**TUTKIMUSRAPORTTI**

VTT-CR-08759-13

# AMM Tietoturva


| | |
|---|---|
| Kirjoittajat: | Pekka Savolainen, Pekka Koponen, Sami Noponen, Janne Sarsama, Jyri Toivonen |


| | |
|---|---|
| Luottamuksellisuus | Julkinen |
| Versio | V1.0 |

| | |
|---|---|
| **Raportin nimi**<br>AMM - Tietoturvaselvitys | |
| **Asiakkaan nimi, yhteyshenkilö ja yhteystiedot**<br>Sähkötutkimuspooli,<br>Sähkötutkimuspoolin asiamies Sirpa Leino,<br>asiakkaan yhteyshenkilö projektissa Osmo Auvinen | **Asiakkaan viite** |
| **Projektin nimi**<br>AMM Tietoturva | **Projektin numero/lyhytnimi**<br>81893 |
| **Raportin laatija(t)**<br>Pekka Savolainen, Pekka Koponen, Sami Noponen, Janne Sarsama, Jyri Toivonen | **Sivujen/liitesivujen lukumäärä**<br>56/ |
| **Avainsanat**<br>tietoturva, älykäs kulutusmittaus, luentajäjärjestelmä, sähkön etäluenta, älymittari, tuntimittaus, kyberturvallisuus | **Raportin numero**<br>VTT-CR-08759-13 |

**Tiivistelmä**

AMM (Automatic Meter Management ) Tietoturva -projektissa tutkittiin sähkön kulutustiedon etäluentaratkaisujen tietoturvaa. Lainsäädännön ohjaamana vuoden 2013 loppuun mennessä vähintään 80% sähkön kulutuslukemista luetaan Suomessa etäluentajärjestelmän avulla. Muutos vanhaan tapaan lukea sähkön kulutuslukemat paikallisesti on suuri. Lisäksi sähkön laatua koskevien tietojen sekä etäkytkentä- ja katkaisukomentojen välittäminen tulee mahdolliseksi. Kahdensuuntainen tietoliikenneyhteys on yksi älykkäiden sähköverkkojen tärkeimpiä ominaisuuksia, mutta se tuo mukanaan myös uudenlaisia tietoturvauhkia. Etäluennan ja -hallinnan järjestelmät koostuvat itse mittareiden lisäksi useista tietojärjestelmistä ja tiedonsiirtoverkoista, ja verkkoyhtiöiden toteutukset ovat yksilöllisiä. Tämä lisää tilanteen haasteellisuutta, kuten myös se, että sopijaosapuolia ja on paljon ja toimitusten alihankintaketjut voivat olla pitkiä ja ulottua valtiorajojen yli.

Projektin tutkimuskohteena olivat mukana olleiden yritysten AMM-ratkaisut, ja myöskin kansainvälinen tutkimus ja standardointi on otettu huomioon. Etäluentajärjestelmän eri osien tietoturvauhkia on käyty läpi projektin osapuolten kanssa järjestetyissä yksilöllisissä työpajoissa

Etäluentajärjestelmiin liittyvien standardien, vaatimusten ja suositusten kehitysnäkymiä on tarkasteltu Euroopan Komission smart grid- ja AMM-järjestelmiin kohdistuvien tavoitteiden ja maakohtaisten esimerkkien kautta. Raportissa esitellään AMM-järjestelmien tietoturvauhkien käsittelyn yhteydessä esiin nousseita keinoja ja mahdollisuuksia, joiden huomioinnilla alan toimijat voivat soveltuvin osin parantaa omien järjestelmiensä tietoturvallisuutta.

Vakavia, helposti hyödynnettäviä tietoturva-aukkoja ei projektin puitteissa etäluentajärjestelmäratkaisuista havaittu. Julkisuuteen, tai projektin osapuolten tietoon ei ole tullut nykyisenkaltaisiin AMM-järjestelmiin kohdistuneita onnistuneita tietoturvahyökkäyksiä Suomessa. Projektissa järjestetyssä suuressa työpajassa arvioitiin erityyppisten etäluentaan liittyvien riskiskenaarioiden todennäköisyyttä ja vakavuutta. Skenaarioista ei ryhmän arvioinnin perusteella löytynyt yhtään sellaista, joka olisi ollut yhtä aikaa esiintymistaajuudeltaan yleinen tai erittäin yleinen ja taloudellisilta seurauksiltaan erittäin vakava tai katastrofaalinen. Merkittävimpinä uhkina pidettiin kulutus –ja asiakastietojen vuotamista kulutustietoa tarjoavilta www-palvelimilta, sekä laajamittaista mittareiden ohjelmiston etäpäivityksen epäonnistumista.

| | |
|---|---|
| **Luottamuksellisuus** | Julkinen |

Oulu, 11.12.2013

| **Laatija** | **Tarkastaja** | **Hyväksyjä** |
|---|---|---|
| Pekka Savolainen<br>projektipäällikkö | Pasi Ahonen<br>erikoistutkija | Projektin ohjausryhmä<br>päätöskokous 6.11.2013 |

**VTT:n yhteystiedot**
Projektipäällikkö Pekka Savolainen, etunimi.sukunimi@vtt.fi, tel. +358 20 722 2489

| **Jakelu (asiakkaat ja VTT)** |
| --- |
| Tilaaja, VTT ja muu jakelu. |
| *VTT:n nimen käyttäminen mainonnassa tai tämän raportin osittainen julkaiseminen on sallittu vain VTT:ltä saadun kirjallisen luvan perusteella.* |

# Alkusanat

Sähkötutkimuspoolin VTT:ltä tilaaman AMM Tietoturva-projektin tavoitteeksi asetettiin selvittää kokonaisvaltaisesti AMM-järjestelmiin (Automatic Meter Management) vaikuttavat tietoturvariskit verkkoyhtiöille ja muille projektin osapuolille sekä esittää järjestelmien kehittämistarpeet joita edellytetään, jotta loppukäyttäjille voidaan taata riittävän turvallinen ja luotettava palvelu.

Selvityksen lähtökohtana on vallitseva tilanne kotimaisissa verkkoyhtiöissä. Valtioneuvoston 2009 antaman asetuksen mukaisesti vuoden 2013 lopussa vähintään 80%:lla jakeluverkkojen asiakkaista tulee olla viestintäverkon kautta etäluettavissa ja etäohjattavissa oleva kulutetun energian tuntimittauslaitteisto. Pääosa Suomessa käytössä olevista sähkömittareista on jo nyt vaihdettu uusiin, asetuksen mukaisiin mittareihin. Samalla on rakennettu etäyhteydet käyttöpaikoille ja uudistettu luenta- ja ohjausjärjestelmät, sekä rakennettu liitännät muihin järjestelmiin kuten mittaustieto- ja taloustieto- ja asiakastietojärjestelmiin. Tämän kokonaisuudistuksen nykyvaiheessa verkkoyhtiöt hyödyntävät uusien, älykkäiden mittareiden mahdollisuuksia tasehallinnassa, laskutuksessa, kulutustietojen välittämisessä loppuasiakkaalle, etäkytkennässä ja etäkatkaisussa sekä kuormanohjauksessa. Älymittareita voidaan hyödyntää myös verkon valvonnassa ja vianhallinnassa.

Toiminnan tieto- / kyber-turvallisuutta ja tietoturvahaasteita selvitettiin projektiosapuolien kanssa järjestetyissä työpajoissa, niin verkkoyhtiöiden vaatimusten ja vastuiden kuin palveluntarjoajien nykyratkaisujen ja kehitysnäkymien kannalta. Palveluntarjoajat edustivat mittarinvalmistajien ja mittarien luenta- ja hallintapalveluiden sekä järjestelmäintegraattoreiden näkökulmia. Tilannekuvaa vahvistettiin Kaupunkiyhtiöt-yhteenliittymän jäsenille suunnatulla AMM-järjestelmien käyttöä ja kehitysnäkymiä selvittävällä kyselyllä. Selvitystyön taustaaineistona perehdyttiin tutkimustuloksiin, joita on julkaistu AMR-, AMI- ja AMM-järjestelmien suunnittelusta, rakenteesta ja toiminnasta, erityisesti järjestelmien tietoturvallisen toiminnan kannalta. Tilannekuvan yhteen vetämiseksi ja kommunikoimiseksi projektin kaikille osapuolille järjestettiin projektin lopussa työpaja, mihin kukin osapuoli sai kutsua myös läheisimpien sidosryhmiensä edustajia.

Yleismaailmalliset trendit, mittausteknologian kehittyminen ja energiatehokkuustavoitteet tulevat vaikuttamaan AMM-järjestelmien kehityssuuntaan myös Suomessa. AMM-järjestelmiin liittyvien standardien, vaatimusten ja suositusten kehitysnäkymiä on tarkasteltu Euroopan Komission smart grid- ja AMM-järjestelmiin kohdistuvien tavoitteiden ja maakohtaisten esimerkkien kautta. Nämä kehitysnäkymät on otettu huomioon kotimaan tilanteen tarkastelussa ja raportin lopussa esitetyissä johtopäätöksissä.

Projektin toimeksiantaja oli Energiateollisuus ry:n alaisuudessa toimiva Sähkötutkimuspooli sekä joukko yrityksiä. Projektin toteutti VTT vuoden 2013 aikana, ja toteutusta ohjasi toimeksiantajan edustajista koottu johtoryhmä, jonka kokoonpano oli seuraava:
Osmo Auvinen, Keravan Energia Oy, ST-Poolin edustaja, johtoryhmän puheenjohtaja
Anu Puhakainen, Oy LM Ericsson AB (edustaen myös Landis+Gyr Oy:tä),
Sami Pyykkö, Kamstrup A/S,
Timo Haatainen, Empower IM Oy,
Mikko Keto, TeliaSonera Finland Oyj,
Jani Karhunen, Enfo Zender Oy,
Raimo Toivanen, PKS Sähkönsiirto Oy, R4 Sähköyhtiöt edustaja,
Mika Sohlman, Aidon Oy,
Jukka Rautava, VTT.

VTT:n projektitiimin jäsenet olivat: Pekka Koponen, Sami Noponen, Janne Sarsama, Jyri Toivonen, Pasi Ahonen sekä projektin projektipäällikkö Pekka Savolainen, joka toimi myös johtoryhmän sihteerinä.

Projektitiimi kiittää johtoryhmää henkilökohtaisesta panostuksesta sekä aktiivisuudesta edustamansa yrityksen asiantuntemuksen tuomisessa projektin käyttöön. Kiitokset myös osallistujayritysten johdolle projektille osoittamistaan resursseista ja yritysten asiantuntijoille, jotka tukivat projektia työpajoihin valmistautumisessa ja antautuivat työpajoissa syvällisiinkin keskusteluihin AMM-järjestelmien toteutuksesta, järjestelmähallinnan menettelytavoista ja niiden perusteista.

# Termit ja lyhenteet

Luvussa on kuvattuna raportissa käytetyt termit ja lyhenteet. Termit on pyritty määrittämään niin, että raportin lukeminen ja ymmärtäminen olisi helppoa. Useille termeille ja lyhenteille erityisesti sähkön etäluennassa esiintyy julkisuudessa monia määritelmiä jotka voivat merkitykseltään poiketa toisistaan.

| | |
|---|---|
| 2G/3G | Toisen/kolmannen sukupolven matkapuhelinverkko. |
| AES | Advanced Encryption Standard- salausalgoritmi. |
| AMI | Advanced/Automatic Metering Infrastructure (= Smart Metering) on järjestelmäkokonaisuus, joka sisältää AMM-järjestelmän lisäksi myös sellaisia kulutuksen mittauksiin ja ohjauksiin liittyviä toiminnallisuuksia jotka palvelevat muita järjestelmiä sekä liitännät joiden kautta mittaustiedot ja AMM-järjestelmän ohjaustoiminnot ovat automaattisesti hyödynnettävissä kaikissa niitä tarvitsevissa järjestelmissä. Voidaan katsoa sisältävän myös hyödyntävien järjestelmien puoleisen osan kyseisistä liitäntärajapinnoista. |
| AMM | Advanced/Automatic Meter Management on järjestelmä joka automaattisesti lukee, ohjaa ja valvoo kulutusmittareita etätiedonsiirtoyhteyksiensä yli. Se sisältää mm. seuraavia toiminnallisuuksia: kulutusmittausten etälukeminen, jännite- ja keskeytystietojen etälukeminen, etäkatkaisu ja -kytkeminen, kuorman ohjaus, mittarin asennuksen, toiminnan ja kunnon valvonta sekä asennuksen ja ylläpidon tuki. |
| AMR | Automatic Meter Reading tarkoittaa kulutusmittausten automaattista luentaa joko suoraan etälukuna mittarinlukujärjestelmään tai mittarin lähistöllä kiertävälle mittarinlukijalle esim. autoon. |
| DLMS/COSEM | Device Language Message Specification/ Companion Specification for Energy Metering. Energiankulutuksen etäluennan tiedonsiirron määrittely, jonka tärkein versio on kansainvälinen tiedonsiirtostandardi IEC 62056. Standardi määrittelee mittareille rajapintamallin ja tiedonsiirtoprotokollat sekä näiden eritasoisia tietoturvaratkaisuja. |
| DMS | Distribution Management System. Käytöntukijärjestelmä. |
| GPRS | General Packet Radio Service. Pakettikytkentäinen tiedonsiirto mobiiliverkossa. |
| KTJ | Käytöntukijärjestelmä. Käytönvalvontajärjestelmän yläpuolella toimiva sähköverkon käyttöä tukeva tietojärjestelmä. |
| KVJ | Käytönvalvontajärjestelmä (SCADA). Se on hajautetun automaatiojärjestelmän paikallisautomaation ja hajautetut toimilaitteet yhdeksi valvomosta käsin hallittavaksi kokonaisuudeksi yhdistävä automaatiojärjestelmä. |
| M-Bus | Meter-Bus. Sähkön ja kaasun etäluennan Eurooppalainen standardi. |
| PLC | Power Line Communications, sähköverkkotiedonsiirto. |
| PLAN | Sähköverkkotiedonsiirron protokolla. |
| PSTN | Public Switched Telephone Network. Kiinteä puhelinverkko. |
| SCADA | Supervisory Control and Data Acquisition. Teollisuusautomaation ohjausjärjestelmä. Katso myös KVJ. |

| | |
|---|---|
| Smart Metering | ”Älykäs” mittarointi tarkoittaa järjestelmäkokonaisuutta (infrastruktuuria) joka tuottaa mittaustietoja kulutuksesta ja muista suureista ja hyödyntää niitä monipuolisesti ja automaattisesti eri tarkoituksiin. Tarkoittaa siis suurin piirtein samaa kuin AMI. |
| Smart Meter | Älykäs mittari tarkoittaa, että mittarissa on tietotekniikkaan perustuvia toiminnallisuuksia. Se, että mittarit ovat älykkäitä ei sinänsä tee mittarointia älykkääksi. Älykäs mittarointi (smart metering = AMI) toki edellyttää mittarilta tiettyjä tietotekniikkaan perustuvia toiminnallisuuksia eli myös mittarin on oltava tietyssä määrin älykäs. |
| SM-GC | Smart Metering Coordination Group |

# Sisällysluettelo

# 1. Johdanto

Nykyisiin sähköverkkoihin ollaan toteuttamassa uudistuksia, jotka parantavat sähköverkon toimivuutta ja sähkön jakelua monella tasolla. Tulevaisuuden tarpeita täyttävää sähköverkkoa kutsutaan älykkääksi sähköverkoksi (smart grid). Sähkön mittaustiedon etäluenta on yksi älykkäisiin sähköverkkoihin liittyvistä uusista merkittävistä ominaisuuksista.

Suomi on ensimmäisten maiden joukossa maailmassa toteuttamassa laajamittaista siirtymistä tuntipohjaiseen kulutusluentaan lainsäädännön ohjaamana. Sähkömarkkinalain mukaan verkonhaltijan on järjestettävä verkossaan sähköntoimitusten mittaus, rekisteröinti ja ilmoittaminen sähkömarkkinoiden osapuolille. Valtioneuvosto antoi yleisistunnossaan helmikuussa 2009 asetukset sähkömarkkinoista sekä sähkötoimitusten selvityksestä ja mittaamisesta. Etäluentaan liittyvät säädökset velvoittavat sähköyhtiöt tarjoamaan asiakkailleen tuntikohtaiset sähkön kulutuslukemat ilman erillistä maksua. Sähkön myyjälle tiedot on ilmoitettava käyttöpaikka- ja mittauskohtaisesti. Asetuksen taustalla on EU:n energiapalveludirektiivi tehokkaasta energian loppukäytöstä ja energiapalveluista (2006/32/EY). Asetuksen tavoitteena on, että 80% jakeluverkkojen asiakkaista on tuntimittauksen ja mittarien etäluennan piirissä vuoden 2013 loppuun mennessä. Mittauspalvelulla on pyrittävä edistämään tehokasta ja säästäväistä sähkönkäyttöä sekä käytön ohjausmahdollisuuksien hyödyntämistä. Uusia vaatimuksia saattaa tulla uusien EU:n direktiivien, kuten 4.12.2012 annetun Energiatehokkuusdirektiivin, toimeenpanon myötä. EU:n energiatehokkuusdirektiivi 2012/27/EU tuli voimaan 4.12.2012 ja se korvaa energiapalveludirektiivin.

Mittauksen ja kysyntäjouston vaatimukset täyttävä AMM-järjestelmä (Automatic Meter Management system) edellyttää laajamittaista tiedon siirtoa mittarin ja tietojärjestelmien välillä, ml. laskutus-, ja raportointijärjestelmät. Muutos vanhaan tapaan lukea analogisen sähkömittarin lukema paikallisesti kerran vuodessa on suuri. AMM-järjestelmä koostuu useista tietojärjestelmistä, toimijoista, laitteista ja kommunikaatioväylistä. Etäluettavan mittarin ominaisuuksiin kuuluu kahdensuuntainen etäyhteys, jota käyttää useampi toimija. Etäyhteyttä voidaan käyttää mittaustietojen välittämisen lisäksi myös käyttöpaikan sähköliitännän etäkatkaisuun ja -kytkentään sekä mittarin päivityksiin ja konfigurointiin.

Etäluettavien mittareiden tietoturvakysymykset ovat herättäneet keskustelua maailmanlaajuisesti, ja myös Suomessa. Tutkimuksia aiheesta on tehty useassa maassa, ja aihetta tutkitaan edelleen laajasti. Alalta puuttuu edelleen yhtenäiset standardit ja kattava tietoturvaohjeistus.

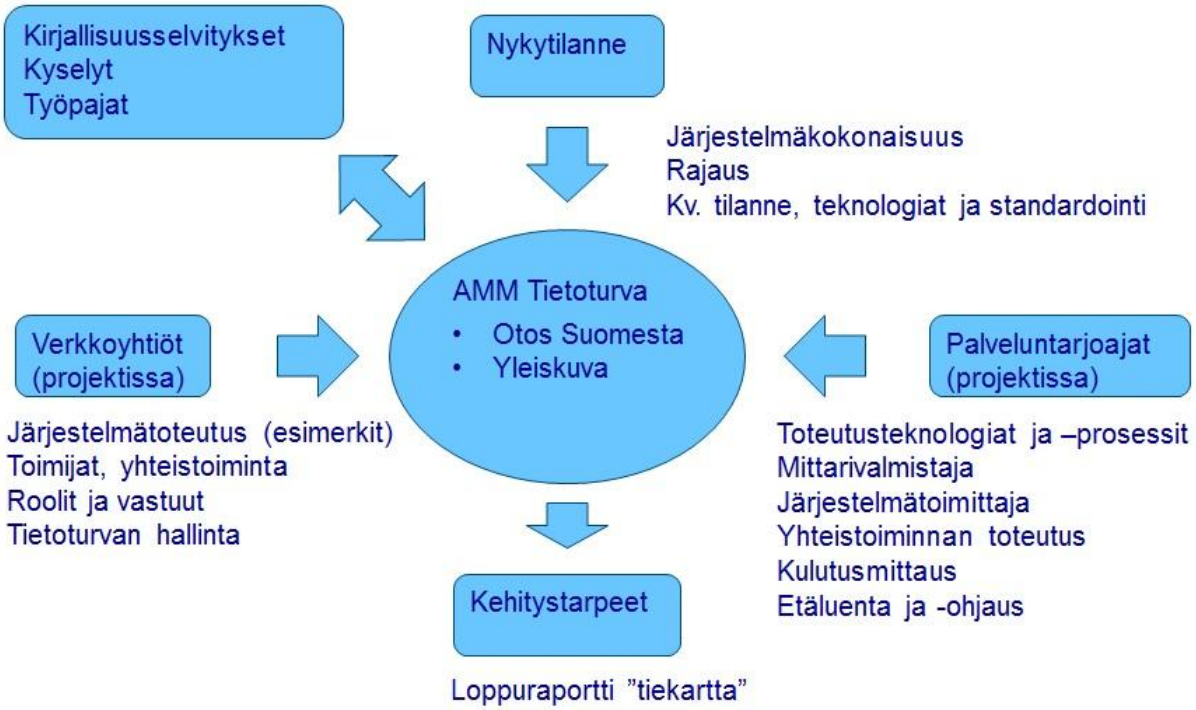
## 1.1 Projektin tavoitteet

Tämä raportti on AMM Tietoturva -projektin loppuraportti. Raportin ensisijaisena tavoitteena on kuvata suomalaisesta näkökulmasta AMM-järjestelmiin (Automatic Meter Management) liittyviä tietoturvauhkia. Tämän lisäksi raportissa esitetään AMM-järjestelmien tietoturvauhkien käsittelyn yhteydessä esiin nousseita keinoja ja mahdollisuuksia, joiden huomioinnilla alan toimijat voivat soveltuvin osin parantaa omien järjestelmiensä tietoturvallisuutta.

Raportti on tarkoitettu suomalaisten jakeluverkkoyhtiöiden ja muiden AMM-kentässä toimivien yritysten käyttöön (palvelutoimittajat, laitetoimittajat, teleoperaattorit, verkostourakoitsijat jne.). Raportti on käytettävissä esimerkiksi lähdemateriaalina toimijoiden mahdollisissa omia järjestelmiään, tuotteitaan tai palveluitaan koskevissa yksityiskohtaisissa uhka- ja riskitarkasteluissa.

Projektissa tarkasteltiin lähtökohtaisesti suomalaisten jakeluverkonhaltijoiden käyttämien AMM-järjestelmien tietoturvallisuutta kuvan 1 mukaisesti. Tällä tarkoitetaan sitä, että tarkastelun kohdetta eli AMM-järjestelmiä on lähestytty siinä muodossa millaisia järjestelmät ovat suomalaisilla toimijoilla arkkitehtuuriltaan, toiminnallisuuksiltaan ja käytetyiltä teknologioil-

taan. Raportissa ei siis kuvata AMM-järjestelmien tietoturvatilannetta yleismaailmallisesti. Kuitenkin työssä on jonkin verran tukeuduttu myös kansainväliseen alaa käsittelevään kirjallisuuteen ja standardointiin. Siihen, miten hyvin raportissa esitetyt asiat ovat linjassa laajemman kansainvälisen tilanteen kanssa, raportissa ei oteta kantaa.




*Kuva 1: Projektin osapuolet yhteistyössä*

## 1.2 Projektin rajaukset

Vaikka raportin näkökulma on Suomessa käytössä olevissa AMM-järjestelmissä, on kuitenkin huomattava, että raportti ei valitettavasti ole täysin kattava tarkastelukohteen osalta. Tämä on seurausta siitä, että raportin tausta-aineisto on vain otos toimijakohtaisista ratkaisuista koostuvasta suomalaisesta AMM-kentästä. Projektissa käsitelty ja tässä raportissa kuvattu aineisto AMM-järjestelmien tietoturvauhkista koottiin keskeisiltä osin projektin aikana tehdyissä päivän mittaisissa yrityshaastatteluissa, työpajoissa, joita projektissa pidettiin kaikkiaan 10 kappaletta (4 verkkoyhtiötä ja 6 laite- tai palvelutoimittajaa).
Työpajoissa ilmenneitä AMM:n tietoturvaan liittyviä luottamuksellisia yritys– ja valmistajakohtaisia havaintoja on käsitelty ainoastaan työpajoissa ja niitä ei ole kuvattu tässä raportissa.

Lisäksi on huomattava, että tehty tarkastelu jää AMM-järjestelmien tietoturvaan liittyvissä kysymyksissä pikemminkin uhkien tunnistamisen ja kuvaamisen tasolle, kuin että raportissa käsiteltäisiin AMM-järjestelmien tietoturvaan liittyviä tarkasti määriteltyjä riskejä. Tällä tarkoitetaan sitä, että AMM-järjestelmien tietoturvaan liittyviä ei-toivottuja asioita ja ilmiöitä ei ole analysoitu tehdyssä työssä niin yksityiskohtaisella tasolla, että niille olisi tehty varsinaista riskin suuruuden tai jopa merkittävyyden arviointia, jonka perusteella niitä voitaisiin sitten asettaa esim. suuruus- tai merkittävyysjärjestykseen. Tällainen arviointi katsottiin tässä yhteydessä epätarkoituksenmukaiseksi siihen liittyvien haasteiden vuoksi. Näistä keskeisimpiä olivat tarkastelukohteen, suomalaisten AMM-järjestelmien, laajuus ja yksittäisten ratkaisujen heterogeenisuus, liiketoimintaverkoston monitahoisuus ja monenlaiset kumppaniroolit, sekä puute sellaisista asiantuntijoista, jotka osaisivat arvottaa riskejä maanlaajuisesti. Voidaan jopa väittää, että yksityiskohtainen riskitarkastelu tässä kontekstissa olisi mielekäs vain yrityskohtaisesti toteutettuna, ei maanlaajuisesti. Riskin suuruuden ja merkityksen arviointiin

sisältyy aina elementtejä, jotka riippuvat oleellisesti toiminnan volyymista ja toiminnanharjoittajan (esim. verkkoyhtiön) arvostuksista.

Kulutusmittaustiedon laajamittainen kuljettaminen organisatorisesti keskitettyjen vaikkakin fyysisesti esimerkiksi pilvipalveluihin hajautettujen mittaustietopalvelualustojen, kuten http://energia.fi/sites/default/files/tuntimittaustiedon_avoin_palvelualusta.pdf [Lehtonen 2013], kautta on kehittymässä ja yleistymässä. Palvelualustaratkaisuja ei tässä raportissa varsinaisesti tarkastella. Avoimen palvelualustan periaate sisältää yksityisyyden suojan ja tietoturvan osalta sellaisia haasteita, että se ansaitsisi oman erillisen tarkastelunsa. Tietojen keskittäminen yhteen järjestelmään lisää mahdollisen onnistuneen tunkeutumisen vaikutuksen laajuutta ja houkuttelevuutta merkittävästi, ja tietoturvan on sekä organisaation että teknisten ratkaisujen osalta syytä olla ainakin samassa suhteessa varmempia.

Raportti ei ole – eikä ollut lähtökohtaisesti tarkoitettukaan olemaan – tieteellinen esitys sen käsittelemästä aihepiiristä. Raportti on tiettyihin rajallisiin resursseihin perustuva mutta luonteeltaan kattava selvitys AMM-järjestelmien tietoturvallisuudesta. Projektissa tämän loppuraportin lisäksi tuotettua taustamateriaalia voi tiedustella ST-Poolilta.

## 1.3 AMM - tietoturvan kehittämismalli

Tavoitteensa mukaisesti AMM Tietoturva –projekti ”selvittää kokonaisvaltaisesti AMM-järjestelmiin (Automatic Meter Management) vaikuttavat tietoturvariskit ja selventää ne verkkoyhtiöille ja muille projektin osapuolille sekä esittää järjestelmien kehittämistarpeet joita edellytetään, jotta loppukäyttäjille voidaan taata riittävän turvallinen ja luotettava palvelu”.

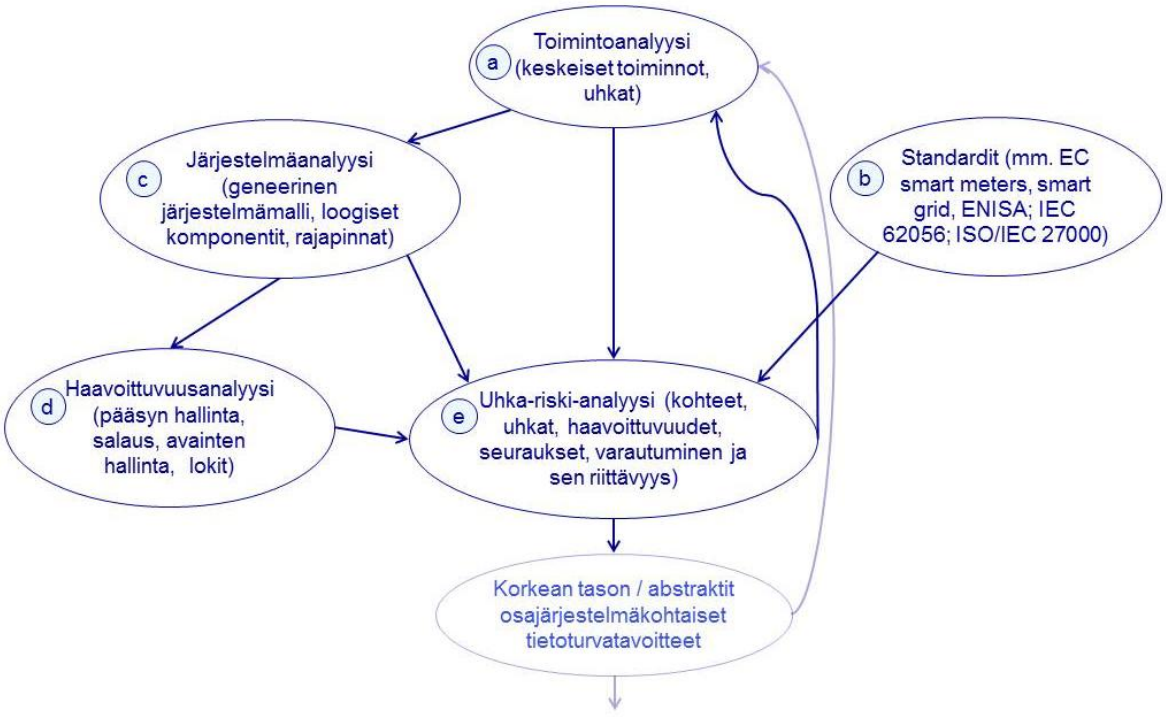
Selvityksen vaiheet on esitetty kuvassa 2. Tämän monitahoisen kohteen, Suomen AMM-järjestelmien, tietoturvariskien analysointi aloitettiin perehtymällä järjestelmän keskeisiin toimintoihin, toimijoihin, rooleihin ja toiminnan haasteisiin (viitaten Kuva 2 kohta a). Tätä varten osallistujayrityksiltä saatuja ja aiemmin omaksuttuja taustatietoja täydennettiin lähdekirjallisuudella, mukaan lukien luvuissa 2 ja 4 esitetyt liittyvien eurooppalaisten ja kotimaisten standardien ja suositusten käsittelyt (b). Yrityskohtaisissa työpajoissa käytiin läpi yritysten toimintatapoja ja analysoitiin vaihtoehtoisia toimintamalleja. Analyysissä korostettiin älymittarien ja soveltuvin osin älykkäiden sähköverkkojen (smart grid) hallinnan tietoturvan kannalta keskeisiä näkökulmia. Analyysissä kartoitettiin AMM-järjestelmien perustoiminnot ja niiden käsittelemät keskeiset suojattavat tiedot (tietovarannot, asset), sekä selvitettiin niihin kohdistuvat, yritysten liiketoiminnan kannalta olennaisiksi koetut uhkat, ja uhkiin varautumiseksi käytetyt keinot.

Toimintoanalyysin perusteella pystyttiin muodostamaan käsitteellinen malli suomalaisten AMM-järjestelmien toiminnasta (c). Käsitteellisen mallin sisältämät komponentit, osakokonaisuudet ja kommunikointirajapinnat esitellään luvussa 3.

Uhkien toteutumismahdollisuuksia selventävä haavoittuvuusanalyysi (d) keskittyy tyypillisiin heikkouksiin joita tämänkaltaisissa verkottuneissa järjestelmissä ja niiden toteutusteknologioissa ilmenee. Esimerkkejä tällaisista haasteista ovat käyttäjien tunnistus, käyttöoikeuksien mukaisen käytön valvonta ja luottamuksellisuuden säilyttäminen komponenttien välisessä kommunikoinnissa. Haavoittuvuusanalyysissä huomioidaan haavoittuvuudet niin teknisissä toteutuksissa kuin toiminnan perustana olevissa operatiivisissa ohjeissa (prosessiheikkoudet) ja henkilöstön koulutuksessa. Haavoittuvuusanalyysissä käsitteellisen mallin rajapinnat käsitellään hyökkäysrajapintoina, luvussa 5 esitetyn mukaisesti. Haavoittuvuudet näissä rajapinnoissa saattavat mahdollistaa uhkan toteutumiseen johtavan hyökkäyksen, esim. tahallisen vahingon teon, tai työntekijän aiheuttaman virhetilanteen, joka johtuu huolimattomuudesta tai asianmukaisen ohjeistuksen puuttumisesta.

Uhka-riski-analyysin perusteella luodaan kuva järjestelmän tieto-/kyber-turvallisuuden tasosta ja pyritään löytämään kohteet joita on tarpeen kehittää. Kohdan (e) uhka-riski-analyysi perustuu projektissa luotuihin järjestelmän virhetilaan johtaviin skenaarioihin, joiden perustana ovat toisaalta järjestelmään kohdistuvat uhkat ja toisaalta siinä mahdollisesti olevat haavoittuvuudet. Skenaarioiden taustalla ei ole tietty, esim. projektissa mukana ollut verkkoyhtiö ja sen AMM-toteutus, vaan ne perustuvat projektin selvityksen mukaiseen geneeriseen AMM-toteutukseen, tyypillisine uhkan toteutumisen seurauksineen ja uhkaan varautumisen keinoineen – tästä myös projektissa käytetty nimitys tyyppiskenaario. Itse analyysi riskien suuruuksien – ja siis mahdollisten kehitystarpeiden – arvioimiseksi tehtiin projektin kaikkien osapuolien yhteisessä työpajassa. Työpajassa osallistujilla oli mahdollisuus keskustella varautumiskeinoista ja uhkien konkretisoitumisen mahdollisuuksista toimitusketjun asiantuntijoiden ja muiden vastaavien järjestelmän omistajien kanssa. Analyysin lähtötiedot ja tulokset on kuvattu luvussa 5.

AMM-järjestelmien tietoturvallisuuden kehittämisen seuraavia vaiheita olisivat osajärjestelmäkohtaisten tietoturvan kehitystavoitteiden määrittäminen ja toteutuksen suunnittelu, esimerkiksi tarkemman osajärjestelmien analysoinnin ja yrityskohtaisen riskien arvioinnin perusteella. Koska toimintaympäristö ja järjestelmän tavoitteet muuttuvat ajan kuluessa, analyysi- ja kehitysprosessi on iteratiivinen.




*Kuva 2: AMM-tietoturvan kehittämismalli*

# 2. AMM-järjestelmiin liittyvä standardien, vaatimusten ja suositusten kehitys Euroopassa

Tässä luvussa esitellään eurooppalaisia AMM-tietoturvan kehitystrendejä perustuen Euroopan komission standardointitoimintaan, julkaistuihin tutkimuksiin ja tulevien AMM-järjestelmien toteutusperiaatteisiin. Tarkastelussa ovat mukana Euroopan komission AMM-järjestelmiin liittyvä standardointityö, sekä AMM-järjestelmien kehitystavoitteet ja ajankohtainen tilanne Iso-Britanniassa, Saksassa, Norjassa ja Alankomaissa. Lopuksi esitellään keskeisimpiä älykkäiden mittareiden ja älykkään mittaroinnin tietoturvallisuutta määrittäviä eurooppalaisia standardeja.

## 2.1 Euroopan komissio

### 2.1.1 Standardoinnin yleistilanne

Euroopan komissio on aktiivinen AMM-järjestelmien kehitykseen – ja yleisemmin älykkäiden sähköverkkojen (smart grid) kehitykseen – kohdistuvassa standardointityössä. Yhtenä työmuotona ovat standardointia käsittelevät konferenssit. Esimerkiksi Euroopan komission älykkäiden sähköverkkojen -standardoinnin tilannetta käsitellyt konferenssi, European Conference on Smart Grid Standardization achievements, European Commission, 28 January 2013, sisälsi myös AMM-tietoturvaa koskevia esitelmiä.

Erityisesti kaksi esitelmää käsitteli AMI-järjestelmien standardeja:

1) Common functional communications standards for smart metering systems, Daniel HEC, CEN-CENELEC-ETSI Smart Meters Coordination Group
2) Smart Metering Systems - Industry perspective, Frank Hyldmar, ESMIG – the European Smart Metering Industry Group)

Myös eräissä muita standardointihankkeita koskevissa esitelmissä oli esillä AMI-järjestelmien tietoturvaan liittyviä asioita. Esimerkiksi on mahdollista, että AMI-järjestelmille tullaan tulevaisuudessa asettamaan vaatimuksia jotka tukevat sähköautojen ohjattua latausta.

Myös kuluttajia standardien valmistelussa edustavan organisaation, ANECin (European Association for the Co-ordination of Consumer Representation in Standardisation AISBL (non-profit organisation); usein käytetään viittausta The European consumer voice in standardisation), näkökulma oli mukana. Esitelmistä kävi ilmi että useat loppuasiakkaiden näkökulmasta tärkeinä pidetyt kulutusmittausjärjestelmien ominaisuudet liittyvät tietoturvaan:

- Asiakkaan tulisi päästä helposti käsiksi AMI-järjestelmien tuottamaan dataan ja mahdollistamiin uusiin palveluihin.
- Myyjän vaihdon tulee olla helppoa.
- Datan tulee olla täysin suojattua ja yksityisyyden suojan toteutua.
- Etätoimintojen väärinkäytön on oltava estetty.
- Erityisen alttiita kuluttajia on erityisesti suojeltava.
- Mittarien on oltava luotettavia, turvallisia ja tietoturvallisia.

Konferenssin esitelmät ovat saatavilla osoitteessa:

http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

### 2.1.2 M/490 eli älykkäiden sähköverkkojen standardointi

Euroopan komission älykkäiden sähköverkkojen standardoinnin Mandaatti M/490 (Smart Grid Mandate M/490.) pyrki parantamaan referenssiarkkitehtuuria, standardointiprosesseja ja yhteistyön työkaluja ja sovittamaan ne yhteensopivuutta, tietoturvaa ja yksityisyyden suojaa koskeviin uusiin vaatimuksiin. Mandaatti päättyi vuoden 2012 lopussa. Mandaattin M/490 rajaus sisältää erityisen tietoturva-tiimin ja koordinoinnin mandaattien M/441 (smart metering) ja M/468 (e-mobility) kanssa. Mandaatin M/490 ensimmäinen standardijoukko pyrkii kattamaan muun muassa myös AMI-järjestelmät ja niihin liittyvät toimistojärjestelmät sekä hajautettujen resurssien sekä kuormien ohjauksen. Havaittuja standardointiaukkoja täyttämään on jo käynnistetty toimenpiteitä. AMI-järjestelmiä näistä sivuavat mittarinlukuprotokollan CO-SEM harmonisointi sähköverkkojen hallinnan Common Information Model (CIM) standardien (IEC 61968 ja IEC 61970) ja verkostoautomaation IEC-61850 standardien kanssa sekä verkostoautomaation tietoturvastandardin IEC 62351 edelleen kehittäminen.

### 2.1.3 M/441 eli AMI-järjestelmien standardointi

Euroopan komission vuonna 2009 standardointijärjestöille CEN, CENELEC ja ETSI antama vuoden 2012 loppuun asti kestänyt mandaatti M/441 koski älykkäiden mittausjärjestelmien eli AMI-järjestelmien (Advanced Metering Inftratructure) standardoinnin ja yhteentoimivuuden kehittämistä.

Mandaatin tarkoituksena oli tukea energiatehokkuuteen pyrkivien ja energiamarkkinoita koskevien Euroopan komission direktiivien vaatimaa 80% kattavuutta älykkäiden kulutusmittarien käyttöönotossa vuoteen 2020 mennessä, mittauspisteisteiden määrällä mitattuna . Vaikka Mandaatilta M/441 pyydetyt tuotokset (Deliverables) ovat valmistuneet, jatketaan sen älykkäiden mittareiden koordinointiryhmän (Smart Meters Goordination Group) työskentelyä kyseisten standardien ylläpidossa ja päivittämisessä ja kytkettynä rinnakkaisiin standardointimandaatteihin M/490 (smat grids) ja M/468 (e-mobility).

AMI-järjestelmien käyttö kysynnän hallinnan toimintoihin kuuluu itse asiassa mandaatin M/490 alle. Kysynnän hallinta sisältää kysynnän energiatehokkuuden parantamisen sekä kysyntäpuolen ohjattavien resurssien (ohjattavat kuormat, energiavarastot ja sulautettu sähkön tuotanto) hallinnan. Tietoturvan ja yksityisyyden suojan osalta peruslähestymistapa on myös otettu älykkäiden sähköverkkojen standardoinnin koordinointiryhmältä (Smart Grid Coordination Group, M/490). Mandaatti M/441 suosittelee, että kehitetään EU referenssijoukko tietoturvan ja yksityisyyden suojan vaatimuksista älykkäille mittausjärjestelmille, eli AMI-järjestelmille, ja tutkitaan mahdollisuutta kehittää tietoturvan ja yksityisyyden suojan sertifiointimenettely.

### 2.1.4 M/441 Smart Meters Coordination Group (SM-GC)

Mandaatin M/441 Älykkäiden mittareiden koordinointiryhmä, Smart Meters Coordination Group, on laatinut teknisen raportin “Functional reference architecture for communications in smart metering systems”, jossa käsitellään myös yksityisyyden suojaa ja tietoturvaa. Yleisestä tietoturvapolitiikasta ja konsepteista esitetään seuraavat periaatteet:

- tietoturva tulee nähdä päästä päähän (end-to-end) -ominaisuutena joka kattaa järjestelmän, prosessit ja ihmiset; tietoturvaa ei siis niinkään tulisi tarkastella yksittäisten komponenttien puitteissa
- tietoturva täytyy suunnitella järjestelmäarkkitehtuurin tasolla eikä vasta jälkikäteen tehtävänä lisäyksenä
- AMI-tietoturva kytkeytyy läheisesti sekä älykkäiden sähköverkkojen että kotiautomaation tietoturvaan
- tietoturvan toteutuksen on oltava helposti laajennettavissa, eli skaalautuva

- järjestelmää tulee kehittää jatkuvasti koko elinkaaren ajan ja varautua uusien uhkien kehittymiseen
- järjestelmiä tulee säännöllisesti testata.

Raportti on saatavissa osoitteessa:
ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartMeters/CEN-CLC-ETSI-TR50572%7B2011%7De.pdf.

Mandaatin M/441 vuoden 2012 loppuun mennessä syntyneet tulokset kerrotaan raportissa ”Introduction and Guide to the work undertaken under the M/441 mandate
A report by the CEN-CENELEC-ETSI Smart Meters Coordination Group at end 2012”.

Raportti on saatavissa osoitteessa:
ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartMeters/CENCLCETSI_SMCG_end2012.pdf

Raportin luvussa 6 kerrotaan, että on tehty erillinen raportti joka käsittelee tietoturvaa ja yksityisyyden suojaa ja että se tullaan julkaisemaan Smart Meter Coordination Groupin elektronisella alustalla, jota toimii IEC/CENELEC yhteistyötyökalulla. Tällä nähtävästi viitataan jäljempänä kuvattuun raporttiin SMCG 2, Privacy and Security approach – part I ja sen mahdollisia seuraavia osia.

Mittaroinnin teollisuusosapuolia edustavan ESMIG-järjestön näkemys mandaattien M/441 ja M/490 vuoden 2012 loppuun aikaansaamista tuloksista oli, että mandaatit ovat toteuttaneet tehtävänsä, mutta edelleen kehitettävää on standardoinnissa erityisesti seuraavissa asioissa:

1) yksityisyyden suojan ja tietoturvan vaatimusten määrittely
2) yhteensopivuuden testaus ja sertifiointi.

ESMIG on saanut työtään jatkavan älykkäiden mittarien työryhmän (SM-CG) agendalle eurooppalaisten vaatimusten kehittämisen älykkään kulutusmittauksen järjestelmille (AMI-järjestelmille). ESMIG on myös tehnyt aloitteen sertifioinnin kehittämisestä.

### 2.1.5 M/441 Smart Meters Coordination Group 2, Privacy and Security approach

Mandaatin M/441 pohjalta on tekeillä AMI-tietoturvaa käsittelevä raportti, jonka ensimmäinen osa, versio 1.00, valmistui huhtikuussa 2013 [Smart Meters Coordination Group 2, Privacy and Security approach – part I, Version: 1.0, April 2013, Task Force Privacy and Security of the Smart Meters Coordination Group, SMCG_Sec0064_DC, 25 s.]. Kyseinen raportti on saatavissa asianomaisten standardointiorganisaatioiden kautta. Raporttiin tutustumista vaikeuttaa se, että osaa raportin sisällöstä ei ole päivitetty julkaisuhetkellä ajan tasalle. Tarkastelu rajautuu SM-CG ryhmän funktionaalisessa referenssimallissa esitettyihin rajapintoihin, jotka pääpiirteissään kerrottuna kattavat mittarin, kotiautomaation, sekä AMI:n tiedonsiirtoverkkojen ja AMI-järjestelmän väliset rajapinnat. Tietoturvan kehittämisen lähestymistapa koostuu seuraavista vaiheista:

1) Vaatimusten keruu ja analysointi. Vaatimusten määrittelyn pohjana on käytetty M/441 puitteissa laadittuja yleisiä käyttötapauksia ja referenssiarkkitehtuuria.
2) Analyysi: Käyttötapauksista ja referenssiarkkitehtuurista on johdettu riskianalyysin kautta vaaditut yksityisyyden suojan ja tietoturvan tasot. Todetaan, että näin johdettujen vaatimusten perusteella voidaan joutua iteroimaan lähtökohtana olleita yleisiä käyttötapauksia.
3) Liitetään yksityisyyden suojan ja tietoturvan vaatimukset toisiinsa.
4) Analysoidaan standardoinnin puutteet ja kattavuus verrattuna vaatimuksiin.

Pyrkimyksenä ei ole tuottaa lopullisia tietoturvavaatimuksia Euroopan tasolla, vaan antaa ohjeita kuinka nämä vaatimukset määritetään ja mitkä ovat tiettyjen käyttötapausten toteuttamistapojen tekniset seuraukset. Raportissa mainitaan että seuraavissa Euroopan komission direktiiveissä on ehtoja jotka AMI-järjestelmien on täytettävä:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy.

Raportin mukaan komissio suosittelee salattujen tiedonsiirtokanavien käyttöä. Jäsenvaltioiden on otettava huomioon että älykkäiden sähköverkkojen komponenttien pitää olla eurooppalaisten standardointiorganisaatioiden tietoturvaan liittyvien standardien mukaisia. Kansainväliset standardit, erityisesti tietoturvastandardi ISO/IEC 27000 (esitelty luvussa 3) tulee ottaa huomioon. Raportti ehdottaa tutkittavaksi mahdollista sertifiointia sekä tuotteille jotka koskevat AMI-järjestelmiä että niitä kehittäville ja käyttäville organisaatiolle.

AMI-tietoturvan osalta tärkeimpinä käyttötapauksina mainitaan erilaisia avainten hallintatapoja, tietoturvan tasojen hallintaa ja salattua tiedonsiirtoa. Käyttöoikeuksien hallinnan ja sanomien suojauksen tietoturvavaatimukset perustuvat dokumenttiin NIST IR 7628 Smart Grid Guidelines for Smart Grid Cyber Security Aug 2010].

Älykkään mittaroinnin kehittämisen työryhmä CENELEC TC13 WG02 P&S on laatinut tietoturvavaatimuksista dokumentin, joka on tarkoitettu pohjaksi Eurooppalaisten referenssivaatimusten luomiselle. TC13 WG02 P&S Task force työstää salausalgoritmijoukkoa, jonka perustana on NSA (National Security Agency, USA) Suite B. Tätä varten DLMS/COSEM protokollastandardia (IEC62056) on päivitetty niin, että se tukee näitä uusia salausalgoritmijoukkoja sen nykyisen AES 128 GCM salausalgoritmijoukon lisäksi. Tämä mahdollistaa entistä paremmin osapuolten välisen päästä päähän tietojen ja sanomien suojauksen. TC205:n osalta esitetään oletus että kotien ja rakennusten energianhallintajärjestelmät olisivat suljettuja järjestelmiä ja siksi riittäisi, että niihin liittyvät älykkään sähköverkon ja AMI-järjestelmän yhdyskäytävät on tehty turvallisiksi. Lukijan näkökulmasta huolestuttavaa on, että noin tärkeä ja haastava asia ohitetaan hyvin pintapuolisesti perustellun oletuksen perusteella. Määrittelyä prEN 13757-3 kehittävä työryhmä (WG4) on todennut että se ei täytä yksityisyyden suojan ja tietoturvan vaatimuksia ja tämän johdosta vertaillut kansallisia ratkaisuja asiaan ja todennut ne keskenään yhteen sopimattomiksi, pääsemättä yksimielisyyteen siitä mitkä niistä pitäisi ottaa kyseiseen Eurooppalaiseen standardiin ja mitkä ei – kyseinen WG4 on avoin ehdotuksille. Raportissa kerrotaan myös ETSI:n AMI-tiedonsiirtoa koskevista johtopäätöksistä ja lopuksi ehdotetaan, että sitä tulevaisuudessa jatkettaisiin SM-CG:n yhteydessä.
Älykkäiden mittarien työryhmä SM-CG suosittelee että
1) vaatimusten määrittelyssä käytetään sen ehdottamaa menettelytapaa (toolbox),
2) EG2 DPIA pohjaa harkitaan käytettäväksi yksityisyyden suojan vaatimuksia määriteltäessä,
3) laaditaan Eurooppalainen referenssijoukko vaatimuksista,
4) Tekniset komiteat käyttävät näitä edellä mainittuja asioita lähtötietoinaan ja että
5) tutkitaan mahdollisia AMI-tietoturvan sertifioinnin tapoja.

SM-CG aikoo vuoden 2013 loppuun mennessä tuottaa raportin version 2, jonka on tarkoitus olla lopullinen. Raportissa tulee olemaan suosituksia tietoturvavaatimusten käytöstä sekä sertifioinnista sekä oma osionsa yksityisyyden suojasta.

### 2.1.6 DLMS/COSEM protokollan kehitys

DLMS/COSEM protokollaan on DLMS User Association (DLMS UA:n) tehnyt tietoturvaa parantavia päivityksiä verrattuna niiden aikaisempiin versioihin. ( http://dlms.com/documents/Excerpt_GB7.pdf). Lähtökohtana on käytetty määrittelyä NIST SP 800-21. Pääpiirteissään suojausta (http://dlms.com/DLMSimages/Security.pdf) on mahdollista toteuttaa monella protokollakerroksella:

> 1) Protokollat joiden päällä DLMS/COSEM protokollaa siirretään voivat olla suojaamattomia tai sisältää salauksen ja autentikoinnin,
> 2) DLMS sanoman sisältö voi olla salattu tai salaamaton ja
> 3) DLMS:n päällä siirrettävä COSEM data voi valitusta salaustasosta riippuen olla suojaamatonta, digitaalisesti allekirjoitettua, alkuperävarmistettua, salattua tai näiden yhdistelmiä.

On mahdollista käyttää molempien osapuolten tunnistusta. Myös suositeltavat suojausalgoritmit on mainittu.

## 2.2 Iso-Britannia

Iso-Britanniassa energian (eli sähkön ja kaasun) vähittäismyyjät ovat vastuussa etäluettavien kulutusmittareiden asentamisesta. Maan hallitus on päättänyt että 53 miljoonaa kaasun ja sähkön kulutusmittaria tulisi vuoteen 2020 mennessä vaihtaa uudet vaatimukset täyttäviin etäluettaviin mittareihin, ja nyt ollaan määrittelemässä niille toiminnallisia vähimmäisvaatimuksia. Tavoitteena on, että samoilla AMM-järjestelmillä luetaan sekä kaasun että sähkön kulutusmittaukset. Vaatimusmäärittelyiden alkuvaiheessa pääpaino on ollut kaasun kulutusmittauksissa. S ja sähkön kulutusmittauksia koskevat asiat ovat olleet heikommin mukana, mutta tilanne näyttäisi kuitenkin olevan nyt korjautumassa.

Department of Energy & Climate Change, DECC, (http://www.gov.uk/decc), vastaa Iso-Britannian kansallisista AMM-mittareiden vaatimusmäärittelyistä, SMETS (Smart Metering Equipment Technical Specifications), joita se kehittää yhdessä energiamarkkinaosapuolien kanssa. . Maan hallitus on heinäkuussa 2013 laatinut sen versiota 2 koskevan vastauksensa toisen osan, jonka luku 4 käsittelee tietoturvaa koskevia kysymyksiä [DECC 2013a].

Isossa-Britanniassa oli päätetty keskittää AMM-tiedonsiirto kuluttajien mittareilta kyseisten mittaustietojen käyttäjille (kaasu- ja sähköyhtiöille) yhden monopolitoimijan kautta, jota kutsutaan nimellä Data Communications Company (DCC) [DECC 2013b]. Nyt ollaan kuitenkin menossa toimintamalliin, jossa DCC-toimijoita olisi useampia, esimerkiksi kolme.

AMM-tietoturvavaatimusten ylläpitämiseksi on perustettu Smart Energy Code Panel (SEC Panel) nimisen komitean alle tekninen alakomitea, joka koostuu hallituksen, teollisuuden ja muiden asianosaisten osapuolten tietoturva-asiantuntijoista. Alakomitean tehtävinä on:

- seurata yksityisyyden suojan ja tietoturvan riskien kehittymistä
- ylläpitää AMM-järjestelmien päästä päähän riskikartoitusta identifioimalla uusia ja muuttuneita riskejä
- ylläpitää tietoturvavaatimusten määrittelyä
- ylläpitää riskien torjunnan suunnitelmaa
- auttaa DCC:tä ja DCC:n asiakkaita (sähkön ja kaasun myyjiä ja verkkoyhtiöitä) tietoturvatapahtumien syiden määrittämisessä jälkikäteen
- auttaa SEC Panelia ratkomaan teknisiä erimielisyyksiä jotka koskevat tietoturvavaatimusten toteutumista.

Alakomitea on päättänyt toteuttaa riippumattoman todentamismenettelyn sille, että tiedetään missä määrin asetetut tietoturvavaatimukset tarkasteltavassa AMM-järjestelmän osassa toteutuvat. Todentamisella saatavan serfikaatin voimassaoloaika on avoin, kaksi vuotta tai kauemmin, samoin serfikaatin menettämisestä seuraavat sanktiot, jotka määräytynevät suhteessa poikkeaman vakavuuteen ja kuluttajille mahdollisesti koituvaan haittaan. Lisäksi tullaan laatimaan täsmentävä lisämäärittely, joka kertoo millaiset ZigBee SEP ja DLMS protokollien ominaisuudet laitteiston tulee täyttää, että sertifiointi voidaan tehdä. Myös CPA – Foundation Level mukainen sertifiointi tullaan laiteille vaatimaan. Näin hyväksyttyjä laitteistoja saa käyttää toteutuksissa automaattisesti. Vaatimusmäärittelyn uusi iterointikierros on menossa tätä kirjoitettaessa.

Uuden sähkön myyjän tietoturvaa koskevat ehdot ovat olleet voimassa siirtymävaiheessa maaliskuusta 2013 alkaen, ks. https://www.gov.uk/government/consultations/smart-metering-security-risk-assessments/ [DECC 2012].

## 2.3 Saksa

Myös Saksassa tähdätään kaasun ja sähkön kulutusmittausten etäluentaan. Lähtökohtana on ollut älykkäiden kulutusmittareiden yhdyskäytävä, jonka kautta molemmat mittarit luettaisiin. Vuoden 2012 loppuun asti oli määritelty kulutuskohteessa olevaa yhdyskäytävää, josta eri osapuolet voivat suoraan hakea kulutustiedot etätiedonsiirtoyhteyden yli. Vastaavia ratkaisuja on suunniteltu aiemminkin, mutta yhdyskäytävät on todettu kalliiksi ja tietoliikenneyhteyden hallinnan ja tietoturvan kannalta haasteelliseksi ratkaisuksi. Vuosien 2012 ja 2013 vaihteessa Saksassakin ilmeisesti havaittiin, aiempien muualla saatujen kokemusten mukaisesti, että näitä ongelmia ei kyetä tyydyttävästi ratkaisemaan, koska Saksa siirtyi malliin, jossa vain yksi osapuoli liikennöi yhdyskäytävälaitteen kanssa ja hallinnoi sitä. Vielä ei ole saatu tarkempia määrittelyjä Saksan uudesta konseptista, mutta määrittelyjen ja vaatimusten tilanteesta aivan vuoden 2012 lopussa on julkista tietoa saatavissa.

Valmistelutyöhön liittyen, [Fries 2013] kertoo älykkäiden sähköverkkojen tietoturvavaatimusten määrittelystä, markkinarooleista ja standardeista (luku 4), sekä viranomaisvaatimuksista ja ohjeista. Erityisesti kohdassa 4.1.2. kerrotaan saksalaisesta älykkäiden mittareiden tietoturvaprofiilista (German BSI Smart Meter Protection Profile).

Profiili määrittää tietoturvavaatimukset älykkään mittarin yhdyskäytävälle, kuten etäkäytön oikeuksien hallintamekanismit, mitatun datan oikeellisuuden ja alkuperäisyyden tarkistusmenettelyt sekä tiedonsiirron päästä päähän salaus. Tekninen ohje TR 03109 määrittelee toteutusvaatimukset em. profiilin mukaisen järjestelmän toteutukselle, mukaan lukien käytettävät tiedonsiirtoprotokollat ja salausalgoritmit. Saksan uusi energiateollisuutta koskeva lainsäädäntö (EnWG) edellyttää profiilin käyttöä asiakkailla joiden kulutus on yli 6 MWh vuodessa. Yksityiskohtaisesti profiilin ja teknisen ohjeen yksityiskohdista kertoo [von Oheimb 2012], arvioiden myös niiden vahvuuksia ja heikkouksia. Vahvuuksina julkaisu mainitsee seuraavat:

- selkeät tietoturvavaatimukset älykkään mittarin yhdyskäytäville
- vahva vakuus älykkään mittauksen kriittisten komponenttien osalta
- vahva kansallinen standardi joka takaa yhteensopivuuden.

Julkaisu kertoo myös joukon merkittäviä heikkouksia, joita eritellään paperissa yksityiskohtaisesti:

- tietoturva-arkkitehtuurin yksipuolisuus, pelkästään älykkään mittarin yhdyskäytäviltä vaaditaan raskaita tietoturvamekanismeja
- raskas tekninen kuormitus: monta suojauskerrosta, täysi julkisen avaimen salausinfrastruktuuri, pakollista käyttää erityistä tietoturvalaitemoduulia, P2P yhteys käyttäen TLS protokollaa

- yhdyskäytävälaitteen korkeat yksikkökustannukset johtuen suuresta määrästä vaativia tietoturvapiirteitä
- korkeat järjestelmän ylläpidon ja käytön kustannukset erityisesti julkisen avaimen palveluiden takia
- klassinen julkisen avaimen menetelmä tuo kriittisen keskitetyn haavoittuvuuskohdan, jossa onnistunut tunkeutuminen voi aiheuttaa merkittävää vahinkoa
- profiili jättää hyvin vähän vapauksia ratkaisujen suunnittelijoille
- Tietoturvamoduulin HSM (Hardware Security Module) integraatio ei ole turvallinen sen suunnittelun heikkouksista johtuen
- vaatimukset estävät tehokkaan ajantasaisen tiedonsiirron (= isot tiedonsiirtoviiveet)
- palvelunestohyökkäyksiltä suojautuminen on unohdettu.

Saksalainen standardi DIN SPEC 27009 (Guidance for information security management of power supply control systems based on ISO/IEC 27002) hyväksyttiin lokakuussa 2012 kansainväliseksi standardiksi ISO 27019. Standardi perustuu osittain tietoturvaa koskevaan määritykseen BDEW – Bundesverband Energie- und Wasserwirtschaft, Datensicherheit, http://www.bdew.de/bdew.nsf/id/DE_Datensicherhei [Fries 2013, luku 4.3.3].

## 2.4 Norja

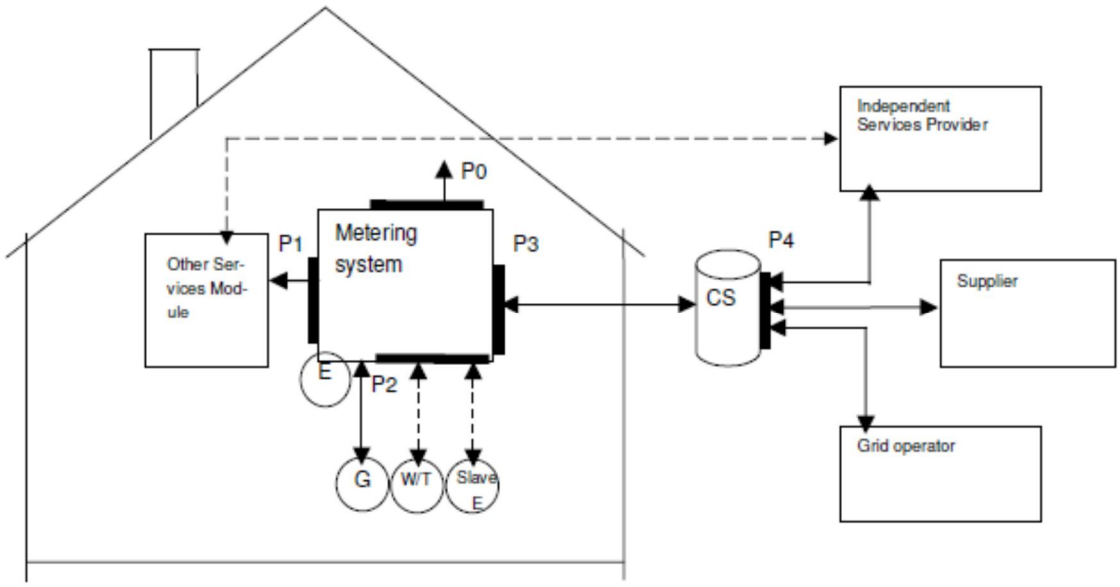
Norjalaiset ovat selvittäneet tietoturvauhkia AMI-järjestelmän demonstraatioprojektissa [Sintef, 2012]. Selvitys kohdistuu tiettyyn AMI-konfigraatioon yleisellä tasolla, menemättä järjestelmätoimittajakohtaiselle tasolle. Tarkastellussa AMI-järjestelmässä mittarit liittyvät keskittimeen Mesh-radioverkkoa käyttäen, ja keskittimen ja lukujärjestelmän välillä käytetään GPRS-tiedonsiirtoa.

Selvitys identifioi uhkia ja arvioi haavoittuvuuksiin vaikuttavia tekijöitä sekä hyökkääjän tavoitteita ja strategioita. Selvitys ei laita uhkia tärkeysjärjestykseen eikä ehdota torjuntakeinoja. Raportissa ei esitetä varsinaista riskianalyysiä, koska se ei ole järjestelmätoimittajien ja verkkoyhtiön kanssa tehtyjen salassapitosopimusten puitteissa mahdollista. Selvityksen lopuksi todetaan, että pelkkä uhkien tunnistaminen on vasta ensimmäinen askel ja sen lisäksi tarvitaan päätöksiä ja toimenpiteitä.

## 2.5 Alankomaat

Alankomaissa etäluettavien älykkäiden kulutusmittareiden laajamittaista asennusta on jouduttu lykkäämään, koska kuluttajien edustajia ei oltu valmistelussa kuultu ja koska tietoturvavaatimuksiin, erityisesti yksityisyyden suojaan [Cuijpers 2013] oli kiinnitetty liian vähän huomiota. Jonkin verran uusia kulutusmittareita on asennettu silti myös aikajaksolla 2012- 2013. Vuonna 2014 on tarkoitus alkaa täysimittakaavainen etäluettavien kulutusmittareiden asennus. Erityisesti kuluttajataho on ollut huolissaan yksityisyyden suojan riittävästä turvaamisesta. Siten tietoturvan ja yksityisyyden suojan vaatimusmäärittelyjä haluttiin vielä tarkastella tarkemmin.

Mittareiden vaatimuksia [DSMR 2011 ja DSMR 2012] (Dutch Smart Meter Requirements) tarkennettiin erityisesti tietoturvan osalta huomattavasti. Kyseisen vaatimusmäärittelyn luvussa 4 (s. 49-56) käsitellään käyttöoikeuksien hallintaa ja tietoturvaa. Erikseen on listattu ja eritelty 24 vaatimusta jotka ovat verraten konkreettisia ja selkeitä. Monista niistä viitataan seuraavassa kuvassa esitettyihin rajapintoihin. Muissakin luvuissa on välillisesti tietoturvaan vaikuttavia vaatimuksia.




*Kuva 3: Hollantilaisen DSMR vaatimusmäärittelyn määrittämät rajapinnat*

Alla määrittelyn [DSMR 2011] tietoturvaa koskevia vaatimuksia:

1. Avaamatta mittarin kantta ei ole pääsyä muihin rajapintoihin kuin P0 ja P1, jotka kuvan 1. mukaisesti periaatteessa siirtävät tietoa pelkästään mittarista poispäin. Jotkut mittarivalmistajat tosin käyttävät rajapintaa P0 mittarin konfigurointiin ja ylläpitoon.
2. Kannen avaamisesta pitää tulla tapahtuma tapahtumalokiin. Pitää riittävästi huolehtia että väärät hälytykset estetään.
3-4. Mittarien rakenteen pitää olla sellainen, että murtautumisesta jää jälki.
6. Rajapinnoissa P0 ja P3 pitää olla käyttöoikeuksien hallinta (autentikointi) jotta voidaan tunnistaa tiedonsiirron osapuolet ja estää luvattomien osapuolten pääsy muuttamaan tietoja. Autentikointimekanismi voi sisältyä salausalgoritmiin tai erillisesti perustua yksilöllisiin käyttäjätunnukseen ja salasanaan.
7. P0 rajapinnan käyttö on voitava mittarin konfiguroinnilla estää tai sallia sen mukaan tarvitaanko sitä vai ei.
8. P3 rajapinnan käyttö on voitava konfiguroinnilla rajata HLS käyttöoikeuksien hallinnan (authentication) mekanismiin 5 eli estää sitä heikompien käyttöoikeuksien hallintamekanismien käyttö.
9. Käyttöoikeudet on hallittava mittarin loogisten komponenttien ja niiden attribuuttien tasolla. (Eli on oltava mahdollista tarkkaan rajata mitä käyttäjät voivat tehdä.)
11. Kaikki tarpeettomat rajapinnat pitää voida poistaa käytöstä.
12. Rajapintojen pitää hylätä virheelliset tai ilman käyttöoikeutta lähetetyt sanomat ja AMM-järjestelmän toiminta ei saa niistä mitenkään häiriintyä.
13. Käyttämättömien fyysisten rajapintojen on oletusarvoisesti oltava pois päältä, eli niiden käyttöönottaminen vaatii rajapinnan avausmekanismin käyttöä.
14. Kaikki verkkoyhtiön käyttämät avaimet on voitava vaihtaa joko paikallisesti portin P0 kautta tai etäyhteyden yli portin P3 kautta. Poikkeuksena on master-avain, joka yksinään ei mahdollista ohjelmistojen, asetusten, lukemien yms. muuttamista. Näin vääriin käsiin joutuneen avaimen aiheuttama vahinko saadaan pieneksi.
15 Avainten jakelun on oltava mahdollisimman nopeaa.
16. Väärällä avaimella tehty kytkeytymisyritys johtaa kyseisen portin lukkiutumiseen 10 sekunnin ajaksi. Yrityksestä on lisäksi jäätävä jälki tapahtumalokiin.
17. Yhteen laitteeseen tunkeutumisen ei pidä antaa esteetöntä pääsyä useisiin laitteisiin.

18. Mittaustietojen, avainten, ohjelmistojen ja kovon oikeellisuuden säilyttämiseksi on oltava tietoturvamekanismit.
19. Oikeellisuuden menetyksestä on tultava raportti ja lokimerkintä.
20. Mittarin konfiguroinnin muutoksista on jäätävä tieto tapahtumalokeihin.
21. Toistohyökkäysten torjuntamekanismi on oltava.
22. Järjestelmän ja laitteiden on sisällettävä "salakuuntelun" estävä toiminnallisuus. Laitteen ja mittarinlukujärjestelmän CS välillä on käytettävä AES-128 salausta kaikessa sovellustason tiedonvaihdossa.
23. Salausavainten hallintamekanismit on oltava mittareissa.
24. Kaikki yksityisyyden suojan suhteen herkät tiedot on aina suojattava. Suojaukseen ole sallittua käyttää yhteisiä salaisuuksia kuten yhteisiä avaimia tai salasanoja, vaan joka mittarilla on oltava oma master-avain. Avaimet, salasanat ja ohjelmistot on suojattava luvattomalta muuttamiselta ja lukemiselta. Ohjelmistojen on oltava päivitettävissä jotta havaitut haavoittuvuudet voidaan tarvittaessa korjata, ja ohjelmiston päivitykseen on oltava tietoturvalliset mekanismit.

Vaatimuksissa korostetaan erityisesti seuraavia asioita:

- vain sähköverkko-operaattorilla eli mittaroinnista vastaavalla osapuolella on pääsy rajapintaan P3
- AMM-järjestelmän toimittajan on taattava tietoturvamekanismien oikea toteutus järjestelmässään
- sisäkkäisiä tietoturvavyöhykkeitä ja mekanismeja on tärkeää käyttää, jotta yksittäinen haavoittuvuus ei anna pääsyä kriittisiin asioihin
- Vaatimusmäärittelyt ovat linjassa ohjelmistojen tietoturvaohjeen WELMEC software Guide 7.2 Issue 4 [WELMEC 2011] kanssa.

## 2.6 Standardiluettelo

### 2.6.1 Kokonaisuuksia suosittelevat dokumentit

Älykkäiden sähkömittarien ja sähköverkkojen standardoinnista on olemassa valmiita kokonaisuuksia joihin tutustuminen on suositeltavaa etsittäessä alan tietoturvastandardeja. Myös monet teolliseen tietoturvaan liittyvät vastaavat kokonaisuudet voivat osoittautua hyödyllisiksi luettavaksi, ja yleispätevät informaatioteknologian tietoturvaa käsittelevät standardit ovat helposti sovellettavissa AMM-järjestelmään tai sen osiin, vaikka eivät kykenekään kattamaan erikoistuneiden järjestelmien kaikkia erityispiirteitä.

| | |
|---|---|
| **ENISA:**<br>**Smart Grid Security**<br>**Security related standards, guidelines and regulatory documents**<br>**[Deliverable – 2012-03-31]** | http://myworks.vtt.fi/projektit/tk8/tk80/tk813/ammconfidential/Documents/ENISA_Annex%20IV%20-%20Smart%20Grid%20Security%20Related%20Standards%20Guidelines%20and%20Regulatory%20Documents.pdf |
| Dokumentti on liite ENISA:n tutkimukseen ”Smart Grid Security: Recommendations for Europe and Member States”, ja siinä luetteloidaan dokumentteja, joiden arvioidaan olevan hyödyllisiä älykkään sähköverkon turvaamisessa. | |
| **CEN/CLC/ETSI/TR**<br>**50572 Functional reference architecture for communications in smart metering**<br>**systems** | ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf |
| Tekninen raportti kuvaa viitteellisen kommunikaatio-arkitehtuurin ja luettelee sille olennaisia standardeja. Arkkitehtuuri pyrkii toteuttamaan Mandaatin M/441 vaatimukset. | |

### 2.6.2 Standardit ja tukevat dokumentit

Tietyt standardit nostetaan erikseen esille tässä dokumentissa, vaikka osa niistä onkin jo esitelty edellä mainituissa selvityskokonaisuuksissa. Syynä tähän on niiden huomionarvoisuus etämittarijärjestelmien turvallisuuden arvioinnissa. Vaikka itse toimintaa ei virallisesti standardoitaisikaan, voivat mainitut standardit helpottaa järjestelmien kehittämistä toimimalla tietoturvatekijöiden tarkastuslistoina tai niiden aihiona.

| | |
|---|---|
| **EN 13757-1: Communication systems for meters and remote reading of meters– Part 1: Data exchange** | EN 13757-1 is a standard established by CEN/TC 294 for Communication system for meters and remote reading of meters (non-electricity). This standard contains OBIS object definitions for non-electricity meters and is referencing other parts of EN 13757 series and standards from IEC/EN 62056 series (DLMS/COSEM), including local interfaces, lower and upper layers, data modelling. |
| **EN 13757** | "**M-Bus** (Meter-Bus) is a *European standard* (EN 13757-2 physical and link layer, EN 13757-3 application layer) for the remote reading of *gas* or *electricity meters*. M-Bus is also usable for other types of consumption meters. The M-Bus interface is made for communication on two wires, making it very cost effective. A radio variant of M-Bus (*Wireless M-Bus*) is also specified in EN 13757-4." (Wikipedia) |
| **IEC 61508** | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems |
| **ISA/IEC-62443 (Formerly ISA-99)** | **Smart meters Co-ordination Group – Privacy and Security approach** |
| ISA (Industrial Automation and Control Systems Security)-standardi käsittelee laajasti tietoturvaa teolisuusautomaation eri osa-alueilla. | |
| **IEC 62056** | IEC 62056-21: Direct local data exchange (3d edition of IEC 61107) describes how to use COSEM over a local port (optical or current loop)<br>IEC 62056-42: Physical layer services and procedures for connection-oriented asynchronous data exchange<br>IEC 62056-46: Data link layer using HDLC protocol<br>IEC 62056-47: COSEM transport layers for IPv4 networks<br>IEC 62056-53: COSEM Application layer<br>IEC 62056-61: Object identification system (OBIS)<br>IEC 62056-62: Interface classes |
| IEC 62056 standardisarjassa (lähinnä IEC 62056-53 ja IEC-62056-61 standardeissa) määritellään myös kulutusmittareiden ja vastaavien laitteiden tiedonsiirron tietoturvan toteutusta. Eli käsitellään sekä tietojen saannin turvaa (data access security) ja sen osana käyttöoikeuksien hallintaa (authentication) että siirrettävien tietojen salausta (data transport security). Tietojen käytöoikeuksien hallinnan osalta IEC 62056 määrittelee kolme tietoturvan tasoa. Alimmalla tasolla puuttuvat kaikki tietoturvamekanismit | |

| | |
|---|---|
| **1377-2012 - IEEE Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables)** | Standardissa käsitellään etäluennan kommunikointiprotollan sovelluskerrosta.<br><br>http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6264063 |
| **ISO/IEC 27000** | **ISO/IEC 27000** viittaa kasvavaan ISO/IEC-standardiperheeseen, jonka yhteinen otsikko on "Informaatioteknologia.Turvallisuus.Tietoturvallisuuden hallintajärjestelmät" (wikipedia)<br>http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view |
| ISO/IEC 27000 –standardiperhe ”Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät.” on sovellettavissa etäluettavien sähkömittarien informaatiojärjestelmien tietoturvallisuuden ja riskien hallintaan. Standardikokoelmaan sisältyy riittävä määrä taustamateriaalia keskeisten vaatimus- ja riskinhallintaosioiden yksiselitteiseksi tulkitsemiseksi. Sertifioiminen standardin mukaisesti edellyttää organisaatiolta sitoutuneisuutta ja tarpeeksi suurta kokoa hyvän kustannustehokkuuden saavuttamiseksi. Kaikkia standardiperheen standardeja ei ole vielä julkaistu, mutta enemmistö julkaistuista on jo suomennettu. VTT on tehnyt oppilaitoksille tiivistelmän standardisarjasta suomalaisille oppilaitoksille kalvosarjan muodossa [Väisänen & Kreus, 2012]. | |

# 3. Suomen AMM-järjestelmien yleinen järjestelmäkuvaus

Suomen sähköverkossa sähköenergia siirretään suurjännitteisiä 110-400 kV kanta –ja alueverkkoja pitkin paikallisille jakeluverkkoyhtiöille. Jakeluverkkoyhtiö vastaa sähköenergian siirrosta ja kulutuksen mittauksesta kotitalouksiin ja teollisuuskohteisiin. Jakeluverkkoyhtiöiden jakeluverkot toimivat 20, 10, 1 tai 0,4 kilovoltin jännitteellä. Suomessa on noin 80 sähkön jakeluverkkoyhtiötä, joista 15 suurinta kattaa 70% jakeluverkoista, käyttäjistä ja yhtiöiden liikevaihdosta. Pienimmät jakeluverkkoyhtiöt toimivat yhden kunnan alueella ja palvelevat pieniä asiakasmääriä. Taulukossa on listattuna käyttöpaikkojen perusteella Suomen 10 suurinta jakeluverkkoyhtiötä.

| Yhtiön Nimi | Käyttöpaikkoja |
|---|---|
| Fortum Sähkönsiirto Oy | 445425 |
| Vattenfall Verkko Oy | 398543 |
| Helen Sähköverkko Oy | 354033 |
| Fortum Espoo Distribution Oy | 181482 |
| Tampereen Sähköverkko Oy | 136663 |
| Savon Voima Verkko Oy | 111386 |
| Vantaan Energia Sähköverkot Oy | 105022 |
| Kymenlaakson Sähköverkko Oy | 101377 |
| Järvi-Suomen Energia Oy | 100112 |
| Oulun Energia Siirto ja Jakelu Oy | 90895 |

*Taulukko 1 Suurimmat jakeluverkkoyhtiöt [Energiamarkkinavirasto, 2011]*

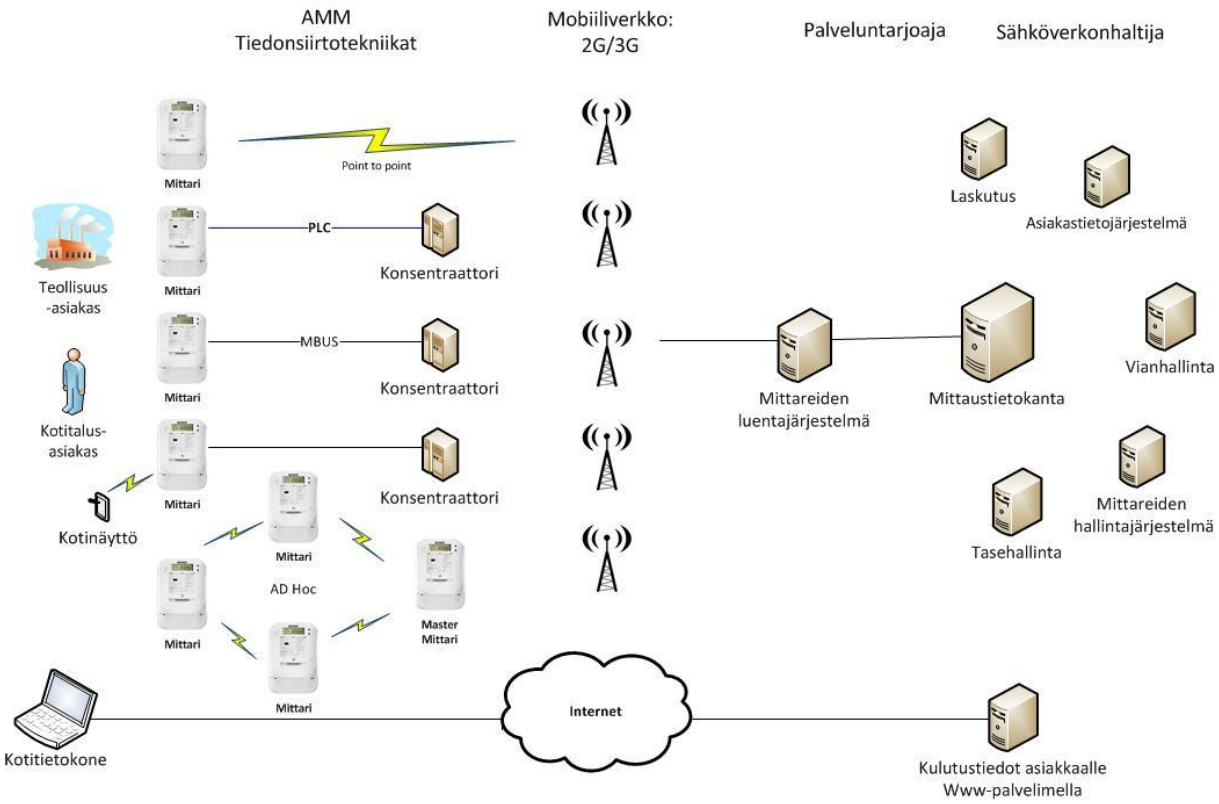
AMM-järjestelmäkokonaisuudet vaihtelevat verkkoyhtiöittäin. AMM-järjestelmät suomessa koostuvat etäluettavista sähkömittareista, konsentraattoreista (eli tiedonsiirron keskittimistä), kommunikointiverkoista, sekä palveluntarjoajan ja sähköverkkoyhtiön tietoverkoista. Tietoverkoissa on lukuisia etäluentaan liittyviä palvelimia ja palveluja, joita kuvataan seuraavassa luvussa.

AMM-järjestelmien tuottamien mittaustietojen ja kuormituksen ohjausmahdollisuuksien avulla saadaan varsinkin maaseudulla erityisesti pienjänniteverkon mutta myös keskijänniteverkon kuormitus ja vikatilanteet entistä paremmin hallintaan. Verkon tila, kuormitus ja sähkön laatu tiedetään tarkemmin ja lisäksi niihin voidaan joskus tarvittaessa vaikuttaa myös AMM järjestelmän kautta kuormia ohjaamalla. Sähkön jakeluverkon kapasiteetti saadaan tarkemmin käyttöön ja komponenttien ylikuormittumista saadaan vähennettyä. Myös vikatilanteiden paikallistaminen ja korjaaminen nopeutuu. Verkon kuormituksen tarkempi tunteminen auttaa myös kohdistamaan ja ajoittamaan verkostoinvestoinnit paremmin.

Sähkönjakeluverkon käyttö muuttuu entistä dynaamisemmaksi ja monimutkaisemmaksi, kun hajautettu tuotanto sekä ohjattavat kuormat ja energiavarastot lisääntyvät. Lisäksi sähkön toimitusvarmuutta ja laatua koskevat vaatimukset ja haasteet kiristyvät. Tästä johtuen jakeluverkkojen hallinta on kehitettävä nykyistä paremmaksi erilaisten tietojärjestelmien ja ohjaustoimintojen avulla [Löf, 2009].

## 3.1 AMM-järjestelmän osakokonaisuudet

Tässä luvussa on kuvattu lyhyesti AMM-järjestelmän eri osakokonaisuudet. Automaattinen mittarinluenta on tuonut lukuisia laitteita ja järjestelmiä ympärilleen. Allaolevassa kuvassa on karkea yleiskuva kulutustietojen luennan kommunikaatioketjusta. Mittaustieto siirtyy suoraan kulutusmittarista luentajärjestelmään lähes aina matkapuhelinverkkoyhteyden välityksellä. Kuvassa ei ole otettu huomioon sitä, että pieni osa kulutustiedoista luetaan lankapuhelinyhteyden avulla (PSTN) tai vanhaan tapaan lukemalla mittaria paikan päällä. Kulutustiedon muoto tarkistetaan luentajärjestelmässä ja validoidaan mittaustietokantaan sopivaan muotoon. Tämän jälkeen kulutustietoja yhdistellään eri tarpeisiin tietojärjestelmien välillä.




*Kuva 4: Etäluennan kokonaiskuva*

### 3.1.1 Etäluettava sähkömittari

Etäluettava sähkömittari mittaa käyttöpaikan sähkönkulutusta, ja välittää mittaustiedon tuntisarjoina vähintään kerran vuorokaudessa jakeluverkkoyhtiön mittaustietokantaan. Etäluettavat sähkömittarit korvaavat vanhat mekaaniset sähkömittarit, jotka luettiin paikallisesti vuosittain, tai asiakkaan vaihtumisen yhteydessä. Etäluettava mittari toimittaa mittaustiedot mittaustietokantaan joko ajastetusti tai mittausjärjestelmän kehotteesta. Muita etäluettavan mittarin ominaisuuksia:

- Mittari mittaa kulutustietojen lisäksi usein keskeisimpiä helposti mitattavia jännitteen laadun suureita, kuten jännitetasoja, pitkiä keskeytyksiä sekä jossakin mielessä myös jännite-epäsymmetriaa. Monissa maissa, kuten Suomessa, mittarien pakollisiin vaatimuksiin kuuluu pitkien jännitekeskeytysten rekisteröinti.
  Mittaustietoja käsitellään ja varastoidaan mittarissa. Mittaustietoja mahtuu mittarin muistiin mallista riippuen useita kuukausia, ja muistipiirit säilyttävät tietosisältönsä myös sähköjen katketessa. Mittaustietojen mittarissa varastoinnin vähimmäisajasta on tyypillisesti kansallisia vaatimuksia.

- Etäluettavien mittareiden laiteohjelmisto on mahdollista päivittää joko etänä tai paikallisesti tai molemmilla tavoilla.
- Mittarin mittaustietokantaan kommunikoiva osio on usein modulaarinen, joten metrologista osaa ei tarvitse välttämättä vaihtaa jos kommunikointitekniikkaa joudutaan vaihtamaan.
- Sähkökatkotietojen keruu
- Hälytykset ja niiden tallentaminen
- Etäluettaviin mittareihin on suunniteltu ja tulossa erityyppisiä kotinäyttöjä, jotka näyttävät käyttöpaikan asukkaalle reaaliaikaista kulutustietoa.
- Varsinainen metrologinen osa ja sen lukemamuisti on pyritty toteuttamaan niin, että kukaan mittauksen osapuoli ei pysty niitä eikä niiden toimintaa muuttamaan ja että ne pelkästään antavat mittaamansa tiedot eteenpäin tietoliikennettä ja tietojen jalostusta hoitavalle moduulille, jonka ohjelmisto on päivitettävissä. Tällä pyritään varmistamaan se, että kukaan osapuoli ei pysty muuttamaan eikä hävittämään varsinaisia mittaustietoja.

### 3.1.2 Konsentraattori ja master-mittari

Konsentraattori (tai keskitin) toimii yhdyskäytävänä sähkömittarin ja luentajärjestelmän välillä. Se kerää mittaustiedot usealta alueen sähkömittarilta, ja välittää tiedot edelleen mittaustietokantaan matkapuhelinverkon yli. Konsentraattorilla voidaan myös hallita kommunikointiyhteydessä olevien mittareiden tilaa. Konsentraattoria käytetään alueilla, joissa käyttöpaikkojen välimatka on riittävän pieni mittareiden väliseen kommunikaatioon. Sähkömittarin ja konsentraattorin välinen kommunikointi tapahtuu pienjänniteverkon yli PLC:lla, langattomalla meshverkolla, tai sarjaväylätekniikoilla kaapelin kautta. Toteutuksesta riippuen konsentraattorina käytetään joko täysin erillistä laitetta, tai master-mittaria. Master-mittari on samanlainen sähkömittari kuin muutkin alueella olevat, mutta se kerää luentatiedot rajatun alueen mittareilta ja on ainoa (käytännössä SIM-kortillinen) laite joka kommunikoi suoraan luentajärjestelmän kanssa.

### 3.1.3 Luentajärjestelmä

Luentajärjestelmää käytetään mittaustietojen lukemiseen etäluettavilta sähkömittareilta. Luetut ja luennan yhteydessä tarkastetut tiedot tallennetaan mittaustietokantaan. Luentajärjestelmällä luetaan tietoja useilta erimallisilta sähkömittareilta eri kommunikaatioväyliä ja rajapintoja pitkin. Käytäntöjä mittareiden lukemiseen on useita.

Luentajärjestelmä voi olla joko sähköverkkoyhtiön tai erillisen palveluntarjoajan hallinnoima. Sama sähköverkkoyhtiö voi käyttää useita erilaisia luentajärjestelmiä. Mittaustiedot luentajärjestelmästä toimitetaan suojatulla yhteydellä mittaustietokantaan.

### 3.1.4 Mittaustietokanta

Mittaustietokannan (tai mittaustiedon hallintajärjestelmän) tehtävänä on tallentaa ja varastoida mittaustietoa. Mittaustietoa tulee järjestelmään mm. luentajärjestelmistä, kannettavista mittarinlukulaitteista sekä muilta markkinaosapuolilta EDI-järjestelmän kautta. Mittaustietokantaan talletetaan tuntilukemat, ennusteet, ja tariffimitattujen asiakkaiden vuosikulutusennusteet [Harjula, 2008].

### 3.1.5 Käytöntukijärjestelmä

Käytöntukijärjestelmällä (Distribution Management System) valvotaan sähköverkon tehokkuutta ja luotettavuutta ja se toimii verkon käytöstä vastaavan henkilöstön päätöksenteon tukijärjestelmänä. Käytöntukijärjestelmä tarjoaa verkon hallinnassa avustavia toimintoja [Koto, 2010].

### 3.1.6 Käytönvalvontajärjestelmä

Käytönvalvontajärjestelmä KVJ on sähkönjakeluverkon valvomo, jolla ohjataan ja tarkkaillaan sähkönjakeluprosessia [Koto, 2010]. KVJ on käytännössä teollisuusautomaation (tässä tapauksessa verkostoautomaation) ohjausjärjestelmä SCADA (Supervisory Control and Data Acquisition). Järjestelmä koostuu palvelimista, operaattoreiden työasemista ohjelmistoineen, sekä jakeluverkossa sijaitsevista päätelaitteita, ala-asemista ja KVJ:n alla toimivista sähköasemien automaatiojärjestelmistä. KVJ valvoo ympäri vuorokauden sähköverkon kuormitustasoa, jännitettä ja vikatilanteita. Sekä normaaleissa käyttötilanteissa että varsinkin vikatilanteissa sähköasemille lähetetään ohjauskäskyjä etänä. KVJ on kriittinen järjestelmä sähkönjakeluverkon toimivuuden ja ehjänä pysymisen kannalta, ja siksi palvelimien kuuluu olla kahdennettu ja varmistettu varavoimalla.

KVJ:stä erillinen suojausjärjestelmä suojelee sähköverkkoa vakavalta ylikuormittumiselta, mutta siinäkin voi olla puutteita ja virheitä. Suojausjärjestelmän kattava toiminnassa testaaminen on vaikeaa ja kallista, eikä sitä ole tarkoituksenmukaista tehdä estämään aivan kaikkia mahdollisia vaarallisia kytkentöjä ja ylikuormitustapauksia. KVJ:n kautta saattaa siksi olla mahdollista tehdä toimenpiteitä, jotka myötävaikuttavat siihen, että verkon komponentteja ylikuormittuu jolloin niiden elinikä lyhenee tai niitä jopa tuhoutuu.

### 3.1.7 Vianhallinta

Etäluettavat sähkömittarit seuraavat sähkön laatua lähinnä jännitetasojen ja niihin perustuvien keskeytystietojen kautta. Poikkeama- ja hälytystiedot lähetetään käytöntukijärjestelmään, jossa tiedot yhdistetään sähköverkon kokonaiskuvaan. Sähkömittarit voivat lähettää tietoja myös vian tyypistä ja sähkökatkosta käytöntukijärjestelmään varavirran avulla vian alkaessa [Löf, 2012].

Kulutusmittareista haettavien tietojen avulla jakeluverkon vikojen korjausta on saatu nopeutettua huomattavasti ja myös pienjänniteverkosto on saatu kunnolla vianhallinnan piiriin. Aikaisemmin pienjänniteverkon vikojen havaitsemin perustui pääasiassa asiakkaiden tekemiin ilmoituksiin ja paikan päällä käyden tehtyihin tarkastuksiin.

### 3.1.8 Sähkön laadun hallinta

Sähkön laadun hallinta perustuu jännitteen laadun valvontaan. Nykyisin sitä tehdään entistä enemmän jatkuvasti etäluettavilla sähkön laadun analysaattoreilla ja mittareilla. Näin havaitaan ja todennetaan sähkön laadun poikkeamat hyvissä ajoin ennen kuin standardin asettamat vaatimukset ehtivät ylittyä ja niiden suhteen yhteensopivat asiakkaan tai verkon omat laitteet ylikuormittua, vahingoittua tai toimia väärin. Sähkön laadun hallintajärjestelmissä käytetään täydentävinä tietoina myös AMM-järjestelmien tuottamaa tietoa jännitetasoista, epäsymmetrioista ym. Sähkön laadun analyysit ja korjaavat toimenpiteet vievät aikaa, joten sähkön laadun hallinta on hyvin harvoin aikakriittistä toimintaa.

### 3.1.9 Asiakastietojärjestelmä

Asiakastietojärjestelmä on tietokantapohjainen järjestelmä, johon talletetaan sähköverkonhaltijan alueella olevien käyttöpaikkojen asiakastiedot. Asiakastietoihin kuuluvat käyttöpaikkakohtaisten tietojen lisäksi osoite-, henkilö-, sähkönkulutus- sekä tariffitiedot.

### 3.1.10 Laskutustietojärjestelmä

Laskutusjärjestelmä tuottaa asiakkaalle lähetettävät laskut, pohjautuen sopimus- ja asiakastietoihin, tarkastettuun kulutuksen ja mahdollisen tuotannon mukaiseen asiakkaan taseeseen.

### 3.1.11 Kulutustietoja asiakkaille tarjoava palvelin

Verkkoyhtiö on velvoitettu tarjoamaan kuluttajalle kulutustiedot tuntisarjoina. Kulutustiedot tulee näkyä asiakkaalle viimeistään samaan aikaan kuin sähkön myyjälle. Käytännössä kulutustiedot näkyvät palvelussa päivän viiveellä, ja historiatietoja pystyy katsomaan ainakin oman sopimuskautensa keston ajalta. Kulutustietojen tarjoaminen on toteutettu www-palvelulla, jonne asiakkaat rekisteröityvät omalla käyttöpaikkanumerollaan ja henkilötiedoillaan.

### 3.1.12 Mittarien asennus ja työmääräimet

Mittarin asennusprosessi suoritetaan asentajan pda-laitteella tai kannettavalla tietokoneella työmääräimeen perustuen. Sähköiset työmääräimet ovat korvanneet vanhat paperiset vastineensa. Työmääräimen tiedot kulkevat palveluntarjoajan palvelimen kautta asentajalle VPN-yhteyden kautta.

### 3.1.13 Liittyvät sähköverkon asiakkaiden järjestelmät

Tulevaisuuden suunnitelmissa ja vaatimuksissa myös koti- ja kiinteistöautomaatio sekä hajautetun sähkön tuotannon hallinta omaavat liitynnän etäluettavaan sähkömittariin paljon nykyistä useammin. Nämä järjestelmät ovat rajattu ulos tutkimusalueesta.

Tyypillisesti nämä muut järjestelmät on kytketty etäpalveluihin ja mahdollisesti Internetiin, käsittelevät yksityisyyden suojan kannalta herkkiä tietoja. Lisäksi useimpien niiden tietoturvallisuutta yhteiskunta ei vielä käytännössä mitenkään vaadi eikä valvo. Myös tietoturvan toteutus on osassa vielä usein hyvinkin puutteellinen. Yleistyessään huonosti tietoturvalliset kulutusta mittaavat ja ohjaavat muut järjestelmät voivat johtaa osin samoihin uhkiin kuin AMM-järjestelmien haavoittuvuudet

## 3.2 Sähkönkulutustiedon etäluennan tiedonsiirtotekniikat

### 3.2.1 PLC

PLC–tekniikan (Power Line Communication) juuret ulottuvat 1920-luvulle. Suurjännitelinjaa pitkin välitettiin huoltopuheluita 1960-luvulle asti [Brown, 1999]. Myöhemmin tekniikkaa on sovellettu laitteiden kauko-ohjaukseen, internet-yhteyksiin ja sähkön kulutustietojen etäluentaan. PLC:n toiminta perustuu informaatiota sisältävän signaalin modulointiin kantoaaltoon, joka tässä tapauksessa siis kulkee sähköverkossa.

CENELEC määritteli 1991 Eurooppalaisen standardin EN-50065-1 pienjänniteverkossa tapahtuvalle signaloinnille. Standardi eroaa paljon Japanin ja USA:n omista standardeista. Taajuusalue 3 kHz - 95 kHz (teollisuudessa A-alue) on varattu sovelluksille, joilla valvotaan tai ohjataan pienjännitejakeluverkkoa, esim. sähkömittareiden kommunikaatiosovellukset. Taajuusalue 95 kHz - 148,5 kHz (teollisuudessa B-, C-, ja D-alue) on määritelty analogisille ja digitaalisille sovelluksille kotitalouksissa, kaupallisissa sekä teollisuusympäristöissä.

PLC-tekniikkaa käytetään sähkön käyttömäärien etäluennassa välittämään tietoa mittarilta konsentraattorille. Suomessa PLC-tekniikka on käytössä TTY:n 2011 tekemän kyselyn mukaan vuonna 2013 noin 30-50%:ssa etäluettavista mittareista. Saman selvityksen mukaan keskimäärin 3,6%:lla mittareista on esiintynyt luentaongelmia (otos 110647 mittaria) [Pakonen, 2012]. Tiedonsiirtoympäristönä sähköverkko on melko haasteellinen ja on kehittynyt haasteellisempaan suuntaan, koska verkkoon liitetyt laitteet ja kytkentätilat muuttuvat vähän väliä, tehoelektroniikan kautta liitetyt laitteet yleistyvät ja sähkön kuluttajille myydään entistä enemmän laitteita jotka eivät käytännössä täytä Eurooppalaisia yhteensopivuusvaatimuksia. Kuluttajien laitteiden yhteensopivuusvaatimuksissa (EMC Electro Magnetic Compatibility) on toistaiseksi aukko taajuusalueella 3-150 kHz. Tällä taajuusalueella ei ole määritelty sitä, millaisia häiriöitä kuluttajien laitteet saavat verkkoon tuottaa ja millainen niiden impedanssi saa olla ja paljonko alueen signaaleja tulee kestää hajoamatta. Esim. kotitalouslaite voi aiheuttaa häiriötä joka aiheuttaa PLC-signaalin häviämisen. Tilanne on melko vaikeasti hallittavissa ja ennakoitavissa kunnes tekeillä oleva standardointi valmistuu ja selkeyttää tilanteen. Toisaalta uusien modulointitekniikoiden käyttöönotto on tuonut ainakin tilapäistä helpotusta myös PLC-tiedonsiirron alueella. Myös langattomilla tiedonsiirtotekniikoilla haasteena on että kaikkien mahdollisten taajuuskaistojen käytöllä on taipumus kasvaa ja siten ne muuttuvat entistä häiriöllisemmiksi.
Projektin työpajojen keskusteluissa ilmeni, että PLC-tekniikan käyttö on työpajoihin osallistuneissa yrityksissä hiljalleen vähenemässä.

### 3.2.2 M-Bus

M-Bus (Meter-Bus) on eurooppalainen standardi sähkön ja kaasun etäluentaan. M-Bus protokolla kommunikoi kaapelia tai ilmarajapintaa pitkin standardista ja toteutuksesta riippuen. Protokollaa käytetään etäluettavan sähkömittarin ja konsentraattorin väliseen kommunikointiin.

Standardit:

- EN 13757-1 Kommunikointi
- EN 13757-2 Fyysinen kerros ja linkkikerros
- EN 13757-3 Sovelluskerros
- EN 13757-4 Langaton mittarinluenta (868MHz-870Mhz Short Range Device Band)
- EN 13757-5 Langaton releointi
- EN 13757-6 Lähiluenta erillisellä laitteella.

### 3.2.3 2G/3G

Etäluettavalta mittarilta tulevat kulutustiedot kulkevat aina matkapuhelinverkon kautta sähköverkkoyhtiölle, joko suoraan mittarilta, tai koottuna konsentraattorilta. Poikkeuksena tähän on, jos mittarilta tulevia tiedot joudutaan lukemaan paikallisesti. Matkapuhelinverkon kanssa kommunikoivassa mittarissa tai konsentraattorissa on yhteyteen määritelty SIM-kortti. Mittari, master-mittari, tai konsentraattori kommunikoivat matkapuhelinoperaattorille oman APN (Access Point Name)-rajapinnan kautta.

### 3.2.4 RS485 ja RS232

RS485 ja RS232 ovat sarjaliikenteen standardeja (Recommended Standard). Tätä liityntätapaa käytetään monimittauskeskuksissa, joissa mittarit ovat lähekkäin samassa tilassa (esim. kerrostalot ja rivitaloyhtiöt). Sarjaliitäntä on yksinkertainen kommunikointitapa, jossa bitit kulkevat peräkkäin sarjamuotoisena. RS485-väylään voi liittyä useita laitteita samanaikaisesti, RS232 on sen sijaan tarkoitettu vain kahden laitteen väliseen kommunikointiin.

### 3.2.5 DLMS/COSEM

DLMS/COSEM on sähkön etäluentaan laadittu kommunikointistandardi. DLMS (Device Language Message specification) määrittelee kommunikoivat entiteetit. COSEM (COmpanion Specification for Energy Metering) määrittää standardeihin pohjautuvat säännöt, joilla tiedonvaihto mittarien ja lukujärjestelmän välillä toteutetaan.

Moni mittarivalmistaja käyttää DLMS/COSEM standardin mukaisia ratkaisuja, jotka kuitenkin eroavat toisistaan muun muassa versioiden ja toteutettujen/käytettyjen tietoturvatasojen osalta. Standardi sallii myös valmistajakohtaiset laajennukset. Käytännössä eri järjestelmien yhteensopivuus rajoittuu pääasiassa vain perustoimintoihin. Joskus perustoimintojenkin osalta on yhteensopimattomuutta, esimerkiksi hieman standardista poikkeavien ajoitusten muodossa. DLMS/COSEM protokollassa on tietoturvavaatimusten mukaan mahdollisuus käyttää eritasoisia tietoturvaratkaisuja aina alkaen salaamattomasta tiedonsiirrosta. Versioiden välillä on eroja myös sen suhteen mitä tietoturvaominaisuuksia niihin sisältyy.

## 3.3 Kulutusmittareiden kautta toteutettavat ohjaustoiminnot

Valtioneuvoston 2009 asetuksen mukaan, etäluettavien mittareiden ominaisuuksiin tulee kuulua myös kysyntäjouston mahdollistavat ohjaustoiminnot. Suomessa kulutusmittareiden kautta ohjataan kuormia seuraavilla tavoilla:

- kuormien etäkytkennät
- aikaohjaukset
- dynaamiset aikaohjaukset
- suorat kuorman ohjaukset.

Tarve kuormien ohjauksiin ja varsinkin dynaamisiin kuormien ohjauksiin lisääntyy. Toisaalta kotien ja rakennusten energianhallinta-automaation ja etäohjauksen yleistyminen tulee aikanaan syrjäyttämään AMM-järjestelmien kautta tapahtuvat ohjaukset. Tällä hetkellä kotien ja rakennusten energianhallintajärjestelmät eivät ole riittävän yleisiä, halpoja, toiminnaltaan luotettavia ja tietoturvallisia siihen, että niiden kautta ohjattaisiin suuria määriä sähkökuormia. Sitä odotellessa AMM-järjestelmien kautta tapahtuvan dynaamisen ohjauksen järjestelmien käyttö lisääntyy, sillä ne tarjoavat tietyillä alueilla kustannustehokkaita mahdollisuuksia kuormien ohjausten kohtalaisen nopeaan toteuttamiseen laajassa mittakaavassa. Mahdollisuuksia on parhaiten siellä, missä uusien AMM-järjestelmien toteutusten yhteydessä ei ole purettu ohjauskohteissa olleita kuormanohjausvalmiuksia.

### 3.3.1 Etäkytkennät

Kaikki uudet mittarit sisältävät etäkytkentätoiminnon, joka yleensä voidaan tarvittaessa sulkea pois käytöstä. Etäkytkentätoiminto on useimmiten aktivoitu, ja varsinkin kohteissa joissa on siihen tavallista suurempi tarve, kuten kuluttajien nopea vaihtuvuus tai laskujen maksun ongelmat. Luentajärjestelmässä on toimintoja yleensä vain yksittäin suoritetuille etäkytkentöjen ohjauksille

### 3.3.2 Aikaohjaukset

Aikaohjauksilla ohjataan tyypillisesti varaavia ja osittain varaavia tilojen ja käyttöveden sähkölämmityksiä. Voimassa oleva sähkömarkkinalainsäädäntö edellyttää, että mittareissa on aikaohjaukseen soveltuva liitäntä ja että jakeluverkon kaikilla pienasiakkailla on mahdollisuus ostaa sähköä aikatariffilla. Tämän takia aikaohjausten takana on Suomessa hyvin paljon ohjattavaa tehoa, keskitalvella jopa yli 1 GW ja suurinta osaa siitä ohjataan AMM-mittareilla.

Ohjauksien toteutus voi vaihdella eli perustua paikalliseen erilliseen kelloon, kulutusmittarin kelloon tai etäohjauskomentoihin, jotka tyypillisesti tulevat AMM-järjestelmän kautta. Aikaisemmin ohjaukset olivat suoria, välittömästi saataessa toteutettavia komentoja, mutta nykyisin käytetään tyypillisesti ennalta lähetettyä ohjauskalenteria, koska nykyisten AMM-järjestelmien tiedonsiirron viiveet ovat verraten pitkiä ja kestoltaan vaihtelevia. Sama ohjauskalenteri lähetetään hyvin monelle mittarille, sillä tyypillisesti sen suhteen kohteet on jaettu vain muutamaan kooltaan merkittävään ryhmään, esimerkiksi kolmeen.

### 3.3.3 Dynaamiset aikaohjaukset ja suorat ohjaukset

Dynaaminen kuormien ohjaus tai dynaaminen kysyntäjousto tarkoittaa kuormien ohjausta, jossa ohjausaikoja voidaan tarvittaessa vaihdella tilanteen mukaan eli seuraavan päivän spot-markkinahintojen mukaan tai vieläkin nopeammin. Toistuvasti saman aikataulun tai muun kiinteän kalenterin ja kellon mukaan tapahtuva kuormien aika-ohjaus ei ole dynaamista ohjausta.

Tarkastelluissa yhtiöissä ei AMM-järjestelmien kautta toteutettuja dynaamisia aikaohjauksia eikä suoria kuormanohjauksia ollut merkittävässä määrin käytössä. Niitä on syytä pohtia siksi, että muualla Suomessa on jo noin 50 MW kuormaa ohjattavissa dynaamisesti ja lisäämiseen tähtääviä hankkeita on menossa. Laajenemista tulee kuitenkin huomattavasti rajoittamaan se, että uusia AMM-mittareita hankittaessa ja asennettaessa tarve dynaamiseen (kuorman-) ohjaukseen on usein jätetty huomioon ottamatta. Periaatteessa tietoturvan suhteen näissä ohjauksissa on lähes samat haasteet kuin aikaohjaustenkin suhteen, ja lisähaasteena on että ohjauskomennot tulevat jakeluverkkoyhtiön ulkopuolelta esimerkiksi sähkön myyjiltä tai järjestelmäoperaattorilta. Dynaamisten ohjausten toteutuksessa on oltava enemmän automaattisia toimintoja kuin tavallisissa varsin staattisissa aikaohjauksissa, mistä on tietoturvamielessä omat haittansa ja hyötynsä. Dynaamiseen ohjaukseen liittyy enemmän automaatiota, mikä voi mennä vikaan; mutta toisaalta dynaamisesti ohjatun mittarin reagointikyky on nopeampi niin kauan kuin se toimii, varmistuksia on enemmän ja ihmisen virhealtista AMM-järjestelmän operointia vähemmän.

# 4. AMM-järjestelmien tietoturvaa koskevat säädökset Suomessa

Sähkömarkkinoita ohjaa sähkömarkkinalaki, jonka lisäksi on määrätty kolme asetusta, jotka tarkentavat eräitä lain kohtia:

- Valtioneuvoston asetus sähköntoimitusten selvityksestä ja mittauksesta
- Valtioneuvoston asetus sähkömarkkinoista
- Työ- ja elinkeinoministeriön asetus sähkötoimitusten selvitykseen liittyvästä tiedonvaihdosta.

Sähkönkulutuksen mittausta koskevat säädökset muuttuivat valtioneuvoston asetuksen 2009/66 myötä. Asetuksen tärkeimpiä etäluentaan liittyviä vaatimuksia:

- Sähkönkäyttöpaikan tuntimittauslaitteisto on luettava vähintään kerran vuorokaudessa.
- Mittauslaitteiston rekisteröimä tieto tulee voida lukea laitteiston muistista viestintäverkon kautta (*etäluentaominaisuus*); (kuitenkaan protokollaa/standardia ei määritellä)
- Mittauslaitteiston tulee rekisteröidä yli kolmen minuutin pituisen jännitteettömän ajan alkamis- ja päättymisajankohta
- Mittauslaitteiston tulee kyetä vastaanottamaan ja panemaan täytäntöön tai välittämään eteenpäin viestintäverkon kautta lähetettäviä kuormanohjauskomentoja
- Mittaustieto sekä jännitteetöntä aikaa koskeva tieto tulee tallentaa verkonhaltijan mittaustietoa käsittelevään tietojärjestelmään, jossa tuntikohtainen mittaustieto tulee säilyttää vähintään kuusi vuotta ja jännitteetöntä aikaa koskeva tieto vähintään kaksi vuotta (Kirjanpitolaki edellyttää tasetietojen säilytystä vähintään 10 vuotta.)
- Asiakkaan sähkönkulutuksen taseselvitys tulee tehdä todellisen mitatun tuntikulutuksen perusteella. Alustava taseselvitys pitää saada asianosaisille sähkömarkkinaosapuolille viimeistään seuraavan päivän kuluessa.
- Asiakkaan tuntimitattu kulutustieto on oltava tarjolla seuraavan päivän kuluessa kaikille asianosaisille sähkömarkkinaosapuolille, myös asiakkaalle.
- mittauslaitteiston ja verkonhaltijan mittaustietoa käsittelevän tietojärjestelmän tietosuojan tulee olla asianmukaisesti varmistettu.

Henkilötietolaki 22.4.1999/523 koskee myös AMM-järjestelmien tuottamia ja käsittelemiä asiakaskohtaisia tietoja, sillä ne katsotaan kyseisen lain tarkoittamaksi rekisteriksi ja siten jakeluverkkoyhtiö sellaisen rekisterin pitäjäksi. Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Laki mm. velvoittaa rekisterinpitäjää huolellisuuteen ja säätää, että sama huolellisuusvelvoite on myös sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. Rekisterin käyttötarkoitus on määriteltävä eikä tietoja saa käyttää muihin tarkoituksiin. Myöhempää henkilötietojen käsittelyä historiallista tutkimusta, tieteellistä tai tilastointia varten ei pidetä yhteensopimattomana alkuperäisten käsittelyn tarkoitusten kanssa. Tällöin mm. vaaditaan, että toimitaan niin, että tiettyä henkilöä koskevat tiedot eivät paljastu ulkopuolisille sekä annetaan määräyksiä siitä, mitä pitää tehdä kun henkilötiedot eivät enää ole tarpeen tutkimuksen suorittamiseksi. Vastaavasti laissa säädetään muistakin erityisistä tarkoituksista. Laki määrää myös tietoturvallisuutta ja tietojen säilytystä koskevia vaatimuksia. Pääpiirteissään henkilötietoja saa käsitellä vain rekisteröidyn antamalla suostumuksella.

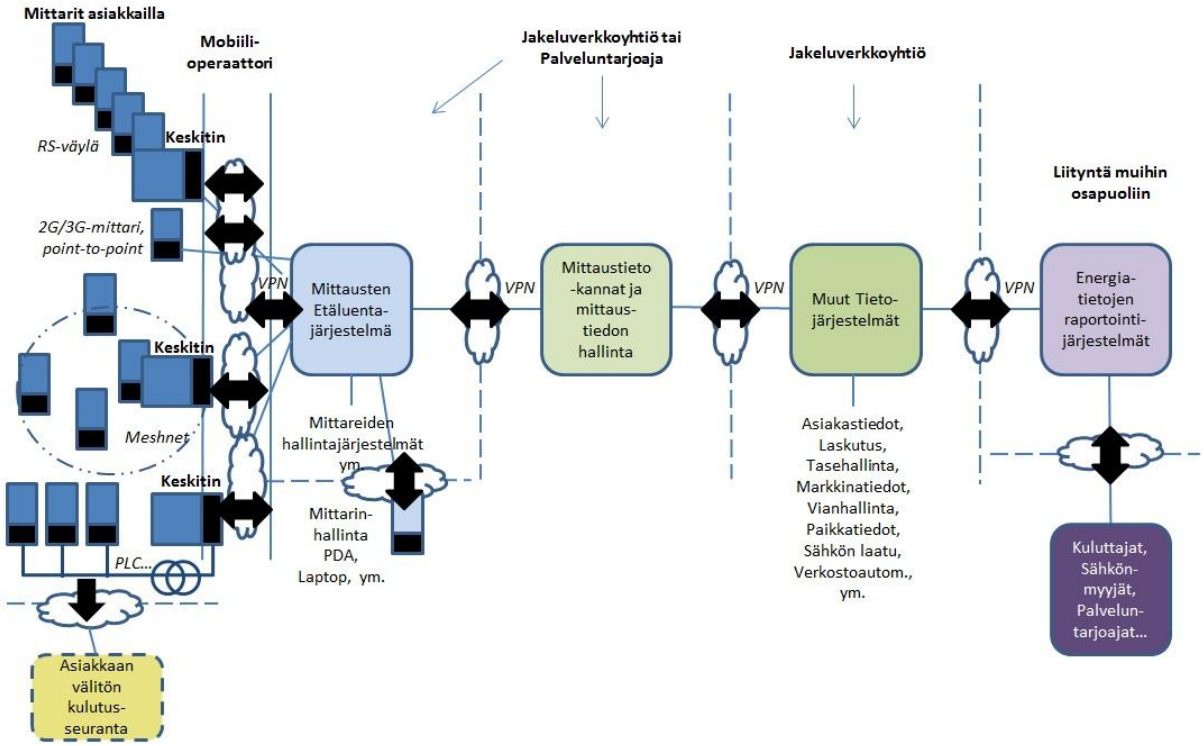
Sähköisen viestinnän tietosuojalaki 16.6.2004/516 määrittelee sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan säädöksiä viestintäverkoille. Lakia sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin ja palveluihin, joissa käsitellään palvelun käyttöä kuvaavia tietoja.

Mittauslaitedirektiivi 2004/22/EY koskee mittauslaitteita (myös sähköenergiamittarit), joille useimmissa EU:n jäsenmaissa asetetaan lakisääteisiä vaatimuksia. Direktiivi määrittelee sähköenergiamittarille mittausteknisiä vaatimuksia, mutta etäluentaan se ei ota kantaa.

Energiatehokkuusdirektiivi 2012/27/EU vaatii vuodesta 2020 alkaen asiakkaille saada todelliseen kulutustietoon perustuvaa laskutustietoa 4 kertaa vuodessa, jos asiakas on valinnut sähköisen laskutuksen ja muussa tapauksessa 2 kertaa vuodessa. Siitä ei siis seuraa Suomessa AMM-mittareille mitään sellaisia vaatimuksia, jotka eivät Suomessa ole jo käytännössä toteutettu jopa ennen sähkön toimituksen selvitystä ja mittausta koskevan Valtioneuvoston asetuksen siintymäajan umpeutumista vuoden 2013 loppuessa.

# 5. AMM järjestelmien potentiaaliset tietoturvauhkat ja haasteet Suomessa

Tässä luvussa on kuvailtu minkä tyyppisiä tietoturvauhkia AMM-järjestelmän eri komponentteihin ja osa-alueisiin kohdistuu. Etäluentaketjuun sisältyy useita kommunikaatiokanavia ja tekniikoita. Tietoa liikutellaan ja varastoidaan lukuisien osapuolien kesken. Etäluennan tiedonsiirtoketju tarjoaa siis paljon mahdollisia kohteita asiansa osaaville hyökkääjille. Alla olevassa kuvassa on kuvattuna AMM-järjestelmän välisiä rajapintoja pääpiirteittäin. Kuvan oikeassa laidassa oleva liityntä muihin osapuoliin voi olla mm. etäyhteyden tarjoaminen sähkömittarivalmistajalle, kulutustietojen välitys sähkön myyjälle tai EDI-sanomien välitys taseselvitykseen.




*Kuva 5 AMM-järjestelmän rajapinnat*

AMM-ympäristöissä, kuten muissakin tietoverkoissa, uhkat realisoituvat vahingoiksi, jos hyökkääjä onnistuu löytämään järjestelmästä haavoittuvuuksia ja hyödyntämään niitä. Haavoittuvuudet voidaan jakaa karkeasti kahteen ryhmään: suunnitteluvirheet ja toteutusvirheet.

Suunnitteluvirheet ovat suunnitteluvaiheessa tehtyjä virheitä; esimerkiksi autentikoinnin puuttuminen yleisesti käytetyssä etäluentaprotokollassa tietyssä rajapinnassa. Suunnitteluvirheille on yhteistä, että ne koskevat isoa joukkoa laitteita, eivät esimerkiksi pelkästään yhtä mallia.

Toteutusvirheet johtuvat toteutuksen aikana tehdyistä ohjelmointivirheistä. Tyypillisin esimerkki toteutusvirheestä on puskurin ylivuotovirhe, jossa ohjelma tallentaa tietoa sille varatun muistialueen ulkopuolelle. Tämä aiheuttaa usein virhetilanteen ohjelmistossa, ja voi saattaa ohjelmiston – ja esim. koko sähkömittarin – toimimattomaan tilaan. Tyypillinen hyökkäys on yrittää aiheuttaa puskurin ylivuotovirhe lähettämällä tietyn tyyppinen syöte protokollaa kuuntelevaan rajapintaan. AMM-järjestelmässä on paljon rajapintoja, joten on tärkeää että toteutukset vastaanottavat vain oikeassa formaatissa olevaa viestiliikennettä ennalta sovituista lähteistä. Haavoittuvuuksina voidaan nähdä myös prosessissa olevat virheet. Vaikka hyökkäys tai hyökkäyksen yritys aiheuttaisi hälytyksen ja merkinnän lokiin, ei hälytyksistä ole hyötyä jos kukaan ei tarkkaile hälytyslokeja.

## 5.1 Eri toimijoista johtuvat tietoturvaongelmat

Tällä hetkellä (2013) Suomessa käytetään usean eri valmistajan sähkömittareita, jotka kommunikoivat useilla eri protokollilla ja rajapinnoilla. Osa kommunikaatiosta voi tapahtua noudattaen yleistä standardia kuten DMLS/COSEM, kun taas usein käytetään kolmannen osapuolen kaupallista suljettua ratkaisua. Myös mittarien luentajärjestelmiä on useita erilaisia. Saman jakeluverkon alueella on siis tyypillisesti eri valmistajien mittareita ja eri luentajärjestelmiä samaan aikaan käytössä. Luentajärjestelmän käyttöön ja hallinnointiin rakennetut etäkäyttöyhteydet saattavat aiheuttaa tietoturvauhkia mikäli etäyhteyskäytännöt ja niiden turvallisuuden seuranta ovat puutteellisesti toteutettuja. Mm. kohdistettuihin hyökkäyksiin kykeneviä haittaohjelmia saattaa tällöin tunkeutua etäluennassa käytettäviin tietoverkkoihin ja tietojärjestelmiin. Usein alihankintaketjut ohjelmistojen ja järjestelmien suhteen ovat pitkiä vaikeuttavat edelleen kokonaisuuden hahmottamista. Ratkaisujen kirjavuus voi aiheuttaa yhteensopivuus- ja tietoturvaongelmia.

### 5.1.1 Sähkömittarit

Tähän kappaleeseen on kerätty Suomessa yleisiä etäluettavien sähkömittareiden malleja. Lähteenä on käytetty kymmenen suurimman sähköverkkoyhtiön verkkosivuja. Etäluettavat mittarit on lueteltu valmistaja – ja mallikohtaisesti. Mittarin tärkeimmät ominaisuudet on kuvattu lukuihin siltä osin kun tietoa on ollut julkisesti saatavilla. Taulukon tarkoituksena on kuvata yleisimpiä mittarimalleja, mittarikannan moninaisuutta sekä mittarien käyttämiä kommunikointirajapintoja. Valmistajien tarjoaman teknisen tiedon taso ja määrä vaihtelee paljon. Osa verkkoyhtiöistä ja mittarivalmistajista tarjoaa hyvinkin tarkkoja kuvauksia mittareista, kun taas osalta on saatavilla ainoastaan mallinumerot.

| Valmistaja | Malli | Mittarien kommunikointi |
|---|---|---|
| Telvent / Echelon | 83332-3IHA | • PLC taajuuskaista (A) 3-95 kHz, salasanasuojatut transaktiot ja liikenteen salaus.<br>• Optinen portti: IEC 62056-21 (salasanasuojattu)<br>• Lisämoduulit: CNX 2000 (ZigBee), CNX 3000 (ISO/IEC 14908-3 C-Band PLC), MCN 3020 WAN Adaptor |
| Landis + Gyr | E120GiME | • Integroitu GSM-moduuli: GPRS, TCP/IP, SMS<br>• Langaton paikallinen kommunikointi 2,4Ghz<br>• M-Bus 4:lle laitteelle: EN 13757-2. |
| Landis + Gyr | E120Lt | • Echelon LONTALK-protokolla (PL-3120 lähetin/vastaanotin) |
| Landis + Gyr | E120M | • Enermetin kehittämä oma PLC-protokolla / 2G/3G-modeemi<br>• Optinen Portti<br>• Langaton M-Bus (868Mhz) |
| Landis + Gyr | E120Gt | • Integroitu GSM/GPRS-moduuli |
| Landis + Gyr | E120Lime | • Integroitu PLC-moduuli (LonTalk-protokolla)<br>• Langaton paikallinen kommunikointi mittarinlukuun ja konfigurointiin.<br>• M-Bus (EN13757-2) Master – liitäntä 4 laitteelle |
| Landis + Gyr | E450 | • PLC (IEC 61334, DLMS/COSEM) tai 2G/3G<br>• Optinen portti: IEC 62056-21 |
| Kamstrup | 162L & 382L | • Optinen liitäntä edessä(DLMS/COSEM, EN 62056-21 mode A)<br>• Paikka kahdelle kommunikaatiomoduulille, joiden vaihtoehdot ovat: PLC, 2G/3G, GSM/GPRS, TCP/IP, RF-Radio, Sarjaväylä(”current loop”), Sarjaväylä RS232/RS485, M-bus(langallinen tai langaton). |
| Kamstrup | 351 (teollisuus – ja muut tehokohteet. | • Optinen liitäntä edessä(DLMS/COSEM, EN 62056-21 mode A) |

| | | |
|---|---|---|
| | | • Paikka kahdelle kommunikaatiomoduulille, joiden vaihtoehdot ovat: PLC, 2G/3G, GSM/GPRS, TCP/IP, RF-Radio, Sarjaväylä(”current loop”), Sarjaväylä RS232/RS485, M-bus(langallinen tai langaton). |
| Aidon | 551X, 5530, 6530, 6531 | • Aidonin mittarit koostuvat energiamittarista ja kommunikointimoduulista (Tarkempaa dataa ei verkkosivuilla saatavilla) |
| IskraEmeco | MT372 | • Integroitu GSM/GPRS-modeemi IEC 62056-46 (DLMS). mahdollisuus lisäantennille. Vaihtoehtona on mahdollisuus asentaa RS485-rajapinta.<br>• Optinen portti (IEC 62056-21) |
| IskraEmeco | MT400 | • Optinen portti (IEC 61107)<br>• Etäluentaan CS-rajapinta (20 mA current loop in compliance with DIN 66348) |

*Taulukko 2 Käytössä olevien etäluettavien sähkömittareiden malleja Suomessa.*

### 5.1.2 AMM-luentajärjestelmät

Projektin osapuolilla käytössä olevia luentajärjestelmiä

| **Nimi ja valmistaja** | **Kuvaus** |
|---|---|
| Landis+Gyr Gridstream AIM | Luentajärjestelmä |
| Aidon Gateware | Luentajärjestelmä |
| Kamstrup | Luentajärjestelmä |

*Taulukko 3 Luentajärjestelmät*

## 5.2 Mittareiden ja luentajärjestelmän välinen kommunikointi

### 5.2.1 Salauksen toteutuksen laatu

Tietoliikenne on salattua kulutustietojen siirtyessä etäluettavalta mittarilta luentajärjestelmään. Käytössä olevia salausmenetelmiä on harvoin mainittu mittareiden tiedoissa julkisesti, mikä viittaa siihen, että salausmenetelmät eivät välttämättä ole yleisesti tunnettuja. Keskimäärin kolmannen osapuolen suljetut salausprotokollat ovat olleet haavoittuvampia, kuin julkiset, yleisesti tutkitut ja tunnetut. Vaikka salausalgoritmi olisikin riittävän hyvä, myös sen toteutuksessa voi piillä ongelmia. Salausavain voi olla liian heikko, ja laskettavissa auki nykyisillä menetelmillä suorittimien laskentatehon kasvaessa. Salausavaimen, tai koko salausmenetelmän vaihto isoon joukkoon mittareita on kallista. Joissakin tapauksissa mittareiden välinen keskinäinen kommunikointi ei ole lainkaan salattua.

### 5.2.2 Autentikointiheikkoudet

Autentikointiheikkoudet ovat joko suunnittelu- tai toteutusvirheitä autentikointiprotokollassa. Esimerkiksi yhteinen salasana kaikkien mittareiden optiselle luentasilmälle on hallinnollisesti helppo tapa toteuttaa autentikointi, mutta samalla hyvin haavoittuva salasanan levitessä julkiseen tietoon. Jos käytettävää tiedonsiirtoväliä ei ole salattu, salasanan kaappaus liikenteestä on mahdollista.

AMM-järjestelmäkokonaisuudessa autentikointia käytetään mm. seuraavilla väleillä:

- Etäluettava mittari: etäpäivitykset, optinen liitäntä, sarjaliitäntä, PLC-kommunikointi, Meshnet, RS485
- Asiakkaan www-yhteys omiin kulutustietoihin
- Sähkömittarin/Konsentraattorin SIM - operaattoriverkko

- VPN-yhteys palveluntarjoajan ja sähköverkkoyhtiön välillä
- Etäyhteydet palveluntarjoajan tai sähköverkkoyhtiön sisäverkkoon.
- Mahdollinen mittarivalmistajan etäyhteys sähkömittarille tai konsentraattorille.

## 5.3 Inhimilliset käytönaikaiset virheet

Inhimilliset käytönaikaiset virheet voivat pahimmillaan aiheuttaa suuria vahinkoja. Virheet voivat olla tahallisia tai tahattomia. Huonosti suunnitellut käyttöliittymät voivat ohjata tietojärjestelmien käyttäjä käyttämään ”helpompia” toimintatapoja, jolloin kierretään turvallisia menettelyjä. Esimerkiksi sähköliittymän etäkytkennät ja katkaisut tulee toteuttaa niin, että kytkettävä käyttöpaikka on varmasti oikea, eikä kytkeminen massana ole mahdollista.

## 5.4 Kulutustietoja asiakkaille tarjoava www-palvelin

Valtioneuvoston asetus vuodelta 2009 velvoittaa sähköverkkoyhtiötä tarjoamaan käyttöpaikan tuntikohtaiset kulutustiedot asiakkaiden saataville viimeistään yhtä aikaa, kun ne ovat valmiita luovutettavaksi sähkön myyjälle. Tämä on toteutettu sähköverkkoyhtiöiden toimesta www-palvelimien avulla. Rekisteröityminen palveluun on toteutettu useimmiten kysymällä käyttäjältä pohjatietoina käyttöpaikan numero, asiakkaan nimi, osoite, ja sähköpostiosoite. Nämä tiedot on helposti saatavilla paperisista laskuista, ja palvelimelle ensimmäistä kertaa rekisteröityvän henkilöllisyyttä ei yleensä varmisteta esimerkiksi pankkitunnuksilla. Tästä johtuen rekisteröityminen toisen henkilön tiedoilla on helppo ja pääsy tarkkailemaan sähkönkulutusta, sekä historiatietoja onnistuu. Paperisia laskuja, joista löytyy rekisteröitymiseen vaadittavat tiedot, löytyy paljon esimerkiksi paperinkeräyslaatikosta. Rekisteröityminen toisen henkilön tiedoilla onnistuu yleensä vain ensimmäistä kertaa rekisteröityessä, joten tämä uhka lievenee kun kuluttajat rekisteröityvät palvelun käyttäjiksi asennusten jälkeen. Todennäköisesti kuitenkin osa kuluttajista ei rekisteröidy palveluun koskaan. Käyttäjätunnukset palveluun voivat paljastua muille käyttäjille myös käyttäjän omasta huolimattomuudesta. Uhkana on myös uuden asukkaan muuttaessa kiinteistöön se, että edellisen asukkaan sähkönkulutustiedot näkyvät www-palvelussa. Palvelussa asiakkaalle näkyvät kulutustiedot tulisi siis rajata aina asiakas –ja sopimuskohtaisesti.

## 5.5 Yksityisyysongelmat

Älykkäiden sähköverkkojen tarkemman tiedonlevityksen yhteydessä nousee esiin huoli yksityisyyden suojasta. Etäluennan myötä kulutustiedot kulkevat useiden kommunikaatioväylien kautta, ja niitä varastoidaan lukuisille palvelimille. Myös asiakastietoja välitetään ja varastoidaan entistä enemmän. Asiakastietoja on tallennettuna verkkoyhtiöstä ja palveluntarjoajasta riippuen useista sadoista tuhansista muutamiin satoihin. Asiakkaiden yksityisyyden suojan säilyttäminen on tärkeä haaste AMM-järjestelmissä. Vaikka yksittäisen asiakkaan asiakastietojen paljastuminen ei välttämättä aiheuta suurta vahinkoa asiakkaalle, tiedonsiirtoketjussa olevien yritysten maine vaarantuu jos tietoja paljastuu.

### 5.5.1 Asiakastiedot

Asiakkaasta tallennetaan verkkoyhtiön järjestelmiin: nimi, osoite, käyttöpaikan numero, laskutustiedot, sopimustyyppi, tariffit ja kulutustiedot. Tahallinen osapuoli voi itse paikan päällä käymättä käyttöpaikan kulutustiedoista päätellä asukkaiden vuorokausirytmiä ja tehdä arvauksia milloin huoneistossa ollaan paikalla. Rajatuissa tapauksissa myös osoittaminen, että henkilö on ollut huoneistossa paikalla tiettynä aikana, voi olla vahingollista tietoa. Yritysten sähkönkulutustietojen urkkimisella voidaan saada kriittistä tietoa kilpailijalle esimerkiksi tuotantolaitosten kapasiteetista ja käyttöasteesta.

### 5.5.2 NILM

NILM (Non-Intrusive Load Monitoring)-termillä tarkoitetaan sähkön kulutustiedon (kuten teho ja loistehot) sekä jännitteenmuutosten tarkkaa noin sekuntitason monitorointia ja analysointia, jolla pystytään tunnistamaan erilaisia sähkölaitteita kotitalouksista. Mittarilta saatua tietoa verrataan valmiiseen kulutusprofiiliin, jonka perusteella laite ja toiminto voidaan päätellä. NILM-tekniikalla voidaan havaita milloin jokin laite käynnistetään ja sammutetaan, ja mikä laite on kyseessä.

Etäluettavat sähkömittarit mahdollistavat entistä tarkemman kulutustiedon seuraamisen, mutta tällä hetkellä Suomessa välitetään pääsääntöisesti vain tuntikulutuslukemat. Nykyisten tuntikulutuslukemien tarkkuudella tarkkoja analyysejä sähkölaitteista ei pystytä tekemään, mutta tulevaisuudessa sähköverkkoyhtiölle tullaan välittämään entistä tarkempaa kulutustietoa.

### 5.5.1 Minuuttitason kulutustiedot

Monet jo nyt käytössä olevat AMM-järjestelmät pystyvät jo nyt käsittelemään minuuttitason kulutusmittaustietoja mutta korkeintaan muutamista kulutuskohteista kerrallaan, koska järjestelmien kapasiteetti on mitoitettu lähinnä tuntimittausten luennan mukaan. Tuntimittauksia tiheämpiä AMM-mittauksia käytetään tarvittaessa esimerkiksi loistehojen ja jakeluverkon kuormituksen hallinnassa.

## 5.6 Sähkömittareihin kohdistuvat tietoturvauhkat

### 5.6.1 Fyysinen pääsy mittarille

Fyysinen pääsy sähkömittarille on useimmiten helppoa. Omakotitaloasujalla sähkömittarille pääsyä ei ole estetty lainkaan. Kerrostaloissa ja rivitaloyhtiöissä kaikki sähkömittarit ovat sijoitettuna samaan lukittuun tilaan. Usein taloyhtiön yleisavaimella pääsee tähän tilaan, ja taloyhtiön jäsen saa yleisavaimen lainaan tai omakseen suhteellisen helposti. Jotkut sähkömittarit ovat rakennusten ulkopuolella muidenkin kuin asukkaiden saatavilla.

Mittareiden tärkeimmät osat ovat suojattuina kannen alle, jonka aukaisusta tulee hälytys. Hälytyksiin reagointi ja niiden tarkkailu on verkkoyhtiön vastuulla. Hyökkääjä on voinut jo perehtyä mittarin komponentteihin etukäteen toisen vastaavanlaisen mittarin tai ohjeiden avulla. Myös kantta aukaisematta voi yhteyden muodostaminen onnistua, sillä kaikki rajapinnat eivät ole kaikissa mittareissa sijoitettuna kannen alle. Optinen luentasilmä on useimmiten mittarin ulkopuolella.

Mittarin kannen alta löytyy mittarin piirilevy, jonka komponentteja hyökkääjä voi sulautetun elektroniikan toteutuksesta riippuen analysoida. Julkaisussa Advanced Metering Infrastructure AMI Attack Methodology kuvaillaan tapoja piirilevyn komponenttien (mikropiirit, EEPROM-muistit ja radiosirut) ja väylien analyysiin [Inguardians, 2009]. Tyypillisimpiä etäluettavan mittarin komponentteja ovat:

- Analog/Digitital-konvertteri
- Mikropiirit
- EEPROM-muisti
- Komponenttien väliset väylät
- Sarjaväylä: Optinen portti, ja yhteys AMR-järjestelmään
- Käyttöliittymä: LCD-näyttö ja napit toimintojen selailuun
- Pulssinäyttö
- Virtalähde / Akku
- Sulautettu tietokone: datan keräys ja lokien hallinta, kello, muistinhallinta.

Yksi AMI Attack Methodology-raportin esittelmistä hyökkäystavoista on väyläanalyysi. Yhdessä raportin esittelemistä menetelmistä monitoroidaan EEPROM komponentin väylää kahdella lääkeruiskusta tehdyllä anturilla. Muistipiirin sisältö voidaan ottaa talteen tällä menetelmällä sähkömittarin ollessa käynnissä. Sähkömittarin komponentteja voidaan myös irrottaa piirilevystä lämmittämällä, ja kytkemällä komponentti analysaattoriin.

### 5.6.2 Optinen yhteys mittariin

Useissa etäluettavissa mittareissa on optinen luentasilmä huolto –ja asennustoimia varten. Optinen yhteys toimii infrapunalla, ja se on tarkoitettu käytettäväksi tarkoitukseen sopivalla asentajan kannettavalla laitteella. Luentasilmä on useimmiten mittarin ulkopuolella, joten mittarin kantta ei tarvitse avata. Porttien kuuluu olla aina salasanasuojattuja, mutta samaa salasanaa voidaan käyttää isonkin mittarijoukon kesken. Edellisessä luvussa kuvatulla komponenttitason analyysillä salasana saattaa paljastua, ellei riittäviä suojausmekanismeja ole olemassa. Salasanan julkaisu esimerkiksi Internetin keskustelupalstalla voi motivoida kokeiluihin.

Optisen yhteyden kautta voi lukea mittarin kulutustietoja, ja myös mittarin mittausparametrien muokkaus saattaa onnistua toteutuksesta riippuen. Tietoturvakäytäntöjen ollessa hyvät mittausparametrien muutos ei ole mahdollista, tai muutoksen tekeminen aiheuttaa hälytyksen joka havaitaan verkkoyhtiössä. Maailmalla on julkaistu hyökkäyksiä etäluettavien sähkömittareiden optisia portteja vastaan [Inguardians, 2012], mutta hyökkäysten toimivuudesta Suomessa käytettäviin mittareihin ei ole tietoa. Hyökkääjä tarvitsee optisen usb-adapterin, joita on saatavilla ulkomaisista verkkokaupoista. Esimerkki optisesta anturista löytyy Abacus Electrics-nimiseltä valmistajalta. Kyseisen valmistajan protokollamääritykset täsmäävät osaan taulukossa 2 listatuista IEC-standardeista.

http://www.abacuselectrics.com/probspec.htm

Alla kaksi open source-työkalua, joilla optista porttia voidaan testata. Mittareiden porttien toteutukset ovat aina valmistajakohtaisia, joten työkalut eivät toimi kaikkien mittareiden kanssa.

- Termineter
  http://code.google.com/p/termineter/

- OptiGuard
  http://code.google.com/p/termineter/

### 5.6.3 SIM-kortti

Etäluettavissa sähkömittareissa, jotka eivät kommunikoi konsentraattorin kanssa on GPRS/3G modeemi, ja liittymään tarvittava SIM (Subscriber Identity Module) -kortti. Kortti on samanlainen kuin matkapuhelimissa käytettävä, mutta liittymä tulee olla rajoitettu omaan APN-yhteyteen. Jos rajaus on toteutettu oikein, SIM-korttiin ei myöskään voi soittaa tai lähettää SMS-viestejä matkapuhelinverkon kautta.

### 5.6.4 Sarjaliitäntä kaapelilla

Mittareiden välinen kommunikointi voi olla toteutettu kaapelilla sarjaliitännällä. Tällöin monimittauskeskuksessa hyökkääjä voi salakuunnella huomaamattomasti kaapelia ja lähettää omaa liikennettä kaapeliin kytketyillä antureilla.

### 5.6.5 Palvelunestohyökkäykset ja häirintä

Palvelunestohyökkäykset ovat yksi tyypillisimmistä hyökkäystavoista tietojärjestelmiin. Ne eivät välttämättä tarvitse kovin suurta osaamista, mutta voivat aiheuttaa huomattavia ongelmia erityisesti saatavuuteen. AMM-järjestelmässä yksi kriittisimmistä palvelunestohyökkäyksen kohteista on konsentraattori (tai master-mittari). Konsentraattori kommunikoi luentajärjestelmään matkapuhelinverkon kautta. Sopivalla Internetistä tilatulla häirintälähettimellä voidaan katkaista pieneltä paikalliselta alueelta kommunikaatio. Häirintälähettimet ovat Suomessa laittomia, mutta Internetistä löytyy useita häirintälähettimiä myyviä verkkokauppoja. Myös mittarin ja konsentraattorin tai mittareiden välistä keskinäistä liikennettä voidaan häiritä. Alla olevassa luvussa on kuvattu PLC-kommunikoinnin häirintää.

### 5.6.6 PLC

PLC:n ongelma tietoturvan kannalta on se, että kommunikaatiota ei voida rajata sähkömittarin ja konsentraattorin väliseksi. PLC kommunikaatio kaikuu sähköjohtoja pitkin ympäri taloyhtiötä, joten sitä voi kuunnella useista eri pisteistä asianmukaisella laitteistolla. Pistorasioita löytyy useimmiten myös taloyhtiön ulkopuolelta. PLC liikenne on yleensä salattua RC4-algoritmilla, mutta valmistajakohtaisia eroja löytyy. Salausavaimet ovat esijaettuina mittareihin ja konsentraattoreihin [Rokka, 2011]. Järjestelmän toteutuksesta riippuu, ovatko salausavaimet samat kaikilla mittareilla, tai samat jopa kaikilla koko verkkoyhtiön mittareilla. Tällöin uhkana on yhden salausavaimen päätyminen hyökkääjälle joka pystyy tämän jälkeen oikealla laitteistolla tarkkailemaan usean talouden kulutusta. Salasanojen vaihtaminen koko mittarikannasta voi olla raskas operaatio, varsinkin jos turvallinen vaihto ei onnistu etänä.

Vaikka hyökkääjä saisikin tallennettua liikennettä, salattua liikennettä ei ole helppoa saada auki. Sen sijaan hyökkääjä voi lähettää itse omalla laitteellaan tallennettua liikennettä eteenpäin, ja yrittää sekoittaa näin tiedonsiirtoyhteyttä. Joissakin tapauksissa salausavain voidaan laskea liikenteestä auki, mikäli liikennettä on mahdollista tallentaa riittävästi, ja varsinkin jos liikenteestä on mahdollista erottaa tunnettuja osia.

PLC-liikenne on myös erittäin altis häiriöille, joita voivat aiheuttaa taajuusmuuttajat, hakkuriteholähteet, energiansäästölamput, UPS-laitteet, himmentimet, suuritaajuinen kohina ja invertterit [Rokka, 2011]. Hyökkääjän tavoitteen ollessa PLC-liikenteen häiritseminen sen toteutus on helppoa, erityisesti taloyhtiöiden monimittauspisteissä, missä mittarit ovat lähekkäin.

Tiedonsiirtokyvyn kannalta PLC ei ole luotettavin vaihtoehto, mutta se on kustannustehokas koska kommunikointikanavaa ei tarvitse erikseen rakentaa. PLC-tekniikan on myös havaittu aiheuttavan häiriöitä sähkölaitteissa, jotka eivät noudata EMC (Electromagnetic Compatibility) -vaatimuksia. Esimerkiksi himmennettävissä valaisimissa on havaittu häiriöitä PLC-tekniikan kanssa [Pikkarainen, 2012].

## 5.7 Luentajärjestelmän kautta mittareihin kohdistuvat hyökkäykset

AMM-järjestelmillä ei pelkästään lueta mittaustietoja ja mittarin toimintaa seuraavia hälytystietoja. Niillä hoidetaan myös mittareiden hallinta etätiedonsiirtoyhteyden yli. Kuormien ja etäkytkentöjen ohjausten lisäksi niillä ylläpidetään mittareiden asetuksia ja ohjelmistoja sekä salasanoja. Onnistuessaan tunkeutumaan AMM-järjestelmän keskitettyihin osiin hyökkääjä voisi päästä vaikuttamaan hyvin suureen määrään mittareita ja siten saada aikaan suuria vahinkoja.

### 5.7.1 Etäkytkentöjen massaohjaukset

Luentajärjestelmässä on toimintoja vain yksittäin suoritetuille etäkytkentöjen ohjauksille. Luentajärjestelmä toteuttaa kuitenkin myös taustalla toimivien informaatiojärjestelmien komentojen välityspalvelua, ilman mahdollisuutta välitettävien komentojen systemaattisiin oikeellisuustarkistuksiin. Niinpä on syytä ottaa huomioon myös se uhka, että etäkytkentöjä jotenkin onnistuttaisiin tekemään suuressa mitassa yhtä aikaa. Esimerkiksi kaikkien kuormien kytkeminen kuormitushuipun aikana pois kaikilta AMM-järjestelmän piirissä olevilta asiakkailta aiheuttaa niin isoja muutoksia tehovirtauksiin, että jännitteen säädöt eivät välttämättä ehdi mukaan ja seurauksena voi olla jakeluverkon katkaisimien laukeaminen asiakkaiden ja verkon suojelemiseksi. Jos sama tapahtuisi useamman verkkoyhtiön alueella, niin valtakunnan verkon tehotasapainon hallinta voisi jopa vaarantua ja laajan sähkökatkon riski oleellisesti kasvaa. Myös sähköjen yhtäaikainen kytkeminen takaisin päälle aiheuttaa vastaavanlaisia ongelmia. Tällöin lisää hankaluuksia aiheuttaa se, että sähköjen palatessa monet kuormat ainakin lyhyen aikaa ottavat varsin korkean virran ladatakseen katkon aikana purkautuneet energiavarastot (lämpötila, liike-energia, sähkövarasto). Yllättäviin etäkytkentöihin liittyy aina myös kuluttajiin kohdistuvia riskejä; jakelupoikkeamat testaavat sähkölaitteita ja saattavat paljastaa piileviä vikoja asiakkaiden järjestelmissä.

Etäkytkentöihin liittyy vakavan vahingon riskejä, jotka saattavat materialisoitua virheellisen etäkytkennän yhteydessä. Jos lämmitys perustuu pääasiassa sähköön ja sähköt ovat liian kauan pois päältä, voi katkaisun seurauksena jäätyminen aiheuttaa kalliisiin vesivahinkoihin johtavia rakennusten putkivaurioita tai poikkeuksellisissa ääritilanteissa jopa asukkaiden paleltumistapauksia. Sähkön syötön kytkeminen ilman asiakkaan varmistusta voi puolestaan johtaa tulipaloon, jos asiakas on ollut poikkeustilanteen aikana huolimaton ja sähkölaitteita on jäänyt keskeytyksen aikana virheellisesti päälle.

Virheellisiä etäkytkentöjä voivat varsinaisten tietoturvahyökkäysten lisäksi aiheuttaa inhimilliset erehdykset, huolimattomuudesta, koulutuksen puutteesta tai puutteellisesta toimintaohjeistuksesta johtuvat virheet – siis prosessivirheet, esim. mittarin asennus- ja käyttöönottoprosessissa – sekä ohjelmistovirheet ja vikaantuneet laitteet kuten ohjausreleet. Asiaton hyvin monen kohteen yhtäaikainen sähköjen päälle tai poiskytkeminen sähköjärjestelmän kannalta hankalaan aikaan voi puolestaan edellä mainittujen haittojen lisäksi merkittävästi lisätä riskiä, että sähköjärjestelmä joutuu paikallisesti, alueellisesti tai laajemmin sellaiseen häiriötilaan, jossa sähkön toimitusvarmuus enemmän tai vähemmän kärsii. Tätä uhkaa pienentää merkittävästi se, että AMM-järjestelmissä ei yleensä ole toteutettu kuormien etäkytkennän massaohjaustoimintoja. Lisäksi useimmat AMM-järjestelmien tiedonsiirtoratkaisut eivät mahdollista ohjauskomentojen yhtäaikaista jakelua, ja etäohjauksen toteutusteknologia voikin aiheuttaa kytkentöjen (ja kuormien ohjausten) toteutukseen useiden minuuttien tai jopa tuntien hajonnan. Näin ollen massana tapahtuvan etäkytkennän toteuttaminen AMM-järjestelmän komennoilla on usein käytännössä lähes mahdotonta tai ainakin hyvin vaikeaa.

### 5.7.2 Kuormien etäohjaukset massana

Kuormien etäohjauksien perässä on huomattavasti vähemmän tehoa kuin etäkytkentöjen piirissä. Toisaalta etäohjauksia on tarvetta käyttää massana eli hyvin monessa kohteessa lähes samanaikaisesti. Muuten tärkeimmät vaikutukset ovat samoja kuin vastaavalla määrällä etäkytkentöjen massaohjauksia. Tosin esimerkiksi mahdollinen jäätymisvaara on vain niissä kohteissa, joissa ohjataan suoraan sähköt katkaisevaa relettä. Jos ohjaus kohdistuu asetusarvoon tai välissä on paikallinen ohjauksen keston rajoitustoiminto, niin jäätymisen vaara on merkittävästi pienempi.

### 5.7.3 Aikaohjaukset

Useimmissa nykyisin käytössä olevissa AMM-järjestelmissä ohjauskalenterin muuttaminen tapahtuu manuaalisesti ja on siksi melko hidasta, mikä saattaa jossakin määrin myös hidastaa reagointia mahdollisiin ongelmiin. On siis syytä huolehtia siitä, että aikaohjauskalenterien

muuttaminen vahingossa tai asiattomasti ei ole liian helposti tehtävissä ja että mahdolliset muutokset huomataan hyvissä ajoin ennen kuin ohjauksien aika tulee. Aikaohjausten takana on niin paljon kuormaa, että ikävästi ajoittuvilla etäohjauksilla on mahdollista pahimmillaan aiheuttaa kohtalaisen isoja vahinkoja kuten laajoja sähkökatkoja. Lämmitys- tai valaistusaikojen muuttaminen liian lyhyiksi aiheuttaa myös sähkön käyttäjille hankaluuksia, kuten rakennusten jäähtymistä tai toiminnan vaarantumista.

AMM-järjestelmien kautta kalenteriin perustuvilla aikaohjauksilla ohjataan myös katuvaloja joissakin jakeluverkkoyhtiöissä, lähinnä silloin kun kyseinen tiedonsiirtoratkaisu ei mahdollista välitöntä ohjausta. Jakeluverkon luotettavan toiminnan kannalta katuvalojen ohjattava teho tuskin riittää aiheuttamaan tehotaseen, jännitetaseiden ja verkon kuormituksen hallinnan suhteen ongelmia, mutta samanaikaisesti muiden ohjattavien kuormien kanssa ohjattuna voi kyllä pahentaa tilannetta merkittävästi.

Varsinkin vanhat, täysin varaavan lämmityksen aikaohjauskohteet on tyypillisesti toteutettu niin, että varaava lämmitys kytkeytyy kokonaan pois eikä suoraa lämmitystä ole juuri lainkaan. Sen sijaan monissa uudemmissa ja osittain varaavissa kohteissa ohjataan lämmityksen asetusarvoja. Tästä tavasta on se etu, että lämmitys ei kokonaan lopu eikä suuria vahinkoja synny vaikka mittarista ei tulisikaan lämmityksen ohjausta takaisin päälle. Asetusarvojen käyttämisen sijasta lämmitystä suoraan ohjattaessa voi mittarin tai ohjausreleen vikaantuminen pahimmillaan johtaa rakennuksen kylmenemiseen niin, että uhkana on putkien jäätyminen ja siitä seuraavat vesivahingot, Jos tietoturvan pettäminen tai ohjelmistovika johtaa suuressa joukossa tällaisia kohteita mittareiden toiminnan yhtäaikaiseen lakkaamiseen kovien pakkasten aikana, voivat kuluttajille aiheutuvat vahingot olla varsin suuria ja korvausvastuukysymykset hankalia. Sen sijaan pitkäkään tietoliikennekatko ei yleensä voi aiheuttaa suurta vahinkoa. Lämmitys palaa kalenterin perusteella, sillä aikaohjaus on nykyisin tyypillisesti toteutettu mittarissa olevan kalenterin kautta, ja uusien ohjaustietojen puuttuessa mittari käyttää aiempia tietoja esimerkiksi edelliseltä vuorokaudelta.

### 5.7.4 Mittareiden ohjelmistojen ja asetusten etäpäivitykset

Mittareiden ohjelmistojen, asetusten ja salasanojen etäpäivitysten kautta on ainakin periaatteessa mahdollista aiheuttaa kaikkia jo edellä kuvattuja vahinkoja hyvin suuressa mittakaavassa eli kaikissa niissä järjestelmissä, joihin kyseinen päivitys kohdistuu. Erityisesti virheellinen päivitys voi pysäyttää mittarin tietoliikenteen, jolloin on käytävä paikan päällä vaihtamassa mittarit ja samalla keräämässä niistä mittausdatat. Vielä paljon pahempi on, jos virheellinen päivitys pysäyttää myös mittausohjelman toiminnan ja mahdollisesti jopa hävittää mittarien muistista mittausdatat. Tällöin on kaikki mittarit käytävä vaihtamassa ja sen lisäksi joudutaan turvautumaan laajaan arviolaskutukseen. Seurauksena olisi kiireellisyydestä johtuvien suurten mittarinvaihtokustannusten lisäksi asiakkaiden luottamuksen menetys sekä valvovien viranomaisten asettamat sanktiot.

Niinpä mittareissa ja lukujärjestelmissä varmistaudutaan monin keinoin siitä, että päivitykset ovat alkuperältään oikeita ja kohdistuvat pelkästään niille rajattuun asiaan. Silti voi jäädä pieni mahdollisuus, että jossakin olisi kohtalokas haavoittuvuus ja päivityksessä siihen kohdistuva haittaohjelma tai virhe. Siksi päivitykset aina testataan ensin laboratoriossa ja sitten otetaan käyttöön vaiheittain pienellä erällä aloittaen.

Päivityksien osalta myös alihankintaketjun sekä varsinkin AMM-järjestelmän toimittajan tietoturvan hallinta ovat kriittisiä. Päivitykset eivät yleensä tule lähdekielisinä, joten kääntämisen ja linkkauksen aikaisia tarkistuksia ja lähdekielen tarkastelua ei päästä tekemään. Näin ollen on toisaalta pakko luottaa järjestelmätoimittajiin ja toisaalta lisäksi syytä kohtuullisessa määrin varautua eri tavoin siihen, että tietyntyyppisiä mahdollisia hyökkääjiä voi houkuttaa päivitysten kautta AMM-järjestelmiin ja mittareihin vaikuttaminen.

## 5.8 Tietojärjestelmiin kohdistuvat hyökkäykset

Jakeluverkkoyhtiön ja palveluntarjoajan tietojärjestelmiin kohdistuu sisäisiä ja ulkoisia tietoturvauhkia, joihin liittyvien riskikokonaisuuksien hallitseminen voi olla vaikeaa. Esimerkiksi asiakas-, paikka- ja laskutustietojen asiaton nuuskinta ja julkaiseminen tai jopa muuttaminen sekä yhdistäminen yksityiskohtaisiin kulutustietoihin voivat uhata normaalin jakeluverkon avulla tehtävän liiketoiminnan jatkuvuutta ja uskottavuutta.

Yksi hyökkäystapa tietoverkkoihin on tulo suoraan Internetistä käsin – hyökkääjä murtautuu verkkoon, ja kerää sekä myy tietoja jotka ovat kerätty esimerkiksi asiakastietopalvelimelta. Sisäverkkoon pääsyn voi mahdollistaa esimerkiksi etäyhteyskäytävä – jota ei alunperin olisi pitänyt edes olla – kolmannen osapuolen huoltotoimenpiteitä varten ja jolla pääsee suoraan sisäverkkoon. Myöskään palveluntarjoajan tai verkkoyhtiön sisäverkko ei välttämättä ole niin turvallinen kuin on määritelty ja luullaan. Tietoverkkojen auditointeja tai penetraatiotestauksia ei vielä nykytilanteessa tehdä järjestelmällisesti ja monet asiat verkkojen hallinnassa perustuvat luottamukseen.

## 5.9 Hyökkäykset AMM-järjestelmän kautta verkkoyhtiön kriittisiin järjestelmiin

AMM-järjestelmä lisää hyökkäysrajapintaa ja haavoittuvuuksia hyökkääjän hyödynnettäväksi, jos jakeluverkkoyhtiön kriittiset järjestelmät, kuten verkostoautomaation operatiiviset järjestelmät (SCADA , sähköasema-automaatio, yms.) eivät ole riittävän hyvin erotettu AMM-järjestelmästä palomuureilla omaksi tietoturvavyöhykkeekseen. Kriittisiin järjestelmiin kohdistunut onnistunut hyökkäys voi pahimmillaan aiheuttaa huomattavasti isomman vahingon kuin AMM-järjestelmään kohdistunut hyökkäys. AMM-järjestelmän ja operatiivisen verkostoautomaation riittävä eristäminen toisistaan sekä niiden välisen liikenteen valvonta eivät ole erityisen vaikeita toteuttaa, sillä kyseisellä välillä tiedonsiirtotarpeet ja osapuolet ovat hyvin tarkkaan tiedossa.

## 5.10 Uhkaskenaarioiden riskin suuruuden arviointi projektin työpajassa

Projektissa järjestettiin 26.9.2013 työpaja, jonka yhtenä sisältönä oli tiettyjen AMM-järjestelmiin kohdistuvien korkean tason uhkaskenaarioiden (projektissa käytetty nimitys ”tyyppiskenaario”) riskin suuruuden arviointi karkealla tasolla. Työpajassa oli mukana AMM-järjestelmien kehittäjien, käyttäjien ja palveluntarjoajien edustajia yhteensä 23 henkilöä. Arvioitavia skenaarioita oli kaikkiaan 16 kappaletta. Lähtökohtaskenaariot, pääosa skenaarioista, oli muodostettu VTT:n projektiryhmän toimesta, ja arviointiin osallistuneet asiantuntijat täydensivät skenaariolistan parilla uudella skenaariolla. Skenaarioihin liittyvän riskin suuruuden arvioimiseksi kohdeympäristö tulee kiinnittää; tässä kohteeksi sovittiin keskimääräinen 100 000 mittarin verkkoyhtiö. Tyyppiskenaariot olivat seuraavat:

Hyökkääjä vaikuttaa sähkönkulutuksen mittaustietoon

1. Yhteen mittariin
2. Lähialueverkko (keskitin, master) kerrallaan
3. Koko luentajärjestelmän laajuudelta

Mittarin ja luentajärjestelmän välinen kommunikointi estetään.

4. Yhteen mittariin
5. Lähialueverkko (keskitin, master) kerrallaan
6. Koko luentajärjestelmän laajuudelta

Asiakaskohtaisten kulutustietojen vuotaminen

7. Yhden asiakkaan tiedot julkisuuteen
8. Koko asiakastietokannan tiedot julkisuuteen
9. Urkinta (ei julkisuuteen)

Hyökkääjä vaikuttaa mittariohjauksiin: päälle/pois-kytkentä

10. Yhteen mittariin
11. Koko luentajärjestelmän laajuudelta

Hyökkääjä vaikuttaa mittariohjauksiin: kuormanohjaukset

12. Yhteen mittariin
13. Koko luentajärjestelmän laajuudelta

14. Hyökkääjä tunkeutuu AMM-järjestelmän kautta verkkoyhtiön kriittisiin järjestelmiin, kuten verkostoautomaatioon

15. Hyökkäys, vahinko tai virhe mittarien ohjelmistopäivityksessä, joka estää mittarin kommunikoinnin

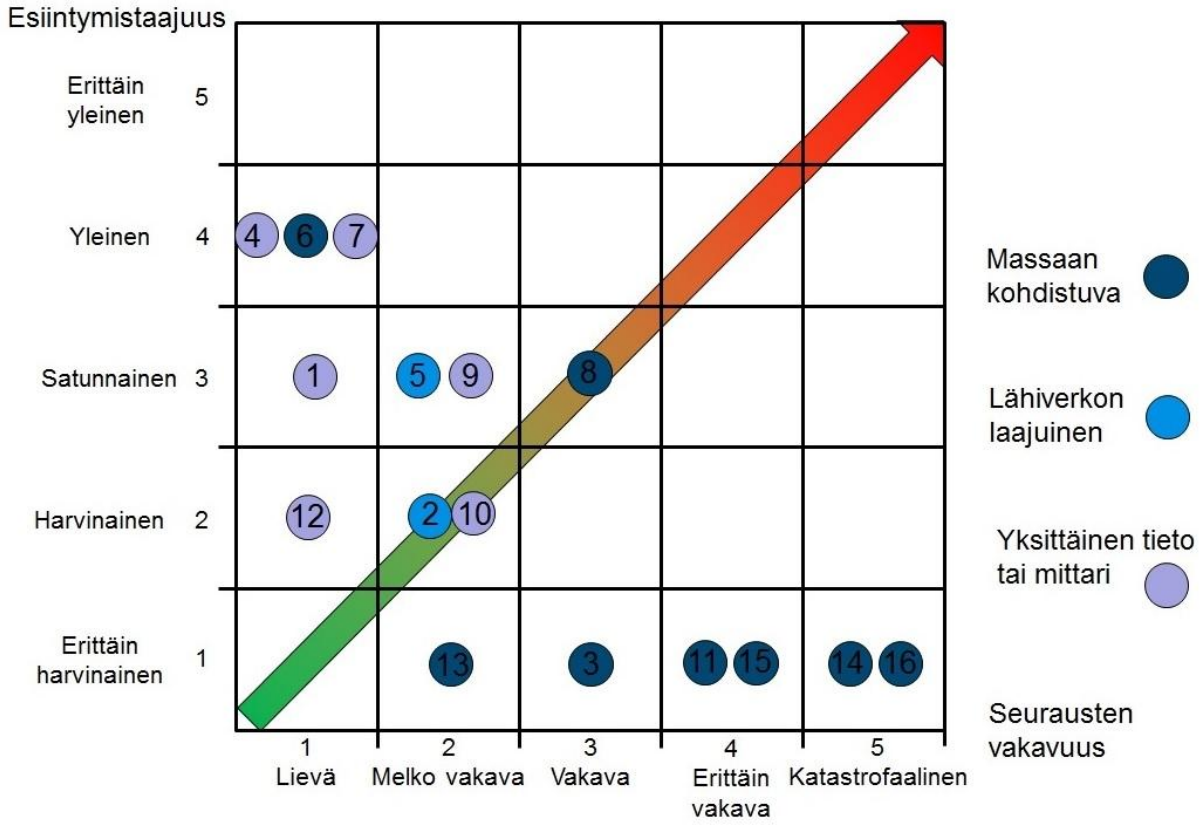
16. Hyökkäys, vahinko tai virhe mittarien ohjelmistopäivityksessä, joka estää mittarin mittaamisen.

Skenaarioihin liittyvä riskin suuruuden arviointi toteutettiin arvioimalla kunkin skenaarion kohdalla erikseen seurausten vakavuutta ja esiintymistaajuutta viisiportaisilla asteikoilla. Käytetyt asteikot on esitetty alla taulukossa 4. Koska jotkut skenaariot voivat realisoitua useista erilaisista syistä (esim. hakkeri, inhimillinen virhe tai laitevika), käytiin eri syytekijöiden todennäköisyyksien osalta välillä melko runsastakin keskustelua skenaarion esiintymistaajuutta arvioitaessa.

| **Seurausten vakavuus** | | **Esiintymistaajuus** | |
|---|---|---|---|
| Luokka | Kuvaus | Luokka | Kuvaus |
| 1 Lievä | Ylimääräiset kustannukset alle 10 000 eur | 1 Erittäin harvinainen | Esiintyy harvemmin kuin kerran 200 vuodessa. |
| 2 Melko vakava | 10 000 – 100 000 eur | 2 Harvinainen | Esiintyy ainakin kerran 200 vuodessa, mutta harvemmin kuin kerran 20 vuodessa. |
| 3 Vakava | 100 000 eur – 1 Meur | 3 Satunnainen | Esiintyy ainakin kerran 20 vuodessa, mutta harvemmin kuin kerran 2 vuodessa. |
| 4 Erittäin vakava | 1 – 10 Meur | 4 Yleinen | Esiintyy ainakin kerran 2 vuodessa, mutta harvemmin kuin viisi kertaa vuodessa |
| 5 Katastrofaalinen | Yli 10 Meur | 5 Erittäin yleinen | Esiintyy ainakin viisi kertaa vuodessa |

*Taulukko 4 Skenaarioiden arvioinnissa käytetyt asteikot*

Arvioitujen skenaarioiden sijoittuminen riskimatriisiin on esitetty kuvassa 7. Riskimatriisista voidaan havaita, että skenaarioista ei ryhmän arvioinnin perusteella löytynyt yhtään sellaista, joka olisi ollut yhtä aikaa esiintymistaajuudeltaan yleinen tai erittäin yleinen (luokka 4 tai 5) ja (taloudellisilta) seurauksiltaan erittäin vakava tai katastrofaalinen (luokka 4 tai 5). Suureen joukkoon mittareita kohdistuneet skenaariot nähtiin esiintymistaajuudeltaan lähes poikkeuksetta erittäin harvinaisina.




*Kuva 6. Skenaarioiden sijoittuminen riskimatriisiin.*

# 6. Suosituksia AMM-järjestelmien tietoturvan parantamiseksi

Luvussa esitellään AMM-järjestelmien tietoturvan osa-alueita, joissa alan toimijoilla voi olla kehittämistarpeita ja joihin tulee kiinnittää erityistä huomiota. Aiheet ovat nousseet esiin työpajakäynneillä käydyissä keskusteluissa, sekä projektin aihepiiriä koskevia julkaisuja ja raportteja tutkittaessa.

**Alihankintaketju ja sopimukset**

Palveluiden tarjoajista ja järjestelmätoimittajista koostuvat alihankkijaketjut ovat usein melko pitkiä ja mutkikkaita. Sopimuksiin, tietoturvatietoisuuteen ja sitä parantavaan koulutukseen, käyttöoikeuksien hallintaan ja sisäpiiriuhkiin on syytä kiinnittää huomiota.

**Asiakastietojen tietoturvallinen käsittely ja tallennus**

Asiakastiedot eivätkä varsinkaan niiden ja asiakkaan kulutustietojen yhdistelmä saa joutua asiattomiin käsiin. Seuraaviin asioihin on syytä kiinnittää huomiota:
1) Mittareiden asennuksissa ja paikan päältä tapahtuvassa ylläpidossa käsitellään asiakastietoja.
2) Palvelurajapinta, jonka kautta kuluttaja voi lukea tuntikulutustietojaan internetin kautta voi sisältää haavoittuvuuksia, joiden kautta ulkopuolinen voi päästä käsiksi toisia kuluttajia koskeviin asiakastietoihin.
3) Oma tai alihankkijan henkilöstö voi vahingossa esim. kiireessä ja ajattelemattomuuttaan tai jopa tahallaan paljastaa ulkopuoliselle asiakastietoja tai pääsyn niitä sisältävään tietokantaan.

**Laajassa käytössä hyväksi havaittujen tietoturvastandardien hyödyntäminen**

Hyvin tunnettuja ja laajalti testattuja tietoturvaratkaisuja käytettäessä tiedetään millainen suojaustaso niillä oikein käytettynä saavutetaan. Esimerkiksi AMM-järjestelmätoimittajan mahdollisten omien tietoturvaratkaisujen ongelmana on se, että niitä ei ole riittävässä määrin voitu riippumattomasti testata ja että useimmiten tiedot niiden ominaisuuksista, tekijöistä ja mahdollisista haavoittuvuuksista eivät ole julkisia. Valmistajakohtaisten tietoturvaratkaisujen tekijöiden puutteellinen tietoturvaosaaminen voi aiheuttaa merkittäviä haavoittuvuuksia esimerkiksi pienten toteutusvirheiden kautta.

On myös havaittu, että teknologia- ja asiantuntijayritysten sekä jopa standardointiorganisaatioiden suosituksiin on syytä suhtautua varauksin. Jopa monien tietoturvastandardien tärkeän lähteen NISTin (the U.S. National Institute of Standards) hyvänä pidetty maine on nyt kärsinyt eikä sekään siis ole epäilysten ulkopuolella [Newman 2013]. Epäilykset perustuvat suurelta osin Edward Snowdenin ja the New York Timesin paljastuksiin siitä, että eräs jo vuonna 2007 tunnetuksi tullut salausalgoritmien haavoittuvuus eräässä NIST:in silti suosittelemassa satunnaislukugeneraattorissa (Dual EC DRBG) oli tahallaan tehty. Äskettäin NIST on tehnyt myös epäilyttäviä muutoksia salausalgoritmien uuteen hash-funktioon (SHA-3) [Newman 2013].

Käytettävien tietoturvastandardien arviointiin tarvitaan kotimaista luotettavaksi tiedettyä tietoturvan asiantuntemusta, vaikka kyber-sodankäynnin kohteeksi joutumisen riskiä ei pidettäisikään merkittävänä. Nykyisin niin aktivistit kuin terroristitkin osaavat etsiä ja käyttää salausmenetelmiin tarkoituksella tehtyjä takaovia, omatoimisesti ja ostopalveluna.

**Tietoturvariskien hallinta**

Systemaattinen tietoturvariskien hallinta on tärkeää AMM-ympäristöjen elinkaaren kaikissa vaiheissa. Apuna voi käyttää esimerkiksi kansainvälistä suomenkielistä SFS-ISO/IEC 27005 tietoturvariskien hallinnan standardia. Standardi on suunnattu organisaation tietoturvariskien

hallinnasta vastaaville johtajille ja tietoturvahenkilöille ja se sovellusalue on laaja. Standardissa käsitellään mm. tietoturvariskien arviointia, ja niiden hallinnan organisointia. Tärkeää on nähdä tietoturvariskien hallinta jatkuvana prosessina.

**Viestiyhteyksien ja autentikoinnin suojaaminen**

Kriittisen infrastruktuurin järjestelmiä kehitettäessä tulee tietoturvan osalta varmistaa käytetyt algoritmit sekä näiden soveltuvuus annettuun käyttötarkoitukseen. Protokollatoteutukset saattavat valita algoritmin toteutusalustan ja käyttöympäristön mukaan. Kriittisten toimintojen osalta on syytä varmistaa että käytössä on aiotut salaus- ja vahvistusalgoritmit ja niiden oikeat versiot.

**Tarkoituksenmukainen tietoturvavyöhykkeisiin jako**
Pitämällä tietoturvavyöhykkeet riittävän pieninä rajoitetaan yksittäisten haavoittuvuuksien vaikutusalue siedettäväksi. Sisäkkäisillä tietoturvavyöhykkeillä (Defence in depth-periaate) varmistetaan että kriittisiin kohteisiin pääsy edellyttää monen haavoittuvuuden löytämistä, varsinkin, jos eri kerrosten palomuurit eroavat riittävästi tekniikaltaan ja asetuksiltaan toisistaan ja sallivat vain tarpeelliseksi tiedetyn tiedonsiirron. Esimerkiksi jakeluverkkoyhtiön on syytä riittävän hyvillä palomuureilla erottaa kriittiset tietojärjestelmänsä, kuten verkostoautomaatiojärjestelmät erilleen AMM-järjestelmästä.

**Verkkojen liikenteen seuraaminen**

AMM-järjestelmissä tunnetaan varsin tarkkaan se, millainen tietoliikenne missäkin järjestelmän osassa on asiaankuuluvaa ja paljonko sitä kuuluu eri aikoihin olla. Niinpä kannattaa hyödyntää sitä, että asiaton tai muuten virheellinen tietoliikenne on verraten helppo havaita liikennettä seuraamalla ja normaalitilaan vertaamalla. On parempi havaita mahdollinen hyökkäys tai virhe ennen kuin siitä ehtii aiheutua haittaa.

**Päivitysten hallinta**

Erityisesti mittareiden ohjelmistojen ja salasanojen etäpäivitysten kautta on mahdollista aiheuttaa isoja ja vaikeasti korjattavia vahinkoja. Pahinta on jos mittareiden tallentama mittausdatakin tuhotaan, tai saatetaan vaikeasti palautettavaan muotoon. Koska AMM-järjestelmien käyttäjät eivät välttämättä saa ohjelmistopäivityksiä lähdekielellä, voi päivitysten turvallisuuden tarkastaminen olla hyvin vaikeaa eli joudutaan luottamaan järjestelmätoimittajiin ja siihen että niillä ohjelmistojen kehitysprosessin tietoturva on hyvin hoidettu. Siksi on tärkeää, että järjestelmätoimittajan omat päivitysten testausmenettelyt ovat kattavia, perusteellisia sekä luotettavaksi tiedetyn henkilöstön tekemiä. Päivitysten alkuperän varmistus on myös hoidettava huolellisesti. Päivitykset on syytä ensin testata laboratoriossa ja sen jälkeen ottaa ne käyttöön aluksi vain pienessä osassa järjestelmää. Aina pitää myös huolellisesti säilyttää mahdollisuus palauttaa nopeasti vanhat toimivat ohjelmistot käyttöön.

**Varautuminen sisäpiirin välityksellä tai toimesta tehtyihin hyökkäyksiin**

Oman sekä alihankkijoiden ja palveluntuottajien henkilöstön kautta tapahtuvia uhkia on mahdotonta kokonaan torjua, mutta niiden todennäköisyyttä voidaan pienentää ja mahdollisten vahinkojen laajuutta rajata monin muutenkin tietoturvaa parantavin tavoin, esimerkiksi:

- laajan järjestelmän jako riittävän pieniin tietoturvavyöhykkeisiin
- käyttöoikeuksien ja kulkuoikeuksien hallinta, henkilökohtaiset salasanat ja käyttäjätunnukset, käyttöoikeuksien rajaus vain tarpeelliseen
- lokitietojen keruu myös avainkäyttäjien ja pääkäyttäjien toimista, täydennettynä seurantajärjestelmällä joka havaitsee potentiaalisesti uhkan kasvamiseen johtavat toimenpiteet, kuten yksittäisen käyttäjän käyttöoikeuksien jatkuvan kasvattamisen
- henkilökunnan taustojen kartoitus ja koulutus
- suunnitelmat ja ennakoivat toimenpiteet mahdollisten vahinkojen rajaamiseksi.

**Etäkytkentöjen ja kuormanohjausten käytettävyyden ja etenkin oikeellisuuden riittävä turvaaminen**

Yleensä AMM-järjestelmissä ei ole etäkytkentöjen joukko-ohjaustoimintoja vaan kullekin mittarille etäkytkentäkäskyt on laadittava ja tehtävä erikseen. On silti syytä huolehtia että isolle joukolle lähetettävän kytkentäkäskyn lähettäminen ei muullakaan tavoin ole mahdollista.

Siellä missä etäkytkentöjen tarve on hyvin harvinainen, voi olla perusteltua estää etäkytkentäohjausten toteuttaminen, niin että mittarissa toiminto pitää erikseen avata käyttöön esim. etäpäivityksenä.

Kuorman ohjaukset on tehtävä isossa joukossa kohteita yhtä aikaa, joten ryhmäohjausten estäminen ei tule kysymykseen. Useimmiten automaattisia ohjauksia tarvitsevat muut sähkömarkkinaosapuolet kuten sähkön myyjät, kysyntäpuolen joustojen aggregaattorit ja siirtoverkko-operaattori. Ohjauspyynnöt tulevat useimmiten verkkoyhtiölle tai sitä palvelevalle osapuolelle muilta sähkömarkkinoiden osapuolilta sanomina (esim XML). Ohjauskomentojen tiedonsiirtoyhteydet on suojattava riittävin salauksin ja alkuperän varmistuksin. On myös huolehdittava siitä, että ohjauskomentojen käsittely ja edelleen lähetys ovat koko matkalta riittävän hyvin suojattuja esim. muuttamista ja palvelunestohyökkäyksiä vastaan. Ohjauksille kannattaa myös tehdä järkevyystarkastuksia esim. ohjauksen keston suhteen, niin että estetään ohjaukset, jotka voisivat tehdä vahinkoa ohjattavalle kohteelle. Tätä noudattamalla yksittäisten kohteiden virheellisistä ohjauksista tuleva vahinko on varsin pieni. Pääpaino kannattaa suunnata siihen, että estetään suurille kuluttajajoukoille menevien virheellisten ohjausten toteuttaminen. Käyttöpaikoissa missä kuormanohjauksia ei käytetä, ei kyseisiä mittarin lähtöjä ole yleensä kytketty mihinkään ohjattavaan kuormaan.

**Rajapinnat sähkömarkkinaosapuoliin ja erityisesti kuluttajiin**

Kuluttajille on lain perusteella annettava pääsy lukemaan oma tuntikulutuksensa. Suomessa tämä lukeminen pääsääntöisesti toteutetaan julkisen internetin kautta. On syytä varautua siihen, että internetin kautta asiattomat yrittävät päästä käsiksi kuluttajien asiakas- ja mittaustietoihin tai tunkeutua AMM-järjestelmään. Ei voida luottaa siihen, että kaikki kuluttajat onnistuisivat aina pitämään salasanansa ja käyttäjätunnuksensa vain omana tietonaan.

Oma palomuureilla DMZ-vyöhykkeeksi erotettu palvelin rajaa mahdollisen tunkeutumisen aiheuttamia vahinkoja. Myös kyselyjen taajuutta kannattaa rajoittaa niin, että mahdollinen palvelunestohyökkäys ei pääse vaikuttamaan laajemmin sisäisiin järjestelmiin.

Pelkästään sähkömarkkinaosapuolten välisen tiedonvaihdon suojaaminen ei riitä, vaan lisäksi on huolehdittava siitä, että se on hyvin eristetty sisäisistä tietojärjestelmistä ja verkoista, joiden kautta tätä tietoa toisaalta tuotetaan. Sähkömarkkinaosapuolet vaihtuvat joten niihin ei ole syytä tarpeettomasti luottaa tietoturvamielessä. Lisäksi sähkömarkkinalaki edellyttää kaikkien sähkön myyjien tasaveroista kohtelua ja rajoittaa tiukasti niiden pääsyä toistensa asiakkaita koskeviin tietoihin.

**Vaatimusten ja suositusten määrittely**

Sekä olemassa olevien järjestelmien kehittämisen että uusien järjestelmien hankkimisen tueksi tarvitaan yhteisiä ohjeita, vaatimuksia ja suosituksia. Vaatimuksia ja suosituksia on päivitettävä säännöllisin väliajoin ja lisäksi aina tarpeen ilmetessä, koska uhkat, haavoittuvuudet ja suojautumiskeinot sekä niitä koskeva tietoisuus kehittyvät.

**Auditointi ja sertifiointi**

Ulkopuolista tietoturvan auditoinnin asiantuntemusta on syytä käyttää silloin kun oma osaaminen ei riitä.

**Verkostoituminen AMM-tietoturva-asioissa**

Luottamuksellisen tiedonvaihtoverkoston perustaminen, jossa ovat mukana kehittäjät (etäluentajärjestelmien ja mittareiden) ja käyttäjät (verkkoyhtiöt, palveluntarjoajat). Tiedonvaihtoverkostossa jaettaisiin teknologiset ratkaisut, parhaat käytännöt, mokat. Vastaavana esimerkkinä energia-alan E-CIP ryhmä, joka toimii CERT-FI kautta.

http://www.cert.fi/palvelut/toiminta/certfipalvelukuvaus.html

**Varautuminen siihen että tietoturva saattaa kuitenkin pettää**

Vahingon rajaaminen, korjaavat toimenpiteet ja tiedottaminen on syytä tärkeimmiltä osin suunnitella ennen kuin vahinkoa on vielä sattunut. Kiireessä huonosti harkitut ratkaisut saattavat pahentaa tilannetta ja hidastaa vahinkojen rajausta ja torjuntaa. Vahingon tapahduttua on myös tärkeää pystyä osoittamaan, että sen estämiseksi on tehty ne toimenpiteet, joita voi kohtuudella edellyttää.

**Jatkuvuuden hallinta**

Tietoturvan kannalta jatkuvuuden hallinta pitää sisällään uhkien ja haavoittuvuuksien kehittymisen seurannan ja ennakoivan varautumisen uhkakuvien mahdolliseen toteutumiseen. Tehokas seuranta kansallisella tasolla edellyttää yhteistyötä viranomaistahojen kanssa (HVK, CERT-FI) ja verkkoyhtiöiden sekä palveluntarjoajien kesken.

Tätä varten suosittelemme verkostoitumista, esim. verkkoyhtiöiden tietoturvasta vastaavien tahojen yhteistyöfoorumin perustamista. Kansallinen foorumi mm. määrittäisi Suomen kannalta kriittiset toiminnot ja teknologiat, seuraisi näihin liittyviä tietoturvatapahtumia yhteistyössä alan toimijoiden kanssa. Keskeisistä toimijoista mainittakoon FISC (Finnish Information Security Cluster) [FISC 2012], joka jäsenyrityksineen on erikoistunut teollisuusautomaation kyber-/tietoturvapalveluihin ja jonka strategisena tavoitteena on kansallinen teollisen Internetin osaamisen vahvistaminen. Foorumi myös laatisi / laadituttaisi näihin liittyviä toimintaohjeita ennakoivasti sekä välittäisi tietoa mahdollisissa akuuteissa uhkatilanteissa ja sillä tavalla pyrkisi estämään kriisitilanteita ja minimoimaan seurauksia.

Kyber-/tietoturvallisuuden kannalta avainasioita ovat myös:

- Sähköverkkoyhtiön tietojärjestelmien ja -verkkojen tietoturva, kuten rajapintojen ja suojausmekanismien huolellinen konfigurointi ja ajan tasalla pito
- Palveluntarjoajan tietojärjestelmien ja -verkkojen tietoturva
- Sekä oman että alihankkijoiden henkilöstön tietoturvatietoisuuden ylläpito ja koulutus
- Ulkopuolinen arviointi, benchmarking.

# 7. Johtopäätökset

Suomen AMM-järjestelmien käyttöönotto ja yleistyminen on ollut nopeimpia maailmassa ja olemme tiettyjen toteutettujen ominaisuuksiensa suhteen jopa muita edellä. Meillä lainsäädännön asettamia vaatimuksia ovat muun muassa 1) asiakkaiden laskutus todellisen tuntimitatun kulutuksen perusteella, 2) kuluttajien pääsy lukemaan edellisen päivän tuntikohtaiset kulutuksensa ja 3) mahdollisuus mittarin kautta tapahtuvaan kuormanohjaukseen. Suomessa AMM-järjestelmien toteutus pääosin valmis vuoden 2013 loppuun mennessä, vaikka kansainvälisesti yritetään vasta sopia yhteisistä standardeista ja tietoturvakäytännöistä. Euroopassa ensimmäiset riittävän yksityiskohtaiset AMM-järjestelmien tietoturvan toteuttamisen yksityiskohtia koskevat standardit, vaatimukset ja suositukset ovat vasta valmistumassa. On odotettavissa että näistä on hyötyä uusille hankittaville AMM-järjestelmille vaatimusmäärittelyjä ja myös tietoturvavaatimuksia laadittaessa, sekä yleisemminkin vaatimusten toteutumisen todentamisessa ja AMM-järjestelmien riskikartoituksia tehtäessä. Jo asennettujen mittareiden tietoturvaratkaisujen parantamisessa niistä lienee vähemmän apua.

AMM-järjestelmät Suomessa rakentuvat useiden osapuolten muodostamista tiedonsiirtoketjuista. Kulutustietoja siirtyy mittarilta tiedonsiirtoväyliä pitkin useaan järjestelmään joissa niitä muokataan, varastoidaan ja yhdistellään mm. asiakas- ja laskutustietoihin. AMM-järjestelmissä tietoturvan tulee toteutua useilla tasoilla, jotta koko mittaus- ja tiedonsiirtoketjuun voidaan luottaa (sähkömittari, kommunikaatioväylä, tietojärjestelmät, tietoverkot ym.). Haasteelliseksi tilanteen tekee se, että osapuolia ja toimijoita on paljon ja alihankintaketjut voivat olla pitkiä ja ulottua valtiorajojen yli. Projektissa käydyissä työpajakeskusteluissa on havaittu, että käytännöt tietoturvavaatimusten laatimisesta ja vaatimusten toteutumisen seuraamisesta sopimuskumppaneiden välillä vaihtelevat suuresti. Usein järjestelmän osien toteutukset ja vaatimusten hallinta pohjautuvat luottamukseen. Myös teknisellä tasolla tilanne on haasteellinen, koska erilaisia kommunikointiprotokollia ja niiden eri versioita on käytössä suuri määrä. Tämä vaikeuttaa analyyseja ja korjaavia toimenpiteitä.

Sähkömittareissa olevat paikalliset liitännät ovat herättäneet maailmalla hakkereiden mielenkiintoa, mutta onnistuneista uusien mittareiden paikallisista manipuloinneista (tavoitteena esim. kulutuslukeman muutos) ei Suomen tasolla ole kuultu. Fyysistä pääsyä mittareille ei useissa tapauksissa voida estää. On tärkeää, että mittareissa käytetään diagnostiikkatoimintoja, jotka ilmoittavat jos mittariin on tunkeuduttu, sen sähköverkkoon kytkentää muutettu, tai sen tiedonsiirtoverkon toiminta estetty tai häiritty. Lisäksi näiden ilmoitusten seurantamekanismit tulee toteuttaa käytettävyysvaatimukset huomioiden, ja palveluntarjoajan täytyy varautua pitämään verkkoyhtiön ilmoitusten seuranta tehokkaana, ja esim. ylläpitotoimenpiteenä poistamaan ilmoitusten joukosta ne ilmoitukset joiden perustellusti voidaan olettaa kertovan diagnostiikkavirheestä eikä itse järjestelmän toiminnan tai kommunikoinnin virheestä. Jos hälytysten toteutus ja suodatus ovat huonosti suunniteltuja, voivat virheelliset, turhat tai tulvivat hälytykset estää hälytystoimintojen hyödyntämisen.

Verkkoyhtiön maineen kannalta kulutustietojen paljastaminen on vakavaa, varsinkin jos niitä paljastetaan toistuvasti tai suurempana massana. Kulutustietojen suojaaminen on tärkeää, ja ne ovat määritelty luottamuksellisiksi. Tällä hetkellä kuluttajat saavat halutessaan kulutustietonsa web-palvelimen kautta. Tämä palvelin on houkutteleva kohde hyökkääjille, koska palvelimen täytyy olla aina julkisessa Internetissä. Yksityisyyden suojan kannalta yksittäisten kulutustietojen paljastuminen ei ole kuluttajan kannalta tällä hetkellä kovin vahingollista, varsinkaan kun tuntikohtaisesta kulutuksesta ei voi helposti yksilöidä sähkölaitteita. Joissain tilanteissa asukkaalle voi olla vahingollista, jos pystytään hyödyntämään tietoja käyttöpaikan vuorokausirytmistä tai paikallaolotiedosta.

Monissa maissa, kuten Suomessa, mittareilla tehdään etäkytkentöjä ja kuorman ohjauksia. Tietoturvan pettäminen voi niiden kautta aiheuttaa hyvin paljon ja isompia vahinkoja kuin kulutustietojen joutuminen vääriin käsiin. Pahimmillaan mahdollisena seurauksena saattaa aiheutua laajoja sähkökatkoja, sähköverkon komponenttien tuhoutumisia ylikuormitukseen,

tulipaloja tai jopa ihmishenkien menetyksiä. Tämän suuruusluokan ongelmien toteutumisen todennäköisyys on projektin puitteissa arvioitu hyvin pieneksi. AMM-järjestelmän tietoturvan parantaminen ei kuitenkaan yksin riitä estämään sitä, että mahdollinen hyökkääjä voisi onnistua vakavasti häiritsemään sähköinfrastruktuurin toimintaa. Kotiautomaation ja rakennusautomaation sekä niiden etähallinnan tietoturvan puutteet saattavat nimittäin toisaalla avata mahdollisuuksia ohjata suurta määrää sähkökuormia.

Tyypillisesti mittareissa on mahdollisuus ohjelmistojen ja parametrien etäpäivitykseen. Virheellinen mittareiden päivitys voi tulla hyvin kalliiksi. Mittareiden ohjelmistopäivitysten alkuperän ja oikean toiminnan tarkistuksista ja testauksista on huolehdittava hyvin päivitysprosessin kaikissa eri vaiheissa. Mittareiden varsinainen alatason mittausohjelmisto on kalibroinnin alaista eikä sitä tai mittausdataa saa muuttaa; niinpä ne on mittareissa pyritty suojaamaan sekä tahallisilta että tahattomilta muutoksilta.

Mittarien luona paikan päällä käynti on kallista. Siihen johtavia syitä olisi monen mittarin oikean toiminnan tai tiedonsiirron lakkaaminen niin, että tilaa ei voida etäpäivityksellä palauttaa. Tällaisiin tilanteisiin johtavilta uhkilta on siis syytä suojautua hyvin.

Tietoturvan kannalta kriittisimpinä Suomen AMM-järjestelmien osina havaittiin kulutustietoja tarjoavat www-palvelimet, sähkömittareiden paikalliset rajapinnat, etäpäivitys ja etäohjaustoiminnot. Suuria vahinkoja voi aiheutua, jos ohjelmistopäivityksien oikeellisuuden varmistaminen tai sisäpiirin henkilöstön luotettavuus pettää.

Muita projektissa havaittuja merkittäviä uhkia ja haavoittuvuuksia:

- Käytännössä kaikkien, etenkin langattomien, tiedonsiirtomenetelmien paikallinen häirintä ja estäminen ovat mahdollisia hyvin vähäisellä teknisellä osaamisella. Paikallisesta häirinnästä hyökkääjän saama hyöty on sen sijaan kyseenalainen, ellei tarkoituksena ole ainoastaan aiheuttaa ongelmia.
- AMM-järjestelmän kautta voi tahallisille ja tahattomille hyökkäyksille avautua pääsy muihin sitä kriittisempiin tieto- ja automaatiojärjestelmiin, jos tietoturvavyöhykkeisiin jako on toteutettu puutteellisesti.
- Eri osapuolten välisissä tietoturvavaatimusten määrittelyissä voi olla puutteita.
- Lokien kerääminen, hyödyntäminen ja seuranta voi olla puutteellista.
- Tietojen elinkaaren mittainen hallinta ja tuhoaminen säilytystarpeen loputtua. Esimerkiksi siirtoketjun eri vaiheiden redundanttia tuntitietojen tallennusta käytetään varmistusmenettelynä, eikä muidenkaan AMM-järjestelmään kertyvien tietojen tuhoamiseen ole tarvinnut ottaa kantaa nyt järjestelmän käytön alkuvaiheessa. Asianmukaiset tuhoamisproseduurit on kuitenkin määriteltävä jotta epäilystäkään tietosuojan loukkaantumisesta ei pääsisi syntymään. Tietosuoja rikkoutuu jos vanhojakin tietoja joutuu julkisesti saataville.
- Henkilöstön tietoturvakouluttamisen määrä vaihtelee merkittävästi ja sen myötä mahdollisesti tietoturvatietoisuus.

Kansallisella tasolla ohjeistukset ja määräykset siitä miten tietoturva AMM:n ja sen tuottaman kulutusdatan suhteen käytännössä toteutetaan puuttuvat. Tietoturvaa vaaditaan sähkömarkkinalainsäädännössä ja henkilötietolaissa teknisesti tarkemmin määrittelemättä.
Kuten muitakin tietoteknisiä järjestelmiä ja ohjelmia suunnitellessa, myös AMM-ympäristöissä tulee huomioida, että havaittuja mahdollisia tietoturvaongelmia on paljon helpompi korjata määrittelyn ja suunnittelun aikana kuin jälkikäteen. Ongelmien jättäminen korjaamatta tulee hyvin todennäköisesti ajan oloon kaikkein kalleimmaksi. AMM-järjestelmien tietoturvamenetelmien ja uhkatilanteen kehittymisen jatkuvaa tai säännöllisesti toistuvaa seurantaa on kansallisella tasolla tarvetta parantaa.

Projektiin osallistuneiden yritysten kesken käytyjen työpajojen ja projektissa läpikäydyn materiaalin perusteella vakavia aukkoja tai ilmiselviä virheitä Suomessa käytettävien AMM-

järjestelmien tietoturvasta ja toteutuksista ei löytynyt. Projektin puitteissa ei kuitenkaan ollut mahdollista eri rajapintojen, tiedonsiirtoprotokollien, ohjelmistopäivitysmenettelyjen ja tietoverkkojen toteutuksien tietoturvatestaus ja systemaattinen tekninen arviointi. Myöskään sopimusten ja vaatimustenhallintamenettelyjen konkreettisia tarkastuksia ei tehty.

Haavoittuvuuksia löytyy kaikista tietoteknisistä järjestelmistä, mutta kun tietoturvasta on huolehdittu usealla tasolla haavoittuvuuksien aiheuttamat riskit lievenevät. Hyökkääjän motivaatio yrittää järjestelmän hyväksikäyttöä pienenee silloin kun kiinnijäämisen todennäköisyys on suuri. Projektiryhmän tietoon ei ole tullut tietoa Suomen tasolla tapahtuneista etäluentaan liittyvistä onnistuneista tietoturvahyökkäyksistä, tai edes niiden yrityksistä. Sähkömittareiden etäluennan laajamittainen käyttö on Suomessa ja maailmalla vasta alussa, joten on todennäköistä että hakkereiden kiinnostus uusia sähkömittareita ja niihin liittyviä järjestelmiä kohtaan lisääntyy. Internet on kustannustehokas ratkaisu yritysten kommunikointitarpeisiin, ja suojattuina samoja teknologioita käytetään myös teollisuuden järjestelmissä, mukaan lukien älykäs mittarointi. Internetin välityksellä myös tiedot mahdollisista tietoturvahaavoittuvuuksista ja ohjeet niiden hyväksikäytöstä leviävät hyvinkin nopeasti – ja jokainen etäohjattava mittari on AMM-järjestelmän tietoturvan päässä globaalista saatavuudesta.

## Lähdeviitteet

Brown, P.A. Power Line Communications – Past Present and Future, 3rd International Symposium on Power-Line Communications and It's Applications, Lancaster UK 30.5-1.4.1999. http://www.isplc.org/docsearch/Proceedings/1999/pdf/0566_001.pdf

Cuijpers, C. and Koops, B-J. 2013: Smart Metering and Privacy in Europe: Lessons from the Dutch Case. 15 Feb 2013. In: S. Gutwirth et al. (eds), European Data Protection: Coming of Age, Dordrecht: Springer, pp. 269-293 (2012). Saatavilla: SSRN: http://ssrn.com/abstract=2218553

DECC 2012: Smart metering security risk assessments. 31 May 2012. Department of Energy & Climate Change (DECC), London UK, 31 May 2012. https://www.gov.uk/government/consultations/smart-metering-security-risk-assessments

DECC 2013a: Smart Metering Implementation Programme, Government Response to the Consultation on second version of the Smart Metering Equipment Technical Specifications, Part 2. Department of Energy & Climate Change (DECC), London UK, 1 July 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/209840/SMIP_E2E_SMETS2_govt_consultation_response_part_2_final.pdf

DECC 2013b: Notification of Core Communication Services Schedule for inclusion in version 1 of the Smart Energy Code and invitation to submit Elective Communication Service Requests. Department of Energy & Climate Change (DECC), London UK, 8 April 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/182437/2013_03_26_SMP_REG_Notification_of_Core_Communication_Schedules_and_Invi_3_P_.pdf

DSMR 2011: Main Document, Dutch Smart Meter Requirements V4.0, Netbeheer Nederland, 22nd April 2011, 147s. ,

DSMR 2012: Release Notes DSMR V4.0.5 Dutch Smart Meter Requirements, Netbeheer Nederland, 15th May 2012, 18s.

Energiamarkkinavirasto. 2011. Sähköverkkotoiminnan tunnusluvut. Taulukko. http://www.energiamarkkinavirasto.fi/files/Sahkoverkon_tt_luvut_2011.xlsx

Energiatehokkuusdirektiivi 2012/27/EU
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0001:0056:EN:PDF

European Conference on Smart Grid Standardization achievements, European Commission, 28 January 2013.
http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

FISC 2012: fisc.fi. Finnish Information Security Cluster.

Fries, S.; Falk, R.; and Sutor, A.2013: Smart Grid Information Exchange – Securing the Smart Grid from the Ground. In: J. Cuellar (Ed.): SmartGridSec 2012, LNCS 7823, pp. 26–44, 2013. © Springer-Verlag Berlin Heidelberg 2013. http://link.springer.com/content/pdf/10.1007%2F978-3-642-38030-3.pdf

Harjula, M. 2008. Mittausvirtoihin liittyvä standardointi –ja koodiehdotus uusilla energiamarkkinoilla. Diplomityö. 81s. Lappeenrannan teknillinen yliopisto. http://www.doria.fi/bitstream/handle/10024/42808/nbnfi-fe200810272033.pdf?sequence=3

Henkilötietolaki 22.4.1999/523
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523
Inguardians. 2009. Advanced Metering Infrastructure Attack Methodology.
http://inguardians.com/pubs/AMI_Attack_Methodology.pdf

Koto, Antti. 2010.Tietojärjestelmien väliset rajapinnat sähkönjakeluverkon käyttötoiminnassa. Diplomityö 102s. Tampereen teknillinen yliopisto.
http://webhotel2.tut.fi/units/set/opetus/pdf%20julkiset%20dtyot/Koto_Antti_julk.pdf

Lehtonen, Jarkko; Nurminen, Teemu. 2013: Tuntimittaustiedon avoin palvelualusta. Loppuraportti. Sähkötutkimuspooli, Jatiko Oy, 27.3.2013.
http://energia.fi/sites/default/files/tuntimittaustiedon_avoin_palvelualusta.pdf

Löf, Atte. 2012. Testing of Low Voltage Network Automation. Pro-Gradu tutkielma. 59s.Tampereen teknillinen yliopisto.
http://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/21390/Lof.pdf?sequence=1

Löf, Niklas. 2009. Pienjänniteverkon automaatioratkaisuiden kehitysnäkymät. Diplomityö. 113s. Tampereen teknillinen yliopisto.
http://webhotel2.tut.fi/units/set/opetus/pdf%20julkiset%20dtyot/Lof_Niklas_julk.pdf

Mandaatti 441. Euroopan Komissio. Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability.
http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf

Mandaatti 468. Euroopan Komissio. Standardisation Mandate to CEN/CENELEC and ETSI concerning the charging of electric vehicles.
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2010_06_04_mandate_m468_en.pdf

Mandaatti M/490. Euroopan Komissio. Smart Grid Mandate. Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment.
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

Mittauslaitedirektiivi 2004/22/EY
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:135:0001:0080:EN:PDF

Newman, Lily Hay, Can You Trust NIST?, IEEE Spectrum, 9.10.2013.
http://spectrum.ieee.org/telecom/security/can-you-trust-nist.

NIST IR 7628. Smart Grid Guidelines for Smart Grid Cyber Security.2010.
http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

NIST IR 7628 Vol. 1: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. 2010.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

NIST IR 7628 Vol. 2: Privacy and the Smart Grid. 2010.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

NIST IR 7628 Vol. 3: Supportive Analyses and References. 2010.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

NIST SP 800-21. Guideline for Implementing Cryptography In the Federal Government
http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

Notification of Core Communication Services Schedule. Department of Energy & Climate Change. UK.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/182437/2013_03_26_SMP_REG_Notification_of_Core_Communication_Schedules_and_Invi____3___P_.pdf

von Oheimb, D. 2012: IT Security architecture approaches for Smart Metering and Smart Grid. In: Cuellar, J. (ed.) SmartGridSec 2012. LNCS, vol. 7823, pp. 1–25. Springer, Heidelberg (2013).

Pakonen, Pertti. 2012. Energiamittareiden sähköverkkotiedonsiirron häiriöiden hallinta. Seminaariesitys. Sähkötutkimuspoolin tutkimusseminaari.
http://energia.fi/sites/default/files/dokumentit/energiateollisuus/Tutkimus/ST-pooli/esitys_pakonen.pdf

Pikkarainen, M. Vehmasvaara, S. Siddiqui, B.A. Pakonen, P. Verho, P. 2012. Interference of touch dimmer lamps due to PLC and other high frequency signals. Electric Power Quality and Supply Reliability Conference. Konferenssijulkaisu.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6256241&queryText%3Dpower+line+communications+tampere

Rokka, Antti. 2011. Sähköverkkotiedonsiirron häiriöt. Insinöörityö. 52s. Metropolia Ammattikorkeakoulu.
https://publications.theseus.fi/bitstream/handle/10024/26098/Antti%20Rokka%20insinoorityo_sahkoverkkotiedonsiirron%20hairiot.pdf

Väisänen, Teemu & Kreus, Juha. Informaatioteknologia. Turvallisuus.Tietoturvallisuuden hallintajärjestelmät.ISO/IEC 27000 standardiperhe Kalvosarja oppilaitoksille Suomen Standardisoimisliitto SFS ry 2012.
http://www.cs.tut.fi/kurssit/TLT-3100/doc/iso-27000.pdf

SFS-ISO/IEC 27005 -Standardi. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. 126s.

Sintef. 2012. Security Threats in Demo Steinkjer. Projektiraportti.
https://demosteinkjer.no/attachment.ap?id=2

Smart Metering Implementation Programme, Government Response to the Consultation on second version of the Smart Metering Equipment Technical Specifications, Part 2. Departement of Energy & Climate Change, London UK, 1 July 2013.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/209840/SMIP_E2E_SMETS2_govt_consultation_response_part_2_final.pdf

Sähköisen viestinnän tietosuojalaki.
http://www.finlex.fi/fi/laki/alkup/2004/20040516

S. Fries, R. Falk, and A. Sutor, Smart Grid Information Exchange – Securing the Smart Grid from the Ground. In: J. Cuellar (Ed.): SmartGridSec 2012, LNCS 7823, pp. 26–44, 2013. © Springer-Verlag Berlin Heidelberg 2013.
http://link.springer.com/content/pdf/10.1007%2F978-3-642-38030-3.pdf

Valtioneuvoston asetus sähköntoimitusten selvityksestä ja mittauksesta. 2009.
http://www.finlex.fi/fi/laki/alkup/2009/20090066
WELMEC 2011: Software Guide (Measuring Instruments Directive 2004/22/EC). WELMEC 7.2. issue 5. Saatavissa
http://www.welmecwg7.ptb.de/Guides/WELMEC_Guide_7_2_Issue5_2011_May.pdf

Sähkömittarit:

IskraEmeco MT372
http://www.iskraemeco.si/emecoweb/eng/products/bdf/MT372_ang.pdf

Kamstrup:162L
http://kamstrup.fi/media/16358/file.pdf

Kamstrup 382L
http://kamstrup.fi/media/15879/file.pdf

Kamstrup 351
http://kamstrup.com/media/14206/file.pdf

Landis + Gyr E120GiME
http://style.landisgyr.com/apps/products/data/pdf2/D000031365_en_a_E120GiME_Fact_Sheet.pdf

Landis + Gyr E120Lt
http://style.landisgyr.com/apps/products/data/pdf1/E120Lt_EN_TechData_v1101.pdf

Landis + Gyr E120M
http://landis.moveodev.com/product/landisgyr-e120m-integrated-meter/

Landis + Gyr E450
http://www.landisgyr.fi/webfoo/wp-content/uploads/2012/09/D000028191_E450_f_en.pdf

Landis + Gyr E120Lime
http://style.landisgyr.com/apps/products/data/pdf1/E120LiME_Fact_Sheet_EN_101.pdf

Telvent Echelon MTR 3000-sarja
http://www.echelon.com/products/smart-meters/docs/MTR_3000_83332-xIxxx.pdf