SmoothEMS
MET GRIDSHIELD

Whitepaper:
Robuuste integratie van IT in het elektriciteitsnet

Inleiding

Gedurende het SmoothEMS met GridShield-project heeft veel innovatie en onderzoek plaatsgevonden. Een terugkerend aspect hierbij is de noodzaak voor systeemintegratie. Dat ging niet altijd zonder slag of stoot, maar uiteindelijk slaagde het altijd wel.

Robuustheid in de praktijk

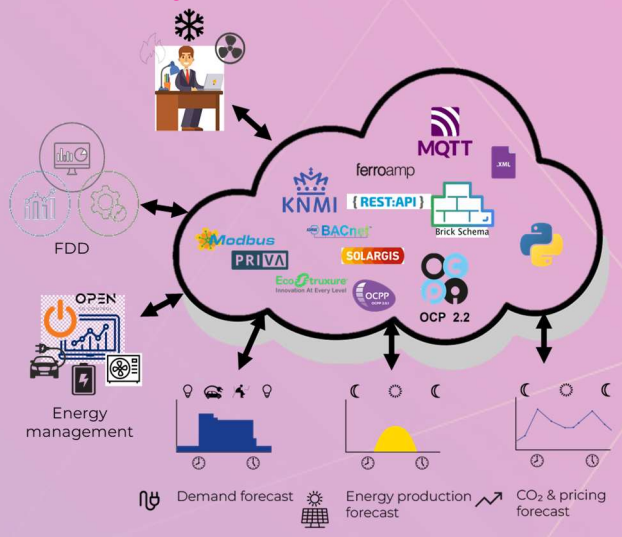
Voor een optimale energetische balans tussen vraag en aanbod is de integratie van systemen ''achter de meter'' essentieel. Daarnaast is centraal beheer van deze systemen noodzakelijk. Naast de koppeling van systemen moeten er maatregelen worden getroffen voor situaties waarin interne en externe systeemkoppelingen niet functioneren. Dit kan veroorzaakt worden door hardwarestoringen, externe software-updates, cyberaanvallen of connectiviteitsproblemen (zowel lokaal als in de cloud). Dit stelt hoge eisen aan de robuustheid van het systeem.

Systeemintegratie bij a.s.r. Utrecht

Open systeemkeuze:

Een belangrijk uitgangspunt is dat systemen en producten gekozen worden die compatibel zijn met 3rd-party-systemen voor monitoring en eventuele sturing. Een praktijkvoorbeeld hiervan is het ontmantelen van laadpalen op een projectlocatie, omdat deze niet via open standaarden gekoppeld konden worden.

Afhankelijkheden



- **Lokale verbindingen** met gebouwbeheersystemen (zoals Priva), onderstations en diverse protocollen zoals BACnet, Modbus TCP/IP, Serieel, MQTT en RESTful API's.
- **Externe verbindingen** voor weerdata (bijv. Solargis), laadsessies (OCPI/CPO) en vraag-aanboddata van het elektriciteitsnet, inclusief CO2- en prijs informatie(ENTSO-E).
- **Lokale of externe** verbindingen voor voorspelmodellen (48 uur vooruit) en anticiperende regelingen (zoals OpenToControl).

Voorbeelden uit de praktijk

Software updates laadinfrastructuur

Wanneer een leverancier FW updates uitvoert kan het zijn dat ook het communicatieprotocol aangepast wordt, zonder afstemming. Met als gevolg dat het SmoothEMS-systeem blind wordt en de laadpalen suboptimaal regelt. In ernstige gevallen resulteert dit in een contractwaarde overstijging (netcongestie). Als oplossing is een variant van het GridShield geïmplementeerd, waarbij het systeem bij externe storingen terugvalt op harde, veilige, limieten.

Verstoring in externe verbindingen

API-updates voor weersvoorspellingen, energieprijzen en netbelasting kunnen voorspelmodellen verstoren. Een adequaat foutdetectiesysteem is essentieel om afwijkingen tijdig te signaleren en een plan B te activeren. In de toekomst zal het naast fout detectie ook de diagnose stap geautomatiseerd gaan worden (**F**ault **D**etection & **D**iagnosis).

Voorspellingen en modeltraining

Voorspelmodellen gebruiken realtime en toekomstige data, zoals weersinformatie. Wanneer deze gegevens wegvallen, verslechtert de optimalisatie. Daarnaast worden modellen automatisch gehertraind om veranderingen in laadgedrag zo goed mogelijk te blijven voorspellen. Hertraining mag niet gebeuren met foutieve data, omdat dit een incorrect getraind model oplevert. Een geautomatiseerd systeem dat afwijkingen in data detecteert, moet hier een vangnet bieden.

Cybersecurity

Een robuust ICT-systeem moet bestand zijn tegen externe dreigingen, waarbij menselijke fouten vaak de zwakke schakel vormen. Training in cybersecurity, bijvoorbeeld volgens NIS2-richtlijnen, is cruciaal voor betrokken medewerkers.

Aanbevelingen

Systeemintegratie, als centraal thema, heeft iets eigenaardigs als het aankomt op onze elektriciteitsinfrastructuur. Een apparaat aan een stopcontact is al systeemintegratie: via het stroomnet vindt interactie plaats. Het verbruik (of de opwek) wordt echter bepaald door elk apparaat afzonderlijk. De opkomst van IT stelt apparatuur in staat om informatie uit te wisselen om zo ons elektriciteitsnet te kunnen verduurzamen en netcongestie tegen te gaan. De keerzijde is dat apparaten en het energiesysteem afhankelijk worden van elkaars informatie. Deze afhankelijkheid zorgt ervoor dat we niet langer enkel kunnen kijken naar een apparaat, maar vooral ook de effecten op het systeem moeten beschouwen.

We hebben 7 aanbevelingen op basis van onze ervaringen:

1. **Systeemdenken:** Werk met een lijst aan afhankelijkheden en stel ook fabrikanten op de hoogte.
2. **Lokale algoritmes en open interfaces:** Aansturing is kritisch en externe (cloud)diensten kunnen falen. Lokale on-site aansturing heeft de voorkeur.
3. **Centrale monitoring:** Zorg voor adequate monitoring om problemen en inconsistenties snel te detecteren.
4. **Fall-back control:** Systemen falen, een lokaal vangnet is een must.
5. **Diversificatie:** Een breder scala aan leveranciers draagt bij aan robuustheid tegen externe problemen, zoals gehackte diensten, *vendor lock-in* te voorkomen en interoperabiliteit te bevorderen.
6. **Leer van de software sector:** Bij softwarepakketten en –bibliotheken zijn afhankelijkheden dagelijkse orde. Fabrikanten van apparatuur zouden daarom *best practices* uit de softwarewereld moeten omarmen.
7. **Heb oog voor opschaling:** Veel technologie ontstaat uit het oplossen van een ogenschijnlijk geïsoleerd probleem. Vergeet niet te reflecteren hoe een nieuwe oplossing effect kan hebben op o.a. het totaalsysteem of *fairness* bij opschaling.