worden aangeduid als omvormer C en omvormer D. Als geschreven wordt over de 'overige omvormers', worden hiermee de vijf andere omvormers uit dit onderzoek bedoeld. Deze overige omvormers zijn dus niet opnieuw onderzocht.

4.3.1 Extra metingen vanwege kwaliteitscontrole

Aan omvormer A en B werden als eerst nieuwe EMC-metingen gedaan. Omvormer A produceerde tijdens die hermeting toch geen limietoverschrijding. De oorzaak voor de verschillen in resultaten bleek een voeding (ondersteunende apparatuur bij metingen).Daarvan wees een latere kwaliteitscontrole uit dat deze defect was bij de eerste meting aan omvormer A. De defecte voeding beïnvloedde de EMC-gedragingen van de omvormer. Daardoor werden eerder bij omvormer A onterecht waarden boven de limiet gemeten.

Omvormer A, B, C en D waren met deze voeding gemeten. Bij de overige omvormers werd een andere voeding gebruikt. Het gebruiken van verschillende voedingen heeft overigens geen invloed op EMC-gedragingen en meetresultaten, omdat meetapparatuur en ondersteunende apparatuur dezelfde specificaties en eventuele kalibraties hebben. Voor omvormer B was al een traject gestart voor nieuwe metingen (zie paragraaf 4.3.2). Wat overbleef, waren de eerdere meetresultaten van C en D, die mogelijk ook beïnvloed waren door de defecte voeding. Naar aanleiding hiervan vroeg de RDI beide omvormers opnieuw op bij de betreffende twee fabrikanten.

De metingen aan omvormer C en D leverden wél exact dezelfde resultaten op als de eerdere resultaten. Op deze metingen aan deze twee omvormers heeft de defecte voeding dus geen invloed gehad. Op basis hiervan stelt de rijksinspectie dat de meetresultaten van de eerdere metingen waarheidsgetrouw zijn, met uitzondering van de resultaten van omvormer A en mogelijk die van omvormer B. Aan de resultaten van omvormer C en D (en de overige omvormers) heeft zij de juiste conclusie verbonden.

4.3.2 Voorstel tot normwijziging

Ook omvormer B werd (tegelijk met omvormer A) opnieuw gemeten op EMC-storing. Daarbij werd, in tegenstelling tot omvormer A, wel opnieuw een limietoverschrijding gemeten. In overleg met de fabrikant experimenteerde de RDI met verschillende meetopstellingen om de oorzaak van de limietoverschrijding te achterhalen. Bij die metingen was de fabrikant zelf ook aanwezig, op uitnodiging van de rijksinspectie.

De RDI concludeerde uiteindelijk dat de in eerste instantie gebruikte meetopstelling, mogelijk ontoereikend is voor de technische specificaties van omvormer B. Een

norm gaat uit van bepaalde productspecificaties. Het al dan niet aarden van een apparaat bijvoorbeeld. Voor omvormers waarvan het de bedoeling is deze niet te aarden, is de gebruikte norm volgens de RDI mogelijk onvolledig. Omvormers B kan hierdoor niet beoordeeld worden op basis van deze geharmoniseerde norm. Voor de overige omvormers (inclusief omvormer A, B en C) geldt dit niet. Daardoor is de gebruikte norm wel geschikt voor die omvormers.

De RDI is van plan om een voorstel in te dienen voor een wijziging van de norm. Dit gaat zij doen in samenwerking met de fabrikant van omvormer B. De rijksinspectie gaat ervan uit dat het 'gat' dat de norm nu bevat voor bepaalde soorten omvormers, zo wordt gedicht. Overigens neemt dit niet de verantwoordelijkheid van de betreffende fabrikant weg, voor eventueel storende omvormers. De RDI verwacht nog steeds dat de fabrikant maatregelen neemt om storing en het verhandelen van non-conforme apparatuur, te voorkomen.

4.4 Breder perspectief

Verder is op dit moment de branche aan zet. De RDI wil niet dat er alleen werk wordt gemaakt van de nu onderzochte omvormers en accessoires. Iedere omvormer of accessoire die op de markt wordt gebracht, hoort te voldoen. Om die reden is het mogelijk dat de rijksinspectie bij een hercontrole een ander model omvormer onderzoekt. Ook hoopt de rijksinspectie dat andere fabrikanten, die nu niet zijn onderzocht, zich bewust zijn van de wettelijke eisen en het stoorpotentieel van de onderdelen van zonnepaneelinstallaties.

Aan de andere kant voert de RDI gesprekken met brancheorganisaties voor het creëren van bewustzijn en om de branche naar de juiste richting te helpen als het gaat om de productie van de onderdelen van zonnepaneelinstallaties. Uiteindelijk ligt de verantwoordelijkheid voor het op de markt brengen van veilige en storingsvrije apparatuur echter volledig bij fabrikanten, importeurs en distributeurs.

5 Conclusie

De RDI maakt zich ernstige zorgen over een groot deel van de PV-omvormers dat op de markt wordt gebracht. De naleving van de eisen die Nederland storingsvrij moeten houden, is ondermaats en niet zoals het moet zijn. Daarnaast is het slecht gesteld met de cyberveiligheid. Dit maakt onze analoge en digitale infrastructuur kwetsbaar, zeker nu het aantal zonnepaneelinstallaties in ons land met de dag groeit.

Om ervoor te zorgen dat iedereen ook in de toekomst probleemloos gebruik kan maken van (draadloze) apparaten en de digitale weerbaarheid van onze energievoorziening is geborgd, is nu actie nodig.

5.1 Stoorpotentieel

Eén van de belangrijkste conclusies van dit onderzoek, is dat als de handel in PV-omvormers doorgaat zonder extra aandacht voor conformiteit en stoorpotentieel, dit ernstige consequenties kan hebben. Die mogelijke consequenties zijn tweeledig.

Enerzijds werd in dit onderzoek per merk één (in één geval twee) omvormer gemeten. Meer dan de helft van die omvormers produceerde storing. In zo'n individueel geval heeft dat misschien niet altijd en direct een aanzienlijk en merkbaar effect. Radiocommunicatie werkt niet continu, maar valt ook niet volledig uit. Een voorbeeld, ter illustratie: een hele straat ligt vol met storende zonnepaneelinstallaties. De storing 'stapelt' zich 'op' en wordt sterker. De kans dat andere (draadloze) apparaten en toepassingen slecht of niet werken wordt dan steeds groter.

In werkelijkheid liggen die zonnepaneelinstallaties niet in slechts één of twéé straten. Deze liggen inmiddels verspreid door heel Nederland. Soms tot wel duizenden panelen bij elkaar. Als deze niet voldoen aan de eisen voor EMC, dan zijn dit in potentie stuk voor stuk storingsbronnen. Vanwege het cumulatieve effect hebben storende omvormers dus wél een aanzienlijk en merkbaar effect. Ook draagt dit bij aan het algehele storingsniveau in de ether, waardoor deze steeds minder goed bruikbaar wordt.

Anderzijds maken organisaties, defensie en bijvoorbeeld C2000 planningen voor de dekking van hun netwerk. Daarin wordt bepaald op welke locaties antennes en zendmasten nodig zijn om in een zo groot mogelijk gebied te kunnen communiceren. Dit is vergelijkbaar met de dekkingsplannen van mobiele providers. De situatie is nu zo dat in dat soort planningen al rekening wordt gehouden met hinderlijke en storende apparaten. Volgens de RDI is dit een ernstige ontwikkeling. Het incalculeren van storing is maar tot in een bepaalde mate werkbaar, omdat frequentieruimte niet onbeperkt is. In het meest extreme geval zijn er op een dag zoveel storende zonnepaneelinstallaties, dat daar niet meer omheen 'te plannen' valt. Dan is het te laat om dit probleem relatief eenvoudig te kunnen herstellen.

5.2 Essentiële eisen en geharmoniseerde normen

Daarnaast blijkt uit de bevindingen en de gesprekken met fabrikanten, dat er te weinig rekening wordt gehouden met praktijksituaties bij de conformiteitsbeoordeling door fabrikanten. Dit komt voort uit het ontbreken van risicoanalyses in de technische documentatie, en het feit dat fabrikanten de geharmoniseerde norm in plaats van de essentiële eisen als uitgangspunt nemen.

Veel fabrikanten zijn (ten onrechte) in de veronderstelling dat het voldoen aan een geharmoniseerde norm automatisch betekent dat er wordt voldaan aan de essentiële eisen van de richtlijnen. Met als gevolg het risico dat een product wel voldoet in een laboratoriumsituatie, maar niet in daadwerkelijk gebruik.
De essentiële eisen zijn leidend en wettelijk vastgesteld. Een (geharmoniseerde) norm is dit niet, en dient 'slechts' als hulpmiddel (aangevuld met bijvoorbeeld een risicoanalyse en andere oplossingen). De RDI ziet deze misvatting overigens in meer sectoren.

5.3 Conclusie cyberaspecten

De laatste conclusie uit dit onderzoek is, dat de mate van cyberveiligheid van omvormers, en daarmee zonnepaneelinstallaties, slecht is. De wettelijke eisen hiervoor zijn weliswaar nog niet actief, maar ook nu vormen digitale kwetsbaarheden een groot risico. Met het toenemende aantal zonnepaneelinstallaties in Nederland, wordt de samenleving steeds afhankelijker van deze vorm van energievoorziening. Het is volgens de RDI onacceptabel dat producten die zo belangrijk zijn voor vitale processen, tal van onbeschermde digitale ingangen bevatten. Daarmee kunnen kwaadwillenden schade aanrichten.

De kwetsbaarheden die blijken uit dit onderzoek kunnen leiden tot zeer onwenselijke situaties. Zo zijn (grootschalige) hacks van zonnepaneelinstallaties denkbaar, waarbij in het meest extreme geval een groot deel van de installaties in Nederland tegelijk wordt uitgeschakeld. Of worden de instellingen van installaties gemanipuleerd of installaties gebruikt voor DDOS-aanvallen. Dit kan schade aanrichten aan vitale infrastructuur. Daarnaast is de privacy van gebruikers in gevaar. Persoonsgegevens en andere data, over bijvoorbeeld stroomverbruik en -opbrengst, kunnen worden onderschept of gestolen.

5.4 Verdere vervolgacties RDI

In het voorgaande hoofdstuk werd al beschreven dat de fabrikanten van de RDI een waarschuwing ontvingen voor de wetsovertredingen. Over een redelijke termen volgen hercontroles en treedt de rijksinspectie mogelijk handhavend op. Daarnaast zoekt de RDI de verbinding met brancheorganisaties.

Dit zijn niet de enige acties die worden ondernomen. Naast dit onderzoek en bijbehorende hercontroles, wordt de PV-markt nauwlettend in de gaten gehouden en vinden meer onderzoeken plaats. Dit kunnen projectmatige onderzoeken zijn, zoals deze. Ook kunnen dit onderzoeken zijn naar aanleiding van (storings)meldingen over individuele omvormers. Zo zijn er in de afgelopen jaren, naast de 9 omvormers uit dit onderzoek, meer omvormers onderzocht door de RDI en werden fabrikanten naar aanleiding daarvan gewaarschuwd of gesanctioneerd. Daarnaast treft de RDI op dit moment voorbereidingen voor een tweede projectmatig onderzoek naar omvormers, dat vergelijkbaar is met dit onderzoek.

5.5 Handelingsperspectief consument

Fabrikanten zijn verantwoordelijk voor de conformiteit van hun producten. Logischerwijs hebben zij de mogelijkheden en invloed om storingsvrije en cyberveilige apparatuur op de markt te brengen. Alleen betekent dit niet dat consumenten hier zelf niets aan kunnen doen.

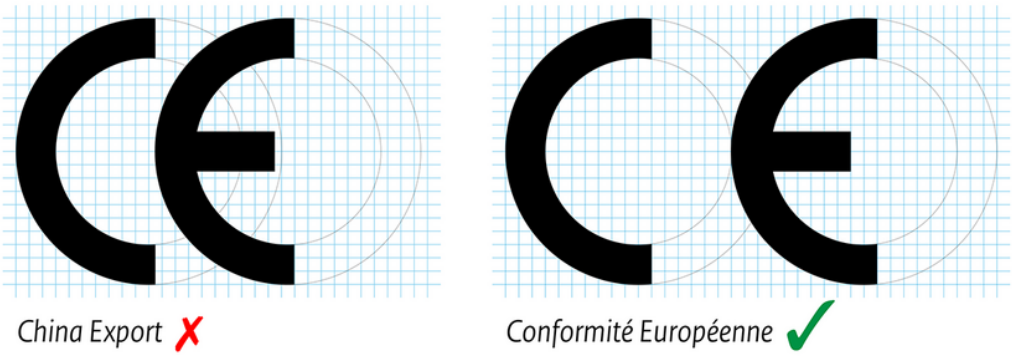
5.5.1 CE-markering

Om te beginnen kunnen gebruikers altijd controleren of een product CE-gemarkeerd is. Uit dit onderzoek blijkt dat in sommige gevallen de CE-markering onterecht op het product is aangebracht. De aanwezigheid van de CE-markering is echter

eenvoudig vast te stellen. En als deze niet is aangebracht, dan voldoet het product zeker niet aan de Europese eisen. Ook voor het formaat van de markering en de afstand tussen de letters gelden eisen.

De figuur op de volgende pagina laat twee markeringen zien: een veelvoorkomende markering die lijkt op de CE-markering, maar dit niet is en de juiste CE-markering.[6]

Figuur 1
China Export-logo en de CE-markering met de wettelijk bepaalde vorm en afmetingen[7]



5.5.2 *Alert op storingen*

Storingen zijn (nu nog) lastig waarneembaar voor burgers. Dit heeft ermee te maken dat de gemiddelde burger beperkte kennis heeft van het radiospectrum. Bij bijvoorbeeld trage Wi-Fi doen zij niet snel een melding. De RDI sluit echter niet uit dat zonnepaneelinstallaties ook op die toepassingen storen.

Daarom kunnen consumenten alerter zijn op storingen. Werkt bijvoorbeeld de radio probleemloos op een bewolkte dag, maar hapert deze zodra de zon schijnt? Dan kan dit een teken zijn dat een zonnepaneelinstallatie of een installatie in de omgeving stoort. Hetzelfde geldt voor bijvoorbeeld de Wi-Fi-verbinding.

Daarnaast kan de manier waarop een zonnepaneelinstallatie is geïnstalleerd, ook invloed hebben op het stoorgedrag van de installatie. Dat heeft bijvoorbeeld te maken met de manier waarop kabels worden gelegd. Consumenten kunnen hier ook op letten. Zo kunnen zij installateurs herinneren aan hun verantwoordelijkheid om zonnepalen storingsvrij te aan te leggen. Uiteraard moeten de omvormer en andere onderdelen wel voldoen aan de eisen. Als dit niet het geval is, kan ook een juist aangelegde installatie storen.[8]

5.5.3 *Cyberaspecten*

Cyberveiligheid hebben consumenten voor een belangrijk deel ook zelf in de hand. Om de gevaren van apparatuur te verminderen, kunnen mensen op het volgende letten:

- Stel sterke en unieke wachtwoorden in (denk hierbij aan een wachtwoord met een combinatie van kleine en grote letters, cijfers, leestekens en

[6] Voor meer informatie over de CE-markering, zie https://www.rdi.nl/onderwerpen/stoor-ik/ce-markering.
[7] De wettelijk bepaalde vorm en afmetingen van de CE-markering zijn vastgelegd in EU-verordening 765/2008.
[8] Voor meer en concrete tips over de installatie van zonnepanelen en het voorkomen van storing, zie https://www.rdi.nl/onderwerpen/tips/voorkom-storingen-door-zonnepanelen.

symbolen). Als een apparaat een standaardwachtwoord heeft, verander deze dan direct bij het eerste gebruik.
- Controleer regelmatig of er updates beschikbaar zijn.
- Als het apparaat wordt verbonden met een Wi-Fi netwerk, doe dit dan via een netwerkverbinding die losstaat van het hoofdnetwerk. Bijvoorbeeld een gastnetwerk.
- Schakel tweefactor-authenticatie in als dit mogelijk is.
- Bedenk of het nodig is dat het apparaat met het internet verbonden is. Is dit niet het geval, dan kunt u het apparaat misschien beter niet met het internet verbinden, om onnodige risico's te vermijden.
- Wees tot slot ook kritisch of het nodig is om bepaalde (persoons)gegevens te verstrekken.

Met de bovenstaande acties kunnen consumenten de kans op een groot aantal risico's verkleinen. Bijvoorbeeld dat gegevens over energieopbrengst of persoonsgegevens inzichtelijk zijn voor buitenstaanders of worden misbruikt. Of dat zonnepaneelinstallatie bewust wordt uitgeschakeld door derden. Daardoor ligt de energievoorziening van een huishouden stil. Ook dragen consumenten hiermee uiteindelijk bij aan de veiligheid van de gezamenlijke digitale infrastructuur en samenleving.