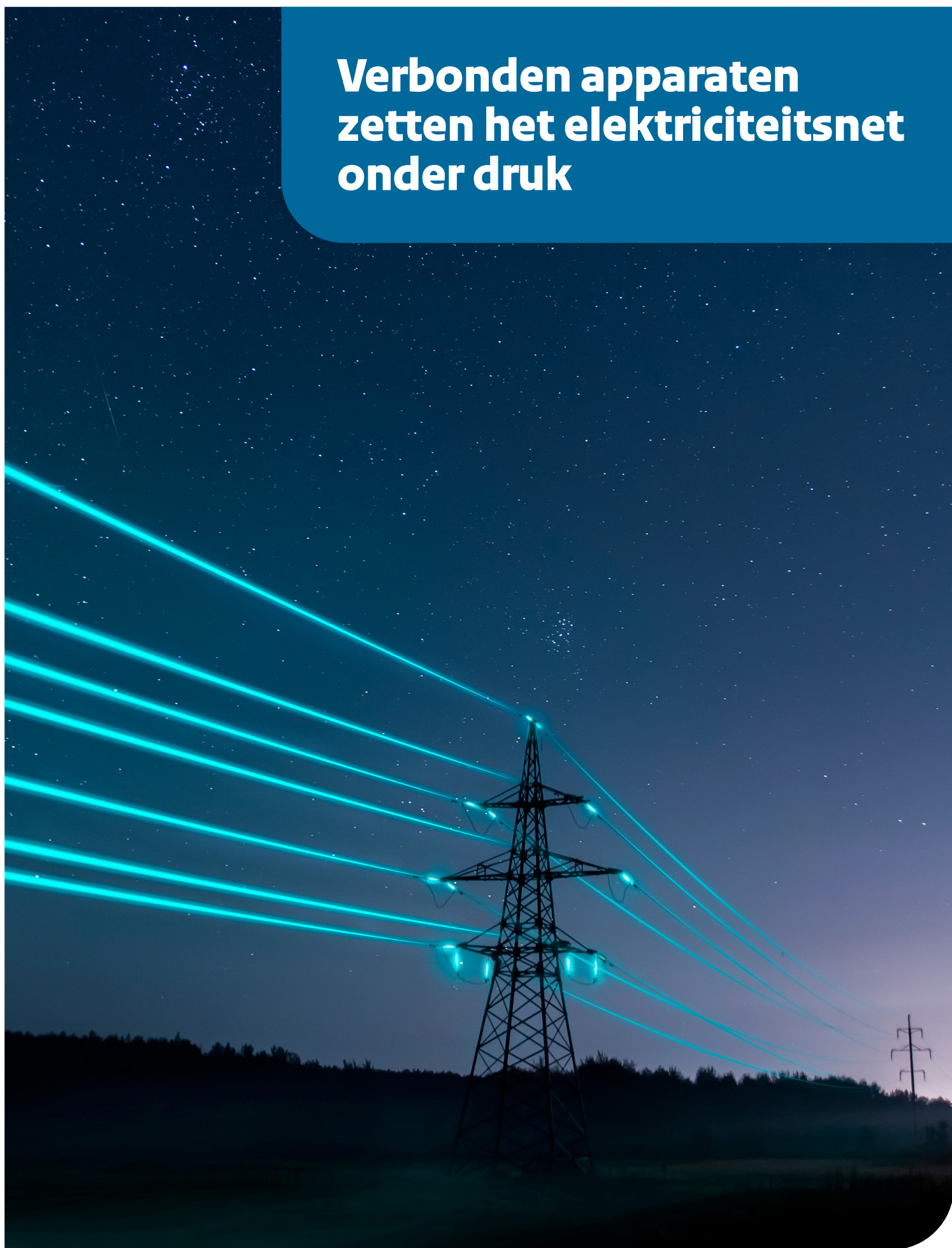




Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Verbonden apparaten zetten het elektriciteitsnet onder druk



Hoofdboodschap

Steeds meer high-power IoT-apparaten zijn verbonden aan het elektriciteitsnetwerk. Dit brengt risico's voor de stabiliteit van het net met zich mee.

Wanneer een groot aantal high-power IoT-apparaten tegelijkertijd beïnvloed wordt, kan dit de stabiliteit van het elektriciteitsnet beïnvloeden. High-power IoT-apparaten kunnen op verschillende manieren op afstand beïnvloed worden. Verstoringen kunnen optreden als er foutieve updates of instellingen zijn doorgevoerd. Ook kunnen verstoringen optreden als er kwetsbaarheden worden uitgebuit of als fabrikanten of aanbieders worden gedwongen door staten met kwaadwillende bedoelingen.

Bestaande wet- en regelgeving, zoals de Cyber Resilience Act (CRA) en NIS2-richtlijn, vangt enkel een deel van deze risico's af. Voor high-power IoT-apparaten stelt de CRA slechts algemene cybersecurityeisen. De NIS2-richtlijn is in de basis alleen van toepassing op organisaties van een bepaalde grootte, ongeacht het vermogen dat zij kunnen aansturen, en is beperkt van toepassing op organisaties buiten de Europese Unie. In de Netcode voor Cybersecurity (NCCS) is er ook nog beperkte aandacht voor high-power IoT.

Er zijn verschillende invalshoeken om het risico van high-power IoT-apparaten te mitigeren, waaronder juridisch, governance, economisch, technisch en systeemontwerp. Dit position paper richt zich vanuit een juridische invalshoek op de cybersecurityverantwoordelijkheden van partijen en definieert hiervoor drie oplossingsrichtingen:

DRIE OPLOSSINGSRICHTINGEN

1

Het stellen van specifieke cybersecurityeisen aan high-power IoT-apparaten en bijbehorende backend.

2

Het stellen van passende cybersecurityeisen aan partijen die op afstand veel vermogen via high-power IoT kunnen beïnvloeden.

3

Het nemen van aanvullende maatregelen om digitale autonomie te versterken.

Aanleiding en probleemdefinitie

HIGH- POWER IOT

Internetverbonden apparaten bij consumenten en bedrijven, zoals zonne-omvormers, thuisaccu's en laadpalen, die samen een groot elektrisch vermogen vertegenwoordigen.

INHOUD

01 Aanleiding en probleemdefinitie	3
02 Stabiliteit van het elektriciteitsnet	4
03 High-power IoT	6
04 Hoe kan high-power IoT beïnvloed worden?	8
05 Waardoor kunnen verbonden apparaten de balans verstoren?	10
06 Relevante wet- en regelgeving	11
07 Uitgangspositie	15
08 Oplossingsrichtingen	15

De energietransitie brengt een snelle digitalisering van het elektriciteitsnet met zich mee.

Deze digitalisering vindt plaats in het elektriciteitsnet van de netbeheerders, evenals bij aangesloten apparaten van consumenten en bedrijven, zoals zonne-omvormers, thuisaccu's en laadpalen.¹ Deze internetverbonden apparaten worden gezamenlijk high-power Internet of Things (IoT) genoemd. De aansluiting van steeds meer van dergelijke apparaten biedt kansen voor efficiënter gebruik van het elektriciteitsnet. Bijvoorbeeld door te sturen op congestie en energieprijzen. Het brengt echter ook nieuwe cybersecurityrisico's met zich mee die de betrouwbaarheid, beschikbaarheid en veiligheid van de energievoorziening in gevaar kunnen brengen.

High-power IoT-apparaten kunnen via internet worden bestuurd, waardoor deze op afstand gelijktijdig in- of uitgeschakeld kunnen worden. Het tegelijkertijd beïnvloeden van een grote hoeveelheid apparaten kan leiden tot grote plotselinge schommelingen in de opwek en afname van elektriciteit. Deze schommelingen kunnen leiden tot verstoringen of uitval van het elektriciteitsnet. De vraag is hoe deze risico's op uitval beperkt kunnen worden, terwijl tegelijkertijd de kansen die digitalisering biedt benut kunnen blijven worden.

'De vraag is hoe deze risico's op uitval beperkt kunnen worden, terwijl tegelijkertijd de kansen die digitalisering biedt benut kunnen blijven worden.'

In dit position paper worden mogelijke oplossingsrichtingen gepresenteerd. Hiervoor wordt eerst de stabiliteit van het elektriciteitsnet uitgelegd, daarna wordt ingegaan op high-power IoT. Vervolgens wordt besproken hoe beïnvloeding van een groot aantal high-power IoT-apparaten kan plaatsvinden en welke wet- en regelgeving van toepassing is. Dit position paper sluit af met mogelijke oplossingsrichtingen om de risico's voor de stabiliteit van het elektriciteitsnet te verkleinen.

¹ <https://www.rdi.nl/actueel/nieuws/2021/07/12/kwetsbare-digitale-infrastructuur-vormt-risico-voor-energietransitie>

Stabiliteit van het elektriciteitsnet: Hoe werkt dit?

50 Hz

De netfrequentie is in balans als deze 50 hertz is.

49,99–50,01 Hz

Buiten deze band activeren de grote netbeheerders de frequentiecontrole.

3 GW

Vanaf dit vermogen kan een plotselinge onbalans in vraag en aanbod tot verstoringen leiden.²

Het is belangrijk dat het elektriciteitsnet in balans is om uitval te voorkomen.

De grote netbeheerders zijn verantwoordelijk voor het handhaven van de netfrequentie. Op het moment dat zowel de opwek als de afname van energie in het hele net gelijk zijn, is het systeem in balans. De netfrequentie is in balans als deze 50 Hertz (Hz) is. Als dit niet zo is, zijn er mogelijkheden om de balans te herstellen. Een te grote onbalans zorgt voor uitval van het elektriciteitsnet.

Inertie is een belangrijke factor om te voorkomen dat de frequentie gelijk instort als de opwek en afname van energie niet gelijk zijn. Inertie is de massa-traagheid van grote draaiende turbines en generatoren in bijvoorbeeld traditionele gas- en kolencentrales of van speciaal daarvoor ingerichte installaties. De werking van inertie is vergelijkbaar met een rijdende auto die langzaam snelheid mindert wanneer de bestuurder het gaspedaal loslaat; de auto staat niet direct stil. Inertie geeft tijd om balans te herstellen: doordat de frequentie niet te snel verandert, is er tijd om met andere middelen het net weer in balans te krijgen.

Wanneer de frequentie buiten de band van 49,99–50,01 Hz komt, wordt door de grote netbeheerders de frequentiecontrole geactiveerd om de balans te herstellen. Het elektriciteitsnet in Nederland is onderdeel van een veel groter elektriciteitsnet: het continentaal-Europese synchrone gebied (CESA). Op het moment dat er een onbalans is, werken alle grote netbeheerders uit de bij CESA aangesloten landen samen om de frequentie weer te herstellen.

Uit onderzoek blijkt dat vanaf 3 GW een plotselinge onbalans in vraag en aanbod op het elektriciteitsnet tot verstoringen kan leiden.² Daarnaast zullen incidenten die leiden tot een afname van 1 Hz per seconde van de netfrequentie in ieder geval leiden tot grote gevolgen, omdat beschermingsmechanismen niet op tijd kunnen bijspringen.³ Naast opwek of gebruik van elektriciteit kan ook de spanningskwaliteit aangetast worden, met invloed op de stabiliteit van het net.

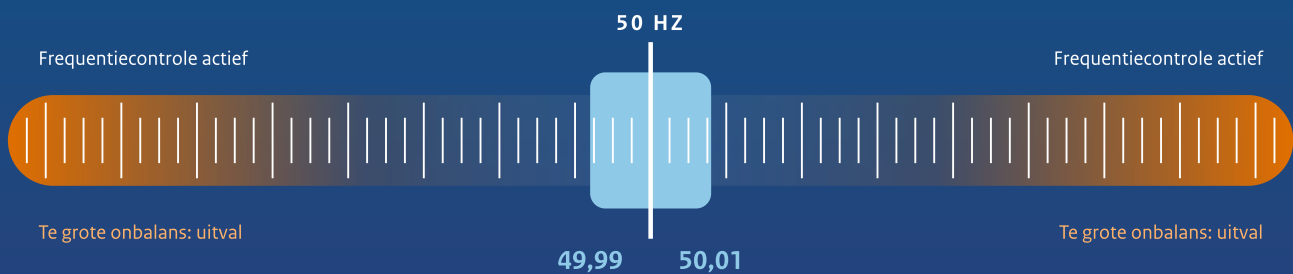
² <https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability>

³ https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Inertia%20and%20RoCoF_v17_clean.pdf, p. 43

Het net in balans

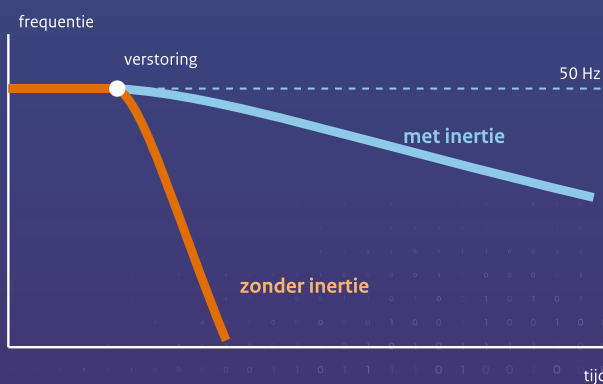


Opwek en afname zijn gelijk: de netfrequentie is 50 Hz.



De frequentieband waarbinnen het net als 'in balans' geldt.

Inertie geeft tijd



Zoals een auto die uitrolt als je het gaspedaal loslaat: grote draaiende turbines en generatoren remmen de daling van de frequentie af.

1 Hz/s

Daalt de netfrequentie met 1 Hz per seconde, dan volgen in ieder geval grote gevolgen: beschermingsmechanismen kunnen niet op tijd bijspringen.

3 GW

Vanaf dit vermogen kan een plotselinge onbalans tot verstoringen leiden.

CESA

Het Nederlandse net is onderdeel van het continentaal-Europese synchrone gebied. Bij onbalans herstellen de netbeheerders samen de frequentie.

High-power IoT

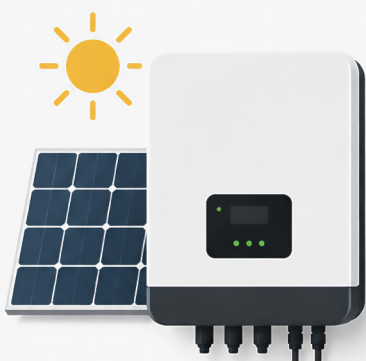
DEFINITIE

Apparaten die via een internetverbinding tegelijkertijd kunnen worden beïnvloed, waardoor in totaal een groot elektrisch vermogen beïnvloed kan worden. Het gaat om zowel opwek als afname.

In dit position paper wordt high-power Internet of Things (IoT) gedefinieerd als apparaten, in gebruik door zowel consumenten als bedrijven, die via een internetverbinding tegelijkertijd kunnen worden beïnvloed en waardoor in totaal een groot elektrisch vermogen beïnvloed kan worden.

Vermogen kan zowel gaan om opwek als afname van elektriciteit. Een aantal voorbeelden van high-power IoT-apparaten die gezamenlijk een groot elektrisch vermogen kunnen hebben, zijn hieronder te vinden.

VOORBEELDEN VAN HIGH-POWER IOT



01 - Zonne-omvormers



02 - Thuisbatterijen



03 - Laadpalen voor EV's



04 - Warmtepompen

Een sterke toename

5_x

zoveel warmtepompen
enlaadpalen in 2024 als in 2019.

Er is de afgelopen jaren een sterke toename
in het aantal high-power IoT-apparaten.

Denk hierbij niet alleen aan energiegerelateerde apparaten, maar ook aan internetverbonden ovens, wasmachines en vaatwassers. Het totale vermogen dat tegelijkertijd beïnvloed kan worden, neemt hierdoor ook toe, omdat groepen van deze apparaten via internet vaak verbonden zijn met eenzelfde digitale backend. In de grafiek hieronder is de toename van 2019–2024 in de aantallen zonne-installaties op woningen⁴, thuisbatterijen⁵, laadpalen voor EV's⁶ en warmtepompen voor woningen⁷ te zien.

⁴ <https://opendata.cbs.nl/#/CBS/nl/dataset/85005NED/table?dl=C48B0>

⁵ <https://www.deb.nl/wp-content/uploads/2025/03/2025-Nationaal-Solar-Trendrapport.pdf>

⁶ https://www.rvo.nl/sites/default/files/2025-12/Rapport_economische_betekenis_en_ontwikkeling_van_sector_elektrisch_vervoer_RVO.pdf, p. 13

⁷ <https://opendata.cbs.nl/#/CBS/nl/dataset/85523NED/table>

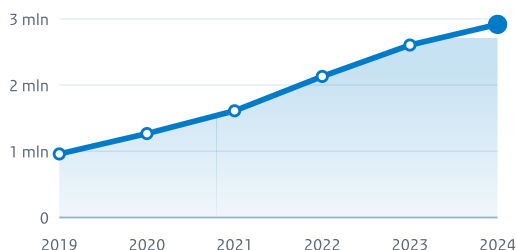
Toename van high-power IoT in Nederland, 2019–2024

Aantal apparaten per jaar. Let op:
elke grafiek heeft een eigen schaal.

Zonne-installaties op woningen

2.916.906

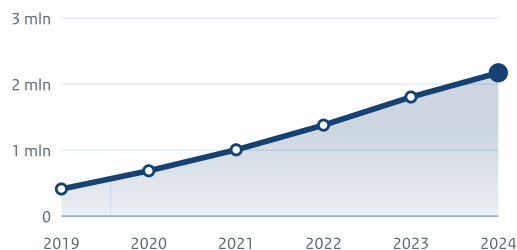
in 2024
3× zoveel als in 2019



Warmtepompen voor woningen

2.172.867

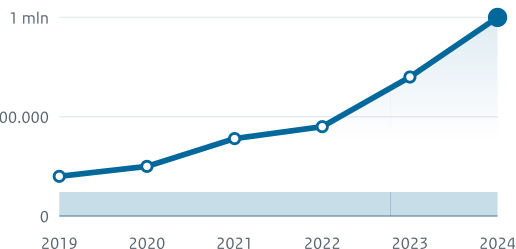
in 2024
5× zoveel als in 2019



Laadpalen voor EV's

1.000.000

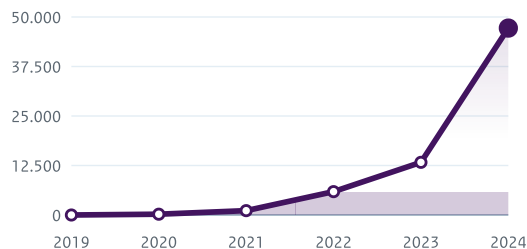
in 2024
5× zoveel als in 2019



Thuisbatterijen

47.200

in 2024
van 200 in 2020 naar 47.200



Bronnen: zie voetnoten 4 tot en met 7

Hoe kan high-power IoT beïnvloed worden?

High-power IoT kan op verschillende manieren gelijktijdig, op grote schaal en op afstand beïnvloed worden. Vijf partijen spelen daarbij een rol.



Fabrikant

High-power IoT heeft bijna altijd een internetverbinding naar de fabrikant van het apparaat. Via deze internetverbinding kunnen de instellingen (configuratie) van het apparaat aangepast worden. Ook kan de interne software (firmware) van de apparaten geüpdatet worden. Daarnaast maken fabrikanten webportalen en digitale koppelingen (Application Programming Interfaces, API's) beschikbaar, waar derde partijen mee kunnen communiceren om via de backend van de fabrikant het apparaat uit te lezen of aan te sturen.



Energy Management Systeem (EMS)

Een EMS monitort het energiegebruik van apparaten en stuurt deze aan. De aansturing vindt plaats via het internet via het API-systeem van de fabrikant of via het lokale netwerk waarop EMS en high-power IoT-apparaat zijn aangesloten.



Cloudplatformen

Fabrikanten en EMS maken vaak gebruik van cloudplatformen om hun backend op te laten draaien. Dat kunnen infrastructuur- en platformdiensten van grote technologiebedrijven zijn. Ook kunnen fabrikanten en EMS'en gebruik maken van andere gedeelde platformen voor het monitoren en aansturen van high-power IoT.



Aggregatoren

Aggregatoren sturen op afstand elektriciteitsgebruik of -opwek van klanten aan om op elektriciteitsmarkten voor zichzelf en de klant financieel voordeel te behalen.



Installateurs

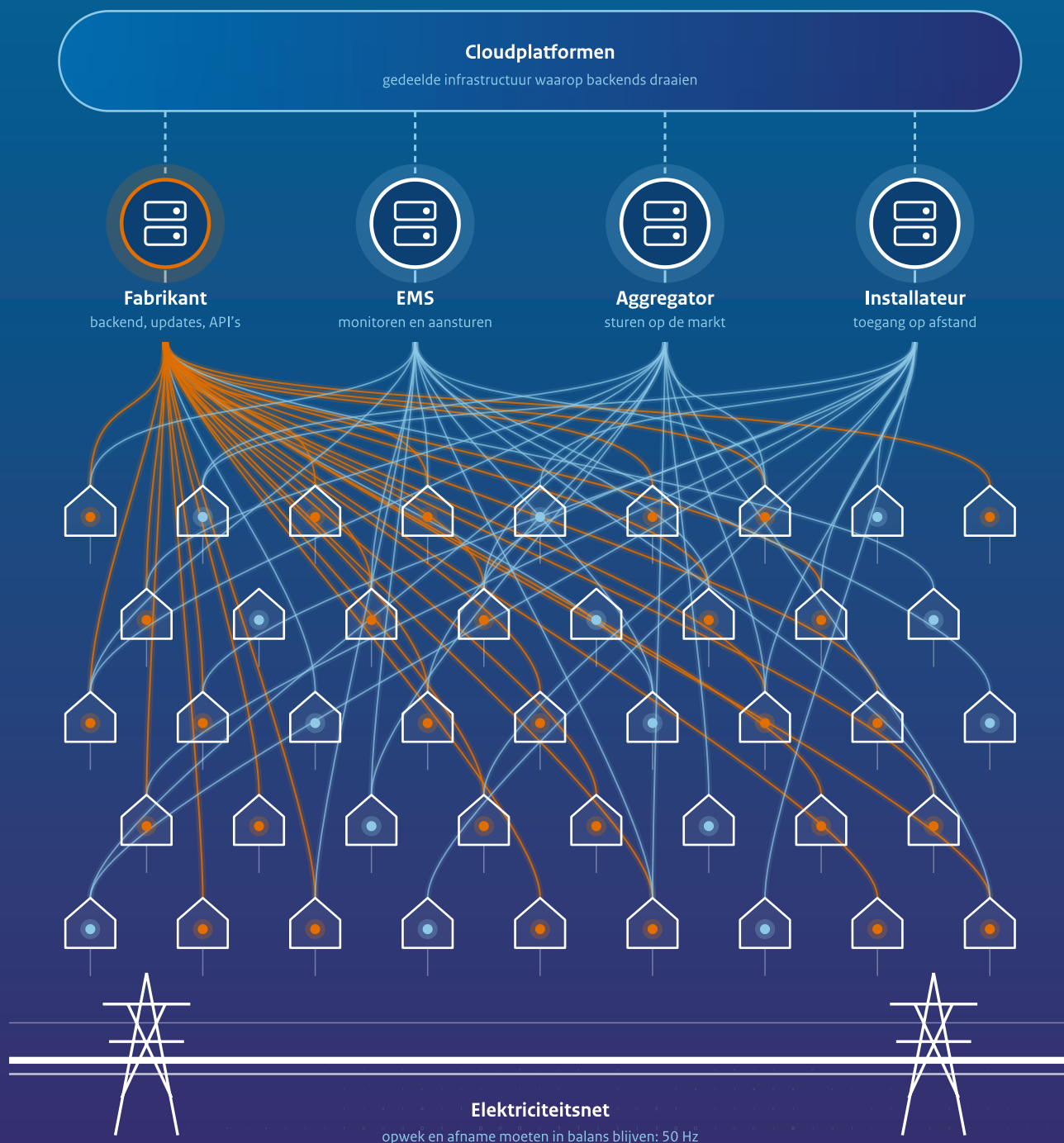
Installateurs hebben vaak op afstand toegang tot high-power IoT-apparaten om deze te monitoren en te onderhouden. Dit kan via kanalen van de fabrikant of via een afzonderlijk geïnstalleerde oplossing.

ÉÉN BACKEND

Een groot aantal apparaten

Groepen apparaten zijn via internet vaak verbonden met eenzelfde digitale backend. Daardoor kan een groot aantal apparaten tegelijk beïnvloed worden. Zie de illustratie op de volgende pagina.

Van backend tot elektriciteitsnet



Een illustratieve weergave van high-power apparaten verbonden met het elektriciteitsnetwerk en de backend van de fabrikant, EMS en/of aggregatoren.

— Aansturing via internet — Eén backend, vele apparaten — Elektriciteitsnet

Waardoor kunnen verbonden apparaten de balans verstoren?

De werking van high-power IoT en daarmee de afname of de opwek van elektriciteit kan op verschillende manieren beïnvloed worden.

1

Ten eerste kan er een verstoring van de werking optreden door foutieve updates of instellingen. De fabrikant kan een foutieve update of verkeerde instelling sturen naar het high-power IoT-apparaat, waardoor het onbedoeld gedrag vertoont. Dit is vergelijkbaar met een recent incident waarbij wereldwijd computerstoringen werden veroorzaakt.⁸ Hetzelfde geldt voor andere partijen die de mogelijkheid hebben om op afstand instellingen te veranderen, zoals EMS, aggregatoren en installateurs.

2

Ten tweede kunnen kwetsbaarheden uitgebuit worden. Cybercriminelen, hackers en statelijke actoren kunnen misbruik maken van kwetsbaarheden in high-power IoT. Deze kwetsbaarheden kunnen in individuele apparaten zitten of in de digitale infrastructuur waarmee ze op afstand aangestuurd worden. Via kwetsbaarheden in de digitale infrastructuur van de fabrikant, EMS, aggregator en de cloudplatformen die zij gebruiken, kan de werking van grote aantallen high-power IoT-apparaten negatief worden beïnvloed.^{9/10/11}

3

Ten derde kan de werking worden beïnvloed door kwaadwillende staten. Zij kunnen over dwangmiddelen beschikken om fabrikanten en aanbieders van EMS, aggregatoren en cloudplatformen die onder hun jurisdictie vallen tot medewerking te dwingen.^{12/13}

Het grootste risico voor gelijktijdige beïnvloeding van een groot aantal high-power IoT-apparaten ligt bij de **backendsystemen** van fabrikanten, EMS en aggregatoren en de cloudplatformen die zij gebruiken.

⁸ <https://nos.nl/artikel/2529477-wat-is-crowdstrike-en-hoe-kon-het-zo-misgaan-dit-is-wat-we-nu-weten>

⁹ <https://www.forescout.com/blog/the-security-risks-of-internet-exposed-solar-power-systems/>

¹⁰ <https://www.forescout.com/blog/grid-security-new-vulnerabilities-in-solar-power-systems-exposed/>

¹¹ <https://www.divd.nl/newsroom/articles/91cd52191c65/>

¹² <https://www.aivd.nl/documenten/2025/07/17/dreigingsbeeld-statale-actoren-2025>

¹³ <https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025>

Relevante wet- en regelgeving

PRODUCTCATEGORIEËN CRA

Kritiek

Nog zwaardere eisen

Belangrijk, klasse 2

Altijd controle door een beoordelingsinstantie

Belangrijk, klasse 1

Europese standaard óf beoordelingsinstantie

Overige producten

Zelfbeoordeling door de fabrikant

- **High-power IoT valt nu hier**

11 dec 2027

Vanaf deze datum moeten nieuwe producten op de Europese markt voldoen aan de CRA.

Wet- en regelgeving speelt een rol bij het beperken van de risico's van high-power IoT.

Hierin worden eisen gesteld aan (fabrikanten van) producten, gebruikers ervan en partijen zoals EMS-aanbieders, aggregatoren en cloudplatformen.

Cyber Resilience Act (CRA)

De CRA regelt de digitale veiligheid van digitale producten. Dit zijn hardware en software en bijbehorende digitale backend die nodig is voor een goede en veilige werking van het product. Ook high-power IoT producten vallen onder de CRA. Vanaf 11 december 2027 dienen al deze producten die in de EU op de markt worden gebracht te voldoen aan de CRA. De CRA kent algemene cybersecurityeisen en biedt ook de mogelijkheid om deze verder in te vullen met gedetailleerde standaarden.

Meestal mag de fabrikant zelf beoordelen of zijn producten voldoen aan de CRA-eisen om het product op de markt te brengen. Dat kan onvoldoende zijn gezien de risico's die samenhangen met een product. Daarom bevat de CRA ook een lijst van belangrijke 'klasse 1'-producten. Daarvoor moet de fabrikant een gedetailleerde Europese veiligheidsstandaard gebruiken voor de zelfcontrole of het product laten controleren door een beoordelingsinstantie. Een tweede uitzondering zijn belangrijke 'klasse 2'-producten, waarbij altijd een beoordelingsinstantie moet controleren of aan de eisen van de CRA is voldaan. Ten slotte zijn er kritieke producten waarvoor nog zwaardere eisen gelden. De CRA biedt de mogelijkheid om later nieuwe soorten van producten belangrijk of kritiek te maken.

De verschillende soorten high-power IoT worden op dit moment niet als belangrijk of kritiek product onder de CRA gezien.

Ook zijn er geen gedetailleerde Europese veiligheidsstandaarden om de cybersecurity van high-power IoT tegen te beoordelen. Ten slotte gelden de cybersecurityeisen van de CRA niet voor producten die al vóór 11 december 2027 op de markt zijn gebracht, tenzij ze daarna ingrijpend zijn gewijzigd.

VALLen (NOG) BUITEN DE REGELS

- Partijen met een **kleine bedrijfsomvang** die wel veel vermogen kunnen aansturen
- Energiepartijen en fabrikanten **zonder vestiging in de EU**
- Fabrikanten en EMS-aanbieders: **nog niet in de voorlopige NCCS-lijst**

TIJDLIJN

- **Okt 2026**
Publicatie position paper
- **11 dec 2027**
Nieuwe producten moeten voldoen aan de CRA
- **Medio 2028**
NCCS-verplichtingen gaan in
- **In ontwikkeling**
RfG 2, DCC 2 en CSA2

Netwerk- en informatiebeveiligingsrichtlijn (NIS2-richtlijn)

De NIS2-richtlijn, in Nederland geïmplementeerd in de Cyberbeveiligingswet (Cbw), verplicht een afgebakende groep van organisaties om hun cybersecurityrisico's te beheersen en om incidenten te melden. De Cbw is onder andere van toepassing op specifieke soorten organisaties binnen de energiesector die in Nederland gevestigd zijn en een middelgrote of grotere economische omvang hebben. Het gaat voor elektriciteit om elektriciteitsleveranciers, netbeheerders, producenten, elektriciteitsmarktbeheerders, organisaties die opslag, aggregatie of vraagsturing leveren op elektriciteitsmarkten en exploitanten van laadpalen. Deze organisaties kunnen high-power IoT zelf gebruiken, bijvoorbeeld zonne-omvormers door een elektriciteitsproducent, of deze aansturen. Als deze organisaties een kleine omvang hebben en dus niet automatisch onder de wet vallen, kunnen ze door de minister alsnog onder de reikwijdte van de Cbw gebracht worden. De Cbw is ook van toepassing op aanbieders van cloudcomputingdiensten en van beheerde diensten en op fabrikanten. Of dat het geval is, hangt af van de vraag of de activiteiten die de betreffende partij uitvoert voldoen aan de specifieke definities die gegeven worden voor clouddiensten, beheerde diensten en fabrikant.

Kortom, de NIS2-richtlijn en daarmee de Cbw kent in het kader van high-power IoT beperkingen. Partijen met een kleine bedrijfsomvang (aantal werknemers, omzet en balanstotaal) die wel veel vermogen kunnen aansturen, vallen erbuiten, tenzij de minister ze heeft aangewezen. Energiepartijen en fabrikanten zonder vestiging in de EU vallen buiten de NIS2-richtlijn. Alleen voor clouddienstaanbieders en beheerders van ICT-diensten geldt dat zij ook zonder vestiging in de EU eronder vallen als zij in de EU diensten aanbieden en van voldoende omvang zijn.

Netcode voor Cybersecurity (NCCS)

Organisaties die een grote grensoverschrijdende impact op het elektriciteitsnet kunnen hebben, vallen onder de NCCS. Zij moeten verplichte cybersecuritymaatregelen treffen. Deze verplichtingen gaan medio 2028 in. Dergelijke organisaties kunnen ook onder het bereik van de NCCS vallen als ze individueel geen grote grensoverschrijdende impact kunnen hebben maar wel deel uitmaken van een groep die gelijktijdig getroffen kan worden en daarmee alsnog gezamenlijk een grote impact kan hebben.

De betreffende organisaties worden door de EU-lidstaten geïdentificeerd op basis van Europese criteria voor hoog-impact en kritieke processen en bijbehorende drempelwaarden. Hiervan is een eerste voorlopige versie gepubliceerd.¹⁴ Hierin worden onder andere aggregatoren, producenten, balansverantwoordelijken en exploitanten van laadpalen genoemd. In deze voorlopige lijst is er echter nog geen aandacht voor de andere partijen die invloed op high-power IoT kunnen hebben, zoals fabrikanten en aanbieders van EMS.

¹⁴ https://www.entsoe.eu/network_codes/nccs/

Welke regels raken welke partij?

Partij	CRA	NIS2 / Cbw	NCCS
Apparaat (product)	● Algemene eisen, zelfcontrole	— N.v.t.	— N.v.t.
Fabrikant en backend	● Algemene eisen, zelfcontrole	● Niet zonder vestiging in de EU, alleen bij voldoende omvang	○ Niet in voorlopige lijst
EMS-aanbieder	● Algemene eisen, zelfcontrole	● Afhankelijk van de bedrijfsactiviteiten, bij voldoende omvang	○ Niet in voorlopige lijst
Cloudplatform	—	● Ook zonder EU-vestiging, bij voldoende omvang	○ Niet in voorlopige lijst
Aggregator	—	● Middelgroot of grote omvang en in NL of EU gevestigd	● Genoemd in voorlopige lijst
Exploitant laadpalen	—	● Middelgroot of grote omvang en in NL of EU gevestigd	● Genoemd in voorlopige lijst
Installateur	—	○ Niet genoemd	○ Niet in voorlopige lijst

● Valt eronder ● Deels of onder voorwaarden ○ Valt erbuiten of niet genoemd — Niet van toepassing

Wet- en regelgeving in ontwikkeling

Momenteel wordt nog gewerkt aan wet- en regelgeving die kan helpen een deel van de risico's van high-power IoT te mitigeren. Het gaat hierbij om de Requirements for Generators 2, de Demand Connection Code 2 en de Cyber Security Act 2.

Requirements for Generators (RfG) 2 en Demand Connection Code (DCC) 2

De RfG en DCC stellen eisen aan apparatuur die wordt aangesloten op het elektriciteitsnet. Momenteel wordt gewerkt aan een nieuwe versie. Een belangrijke wijziging is dat bepaalde aangesloten apparaten, waaronder batterijen en elektrische auto's, laadpalen en warmtepompen niet alleen het elektriciteitsnet moeten volgen maar de stabiliteit daarvan ook actief dienen te ondersteunen.^{15/16} Ook dienen deze apparaten langer goed te kunnen functioneren wanneer het elektriciteitsnet niet normaal functioneert. Dit maakt het elektriciteitsnet weerbaarder tegen grote verstoringen, bijvoorbeeld incidenten door high-power IoT.

Cyber Security Act 2 (CSA2)

De Europese Commissie heeft een nieuwe versie van de CSA voorgesteld. Daarin wordt voorgesteld dat de Europese Commissie derde landen en leveranciers daarbinnen kan aanwijzen die een serieus risico vormen voor de veiligheid van ICT in de Europese Unie.¹⁷ Organisaties die onder de NIS2-richtlijn vallen, kunnen vervolgens verplicht worden om binnen specifieke processen niet meer gebruik te maken van ICT-producten van een dergelijke leverancier. Ook kunnen dergelijke partijen uitgesloten worden van subsidies, aanbestedingen en betrokkenheid bij het opstellen van Europese standaarden.

¹⁵ https://www.acer.europa.eu/sites/default/files/documents/Recommendations_annex/ACER_Recommendation_03-2023_Annex_1a_NC_RfG_TC_to_original.pdf

¹⁶ <https://www.acer.europa.eu/news/acer-will-consult-amendments-electricity-grid-connection-network-codes>

¹⁷ <https://open.overheid.nl/documenten/deb43911-5bca-448a-bace-0a8dc6e6cfe5/file>

Voordelen behouden, risico's mitigeren

High-power IoT brengt een aantal dilemma's met zich mee in de energiesector. De uitdaging is om de voordelen te behouden en risico's te mitigeren.

Automatische updates

VOORDEEL

Automatische software-updates zorgen ervoor dat softwarekwetsbaarheden in verbonden apparaten snel door een fabrikant verholpen kunnen worden. Dit beschermt tegen uitbuiting van kwetsbaarheden door criminelen en staten.

RISICO

Tegelijkertijd zorgt dit voor de mogelijkheid dat een foutieve update het apparaat verstoort. Ook zouden staten fabrikanten kunnen dwingen om automatische updates te misbruiken.

Flexibiliteit

VOORDEEL

Via het internet kunnen verbonden apparaten makkelijk ontsloten worden om flexibiliteit voor het net te leveren. Zo kunnen ze bijdragen aan de stabiliteit van het net en congestie tegengaan.

RISICO

Tegelijkertijd zorgt deze verbondenheid ervoor dat grote groepen verbonden apparaten tegelijkertijd ongewenst beïnvloed kan worden met juist risico's voor de stabiliteit van het net.

Schaalvoordelen

VOORDEEL

Het op grote schaal produceren van apparaten met dezelfde software en het beheren van apparaten vanuit één centraal platform drukt de kosten vanwege schaalvoordelen.

RISICO

Tegelijkertijd zorgt dit voor een monocultuur waardoor een groot aantal apparaten tegelijk beïnvloed kan worden.

Uitgangspositie

REGELGEVING VANGT DEELS AF

- **CRA:** slechts algemene veiligheidseisen
- **NIS2:** afhankelijk van bedrijfsomvang, beperkt buiten de EU
- **NCCS:** nog beperkte aandacht

Steeds meer high-power IoT-apparaten zijn verbonden aan het elektriciteitsnetwerk. Dit brengt risico's voor de stabiliteit van het net met zich mee.

Wanneer een groot aantal high-power IoT-apparaten tegelijkertijd beïnvloed wordt, kan dit de stabiliteit van het elektriciteitsnet beïnvloeden. High-power IoT kan op verschillende manieren op afstand beïnvloed worden. Verstoringen kunnen optreden als er foutieve updates of instellingen zijn doorgevoerd, als er kwetsbaarheden worden uitgebuit of als fabrikanten of aanbieders worden gedwongen door staten met kwaadwillende bedoelingen.

Bestaande wet- en regelgeving zoals de CRA en de NIS2-richtlijn vangt enkel een deel van deze risico's af. Voor high-power IoT stelt CRA slechts algemene cybersecurityeisen. De NIS2-richtlijn is in principe alleen van toepassing op organisaties van een bepaalde grootte, ongeacht het vermogen dat zij kunnen aansturen, en is beperkt van toepassing op organisaties buiten de Europese Unie. In de NCCS is nog beperkte aandacht voor high-power IoT.

Oplossingsrichtingen

Er zijn verschillende invalshoeken om het risico van high-power IoT-apparaten te mitigeren. Denk aan:

01

Juridisch

Welke juridische verantwoordelijkheden zijn er voor partijen?

02

Governance

Welke rollen en verantwoordelijkheden zijn er voor partijen?

03

Economisch

Welke marktprikkels zijn er voor partijen?

04

Technisch

Welke technische maatregelen zijn er mogelijk om kans en impact van high-power IoT incidenten te beperken?

05

Systeemontwerp

Hoe kan het elektriciteitsnet zo vormgegeven worden dat het high-power IoT incidenten beter kan weerstaan?

Deze invalshoeken kunnen onderlinge afhankelijkheden hebben. In dit position paper hebben wij ons vanuit de juridische invalshoek gericht op de cybersecurityverantwoordelijkheden van partijen. Hierna volgen voor deze invalshoek drie oplossingsrichtingen.

OPLOSSINGSRICHTINGEN

Een antwoord op Europees niveau op deze vragen is noodzakelijk, omdat het elektriciteitsnet Europees sterk verweven is.

OPLOSSINGSRICHTING 1

Specifieke cybersecurityeisen aan producten

Het stellen van specifieke cybersecurityeisen aan high-power IoT-apparaten en bijbehorende backend.

Onder de CRA gelden voor high-power IoT-apparaten en de digitale backend alleen algemene cybersecurityeisen en een zelfcontrole van de fabrikant daarop. Om het risico van onveilige high-power IoT en bijbehorende backend te beperken zouden verticale geharmoniseerde standaarden voor verschillende categorieën van high-power IoT-apparaten vastgesteld kunnen worden. In de standaarden kan qua cybersecurityeisen rekening worden gehouden met de risico's voor het elektriciteitsnet.

Daarnaast kunnen categorieën van high-power IoT worden toegevoegd aan de lijst van belangrijke producten klasse 2 van de CRA. Daardoor vervalt de zelfcontrole en moet een onafhankelijke instantie controleren of zij aan de cybersecurityeisen voldoen voordat ze op de Europese markt mogen worden gebracht. Dit geeft meer zekerheid over het gewenste niveau van cybersecurity van high-power IoT producten en bijbehorende backend, wat de risico's voor het elektriciteitsnet verkleint.

INSTRUMENT

CRA: geharmoniseerde standaarden en klasse 2

OPLOSSINGSRICHTING 2

Cybersecurityeisen voor partijen die kritieke vermogens kunnen aansturen

Het stellen van passende cybersecurityeisen op voor partijen die op afstand veel vermogen via high-power IoT kunnen beïnvloeden.

De systematiek van de NIS2-richtlijn maakt dat partijen die op afstand veel vermogen via high-power IoT kunnen aansturen buiten de reikwijdte van de richtlijn kunnen vallen. Dit kan komen doordat ze een kleine bedrijfsomvang hebben, niet in de Europese Unie gevestigd zijn of doordat ze geen specifieke bedrijfsactiviteiten hebben waarmee ze onder de NIS2-richtlijn vallen.

Deze lacune kan worden gedicht door organisaties die op afstand kritieke vermogens kunnen aansturen, waardoor de stabiliteit van het elektriciteitsnet in gevaar gebracht kan worden, ongeacht hun bedrijfsomvang en vestigingslocatie, onder de NIS2-richtlijn te brengen. Ook zouden daarbij specifieke Europese eisen gesteld kunnen worden waarin rekening wordt gehouden met de risico's voor het elektriciteitsnet. Zo kunnen de risico's voor het elektriciteitsnet worden verkleind.

INSTRUMENT

NIS2-richtlijn: reikwijdte op basis van aanstuurbaar vermogen

Digitale autonomie versterken

Het nemen van aanvullende maatregelen om digitale autonomie te versterken.

De snelle toename van high-power IoT en de impact die dit kan hebben op het elektriciteitsnet raakt de digitale autonomie van ons elektriciteitsnet. Partijen die high-power IoT-apparaten op grote schaal kunnen beïnvloeden, bevinden zich deels buiten de Europese Unie. Hierdoor ontstaan geopolitieke risico's. Onder politieke druk kan dienstverlening van dergelijke partijen wegvallen of beïnvloed worden, ongeacht welke cybersecurityeisen vanuit de Europese Unie aan dergelijke partijen wordt gesteld. In lijn met de position paper 'De route naar digitale autonomie' is het voor vitale processen van belang om dergelijke afhankelijkheidsrisico's te beperken.¹⁸ Daarbij blijft het uiteraard belangrijk om óók grip te houden op andere afhankelijkheden, kwetsbaarheden en risico's om zo tot een digitaal weerbaar systeem te komen.¹⁹

INSTRUMENT

Weerbaar ontwerp van het energiesysteem en digitale autonomie

¹⁸ <https://www.rdi.nl/documenten/2026/07/10/de-route-naar-digitale-autonomie>

¹⁹ <https://www.rdi.nl/actueel/nieuws/2026/04/23/digitale-autonomie-is-de-basis-voor-digitale-weerbaarheid>

Dit is een uitgave van
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

📍 Emmasingel 1 Groningen

📞 088 - 041 60 00

✉ info@rdi.nl

🌐 www.rdi.nl

Oktober 2026

De afbeeldingen op pagina 6 en 9 zijn met behulp van AI gegenereerd.



#wijzijnRDI