Over de kwetsbaarheden van HEMS

Maarten Legius

26 juni 2025

Energiemanagementsystemen (HEMS) gebruiken vaak oudere protocollen zoals Modbus TCP. Maar die zijn nooit ontworpen voor open en gedeelde netwerken. De risico's zijn aanzienlijk. Fabrikanten zouden op veilige protocollen moeten standaardiseren.

Om onafhankelijker van energieleveranciers te zijn, energiekosten te beperken of de belasting op het elektriciteitsnet te verlagen, is een Home Energy Management System (HEMS) noodzakelijk. HEMS meten energiegebruik, kunnen warmtepompen, zonnepanelen en laadpalen van elektrische auto's aansturen op basis van persoonlijke wensen en actuele informatie, zoals energieprijzen en weersverwachtingen.

Toegang tot duizenden HEMS

Meer comfort tegen lagere prijzen dus. Tot zover het goede nieuws. Recente cyberaanvallen zoals FrostyGoop en Vo1d malware benadrukken echter de kwetsbaarheden en de potentiële gevolgen voor huishoudens en het bredere energiesysteem. Zo valt te lezen in de whitepaper Cyberweerbare toekomst van HEMS, in juni 2025 door auteur Harm van den Brink van Innoshift opgesteld voor Rijksdienst voor Ondernemend Nederland en de Topsector Energie. Het whitepaper spreekt over grootschalige risico's als kwaadwillenden toegang krijgen tot duizenden HEMS tegelijk.

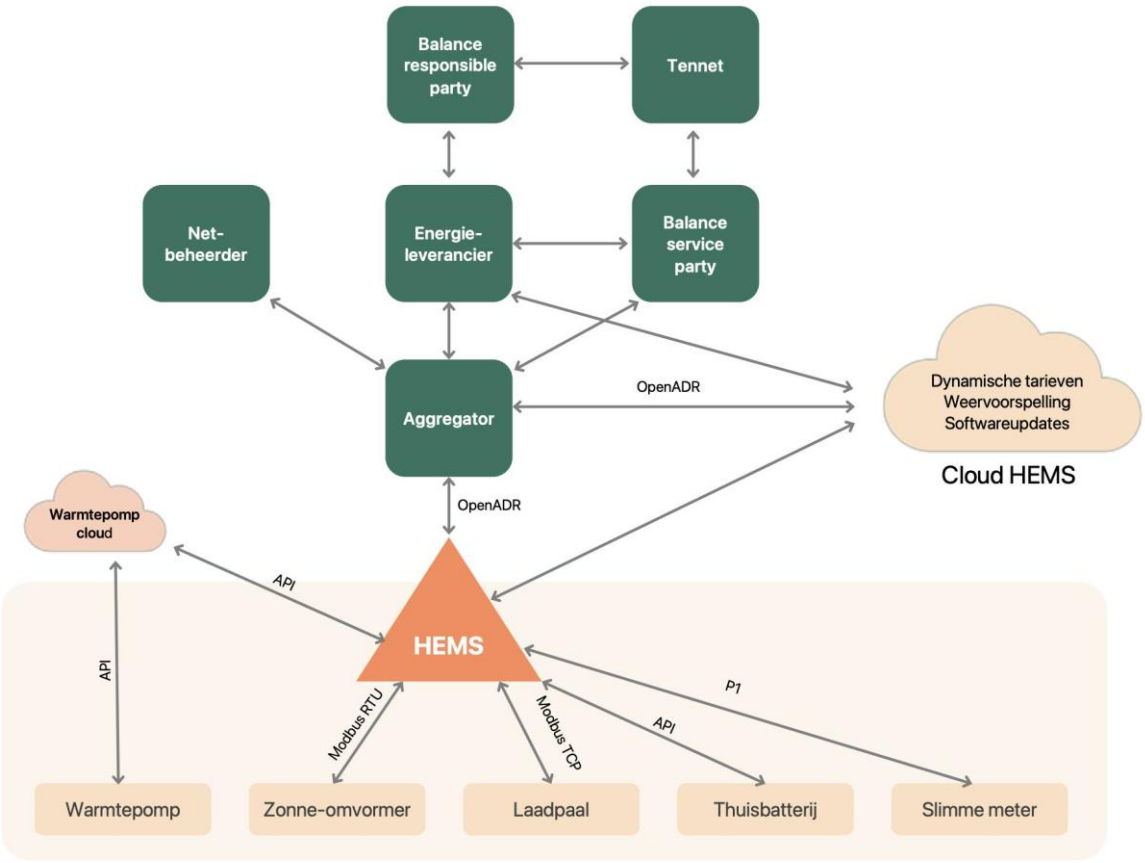
Communicatieprotocollen

HEMS communiceren via diverse protocollen en technieken, variërend van generieke communicatieprotocollen zoals Modbus TCP, Wireless M-bus, en Z-Wave, tot specifieke protocollen

voor energiebeheer zoals Sunspec Modbus, IEEE 2030.5 en EEBus. Veel gebruikte communicatietechnieken zijn MQTT en API's, vaak via cloudplatformen. Zowel deze cloudsystemen als de protocollen brengen gevaren met zich mee. Met name oudere protocollen, zoals Modbus TCP, oorspronkelijk niet ontworpen voor dit soort open en gedeelde toepassingen.

Arhitectuur van een HEMS

Een HEMS is een combinatie van hardware en software en kan in verschillende hoedanigheden voorkomen. Het kan een kleine microcontroller zijn met vaste software en een specifieke taak, maar het kan ook een kleine computer (zoals een single board computer) zijn met besturingssoftware (OS) en andere programmatuur voor tal van functies. De een is doorgaans eenvoudig en betrouwbaar, maar niet flexibel. En de ander kan veel meer, maar is complexer, minder betrouwbaar en doorgaans onveiliger (denk aan beveiligingsupdates). Verder is daar nog de firmware, zoals aanwezig in laadpaal en omvormer. En tot slot de toepassing van open source software, waarvan de broncode voor iedereen vrij beschikbaar is. Verder is een cloudkoppeling een cruciaal onderdeel van het HEMS, omdat het zorgt voor actuele data, software-updates, en (optionele) aansturing door derden.



Architectuur van een HEMS.

De gevaren komen uit 3 hoeken

Het zal geen verbazing wekken dat dit Lego-bouwwerk van hardware en software lastig tot een gesloten vesting te maken is. Volgens Innoshift kunnen de gevaren uit drie hoeken komen. Zo kan ten eerste de cloud van de HEMS worden aangevallen. Daarnaast kan de HEMS zelf (als die lokaal draait) en de communicatie naar de apparaten slachtoffer worden van een aanval. En tot slot is er de mogelijkheid van onopzettelijke kwetsbaarheden door fouten in algoritmes en/of beschikbare data.

Encryptie en authenticatie

Concreet zit het 'm vaak in niet goed beveiligde verbindingen, het ontbreken van encryptie en authenticatie, slecht wachtwoordbeheer en fouten in de cloud-sofware, slecht autorisatiebeheer (wie heeft welke rechten), slechte beveiliging van wifi-netwerken, veroudere firmware en oudere communicatieprotocollen. Het zal duidelijk zijn dat de impact ongekend groot kan zijn als duizenden woningen via 1 cloudplatform worden beheerd.

Modbus onveilig

In de whitepaper wordt vanwege de brede toepassing specifiek op Modubs ingegaan. Modbus TCP is een bewezen protocol, dat goed werkt voor aansturing van industriële apparaten, maar vaak de nodige beveiligingsmechanismen mist. Er is geen mogelijkheid tot goede authenticatie. En versleuteling is wel mogelijk maar dit wordt volgens Van den Brink door nagenoeg niemand geïmplementeerd. Dit betekent dat iedereen op hetzelfde netwerk commando's kan sturen naar een apparaat via Modbus TCP. Geen probleem op een gesloten netwerk, maar tegenwoordig is alles met elkaar verbonden.

Uitval en financiële risico's

De gevaren liggen voor de hand. De consument zal bij een niet werkende HEMS al snel letterlijk in de kou zitten of de elektrische auto niet kunnen opladen. Energiebedrijven lopen flinke financiële risico's als hackers via HEMS prognoses van energiegebruik beïnvloeden en de voorspelling (op basis waarvan men handelt) plotseling sterk afwijkt van de werkelijkheid. En als HEMS gebruikt worden door netbeheerders om op bepaalde momenten de belasting omlaag te brengen, kunnen kwaadwillenden juist het omgekeerde doen en de belasting opvoeren. Dat leidt tot overbelasting van transformatoren en leidingen. Omdat het energienet een groot verbonden netwerk is, kan het zich razendsnel verspreiden over meerdere landen.

De oplossing?

De grote variatie aan communicatieprotocollen en koppelingen tussen en met apparaten, wordt door Innoshift als een van de grootste uitdagingen genoemd. En dan is standaardisatie iets wat zorgt voor minder integratieproblemen en meer cyberveiligheid. Daarbij wijst de auteur naar de fabrikanten die op bepaalde protocollen zouden moeten standaardiseren. Natuurlijk blijft een veilige oplevering van de apparaten (in bedrijf stellen en koppelen) belangrijk. En tot slot pleit de auteur voor uitfasering van verouderde protocollen, waaronder Modbus.

Protocollen voor HEMS

Generieke protocollen voor communicatie tussen apparaten in woningen.

- Modbus RTU wordt via seriële verbindingen (twee draadjes) toegepast voor het uitlezen en aansturen van diverse apparaten.
- Modbus TCP is hetzelfde als Modbus RTU maar hierbij vindt de communicatie plaats via een TCP/IP-netwerk.
- Matter is een op IP gebaseerde smarthome standaard die fabrikant-onafhankelijke interoperabiliteit tussen slimme apparaten mogelijk maakt over netwerken zoals Wi-Fi, Ethernet en Thread.
- OpenTherm wordt gebruikt voor de communicatie tussen thermostaten en warmtepompen en biedt daarmee een standaardmethode voor de aansturing van verwarmingssystemen.
- P1 (DSMR) is het protocol van de slimme meter in Nederland, waarmee near realtime data uit de slimme meter gehaald kan worden.
- Wireless M-Bus is een standaard die zich richt op het uitlezen van water-, gas of elektriciteitsmeters.
- Z-Wave is een standaard voor smart homes en kan slimme apparaten bedienen zoals lampen en sloten of sensoren uitlezen.

Specifieke protocollen voor energiediensten.

- Sunspec Modbus, gestandaardiseerde Modbus registers, richt zich op de toepassing in zonne-energiesystemen en energieopslag, waarbij de communicatie tussen PV-omvormers en batterijsystemen gestandaardiseerd wordt.
- S2-protocol biedt een abstractielaag zodat apparaten, ondanks uiteenlopende eigen protocollen, gezamenlijk aangestuurd kunnen worden.
- IEEE 2030.5 wordt ingezet voor de integratie van gedistribueerde energiebronnen in smart grids.
- EEBus richt zich op de interoperabiliteit tussen smart home apparaten en energiesystemen.
- SG-ready is ontwikkeld voor de fysieke, hardwired aansturing van apparaten zoals warmtepompen en boilers.
- OCPP-protocol wordt gebruikt voor de communicatie tussen laadpalen en backend-systemen, waardoor een standaardisatie van laadpalen mogelijk wordt.

Bron: *Whitepaper Cyberweerbare toekomst van HEMS*

Website: https://groenerzoeterwoude.nl/

Bron : Installatie Journaal