12.3.2025

# Kotiautomaation kyberturvallisuusriskit sähköjärjestelmälle

Laajamittaisen kyberhyökkäyksen vaikutukset sähköjärjestelmälle

Sami Repo, Jari Seppälä ja Muhammad Hamza. Tampereen yliopisto

Samuli Honkapuro, Aleksi Koivu, Aleksei Romanenko. LUT-yliopisto

# Esipuhe

Tässä raporttissa on esitetty projektin “Your Lightbulb Might be Too Smart - Assessment of the Emerging Cybersecurity Risks of Home Automation” keskeisimmät tulokset. Tutkimusprojektissa tarkasteltiin kotitalouskuluttajien saatavilla olevien kotiautomaatiolaitteiden kyberturvallisuusriskejä sekä niiden vaikutuksia sähköverkon ja sähköjärjestelmän kannalta.

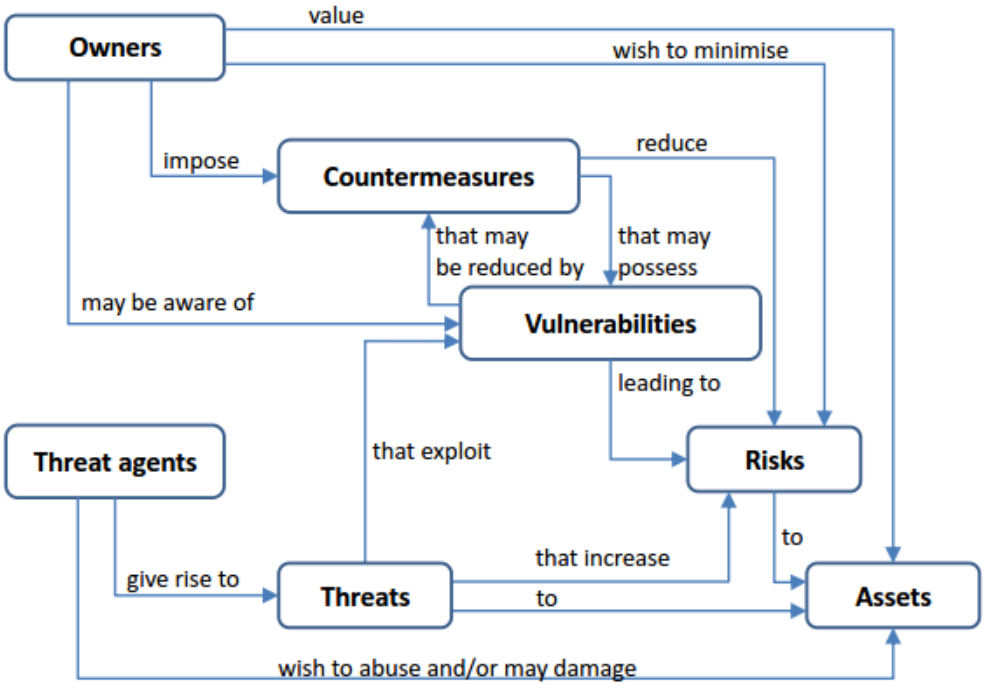
Tutkimuksen toteuttivat Tampereen yliopiston ja LUT yliopiston tutkijat vuosina 2022–2024. Tutkimusprojektin rahoittivat Sähkötutkimuspooli, STEK ry., Järvi-Suomen Energia sekä yliopistot.

# Sisällysluettelo

# 1. Johdanto

Sähköenergiajärjestelmällä on haavoittuvuuksia, jotka kohdistuvat siihen laajamittaisen kyberhyökkäyksen ja kotiautomaation haavoittuvuuksien kautta. Tästä muodostuvaa riskiä voidaan arvioida kuvan 1 mukaisesti haavoittuvuuksien ja uhkien kautta. Parannuskeinoja kotiautomaation kyberturvallisuuden parantamiseksi on toki olemassa lukuisia, mutta tässä tutkimuksessa oletetaan, että kotiautomaatio on suhteellisen haavoittuvainen johtuen omistajapohjan laaja-alaisuudesta ja kyberturvallisuuden perustuntemuksen alhaisesta tasosta.

Uhkaskenaariona käsitellään lähinnä hyvin laaja-alaista pilvipohjaisten automaatiojärjestelmien kautta tapahtuvaa keskitettyä hyökkäystä kotiautomaatioon. Hyökkäyksellä voidaan aiheuttaa seurauksia kotiautomaation omistajan sähköenergian kulutukselle ja sen käyttökohteille, ja edelleen paikalliselle sähkönjakeluverkolle ja sähkömarkkinoille, jos hyökkäys onnistutaan toteuttamaan samanaikaisesti riittävän monessa kohteessa. Käyttökohteina tarkastelut kohdistetaan lähinnä sähkölämmitykseen ja sähköautojen lataukseen. Molemmat ovat potentiaalisia kotiautomaation sovelluskohteita, suurimpia sähkönkulutuksen etäohjattavia laitteita, ja laajasti hyödynnettyjä sähköenergian käyttökohteita. Siten ne voivat saada aikaiseksi merkittävän haitallisen kokonaisvaikutuksen sähköjärjestelmälle kyberhyökkäyksen seurauksena.




Kuva 1. Kyberturvallisuuden riskien arviointikehys kyber-fyysisille järjestelmille.

Tässä tutkimuksessa ei tarkastella kaikkia kotiautomaatioon liittyviä uhkia ja haavoittuvuuksia ja siten määritetä niiden aiheuttamaa riskiä sähköjärjestelmälle, vaan tarkastelu toteutetaan käänteisesti tarkastelemalla mahdollisia sähköjärjestelmän vaikutusskenaarioita. Näistäkin tarkastellaan ainoastaan niitä vaikutusskenaarioita, joilla arvioidaan olevan kaikkein suurimmat vaikutukset sähköjärjestelmälle.

Sähköjärjestelmän vaikutuksia tarkastellaan sekä sähkönjakeluverkon että sähköjärjestelmän säätö- ja reservimarkkinoiden näkökulmista. Samanaikaisesti toteutettu kyberhyökkäys todennäköisesti vaikuttaa näihin ensimmäisenä tai vähäisemmillä kaapatuilla resursseilla. Koko sähköjärjestelmän tehotasapainon vaarantumista ei tarkasteltu tarkemmin sen vaatiessa huomattavasti suuremman resurssimäärän kuin paikalliset vaikutukset ja kaupankäyntimääriltään pienempien markkinoiden manipulointi.

# 2. Tutkimusmenetelmä

## 2.1 Vaikutusskenaarioiden valinta

Erilaisina sähköjärjestelmään kohdistuvina vaikutusskenaarioina tarkasteltiin kansallisen sähköjärjestelmän tehotasapainoa, paikallisen jakeluverkon jännitteenlaadun tai kuormitettavuuden vaarantumista, ja sähkön loppukäyttäjän harmia.

Sähköjärjestelmän tehotasapainon vaarantuminen kyberhyökkäyksen seurauksena voi toki olla mahdollista, mutta sen riskiä pidettiin kuitenkin niin pienenä, ettei tätä vaikutusskenaariota tarkasteltu alkuanalyysiä tarkemmin. Vaikutusten toteutuminen edellyttäisi monen harvinaisen tapahtuman samanaikaisuutta kyberhyökkäyksen käynnistämisen kanssa. Vaikka tällainen hyökkäys saattaisi olla kiinnostava joillekin valtiollisille hyökkääjätahoille, niin se edellyttäisi hyvin suuria resursseja kaapattujen kohteiden osalta. Sähköjärjestelmä kestää suunnitellusti vähintään ns. mitoittavan vian suuruisen häiriön, joka Suomessa on tehotasapainon näkökulmasta Olkiluoto 3 ydinvoimayksikön suuruinen tehonmuutos vähennettynä järjestelmäsuojan teholla. Tehonmuutoksen tulisi ylittää vähintään 1300 MW, jotta tehoepätasapaino voisi vaarantua kaikkein pahimmassa mahdollisessa tilanteessa. Käytännössä sähköjärjestelmä on tällaisessa tilassa äärimmäisen harvoin, jolloin tehonmuutoksen tulisi olla vielä tätäkin suurempi. Kokoamalla yhteen kaikkien kotitalouksien kotiautomaation ohjauksessa olevat sähkölämmityskohteet ja sähköautojen lataukset, tällainen tehonmuutos voisi olla teoriassa toteutettavissa.

Tehotasapainoon voidaan kuitenkin vaikuttaa helpommin säätö- ja reservimarkkinoiden välityksellä. Vaikutukset eivät tällöin ole yhtä dramaattisia, eli sähköjärjestelmä todennäköisesti säilyttää tasapainonsa, mutta taajuuden laatu voi häiriintyä ja siten luoda uhan sähköjärjestelmän käyttövarmuudelle. Toiseksi säätö- ja reservimarkkinoiden manipulointi voi kasvattaa tehotasapainon hallinnan kustannuksia kantaverkkoyhtiölle ja tasevastaaville. Kyberhyökkäyksen avulla voidaan luoda tilanne, jossa samanaikaisesti on pula säätö- ja reservimarkkinoiden tarjouksista ja hyökkäyksen kautta luodaan tehoepätasapaino, johon markkinoiden kautta hankitut säätö- ja reserviresurssit reagoivat ja siten kasvattavat eri osapuolten kustannuksia. Tämän vaikutusskenaarion todennäköisyyttä pidettiin suurempana kuin edellistä skenaariota, joten tämä vaikutusskenaario valittiin tarkempiin jatkotarkasteluihin. Perusteluna valinnalle voidaan pitää esimerkiksi sitä, että säätö- ja reservimarkkinoiden tarjouksista on ajoittain ollut pulaa Suomessa ja siten kaupankäyntihinnoissa on hyvin suurta volatiliteettia. Lisäksi säätö- ja reservipalveluiden tarve

on kasvamassa lähivuosina tuuli- ja aurinkovoiman kasvun ja koko yhteiskunnan sähköistymisen myötä.

Vaikka paikallisten sähkönjakeluverkkojen kuormitusaste on keskimäärin alhainen, niin ajoittain ja erityisesti heikommin mitoitetuissa haja-asutusalueen jakeluverkoissa jännitteen alenema tai nousu aiheuttaa haasteita verkon käytölle. Erityisesti tällaisia tilanteita voi syntyä poikkeuksellisten kytkentätilanteiden aikana, jolloin esimerkiksi kokonaisen sähköaseman verkkoalue syötetään naapuriasemien ja varasyöttöyhteyksien kautta. Tällaiset jänniteongelmat esiintyvät normaalisti verkon huippukulutustilanteissa jännitteen alenemana hyvin paikallisena ongelmana säteittäisen keskijännitelähdön reuna-alueilla. Vastaavasti jännitteennousua esiintyy hajautetun tuotannon vaikutuksesta, kun koko keskijännitelähdön tehonsiirron suunta vaihtuu päinvastaiseksi asiakkaiden syöttäessä tehoa kohti sähköasemaa, jolloin jännite nousee verkon reuna-alueilla nimellisjännitettä suuremmaksi. Kohdistamalla kyberhyökkäys näihin ajankohtiin erityisesti niillä verkkoalueilla, joissa jänniteongelmia esiintyy, niin ongelman laajuutta ja vakavuutta saadaan kasvatettua hyvinkin pienillä resursseilla. Mitä tarkemmin hyökkäys osataan kohdistaa sähköverkon kannalta epäedulliseen kohteeseen ja ajankohtaan, niin sitä vähäisemmillä resursseilla saadaan haitallista vaikuttavuutta sekä sähköverkolle (verkon vahvistustarve kasvaa) että loppukäyttäjille (jännitteen laatupoikkeamat voivat aiheuttaa kulutus- ja tuotantolaitteiden vikaantumista tai käyttöhäiriöitä). Tarkempien tarkasteluiden osalta keskityttiin ainoastaan kuormituksen kasvattamiseen ja siten jännitteen aleneman tutkimiseen.

Samoilla tarkasteluilla analysoidaan myös verkon komponenttien ja käyttöpaikkojen ylikuormittumista. Vaikka normaalisti verkon komponenttien kuormitusaste on N-1 suunnitteluperiaatteen takia alle 50 % ja siten verkossa pitäisi olla reilusti kapasiteettia kasvattaa kuormitusta, niin kyberhyökkäyksen seurauksena syntyvä sähkönkulutuslaitteiden samanaikaisen käyttö voi johtaa verkon ja käyttöpaikkojen ylikuormittumiseen. Sähköverkon suunnittelussa hyödynnetään tietoa laitteiden käytön vuorottelusta, eli kokemuksesta tiedetään, etteivät kaikki laitteet ole samanaikaisesti käytössä. Esimerkiksi sähkölämmityskohde (10-15 kW), jossa on lisäksi kolmivaiheinen sähköauton lataus (11 kW) ja käyttöveden lämmitys (11 kW), niin näiden kolmen laitteen yhteisteho riittää ylikuormittamaan 3*25 A pääsulakkeet (17 kW), vaikka normaalisti laitteiden käyttö onnistuu ongelmitta. Jos samanlaisia käyttökohteita on useampia samassa pienjänniteverkossa, niin myös pienitehoisen jakelumuuntajan ja pienjännitekaapeleiden ylikuormittaminen onnistuu helposti. Pääsulakkeiden palamisesta aiheutuva haitta loppuasiakkaalle voi olla merkittävä kiinteistön jäätyessä tai sähköauton akun

jäädessä lataamatta. Sähkönjakeluverkolle vaikutukset voivat äärimmillään olla tuhoutuneita komponentteja ylikuormituksen seurauksena tai niiden ennenaikaista ikääntymistä, mitkä molemmat kasvattavat investointitarvetta, ja siten vaikuttavat myös loppukäyttäjien kustannuksiin.

Muita mahdollisia loppukäyttäjän kyberhyökkäyksen ja sähkönkäytön manipuloinnin haittoja ei tarkasteltu lähemmin. Hintaohjatun sähkönkäytön logiikkaan voidaan vaikuttaa todella helposti vääristämällä pilvipalvelusta kotiautomaatiolle menevää ohjaussignaalia. Jos ohjaussignaalina käytetään esimerkiksi sähkömarkkinan spot-hintaa, niin kääntämällä hintasignaali peilikuvakseen, saadaan asiakkaan sähkönkulutuksen kustannukset kasvamaan toisinaan merkittävästikin. Loppukäyttäjän lisäksi haittaa aiheutuu sähkönmyyjälle ja tasevastaavalle sähkönmyyjän päivää edeltävän markkinan hankintaennusteen virheiden kautta, kun loppukäyttäjän käyttäytyminen poikkeaa merkittävästi ennustetusta. Mitä useamman asiakkaan käyttäytymistä saadaan muokattua, sitä suuremmaksi myyjän hankintaennusteen virhe kasvaa. Jos samanaikaisesti on vielä manipuloitu säätösähkömarkkinaa, voivat tasekustannukset kasvaa huomattavan suuriksi.

Kaikille vaikutusskenaarioille on yhteistä, että ne tulevat laajamittaisesti mahdolliseksi keskitettyjen pilvipalveluiden haavoittuvuuksien kautta. Hyökkäys pilvipalveluihin voi tapahtua esimerkiksi riittämättömästi suojaamattomien kotiautomaatiolaitteiden kautta. Vaikka laitteet myytäessä olisivatkin olleet kyberturvallisia, niin niiden päivitys jää usein loppukäyttäjien vastuulle ja siten huolehtimatta. Toki varautumista on tehostettava ja tulisikin parantaa, mutta houkutus myydä edullisia laitteita ja järjestelmiä voi olla liian suuri, jos huolellisesti ylläpidettyjä järjestelmiä ei ole pakko toteuttaa. Loppukäyttäjän vastuuta kyberturvallisuusasetteluiden ja -päivitysten toteuttamisesta tulisin siirtää laite- ja järjestelmätoimittajille.

## 2.2 Säätö- ja reservimarkkinoiden analyysi

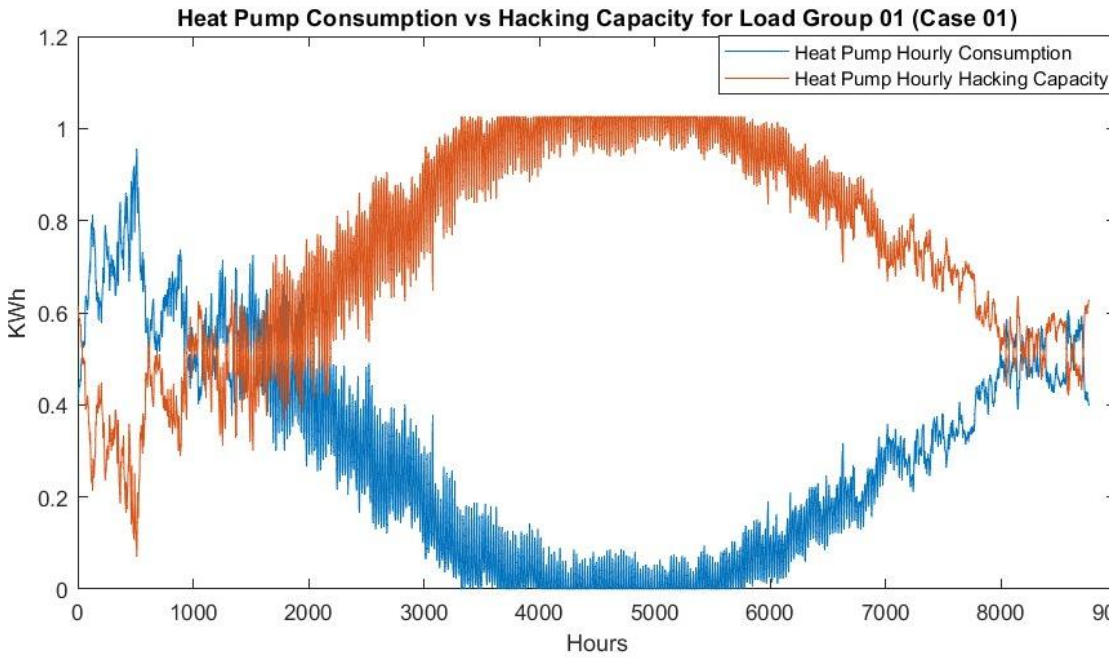
Säätö- ja reservimarkkinoiden analyysi toteutettiin tarkastelemalla vuosien 2019-2023 toteutuneita kaupankäyntimääriä ja -hintoja. Riskinä arvioidaan, kuinka helposti kyberhyökkäyksellä voidaan manipuloida kyseisiä markkinoita, joko luomalla pulaa tarjouksista tai manipuloimalla toteutuneiden kauppojen hintaa.

## 2.3 Sähkönjakeluverkon analyysi

Sähkönjakeluverkkojen analyysi toteutettiin manipuloimalla jakeluverkkojen laskennassa käytettäviä kuormituskäyriä vastaamaan kyberhyökkäyksen mukaista tilannetta. Verkostolaskenta toteutettiin myös normaalille käyttötilanteelle, johon lisättiin sähkölämmityskulutusta ja sähköautojen latausta kaikkiin käyttöpaikkoihin. Tällä tavoin saatiin selville vertailukohta kyberhyökkäyksen vaikutuksille. Hyökkäysskenaariossa oletettiin, että kaikki kyseisen tarkastelun sähkölämmityskohteet tai sähköautojen lataukset ovat hyökkääjän hallussa. Tällä tavoin saadaan selville pahin mahdollinen tilanne.

Tarkempi kuvaus kuormituskäyrien muokkauksesta normaali- ja hyökkäystilanteille on kuvattu lähteessä [1]. Normaalitilanteen (referenssitilanteen) asiakkaiden kuormitusta muokattiin sen mukaan, oliko heille lisätty lämpöpumppua tai sähköautoa. Muokattavina asiakasryhminä hyödynnettiin omakoti- ja rivitaloja, vapaa-ajan asuntoja ja maatiloja. Hyökkäyksen aikana muiden kulutuslaitteiden peruskuormituskäyrä säilyi ennallaan, mutta hyökkäyksen kohteeksi joutuneen laitteen teho kasvatettiin nimellistehon suuruiseksi. Tehonjakotarkastelut tehtiin kaikille vuoden tunneille sekä referenssitilanteille että hyökkäystilanteille. Tarkasteltavana verkkona hyödynnettiin Järvi-Suomen Energian keskijännite- ja pienjänniteverkkoa kokonaisuudessaan.

Kuvassa 2 on esitetty esimerkki lämpöpumpun kuormituskäyrästä normaalitilanteessa (sininen käyrä) ja hyökkäyksen käytettävissä oleva ylimääräinen kapasiteetti normaalitilanteeseen nähden (oranssi käyrä). Normaalitilanteen kuormitusprofiili riippuu voimakkaasti ulkolämpötilasta, joten kulutus on suurempaa kylmempään vuodenaikaan ja on hyvin vähäistä kesäkuukausina. Hyökkäyksen käytettävissä oleva lisäkapasiteetti on normaalitilan profiilin peilikuva, koska yhteenlaskettu teho tulee olla laitteen nimellistehon suuruinen. Kuten myöhemmin havaitaan, niin hyökkäyksen haitta lämpöpumpuilla jää suhteellisen vähäiseksi johtuen vähäisestä lisäkapasiteetista, joka hyökkäyksellä on tavikuukausina käytettävissään. Lämpöpumpun lisääminen ei-sähkölämmitteiseen kohteeseen luonnollisesti kasvattaa kuormitustasoa enemmän kuin lämpöpumpun korvatessa suoraa sähkölämmitystä.




Kuva 2. Kuormityskäyräryhmän 1 (sähkölämmitteinen omakotitalo) lämpöpumpun kuormituskäyrä.

Sähköautojen latauksen osalta päivittäistä lataustarvetta arvioitiin Traficom:n liikennetilastojen perusteella. Lisäksi oletettiin (epärealistisesti), että kaikkia autoja ladataan päivittäin kotona joko yksivaiheisen tai kolmivaiheisen latauspistokkeen kautta. Kullekin kiinteistölle lisättiin yksi sähköauto. Hyökkäys kohdistettiin ajankohtaan, jolloin sähköverkkoon oli kytkettynä eniten sähköautoja ja siten ajoittamalla mahdollisimman suuri lataustehо samanaikaisesti. Periaatteessa vastaava ilmiö voisi toteutua hintaohjauksen kautta ilman kyberhyökkäystäkin.

Taulukossa 1 on yhteenveto muokattujen kuormituskäyrien vaikutuksesta käyttöpaikkojen huipputehoon normaali- ja hyökkäystilanteessa. Lämpöpumppujen lisäys sähkölämmitteisiin kohteisiin ei kasvata huipputehoa, vaan se pysyy suoraa sähkölämmitystä vastaavalla tasolla. Ei-sähkölämmittäjien osalta lämpöpumppu toki kasvattaa huipputehoa sekä normaali- että hyökkäystilanteessa merkittävästi. Sähköautojen latauksen vaikutukset riippuvat luonnollisesti lataustehosta ja suhteessa aikaisempaan kuormitustasoon. Muutokset huipputehossa ovat ei-sähkölämmittäjien tapauksessa todella merkittävästi suurempia erityisesti nopealla latauksella.

Taulukko 1. Yhteenveto muokatuista kuormituskäyristä ja niiden huipputehoista.

| Customer | Energy | Peak load (normal) | Peak load (attack) |
|---|---|---|---|
| **Direct electric heating** | | Q | |
| + heat pump | Decrease | <Q | Q |
| + electric vehicle 1.84 kW | Increase | ~1.2*Q | ~1.4*Q |
| + electric vehicle 11 kW | Increase | 1.2-1.7*Q | 3-4.5*Q |
| **Non-electric heating** | | QQ | |
| + heat pump | Increase | ~2*QQ | ~3*QQ |
| + electric vehicle 1.84 kW | Increase | ~1.7*QQ | ~2.5*QQ |
| + electric vehicle 11 kW | Increase | ~2*QQ | 8-13*QQ |

# 3. Kotiautomaatio bottinetin uhka ja sen vaikutus sähköverkkoon

Tämän osion tarkoituksena on tutkia kotiautomaatiolaitteista koostuvan bottinetin muodostamaa uhkaa ja minkälainen vaikutus sillä voisi olla sähköverkkoon. Tässä esitetyt tulokset perustuvat Aleksi Koivun diplomityöhön [2], jossa tutkimusta on kuvattu laajemmin.

Työssä aluksi selvitetään kotiautomaation bottinetin muodostumisen mahdollisuutta ja kuinka suurta kuormaa hyökkääjä voisi bottinetin avulla mahdollisesti ohjata. Tämä tehdään tutkimalla erilaisten kotiautomaatiolaitteiden haavoittuvuuksia ja tutkimalla bottinettien historiallista leviämistä.

## 3.1 Laitteiden haavoittuvuudet

Laitteiden tietoturvallisuuden analyysissä tutkitaan seuraavia heikkouksia:

- Man-In-The-Middle (MITM) hyökkäys käyttäen ARP poisoning tai DHCP spoofing menetelmiä
- Denial-of-Service (DoS) käyttäen TCP SYN flood menetelmää
- TLS implementaatio virheitä, kuten:
    - Laite tukee vanhentuneita salaussarjoja
    - Laite ei tarkista sertifikaattia
    - Sertifikaatissa on liian heikko avain sen voimassaolo ajalle
        - avainten vahvuussuositukset otetaan NIST arvion mukaan
    - Hyväksyy sertifikaatin, jonka voimassaoloaika on mennyt ohi
        - Testataan antamalla laitteelle väärennetty NTP viesti
    - Ei käytä molemminpuolista todennusta
- Laite käyttää salaamatonta viestintää
- Salaamaton viestintä ei käytä mitään todennus menetelmää
- Laite käyttää haavoittuvaista verkko käyttöliittymää

Seuraavassa avataan hieman tutkittuja heikkouksia. Tarkemmin eri protokollien, kuten ARP ja DHCP, toimintaan ei kuitenkaan mennä. MITM hyökkäyksen tarkoituksena on päästä tilaan,

jossa hyökkääjä pystyy kontrolloimaan viestintää kahden laitteen välillä. DoS hyökkäyksen tarkoituksena on estää kohdelaitetta viestimästä. TLS käyttää salaussarjoja, jotka määrittelevät mitä asymmetristä ja symmetristä salausta käytetään, sekä mitä todennusmenetelmää ja digitaalista allekirjoitusmenetelmää käytetään. Vanhentuneet salaussarjat jaetaan kahteen luokkaan: heikkoihin ja epäturvallisiin. Heikot salaussarjat suositellaan poistamaan käytöstä, kun sopiva tilaisuus esiintyy. Epäturvalliset salaussarjat suositellaan poistamaan käytöstä heti kun mahdollista. Sertifikaatteja käytetään todentamaan vastapuoli ja salaamaan symmetrisen avaimen vaihto. Sertifikaateissa on voimassaoloaika, jonka jälkeen sertifikaattia ei tulisi enää hyväksyä.

Työssä tutkitaan 16 laitetta, jotka ovat:

- kaksi Wi-Fi/Bluetooth gateway laitetta
- Wi-Fi/Zigbee gateway, joka on tarkoitettu Zigbee valojen ohjaamiseen
- Wi-Fi jatkojohto
- kaksi Wi-Fi sähkölämmitintä
- ethernet/6LowPAN gateway, jota käytetään 6LowPAN termostaatin kanssa
- Wi-Fi termostaatti
- Wi-Fi kaiutin
- Wi-Fi kahvinkeitin
- kaksi Wi-Fi lamppua
- Wi-Fi pistoke
- ethernet/Wi-Fi älykoti hub
- Wi-Fi älykoti hub:in kantaman laajentaja
- ethernet/Wi-Fi gateway kahdella kantaman laajentajalla

Kaikki tutkitut laitteet on ostettu suomalaisista verkkokaupoista ja ovat siten kuluttajien saatavilla ja yleisesti käytettyjä. Tarkasteluun otettiin mukaan myös vähäisen sähkönkulutuksen laitteita, jotta saatiin parempi kokonaiskuva laitteiden haavoittuvuuksista.

MITM hyökkäykseen 14 laitetta on haavoittuvaisia. DoS hyökkäykseen kahdeksan laitetta on haavoittuvaisia. 15 laitetta tukee heikkoja salaussarjoja ja kaksi laitetta tukee epäturvallisia salaussarjoja. Tutkituista laitteista seitsemän käyttää sertifikaattia. Kaksi laitetta hyväksyy väärennetyn sertifikaatin: kahvinkeitin ja yksi lämmittimistä. Kuusi laitetta käyttää sertifikaatissa liian heikkoja avaimia voimassaoloaikaan nähden. Kolme laitetta hyväksyy vanhentuneen sertifikaatin. Kolme laitetta ei ilmaise millään tavalla, että on hyväksynyt väärennetyn NTP viestin ja hyväksyy vielä sertifikaatin. Näissä tapauksissa oletetaan, että laite hyväksyy uuden ajan, koska oletettavasti laite reagoisi väärennettyyn viestiin kysymällä aikaa uudestaan tai kysymällä aikaa toiselta taholta. Yksi laite ei hyväksynyt sertifikaattia. Vain yksi laite käyttää molemminpuolista todennusta. Kahdeksan laitetta käyttää salaamatonta viestintää. Laitteista kolme lähettää käskyjä salaamattomalla viestinnällä, joista kaksi käyttää jotain todennusmenetelmää. Testatuista laitteista yksikään ei käytä verkkokäyttöliittymää.

## 3.2 Bottinetin leviäminen ja vaikutukset

Bottinetin leviämistä arvioidaan tarkastelemalla vastaavien haittaohjelmien leviämistä. Tällä hetkellä eniten levinnyt IoT bottinetti on Mirai. Laajimmillaan se levisi 600 000 laitteeseen globaalisti, mikä verrattuna silloiseen 5,5 miljardiin IoT laitteeseen, vastaa noin 0,11 %:in läpäisyosuutta. Suomessa Mirai tartuntoja oli enimmillään noin 20 000. Muiden haittaohjelmien leviäminen on ollut vaatimattomampaa.

Kotiautomaatio bottinetin vaikutuksia sähköverkon toimintaan on tutkittu aiemmin mm. Huang et al. [3], Shekari et al. [4] ja Shekari et al. [5]. Huang et al. (2019) tutkii verkon taajuuteen vaikuttamisen mahdollisuutta. Shekari et al. [4] tutkii jännitteeseen vaikuttamisen mahdollisuutta. Shekari et al. [5] tutkii hintoihin vaikuttamisen mahdollisuutta. Aiempien tutkimusten perusteella vaaditaan 0,2–10 % kuormituksen hallintaa, skenaariosta riippuen, aikaansaamaan merkittävää häiriötä sähköjärjestelmässä.

Mirain 0,11 % läpäisyosuus ei vielä ylitä vaikutuksen kynnystä. Mikäli bottinetti leviäisi Mirain tapaan 20 000 kotitalouteen, ja jos oletetaan että jokaisen kotitalouden huipputeho on 17 kW, olisi bottinetin vaikutuksen piirissä jo yli 2 % valtakunnallisesta tehosta, jolloin bottinetillä voisi olla vaikutusta järjestelmän kannalta. Tässä pessimistisessä skenaariossa kuitenkin bottinetin vaikutuksen piirissä pitäisi olla kaikki kotitalouden merkittivät sähkönkulutuskohteet, ei ainoastaan yksittäiset laitteet.

Yhteenvetona bottinettiskenaariosta voidaan todeta, että testatuissa kotiautomaatiolaitteistoissa oli merkittävän paljon tietoturvahaavoittuvuuksia, joita käyttäen hyökkääjä voisi saada

laitteiston käyttöönsä. Yksittäisen laitteen hallinnasta syntyisi kuitenkin vain harmia laitteen omistajalle. Laajempaa häiriötä aiheuttaakseen hyökkään tulisi saada laitteita haltuunsa kymmeniä tuhansia. Näin muodostetulla bottinetillä voisi mahdollisesti aiheuttaa haittaa järjestelmälle, mutta todennäköisesti hyökkääjä ei saisi niin suurta kuormaa haltuunsa, että se vaarantaisi koko sähköjärjestelmän.

# 4. Simulointitulokset

## 4.1 Säätö- ja reservimarkkinoiden analyysi

Yksityiskohtaiset analyysit säätö- ja reservimarkkinoiden tarjousmäärien vähäisyydestä (volyymiriski) ja hintasensitiivisyydestä (hintariski) kunkin markkinan osalta on esitetty lähteessä [1]. Potentiaalisia tilanteita, joissa kyberhyökkäys voi vaikuttaa sähköjärjestelmään markkinoiden manipuloinnin kautta on esiintynyt Suomessa. Tarkasteluissa ei kuitenkaan arvioitu kuinka todennäköistä tällaisen manipuloinnin onnistuminen on tai millaisia vaikutuksia manipuloinnilla olisi, joten tuloksesta ei voida johtaa kovin pitkälle meneviä johtopäätöksiä. Potentiaalinen riski on siis olemassa ajoittain muutamina kertoina vuodessa. Kuvissa 3 ja 4 on esitetty hinta- ja volyymiriskit FCR-D ylössäätö tuotteen osalta. Eri väreillä on indikoitu riskikategorioita ja molemmissa kuvissa esiintyy useita korkean riskin tilanteita. Kokonaisriski muodostuu näiden kahden indikaattorin ”tulona” ja usein toteutuneet korkean riskin tilanteet ovatkin punaisella molempien indikaattoreiden perusteella.

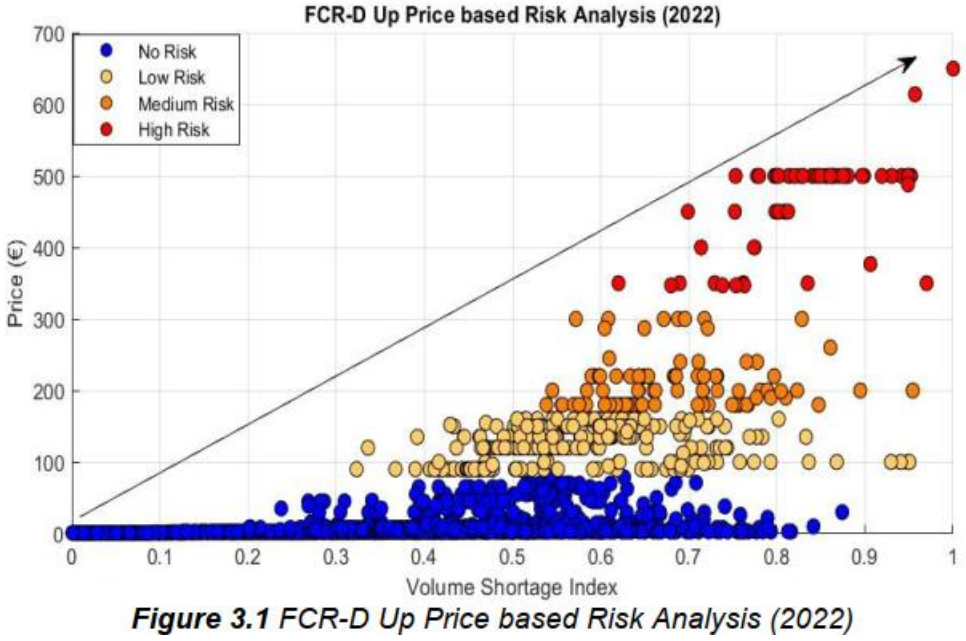



***Figure 3.1** FCR-D Up Price based Risk Analysis (2022)*

Kuva 3. FCR-D ylössäätö tuotteen hintariski.

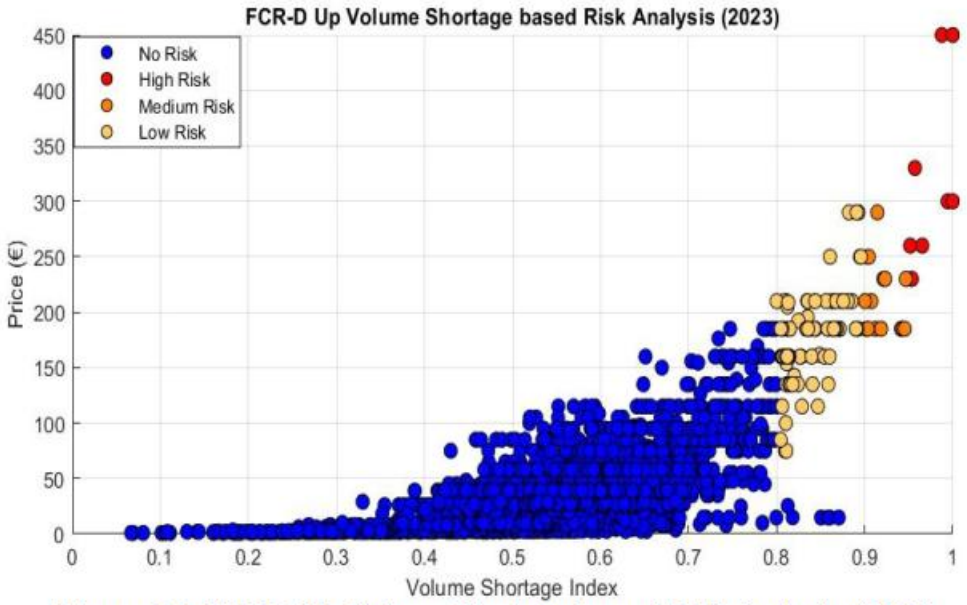


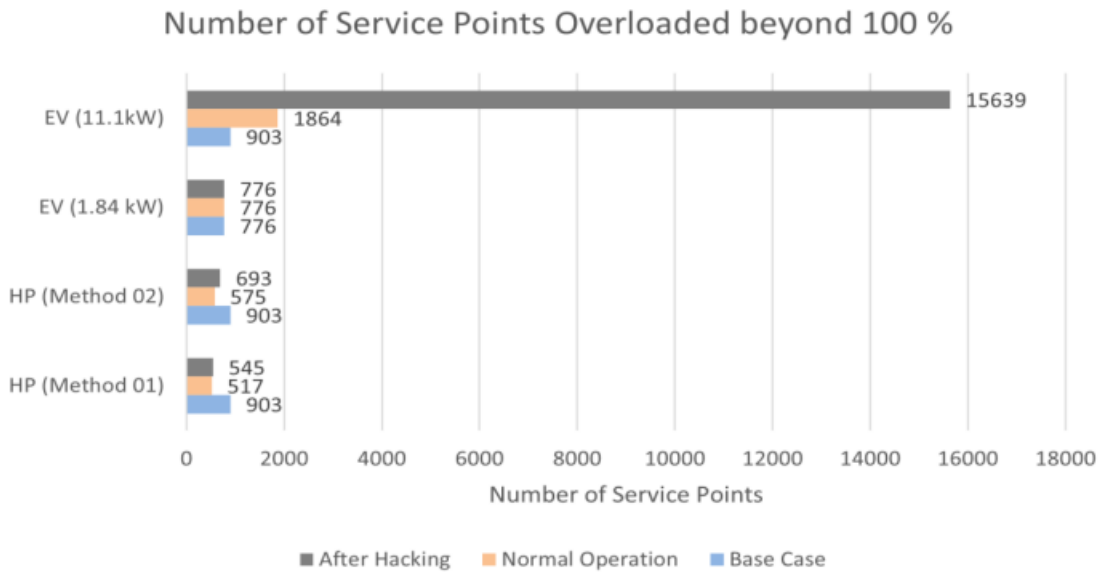
***Figure 3.2** FCR-D Up Volume Shortage based Risk Analysis (2023)*

Kuva 4. FCR-D ylössäätö tuotteen volyymiriski.

## 4.2 Sähkönjakeluverkon analyysi

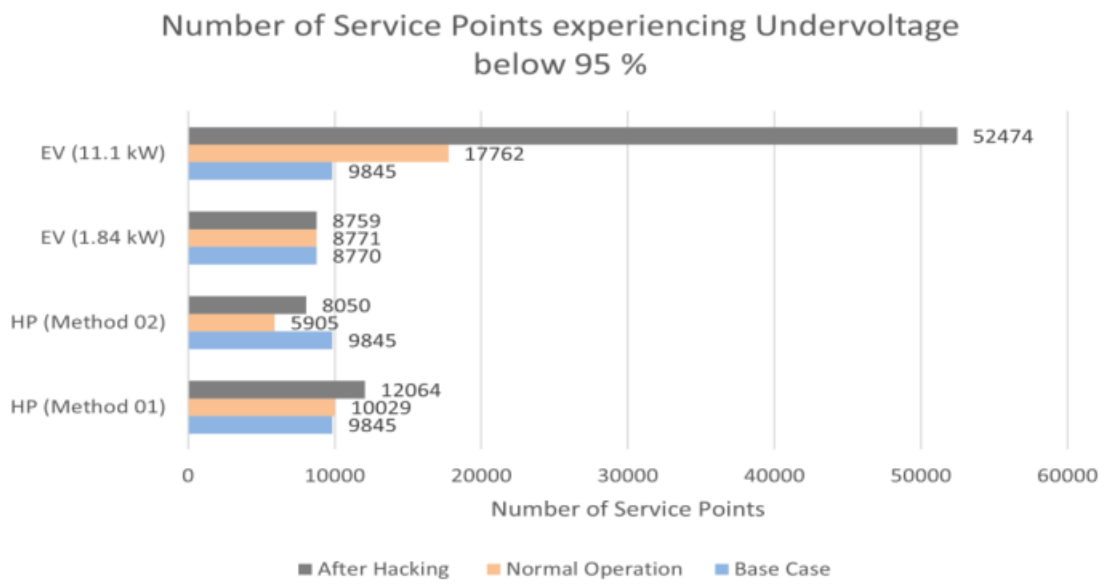
Sähkönjakeluverkon analyysi lämpöpumppujen ja sähköautojen latauskuorman lisäykselle on esitetty kokonaisuudessaan lähteessä [1]. Perustilanne (Base case) edustaa verkon tilaa ennen näiden kuormien lisäystä, joten ne edustavat verkon nykytilaa. Normaalitila (Normal operation) edustaa lisättyjen lämpöpumppujen ja sähköautojen vaikutusta ennen kyberhyökkäystä. Vastaavasti hyökkäyksen jälkeinen (After hacking) tilanne edustaa kyberhyökkäyksen vaikutuksia sähkönjakeluverkossa.

Käyttöpaikkojen osalta analyysin keskeiset tulokset on esitetty kuvissa 5 ja 6. Koko verkossa on noin 80 000 käyttöpaikkaa. Kaikissa skenaarioissa esiintyy jonkin verran ylikuormittuneita käyttöpaikkoja mukaan lukien perustilanne ennen lisättyjen lämpöpumppu- ja sähköautokuormia. Merkittävin muutos tapahtuu kolmivaiheisen sähköautojen latauksen skenaarioissa, jossa normaalitilanteessakin ennen hyökkäystä esiintyy jonkin verran perustilannetta enemmän ylikuormittumisia. Oleellisin muutos tapahtuu kuitenkin kyberhyökkäyksen seurauksena, jolloin hieman vajaa 20 % käyttöpaikoista ylikuormittuu.



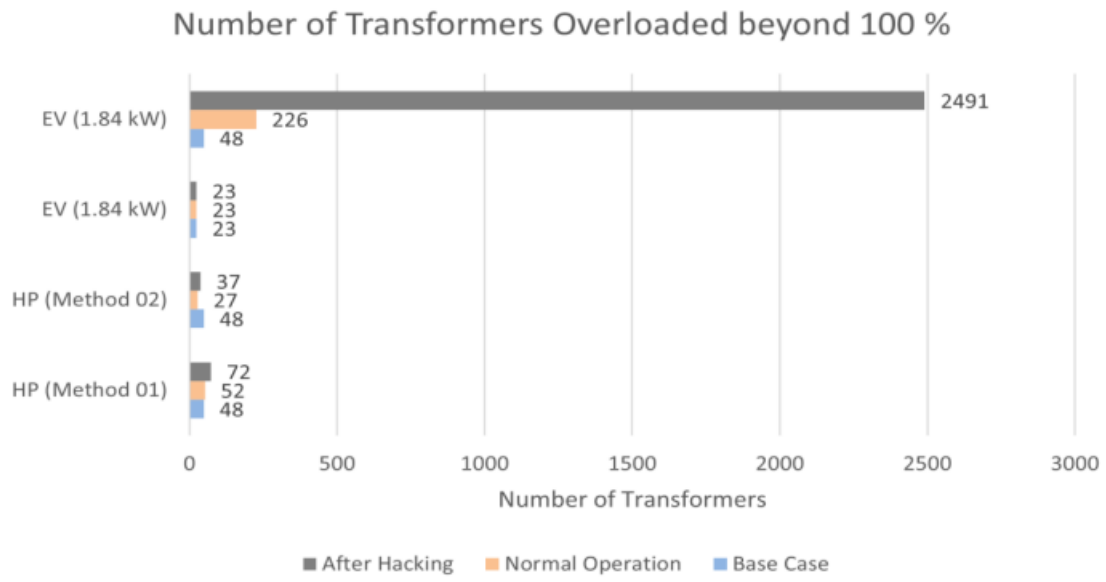

Kuva 5. Ylikuormittuneiden käyttöpaikkojen lukumäärät.

Vastaavasti kuvassa 6 näkyy kolmivaiheisen sähköautojen latauksen vaikutus käyttöpaikkojen alijännitteiden lukumääriin merkittävänä kohoamisena normaalitilanteessa ja erittäin merkittävänä kohoamisena hyökkäystilanteessa. Alijännitteenä tässä tarkastelussa on pidetty 95 %:n jännitettä suhteessa nimellisjännitteeseen. Normaalitilanteessakin yli 22 % käyttöpaikoista kokee alijännitettä ja hyökkäyksen aikana noin 65 % käyttöpaikoista. Vaikka alijännitteen raja asetettaisiin 90 %:iin, niin tulos olisi yhä samansuuntainen, alijännitteisten käyttöpaikkojen lukumäärän noin puolittuessa, mutta silti aiheuttavan merkittävää haittaa käyttöpaikoille.



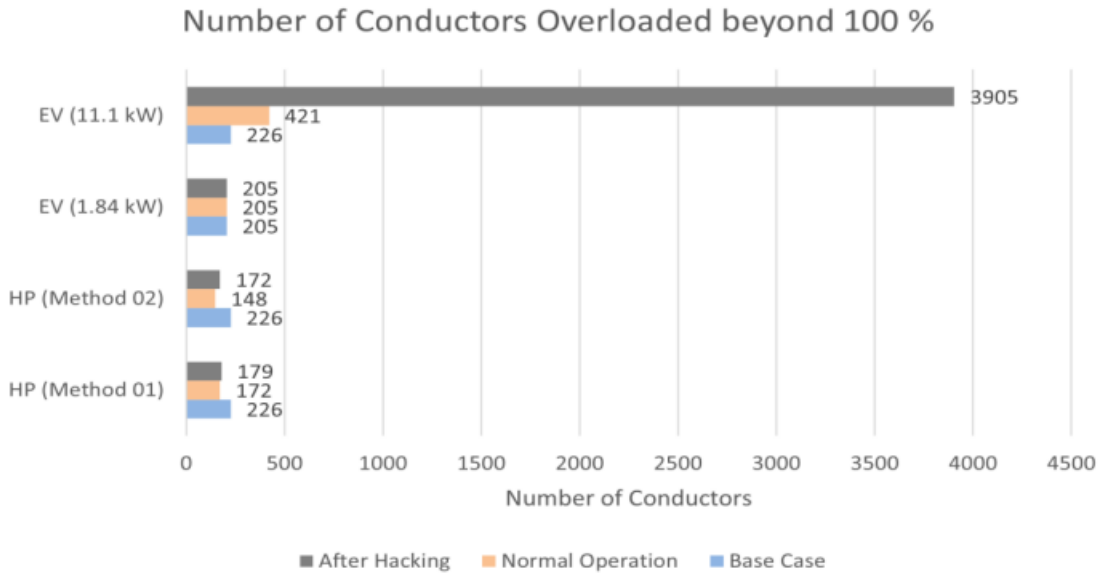

Kuva 6. Alijännitteisten käyttöpaikkojen lukumäärät.

Kyseisessä jakeluverkossa on noin 9 500 jakelumuuntajaa, joiden ylikuormittuminen käyttäytyy samansuuntaisesti käyttöpaikkojen kanssa. Ylikuormitettujen jakelumuuntajien lukumäärä kasvaa kolmivaiheisen sähköautojen latauksen vaikutuksesta sekä normaalitilanteessa että erityisesti hyökkäystilanteessa. Yli 130 %:n ylikuormitustakin esiintyy 32 ja 1 460 jakelumuuntajalla normaali- ja hyökkäystilanteissa kolmivaiheisen sähköautojen latauksen yhteydessä. Tarkempi tarkastelu edellyttäisi ylikuormittuneiden jakelumuuntajien sijainnin (sisällä, kopissa vai pylväässä) tarkastelua yhdessä ylikuormituksen ajankohtien (ulkolämpötilan) tarkastelua, jotta muuntajien jäähdytysolosuhteet tulisivat huomioiduksi. Kyberhyökkäyksen vaikutus jakeluverkolle on joka tapauksessa erittäin merkittävä.




Kuva 7. Ylikuormitettujen jakelumuuntajien lukumäärät. (kuvassa virhe EV (1.84 kW) kohdalla, joista ylemmän pitäisi olla EV (11 kW))

Johtimia jakeluverkosta löytyy kaikkiaan reilu 244 000. Johtimien ylikuormittuminen noudattelee käyttöpaikkojen ja jakelumuuntajien tuloksia. Prosentuaalisesti johtimista ylikuormittuu ainoastaan 1,6 % sähköautojen nopean latauksen hyökkäysskenaariossa, mikä on huomattavan vähän jakelumuuntajiin verrattuna. Lähes kaikki ylikuormitetut johdot ovat pienjännitejohtoja. Ainoastaan muutamia keskijännitejohtimia ajautui ylikuormaan.




Kuva 8. Ylikuormitettujen johtimien lukumäärät.

# 5. Johtopäätökset

## 5.1 Kyberhyökkäyksen vaikutukset sähköjärjestelmälle

Loppupäätelmänä voidaan todeta, että kotiautomaation kyberturvallisuuden haavoittuvuudet luovat merkittävän riskin sähköjärjestelmälle. Riski on suurin käyttöpaikoissa eli kotiautomaation omistajille itselleen. Tämän riskin kohoaminen edellyttää ainoastaan yhden kotiautomaation kaappausta ja siten se on toteutettavissa hyvinkin vähäisillä hyökkäysresursseilla. Projektissa huomattiin myös, että testatuissa kotiautomaatiolaitteistoissa oli merkittävän paljon tietoturvahaavoittuvuuksia, joita käyttäen hyökkääjä voisi saada laitteiston käyttöönsä. Seuraukset voivat olla suhteellisen merkittäviä kotiautomaation omistajalle esimerkiksi kiinteistön jäätyessä tai sähkönkulutuksen kustannusten kasvaessa pidemmällä aikavälillä. Pienempää harmia aiheuttavat lämpimän käyttöveden puuttuminen tai sähköauton lataamattomuus.

Riski paikalliselle jakeluverkolle on myös erittäin merkittävä, kun kotiautomaation soveltaminen laajenee lämpöpumppujen ja sähköautojen käyttöönoton myötä. Kotiautomaatio ei välttämättä tarkoita näissä yhteyksissä erikseen ostettavaa automaatiolaitteistoa ja -järjestelmää, vaan kotiautomaatio otetaan käyttöön huomaamattomasti lämpöpumppujen ja sähköauton latauksen etäohjauksen kautta. Nämä ovat yleisesti yhteydessä valmistajan pilvipalveluihin, mitä kautta laajamittainen hyökkäys tulee mahdolliseksi. Sähkönjakeluverkon haittavaikutusten kannalta onkin oleellista kuinka laajamittaisena ja kohdennettuna hyökkäys voidaan toteuttaa. Verkostovaikutusten kannalta eroja syntyy, kun manipuloinnin kohteena on 10, 100 tai 1 000 kulutuskohdetta, ja ovatko nämä kohteet saman pienjänniteverkon alueella, yhden verkkoyhtiön alueella vai hajallaan ympäri Suomea.

Suurimmat haittavaikutukset sähkönjakeluverkoissa saadaan aikaiseksi kolmivaiheisen sähköautojen latauksen kautta. Poiketen monista aikaisemmista sähköautojen lataustarkasteluista, nämä analyysit eivät tuota yhtä dramaattisia lopputuloksia normaalitilanteen osalta, vaikka jakeluverkon ylikuormittumista ja alijännitteitä yleisesti esiintyykin. Tämä johtuu pitkälti valitusta mallinnustavasta, jolla erityisesti sähköautojen kolmivaihelataus on analysoitu, johtaen merkittävästi suurempaan risteilyyn asiakkaiden välillä.

Laajamittaisen kyberhyökkäyksen vaikutukset sähkönjakeluverkossa konkretisoituvat ehkä selkeimmin jakelumuuntajien ylikuormittumisen kohdalla. Laajamittainen sähköautojen käyttöönotto johtaa jossain määrin sähkönjakeluverkon vahvistustarpeisiin jakelumuuntajien

ylikuormittumisen myötä. Normaalitilanteessa ylikuormittuneita jakelumuuntajia on 2,3 % muuntajista, mutta yli 130 %:n ylikuormassa on ainoastaan 0,3 %:a jakelumuuntajista. Jos oletetaan, että ylikuormittumiset tapahtuisivat talviaikaan, niin jakelumuuntajien vahvistustarve johtuen sähköautojen latauksesta on hyvin vähäinen haja-asutusalueella, jossa muuntajat ovat pääasiassa pylväissä tai eristämättömissä kopeissa. Laajamittaisen kyberhyökkäyksen vaikutuksesta latauskuormien risteily kuitenkin häviää ja kaikki verkkoon kytketyt sähköautot kuluttavat sähköä samanaikaisesti. Tällöin 26 %:a jakelumuuntajista päätyy ylikuormaan ja yli 130 %:nkin ylikuormassa on 15 %:a jakelumuuntajista.

Jos laajamittainen kyberhyökkäys onnistuu tuhoamaan merkittävän määrän ylikuormaan joutuneista jakelumuuntajista, niin verkkoyhtiön tai urakoitsijan varastossa olevat jakelumuuntajat eivät tule riittämään tuhoutuneiden muuntajien korvaamiseksi. Lisäksi muuntajien vaihtotyö vie merkittävän määrän aikaa, vaikka urakoitsija onnistuisikin löytämään lisäresursseja vaihtotyöhön. Tämän seurauksena sähkönjakelun jatkuvuus on erittäin merkittävästi vaarantunut laajalla alueella. Vaikka laajamittaisen ja onnistuneen kyberhyökkäyksen todennäköisyys olisi erittäin pieni, niin kokonaisriski verkostovaikutusten kautta kasvaa merkittävän suureksi. Kyberhyökkäys muodostaakin uuden suurhäiriöriskin sähkönjakelun jatkuvuudelle, mikä tulisi huomioida sähkönjakeluverkkojen kehittämisessä sääilmiöiden aiheuttaman suurhäiriöriskin rinnalla.

## 5.2 Kyberhyökkäyksen vaikutusten pienentäminen

Kyberhyökkäyksen jänniteongelmia voidaan poistaa asentamalla lämpöpumppuihin ja sähköautojen latauksen yhteyteen paikallisesti mitattu jännitteestä riippuva logiikka (esimerkiksi älymittarin HAN-portista saatava tieto). Kun jännite laskee valitun rajan alle, alkaa kyseinen laite automaattisesti rajoittamaan tehoaan sitä enemmän mitä alhaisempi jännite on (droop-säädön periaate). Vastaavaa toimintoa sovelletaan jo hajautetulle tuotannolle vaarallisten ylijännitteiden varalta alentamalla tuotantotehoa ennen kuin jänniterele kytkee koko tuotantolaitteen eroon verkosta. Jänniteraja tulisi asettaa niin alhaiseksi, ettei sitä rikota normaalitilanteessa edes poikkeuksellisten keskijänniteverkon kytkentätilanteiden aikana. Tällä tavoin voitaisiin kuitenkin kustannustehokkaasti lieventää kyberhyökkäyksen vaikutuksia erityisesti haja-asutusalueen jakeluverkoissa.

Samaa logiikkaa voidaan soveltaa myös ylikuormittumisen estämiseen käyttöpaikan osalta. Käyttöpaikan virran ylittäessä pääsulakkeiden nimellisvirran tehoa rajoitettaisiin esimerkiksi

sähköauton latauksen osalta. Logiikan toteuttaminen suuntaajissa on edullisinta, koska erillistä laitteistoa tätä varten ei tarvita. Periaatteessa ohjaus voitaisiin toteuttaa myös vaihekohtaisesti, mikä edellyttää tietoa mihin vaiheeseen ohjattavat laitteet ovat kytkeytyneet. Älymittarin HAN-portin kautta saatavien tietojen perusteella suuntaajassa oleva logiikka voi tämän kuitenkin päätellä tarkkailemalla itsensä aiheuttamia muutoksia älymittarin mittaamassa vaihekohtaisessa kokonaisvirrassa.

Jakeluverkon ylikuormittumisen osalta kokonaiskuvan saaminen älymittarin tietojen pohjalta ei ole kuitenkaan mahdollista. Esimerkiksi tieto jakelumuuntajan ylikuormittumisesta voitaisiin kuitenkin välittää älymittarille ulkopuolisena tietona, jonka perusteella kulutuslaitteen tehoa hallittaisiin. Tieto jakelumuuntajan ylikuormittumisesta voidaan saada mittaamalla itse jakelumuuntajaa esimerkiksi toisella älymittarilla ja jakamalla tämä tieto kaikille kyseisen pienjänniteverkon älymittareille. Toinen vaihtoehto, jolla voidaan tunnistaa myös johtimien ylikuormittuminen, on hyödyntää tilaestimointia. Jakeluverkon ohjatessa kulutuslaitteita ylikuormitustilanteissa, tulee ylikuormittumisen olla selkeää ja päätoiminto olla sähköjakelun jatkuvuuden turvaamisessa esimerkiksi jakelumuuntajan tuhoutumisen välttämiseksi.

Esitetyt keinot ovat varautumista kyberhyökkäyksen verkostovaikutuksia ajatellen. Kokonaisuuden kannalta tehokkaampaa olisi toki suunnitella ja ylläpitää kotiautomaatiota siten, että kyberhyökkäyksen toteutuminen on mahdollisimman harvinaista. Tämän toteuttamiseksi kotiautomaation kyberturvallisuuden kokonaisvastuuta on siirrettävä loppukäyttäjiltä kyseisten laitteiden ja järjestelmien toimittajille, joilla on riittävä kyky ja resurssit kyberturvallisuuden ylläpitämiseksi. Hyökkäyksen onnistumista ei käytännössä voida kuitenkaan täysin poissulkea, joten varautumiskeinot verkostovaikutusten osalta ovat myös tarpeen. Samoja varautumiskeinoja voidaan hyödyntää toki myös normaalitilanteessa esiintyvien poikkeustilanteiden kuten 23.11.2023 virheellisen sähköpörssitarjouksen seurauksena syntyneiden pitkäkestoisten negatiivisten pörssihintojen ja kulutuspiikkien varalta.

# Lähteet

[1] Muhammad Hamza, Impacts of cyberattack through home automation system on Finland's frequency reserve markets, medium & low voltage networks in south Savo Finland, and individual customers, diplomityö, Tampereen yliopisto, 2024. https://urn.fi/URN:NBN:fi:tuni-202407107583

[2] Koivu, A. The threat of a home automation botnet and its impact on the power grid. Master thesis. LUT University 2023. https://urn.fi/URN:NBN:fi-fe2023061956332

[3] Huang, B., Cardenas, A. A. & Baldick, R. 2019. Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks. Proceedings of the 28th USENIX Security Symposium. Santa Clara, CA, USA. p. 1115 – 1132.

[4] Shekari, T., Cardenas, A. A. & Beyah, R. 2022. MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. Proceedings of the 31st USENIX Security Symposium. Bostan, MA, USA. p. 3539 – 3556.

[5] Shekari, T., Irvene, C., Cardenas, A. A. & Beyah, R. 2021. MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. ACM digital library. CCS '21: Proceedings of the 2021 ACM SIGSAG Conference on Computer and Communications Security. p 1338 – 1356.