Westerduinweg 3
1755 LE Petten
Postbus 15
1755 ZG Petten

www.tno.nl

T +31 88 866 50 65

TNO-rapport

TNO 2020 R12069 | Eindrapport

Verkenning van toekomstige risico's voor het elektriciteitsnet

Datum	26 mei 2021
Auteur(s)	E.J. Wiggelinkhuizen B.H. Bulder A.B. Schwedersky M.P.W. van Berlo
Exemplaarnummer	
Oplage	
Aantal pagina's	46 (incl. bijlagen)
Aantal bijlagen	
Vraagsturing	Vraaggestuurd Programma Veilige Maatschappij (VPVM)
Projectnaam	P2107 – Kennisopbouwprogramma NCTV
Projectnummer	060.43638

Samenvatting

Aanleiding

De elektriciteitsvoorziening is een cruciaal onderdeel voor het kunnen functioneren van de Nederlandse maatschappij. Daarom kan kortdurende en regionale uitval van elektriciteit (brownout) al leiden tot grote cascade-effecten als uitval van bijvoorbeeld openbaar vervoer en ICT netwerken. Grootschalige volledige uitval (blackout) leidt tot ernstige economische en, afhankelijk van de duur, mogelijk ook tot fysieke schade en maatschappelijke onrust.

In de komende decennia zal het elektriciteitssysteem in Nederland en in de ons omringende landen ingrijpende veranderingen ondergaan, hoofdzakelijk vanwege de energietransitie. Hiermee samenhangende ontwikkelingen zijn de verdere digitalisering van de maatschappij en het elektriciteitsnet en de toename van “Internet of Things” (IoT), waardoor tal van gebruiksfuncties, zoals toegang, signalering, bediening en beveiliging van voorzieningen, kunnen uitvallen bij verstoring van de elektriciteitsvoorziening. Deze ontwikkelingen vertalen zich in nieuwe en verschuivende risico’s en kwetsbaarheden, waarbij naar verwachting de kans op verstoringen en de omvang daarvan (qua duur en geografische schaal) zullen toenemen. Met de verdere elektrificatie van de energievoorziening, zoals bijvoorbeeld vervoer en de energie-intensieve industrie, en de grotere afhankelijkheid van IT, zal naar verwachting de impact van verstoringen toenemen.

Doel en aanpak van de studie

Met het oog op deze ontwikkelingen is er binnen het domein van de NCTV behoefte aan meer kennis en inzicht in toekomstige manieren waarop en de mate waarin de transport- en distributienetten van elektriciteit kwetsbaar zijn of kunnen worden met potentiële gevolgen voor de nationale veiligheid. In aansluiting daarop heeft TNO, in afstemming met NCTV en EZK, de volgende onderzoeksvraag geformuleerd: “*Welke nieuwe risico’s voor de nationale veiligheid kunnen de komende 10-20 jaar ontstaan binnen het Nederlandse elektriciteitsnetwerk als gevolg van (ontwikkelingen vanuit) de energietransitie en toenemende digitalisering?”* Hierbij is gekeken naar risico’s met betrekking tot 1) continuïteit van vitale processen; 2) de integriteit van kennis en informatie; 3) de opbouw van ongewenste strategische afhankelijkheden.

De mate van waarschijnlijkheid van optreden van de geïdentificeerde risico’s is nadrukkelijk niet in deze verkenning meegenomen. Dat is immers ook voor een belangrijk deel afhankelijk van de effecten van huidige en in ontwikkeling zijnde maatregelen om het weerbaarheidsniveau binnen de elektriciteitssector op peil te houden c.q. te verhogen. In deze verkenning is uitsluitend gekeken naar mogelijke nieuwe risico’s voor het elektriciteitsnet als gevolg van de energietransitie, de digitalisering en IoT. Het verder uitwerken en analyseren hiervan, mede in het licht van huidige en reeds voorgenomen maatregelen, is onderwerp van mogelijk vervolgonderzoek.

In deze studie is een verkenning van nieuwe risico's en kwetsbaarheden opgesteld op basis van bestaande documentatie van onder meer het Analistennetwerk Nationale Veiligheid (ANV), interviews met TNO experts en een enquête onder enkele leden van de Information Sharing and Analysis Centre Energie van het Nationaal Cyber Security Center. Hieruit is een omschrijving opgesteld hoe het toekomstige Nederlandse elektriciteitssysteem naar verwachting zal zijn opgebouwd en zal worden bedreven. Daarbij wordt beschreven welke nieuwe mogelijke risico's hierbij kunnen optreden. In de context van deze toekomstbeelden in 2030 en 2040 zijn aan de hand van enkele scenario's nieuwe risico's verkend met daarbij mogelijke cascade-effecten die kunnen ontstaan. Daarbij is aandacht voor gevolgen op het gebied van de nationale veiligheid.

Mogelijke nieuwe risico's in relatie tot de nationale veiligheid

In deze studie zijn de volgende nieuwe risico's (voor 2030-2040) en mogelijke implicaties voor de nationale veiligheid geïdentificeerd. Voor de leesbaarheid zijn de risico's opgedeeld in drie secties: 1) continuïteit van vitale processen; 2) de integriteit van kennis en informatie; 3) de opbouw van ongewenste strategische afhankelijkheden.

<u>Continuïteit van vitale processen</u>

- Door weersafhankelijk aanbod van elektriciteit uit zon en wind en onvoldoende back-up vermogen, kan onbalans tussen vraag en aanbod ontstaan. Wanneer door onvoldoende back-up capaciteit en/of transportbeperkingen de balans niet tijdig kan worden hersteld, moeten gebruikers deels worden afgeschakeld van het net. Hierbij speelt ook de te verwachten grotere strategische afhankelijkheid van het buitenland voor back-up vermogen, zowel direct door import van elektriciteit, als indirect door import van aardgas voor flexibel regelbare elektriciteitsopwekking.
- Hogere belasting en grotere complexiteit van het elektriciteitsnetwerk, waarbij omwille van snelle uitbreiding en kostenbesparingen minder redundantie beschikbaar is, waardoor relatief kleine verstoringen kunnen leiden tot meer grootschalige congestie of (gedeeltelijke) netuitval. In het kader van de nationale veiligheid kan dit zorgen voor problemen van de beschikbaarheid van vitale infrastructuur in Nederland waardoor vitale processen in het geding kunnen komen, maar wellicht ook voor strategische afhankelijkheden. Daarnaast kan dit zorgen voor het creëren van meer aantrekkelijke doelwitten voor kwaadwillende actoren.
- Onvoldoende fysieke beveiliging van offshore windparken en netten in combinatie met de hoge kapitaalkosten, de hoge vermogens (van meerdere GW per kabelpaar) en de langdurige reparatietijden. In het kader van de nationale veiligheid is het belangrijk om zicht te hebben op de aders van onze maatschappij, zo ook de offshore windparken en netten. Wanneer onvoldoende aandacht is voor nieuwe zaken die beveiliging vereisen, kunnen deze onopgemerkt zorgen voor een risico (zeker in het kader van moedwillig handelen).

<u>Integriteit van kennis en informatie</u>

- Ten aanzien van het beheer van IT systemen worden door beperkte toegang tot informatie kwetsbaarheden en (cyber)aanvallen op IT systemen mogelijk niet (tijdig) gedetecteerd. Daarbij kunnen er beperkte mogelijkheden zijn tot het

doorvoeren van updates en het actief en geautomatiseerd detecteren en testen van inbraken en kwetsbaarheden. Mogelijke redenen hiervoor zijn onduidelijkheden tussen partijen over de verantwoordelijkheden, beperkte (wettelijke) bevoegdheden, technische beperkingen, zoals het garanderen van de continuïteit, of economische redenen. In het kader van nationale veiligheid is het belangrijk te voorkomen dat onopgemerkte kwetsbaarheden (gedurende langere tijd) kunnen bestaan. Naast een direct risico voor verstoringen van het betreffende IT systeem kunnen op langere termijn ook problemen ontstaan op gebied van interoperabiliteit tussen verschillende IT systemen.

- Grote aantallen decentrale opwekkers en verbruikers (zon-PV, EV) die autonoom of centraal aangestuurd reageren op een elektriciteitsvraag of marktprijs, en daardoor onvoorspelbaar gedrag vertonen dat negatief kan uitwerken op de beschikbare netcapaciteit of de netstabiliteit. Dit fenomeen is niet nieuw, maar is met de huidige 20% duurzame opwekking goed behapbaar. Bij een dominant aandeel duurzame opwekking en uitfasering van conventionele centrales ontstaan veel grotere aanbodfluctuaties die leiden tot sterke prijsschommelingen en daarop reagerende vraag. Achterlopende of ontbrekende regelgeving maakt het voor netbeheerders moeilijk om hier inzicht in te krijgen en om dit de voorkomen. In het kader van nationale veiligheid zijn problemen met de capaciteit of stabiliteit per definitie problematisch, bijvoorbeeld i.v.m. uitval van vitale processen. Deze problemen worden versterkt wanneer onvoorspelbaar gedrag optreedt dat voortvloeit uit autonoom handelen van een grote groep verbruikers die extern wordt aangestuurd.

<u>Opbouw van ongewenste strategische afhankelijkheden</u>

- Grotere verwevenheid tussen het operationele en IT domein, waarbij onvoldoende zicht is op de afhankelijkheden, bijv. bij outsourcing van IT oplossingen, onderliggende diensten en gestandaardiseerde ICT platforms. In het kader van nationale veiligheid is dit een probleem omdat onduidelijke afhankelijkheden kunnen zorgen voor onverwachte uitval van (vitale) processen. Zonder overzicht van de (afhankelijkheden van) de betreffende (IT) infrastructuren is het lastig om te achterhalen waar problemen, uitval en verstoringen vandaan kunnen komen. Dit zorgt voor vertraging in de opvolging van dergelijke problemen.
- Onvoldoende zicht op het beheer van IT en IoT en beperkte mogelijkheden voor het doorvoeren van updates en voor het actief en geautomatiseerd detecteren en testen van inbraken en kwetsbaarheden. Hierdoor ontstaat het risico dat een groot aantal aan het elektriciteitsnet gekoppelde (decentrale) opwekkers en verbruikers onvoorspelbaar en ongewenst gedrag vertonen, waardoor problemen kunnen ontstaan met de lokale netspanning of - op grotere schaal - met de balans tussen vraag en aanbod, wat tot snelle schommelingen in de netfrequentie leidt. Mogelijke redenen voor deze kwetsbaarheden zijn onduidelijkheden tussen partijen over de verantwoordelijkheden, technische beperkingen, economische redenen of i.v.m. de continuïteit. Toekomstige risico’s IoT apparaten op het elektriciteitssysteem zijn momenteel moeilijk in te schatten, mede omdat de sterke groei van IoT vrij recent is gestart en omdat nieuwe toepassingen niet goed zijn te voorspellen. In het kader van nationale veiligheid is het belangrijk om duidelijke verantwoordelijkheden van beheer te hebben zodat geen onopgemerkte kwetsbaarheden (gedurende langere tijd) kunnen bestaan. Anders zorgt dit voor onvoldoende zicht op de systemen en onvoldoende beheer, en kan dit op

lange termijn ook problemen veroorzaken wanneer we kijken naar interoperabiliteit van systemen.

Vervolgstappen

De genoemde risico scenario's geven een mogelijke vooruitblik over een periode van 10 tot 20 jaar, gebaseerd op huidige trends en verwachte ontwikkelingen. Deze zijn echter nog niet geverifieerd met de stakeholders, en het wordt aanbevolen dat alsnog te doen als eerste vervolgstap, bijvoorbeeld in de vorm van meerdere workshops. Daarin kan ook meer gedetailleerd worden bepaald welke impacts en cascade-effecten kunnen optreden en welke strategische afhankelijkheden hierbij relevant zijn. Voorbeelden van mogelijke cascade-effecten die als startpunt kunnen dienen voor het uitwerken en analyseren van risico-scenario's zijn:

- Bij teveel 112 meldingen en grootschalige verstoringen in het elektriciteitssysteem kunnen niet alle mensen altijd snel geholpen worden. Hulpverleners rijden allemaal elektrisch en kunnen voertuigen niet meer voldoende opladen. Hierdoor zal maatschappelijke onrust toenemen.
- Een mogelijk effect van imagoschade van een elektriciteitsbedrijf op de korte/middellange termijn is een gebrek aan voldoende financiële ruimte voor innovaties in de cybersecurity en/of het aantrekken van voldoende gekwalificeerd personeel, waardoor de kwetsbaarheid voor cyberaanvallen toeneemt.
- Hoge schadevergoedingen als gevolg van grootschalig en/of frequent uitval van de elektriciteitsvoorziening kan leiden tot een vijandelijke overname van een bedrijf door een bedrijf dat nauwe contacten onderhoudt met een buitenlandse overheid waar Nederland een minder goede relatie mee heeft.

Een tweede vervolgstap is identificeren welke maatregelen er kunnen worden getroffen om de beschreven toekomstige risico's en mogelijke (cascade) effecten te mitigeren als onderdeel van een bredere strategie. Vanuit deze studie komen hiervoor enkele aandachtspunten naar voren. Bij de ontwikkelingen in het energiesysteem in de komende jaren ligt grote nadruk op snelheid en kosten. Bij het herontwerp van het energiesysteem (incl. IT, beheerssystemen en regelgeving) zou daarnaast een even grote aandacht moeten uitgaan naar het analyseren en meewegen en managen van risico's, evenals het eigenaarschap van de systemen en verantwoordelijkheid voor de security.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Nationale veiligheid is een dynamisch en veelzijdig begrip en is in het geding als één of meer vitale belangen van de Nederlandse staat en/of samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting (NCTV, 2019, p.15). Daarbij worden zes nationale veiligheidsbelangen onderscheiden: 1) territoriale veiligheid, 2) fysieke veiligheid, 3) economische veiligheid, 4) ecologische veiligheid, 5) sociale en politieke stabiliteit, en 6) internationale rechtsorde (NCTV, 2019). De elektriciteitsvoorziening is een cruciaal onderdeel voor het kunnen functioneren van de Nederlandse maatschappij en heeft in meer of mindere mate een impact op al deze veiligheidsbelangen. Het landelijke transport- en distributienetwerk voor elektriciteit is een vitaal proces categorie A met de hoogste gevolgen bij uitval. Het uitvallen van regionale elektriciteitsdistributie netwerken valt in categorie B processen (NCTV, 2017). Een verstoring van het elektriciteitsnetwerk, waarbij zowel gedacht kan worden aan een brownout, regionale en tijdelijke uitval, als aan een blackout, uitval van het complete landelijke elektriciteitsnetwerk voor langere tijd, heeft doorgaans vergaande gevolgen, zowel voor de economie als voor de fysieke veiligheid. In het kader van deze verkenning wordt met betrekking tot nationale veiligheid specifiek gekeken naar de risico's met betrekking tot 1) continuïteit van vitale processen; 2) de integriteit van kennis en informatie; 3) de opbouw van ongewenste strategische afhankelijkheden.

1.2 Aanleiding

De elektriciteitsvoorziening in Nederland geldt als een van de meest betrouwbare wereldwijd, door een moderne infrastructuur met voldoende opwek- en transportcapaciteit, sterk internationaal verbonden transportnetten en geïntegreerde markten. Daarbij geldt zowel in EU-verband als nationaal wet- en regelgeving omtrent de betrouwbaarheid en leveringszekerheid (zie ook EC Security of electricity supply (European Commission, 2021)). Dit betreft specifiek de verplichting van EU lidstaten om plannen operationeel te hebben hoe om te gaan met toekomstige crisissituaties in de elektriciteitsvoorziening, inclusief de benodigde middelen ter voorkoming, voorbereiding en beheersing hiervan. In de komende decennia zal de elektriciteitsvoorziening echter sterk en in snel tempo veranderen, wat mogelijke nieuwe risico's voor de nationale veiligheid met zich mee brengt. Het op peil houden van kennis van deze veranderingen en het vergroten van inzicht in mogelijk nieuwe risico's is van belang bij het vormgeven en de bedrijfsvoering van het toekomstige elektriciteitssysteem.

Dit rapport, dat is opgesteld binnen het Vraaggestuurd programma Veilige Maatschappij CTER/NCTV 2020, beschrijft een verkenning van toekomstige risico's voor het elektriciteitsnetwerk in Nederland. De focus ligt daarbij op te verwachten mogelijke risico's in de komende 10 tot 20 jaar ten gevolge van de energietransitie, de digitalisering en het IoT "Internet of Things".

De mate van waarschijnlijkheid van optreden van de geïdentificeerde risico's is nadrukkelijk niet in deze verkenning meegenomen. Dat is immers ook voor een belangrijk deel afhankelijk van de effecten van de huidige en in ontwikkeling zijnde

maatregelen om het weerbaarheidsniveau binnen de elektriciteitssector op peil te houden c.q. te verhogen. In deze verkenning is uitsluitend gekeken naar mogelijke nieuwe risico's voor het elektriciteitsnet als gevolg van de energietransitie, de digitalisering en IoT. Het verder uitwerken en analyseren hiervan, mede in het licht van huidige en reeds voorgenomen maatregelen, is onderwerp van mogelijk vervolgonderzoek.

1.3 Toelichting op ontwikkelingen in de elektriciteitsvoorziening

De ingezette energietransitie, die noodzakelijk is voor het behalen van de gestelde klimaatdoelen, zal in de komende decennia bepalend zijn voor de ontwikkelingen in het elektriciteitssysteem. Hierbij gaat het zowel om verduurzaming van de elektriciteitsopwekking, met een sterke toename van zonne- en windenergie, als van energieverbruikers, zoals verwarming van gebouwen, transport en energie-intensieve industrie (2020) via elektrificatie en energieconversie naar groene brandstoffen en grondstoffen (voornamelijk op basis van groene waterstof en daaruit gesynthetiseerde producten). Het aandeel van elektriciteit in de energiemix zal daarmee sterk toenemen (2019), en daarmee ook de afhankelijkheid van de energieverbruikers van een betrouwbare elektriciteitsvoorziening.

Een tweede ontwikkeling die het elektriciteitssysteem raakt is de voortschrijdende digitalisering. Dit houdt verband met het real-time kunnen monitoren en besturen van grote aantallen decentrale opwekkers en verbruikers, zoals fotovoltaïsche (zon-PV) installaties, windparken en laders voor Elektrisch Vervoer (EV), eventueel gecombineerd met lokale elektriciteitsopslag. Andere aanleidingen zijn hogere eisen aan de besturing van netten, bijvoorbeeld ter voorkoming van congestie bij hogere en snel wisselende netbelastingen, en kostenbesparingen.

Een derde ontwikkeling is de toename van slimme appraten die zowel met het elektriciteitsnet als met Internet zijn verbonden (IoT). Dit maakt bijvoorbeeld bediening op afstand of autonoom reageren op marktprijzen mogelijk.

De genoemde ontwikkelingen zijn relevant voor de verkenning van nieuwe risico's die tot nieuwe kwetsbaarheden kunnen leiden, omdat deze ontwikkelingen leiden tot een meer complexe en intensief belaste infrastructuur en een sterkere verwevenheid met het domein van Informatie Technologie (IT).

1.4 Onderzoeksvraag en aanpak

In afstemming met NCTV en EZK is de volgende onderzoeksvraag geformuleerd van deze verkenning: "*Welke nieuwe risico's voor de nationale veiligheid kunnen de komende 10-20 jaar ontstaan binnen het Nederlandse elektriciteitsnetwerk als gevolg van (ontwikkelingen vanuit) de energietransitie en toenemende digitalisering?"* Hierbij is gekeken naar risico's met betrekking tot 1) continuïteit van vitale processen; 2) de integriteit van kennis en informatie; 3) de opbouw van ongewenste strategische afhankelijkheden."

De volgende activiteiten zijn uitgevoerd om de onderzoeksvragen te beantwoorden:

- Beknopte beschrijving van de lay-out van het elektriciteitssysteem (hoe zit het in elkaar, wie is waarvoor verantwoordelijk, wat zijn de bijhorende verantwoordelijkheden);

- Inventarisatie van de ontwikkelingen in het elektriciteitssysteem door de energietransitie, waarbij zal worden gefocust op de sterke toename van zonne- en windenergie en de verdere elektrificatie van de vraag: deze hebben immers de grootste impact op het elektriciteitssysteem.
- Inventarisatie van veranderingen in het elektriciteitssysteem door digitalisering van zowel het netwerk zelf als aan de gebruikerskant;
- Inventarisatie van risico's die betrekking hebben op de continuïteit van vitale processen die samenhangen met verstoringen van het elektriciteitssysteem, de integriteit en exclusiviteit van kennis, informatie en systemen (bijvoorbeeld doordat derden toegang hiertoe hebben), en de opbouw van ongewenste strategische afhankelijkheden;
- Inventarisatie van de mogelijke impact en cascade-effecten indien een verstoring of uitval plaatsvindt.

Deze verkenning van nieuwe risico's voor het elektriciteitssysteem is opgesteld op basis van de veronderstelde ontwikkelingen en beschikbare documenten, aangevuld met inzichten uit interviews met TNO-experts en met de resultaten van een enquête onder enkele leden van het Information Sharing and Analysis Centre Energie van het Nationaal Cyber Security Center. In deze enquête zijn enkele toekomstbeelden en risico-scenario's geschetst (zie ook Bijlage A), waarbij is gevraagd deze te becommentariëren en aan te vullen, en daarbij aan te geven welke ontwikkelingen en risico's vanuit het oogpunt van hun verantwoordelijkheden en expertises het meest belangrijk zijn. Deze enquête is via de NCTV en het NCSC als interactieve-PDF uitgezet. Vanwege de zeer korte tijdperiode konden slechts 4 responses worden ontvangen.

1.5 Structuur en doel rapportage

Hoofdstuk 2 geeft een beknopt overzicht van bestaande risicoanalyses en enkele historisch gebeurtenissen, welke cascade-effecten kunnen optreden en hoe deze een impact kunnen hebben op de nationale veiligheid. Hoofdstuk 3 geeft een beschrijving van de verwachte ontwikkelingen in het huidige elektriciteitssysteem voor de komende 10 tot 20 jaar als gevolg van de energietransitie, digitalisering en IoT. Daarbij wordt beschreven welke nieuwe risico's deze ontwikkelingen met zich mee brengen. In hoofdstuk 4 zijn deze nieuwe risico's aan de hand van enkele scenario's geïllustreerd. Hoofdstuk 5 sluit af met de conclusies en aanbevelingen. In de gerapporteerde ontwikkelingen en verkenning van nieuwe risico's zijn de resultaten van de interviews en enquêteresultaten verwerkt.

Deze verkennende inventarisatie dient als input voor een meer volledige impactanalyse en beschrijving van mogelijke cascade-effecten, die echter buiten de scope van dit project valt.

2 Huidige status risico inventarisatie elektriciteitsnetwerk

2.1 Documentstudie risico analyses elektriciteitsnetwerk

Deze paragraaf geeft aan de hand van openbare documenten een overzicht van risico's van verstoringen in het elektriciteitssysteem in relatie tot de onderzoeksvraag. Deze documenten betreffen beschrijvingen van enkele daadwerkelijke verstoringen in het elektriciteitssysteem, zowel in Nederland als internationaal, met relatief grote impact. De gebeurtenissen beslaan een periode van de afgelopen 15 jaar, waarbij de meeste van meer recente datum zijn. Daarnaast zijn aan de hand van bestaande risicoanalyses mogelijke impacts als gevolg van deze kwetsbaarheden beschreven, waarbij strategische afhankelijkheden met het oog op de nationale veiligheid worden meegenomen.

2.1.1 Aanleidingen en impacts

Mogelijke soorten oorzaken van risico's zijn onder te verdelen in intern systeemfalen en externe omstandigheden, die weer verder onder te verdelen zijn in natuurlijke oorzaken en onbedoeld en moedwillig menselijk handelen. Systeemfalen kan optreden doordat het systeem buiten de specificatie (ontwerpgrenzen) wordt gebruikt of door slijtage en/of veroudering, maar ook dat door "pech" de statistische kans ontstaat dat een cruciaal onderdeel kapot gaat binnen de normale levensduur. Externe omstandigheden kunnen weer worden opgesplitst in natuurlijke fenomenen of menselijke oorzaken. De menselijke oorzaken kunnen worden onderverdeeld in onbedoelde effecten van handelen (fouten) of moedwillig handelen (sabotage, aanslag), waarbij dit door een eenling, groepen of statelijke actoren kan worden gedaan. Met name opzettelijk menselijk handelen is via digitale kanalen mogelijk (cybercrime/terrorisme).

Bij directe impact (nog zonder afhankelijkheden mee te nemen) kan als eerste worden gedacht aan netuitval, waarbij onderscheid wordt gemaakt tussen een onverwacht langdurige uitval van een volledig (landelijk) netwerk (blackout), en een uitval van kortere duur en op een kleinere geografische schaal (brownout). Ook kan een netwerkbeheerder genoodzaakt zijn om, bijvoorbeeld bij optredende of dreigende overbelasting, een deel van het netwerk af te schakelen ter voorkoming van mogelijke grotere gevolgen, zoals een blackout. Het opstarten na een blackout moet gestructureerd en gefaseerd worden uitgevoerd om te voorkomen dat tijdens de herstart weer een blackout zal ontstaan. Het opstarten na een brownout gebeurt vaak sneller en automatisch. Voor de analyse voor zowel een blackout als een brownout zijn het transmissieniveau (met netbeheerder TenneT) en het distributieniveau (met diverse regionale netbeheerders) beide van belang, waarbij ook een sterke samenhang en wisselwerking bestaat tussen de verschillende niveaus.

In de Europese wetgeving zijn sinds 2019 vernieuwde verplichtingen opgenomen ten aanzien van risk-preparedness (Europees Parlement & Raad van de Europese Unie, 2019), waaronder het opstellen van risicoanalyses en plannen om voorbereid

te zijn op crises in de elektriciteitsvoorziening, en plannen voor risicomanagement, evaluatie en monitoring.

2.1.2 Gerapporteerde gebeurtenissen

Van daadwerkelijke grootschalige verstoringen van de elektriciteitsvoorziening in Nederland en West Europa zijn niet veel voorbeelden bekend. In 2006 is een grote blackout geweest (Union for the co-ordination of transmission of electricity (UTCE), 2007) die zich over een groot deel van West Europa uitstrekte. Oorzaak van die verstoring was het afschakelen van een 380 kV transport kabel over de Ems resulterend in een onbalans in het Europese hoofdelektriciteitsnet waardoor in een groot deel van Duitsland, Nederland, België, Frankrijk, Spanje en Portugal het elektriciteit netwerk uitviel. De uitval had gevolgen voor 15 miljoen mensen. Herstel van het netwerk heeft tussen 30 minuten en 2 uur geduurd.

Een ander meer regionaal voorbeeld is uit 2007 (Nederlands Instituut Fysiek Veiligheid Nibra et.al., 2008) waarbij door een helikopter van de luchtmacht een hoogspanningskabel werd geraakt en beschadigd, resulterend in een blackout van twee dagen in de Betuwe. Meer recent werd in 2015 een regionale blackout veroorzaakt door het uitschakelen van een 380 kV substation in Diemen, door een kortsluiting en onjuist menselijk handelen, waardoor een groot deel van Noord-Holland en Flevoland zonder stroom kwamen te zitten (TenneT, 2017).

Op 8 januari 2021 vond een grootschalige frequentieverstoring plaats die samenhing met de uitval van meerdere centrales in Zuidoost Europa, waardoor het net tussen Noordwest en Zuidoost Europa werd ontkoppeld. Na iets meer dan een uur werden deze weer met elkaar verbonden, waarbij in de tussentijd verschillende fossiele centrales en waterkrachtcentrales maximaal vermogen hebben moeten leveren om een blackout te voorkomen. Naar aanleiding hiervan waarschuwde in een persbericht de Duitse “Industrie Verband der Industriellen Energie und Kraftwirtshaft” bezorgd te zijn dat door de uitfasering van conventionele (kolen- en kern-) centrales de leveringszekerheid in gevaar komt (Verband der Industriellen Energie- & Kraftwirtschaft, 2021).

2.1.3 Elektriciteitsvoorziening in relatie tot nationale veiligheid

Een groot aantal risico studies is beschikbaar zowel voor Nederland als in Europese context. In deze en de volgende paragrafen worden een aantal rapportages thematisch besproken.

De elektriciteitsvoorziening is een cruciaal onderdeel van de Nederlandse maatschappij. Het landelijke transport- en distributienetwerk voor elektriciteit is een categorie A proces, met de hoogste gevolgen bij uitval. Het uitvallen van regionale elektriciteitsdistributie netwerken valt in categorie B processen (NCTV (2017)). Een betrouwbare elektriciteitsvoorziening is essentieel voor het functioneren van vitale organisaties, zoals first responders (brandweer, ambulance en politie), gezondheidszorg, en een groot aantal vitale functies, zoals onder andere de drinkwatervoorziening, de waterhuishouding (gemalen, riolering, waterzuivering), het aardgasnet, communicatie, signalering en bediening voor weg- en waterwegen, koeling.

Langdurige verstoringen of uitval leiden nu en in de toekomst tot economische schade, maar hebben ook impact op gezondheid en veiligheid, en kunnen daarmee de maatschappij ontwrichten. Het elektriciteitsnet ondergaat in de komende decennia grote veranderingen vanwege de energietransitie, die onder grote tijdsdruk kostenefficiënt moet worden gerealiseerd, en vanwege de toenemende digitalisering en IoT. Hierdoor vindt een verschuiving plaats van de risico's voor het elektriciteitssysteem, waarbij ook de impacts in het licht van de veranderende maatschappelijke omstandigheden moeten worden bezien, bijvoorbeeld meer werken op afstand en een grotere mate van verstedelijking. Het is daarom ook zaak om de relatie tussen nationale veiligheid en het elektriciteitsnet te blijven bestuderen.

Bestaande risicoanalyses, zoals enkele van het Analistennetwerk Nationale Veiligheid (ANV) (2014; 2016), zijn als basis gebruikt voor deze inventarisatie. Hierin zijn voor een aantal scenario's inschattingen gemaakt wat de risico's zijn, gericht op de kortere termijn. Deze zijn in een risicodiagram weergegeven, waarbij op de horizontale as de waarschijnlijkheid van een event is weergegeven en op de verticale as de impact van een bepaald event (zie Figuur 1).

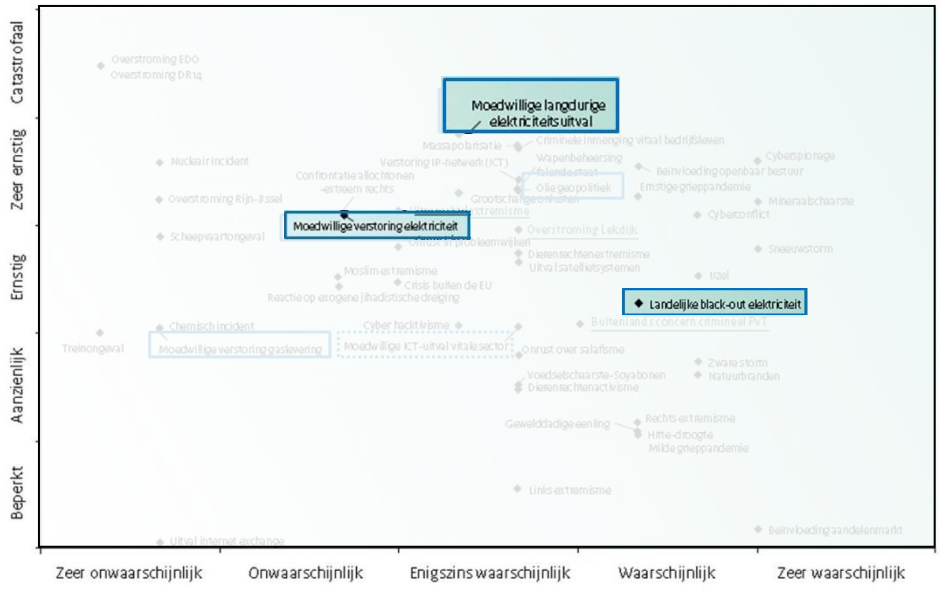
In de themarapportage van het ANV (2016) zijn drie soorten verstoringen van de vitale infrastructuur uitgewerkt, namelijk:

- Eigenstandige verstoring van vitale processen met maatschappij ontwrichtende gevolgen;
- Common-causes: Verstoring van meerdere vitale processen door dezelfde oorzaak;
- Keteneffecten: Verstoring van vitale processen als gevolg van uitval van andere vitale processen.

Deze themarapportage signaleert de sterkere koppeling tussen de elektrische en IT infrastructuur. IoT wordt daarbij als een belangrijke ontwikkeling genoemd met betrekking tot de kwetsbaarheid en betrouwbaarheid van vitale infrastructuur waarbij deze afhankelijk worden van door IoT apparaten aangeleverde data. Hierbij valt de denken aan korte-termijn elektriciteitsmarkten zoals voor balancering. Uitval, manipulatie of het lekken van waardevolle data is met de huidige beperkte beveiliging van veelal goedkope IoT apparatuur een reëel risico. Verder noemt het rapport de toename van duurzame en decentrale opwekking, waardoor de besturing van het netwerk complexer wordt, als een factor die tot meer en omvangrijkere verstoringen van de elektriciteitsvoorziening kan leiden. Ook wordt aangenomen dat door de sterkere koppeling tussen (Europese) netwerken verstoringen kunnen doorwerken in verschillende netwerken. Als laatste wordt een toename van cyberaanvallen verwacht door de toenemende vaardigheden van kwaadwillende actoren en vanwege geopolitieke motieven. Daarbij worden de gevolgen van grootschalige elektriciteitsuitval voor de nationale veiligheid in een uitgewerkt scenario beoordeeld als: Fysiek en Sociaal-politiek (beoordeeld als "zeer ernstig") en economisch (beoordeeld als "ernstig").

Ook in de daaraan voorafgaande themarapportage van TNO (2015) worden een aantal scenario's beschreven voor verstoringen van het elektriciteitsnetwerk, waaronder een blackout over een groot deel van Europa veroorzaakt door een

frequentiedaling in het elektriciteitsnet. In twee andere scenario's wordt gesproken van moedwillige verstoring van elektriciteitsvoorziening.



Figuur 1: Risico diagram uit NRB, 6, 2014, met de risico inschatting t.a.v. elektriciteit uitgelicht

Deze themarapportage vermeldt al wel ontwikkelingen in de elektriciteitsvoorziening, zoals de geplande forse toename van zon PV en wind waardoor de elektriciteitsproductie kwetsbaarder wordt voor weersextremen. Ook worden decentrale opwekking en smart grids genoemd. Het themarapport refereert hierbij aan de eerdere studie van het Planbureau voor de leefomgeving (PBL) (2015):

Het PBL ziet de volgende factoren voor de kwetsbaarheid van Nederland voor klimaatverandering: *"Klimaatverandering vergroot de waarschijnlijkheid van elektriciteitsuitval."* Hierbij doelt het rapport op uitval ten gevolge van weersextremen, waarbij als factoren voor de toename van de waarschijnlijkheid worden genoemd: verandering energiemix, toename weersextremen/droogte en vervlechting Europees netwerk. *"Maatschappelijke ontwikkelingen, zoals een toenemende afhankelijkheid van elektriciteit, vergroten de gevolgen van een stroomuitval. De elektriciteitsnetwerken in Europa worden meer en meer onderling verbonden. Enerzijds zorgt dat voor meer redundantie en flexibiliteit, anderzijds kan uitval van het elektriciteitsnetwerk in het buitenland ook consequenties hebben voor Nederland. Technologische ontwikkelingen rond bijvoorbeeld opslag en decentrale opwekking kunnen de gevolgen verkleinen."* Het PBL rapport kijkt breder dan alleen de elektriciteitsvoorziening. Zo is droogte niet meteen een groot probleem, maar is er wel een verband te leggen, namelijk dat door koelwaterproblemen in droge zomerperiodes er een beperkte opwekking van elektriciteit met conventionele centrales in NL en omringende landen kan plaatsvinden. Dit rapport noemt geen directe voorbeelden van deze consequenties in relatie tot nationale veiligheid, maar schetst mogelijke internationale beïnvloeding op de volgende terreinen: handelsketens of aanvoer van grondstoffen, financieel door schade aan Nederlandse investeringen in het buitenland, door schade aan vitale diensten zoals energie of ICT, via mensen door reizen naar landen met grotere risico's voor de gezondheid. Of zelfs via de geopolitieke route door conflicten of migratie.

2.2 Energietransitie

Vanwege de energietransitie zullen naar verwachting grote veranderingen in het energiesysteem plaatsvinden, waaronder ook in de elektriciteitsvoorziening in Nederland. Om daarbij de betrouwbaarheid en betaalbaarheid van de elektriciteitsvoorziening op peil te kunnen houden is het belangrijk om toekomstige risico's te analyseren en lering te trekken uit recente verstoringen die samenhangen met de reeds ingezette energietransitie. In deze paragraaf wordt aan de hand van vier studies besproken welke toekomstige risico's al zijn geïdentificeerd, waarvan ANV, Clingendael en Berenschot ingaan op risico's in Nederland voor de nabije toekomst, en een rapport uit het EU project MIGRATE een risico benoemt van technische aard, met name gericht op het Europese elektriciteitsnet. Een vijfde document betreft een beschrijving en analyse door de netbeheerder in het Verenigd Koninkrijk NationalGrid ESO van een recente grote verstoring die samenhing met het gedrag van een groot offshore windpark.

In een rapportage van het ANV (2019) zijn enkele concrete scenario's uitgewerkt voor de komende 5 jaar voor het thema 'elektrificatie en zon- en windenergie' met de nadruk op impacts. Ook zijn twee scenario's vergeleken met andere risico's in het Nationaal Veiligheidsprofiel, namelijk: 1) Verstoring elektriciteitsvoorziening, en 2) Keteneffecten elektriciteitsuitval. Deze zijn respectievelijk geclassificeerd als 'Waarschijnlijk/Ernstig' en 'Onwaarschijnlijk/Zeer ernstig'. Verder is een algemene beschouwing gewijd aan meer lange-termijn risico's die samenhangen met de energietransitie met een verschuiving van risico's, waarbij het belang wordt genoemd van een goede afstemming tussen de onderdelen van het nieuwe energiesysteem.

In een rapport van het Instituut Clingendael (2019) wordt de klimaattransitie en de mogelijke drastische en abrupte veranderingen in klimaatbeleid in relatie gebracht met negatieve gevolgen voor de Nederlandse economie waarbij met name elektriciteitscentrales die op kernenergie werken worden benoemd. Daarnaast wordt ook toenemende digitalisering en elektrificatie van de maatschappij genoemd als een kwetsbaarheid. Voor de leveringszekerheid van elektriciteit wordt nog genoemd dat weersomstandigheden de elektriciteitsproductie zodanig kunnen beïnvloeden dat leveringszekerheid niet is gegarandeerd.

Tevens wordt de toenemende weerstand vanuit de bevolking tegen duurzame energieparken en tegen beleidsmatige veranderingen die investeringen vergen genoemd, waarbij wordt aangegeven dat die acties bijdragen aan polarisatie en economische gevolgen kunnen hebben voor de betrokken projectontwikkelaars. Een ander risico dat naar voren wordt gebracht is dat er binnen 5 jaar minimaal één land door geo-engineering gaat proberen om het weer te beïnvloeden. Een voorbeeld dat daarover wordt genoemd is het verlagen van de temperatuur met behulp van het in de atmosfeer brengen van zwavel (Smulders, 2018). Dergelijke weersbeïnvloeding kan de hoeveelheid opgewekte energie uit duurzame bronnen (die nu qua energieaanbod juist op gunstige locaties zijn opgesteld, zoals de Noordzee) structureel verlagen. Actieve weersbeïnvloeding is niet in de huidige weermodellen meegenomen, waardoor ook de voorspelbaarheid van de energieproductie uit zon en wind kan afnemen.

Uit een simulatie door Berenschot (2018) van de Nederlandse elektriciteitsvoorziening voor een koude winterperiode in 2030 volgt dat al op ca. 300 momenten tekorten optreden. De duur hiervan is een stuk langer door de grotere mate van elektrificatie die is aangenomen in vergelijking met de PBL Klimaat- en Energieverkenning voor 2030 (in het rapport “het (basis) PBL pakket” genoemd). Het grote aantal tekorten en de hoge pieken hierin worden veroorzaakt door een combinatie van elektrificatie en tegelijkertijd een sterke reductie in het opgestelde vermogen van back-up centrales.

De impact van een groot offshore windpark bij een grote netuitval in Engeland op 9 augustus 2019 is door de netbeheerder NationalGrid ESO geanalyseerd (2019). Deze netuitval werd in eerste instantie veroorzaakt door blikseminslag in een transmissieverbinding, waarop de beveiliging naar behoren heeft gefunctioneerd: na 20 seconden kwam de verbinding weer in bedrijf. Meteen na de blikseminslag verminderde het offshore windpark Hornsea echter de productie met 737MW en viel ook een conventionele centrale van 244MW uit. De daaruit volgende snelle daling van de netfrequentie zorgde, ondanks de inzet van back-up vermogen door de netbeheerder, voor uitval bij 1 miljoen klanten gedurende 15 tot 45 minuten. Volgens de windpark operator Ørsted was de oorzaak van de grote reductie van de windpark productie een laagfrequente (zg. sub-synchrone) elektrische resonantie. De windturbine regeling met de standaard fabrieksinstellingen zorgde voor onvoldoende demping. Na deze uitval zijn deze instellingen aangepast en getest.

Dit voorbeeld geeft aan dat risico’s bestaan bij invloeden van elektriciteit op het net van grootschalige windparken (en zonneparken), die waarschijnlijk toenemen met de geplande uitbreiding hiervan. Het risico betreft hier zowel de afhankelijkheid van de grootschalige duurzame productie (verstoringen als deze wegvalt) als om het effect dat grote parken op kunnen hebben op de regeling en beveiliging van het elektriciteitsnet en daarop aangesloten centrales (en de verstoringen als deze uitvallen). Voor dit specifieke geval in de UK en voor dit moment zijn de problemen verholpen, maar dit biedt in de toekomst geen garanties, omdat de karakteristieken van het elektriciteitsnet continu veranderen. Wanneer bijvoorbeeld in dezelfde regio meerdere nieuwe windparken worden aangesloten, moeten de regeling en beveiliging daarop worden aangepast en getest. Bij dit voorbeeld past wel de nuancering dat het Nederlandse elektriciteitsnet gekoppeld is aan het Europese net, in tegenstelling tot het Britse elektriciteitsnet. Zolang die koppeling in stand blijft zal uitval van eenzelfde hoeveelheid opwekvermogen in Nederland tot een minder snelle en minder diepe frequentiedaling leiden. Dit is overigens wel afhankelijk van de aanwezigheid van roterende massa, die in het Europese elektriciteitsnet ook aan het afnemen is

Naast specifieke problemen met grote windparken leidt de toename van vermogens-elektronische omzetters, bijvoorbeeld voor netkoppeling van zon-PV en laadstations tot veranderingen in de elektriciteitsnetten. Deze veranderingen nopen tot het doorvoeren van aanpassingen in de regeling en beveiliging van elektriciteitsnetten en de daarvoor benodigde ICT (zie tabel 18 met belangrijkste problemen in (Rüberg, 2016)). De verminderde roterende massa in het net, wanneer conventionele synchrone generatoren en motoren worden vervangen door vermogens-elektronische omvormers, leidt bij onbalans tussen vraag en aanbod tot grotere en sneller variërende frequentieverstoringen. Hoewel vermogens-elektronische omvormers kunnen bijdragen aan het corrigeren van deze frequentie-

variaties, zijn de mogelijkheden daartoe beperkter dan voor conventionele centrales. Hierdoor bestaat het risico dat bij te grote variaties er centrales of verbindingen uitvallen, met grootschalige netuitval tot gevolg. Daarbij kan door de verminderde back-up capaciteit vanuit conventionele centrales de duur van de uitval langer zijn. Daarnaast kunnen problemen in de netspanning, zoals instabiliteit of dips ten gevolge van kortsluiting, in een groter gebied merkbaar zijn vanwege de lagere bijdrage van vermogens-elektronische omzetters aan de kortsluitstroom. Hoewel aan oplossingen wordt gewerkt voor aanvullende functionaliteit van duurzame opwekkers voor netondersteuning, zal voor grootschalige implementatie nog enige jaren nodig zijn. Een voorbeeld van zo'n oplossing is de zgn. black-start-voorziening, waarbij duurzame opwekkers bij uitval van het elektriciteitsnet zelfstandig kunnen opstarten en daarbij het elektriciteitsnet weer op spanning kunnen brengen en synchroniseren. Daarnaast zijn vanwege de continue ontwikkelingen in het elektriciteitssysteem, zoals de toename van zon-PV en wind, en in de markten, voortdurend aanpassingen nodig in de monitoring en regeling van de Europese netten.

2.3 Cybersecurity risico's als gevolg van digitalisering en IoT

In een rapport van TKI Top Sector Energie (2019), wordt aangeven dat de elektriciteitslevering meer en meer afhankelijk wordt van o.a. offshore windparken en dat het van cruciaal belang is om cybersecurity vanaf begin af aan te waarborgen. Mogelijkheden voor cyberaanvallen kunnen zowel optreden door beïnvloeden van het operationele en beheer domein als in het verhandelen van de elektriciteit. Een webinar van Underwriters Laboratories (UL, 2019) verduidelijkt dat de energiesector in de VS de op een na hoogste financiële schade ondervond van cyber criminaliteit en in de jaarlijkse Incident Response Summary Report als eerste of tweede belangrijkste staat genoemd ten aanzien kwetsbaarheid voor cybercrime; een beeld dat ook in andere landen op gaat. Daarbij ontstaan door de toename van duurzame opwekkers en smart grid infrastructuur meer kwetsbaarheden, zowel via Internet als via fysieke toegang.

Het Cybersecuritybeeld Nederland (CSBN) (NCTV, 2020), geeft aan dat vitale processen volledig zijn gedigitaliseerd met behulp van industriële controle systemen (ICS). Tevens wordt geconstateerd dat de dreiging van cybercriminelen tegen ICS toeneemt en dat een aanval ontwrichtende werking kan hebben op de continuïteit. Tot nu werden digitale aanvallen op ICS hoofdzakelijk door statelijke actoren veroorzaakt. Er wordt echter ook opgemerkt dat financieel gewin van individuen/organisaties een motivatie kan zijn.

Het Energy Expert Cyber Security Platform (2017) signaleert tien uitdagingen met betrekking tot cybersecurity in de energiesector, waaronder "protection concepts reflecting current threats and risks". Hierbij benoemt het rapport ICT zowel essentieel voor de modernisering van het elektriciteitssysteem als een kritieke factor, in de zin van toegenomen complexiteit, verwevenheid en kwetsbaarheid. Deze kwetsbaarheid hangt onder meer samen met de combinatie van moderne en gedateerde ICT systemen, de onmogelijkheid om essentiële ICT systemen te isoleren of uit te schakelen en de noodzaak voor ondersteuning door nationale veiligheidsdiensten (intelligence) voor het detecteren van en acteren op gecompliceerde cyberaanvallen. Verder worden de volgende nieuwe uitdagingen genoemd die samenhangen met digitalisering: IoT apparatuur, cloud-based

services, ‘big data’ analytics, uitbreiding van (mobiele) telecommunicatiediensten en toepassingen op het gebied van sturing van energievraag en -aanbod.

3 Toekomstige ontwikkelingen in de elektriciteitsvoorziening in Nederland

Dit hoofdstuk beschrijft toekomstige ontwikkelingen in het Nederlandse elektriciteitssysteem die primair samenhangen met de energietransitie en daarnaast met de trend naar verregaande automatisering en slimme apparatuur, ook wel the Internet of Things (IoT) genoemd. Deze ontwikkelingen worden bezien met als achtergrond een toenemende vraag naar elektriciteit, die ook meer geconcentreerd zal zijn door verdere bevolkingsgroei in met name stedelijke gebieden.

Een overzicht is gemaakt voor elk van deze ontwikkelingen op basis van beschikbare documentatie, interviews met TNO experts en een enquête onder enkele leden van het Information Sharing and Analysis Centre Energie van het Nationaal Cyber Security Center. Hieruit volgt een omschrijving hoe het toekomstige Nederlandse elektriciteitssysteem naar verwachting zal zijn opgebouwd en zal worden bedreven. Daarbij wordt beschreven welke nieuwe risico's hierbij kunnen optreden. Uitgangspunt is de vereenvoudigde structuur van het elektriciteitssysteem in 2020 inclusief verantwoordelijkheden zoals in bijlage B grafisch is weergegeven.

3.1 Energietransitie

Voor het behalen van de nationale doelstelling van het klimaatverdrag van Parijs heeft Nederland in 2019 het Klimaatakkoord afgesloten met daarin concrete maatregelen voor 49% reductie[1] van de CO_2 uitstoot in 2030 vergeleken met 1990. Dit leidt tot ingrijpende veranderingen in zowel de energie infrastructuur als in beleid en regelgeving (zoals energiemarkten, CO_2-beprijzing, ruimtelijke ordening), die economische gevolgen hebben voor zowel bedrijven als consumenten.

3.1.1 Ontwikkelingen

De afspraken in het Klimaatakkoord houden een snelle verduurzaming in van de elektriciteitssector met 70% aandeel groene stroom in 2030 als doelstelling (Afspraken voor Elektriciteit, 2021). Hierbij wordt sterk ingezet op groei van de geïnstalleerde capaciteit van zon-PV, wind op zee en wind op land. Om deze nieuwe opwekkers aan te sluiten moeten de transport- en distributienetten sterk en in hoog tempo worden uitgebreid en verzwaard. Daarnaast vergt het in balans houden van het weersafhankelijke elektriciteitsaanbod met de vraag meer flexibiliteit, waarvoor een scala van maatregelen benodigd is. Hiervoor is onder andere regelbaar vermogen nodig dat ook gedurende langere periodes tekorten kan opvangen, bijvoorbeeld centrales met CO_2-vrije brandstoffen, dan wel biobrandstoffen met Carbon Capture and Storage (CCS). Hoewel er tussen landen grote verschillen bestaan in de huidige energievoorziening en de mogelijkheden voor verduurzaming, staan we wereldwijd veelal voor dezelfde uitdagingen voor de grootschalige inpassing van duurzame opwekking (IEA task 25, 2020) en de transformatie van het elektriciteitssysteem als geheel (IEA, 2020).

[1] Deze doelstelling zal worden aangescherpt in lijn met de recentelijk verhoogde Europese CO_2 reductie doelstelling van 55% in 2030 (https://ec.europa.eu/clima/policies/strategies/2030_en)

Om de klimaatdoelstellingen te halen moet ook de energievraag worden verduurzaamd door elektrificatie, bijvoorbeeld door elektrisch rijden t.o.v. rijden op benzine of diesel, en door elektrisch verwarmen, via conversie naar duurzame brandstoffen, zoals groene waterstof of synthetische diesel, en grondstoffen. Wanneer de vraag naar groene stroom achter blijft bij de productie (m.a.w. de investeringen in zon, wind en elektriciteitsnetten zijn al wel gedaan, maar de duurzaam opgewekte elektriciteit wordt niet afgenomen) betekent dit dat de opbrengsten van duurzame opwekkers achter blijven bij de kosten. Daarnaast blijven de sectoren die niet geëlektrificeerd worden afhankelijk van (geïmporteerde) fossiele grondstoffen en brandstoffen. Dit leidt tot een ongunstig marktperspectief voor duurzame opwekkers. Verder is de import-afhankelijkheid van fossiele brandstoffen en grondstoffen, m.n. aardgas, een risico voor de continuïteit van vitale processen in het kader van de nationale veiligheid.

In verband met de energietransitie worden nu en in de toekomst veel projecten uitgevoerd door beheerders van het transmissienet (TenneT, 2017) en de distributienetten om deze uit te breiden en te verzwaren voor nieuwe aansluitingen van wind op zee, zon-PV en nieuwe verbruikers, zoals elektrisch vervoer en warmtepompen. De hoge kosten voor deze netuitbreidingen moeten worden gefinancierd uit hogere energietarieven en/of belastingen. Verder is de snelheid voor het realiseren van deze uitbreidingen in veel gevallen een beperkende factor voor het tempo van deze transitie. Vanwege deze tijdsdruk en om verschillende nationale en regionale ontwikkelingstrajecten voor infrastructuur van elektriciteit, waterstof, CO_2, stoom en warmte beter te integreren zal de rijksoverheid de regie nemen, zoals gesteld in de Kamerbrief van oktober 2020 (Wiebes, 2020), daarbij ondersteund door onder meer het Energietransitie Programma van Netbeheer NL (Netbeheer Nederland, 2019).

Om de wisselende elektriciteitsproductie vanuit zon en wind in balans te houden met de groeiende en sterker wisselende elektriciteitsvraag moet extra flexibiliteit worden ontwikkeld, waarmee eventuele tekorten worden opgevangen en waarmee tijdelijke overproductie wordt benut (i.t.t. curtailment). Dit betreft zowel de aanbodkant (bijv. korte-termijn markten), als de netten (bijvoorbeeld interconnecties, regeling voor congestiemanagement en energieconversie en -opslag), en de vraagkant (bijv. slim laden). Daarbij moeten leveringszekerheid en stabiliteit op een brede tijdschaal worden beschouwd, van langjarige strategische planning van net- en opwekcapaciteit (tot 30 jaar vooruit), de inzet van energieopslag en flexibele opwekking (dagen tot uren) tot het stabiliseren van korte termijn onbalans (minuten tot seconden). Om flexibiliteit op voldoende grote schaal en kosteneffectief te kunnen realiseren is nog veel technologieontwikkeling noodzakelijk, alsook aanpassingen in de huidige regelgeving (2020). Wanneer hierop onvoldoende wordt ingezet en er daardoor onvoldoende flexibiliteit in het elektriciteitssysteem is gerealiseerd zal de kans op tekorten in de elektriciteitsvoorziening, alsook de omvang en duur daarvan toenemen. Hierdoor zullen hoge prijspieken optreden en moeten mogelijk delen van het net worden uitgeschakeld.

Voor de totstandkoming en de uitwerking van het Klimaatakkoord vond en vindt op nationaal en regionaal niveau veel overleg plaats met daarnaast discussie- en informatiesessies, zoals de webinar ‘Spanning op de netten’ (Klimaatakkoord.nl, 2020). Hieruit komt naar voren dat het oplossen van knelpunten in de

elektriciteitsnetten van belang is voor het tempo van de energietransitie. Bij de implementatie zijn nu al knelpunten zichtbaar op het gebied van beleidsontwikkeling, infrastructuur en maatschappelijk draagvlak. Voorbeelden zijn de verdeling van kosten en de beheersing van investeringsrisico's, de beprijzing van CO_2, de lange looptijden voor netverzwaring en -uitbreiding en de maatschappelijke weerstand tegen nieuwe windparken, zonneparken en hoogspanningslijnen.

3.1.2 Toekomstbeelden

Voor het Nederlandse energiesysteem zijn verschillende toekomstscenario's beschikbaar. Deze zijn veelal opgesteld om te verkennen op welke manieren en tegen welke kosten aan de afgesproken klimaatdoelstellingen kan worden voldaan (TNO, 2020), of welke maatregelen en/of infrastructuur hiervoor zijn benodigd (Berenschot, 2018; Netbeheer Nederland, 2019; DNV-GL, 2020a; DNV-GL, 2020b).,Hierbij gaat het rapport van Berenschot (2018) nader in op systeemkeuzes en risico's ten aanzien van leveringszekerheid. Deze scenario's verschillen op aspecten als de mate van en de manier van de inzet van biomassa, CCS en waterstof en de daarvoor benodigde infrastructuur en beleidsmaatregelen. In alle gevallen is de trend richting een meer complex energiesysteem, met een sterke groei van het aandeel elektriciteit, grotendeels opgewekt uit zon en wind, en met verregaande automatisering en decentralisatie. CE Delft (2017) geeft op basis van vier mogelijke toekomstscenario's inzicht in de keuzes voor de regie van de energietransitie en de effecten daarvan op onder meer kosten, ruimtegebruik en keuzevrijheid. Specifiek wordt ingegaan op het belang van maatschappelijk draagvlak. Dit komt echter onder druk te staan door hogere kosten, groter ruimtebeslag voor energie infrastructuur en beperking van keuzevrijheid als gevolg van het (collectief) opdringen van oplossingen. De maatschappelijke weerstand die dit oproept, leidt mogelijk tot vertraging en hogere kosten van de energietransitie.

Ook op Europese schaal zijn er vele vergelijkbare scenario's opgesteld, waarbij naast kosten/baten en leveringszekerheid ook op IT-aspecten wordt ingegaan, ETIP SNET (2018a, 2018b). Deze aspecten, die sterk samenhangen met de energietransitie, worden verder besproken in de volgende paragrafen.

Voor het identificeren van mogelijke nieuwe risico's op de langere termijn zijn, op basis van de literatuur en interviews met TNO-experts, de onderstaande toekomstbeelden geschetst voor 2030 en 2040. Deze beelden zijn niet zo zeer bedoeld om de meest waarschijnlijke scenario's compleet weer te geven, maar om een zinvolle context te geven voor de mogelijke toekomstige risico's en kwetsbaarheden.

De energietransitie leidt tot een meer complex elektriciteitssysteem, dat er rond het jaar **2030** als volgt uit zou kunnen zien:

- De elektriciteitsopwekking in 2030 bestaat voor 70% uit hernieuwbare bronnen, waarvan het merendeel een weersafhankelijk productieprofiel heeft;
- Door het substantiële aandeel van zon en wind in Nederland en elders in Europa vindt meer uitwisseling van elektriciteit plaats, omdat per land (of regio) vaker (en grotere) overschotten en tekorten optreden bij een sterk weersafhankelijke productie. Door deze uitwisseling worden deze overschotten

deels nuttig gebruikt en worden tekorten deels gecompenseerd, zoals ook nu reeds het geval is. Echter, door de hoge mate van gelijktijdigheid van vraag en aanbod van elektriciteit binnen Europa, het beperkt aantal snel regelbare conventionele centrales en de beperkte transportcapaciteit tussen landen kunnen er nog steeds tekorten optreden, met name in langdurige periodes met weinig wind en zon;

- Nederland blijft nog sterk afhankelijk van de import van gas. Hierbij zijn in verband met de leveringszekerheid grote seizoensbuffers nodig zijn. Ook bestaat er financiële onzekerheid bestaat over de prijsontwikkeling op langere termijn;
- Conventionele centrales, met daaraan gekoppelde CCS met onderzeese CO_2 opslag, worden slechts voor beperkte tijd ingezet (tezamen met import) om bij een piekvraag of beperkt aanbod van zon en wind de productie aan te vullen;
- Tijdens periodes met een hoog wind en zon aanbod en een beperkte vraag treden lage marktprijzen op. Conventionele centrales zijn daardoor al vaak uitgeschakeld en zijn mogelijk niet meer rendabel. Bij te lage (mogelijk negatieve) marktprijzen worden ook enkele duurzame opwekkers (m.n. offshore wind) uitgeschakeld om op onderhoudskosten te besparen, waardoor tekorten in de elektriciteitsvoorziening kunnen ontstaan;
- Voor balancering van vraag en aanbod zijn extra interconnectoren met de buurlanden aangelegd. Daarnaast zijn enkele contracten met grote opwekkers en verbruikers afgesloten voor het leveren van reservecapaciteit (een garantie voor het kunnen leveren of afregelen van een bepaalde hoeveelheid elektrisch vermogen in het geval van een tekort of overschot) en reservevermogen (het daadwerkelijk op- of afregelen van productie of verbruik voor balancering). Dit is echter onvoldoende om tekorten te voorkomen, zodat enkele kostbare piekcentrales operationeel moeten blijven.
- Het merendeel van de elektriciteit met een fluctuerend aanbodprofiel wordt inmiddels verhandeld op korte-termijn (Intra-Day) markten, die geheel gekoppeld zijn in NW-Europa;
- Het transportnetwerk wordt continu uitgebreid, zowel het (offshore) transportnet als de distributienetten. Deze uitbreidingen bepalen het tempo waarin nieuwe opwekkers en verbruikers kunnen worden aangesloten. Deze uitbreidingen worden voor het merendeel gefinancierd vanuit de internationale kapitaalmarkt. Alle activiteiten van TenneT in Nederland worden in dit 2030 toekomstbeeld aangestuurd vanuit het hoofdkantoor in Bayreuth in Duitsland.
- Distributienetten zijn in de regel aangelegd met voldoende overcapaciteit om in geval van onderhoud of storing netcongestie te voorkomen. De aanvraag van aansluitingen voor nieuwe installaties zoals zon-PV en EV-snelladers gebeurt veelal niet tijdig om voldoende netuitbreiding te kunnen realiseren. Dit leidt in veel gevallen tot vertragingen en hoge investeringen. Om toch in de grote vraag naar aansluitcapaciteit te kunnen voorzien worden nieuwe distributienetten met minder redundantie ontworpen en worden bestaande netten in hoge mate belast, waardoor ook de redundantie afneemt. (zie ook de presentatie van Netbeheer Nederland (Netbeheer Nederland, 2020));
- Op het High Voltage Direct Current (HVDC) Noordzeenet is ca. 50GW aan offshore windparken aangesloten, zoals IJmuiden Ver, Norfolk (VK) en diverse parken in VK en de Duitse bocht. Daarbij is maximaal ca. 25GW aan transportcapaciteit beschikbaar voor uitwisseling van elektriciteit tussen NL en ander Noordzeelanden (op momenten dat alle windparken uit zouden staan).

Dit net wordt bedreven door een NW-Europese Independent System Operator voor zowel elektriciteit als gas.
- Vervoer en verwarming zijn grotendeels geëlektrificeerd;
- De energie-intensieve industrie werkt nauw samen met elektriciteitsproducenten en netwerkbedrijven voor verdere decarbonisatie, via elektrificatie en duurzame (rest)warmte, waterstof en CCS;
- Alle nieuwe auto's zijn in staat om slim te laden, daarbij centraal aangestuurd door een aggregator die acteert op de stroommarkten;
- Door middel van lokale opslag achter de meter (thuis- of buurtaccu's, EV's) worden pieken in de opwekking (zon-PV) en vraag verminderd, waardoor netcongestie afneemt. Gedurende de zomerse dagen worden echter veel PV installaties door de netbeheerder nog afgeregeld om overbelasting in het net te voorkomen. Van PV installaties wordt het vermogen via Internet centraal gemeten. Met deze metingen worden nauwkeurige (lokale) opbrengstvoorspellingen gemaakt.
- Netbeheerders hebben nog onvoldoende wettelijke mogelijkheden om bijvoorbeeld met lokale opslag netcongestie of lokale spanningsproblemen te verminderen;
- Daarnaast is de regelgeving voor decentrale opwekkers, aggregators en verbruikers (service providers van laadstations) nog niet geheel op orde, waardoor onvoorspelbaar gedrag kan optreden dat de netstabiliteit negatief kan beïnvloeden;
- Opslagcapaciteit wordt gedeeld tussen partijen met verschillende verbruikspatronen, zowel gekoppeld via het elektrische netwerk als via IT.

In **2040** is volgens de nationale doelstelling de Nederlandse elektriciteitsvoorziening 100% verduurzaamd, waarbij het aandeel elektriciteit in de energiemix naar schatting tweemaal hoger is dan het huidige aandeel. Hiermee voldoet de elektriciteitssector als eerste aan de CO_2 reductie doelstellingen. Inmiddels is er in dit scenario een landelijke infrastructuur voor waterstof en een (meer regionale) infrastructuur voor CO_2 en warmte. Deze worden echter nog niet ten volle benut omdat een deel van de zware industrie, luchtvaart en scheepvaart nog verder moeten verduurzamen. Inmiddels zijn de gevolgen van de klimaatverandering al wel duidelijk merkbaar, zoals periodes met extreme droogte en veel zware stormen in combinatie met hoge waterstanden. In deze context zou het elektriciteitssysteem er als volgt uit zou kunnen zien:

- De geïnstalleerde capaciteit aan zon en wind is tweemaal hoger dan de piekvraag, waarbij de helft van de productie uit deze bronnen wordt omgezet in en opgeslagen als groene waterstof of warmte;
- Naast de groei van 2 GW per jaar aan offshore wind is de vervangingsvraag van vergelijkbare omvang: windparken worden na ca. 25 jaar ontmanteld en vervangen door nieuwe. Hierdoor bestaan er grote tekorten aan arbeidskrachten en grondstoffen, wat deels wordt opgevangen door inspecties en onderhoud door drones en robots;
- De nog resterende conventionele piekcentrales zijn omgebouwd op waterstof, maar leveren onvoldoende vermogen tijdens vraagpieken in de winter bij een laag aanbod van zon en wind.
- Een deel van de elektriciteitscentrales, hoogspanningsstations en de industrie wordt uit de kuststreek verplaatst naar Oost-Nederland vanwege de kans op overstromingen;

- Een groot aantal partijen levert flexibiliteit via batterijen, die autonoom op de korte-termijn elektriciteitsmarkten acteren en die ook direct op afwijkingen van de netfrequentie reageren. Voor levering van back-up vermogen op langere tijdschalen zijn brandstofcellen aangesloten, met name in steden, waarbij deze ook restwarmte aan gebouwen leveren;
- Ondanks deze grootschalige energieopslag ontstaan er in de wintermaanden tekorten, waardoor vanwege hoge elektriciteitsprijzen enkele grootverbruikers hun elektriciteitsconsumptie verlagen;
- Alle grootverbruikers en ook de helft van alle huishoudens zijn via het internet gekoppeld, zodat deze autonoom reageren op marktprijzen. Daarnaast is de helft van alle huishoudens energieneutraal;
- Vervoer is 100% verduurzaamd: elektrisch voor personenvervoer en regionaal transport en groene waterstof en biobrandstoffen voor zwaar transport;
- 90% van alle opwekkers en gebruikers is gekoppeld via vermogens-elektronische interfaces. De batterijen in de distributie-onderstations worden ook ingezet voor het regelen van de netspanning en voor verbetering van de (harmonische) spanningskwaliteit;
- In nieuwe wijken en industriegebieden worden standaard gelijkstroom-netwerken aangelegd, die bij uitval van het openbare net nog enkele uren kunnen opereren. Een ander deel van de huishoudens is geheel zelfvoorzienend, zonder aansluiting op het gasnet of het elektriciteitsnet;
- Op transmissieniveau moeten maatregelen worden getroffen om de sterkere frequentieschommelingen in het net van de laatste jaren te beperken. Hierbij kan worden gedacht aan aanvullende eisen aan opwekkers voor de bijdrage aan frequentiestabiliteit en aan het toevoegen van installaties in het net die hieraan bijdragen.
- De beveiliging van distributienetten wordt aangepast, zie ook ESIG (ESIG, 2020) naar een elektronische beveiliging, omdat thermische zekeringen niet meer betrouwbaar werken.

3.1.3 Nieuwe mogelijke risico's

Op basis van deze documentatie en interviews met experts ontstaat het volgende beeld ten aanzien van nieuwe mogelijke risico's en kwetsbaarheden, die samenhangen met de energietransitie:

- Decentralisatie van de energievoorziening op land leidt naar verwachting eerder tot een verschuiving van risico's dan tot grotere risico's. Door de geografische spreiding van een groot aantal kleinere opwekkers zal bijvoorbeeld minder snel sprake zijn van een abrupte grootschalige uitval dan bij een beperkt aantal grote centrale opwekkers, gesteld dat er geen grootschalige verstoring in het Nederlandse elektriciteitsnet optreedt waardoor wind- en zonne-parken afschakelen. Daarentegen ontstaan er nieuwe risico's op lokale congestie of lokale uitval.
- De samenleving wordt in nog grotere mate afhankelijk van een betrouwbare elektriciteitsvoorziening, vanwege elektrificatie van onder meer vervoer, verwarming en de energie-intensieve industrie. Ook de grotere afhankelijkheid van IT draagt hieraan bij.
- Door het grote aandeel van zon en wind in de elektriciteitsvoorziening ontstaan grote fluctuaties en onvoorspelbaarheid in het aanbod, wat zich vertaalt in sterke fluctuaties van marktprijzen. Dit leidt tot financiële risico's voor

investeerders en operators, wanneer bij overschotten lage marktprijzen ontstaan of wanneer bij tekorten duur reservevermogen moet worden ingekocht. Ook kunnen tijdelijke tekorten ontstaan als gevolg van de onzekere vraag- en aanbodvoorspellingen, wat de leveringszekerheid kan beïnvloeden.
- Door uitfasering van conventionele (kolen)centrales in combinatie met onvoldoende snelle groei van duurzame opwekking zal, in combinatie met de verminderde binnenlandse gasproductie, Nederland voor de elektriciteitsvoorziening tijdelijk sterk afhankelijk zijn van de import van gas, en daarmee kwetsbaar in geval van geopolitieke spanningen.
- Door de snelle toename van het aandeel zon en wind zal bij een groot aanbod vaker congestie in de transport- en distributienetten ontstaan, waardoor de elektriciteitsproductie uit zon en wind moet worden verminderd (curtailment) om overbelasting te voorkomen. Een versterkend effect hierbij is de grote mate van elektrificatie van de vraag.
- De processen in de energie-intensieve industrie zijn gevoelig voor fluctuaties in het aanbod en de prijs van elektriciteit, waardoor economische schade optreedt en mogelijk ook milieuschade kan ontstaan, bijvoorbeeld doordat chemische processen worden verstoord of moeten stilgelegd;
- Door de verminderde back-up capaciteit vanwege uitfasering van conventionele centrales, kunnen bij uitval van een elektriciteitscentrale, windpark of netwerkverbinding cascade-effecten optreden, met als mogelijk gevolg grootschalige en langdurige uitval.
- Transmissienetwerken worden verder uitgebreid. Hierdoor is, met name op zee, de fysieke beveiliging van installaties als windparken en onderstations en kabels moeilijk realiseerbaar. Verondersteld wordt dat het niveau van beveiliging bij onbemande platforms laag is. Daardoor zijn er risico's op ongeautoriseerde toegang tot de installaties en de IT netwerken die deze besturen en monitoren.

3.2 Digitalisering

3.2.1 Ontwikkelingen en toekomstbeelden

De ontwikkelingen in het domein van Operationele Techniek (OT) van het energiesysteem hangen sterk samen met die in het IT domein. Zo is de bedrijfsvoering van zon-PV en windparken (aanbodvoorspelling, regeling en beveiliging) rond 2040 volledig geautomatiseerd, alsook de afstemming van de vraag van grote verbruikers op het voorspelde aanbod. Ook in de elektriciteitsnetten wordt verdere automatisering doorgevoerd, vanwege de steeds hogere en sterker wisselende bezettingsgraad. Daarnaast vindt ook meer en sneller variërende uitwisseling van elektriciteit tussen Europese landen plaats. Deze ontwikkelingen vereisen meer en snellere uitwisseling van informatie (tussen partijen aan de aanbod- en vraagzijde onderling en met netwerkoperators op transmissie-distributie niveau) waarop ook sneller moet worden geacteerd, bijvoorbeeld in geval van dreigende overbelasting of onbalans. Automatisering van netten is daarbij ook een middel om operationele kosten te kunnen besparen. Ook aan de vraagzijde neemt automatisering gestaag toe door vraagsturing en decentrale elektriciteitsproductie en opslag.

Een van de vele complicerende factoren daarbij is dat er veel nieuwe aangesloten partijen actief zijn die autonoom kunnen acteren. Hierbij kan worden gedacht aan

laders voor elektrische auto's of voor batterijen in woningen die afhankelijk van de (verwachte) marktprijs laden dan wel terugleveren aan het net. Daarnaast kost de modernisering van netten (m.n. distributienetten) veel tijd en geld, waardoor nieuwe en oude systemen voor lange tijd naast elkaar operationeel zijn.

In een position paper van ETIP SNET (2018a) zijn de verschillende nieuwe mogelijkheden van verdere digitalisering voor het toekomstige elektriciteitsnet uiteengezet, zoals DC netwerken, digitale onderstations, en vraagsturing via agents. Vanwege onder meer decentrale opwekking en vraagsturing ontstaat de noodzaak tot actief beheer van distributienetten, zowel voor monitoring, beveiliging, voorspelling en (terug)regelen van decentrale opwekking. Vanwege de geografische spreiding, de continue veranderingen in het elektriciteitssysteem, de vele actoren en de grote hoeveelheid aan data wordt cloud-based computing in combinatie met 5G IT beschouwd als de meest kansrijke oplossing voor een dergelijk "Smart Energy Platform". Hiermee kunnen concepten als een digital twin mogelijk worden geïmplementeerd, waarbij de efficiëntie en betrouwbaarheid van het elektriciteitssysteem kunnen worden geoptimaliseerd. Ook de toepassing van remote inspectie en onderhoud met drones en robots kan de efficiëntie en betrouwbaarheid vergroten.

In het advies van RLI (2018) worden kwetsbaarheden van een gedigitaliseerd energiesysteem genoemd aan de hand van historische gebeurtenissen: 1) software fouten, 2) onvoorzien gedrag van autonome systemen, 3) moedwillige verstoringen, en 4) digitale systemen in Europese context. Daarmee zijn dit niet strikt nieuwe kwetsbaarheden maar nemen deze toe met verdere digitalisering.

3.2.2 Nieuwe mogelijke risico's

Uit de interviews met TNO experts, documenten en enquêteresultaten volgt de onderstaande beschrijving van specifieke risico's:

- De verdere digitalisering en invoering van IoT in de elektriciteitsvoorziening vergroot in het algemeen het aantal kwetsbaarheden. Er is een verschuiving gaande van een passief ontworpen systeem met ruime veiligheidsmarges naar een meer agile aanpak. De voordelen zijn vooral economisch, bijvoorbeeld lagere operationele kosten of doordat met extra flexibiliteit netuitbreidingen kunnen worden beperkt.
- De afhankelijkheid van cloud-based computing en data, nauwkeurige tijdsynchronisatie en complexe netmodellen voor de bedrijfsvoering van netten. Bij uitval of verstoring van (een deel van) deze ICT systemen bestaat het risico dat er onvoldoende of onjuiste informatie beschikbaar komt bij netbeheerders om adequaat te kunnen handelen, teneinde het elektriciteitsnet stabiel te houden.
- Er wordt (uit kosten overwegingen) ook steeds meer gebruik gemaakt van het Internet, in plaats van ICT netwerken die niet fysiek zijn gekoppeld aan het Internet. Dit leidt, ondanks beveiligingsmaatregelen, tot grotere risico's voor cyber crime.
- Het gebruik van commerciële dienstverleners door netbeheerders creëert onderliggende afhankelijkheden, die ook bestaan tussen verschillende partijen (zie ook SEGRID Whitepaper (2017)). Verschillende dienstverleners kunnen

bijvoorbeeld gebruik maken van hetzelfde glasvezelnetwerk, of dezelfde data servers, waardoor bij uitval beide diensten uitvallen.
- Kwetsbaarheid door standaardisatie en afhankelijkheid van een beperkt aantal leveranciers (al wordt deze kleiner geacht dan bij 5G ICT netwerken). Hierdoor kan een kwetsbaarheid in één type gestandaardiseerd onderdeel in het elektriciteitssysteem tot een grootschalig risico leiden. Voorbeelden zijn grote aantallen van hetzelfde type zon-PV inverters die vanwege een software fout zichzelf gelijktijdig hebben afgeschakeld.
- Offshore IT-infrastructuur kan onvoldoende (fysiek) worden beveiligd.
- De sterke toename van het aantal cyberaanvallen, zowel grootschalige (langdurig voorbereide) aanvallen als ransomware, vergroot de noodzaak tot het testen van IT systemen en geautomatiseerde cybersecurity. Dit is echter kostbaar en vereist specialistische kennis, wat ook geldt voor het realiseren van robuuste systemen (zoals bijvoorbeeld redundante, elkaar controlerende systemen). Hierdoor ontstaat het risico dat onvoldoende beveiligingsmaatregelen (kunnen) worden getroffen waardoor IT systemen extra kwetsbaar zijn voor cyberaanvallen.
- Digitalisering van de maatschappij kan bij verstoringen in de elektriciteitsvoorziening leiden tot storingen in (publieke) voorzieningen met als mogelijk gevolg onduidelijkheden bij bijvoorbeeld hulpdiensten, al zijn de risico's niet per se groter. Voorbeelden zijn uitval van elektronische toegang van gebouwen en terreinen, signalering en andere veiligheidsvoorzieningen.

3.3 Internet of Things

3.3.1 Ontwikkelingen

Met de modernisering van het elektriciteitssysteem worden grote aantallen apparaten met elkaar verbonden via het Internet (IoT). Omdat IoT als sleuteltechnologie wordt gezien, onder meer voor smart cities, maakt dit een stormachtige groei door. Het betreft vooral het op afstand bedienen van kleinere elektriciteitsverbruikers voor consumenten, zoals koelkasten en verwarmingsinstallaties, maar ook publieke voorzieningen in ziekenhuizen en hotels, en installaties met vermogens-elektronische omzetters voor de netkoppeling van zon-PV installaties, windparken en EV-laders. Mogelijk maken ook netbeheerders, grote utilities en industrie hiervan gebruik, naast hun private IT-netwerken, bijvoorbeeld door slimme sensoren toe te passen die communiceren via het publieke internet.

Veel IoT apparatuur is echter slecht beveiligd, vanwege kwetsbaarheden in het ontwerp en onvoldoende beveiligingsinstellingen door de gebruikers. Dit soort appratuur is veelal niet volgens de principes van "security by design" ontworpen, waardoor bijvoorbeeld geen beveiligingsupdates kunnen worden geïmplementeerd. Daarnaast worden mogelijkheden voor betere beveiliging, zoals firmware updates of het wijzigen van default username/password combinaties, vaak niet benut. Ook kunnen door fabrikanten mogelijkheden zijn ingebouwd om toegang te krijgen tot de besturing van deze apparatuur, of tot data hieruit, bijvoorbeeld voor het aanbieden van Internet Cloud diensten. Veel IoT apparatuur is onbeheerd, waardoor niet bekend is of en welke communicatie met externe partijen plaatsvindt.

3.3.2 Nieuwe mogelijke risico's

Uit de interviews met TNO experts, documenten en enquêteresultaten volgt de onderstaande beschrijving van specifieke risico's:

- Een aanval op groot aantal verbruikers (bijvoorbeeld snelladers) is denkbaar, waardoor verstoring/instabiliteit kan ontstaan door gelijktijdig en aan-/uitschakelen.
- Veel apparatuur (m.n. in goedkopere segment) is niet ontworpen volgens "security by design" en is niet te updaten, met een grote kans op kwetsbaarheden die bovendien niet kunnen worden verholpen. Dit kan zowel leiden tot ongewenst en onvoorspelbaar gedrag in de besturing van deze apparatuur, zoals gelijktijdig en snel aan en uit schakelen, als tot het lekken van gebruikersdata of andere ongewenste communicatie zoals gedistribueerde data mining of gerichte aanvallen op servers.
- Storingen in de elektriciteitsvoorziening leiden tot tijdelijke uitval van of schade aan IoT apparatuur, waardoor een groot aantal voorzieningen niet meer werkt.

4 Scenario's voor de verkenning van nieuwe risico's

In dit hoofdstuk worden aan de hand van enkele scenario's nieuwe risico's verkend met daarbij mogelijke cascade-effecten die kunnen ontstaan. Daarbij is aandacht voor gevolgen op het gebied van de nationale veiligheid.

Tabel 4-1 geeft een voorgestelde categorisering van risico's aan die gebaseerd is op bestaande methodieken van het ANV. In de volgende drie paragrafen worden verschillende oorzaken van risico's genoemd, gerangschikt naar de drie categorieën 'technisch falen', 'menselijk falen' en 'moedwillig'.

Tabel 4-1: Categorisering van risico's

OORZAAK	ACTOR	MOTIEF	DOELWIT	GETROFFENEN	AARD VAN DE AANTASTING	GEOGRAFISCHE SCHAAL	DUUR
Technisch falen	Beroeps-criminelen	Economisch	HS/MS onderstation	Openbaar bestuur, politiek	Beschikbaarheid	Lokaal (wijk)	< 24 uur
Menselijk falen	Staten	Ideologisch	Offshore windpark	Vitale sectoren	Integriteit	Regionaal (provincie)	2-6 dagen
Moedwillig	Terroristen	Politiek	ICT systeem netbeheerder	Bedrijfsleven	Vertrouwelijkheid	Landelijk	1-4 weken
	Cybercriminelen	Ego, wraak, profilering	ICT decentrale opwekking of verbruikers	Burgers		Internationaal (NW-Europa)	1-6 maanden
	Activisten		IoT apparatuur				> 6 maanden
	Interne actoren						onherstelbaar

4.1 Technisch falen

Technisch falen kan worden onderverdeeld tussen interne risico's en externe risico's. Interne risico's worden veroorzaakt door falen van interne componenten, externe risico's door externe omstandigheden.

Voorbeelden interne oorzaken:

- Onbalans tussen vraag en aanbod t.g.v. uitval van opwerkeenheden (evt. import via Interconnector) of foutieve vraag- of aanbodvoorspelling (zon, wind) in combinatie met onvoldoende beschikbare reservecapaciteit om dit te herstellen.
- Snelle schommelingen van de netfrequentie t.g.v. de verminderde roterende massa in het elektriciteitssysteem en waarbij de regelingen van de aangesloten (opwek)eenheden niet voldoende bijdragen aan de demping van deze frequentieschommelingen (of zelfs zorgen voor opslingering).
- Gelijktijdig aan- en afschakelen van verbruikers die geautomatiseerd reageren op de variërende marktprijs (bijv. EV, WKKs).
- Lokale verstoring van de netspanning in distributienetten door snel wisselende opwekking (bijv. zon-PV).
- Spanningsdip door kortsluiting, waarvan de omvang en duur worden vergroot ten gevolge van onvoldoende kortsluitvermogen vanwege het uitfaseren van conventionele opwekkers.
- Netvervuiling door onbedoelde interacties tussen vermogens-elektronische omzetters (met het net of onderling).
- Congestie in het distributienet door decentrale opwekking waardoor het verminderen van decentrale productie (curtailment) noodzakelijk is.

- Overbelasting van het transmissienet in NL of buurlanden waardoor een deel van het net moet worden afgeschakeld.
- Uitval van communicatie met geautomatiseerde opwekkers of verbruikers, waardoor deze afschakelen of onvoorspelbaar gedrag vertonen.
- Uitval van communicatie van netbedrijven op Europese schaal, waardoor de systeembalans kan worden verstoord, of tussen de TSO en DSOs, waardoor congestie kan ontstaan.

Voorbeelden van externe oorzaken zijn:
- Een zonnestorm, waardoor ICT en vermogens-elektronische omzetters uitvallen en deels defect raken.
- Extreem hoge windsnelheden, die deels onverwacht optreden, zowel qua sterkte als timing. Hierdoor kan een windpark tijdelijk uit bedrijf gaan.
- Door een extreme storm raakt een schip op drift in een windpark, waardoor wind turbines worden beschadigd en mogelijk ook het TenneT hoogspanningsstation. Het slepende anker beschadigt een groot deel van de kabels in het windpark.
- Door slecht weer verongelukt een crew transfer vessel (een transportvaartuig voor vervoer van personeel naar een windpark) of heli in een windpark op zee.

4.2 Menselijk falen

Het gaat hier om zaken die worden veroorzaakt door menselijk falen (onbedoeld handelen, geen opzet).

Voorbeelden:
- Ontwerpfout in de besturingssoftware van IoT consumenten apparatuur waardoor deze ongecontroleerd aan- en afschakelen. Hierdoor ontstaan snelle spanningsvariaties op wijkniveau waardoor een groot aantal laagspanningsdistributienetten uitvallen.
- Bug in software update van windturbines waardoor deze tegelijkertijd afschakelen, bijv. bij afwijkingen in de netfrequentie.
- Een 2GW onderzeese elektriciteitskabel (Interconnector en/of verbinding naar een windpark) raakt defect door een scheepsanker dat niet is gelicht of op een verkeerde locatie is neergelaten.
- Onvoldoende reservevermogen ingekocht als voorziening bij uitval of onderhoud met als gevolg extreem hoog oplopende marktprijzen.
- Optimistische inschatting van kosten en doorlooptijd netuitbreiding, die bijv. kunnen leiden tot vertraging aansluiting van windparken.
- Door politieke druk om meer duurzame energie aan te sluiten wordt een deel van de benodigde (N-1) reserve transportcapaciteit bezet. Daarnaast leidt de grote vraag naar aansluitcapaciteit op distributieniveau tot keuzes om een deel van de bestaande overcapaciteit aan te spreken, waardoor de redundantie afneemt.

4.3 Moedwillig handelen

Onder deze categorie vallen oorzaken door moedwillig handelen (opzet) door een breed scala van actoren en motieven.

Voorbeelden:
- Fysieke toegang tot offshore windpark, waardoor de besturing kan worden overgenomen of sabotage kan worden gepleegd.
- Cyberaanval op IT systeem van offshore windpark operator waardoor de besturing kan worden overgenomen dan wel geblokkeerd.
- Cyberaanval op IT systeem van offshore windpark operator waardoor toegang tot gevoelige (markt)data kan worden verkregen.
- Cyberaanval op IT systeem van netbeheerder waardoor de besturing van onderstations kan worden verstoord.
- Cyberaanval op IT systeem van grote vloot laadpalen waardoor deze tegelijkertijd aan- of afschakelen.
- Cyberaanval op slecht beveiligde IoT consumentenapparatuur waardoor deze onbruikbaar worden of data kan worden gelekt.
- Cyberaanval op smart meters waardoor verbruiksdata kan worden ingezien en gemanipuleerd en mogelijk verbruikers kunnen worden afgesloten.
- Beïnvloeding besluitvorming t.a.v. uitbreiding/modernisering/vergroening van het elektriciteitssysteem: “In Duitsland lopen de energiepolitiek en de aandeelhoudersbelangen meer door elkaar”, aldus de CFO van TenneT (Energeia, 2020).

4.4 Beschrijving mogelijke scenario’s

In deze paragraaf worden enkele scenario’s geschetst van risico’s en mogelijke (cascade) effecten.

4.4.1 Technisch falen

In 2040 is de elektriciteitsopwekking in NL verduurzaamd, met 30 GW offshore wind, 30 GW zon PV, nog 5 GW conventioneel vermogen en 5 GW duurzaam vermogen (biomassa/H2). Personenvervoer rijdt 100% op elektriciteit en het vrachtvervoer rijdt grotendeels op waterstof. Verwarming gebeurt of elektrisch d.m.v. van warmtepompen, of via restwarmte uit datacenters, elektrolyse, (biomassa)WKKs of industrie.
Door extreme weersomstandigheden in de winter is de productie uit zon en wind veel lager dan verwacht. Het ontstane tekort, geschat op 20GW, kan onvoldoende worden aangevuld met import, vanwege vergelijkbare tekorten in de buurlanden en overbelasting van Interconnectoren naar Zuid-Europa.

Dit heeft tot gevolg:
- Economische schade door het afschakelen (en financieel compenseren) van enkele grootgebruikers om een rolling blackout/brownout te voorkomen.
- Door de schaarste van elektriciteit treden er extreem hoge prijzen op, waardoor datacenters om economische redenen deels afschakelen en het Internet verkeer wordt ontregeld.
- Imagoschade door de minder gebleken betrouwbaarheid van de energieleverantie.

4.4.2 Menselijk falen

In 2030 is volgens plan 11.5 GW offshore wind capaciteit operationeel. Het grootste windpark IJmuiden Ver 2 x 2000MW bestaat uit windturbines van eenzelfde type, centraal aangestuurd vanuit het control center van de buitenlandse fabrikant. Een recent geïmplementeerde update van de windturbine regeling is op een enkele windturbine succesvol getest. Echter door onbedoelde interacties met het HVDC offshore station valt het lokale offshore windpark net uit en lukt het niet om deze weer op te starten. De vermoedelijke oorzaak wordt gemeld aan de netbeheerder die een onderzoek instelt naar mogelijke schade aan apparatuur en naar de oorzaak van de uitval. De software update wordt teruggedraaid en na een week wordt het offshore wind stapsgewijs weer opgestart.

Dit heeft tot gevolg:
- Uitval van service: Door een groot windaanbod ten tijde van de uitval ontstaat acute onbalans in het net, waardoor grootverbruikers worden afgeschakeld en een deel van het net uitvalt.
- Een grote waterstoffabriek moet hierdoor de productie stoppen, waardoor in de dagen erna tekorten ontstaan bij waterstof tankstations in de randstad.
- Economische schade: inkoop van extra opwekcapaciteit/vermogen, schadeclaims.
- Imagoschade: windturbine fabrikant verlies toekomstige orders en moet naast het herstellen ook schadevergoeding betalen.

4.4.3 Moedwillig handelen

In 2030 is volgens plan 11.5 GW offshore wind capaciteit operationeel, waarvan het merendeel bestaat uit grote gestandaardiseerde offshore onderstations (5 x 700MW HVAC en 2 x 2000MW HVDC). Door de beperkte fysieke beveiliging vindt sabotage plaats van hoogspanningsapparatuur, waardoor een groot deel van deze onderstations onklaar wordt gemaakt. Daarbij is eerst ook in de server van de netbeheerder op dit platform overgenomen, waardoor niet meteen zichtbaar wordt bij de operators dat er een probleem is en er niet adequaat wordt opgetreden. Tegelijkertijd raakt het communicatie systeem van zowel de netbeheerder als de betreffende windturbine operators door een gerichte aanval overbelast.

Gevolg is dat binnen een kort tijdsbestek ca. 8000MW aan opwekcapaciteit langdurig wegvalt, wat leidt tot:
- Uitval van service: In geval van een groot windaanbod ten tijde van de uitval ontstaat acute onbalans in het net, waardoor grootverbruikers worden afgeschakeld en een deel van het noordwest Europese net uitvalt.
- De hulpdiensten rijden allemaal elektrisch en kunnen na verloop van enkele uren tot dagen niet meer voldoende opladen om uit te rukken. Ook bij 112 meldingen kunnen mensen niet meer altijd worden geholpen. Door deze uitval en onzekerheid over de duur ontstaat een gevoel van onveiligheid.
- Er komt een tekort aan (mobiele) noodstroom voorzieningen, waardoor enkele publieke voorzieningen als scholen en ziekenhuizen moeten worden gesloten en als gevolg maatschappelijke onrust ontstaat.
- Economische schade: Langdurige tekorten, waardoor opwekcapaciteit moet worden gereserveerd en aangesproken.

- Economische schade: Schade aan onderstations met lange reparatietijden (1 week tot 1 maand, afhankelijk van besteltijd van apparatuur, mobilisatietijd van (kraan)schepen en personeel en weersomstandigheden).
- Imagoschade: Vanwege getoonde kwetsbaarheid van offshore energieopwekking en elektriciteitstransport.

5 Conclusies en aanbevelingen

De energietransitie, digitalisering en IoT leiden tot ingrijpende ontwikkelingen in het Nederlandse elektriciteitssysteem, die zich vooral vertalen in nieuwe en verschuivende risico's en kwetsbaarheden. Als hierop onvoldoende wordt geanticipeerd zullen de kans op verstoringen en de omvang daarvan (qua duur en geografische schaal) toenemen. De daaruit volgende impact kan, net als in het huidige elektriciteitssysteem het geval is, ernstig zijn. Met de verdere elektrificatie van de energievoorziening, zoals bijvoorbeeld vervoer en de energie-intensieve industrie, en de grotere afhankelijkheid van IT, zal naar verwachting de impact van verstoringen c.q. uitval toenemen.

5.1 Risico's in relatie tot nationale veiligheid

Samenvattend worden de volgende mogelijke nieuwe risico's die kunnen ontstaan voor de periode 2030-2040 en mogelijke implicaties voor de nationale veiligheid geïdentificeerd. Per risico wordt aangegeven op welk(e) nationale veiligheidsbelang(en) deze met name betrekking hebben: 1) territoriale veiligheid, 2) fysieke veiligheid, 3) economische veiligheid, 4) ecologische veiligheid, 5) sociale en politieke stabiliteit, en 6) internationale rechtsorde. In Tabel 5-1 staan de impactcriteria per nationaal veiligheidsbelang (NCTV, 2019).

De mogelijke risico's kunnen ieder op zich leiden tot een breed scala van gevolgen, afhankelijk van de keten van gebeurtenissen die volgt op de kwetsbaarheid (de cascade-effecten). Voor ieder risico is in ieder geval uitval van het net in meer of mindere mate een mogelijk gevolg, waardoor de impact op sociale en politieke stabiliteit, specifiek de verstoring van het dagelijkse leven, van toepassing is. Daarom is het impact criterium 5.1 'verstoring van het dagelijkse leven' m.b.t. het nationaal veiligheidsbelang (5) niet bij ieder risico als zodanig aangeduid: dit is als het ware de rode draad door de impact van de gebeurtenissen. Hierdoor is tegelijkertijd meer oog voor de andere vormen van impact die de mogelijke risico's en kwetsbaarheden met zich mee kunnen brengen.

Tabel 5-1: Impactcriteria per nationaal veiligheidsbelang (NCTV, 2019).

Nationaal veiligheidsbelang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het (Nederlands) grondgebied 1.2 Aantasting van de integriteit van de internationale positie van Nederland 1.3 Aantasting van de integriteit van de digitale ruimte
2. Fysieke veiligheid	2.1 Doden 2.2 Ernstig gewonden en chronisch zieken 2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten 3.2 Aantasting van de vitaliteit van de Nederlandse economie
4. Ecologische veiligheid	4.1 Langdurige aantasting van het milieu en de natuur
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtstaat 5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens 6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel 6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties

Voor de leesbaarheid zijn de risico's opgedeeld in drie secties: 1) continuïteit van vitale processen; 2) de integriteit van kennis en informatie; 3) de opbouw van ongewenste strategische afhankelijkheden.

Continuïteit van vitale processen

- Door snelle (weersafhankelijke) schommelingen in het aanbod van elektriciteit uit zon en wind of in de vraag naar elektriciteit door geëlektrificeerde processen kan onbalans tussen vraag en aanbod ontstaan. Wanneer door onvoldoende back-up capaciteit en/of transportbeperkingen de balans niet tijdig kan worden hersteld, moeten gebruikers deels worden afgeschakeld. Hierbij speelt ook de te verwachten grotere strategische afhankelijkheid van het buitenland voor back-up vermogen, zowel direct door import van elektriciteit, als indirect door import van aardgas voor flexibel regelbare elektriciteitsopwekking. (Met name impactcriteria 2.3, 3.1, 3.2).
- Hogere belasting en grotere complexiteit van het elektriciteitsnetwerk, waarbij omwille van snelle uitbreiding en kostenbesparingen minder redundantie is, waardoor relatief kleine verstoringen kunnen leiden tot meer grootschalige congestie of netuitval. In het kader van de nationale veiligheid kan dit zorgen voor problemen van de beschikbaarheid van vitale infrastructuur in Nederland waardoor vitale processen in het geding kunnen komen, maar wellicht ook voor strategische afhankelijkheden. Daarnaast zorgt het voor het creëren van meer aantrekkelijke doelwitten voor kwaadwillende actoren. (Met name impactcriteria 1.1, 2.1, 2.3, 3.2, 5.3).
- Onvoldoende fysieke beveiliging van offshore windparken en offshore netten waardoor deze kwetsbaar zijn voor (evt. gecoördineerde) sabotage. Wanneer onvoldoende aandacht is voor nieuwe installaties die beveiliging vereisen, kunnen deze onopgemerkt zorgen voor een risico (zeker in het kader van moedwillig handelen). In combinatie met de hoge kapitaalkosten, de hoge vermogens (van meerdere gigawatt per kabelpaar) en de langdurige reparatietijden kan dit leiden tot hoge reparatiekosten, grootschalige (gelijktijdige) uitval van het elektriciteitsaanbod uit offshore wind, met als onmiddellijk gevolg grootschalige elektriciteitsuitval op land, met het risico op uitval/verstoring van de continuïteit van vitale processen. Op langere termijn bestaat het risico van een langdurig tekort aan opwek- en interconnectie-capaciteit in Nederland, met grote economische schade als gevolg. (Met name impactcriteria 1.1, 2.1, 2.3, 3.1, 5.3, 6.3).

Integriteit van kennis en informatie

- Ten aanzien van het beheer van IT systemen worden door beperkte toegang tot informatie kwetsbaarheden en (cyber)aanvallen op IT systemen mogelijk niet (tijdig) gedetecteerd. Daarbij kunnen er beperkte mogelijkheden zijn tot het doorvoeren van updates en het actief en geautomatiseerd detecteren en testen van inbraken en kwetsbaarheden. Mogelijke redenen hiervoor zijn onduidelijkheden tussen partijen over de verantwoordelijkheden, beperkte (wettelijke) bevoegdheden, technische beperkingen, zoals het garanderen van de continuïteit, of economische redenen. In het kader van nationale veiligheid is het belangrijk te voorkomen dat onopgemerkte kwetsbaarheden (gedurende langere tijd) kunnen bestaan. Naast een direct risico voor verstoringen van het betreffende IT systeem kunnen op langere termijn ook problemen ontstaan op

gebied van interoperabiliteit tussen verschillende IT systemen. (Met name impactcriteria 1.1, 1.2, 1.3, 2.1, 2.3).

- Grote aantallen decentrale opwekkers en verbruikers (zon-PV, EV) die autonoom of centraal aangestuurd reageren op een elektriciteitsvraag of marktprijs, en daardoor onvoorspelbaar gedrag vertonen dat negatief kan uitwerken op de beschikbare netcapaciteit of de netstabiliteit. Dit fenomeen is niet nieuw, maar is met de huidige 20% duurzame opwekking goed behapbaar. Bij een dominant aandeel duurzame opwekking en uitfasering van conventionele centrales ontstaan veel grotere aanbodfluctuaties die leiden tot sterke prijsschommelingen en daarop reagerende vraag. Achterlopende of ontbrekende regelgeving maakt het voor netbeheerders moeilijk om hier inzicht in te krijgen en om dit de voorkomen. In het kader van nationale veiligheid zijn problemen met de capaciteit of stabiliteit per definitie problematisch, bijvoorbeeld i.v.m. uitval van vitale processen. Dit wordt echter versterkt door het onvoorspelbare gedrag dat voortvloeit uit autonoom handelen, waarbij mogelijk een grote groep verbruikers extern wordt aangestuurd, omdat het vinden van de oorzaak en zorgen voor een oplossing daarmee complexer wordt. (Met name impactcriteria 3.1, 5.3).

<u>Opbouw van ongewenste strategische afhankelijkheden</u>

- Grotere verwevenheid van OT met IT en IoT, waarbij onvoldoende zicht is op de afhankelijkheden, bijvoorbeeld bij outsourcing van IT oplossingen, onderliggende diensten en gestandaardiseerde ICT platforms. In het kader van nationale veiligheid is dit een probleem omdat onduidelijke afhankelijkheden kunnen zorgen voor onverwachte uitval van (vitale) processen. Zonder overzicht van de (afhankelijkheden van) de betreffende (IT) infrastructuren is het lastig om te achterhalen waar problemen, uitval en verstoringen vandaan kunnen komen. Dit zorgt voor vertraging in de opvolging van dergelijke problemen. (Met name impactcriteria 1.3, 2.3, 3.1, 4.1).
- Onvoldoende zicht op het beheer van IT en IoT en beperkte mogelijkheden voor het doorvoeren van updates en voor het actief en geautomatiseerd detecteren en testen van inbraken en kwetsbaarheden. Hierdoor ontstaat het risico dat een groot aantal aan het elektriciteitsnet gekoppelde (decentrale) opwekkers en verbruikers onvoorspelbaar en ongewenst gedrag vertonen, waardoor problemen kunnen ontstaan met de lokale netspanning of - op grotere schaal - met de balans tussen vraag en aanbod, wat tot snelle schommelingen in de netfrequentie leidt. Mogelijke redenen voor deze kwetsbaarheden zijn onduidelijkheden tussen partijen over de verantwoordelijkheden, technische beperkingen, economische redenen of in verband met de continuïteit. Toekomstige risico’s van IoT apparaten op het elektriciteitssysteem zijn momenteel moeilijk in te schatten, mede omdat de sterke groei van IoT vrij recent is gestart en omdat nieuwe toepassingen niet goed zijn te voorspellen. In het kader van nationale veiligheid is het belangrijk om duidelijke verantwoordelijkheden van beheer te hebben zodat geen onopgemerkte kwetsbaarheden (gedurende langere tijd) kunnen bestaan. Anders is er onvoldoende zicht op de systemen en onvoldoende beheer, en dat kan op lange termijn ook problemen veroorzaken wanneer we kijken naar interoperabiliteit van systemen. (Met name impactcriteria 1.3, 2.3, 3.2, 5.1).

5.2 Aanbevelingen

De genoemde risico scenario's zijn nog niet geverifieerd met alle betrokken stakeholders, en het wordt aanbevolen dat alsnog te doen als eerste vervolgstap, bijvoorbeeld in de vorm van meerdere workshops. De bijdragen vanuit de diverse expertises van de stakeholders zijn nodig om risico's vollediger in kaart te brengen en deze vervolgens te wegen en te verifiëren met de betreffende sectoren. Daarin kan ook meer gedetailleerd worden bepaald welke impacts en cascade-effecten kunnen optreden, hierbij rekening houdend met (voor)genomen maatregelen om de weerbaarheid van het elektriciteitsnetwerk te verhogen, en welke strategische afhankelijkheden hierbij relevant zijn. Voorbeelden van mogelijke cascade-effecten die als startpunt kunnen dienen voor het uitwerken en analyseren van risico-scenario's zijn:

- Bij grootschalige verstoringen in het elektriciteitssysteem wordt het 112 alarmnummer overbelast en kunnen niet alle mensen altijd snel geholpen worden. Hulpverleners rijden allemaal elektrisch en kunnen voertuigen niet meer voldoende opladen. Hierdoor zal maatschappelijke onrust toenemen.
- Een mogelijk effect van imagoschade van een elektriciteitsbedrijf op de korte/middellange termijn is een gebrek aan voldoende (financiële) ruimte voor het implementeren van de laatste stand der techniek op het gebied van cybersecurity en/of het aantrekken van voldoende gekwalificeerd personeel, waardoor de kwetsbaarheid voor cyberaanvallen toeneemt.
- Hoge schadevergoedingen als gevolg van grootschalige en/of frequente uitval van de elektriciteitsvoorziening kan leiden tot een kwetsbare financiële positie. Dit zou kunnen leiden tot een inmenging of vijandelijke overname door een bedrijf dat nauwe contacten onderhoudt met een buitenlandse overheid waar Nederland een minder goede relatie mee heeft. Dit risico lijkt nu minimaal met de huidige investeringstoets, maar vanwege toekomstige hoge investeringen van TenneT, grotendeels in Duitsland, is dit niet uit te sluiten.

Een tweede vervolgstap is identificeren welke maatregelen kunnen worden getroffen om de beschreven toekomstige risico's en mogelijke (cascade) effecten te mitigeren als onderdeel van een bredere strategie. Vanuit deze studie komen hiervoor enkele aandachtspunten naar voren. Bij de ontwikkelingen in het energiesysteem in de komende jaren ligt nu grote nadruk op snelheid en kostenbeheersing. Bij het herontwerp van het energiesysteem (incl. IT, beheerssystemen en regelgeving) zou daarnaast een even grote aandacht moeten uitgaan naar het analyseren en meewegen en managen van risico's, evenals het eigenaarschap van de systemen en verantwoordelijkheid voor de security.

6 Referenties

Afspraken voor Elektriciteit. (2021, februari 8). Opgehaald van Klimaatakkoord: https://www.klimaatakkoord.nl/elektriciteit

Analistennetwerk Nationale Veiligheid. (2014). *Nationale Risicobeoordeling 6.*

Analistennetwerk Nationale Veiligheid. (2016). *Themarapportage Verstoring Vitale Infrastructuur.*

Analistennetwerk Nationale Veiligheid. (2019). *Verkenning risico's van de Energietransitie voor de nationale Veiligheid.*

Berenschot. (2018). *Richting 2050: systeemkeuzes en afhankelijkheden in de energietransitie.*

CE Delft. (2017). *Net voor de Toekomst.* Opgehaald van https://www.ce.nl/publicaties/download/2416

DNV-GL. (2020). *North Sea Energy outlook.* Opgehaald van https://www.dnvgl.com/publications/north-sea-energy-outlook-192287

DNV-GL. (2020). *Taskforce Infrastructuur Klimaatakkoord Industrie - Meerjaranprogramma Infrastructuur Energie en Klimaat.* Opgeroepen op 2020, van https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/04/15/bijlage-rapport-taskforce-infrastructuur-klimaatakkoord-industrie/bijlage-rapport-taskforce-infrastructuur-klimaatakkoord-industrie.pdf

Energeia. (2020, 11 17). Tennet vreest dat Duitsland als aandeelhouder te dikke vinger in de pap wil hebben. *Energeia*. Opgehaald van https://energeia.nl/energeia-artikel/40090602/tennet-vreest-dat-duitsland-als-aandeelhouder-te-dikke-vinger-in-de-pap-wil-hebben

Energy expert Cyber Security Platform. (2017). *Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.* Opgehaald van https://ec.europa.eu/energy/sites/default/files/documents/eecsp_report_final.pdf

ESIG. (2020). *Grid Reliability Under High Levels of Renewables: Rethinking Protection and Control.* Opgehaald van https://www.esig.energy/wp-content/uploads/2020/06/Grid-Reliability-Under-High-Levels-of-Renewables-Rethinking-Protection-and-Control.pdf

ETIP SNET. (2018). *Digitalization of the Electricity System and Customer Participation" description and recommendations of Technologies, Use Cases and Cybersecurity.* Opgehaald van https://www.etip-snet.eu/wp-content/uploads/2018/10/ETIP-SNET-Position-Paper-on-Digitalisation-FINAL-1.pdf

ETIP SNET. (2018). *Vision 2050, Integrating Smart Networks for the Energy Transition, Serving Society and Protecting the Environment.* Opgehaald van https://www.etip-snet.eu/wp-content/uploads/2018/06/VISION2050-DIGITALupdated.pdf

European Commission. (2021, februari 8). *Security of electricity supply*. Opgehaald van European Commission: https://ec.europa.eu/energy/topics/energy-security/security-electricity-supply_en#:~:text=%20Security%20of%20electricity%20supply%20%201%20Network,a%20forum%20for%20the%20exchange%20of...%20More

Europees Parlement & Raad van de Europese Unie. (2019). Verordening (EU) 2019/941 van het Europees Parlement en de Raaad van 5 juni 2019 betreffende risicoparaatheid in de elektriciteitssector en tot intrekking van Richtlijn 2005/89/EG. *Publicatieblad van de Europese Unie*. Opgehaald van https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0941&from=EN

Frank Fransen, R. W. (2017). *Security for smart Electricity Grids.* TNO. Opgehaald van https://segrid.eu/wp-content/uploads/2017/07/Whitepaper-SEGRID.pdf

IEA. (2020). *Power systems in transition, Challenges and opportunities ahead for energy security.* Opgehaald van https://www.iea.org/reports/power-systems-in-transition#

IEA task 25. (2020). *Factsheet Wind and Solar Integration Issues.* IEA. Opgehaald van https://community.ieawind.org/task25/integration

Instituut Clingendael. (2019). *Horizonscan Nationale Veiligheid 2019.* RIVM, Analistenetwerk Nationale Veiligheid 2019.

Klimaat- en Energieverkenning 2019. (2019). *Planbureau voor de Leefomgeving.*

Klimaatakkoord.nl. (2020, november 12). *Webinar 'Spanning op de netten'*. Opgehaald van Klimaatakkoord: https://www.klimaatakkoord.nl/actueel/nieuws/2020/11/12/webinar-%E2%80%98spanning-op-de-netten%E2%80%99

National grid ESO. (2019). *Technical Report on the events of 9 August 2019.* Opgehaald van https://www.nationalgrideso.com/document/152346/download

NCTV. (2017). *Weerbare Vitale Infrastructuur - Factsheet .*

NCTV. (2019). *Nationale Veiligheid Strategie.* NCTV. Opgehaald van https://www.nctv.nl/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019

NCTV. (2020). *Cybersecuritybeeld Nederland 2020.* Min. van Justitie; NCTV.

Nederlands Instituut Fysiek Veiligheid Nibra et.al. (2008). *Stroomuitval in de Bommeler- en Tielerwaard in december 2007.* Arnhem: Nederlands Instituut Fysiek Veiligheid Nibra.

Netbeheer Nederland. (2019). *Factsheet opschaalbare oplossingen voor Transportschaarste.* Opgehaald van https://www.netbeheernederland.nl/_upload/Files/Netcapaciteit_60_a7ae27bf52.pdf

Netbeheer Nederland. (2019). *Integrale Infrastructuur verkenning 2030-2050.* Opgehaald van https://www.netbeheernederland.nl/_upload/Files/Toekomstscenario%27s_64_5c3eab73b6.pdf

Netbeheer Nederland. (2020, september). Factsheet: opschaalbare oplossingen voor transportschade. Opgehaald van https://www.netbeheernederland.nl/_upload/Files/Netcapaciteit_60_a7ae27bf52.pdf

NVDE. (2017). *Position paper flexibiliteit.*

PBL. (2015). *Aanpassen aan klimaatverandering, kwetsbaarheden zien, kansen grijpen.*

RLI. (2018). *Stroomvoorziening onder Digitale Spanning.* Opgehaald van https://www.rli.nl/sites/default/files/stroomvoorziening_onder_digitale_spanning_rli_advies.pdf

Rüberg, S. (2016). *MIGRATE - D1.1 - Report on systemic issues.* Opgehaald van https://www.h2020-

migrate.eu/_Resources/Persistent/9bf78fc978e534f6393afb1f8510db86e56a1177/MIGRATE_D1.1_final_TenneT.pdf

Smulders, S. (2018). Kan en zal de wereld het klimaat redden door geo-engineering? *ESB*. Opgehaald van https://esb.nu/kvs/20047494/kan-en-zal-de-wereld-het-klimaat-redden-door-geo-engineering

Technolution in opdracht van TKI Top Sector Energie. (2019). *Research recommendations cyber security for offshore wind energie.* TKI Wind op Zee.

Tennet. (2015, juni 12). Toelichting onderzoek uitval 380 kV station Diemen. Opgehaald van https://www.tennet.eu/nl/nieuws/nieuws/toelichting-onderzoek-uitval-380-kv-station-diemen/

TenneT. (2017). *KDC 2017.* Opgehaald van https://www.tennet.eu/fileadmin/user_upload/Company/Publications/Technical_Publications/Dutch/TenneT_KCD2017_samenvatting.pdf

TNO. (2015). *NVP Themarapport Uitwerking verstoring energievoorziening.*

TNO. (2020). *Scenario's voor Klimaatneutraal Energiesysteem.* Opgeroepen op 2020, van http://publications.tno.nl/publication/34636594/KRZna2/TNO-2020-scenario.pdf

TNO. (2020). *Verkenning instrumentatie voor industriële elektrificatie.* Opgehaald van http://publications.tno.nl/publication/34637520/GMXtCg/TNO-2020-P11648.pdf

UL. (2019, januari 17). Cybersecurity for Windfarms. Opgehaald van https://www.ul.com/news/cybersecurity-windfarms

Union for the co-ordination of transmission of electricity (UTCE). (2007). *Final Report System disturbance on 4 November 2006.* UTCE.

Verband der Industriellen Energie- & Kraftwirtschaft. (2021, januari 11). Versorgungssicherheit der Industrie in Europa ist gefährdet. Opgehaald van https://www.vik.de/news-und-presse/pressemitteilungen/versorgungssicherheit-der-industrie-in-europa-ist-gefaehrdet/

Wiebes, E. (2020, oktober 16). Kabinetsreactie op het advies van de Taskforce Infrastructuur Klimaatakkoord Industrie (TIKI). *Kamerbrief*. Ministerie van Economische Zaken en Klimaat.

7 Ondertekening

Petten, <datum>	TNO
M.H. Langelaar Research Manager Wind Energy	
	E.J. Wiggelinkhuizen
B.H. Bulder A.B. Schwedersky	
	M.P.W. van Berlo
Afdelingshoofd	Auteur

A Enquête

Onderstaande tekst geeft de inhoudelijke toelichting en vragen weer van de enquête die onder externe experts is gehouden. Deze enquête heeft slechts een beperkt aantal reacties opgeleverd, die echter de reeds bestaande inzichten en ook elkaar goed aanvullen. Deze reacties komen van diverse specialisten, zie onder Algemene vragen:

Deel 1: Algemene vragen

Vraag 1: Omschrijf uw organisatie, functie en expertise of achtergrond

- OT security bij een DSO, specialist Information Security Management Systems, HV stations, control centers incl. responsible personnel;
- Vitaal, Cybersecurity, Data, Hoogwaterbescherming, specialist veiligheid/beveiliging (drink)watersystemen, beleidskennis cybersecurity
- Strategisch analist bij een utility, specialisme Europese elektriciteitsmarkt
- Utility, Digital Business Partner BA Wind Digitalisation portfolio + Project Manager Business Area Wind ISMS implementation

Deel 2: Tijdsbeeld 2030 en 2040

Eerst schetsen wij kort de achtergrond van de energietransitie, digitalisering en IoT. Vervolgens ziet u de (voor de vragenlijst mogelijk relevante) tijdsbeelden voor 2030 en 2040 en vragen wij u deze te controleren, en waar nodig aan te vullen en te concretiseren.

Energietransitie
Voor het behalen van de doestellingen van het klimaatverdrag van Parijs, heeft Nederland in 2019 een Klimaatakkoord afgesloten met daarin concrete maatregelen voor 49 procent reductie van de CO2 uitstoot in 2030 vergeleken met 1990. Hierdoor wordt een sterke groei van duurzame energie opwekking verwacht, met name van zon-PV en wind op zee. Ook de energievraag moet worden vergroend, zowel direct (bijv via elektrisch verwarmen en elektrisch vervoer), als indirect via groene brandstoffen en op termijn grondstoffen (bijv vervanging van aardolie in de petrochemie). Dit vereist snelle en sterke uitbreidingen en versterkingen van het transmissienet en de distributienetten. Deze netontwikkelingen zijn over het algemeen kostbaar met lange doorlooptijden, wat een beperkende factor is voor het tempo van deze transitie.

Om de wisselende elektriciteitsproductie van zon en wind en de elektriciteitsvraag in balans te houden is extra flexibiliteit nodig. Dit betreft zowel de aanbodkant (bijv. reservecapaciteit en -vermogen op korte-termijn markten), als de netten (bijv. interconnecties, regeling voor congestiemanagement en energieconversie en -opslag), en de vraagkant (bijv. slim laden). Om deze maatregelen op voldoende schaalgrootte en kosteneffectief te kunnen inzetten zijn zowel technologieontwikkeling als aanpassingen van de regelgeving noodzakelijk.

Digitalisering en IoT

De genoemde ontwikkelingen in het energie domein hangen sterk samen met die in het IT domein. Zo is de bedrijfsvoering van zon-PV en windparken (aanbodvoorspelling, regeling en beveiliging) volledig geautomatiseerd. Ook in de elektriciteitsnetten is verdere automatisering van belang, door de steeds hogere en sterker wisselende bezettingsgraad. Daarnaast vindt ook meer en snellere uitwisseling van elektriciteit tussen Europese landen plaats. Deze ontwikkelingen vereisen meer en snellere uitwisseling van informatie waarop ook sneller moet worden geacteerd, bijvoorbeeld in geval van dreigende overbelasting of onbalans. Automatisering van netten is daarbij ook een middel om operationele kosten te kunnen besparen. Ook aan de vraagzijde neemt automatisering gestaag toe door vraagsturing en lokale elektriciteitsproductie en opslag.

Een van de vele complicerende factoren daarbij is dat veel nieuwe aangesloten partijen actief zijn die autonoom kunnen acteren. Daarnaast kost de modernisering van netten (m.n. distributienetten) veel tijd en geld, waardoor nieuwe en oude systemen voor lange tijd naast elkaar operationeel zijn.

Met de modernisering van het elektriciteitssysteem worden grote aantallen apparaten met elkaar verbonden via het Internet (IoT). Het betreft hier zowel grote installaties als HVDC onderstations van TenneT, als middelgrote vermogens-elektronische omzetters voor de netkoppeling van windturbines, zon-PV en EV, alsook een grote hoeveelheid kleine consumentenapparatuur.

Deze ontwikkelingen kunnen leiden tot de op de volgende pagina geschetste beelden in 2030 en 2040.

Tijdsbeeld 2030

- De elektriciteitsopwekking in 2030 bestaat voor 70% uit duurzame bronnen, waarvan het merendeel een weersafhankelijk productieprofiel heeft.
- Tijdens periodes met een hoog wind en zon aanbod en een beperkte vraag worden deze parken uitgeschakeld vanwege de te lage (negatieve) marktprijs.
- Tijdens de koude wintermaanden blijft Nederland nog sterk afhankelijk van de import van gas en elektriciteit.
- Het transportnetwerk wordt continu uitgebreid, zowel het (offshore) transportnet als de distributienetten. Deze uitbreidingen bepalen het tempo waarin nieuwe opwekkers en verbruikers kunnen worden aangesloten. Deze uitbreidingen worden voor het merendeel gefinancierd vanuit de internationale kapitaalmarkt.
- Alle activiteiten van TenneT in Nederland worden in dit 2030 toekomstbeeld aangestuurd vanuit het hoofdkantoor in Bayreuth in Duitsland.
- Distributienetten zijn in de regel aangelegd met voldoende overcapaciteit om in geval van onderhoud of storing netcongestie te voorkomen. De aanvraag van aansluitingen voor nieuwe installaties zoals zon-PV en EV-snelladers gebeurt veelal niet tijdig om voldoende netuitbreiding te kunnen realiseren. Dit leidt in veel gevallen tot vertragingen en hoge investeringen. Om toch in de grote vraag naar aansluitcapaciteit te kunnen voorzien worden nieuwe distributienetten met minder redundantie ontworpen en worden bestaande netten in hoge mate belast, waardoor ook de redundantie afneemt.

- Op het HVDC Noordzeenet is ca. 50GW aan offshore windparken aangesloten en er is maximaal 25GW Interconnectie-capaciteit beschikbaar (wanneer alle windparken uit zouden staan). Dit net wordt bedreven door een NW-Europese Independent System Operator voor zowel elektriciteit als gas.
- Vervoer en verwarming zijn grotendeels geëlektrificeerd en deels gevoed uit groene waterstof.
- Alle nieuwe auto's zijn in staat om slim te laden, daarbij centraal aangestuurd door een aggregator die acteert op de stroommarkten.
- Door middel van lokale opslag op huishoud- en wijkniveau worden pieken in de opwekking (zon-PV) en vraag verminderd, waardoor netcongestie afneemt. Gedurende zomerse dagen worden echter veel PV installaties door de netbeheerder nog terug-geregeld om overbelasting in het net te voorkomen.

Tijdsbeeld 2040

- De geïnstalleerde capaciteit aan zon en wind is tweemaal hoger dan de piekvraag, waarbij de helft van de productie wordt omgezet in, en opgeslagen als, groene waterstof of warmte.
- Naast de groei van 2GW per jaar aan offshore wind is de vervangingsvraag van vergelijkbare omvang.
- De nog resterende conventionele piekcentrales zijn omgebouwd op waterstof, maar leveren onvoldoende vermogen tijdens vraagpieken in de winter bij een laag aanbod van zon en wind.
- Een deel van de hoofdstations en de industrie wordt uit de kuststreek geëvacueerd naar Oost-Nederland vanwege de reële kans op overstromingen.
- In de distributienetten en het transmissienet is een groot aantal batterijen operationeel, elk >100MWh/100MW, voor het balanceren van vraag en aanbod op tijdschalen van enkele seconden tot ca.1 uur, aangevuld met eenzelfde omvang aan brandstofcellen voor back-up vermogen op langere tijdschalen.
- Ondanks deze grootschalige energieopslag ontstaan in de wintermaanden tekorten, waardoor enkele grootverbruikers langere tijd worden afgeschakeld.
- Alle grootverbruikers en ook de helft van alle huishoudens zijn via het internet gekoppeld, zodat deze autonoom reageren op marktprijzen. Daarnaast is de helft van alle huishoudens energieneutraal.
- In distributie-onderstations worden op grote schaal batterijen ingezet voor het opvangen van vermogenspieken;
- In nieuwe wijken en industriegebieden worden standaard gelijkstroom-netwerken aangelegd die bij uitval van het openbare net nog enkele uren kunnen opereren.
- Op transmissieniveau moeten maatregelen worden getroffen om de sterkere frequentieschommelingen in het net van de laatste jaren te beperken.
- De beveiliging van distributienetten wordt momenteel aangepast naar een elektronische beveiliging, rekening houdend met lagere kortsluitstromen.

Vraag 2.1: Zijn er ontwikkelingen niet genoemd, die hier wel genoemd hadden moeten worden?

Vraag 2.2: Mist u bepaalde elementen, of zijn er nuances nodig, in de tijdsbeelden 2030/2040?

Vraag 2.3: Welk van de genoemde ontwikkelingen zijn het meest relevant voor uw organisatie in 2030-2040 en waarom?

Deel 3: Risico's elektriciteitsnet

Hier worden enkele risico's genoemd, behorend bij de beschreven ontwikkelingen. Deze zijn gegroepeerd in vier categorieën: systeemfalen, natuurlijke oorzaken, menselijk falen, en opzettelijk handelen. Lees deze door en geef aan welke het meest belangrijk zijn volgens u en waarom. Een inventarisatie met risico's is zelden compleet, zeker als we 10 tot 20 jaar vooruit kijken. Daarom vragen wij u ook om aanvullingen te doen waar dat kan.

Systeemfalen

- Onbalans t.g.v. uitval van opwerkeenheden (evt. import via Interconnector) of foutieve aanbodvoorspelling.
- Snelle schommelingen van de frequentie t.g.v. de verminderde roterende massa in het net.
- Gelijktijdig aan- en afschakelen van verbruikers die geautomatiseerd reageren op de variërende marktprijs (bijv. elektrisch vervoer, WKKs).
- Lokale verstoring van de netspanning in distributienetten door snel wisselende opwekking (bijv. zon-PV).
- Spanningsdip door kortsluiting, waarvan de omvang en duur worden vergroot t.g.v. onvoldoende kortsluitvermogen.
- Netvervuiling door onbedoelde interacties tussen vermogens-elektronische omzetters (met het net of onderling).
- Congestie in distributienet door decentrale opwekking waardoor curtailment noodzakelijk is.
- Overbelasting van het transmissienet in NL of buurlanden waardoor het net deels moet worden afgeschakeld.
- Uitval van communicatie met geautomatiseerde opwekkers, onderstations of verbruikers.

Natuurlijke oorzaken

- Uitval van ICT en vermogens-elektronische omzetters t.g.v. een zonnestorm (natuurlijke/technische oorzaak).
- Extreem hoge windsnelheden, die deels onverwacht optreden, zowel qua sterkte als timing: hierdoor kan een windpark tijdelijk uit bedrijf gaan.
- Tijdens een koude en windstille periode moet elektriciteit tegen hoge prijzen worden geïmporteerd en moeten in de randstad enkele grootverbruikers afschakelen om overbelasting van Interconnectoren te voorkomen.
- Door een extreme storm raakt een schip op drift in een windpark, waardoor wind turbines worden beschadigd en mogelijk ook het TenneT onderstation; het slepende anker beschadigt een deel van de kabels in het windpark.
- Door slecht weer komt een crew vessel of heli in een windpark in problemen.

Menselijk falen

- Ontwerpfout in de besturingssoftware van IoT consumenten apparatuur waardoor deze ongecontroleerd aan- en afschakelen.
- Bug in software update van windturbines waardoor deze tegelijkertijd afschakelen, bijv. bij afwijkingen in de netfrequentie.

- Een 2GW onderzeese elektriciteitskabel (Interconnector en/of verbinding naar een windpark) raakt defect door een scheepsanker dat niet is gelicht of op een verkeerde locatie is neergelaten.
- Onvoldoende reservevermogen ingekocht als voorziening bij uitval of onderhoud met als gevolg extreem hoog oplopende marktprijzen.
- Optimistische inschatting van kosten en doorlooptijd netuitbreiding, die bijv. kunnen leiden tot vertraging aansluiting van windparken.
- Door politieke druk om meer duurzame energie aan te sluiten wordt een deel van de benodigde (N-1) reserve transportcapaciteit bezet.

Opzettelijk handelen

- Fysieke toegang van kwaadwillenden tot een offshore windpark, waardoor de besturing kan worden overgenomen, (met uitval van het windpark en/of verstoring van de netstabiliteit), of sabotage kan worden gepleegd (met langdurige schade aan windturbines, het offshore onderstation en onderzeese kabels).
- Een fysieke of cyber aanval op control centers van netbeheerders waarop de centrale aansturing draait, waardoor de levering van elektriciteit uitvalt.
- Het hacken van het systeem van een offshore windpark operator waardoor de besturing kan worden overgenomen, geblokkeerd of gevoelige data kan worden verkregen.
- Cyberaanval op het systeem van een netbeheerder waardoor de besturing van onderstations kan worden verstoord.
- Cyberaanval op systeem van grote vloot laadpalen waardoor deze tegelijkertijd aan- of afschakelen, waardoor de spanningsregeling in het betreffende distributienetten instabiel raakt, met afschakeling tot gevolg.
- Cyberaanval op slecht beveiligde (IoT) consumentenapparatuur waardoor deze onbruikbaar worden of data kan worden gelekt.
- Cyberaanval op smart meters of onderliggende systemen waardoor verbruiksdata kan worden ingezien en gemanipuleerd, waardoor illegaal en ongemerkt stroom kan worden getapt, of mogelijk verbruikers kunnen worden afgesloten.
- Beïnvloeding van besluitvorming t.a.v. uitbreiding, modernisering, vergroening van het elektriciteitssysteem, bijv. vanuit buitenlandse politiek of aandeelhouders.

Vraag 3.1: Ziet u belangrijke risico's die nog niet zijn benoemd?

Vraag 3.2: Welk van de genoemde risico's vind u het meest relevant? Waarom?

Vraag 3.3: Welke risico's zijn het meest relevant voor (de ontwikkeling van) uw organisatie?

Deel 4: Impact

Hier volgen drie scenariobeschrijvingen. Lees deze door en geef daarbij aan hoe u de impact van een dergelijk incident zou beleven in 2030/2040. Waar zou dit een doorwerking op kunnen hebben, zijn er cascade-effecten die hier van toepassing

zijn? En zijn er in uw organisatie of werkveld mogelijk ontwikkelingen die hier aan raken?

Scenario 1 : Menselijk falen
In 2030 is 11.5 GW offshore windcapaciteit operationeel. Het grootste windpark IJmuiden Ver 2 x 2000MW bestaat uit windturbines van eenzelfde type, centraal aangestuurd vanuit een control center. Een recent geïmplementeerde update van de windturbine regeling is op een enkele windturbine succesvol getest. Echter, door onbedoelde interacties met het HVDC offshore station valt het lokale offshore windparknet uit en lukt het niet om deze weer op te starten. De vermoedelijke oorzaak wordt gemeld aan de netbeheerder die een onderzoek instelt naar mogelijke schade aan apparatuur en naar de oorzaak van de uitval. De software update wordt teruggedraaid en na een week wordt het offshore wind stapsgewijs weer opgestart.

Dit heeft tot gevolg:
- Uitval van service: door een groot windaanbod ten tijde van de uitval ontstaat er acute onbalans in het net, waardoor grootverbruikers worden afgeschakeld en een deel van het net uitvalt.
- Economische schade: inkoop van extra opwekcapaciteit/vermogen, schadeclaims.
- Imagoschade: voor de windturbine fabrikant.

Vraag 4.1: Welke impact heeft dit scenario in 2030-2040, hoe zou u of uw organisatie dat beleven en zijn er cascade-effecten van toepassing? En zijn er in uw organisatie of werkveld mogelijk ontwikkelingen die hier aan raken?

Scenario 2: Doelbewust menselijk handelen
In 2030 is 11.5 GW offshore wind capaciteit operationeel, waarvan het merendeel bestaat uit grote gestandaardiseerde offshore onderstations (5 x 700MW HVAC en 2 x 2000MW HVDC). Door de beperkte fysieke beveiliging vindt sabotage plaats en kan het IT-systeem sneller worden gehackt, waardoor een groot deel van deze onderstations onklaar wordt gemaakt.

Gevolg is dat in korte tijd ca. 8000MW aan opwekcapaciteit wegvalt, wat leidt tot:
- Uitval van service: In geval van een groot windaanbod ten tijde van de uitval ontstaat acute onbalans in het net, waardoor grootverbruikers worden afgeschakeld en een deel van het net uitvalt.
- Economische schade: Langdurige tekorten, waardoor opwekcapaciteit moet worden gereserveerd en aangesproken.
- Economische schade: Schade aan onderstations met lange reparatietijden (1 week tot 1 maand, afhankelijk van besteltijd van apparatuur, mobilisatietijd van (kraan)schepen en personeel en weersomstandigheden)
- Imagoschade: Vanwege getoonde kwetsbaarheid van offshore energieopwekking en transport.

Vraag 4.2: Welke impact heeft dit scenario in 2030-2040, hoe zou u of uw organisatie dat beleven en zijn er cascade-effecten van toepassing? En zijn er in uw organisatie of werkveld mogelijk ontwikkelingen die hier aan raken?

Scenario 3: Doelbewust menselijk handelen
Beïnvloeding (manipuleren dan wel blokkeren) van de informatiestomen uit de markt en/of het real-time IoT sensornetwerk van de netbeheerders (Wide-Area Monitoring) door hackers vanuit statelijke actoren. Hierdoor wordt de balanshandhaving verstoord op Europese schaal. Cruciale verbindingen tussen Noordwest Europa en Zuid Europa vallen uit door overbelasting, waardoor deze deelnetten van elkaar losraken.

Gevolg is dat in korte tijd ca. 8000MW aan opwekcapaciteit wegvalt, wat leidt tot:
- Blackout in Nederland en meerdere buurlanden met lange hersteltijd voor het synchroniseren van de netten tussen Noordwest en Zuid-Europa
- Economische schade: tekorten, waardoor opwekcapaciteit moet worden gereserveerd en aangesproken
- Lekken van gevoelige data
- Imagoschade vanwege getoonde kwetsbaarheid van netwerk operations

Vraag 4.3: Welke impact heeft dit scenario in 2030-2040, hoe zou u of uw organisatie dat beleven en zijn er cascade-effecten van toepassing? En zijn er in uw organisatie of werkveld mogelijk ontwikkelingen die hier aan raken?

B Overzicht NL elektriciteitsnetwerk, versimpelde structuur en afhankelijkheden