TOPSECTOR ENERGIE
Innovatie voor een duurzame toekomst

Netwerkevenement Topsector Energie Digitalisering

Verslagen ronde tafel sessies

22 september 2022

Inhoudsopgave

Sessie 1:
‘Ontwerpen referentiearchitectuur: een proces van de lange adem’

Een referentiearchitectuur voor Nederlandse energie-infrastructuur is één van de drie strategische thema’s op de digitaliseringsagenda van de Topsector Energie. De gedachte is dat het ontwerpen van een referentiearchitectuur de sector helpt om digitale innovaties eenvoudiger in het energiesysteem in te passen én maatschappelijke waarden zoals transparantie en toegankelijkheid beter te borgen. Maar hoe kom je tot zo’n referentiearchitectuur?

Deze vraag stond centraal aan ronde tafel 1. Onder leiding van moderator Harold Veldkamp (Topsector Energie) en expert Marcel Volkerts (directeur Baringa Partners) zochten de deelnemers naar een antwoord. Adviesbureau Baringa onderzocht van februari tot oktober 2022 in opdracht van RVO – voor het programma digitalisering van de Topsector Energie - hoe in Nederland een referentiearchitectuur ontwikkeld en toegepast kan worden - voor alle energievormen. Van elektriciteit tot warmte, en van ‘achter de meter’ tot ‘voorbij de centrale’.

Volkerts: “Komen tot een referentiearchitectuur is een proces van de lange adem. En je moet het samen doen. De vraag is: hoe? Wil je eerst de diepte in, of eerst de breedte in? Ga je zoeken naar witte vlekken, met het risico dat je het grotere plaatje uit het oog verliest? Of ga je eerst zoveel mogelijk problemen oplossen?” Beide extremen kunnen tot een lappendeken van deeloplossingen leiden, stelde Volkerts. “En dat is precies wat we niet willen. Hoe voorkomen we dat?”

Tijdens de rondetafelgesprekken dachten de deelnemers steeds in twee- of drietallen na over deze vraag. Iedereen herkende en erkende de noodzaak tot het ontwikkelen van een referentiearchitectuur. Over de uitdagingen die daarbij horen kwamen zij met de volgende ideeën en adviezen:

- Benoem het doel van de referentiearchitectuur en stel kaders, om zo de opgave in behapbare stukken op te delen.
- Gebruik een Agile-benadering en stel iteratief je doel en scope bij.
- Hergebruik waar mogelijk bestaande referentiearchitecturen. Er is al veel ontwikkeld, in Nederland en daarbuiten.
- Identificeer het ‘laaghangend fruit’ en ontwikkel als eerste de use cases waar nu behoefte aan is. Bijvoorbeeld voor slim laden. Dergelijke use cases laten ook zien dat de referentiearchitectuur niet los ontwikkeld kan worden van de andere twee strategische thema’s van het netwerkevent: cybersecurity en data governance;
- Een succesvolle referentiearchitectuur is van ons allemaal en vervult de behoeften van de hele sector en zijn stakeholders. Het betrekken van een brede community bij de ontwikkeling is daarom cruciaal.
- Vier je successen!

Sessie 2:
‘Spraakverwarring bij ontwikkelen referentiearchitectuur lastig te voorkomen’

Het ontwerpen van een referentiearchitectuur voor Nederlandse energie-infrastructuur is één van de drie strategische thema’s op de digitaliseringsagenda van de Topsector Energie. De gedachte is dat het ontwerpen van een referentiearchitectuur de sector helpt om digitale innovaties eenvoudiger in het energiesysteem in te passen én maatschappelijke waarden zoals transparantie en toegankelijkheid beter te borgen. Maar hoe zorg je dat alle partijen bij het ontwikkelen van zo’n referentiearchitectuur dezelfde ‘taal’ spreken?

Deze vraag stond centraal aan ronde tafel 2. Onder leiding van moderator Claire Groosman (RVO) en expert Jop Spoelstra (innovatiemanager bij Technolution) zochten de deelnemers naar antwoorden op deze vraag. In een inleiding gaf Spoelstra aan dat, als het gaat om het ontwikkelen van een breed gedragen architectuur in de energiesector, er regelmatig spraakverwarringen ontstaan.

“Dat komt door de grote diversiteit van het domein, waarin allerlei partijen met een eigen achtergrond, problematiek, scope en tijdshorizon kijken naar bruikbare en functionele architecturen”, aldus Spoelstra. “Soms lijken partijen op zoek naar een antwoord op dezelfde vraag, terwijl de benodigde technische en functionele architectuur die zij nodig hebben bijna niet overeenkomt”, zegt hij. Het is daarom erg belangrijk om vooraf goed af te stemmen hoe we voorkomen dat partijen langs elkaar heen praten, aldus Spoelstra.

Een belangrijk inzicht aan deze ronde tafel was, dat je een ‘spraakverwarring’ waarschijnlijk niet kunt voorkomen. Daarvoor is de energiesector te onoverzichtelijk en te dynamisch. En zijn er te veel subsystemen. Wel kan het helpen om tijdens iedere stap van het ontwikkeltraject eerst samen duidelijke doelen en kaders te formuleren. Tussentijds kun je dan steeds valideren of iedereen nog aan de gezamenlijke uitdagingen en waarden werkt, binnen de geformuleerde doelen en kaders. Nauw contact tussen de betrokken partijen is nodig, zodat steeds sprake is van feedback op het ontwikkelproces.

Ook werd geopperd dat het kan helpen om gewoon aan de slag te gaan en te laten zien wat je ontwikkeld hebt, via proeven. Zoals dat al gebeurt binnen USEF (het Universal Smart Energy Framework), een Nederlands initiatief gericht op smart energy technologies.

Algemene conclusie aan deze ronde tafel was dat bij het ontwikkelen van een referentiearchitectuur spraakverwarringen niet volledig voorkomen kunnen worden. Wel kan het helpen om duidelijke kaders af te bakenen waarbinnen het ontwikkelproces plaatsvindt. Daardoor wordt de waaier waarbinnen miscommunicatie kan ontstaan kleiner. Hierbij kunnen handvatten als NEN-normen, data-architecturen en het helder omschrijven van doelen en functies, partijen, middelen en scenario’s, systeemelementen en bijbehorende architecturen aanzet zijn tot het spreken van een ‘gemeenschappelijke taal’.

Sessie 3:
‘Sector moet verantwoordelijkheid nemen voor tekort aan cybersecurity-specialisten’

Hoe kunnen we het tekort aan operational technology (OT) cybersecurity-specialisten oplossen? Deze vraag stond centraal aan ronde tafel 3. Onder leiding van moderator Maaike Drok (Topsector Energie) en expert Anjos Nijk (directeur van het European Network for Cybersecurity) zochten de deelnemers naar antwoorden op deze vraag. Volgens Nijk neemt in onze energienetten het aanvalsoppervlak voor hackers enorm toe, door integratie van nieuwe systemen en technologieën. Ook ziet hij een toenemende aanvalsdreiging door geopolitieke ontwikkelingen.

Tegelijkertijd constateert hij dat netbeheerders en hun stakeholders grote moeite hebben met het vervullen van vacatures die te maken hebben met de energietransitie. Nijk: “Dit geldt voor technische functies in het algemeen, voor cybersecurity-specialisten in het bijzonder en het meest voor OT-cybersecurity-specialisten.” Deze laatste categorie is broodnodig om de ‘weerbaarheid’ van onze energienetten te vergroten, zegt hij. Dit vraagt om specialisten met de juiste kennis en middelen, die weten wat hen te doen staat, stelt Nijk. Maar waar vinden we die specialisten?

Tijdens twee rondetafelgesprekken gaven de deelnemers aan dat het eerst zaak is om in kaart te brengen hoe groot dit probleem is. Wat is het aantal vacatures, op welke niveaus en functies en welke vaardigheden zijn nodig? Ook werd vastgesteld dat cybersecurity relevant is voor alle bedrijfsonderdelen. Welke kennishiaten zijn er per onderdeel? Daarna kan opleiden intern en extern gebeuren. Voor interne opleiding is awareness in alle lagen van de organisatie nodig. Ook moet er een duidelijk carrièrepad geschetst worden voor specialisten die geïnteresseerd zijn in om- of bijscholing.

Lukt het intern niet om specialisten te vinden of te werven, dan kun je extern mensen met specifieke skills gaan zoeken. Hiervoor is het belangrijk om deze functies aantrekkelijk te maken, bijvoorbeeld via incentives. Verder is het noodzakelijk om voor de verschillende domeinen en functies de opleidingsbehoefte vast te stellen. Er is op allerlei niveaus behoefte aan expertise die er onvoldoende is én die up-to-date moet blijven. Dat kun je borgen door een structureel opleidings- én trainingsprogramma in te richten.

Zo’n opleidingsprogramma kun je inrichten via een samenwerkingsverband of bij een instituut. Daarnaast moeten de curricula van relevante mbo- en hbo-opleidingen voldoende aandacht besteden aan cybersecurity. Om de installed base binnen de sector mee te krijgen, is positionering en eigenaarschap van dit probleem belangrijk, gaven deelnemers aan. De energiesector heeft weliswaar een cultuur van cybersecurity-denken ingezet, maar moet nu ook verantwoordelijkheid gaan nemen voor de acties die hieruit volgen. In de samenwerking tussen partijen kan het helpen om een soort NAVO-principe af te spreken: een aanval op één is een aanval op allen.

Sessie 4: ‘Afsprakenstelsel nodig voor gebruik hard- en software in de energiesector’

Heeft de energiesector een afsprakenstelsel nodig voor het gebruik van hard- en software? Deze vraag stond centraal aan ronde tafel 4. Onder leiding van moderator Leon van der Palen (RVO) en expert Rick van der Kleij (cybersecurity-onderzoeker bij TNO) zochten de deelnemers naar een antwoord.

In zijn inleiding gaf Van der Kleij aan dat veel systemen in de energiesector worden aangestuurd, gecontroleerd en/of onderhouden door informatietechnologie die door bijvoorbeeld virussen of hacks kan worden verstoord of lamgelegd. “Ook laadpalen en andere slimme apparaten bevatten informatietechnologie die beveiligd moet worden tegen hackers, zodat achterliggende systemen afgeschermd zijn”, zei hij.

Zijn stelling is dat een afsprakenstelsel nodig is voor minimale eisen van hard- en software en de werking ervan. Denk daarbij aan identificatie, authenticatie en autorisatie van datastromen. Van der Kleij: “Maar de vraag is: hoe maken we zo’n stelsel en wat staat erin? Hoe passen we de afspraken toe en borgen we ze gedurende de levenscyclus van systemen? En hoe zorgen we dat afspraken ook aandacht hebben voor de perspectieven van de (eind)gebruikers van systemen?”

In de eerste sessie splitste de groep zich in tweeën. De helft van de groep boog zich over Van der Kleijs stelling en constateerde dat zo’n afsprakenstelsel een moving target is. Het is nooit af en verdient continu aandacht en updates. Een afsprakenstelsel is dan een soort ‘requirements document’, waarbij iedere update zorgt voor verbeterde security op alle levels van je systemen. Dus niet alleen security by design, maar ook impermeability, performance, maintainability, diagnosability, resilience and usability by design.

De andere helft van de groep boog zich over de vraag hoe je voorkomt dat je door het borgen van security inboet op gebruikersvriendelijkheid. Vanuit deze groep kwam de suggestie om niet te veel effort te stoppen in security ‘achter de meter’. Daarmee accepteer je de onveiligheden in de systemen die consumenten zelf installeren en gebruiken. Echter, een inbreuk blijft dan beperkt tot de omgeving van een individuele consument.

Tijdens de tweede sessie voerden de deelnemers een centrale discussie over Van der Kleijs stelling. De groep concludeerde dat een afsprakenstelsel eraan bijdraagt dat consumenten erop kunnen vertrouwen dat zij apparaten en software in huis halen en installeren waarvan de veiligheid gewaarborgd is. Daarbij weegt mee dat niet alle consumenten voldoende kennis en vaardigheden hebben om de systemen die zij gebruiken goed te beveiligen. Met een afsprakenstelsel zijn zij ervan verzekerd dat systemen niet onveilig zijn.

Sessie 5:
‘Energietransitie vraagt om het weerbaar maken van het energiesysteem’

Het grootste risico op het gebied van cybersecurity in het energiedomein ligt bij consumenten. Deze stelling stond centraal aan ronde tafel 5. Onder leiding van expert Harm van den Brink (IT-architect Electric Vehicles bij ElaadNL) en moderator Soe van Dijk (Topsector Energie Digitalisering) zochten de deelnemers naar standpunten bij deze stelling.

Volgens Van den Brink is digitalisering een onmisbaar onderdeel van de energietransitie, maar groeien daarmee ook de veiligheidsrisico’s. “Er komt steeds meer decentrale opwek uit hernieuwbare energiebronnen, die minder goed stuurbaar zijn. Dat leidt tot het toevoegen van digitale componenten aan het energiesysteem, om vraag en antwoord beter op elkaar af te stemmen”, aldus Van den Brink. “Denk aan omvormers, slimme meters en sensoren die data generen.” De almaar toenemende digitalisering maakt het elektriciteitsnet niet alleen flexibeler, maar ook kwetsbaarder, stelt hij.

“Veel apparaten zijn verbonden met zowel het elektriciteitsnet als het internet. Dat maakt de energiesector in toenemende mate interessant voor cyberaanvallen. Een grootschalige aanval op consumentenapparaten met een relatief hoog vermogen, zoals laadpunten, warmtepompen, ovens en omvormers voor zonnepanelen, kan het elektriciteitsnet destabiliseren”, legde hij uit. Zijn vraag aan de deelnemers was hoe zij dit cybersecurity-risico zien en hoe dit veiliger kan. Wat kunnen we hierin van consumenten verwachten en wat moet hierover in wet- en regelgeving worden vastgelegd?

De deelnemers waren het erover eens dat het risico op cyberaanvallen bij consumenten groot is. Het ontbreekt hen vaak aan de kennis om apparaten goed te beveiligen. ‘Achter de voordeur’ ingrijpen is lastig en misschien ook onwenselijk? Wel is binnen de hele keten – inclusief de consument - een groeiend bewustzijn van de veiligheidsrisico’s nodig. Hierin heeft ook de overheid een rol. Als sector moet je ervan uitgaan dat de vijand al binnen is. Daarom gaat het erom dat je het stroomnet meer resilient (weerbaar) maakt.

Aan de andere kant werd ook de opmerking gemaakt dat een meer decentraal systeem juist weerbaarder is. Het ‘oude’ systeem heeft als het ware één ‘controlekamer’. Als dat gehackt wordt, ligt alles plat. In het nieuwe systeem ontstaan risico’s sneller aan de 'randen' van het energienetwerk, ook op de plekken waar energie opgewekt wordt. Netbeheerders krijgen in toenemende mate de uitdaging op daarop te kunnen sturen of ingrijpen.

Dit vraagt erom dat zij zich bewust zijn van de veiligheidsrisico’s op de niveaus boven de consument, gaven gespreksdeelnemers aan. Bijvoorbeeld bij laadpalen of clouddiensten. Voor de eigenaars en beheerders van zulke toepassingen kan de overheid eisen opstellen, zoals een meld- en zorgplicht bij cyberaanvallen. Verplicht daarnaast de certificering van apparaten, zodat

ze een basisveiligheid hebben. Regelgeving en certificering kun je bovendien Europees/internationaal aanpakken, want dit is niet uitsluitend een Nederlands probleem.

Sessie 6:
‘Bij delen van data moeten consumenten de regie hebben én houden’

Wat zijn best practices van data governance in het private domein en wat kunnen we daarmee in het perspectief van de energietransitie? Die vraag stond centraal aan ronde tafel 6. Onder leiding van moderator Rosalie Braakman (Topsector Energie) en expert Romy Dekker (Rathenau Instituut) zochten de deelnemers naar een antwoord op deze vraag.

Dekker is mede-auteur van het rapport ‘Stroom van Data’ dat het Rathenau Instituut eerder dit jaar publiceerde. Het rapport behandelt de vraag wat nodig is om data te kunnen benutten voor de energietransitie. Ze gaf aan: “In het rapport stellen wij dat partijen moeten verhelderen hoe datagebruik bijdraagt aan doelen van het energiebeleid, zoals duurzaamheid, betaalbaarheid, betrouwbaarheid, ruimtelijke inpasbaarheid en veiligheid. Ook moet datagebruik altijd plaatsvinden binnen de grenzen van publieke waarden als rechtvaardigheid, privacy en zeggenschap.”

Ze legde verder uit dat afspraken over data governance binnen de energiesector een blinde vlek hebben. “Ze gaan vooral over data van slimme meters, terwijl ook afspraken nodig zijn voor data uit bijvoorbeeld warmtepompen, omvormers van zonnepanelen of voor het realiseren van smart grids. Zo voorkomen we dat consumenten hun zeggenschap verliezen of dat lock-in-situaties ontstaan.”

De zoektocht naar goede voorbeelden van data governance leidde tot een interessant overzicht van apps, toepassingen en projecten op allerlei gebieden: mobiliteit, energiebeheer, smart grids, medische data, dataopslag en slimme gebouwen en steden. Geconcludeerd werd dat de data die in dergelijke toepassingen en projecten verzameld wordt, veelal in het private domein valt. En daarom buiten de juridische reikwijdte van de elektriciteitswet en toekomstige energiewet. Daarom is vaak niet duidelijk wat ermee kan, mag en wordt gedaan.

Een belangrijke gedeelde mening was dat consumenten altijd de keus moeten hebben welke data zij wel en niet willen delen. Ook moet duidelijk zijn wat er met hun data gebeurt. Dit vraagt om maatschappelijke verantwoordelijkheid: de consument moet de regie hebben én houden, maar er ook op kunnen vertrouwen dat er goed met hun data wordt omgegaan. Dat vertrouwen ontbreekt regelmatig, was een conclusie.

Het elektronisch patiëntendossier kwam op tafel als voorbeeld hiervan. Voor patiënten is niet duidelijk wie toegang heeft tot welke medische gegevens en patiënten hebben daar zelf geen zicht of grip op. Als tegenhanger werd telecom genoemd als voorbeeld van een sector waarin het delen van data nauwelijks als probleem wordt ervaren. Maar hoe komt dat? Is het framing, of zijn de directe en indirecte baten van het delen van data in de telecomsector duidelijker dan in andere sectoren?

Hoe de goede voorbeelden van het delen van data kunnen bijdragen aan de energietransitie, was niet in alle gevallen duidelijk. Wel is bij de meeste voorbeelden ruime aandacht voor privacy, veiligheid en zeggenschap. Op het gebied van data governance kan de energiesector hiervan leren. Een belangrijke vraag om hierin stappen te zetten is: hoe dan? Welke kennis over data (delen) is nog nodig?

Sessie 7:
‘Zicht op de waarde van data is cruciaal om data succesvol te delen’

Deze stelling stond centraal aan ronde tafel 7. Onder leiding van moderator Jade Tjiong (RVO) en expert Herman Pals (senior business consultant bij TNO) zochten de deelnemers naar standpunten bij deze stelling. Volgens Pals helpt het om te weten wat er in de praktijk speelt. “Dan kun je veel concreter stappen zetten in het organiseren van data governance.”

Het businessmodel van data governance wordt vaak vergeten, benoemde Pals. “Het is belangrijk om daarin te investeren. Niet dat data altijd gratis gedeeld moet worden. Maar bedrijven en consumenten weten niet altijd wat de waarde is van data”, zei hij.

In de eerste sessie aan deze tafel constateerden de deelnemers dat de waarde van data afhankelijk is van de kwaliteit ervan. Om de waarde van data te bepalen, is standaardisatie van de indicatoren/data nodig. Door te betalen voor data, verwacht je een bepaalde kwaliteit. Bijvoorbeeld service, of beschikbaarheid. Om de kwaliteit te waarborgen, zou het uitgangspunt moeten zijn dat data niet gratis is. Hierover is gesprek nodig tussen betrokken partijen: burgers, bedrijven en overheid. Vaak wordt deze discussie niet gevoerd, of te laat.

Tijdens de tweede sessie bespraken de deelnemers de (financiële) waarde, het delen en het eigenaarschap van data. De vraag kwam op tafel of data überhaupt waarde heeft. Of is het de dienst die je dankzij de data kunt aanbieden die waarde heeft? Geopperd werd dat in het energiesysteem van de toekomst energie wellicht gratis is, terwijl de waarde in de data zit. Om daar te komen moet je eerst inzichtelijk krijgen wat je als sector hebt qua datahuishouding. Daarbij mag het aspect AVG/GDPR niet vergeten worden. Want: wil de eigenaar bepaalde data delen of alleen inzage geven? En is het delen een eenmalige actie, of mag de andere partij het onbeperkt gebruiken? Deel je data voor een bepaalde dienst, dus als betaling, of niet?

En wie is de eigenaar van data? Zijn dat de dienstverleners of is het de consument? Dienstverleners zien data vaak als hun bezit, maar is dat zo? En hoever wil je gaan op het gebied van het gedwongen delen van data? Gebruik je de ‘stick motivation’ (dreigen met straf) waarbij je wettelijk afdwingt dat data gedeeld moet worden? Of kies je voor de effectievere ‘carrot motivation’ (gedrag belonen), waarbij de betrokken partijen samen kunnen bepalen hoe ze de ‘taart met elkaar willen verdelen’. Belangrijke conclusie was dat het bij het delen en gebruiken van data aankomt op het vertrouwen dat we een gezamenlijk doel hebben en dat er zorgvuldig met data omgegaan wordt.

Sessie 8:
‘Data goed bruikbaar om te sturen op directe besparing’

Wat is de rol van data binnen de sociale energietransitie? Die vraag stond centraal aan ronde tafel 8. Onder leiding van moderator Herma de Heer (RVO) en expert Michiel Sintenie (innovatiemanager Europa bij Vattenfall) zochten de deelnemers in kleinere groepjes naar een antwoord op deze vraag. Eén van de vragen die hierbij op tafel kwam is welke invloed consumenten kunnen hebben op hun verbruik. De conclusie was: met behulp van data kun je jouw gebruik beter voorspellen en bijsturen.

Inzicht in jouw (verbruiks)data helpt dus bij gedragsverandering. Maar dan moeten bedrijven data wel goed toegankelijk maken. Deelnemers stelden voor om data ook via bijvoorbeeld facturen te delen, in plaats van uitsluitend via apps. Bij de vraag wie eigenaar is – of moet zijn – van data, was de overeenstemming dat eigenaarschap bij de consument moet liggen. Burgers die niet gewend zijn aan dataverzameling moeten beschermd worden. Belangrijk is ook dat data ‘onafhankelijk’ is en het gebruik van data niet commercieel gedreven.

Volgens één van de groepen is kennis van je eigen data belangrijk in de sociale energietransitie. Zo kun je als consument besparen op jouw energiekosten én zelf een bijdrage leveren aan de CO^2-reductie. Bedrijven kunnen je hierin stimuleren door voordelen in de vorm van incentives aan te bieden. Een relevante vraag in deze groep was verder: waar moet data opgeslagen worden? Lokaal of centraal? En hoe zorg je ervoor dat tussenpersonen onafhankelijk zijn? Een andere groep vulde aan dat je het ophopen van data moet voorkomen en kwam met de vraag: hebben we behoefte aan zelflerende systemen? Anders gezegd, willen burgers zelf grip houden op hun data, of willen ze liever ontzorgd worden met analyses en adviezen over besparing?

Vastgesteld werd dat de rol van data in de energietransitie momenteel beperkt is. Consumenten hebben weinig zicht op hun data en inzicht in de waarde ervan. Zij gaan alleen iets doen met hun data als deze duidelijk en overzichtelijk is. Deze vaststelling leidde tot de opmerking dat betrouwbare energiecoaches consumenten kunnen helpen om hun data om te zetten naar concrete (besparings)acties. Ook educatieprogramma’s voor kinderen kunnen consumenten aanzetten tot ‘goed gedrag’.

De laatste groep sloot zich hierbij aan en stelde dat data goed bruikbaar is om te sturen op directe besparing. Geopperd werd dat het kunnen zien van je real time-verbruikskosten een goed idee kan zijn. Belangrijk is dat consumenten makkelijk kunnen zien hoe en waar besparing mogelijk is.