Aalto-yliopisto
Sähkötekniikan korkeakoulu

Tuomas Tammelin

Langattomien yhteyksien hyödyntäminen huoltovarmuuskriittisessä energiantuotannon järjestelmissä

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten tietoliikennetekniikan tutkinto-ohjelmassa.

Espoossa, 12.12.2014

Työn valvoja: Professori Riku Jäntti
Työn ohjaaja: Diplomi-insinööri Pekka Salimäki

Tekijä Tuomas Tammelin

Työn nimi Langattomien yhteyksien hyödyntäminen huoltovarmuuskriittisessä energiantuotannon järjestelmissä

Koulutusohjelma Tietoliikennetekniikka

Valvoja Riku Jäntti **Professuurikoodi** S-38

Laitos Sähkötekniikan korkeakoulu

Työn ohjaaja(t)/Työn tarkastaja(t) Pekka Salimäki

Päivämäärä 15.9.2014 **Sivumäärä** 114+37 **Kieli** Suomi

Tiivistelmä

Langaton tiedonsiirtoteknologia on eri muodoissaan olennainen osa nykyaikaista yhteiskuntaa. Langattomuuden tarjoamat edut ovat tuoneet nämä teknologiat myös osaksi teollisuusympäristöä esimerkiksi erilaisten langattomien anturiverkkojen (WSN, wireless sensor network) muodossa. Anturiverkkojen lisäksi langatonta tiedonsiirtoa voi olla mahdollista hyödyntää tarjoamaan helppo pääsy kentältä teollisuuslaitosta ohjaaviin järjestelmiin käyttäen WLAN (Wireless Local Area Network)-tekniikkaa.

Tässä työssä on tavoitteena selvittää kuinka langatonta tiedonsiirtoa voitaisiin hyödyntää huoltovarmuuskriittisessä voimalaitosympäristössä ja minkälaisia vaatimuksia kyseinen ympäristö asettaa tekniikalle. Oleellisimmat vaatimukset liittyvät tiedonsiirron tekniseen toimivuuteen, langattomien järjestelmien tietoturvallisuuteen sekä käytettävyyteen. Työssä perehdytään ensin hieman IEEE 802.11- ja IEEE 802.15.4-standardeihin pohjautuvien verkkojen toimintaan ja selvitetään mitä mahdollisia etuja ja ongelmia langattomat verkot voivat tuoda voimalaitoskäyttöön. Lisäksi esitellään muutamia mahdollisia sovelluksia langattomille verkoille perustuen edellä mainittuihin standardeihin.

Työn puitteissa tehdään myös mittauksia voimalaitosympäristössä käyttäen WLAN-laitteita. Näillä mittauksilla on tarkoitus selvittää tiedonsiirron toimivuus haastavassa ympäristössä sekä 2,4GHz- että 5GHz-taajuusalueilla. Mittausten perusteella pyritään selvittämään onko langaton tiedonsiirto ylipäätään teknisesti hyödynnettävissä voimalaitoksella.

Avainsanat: WLAN, WSN, IEEE 802.11, IEEE 802.15.4, automaatio, langattomat tiedonsiirtoverkot, ISM-taajuusalueet

Aalto University
School of Electrical
Engineering

Aalto-university, PL 11000, 00076 AALTO
www.aalto.fi

Abstract of the Master's Thesis

Author	Tuomas Tammelin
Title	Utilization of wireless networks in energy production systems of critical infrastructure
Degree programme	Communications Engineering
Supervisor	Riku Jäntti
Major Subject Code	S-38
Department	School of Electrical Engineering
Supervisor(s)/Instructor(s)	Pekka Salimäki
Date	15.9.2014
Number of pages	114+37
Language	Finnish

Abstract

Different types of wireless networks are an integral part of life in a modern society. The potential benefits of wireless communication have brought these technologies to the industrial environment for example in the form of wireless sensor networks (WSNs). A WLAN (Wireless Local Area Network)-connection could also be used to provide a wireless connection to industrial control systems from the field.

The goal of this thesis is to identify possible uses for wireless networks in a power plant that is part of the nation's critical infrastructure. The aim is also to identify any special requirements that this environment might pose for the utilization of wireless networks, technical or otherwise. The most important requirements are associated with the technical reliability of wireless data transfer, security and usability. This thesis takes a look at the IEEE 802.11 and IEEE 802.15.4 standards and the possible benefits and problems associated with utilization of wireless networks. Also some possible applications for wireless networks based on these standards are presented.

Measurements in the field are also conducted using WLAN-devices on the 2,4GHz and 5GHz-bands. The aim of these measurements is test the functioning of wireless data transfer in a challenging environment and to determine overall feasibility of using wireless networks in a power plant environment.

Keywords WLAN, WSN, automation, wireless networks

Alkusanat

Tämä diplomityö tehtiin Helsingin Energian HelenEngineering-yksikön Sähkö- ja automaatioryhmässä. Työn tilaajana toimi Salmisaaren voimalaitoksen HelenVoima liiketoimintayksikkö ja se toteutettiin osittain voimalaitoksella meneillään olevan modernisaatioprojektin yhteydessä. Kiitokset sekä HelenEngineeringille sekä Salmisaaren voimalaitokselle hyvästä työilmapiiristä ja mahdollisuudesta työn tekemiseen.

Haluan kiittää työn valvojaa professori Riku Jänttiä hyvästä opastuksesta työn kirjoituksessa. Erityiskiitokset työni ohjaajalle Pekka Salimäelle, joka on kärsivällisesti auttanut ja kannustanut työni toteutumisessa. Lisäksi haluan kiittää automaatiomekaanikko Esa Liedestä avusta työn käytännönosuuden kanssa sekä Lassi Kalmista ja Eero Söderholmia neuvoista ja hyvistä näkemyksistä työhöni liittyvissä kysymyksissä.

Haluan lisäksi kiittää vanhempiani ja veljeäni Lauria koko opintojeni aikana saamastani tuesta ja kannustuksesta. Suurkiitos monista antoisista opiskeluvuosista kuuluu opiskelukaverilleni Eero Hyytiselle.

Helsingissä 15.9.2014

Tuomas Tammelin

Sisällysluettelo

Lyhenteet ja käsitteet

5G	5th Generation mobile networks, 5. sukupolven matkapuhelinverkot
AES	Advanced Encryption Standard, lohkosalausmenetelmä
ATEX	atmosphères explosibles, räjähdysvaarallisissa tiloissa käytettäviä laitteita koskeva määräys
BSS	Basic Service Set, peruspalveluryhmä
BSSID	Basic Service Set Identification, peruspalveluryhmän tunnus
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, siirtotien varausmenetelmä, jossa törmäykset pyritään välttämään
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, siirtotien varausmenetelmä, jossa törmäykset havaitaan ja sen perusteella tehdään uudelleenlähetys
DCF	Distributed Coordination Function, WLAN:n siirtotielle pääsystä vastaava toiminnallisuus
DSSS	Direct Sequence Spread Spectrum, suorasekventointi
EIRP	Equivalent Isotropically Radiated Power, lähettimen teoreettinen tasaisesti joka suuntaan säteilemä lähetysteho
ERP	Equivalent Radiated Power, lähettimen teoreettinen lähetysteho, joka huomioi järjestelmän häviöt ja vahvistukset
ESS	Extended Service Set, laajennettu palvelurhmä
FFD	Full Feature Device, täyden toiminnallisuuden laite
GTS	Guaranteed Time Slot, varattu aikaväli
HART	Highway Addressable Remote Transducer, 4-20 mA viestejä hyödyntävä kenttäväyläprotokolla
HSE	Health, Safety, Environment, terveys, turvallisuus, ympäristö
IBSS	Independent Basic Service Set, itsenäinen peruspalveluryhmä
IDS	Intrusion Detection System, tunkeilijan havaitsemisjärjestelmä
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
IEEE 802.3	IEEE standardi langallisille lähiverkoille
IEEE 802.11	IEEE standardi ISM-taajuusalueella toimiville langattomille tietokoneiden välisille lähiverkoille
IEEE 802.15.4	IEEE standardi lyhyen kantaman langattomille PAN-verkoille
IoT	Internet of Things, esineiden Internet

IP	Ingress Protection, sähkölaitteiden suojausluokittelu
IPS	Intrusion Prevention System, murron estämisjärjestelmä
ISA	The International Society of Automation, automaatiotekniikkaan keskittynyt yhdistys
ISM	Industrial Scientific Medical, teollisuus, tiede, lääketiede
KVJ	Kunnonvalvontajärjestelmä
LAN	Local Area Network, lähiverkko
M2M	Machine-to-machine, koneiden välinen tiedonsiirto
MAC	Media Access Control, siirtotielle pääsyn hallinta
OSI	Open Systems Interconnection, tiedonsiirtoprotokollien kerrokset kuvaava malli
PAN	Personal Area Network, likiverkko
PoE	Power-over-Ethernet, jännitesyöttö käyttäen Ethernet-kaapelia
RADIUS	Remote Authentication Dial In User Service, autentikoinnin, valtuutuksen ja tilastoinnin tarjoava verkkoprotokolla
RFD	Reduced Feature Device, rajatun toiminnallisuuden laite
RFID	Radio-Frequency Identification, radiotaajuinen etätunnistus
RSSI	Received Signal Strength Indicator, vastaanotetun signaalin teho
SSID	Service Set Identifier, palveluryhmätunniste
TCP	Transmission Control Protocol, OSI-mallin 4. tasolle sijoittuva yhteydellinen tietoliikenneprotokolla
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla WLAN-yhteyksien salaamiseen ja turvaamiseen
TLJ	Turvallisuuteen Liittyvä Järjestelmä
UDP	User Datagram Protocol, OSI-mallin 4. tasolle sijoittuva yhteydetön tietoliikenneprotokolla
WEP	Wired Equivalent Privacy, 1. sukupolven WLAN tietoturvaprotokolla
WIA-PA	Wireless network for Industrial Automation-Process Automation, langaton tiedonsiirtoprotokolla automaatiojärjestelmiin
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, ensimmäinen versio 2. sukupolven WLAN tietoturvaprokotollasta
WPA2	Wi-Fi Protected Access II, toinen versio 2. sukupolven WLAN tietoturvaprotokollasta
WPAN	Wireless Personal Area Network, langaton likiverkko

WPS	Wi-Fi Protected Setup, WLAN-verkkojen turvaamisen helpottamiseksi kehitetty tietoturva standardi
WSN	Wireless Sensor Network, langaton anturiverkko

1. Johdanto

1.1 Tausta ja motivaatio

Voimalaitokset, kuten muutkin teolliset laitokset, vaativat tänä päivänä toimiakseen erittäin paljon nykyaikaista teknologiaa. Suuri osa tästä keskittyy automaatiojärjestelmiin, joilla ohjataan sekä itse voimalaitosprosessia, että pienempiä osajärjestelmiä. Järjestelmien tiedonsiirto on perinteisesti toteutettu langoitetulla teknologialla. Tämä johtuu pitkälti automaation vikasietoisuus, viive-, varmuus- ja tietoturvavaatimuksista [1][2]. Kiristyvät vaatimukset esimerkiksi päästöjen, energiatehokkuuden sekä asennuskustannusten suhteen aiheuttavat tarpeen selvittää uusien teknologioiden sovelluskelpoisuutta. Nykyisin on mahdollista siirtää myös automaatiojärjestelmän mittaus- ja ohjaustietoa, kuten mitä tahansa muuta digitaalista tietoa, langattomasti. Langaton tiedonsiirto ei lähtökohtaisen epävarmuutensa johdosta kuitenkaan voi vielä korvata kaikkea johdotusta automaatiojärjestelmässä, mutta sille on mahdollista löytää sopivia sovelluskohteita oikeanlaisella toteutuksella. Langattomiin järjestelmiin siirryttäessä tavoitteena onkin yleensä parantaa järjestelmän kustannustehokkuutta pienentämällä asennus ja ylläpitokustannuksia sekä parantaa järjestelmän tuotanto- ja toimintatehokkuutta [2] [3]. Oikein toteutettu langaton järjestelmä, esimerkiksi langaton anturiverkko, osana automaatiojärjestelmää voi tuoda huomattavasti lisää joustavuutta järjestelmän toteutukseen ja käyttöön [3]. Esimerkiksi rinnakkaisen tiedonsiirtoväylän rakentaminen tiedonsiirron varmistamiseksi hankalaan sijaintiin voi olla halvempaa ja helpompaa langattomasti kuin langoitettuna [3] [4].

Automaation ja anturiverkkojen lisäksi mahdollinen langattomien tietoverkkojen hyödyntämiskohde voimalaitosympäristössä on langaton tiedonsiirtoverkko prosessitiloissa. Tämänkaltaisella verkolla voidaan tuoda tarvittavaa tietoa kentällä työskentelevien työntekijöiden käyttöön. Luonnollisesti tiedonsiirto onnistuu myös toiseen suuntaan, eli tietoa voidaan

tuoda kentältä esimerkiksi valvomoon. Esimerkkeinä sovelluksista voidaan mainita langaton dokumentin hallinta, jossa tietoa tuodaan kentälle ja toiseen suuntaan langaton kameravalvonta, jossa kerätään tietoa kentältä. Mahdollisimman joustava järjestelmä vaatii tietysti tukiasemien sijoittelun tarkoin harkittuihin paikkoihin, jotta verkko kattaisi suurimman mahdollisen alueen kustannustehokkaasti. Voimalaitoksen prosessitilat asettavatkin omanlaisensa haasteet langattomille verkoille. Tiloissa on paljon suuritehoisia sähkölaitteita sekä paksuja seiniä ja paljon metallirakenteita. Langattomien laitteiden sijoittelu vaatiikin tarkkaa suunnittelua ja käytännön mittaustyötä optimaalisen ratkaisun löytämiseksi. Olemassa olevat sähkö- ja tietoverkot asettavat myös omat rajoituksensa laitteiden sijoittelulle. Tällaisen järjestelmän todennäköisin toteutustapa siirrettävästä tietomäärästä johtuen, on luultavimmin langaton lähiverkko eli WLAN (Wireless Local Area Network).

Langattomia järjestelmiä toteutettaessa tietoturvaan tulee kiinnittää eri tavalla huomiota kuin perinteisissä langallisissa järjestelmissä. Koska kyseessä on huoltovarmuuskriittinen voimalaitos, jonka johdosta tietoturvan merkitys korostuu entisestään. Tietomurto voimalaitosjärjestelmään voisi olla seuraamuksiltaan erittäin vakava. Tämän johdosta tietoturvaan tullaan kiinnittämään erityistä huomiota myös tätä työtä tehdessä.

Ennen kuin langattomia järjestelmiä voidaan toteuttaa käytännössä, tarvitaan myös riittävä ymmärrys teoriasta sekä toteutuksessa huomioitavista tekijöistä. Tämän työn motivaationa on tehdä tarvittava selvitystyö, ja luoda pohja langattomien järjestelmien tehokkaalle hyödyntämiselle.

Kuten kaiken tekniikan suhteen, on tässäkin yhteydessä hyvä muistaa, että tekniikka yksistään ei saa olla itsetarkoitus. Tekniikan tulee palvella loppukäyttäjiään ja sen tuomat mahdolliset edut on tärkeä selvittää etukäteen.

1.2 Tavoitteet ja rajaus

Työn tavoitteena on selvittää miten langattomat verkot soveltuvat erilaisiin käyttötarkoituksiin voimalaitosympäristössä. Tärkeimmät tarkastelukohteet

ovat langattomien verkkojen hyödyntäminen osana automaatiojärjestelmää ja yleisenä tiedonsiirtoverkkona prosessitiloissa. Tutkimuksen tavoitteena on selvittää yleisesti langattoman teknologian sovelluskohteita teollisuudessa ja energiantuotannossa. Tavoitteena on perehtyä alan tutkimukseen ja luoda yleiskäsitys teknologian tarjoamista mahdollisuuksista ja todennäköisistä haasteista. Kirjallisuustutkimuksen lisäksi tavoitteena on tutkia voimalaitoksen prosessitilojen radioympäristöä. Selvityksen perusteella voidaan antaa ehdotuksia ja ohjeita mahdollisiin tulevaisuuden langattomiin projekteihin. Työn ajankohta osuu yhteen voimalaitoksen automaatiouudistuksen kanssa, joka voi tarjota mahdollisuuden hyödyntää järjestelmätoimittajan tietämystä. Työn tarkastelussa keskitytään pääasiassa ITU-R (International Telecommunications Union-Radiocommunication)-organisaation määritelmän mukaisella ISM-taajuusalueella [5] toimiviin lyhyenkantaman radiolaitteisiin, sillä työn pääfokus on laitoksen sisäisessä tiedonsiirrossa. Lopullinen tavoite työssä on vetää yhteen kirjallisuudesta ja käytännön mittauksissa opitut asiat ja luoda peruskonsepti ja vaatimukset langattomien järjestelmien toteuttamiseen voimalaitosympäristössä. Tavoite on, että konseptiin on kerätty mahdollisimman hyvin kaikki todennäköiset kompastuskivet ja huomioitavat asiat. Konseptin pohjalta on tarkoitus, että langaton järjestelmä voidaan toteuttaa tehokkaasti, turvallisesti ja kaikki huoltovarmuusvaatimukset täyttäen missä tahansa vastaavanlaisessa ympäristössä.

Työ on jäsennelty seuraavasti: kappaleessa 2 perehdytään langattomien verkkojen perusteisiin, keskittyen pääasiassa IEEE 802.11- ja 802.15.4-standardien [6] [7] mukaisiin verkkoihin. Kappaleessa 3 esitellään voimalaitosalue ja selvitetään siihen liittyviä haasteita langattomuuden kannalta. Tämän lisäksi luodaan katsaus tällä hetkellä Salmisaaren voimalaitoksella jo käytössä oleviin automaatio- ja tiedonsiirtojärjestelmiin. Kappaleessa 4 perehdytään hieman tietoturvaan sekä yleisesti, että tarkemmin langattomien verkkojen kannalta. Kappaleessa 5 esitellään erilaisia sovellusmahdollisuuksia langattomuudelle voimalaitosympäristössä, ja selvitetään eri sovellusten tuomat edut ja mahdolliset haasteet.

Kappaleessa 6 esitellään voimalaitoksen prosessitiloissa tehdyt mittaukset ja niiden tulokset ja johtopäätökset. Kappale 7 on työn yhteenveto.

1.3 Langaton tiedonsiirto teollisuusympäristössä

Nykyisin pääasiassa tietoa siirretään voimalaitosautomaatiossa käyttäen erilaisia langoitettuja liityntöjä. Myös kenttäväyliä[8] käytetään joissain sovelluksissa. Antureilta luetaan esimerkiksi binääri-, analogi- ja sarjatietoa. Tiedonsiirtoon käytetyt kaapelit on jo jonkin aikaa voinut korvata myös langattomalla tiedonsiirrolla [9]. Nyt tarkastelun kohteena olevalla voimalaitoksella tiedonsiirto tapahtuu käytännössä täysin langoitettuna. Tämän työn kanssa samaan aikaan osuva automaatiojärjestelmien modernisointi tuo käyttöön myös nykyaikaista kenttäväylätekniikkaa.

Langattoman tiedonsiirtotekniikan kehitys ja yleistyminen on tuonut langattomat sovellukset myös osaksi teollisuuden tiedonsiirtoa [10]. Teollisuusautomaation tarpeisiin on IEEE 802.15.4-standardin [7] pohjalta kehitetty esimerkiksi HART-protokollaan pohjautuva WirelessHART [11], ISA100.11a-protokolla[12] sekä ZigBee PRO-protokolla [13]. Näistä kahteen ensimmäiseen perehdytään hieman myös tässä työssä. Kyseiset protokollat on suunniteltu tarjoamaan luotettavaa, tietoturvallista ja teollisuuden viivevaatimukset täyttävää tiedonsiirtoa 2,4GHz ISM (Industrial, Scientific and Medical)-taajuusalueella. Näiden protokollien tarkoituksena ei siis ole niinkään tarjota äärimmäisen suuria tiedonsiirtonopeuksia, vaan siirtää pienehkö määrä tietoa rajallisella kaistanleveydellä. Protokollat on suunniteltu pääasiassa automaatiojärjestelmien sisäiseen tiedonsiirtoon esimerkiksi mittaustiedon siirtämiseen yhdeltä tai useammalta anturilta järjestelmään. Näiden protokollien tarjoama vasteaika on n. 10–20 ms [10], joka rajoittaa niiden käyttöä tätä lyhyempää vasteaikaa vaativissa sovelluksissa. Voimalaitosympäristössä näin lyhyitä vasteaikoja vaativia kohteita on melko vähän.

Edellä mainitut automaatiojärjestelmiin kehitetyt protokollat ovat vain osa olemassa olevia langattomia tekniikoita. Ne ovat luonnollisesti hyvä lähtökohta teollisuuslaitoksen langattomaan tiedonsiirtoon perehdyttäessä, mutta tässä työssä pyritään löytämään myös hieman laajempia sovelluskohteita langattomille verkoille. Siksi työssä perehdytään myös IEEE 802.11-protkollaperheen [6], tutummin WLAN, toimivuuteen voimalaitosympäristössä. Erityisenä mielenkiinnonkohteena on 5GHz-taajuusalueen toimivuus. WLAN-tekniikkaa voidaan hyödyntää osana automaatiojärjestelmien tiedonsiirtoa, mutta riittävän kattava ja nopea WLAN-verkko voi mahdollistaa langattomien päätelaitteiden hyödyntämisen kentällä esimerkiksi osana kunnossapito- tai huoltotoimenpiteitä.

Nämä edellä mainitut standardiperheet eivät tietenkään ole ainoita mahdollisuuksia langattomien verkkojen hyödyntämiseen teollisuudessa, mutta tässä työssä tarkastelu rajataan näihin kahteen pääfokuksen ollessa WLAN-tekniikassa, jotta työn laajuus pysyisi järkevänä.

2. Langattomat verkot

Tässä kappaleessa perehdytään yleisellä tasolla langattomaan tiedonsiirtoon. Langaton tiedonsiirto on nimensä mukaisesti tiedon siirtämistä kahden sellaisen pisteen välillä, joita ei ole liitetty toisiinsa johtimella. Tiedonsiirrossa hyödynnetään sähkömagneettisia säteilyä radiotaajuusalueella 9kHz – 400GHz [14] [15]. Tässä työssä keskitytään lähinnä 2,4GHz ja 5GHz ISM-radiotaajuuksille [14] [15].

2.1 Lupavapaat ja ISM-radiotaajuudet

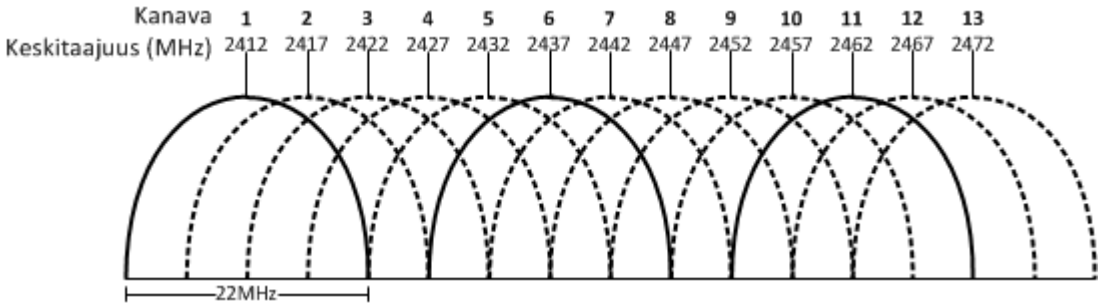
Käytettävissä oleviin radiotaajuuksiin vaikuttavat fysiikan lakien lisäksi olennaisesti kansalliset ja kansainväliset määräykset. Vain tietyt taajuusalueet ovat käytettävissä ilman viranomaisten antamaa lupaa, ja suurin osa alueista onkin varattu kaupalliseen käyttöön. Kaupalliseen käyttöön varatuilla taajuusalueilla toimiminen on luvanvaraista. Suomessa radiotaajuuksien käytöstä ja tarvittavista luvista vastaa Viestintävirasto. Tärkeimmät vapaasti, ilman virallista lupaa, tiedonsiirtoon käytettävät taajuusalueet ovat 2,4GHz sekä 5GHz [14] [15]. Nämä ovat ns. ISM (Industrial, Scientific and Medical) taajuuksia [5], jotka on tarkoitettu nimensä mukaan lupavapaaseen teolliseen, tieteelliseen sekä lääketieteelliseen käyttöön. Lisäksi käytettävissä on 868MHz-taajuusalue, jolla esimerkiksi jotkin ZigBee-laitteet [13] toimivat sekä 433Mhz-taajuusalue, jota käytetään esimerkiksi joissakin RFID-laitteissa [16]. Kaikkiin näihin taajuuksiin pätee kuitenkin rajoituksia lähetystehon sekä 868MHz ja 433MHz alueilla myös toimintasuhteen kannalta [15]. Näiden lisäksi on luonnollisesti olemassa muitakin luvasta vapautettuja taajuusalueita, mutta niille määritellyt käyttötarkoitukset eivät sovellu tähän tarkasteluun. Sopivaa taajuusaluetta valitessa on otettava huomioon myös, minkälaisia laitteita kullekin alueelle on kaupallisesti saatavilla. Laitesaatavuuden johdosta käytettävät taajuudet osuvat luultavimmin juuri ISM- tai lupavapaille taajuusalueille. Toisaalta hyvä laitesaatavuus tarkoittaa myös sitä, että samalla taajuudella on paljon muita samanaikaisia signaalilähteitä, josta voi aiheutua koeksistenssi ongelmia.

IEEE 802.11-, IEEE 802.15.4- ja IEEE 802.15.1-standardit käyttävät Euroopassa 2400MHz – 2483MHz taajuusaluetta. 802.11 käyttää 13 kpl 22MHz leveitä kanavia 5MHz välein, jotka on numeroitu 1 – 13. 802.15.4 käyttää16 kpl 5MHz kanavia, jotka on numeroitu 11 - 26. 802.11 kanavista 1, 6, 11 eivät osu toistensa päälle, ja näitä kolmea käyttäessä 802.15.4:lle vapaaksi jäävät kanavat 15, 20, 25 ja 26, joista kanava 26 ei ole käytössä WirelessHART:ssa, vain ISA100.11a:ssa [17]. Kanava 14 on käytössä vain Japanissa, joten se on jätetty tästä tarkastelusta pois. 2,4GHz taajuusalueella WLAN-verkko kannattaa suunnitella siis siten, että vierekkäiset tukiasemat käyttävät edellä mainittuja kolmea kanavaa häiriöiden minimoimiseksi. 802.11 ja 802.15.4 kanavajaot näkyvät kuvissa 1 ja 2.

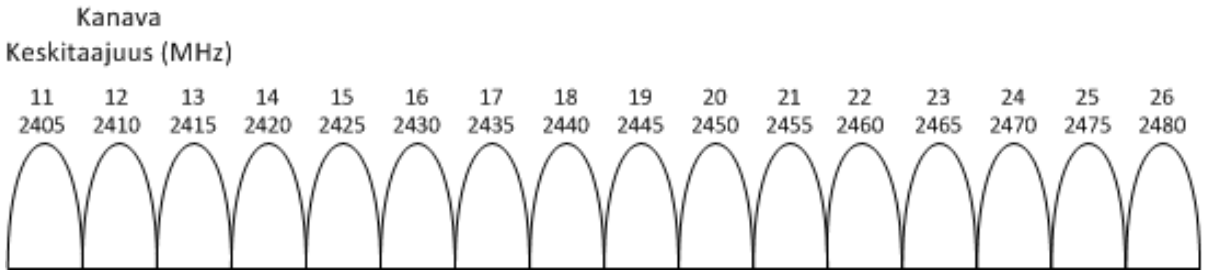
5GHz-taajuusalueella 802.11-standardi käyttää Euroopassa 19 kpl 20-40MHz leveitä kanavia. Käytössä olevista kanavista ensimmäiset ovat numerot 36, 40, 44 ja 48, jotka sijoittuvat taajuusalueelle 5150 – 5250MHz ja käyttö on sallittu vain sisätiloissa. Kanavat 52, 56, 60 ja 64 sijoittuvat taajuusalueelle 5250 – 5350MHz näidenkin käyttö on sallittu vain sisätiloissa, lisäksi kanavia käyttäessä tulee käyttää dynaamista taajuuden valintaa (dynamic frequency selection) ja lähetystehonsäätöä (transmit power control) [15].

Kanavien uudelleenkäyttö tulee suunnitella siten, että samalla kanavalla toimivat tukiasemat eivät ole fyysisesti lähellä toisiaan. Kanavan ollessa vapaa saavutetaan korkein mahdollinen siirtonopeus, kun vierekkäiset tukiasemat eivät joudu vuorottelemaan tiedonsiirrossa [18]. Uudelleenkäyttöön vaikutta myös mahdollisuus kahden kanavan käyttöön 802.11n-standardin mukaisilla laitteilla [19]. Kahden kanava samanaikainen käyttö varaa siis yhteensä 40MHz osan taajuusalueesta. Jos kahdella laitteella on käytössään 40MHz kaistanleveys, kanavia on käytössä yhteensä 4 kpl. Tällöin on mahdotonta valita kanavat siten, että ne eivät olisi päällekkäisiä. Kuvasta 1 nähdään, että ei-päällekkäisiä kanavia on vain 3 kpl. Voimakkaasti suuntaavilla antenneilla voidaan helpottaa taajuuksien

uudelleenkäyttöä rajoittamalla signaalin kuulumista ei-toivottuun suuntaan. Tämän johdosta 802.11n-standardi vaatii koeksistenssi mekanismien käyttöä, kun käytetään 40MHz kanavia 2,4GHz taajuusalueella [18].



Kuva 1, IEEE 802.11 kanavajako 2,4GHz taajuusalueella



Kuva 2, IEEE 802.15.4 kanavajako, 2,4GHz taajuusalueella

On hyvä huomata, että 2,4GHz taajuusalueella koeksistenssi voi nousta ongelmaksi 802.11 ja 802.15.4 laitteiden välillä [20]. Jos laitteita on paljon voi olla suositeltavaa käyttää 802.11 laitteilla 5GHz taajuuksia mahdollisimman paljon, jolloin 2,4GHz-alue jää vapaaksi 802.15.4 laitteille. Tuki 5GHz taajuuksille löytyy vain 802.11n ja uudemmista standardeista, 802.11ac standardi keskittyykin parannuksiin vain 5GHz alueella [18] [21]. Koeksistenssiin perehdytään tarkemmin myöhemmissä kappaleissa.

Viranomaiset ovat asettaneet määräyksiä käytettävien taajuuksien lisäksi myös radioiden lähetystehoille ja toiminta-ajoille[15]. Kaikkien tietyillä taajuuksilla toimivien radiolaitteiden tulee määräysten asettamat vaatimukset.

Vaatimukset:

- Toiminta-aika määrittelee prosentuaalisesti kuinka suuren osan ajasta signaali on aktiivinen [22]. Aika voidaan laskea kaavalla: $D = \frac{T}{P} \times$

$100\,\%$, jossa T on aika, jonka signaali on aktiivinen ja P signaalin jakso.

- Lähetysteho määritellään joko EIRP- tai ERP-muodossa. EIRP (Equivalent isotropically radiated power) on teho, jonka ideaalinen isotrooppinen, eli joka suuntaan tasaisesti säteilevä, antenni lähettäisi tuottaakseen korkeimman tehotiheyden suunnassa, jossa antennivahvistus on voimakkain [23]. ERP (Effective radiated power) on standardoitu teoreettinen lähetysteho, joka huomioi antennijärjestelmän vahvistukset ja häviöt [22].
- Tehotiheys on signaalin teho suhteutettuna kaistanleveyteen.

Tarkemmat määräykset toimimiseen eri luvasta vapautetuilla taajuusalueilla löytyvät liitteestä 1.

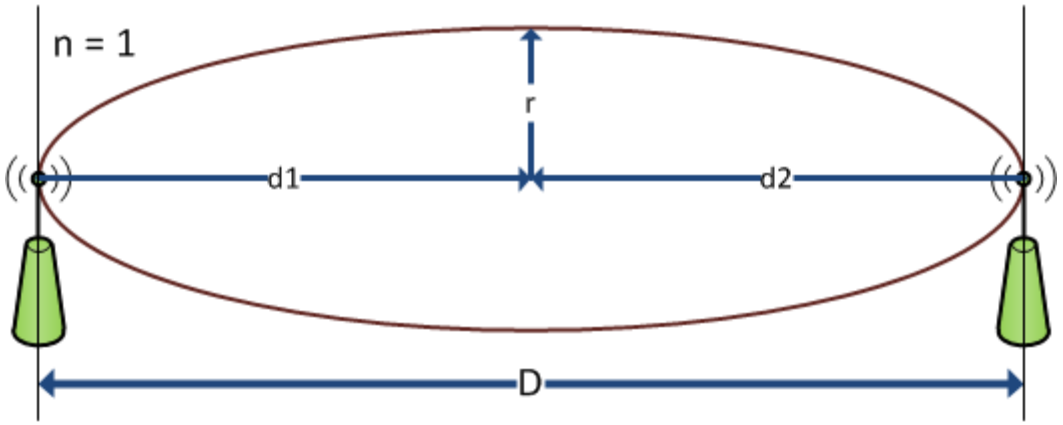
2.2 Radiosignaalin eteneminen

Langattoman tiedonsiirron signaalin etenemiseen pätevät tietyt fysiikan lainalaisuudet. Tässä kappaleessa selvitetään tärkeimmät tekijät sekä suoran näköyhteyden etenemisessä, että monitie-etenemisessä [24]. Monitie-etenemisessä signaali saapuu vastaanottajalle kahta tai useampaa erillistä reittiä pitkin.

2.2.1 Suoran näköyhteyden eteneminen

Tämän työn kannalta ensimmäinen oleellinen tekijä on Friisin-yhtälö [25] radiosignaaleille, joiden välillä on suora näköyhteys ideaalisissa olosuhteissa. Friisin-yhtälön $P_R = \frac{P_T G_T G_R c^2}{(4\pi R f)^2}$, mukaan suuremmilla taajuuksilla vastaanotettu teho pienenee kääntäen verrannollisesti suhteessa etäisyyden (R) ja taajuuden (f) neliöön, yhtälö ottaa huomioon myös lähettävän (G_T) ja vastaanottavan (G_R) antennin vahvistuksen. Oleellista on siis huomioida, miten taajuuden kasvaessa signaalin kantama pienenee. Tällä on merkittävä vaikutus siihen, minkälaiseen käyttöön eri taajuusalueilla toimivat langattomat tiedonsiirtojärjestelmät sopivat. Tutkimuksen kannalta tämä tieto lähinnä

antaa suuntaa taajuusalueen valinnalle käyttöetäisyyden suhteen. Matalat taajuudet toimivat teoriassa korkeita taajuuksia paremmin pitkillä etäisyyksillä. Friisin-yhtälö ei kerro koko totuutta tiedonsiirron tehokkuudesta eri etäisyyksillä tiettyjä taajuuksia käyttäen, vaan on huomioitava myös erilaiset koodaus- ja modulaatiotekniikat sekä monitie-eteneminen (multipath propagation). Lisäksi on huomioitava signaalin ympäristöstä aiheutuvat häviöt (path loss), jotka aiheuttavat signaalin vaimenemista (attenuation). Häviö voidaan laskea yksinkertaisimmillaan kaavalla [26] $L = 10\,n\,\log_{10}(d) + C$, jossa n on ympäristöstä riippuva häviökerroin (path loss exponent), mitä suurempi kerroin sitä suurempi häviö on. Häviökerroin määräytyy ympäristön mukaan, signaalia vaimentavat rakenteet, ihmiset ja muut häiriöt kasvattavat kerrointa. Muuttuja d on asemien välinen etäisyys metreinä ja C on järjestelmän muut vakio häviöt. Jos halutaan tietää häviö vain kahden pisteen välillä vapaassa tilassa, se voidaan laskea kaavalla [26] $L = 20\log_{10}(\frac{4\pi d}{\lambda})$, jossa λ on aallonpituus ja d asemien välinen etäisyys. Jos signaalin vaimeneminen on aikariippuvaista, puhutaan häipymisestä (fading).



Kuva 3, Fresnelin Alue

Edellisten lisäksi huomioitava radiosignaaleiden fysikaalinen tekijä on ns. Fresnelin alue [27], eli radioasemien välillä oleva 3-ulotteinen ellipsoidin mallinen tila, jossa radioaallot etenevät. Aluetta on havainnollistettu kuvassa 3. Mahdollisimman häiriöttömän radioympäristön takaamiseksi tämän alueen tulisi olla vapaa esteistä. Eniten vaikutusta tällä on pitkillä etäisyyksillä, sillä alueen halkaisija kasvaa etäisyyden kasvaessa. Yhtälö alueen halkaisija

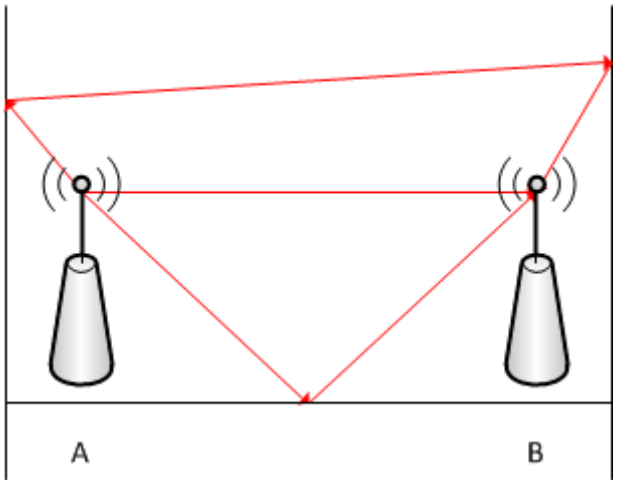
saadaan Fresnelin yhtälöstä: $F_N = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$. Kuvassa nähdään ensimmäinen (n=1) Fresnelin alue. Kun yhtälöön sijoitetaan aallonpituuden tilalle termi, $\lambda = \frac{c}{f}$ havaitaan, että alueen halkaisija (F_N) suurenee taajuuden ja etäisyyden kasvaessa. Fresnelin alue on tärkeää pitää mielessä langattomia tiedonsiirtotietä suunniteltaessa. Varsinkin etäisyyden kasvaessa häiriötön tiedonsiirto vaatii suuren kolmiulotteisen tilan, pelkkä suora näköyhteys ei välttämättä takaa tiedonsiirron toimivuutta.

Pienemmät taajuudet tarjoavat pidemmälle kantavia signaaleita ja parempaa läpäisykykyä, joista varsinkin jälkimmäinen voi olla hyödyllinen ominaisuus voimalaitosympäristössä. Lyhyillä etäisyyksillä käytettäessä pieniä taajuuksia myös Fresnelin alue jää melko pieneksi. Tästä voi olla hyötyä paljon esteitä sisältävässä ympäristössä, jos tiedonsiirtomäärät eivät ole suuria jolloin voidaan käyttää esimerkiksi 868MHz alueella toimivia laitteita. Suuremmilla taajuuksilla tiedonsiirron fyysinen esteettömyys on tärkeämpää ja saattaa vaikeuttaa suunnittelua. Vaatimus suuremmalle tiedonsiirtokapasiteetille voi monissa tapauksissa kuitenkin olla riittävä syy käyttää korkeita taajuuksia. Taajuus määrää myös signaalin aallonpituuden, joka lasketaan kaavalla $\lambda = \frac{c}{f}$. Aallonpituus määrää pienimmän mahdollisen aukon halkaisijan, jonka läpi signaali voi kulkea suoraan häiriintymättä. Tämä on oleellista sillä teollisuusympäristössä kulku- ja huoltotasot on usein rakennettu metallisista ritilätasoista. Jos signaali ei pääse heijastumaan tasojen ohi päästäkseen tason toiselle puolelle, tulee sen päästä tason aukoista lävitse. Sähkömagneettiset aallot voivat myös muuttaa suuntaansa osuessaan johonkin terävään reunaan diffraktiosta johtuen [28]. Suunnanmuutoksen suuruus on riippuvainen radioaallon taajuudesta, pienemmät taajuudet muuttavat suuntaansa enemmän. On hyvä tiedostaa, että teräväreunaisia esineitä saattaa voimalaitosympäristössä olla paljon, tämä vaikeuttaa signaalin etenemisen ennustamista.

Edellä mainitut kaavat ja periaatteet on esitelty tässä lähinnä antamaan peruskäsitys radiosignaalin etenemisestä. Käytännössä etenemisen ei ole näin suoraviivaista. Uudempien 802.11n [19]- ja 802.11ac [29]-standardien tapauksessa käytössä on MIMO (Multiple-Input and Multiple-Output) monitie-eteneminen, jossa aiemmin haitalliset heijastukset voidaan käyttää hyödyksi vahvistamaan vastaanotettua signaalia [18] [21].

2.2.2 Monitie-eteneminen

Edellisessä kappaleessa perehdyttiin hieman radiosignaalin etenemiseen suoraan kahden pisteen välillä ideaalisessa tilanteessa. Käytännössä tilanne ei ole näin yksinkertainen vaan radiosignaali etenee usein vastaanottajalleen useampaa epäsuoraa reittiä pitkin. Tätä kutsutaan monitie-etenemiseksi [30], ilmiötä on havainnollistettu kuvassa, jossa signaali lähtee asemalta A ja päätyy asemalle B. Kuvan 4 esimerkissä on käytössä ympärisäteilevä antenni, eli signaali lähetetään tasaisesti kaikkiin suuntiin. Ympärisäteilevän antennin suuntakuvio ulottuu joka suuntaan ympyränmuotoisena. Radioaaltojen törmätessä johonkin sopivasta materiaalista valmistettuun pintaan, esimerkiksi metalliseinään, ne heijastuvat ja muuttavat suuntaansa. Jos heijastus osuu sopivaan kohtaan, voi heijastunut signaali jatkaa matkaansa kohti vastaanottajaa. Heijastumien kautta vastaanottajalle tulevat signaalit saapuvat eri aikaan kuin suorinta reittiä kulkenut signaali, ne voivat olla eri vaiheessa ja ne ovat vaimentuneet enemmän. Riippuen vastaanotettujen signaalien vaihe- ja amplitudierosta voivat ne joko vääristää, vahvista tai heikentää toisiaan. Tätä ilmiöitä kutsutaan interferenssiksi. Signaalien vahvistaessa toisiaan on kyse



Kuva 4, Radiosignaalin monitie-eteneminen

konstruktiivisesta interferenssistä, kun taas signaalien heikentäessä toisiaan kyse on destruktiivisesta interferenssistä. Tätä vahvistavaa vaikutusta hyödynnetään esimerkiksi 802.11n ja uudemmissa WLAN-standardeissa [18].

Valitsemalla sopivat antennit voidaan vaikuttaa radiosignaalin säteilykuvioon (radiation pattern), eli siihen mihin radioaallot säteilevät suhteessa antenniin. Tässä työssä ei ole tarkoitus perehtyä antenniteoriaan, mutta yleisesti on hyvä tiedostaa antennivalinnan vaikutus signaalien etenemiseen ja vastaanottamiseen. Yksinkertaisin ja yleisesti käytetty antennimalli esimerkiksi WLAN-tukiasemissa on ympärisäteilevä antenni. Ympärisäteilevän antennin säteilykuvio muistuttaa muodoltaan donitsia, jonka keskellä antenni on pystyssä. Signaali suuntautuu siis voimakkaimmin pystyssä olevan antennin sivuille ja antennin molempiin päihin jää alue johon signaali ei kuulu lainkaan. Ympärisäteileviä antenneja käytettäessä on todennäköistä, että signaali pääsee heijastumaan jolloin tapahtuu myös monitie-etenemistä. Suunta-antenni nimensä mukaisesti suuntaa radiosignaalin johonkin tiettyyn suuntaan siten, johon signaali kuuluu voimakkaimmin. Tällöin voidaan pyrkiä kontrolloimaan signaalin etenemissuuntaa ja siten myös signaalin heijastumista. On kuitenkin hyvä muistaa, että vaikka käytössä olisi voimakkaasti suuntaavia antenneja, vaatii radiosignaali aina jonkin verran vapaata tilaa edetäkseen. Lisäksi on huomioitava, että suuntaavat antennit keskittävät lähetetyn tehon pienemmälle alueelle jolloin antennivahvistus kasvaa eli vaarana on säteilytehon nouseminen yli viranomaisrajojen. Jotta säteilyteho pysyy rajojen sisällä, voi tarpeen olla pienentää lähetystehoa kasvaneen antennivahvistuksen kompensoimiseksi. Vastaanottopäässä tätä ongelmaa ei ole ja suunta-antenneilla voidaan parantaa vastaanotetun signaalin laatua, jos tiedetään signaalin saapumissuunta.

2.3 Langattomat teknologiat

Kuten aiemmin jo mainittiin, tässä työssä keskitytään pääasiassa ISM-taajuusalueella toimiviin IEEE 802.11 [6]- ja IEEE 802.15.4 [7]-standardien

mukaisiin teknologioihin ja ratkaisuihin. Tämä rajaus johtuu pitkälti laitesaatavuudesta ja toteutuksen helppoudesta. Tarkoituksena on hyödyntää jo muissa yhteyksissä toimivaksi todettua teknologiaa sekä selvittää niiden toimivuutta ja soveltuvuutta voimalaitosympäristöön. 802.11-standardi tarjoaa ratkaisut, kun on tarve siirtää suuria tietomääriä, mutta standardi ei sisällä määrittelyjä teollisuuden vaatimusten täyttämiseksi. 802.15.4 standardiperhe soveltuu teolliseen käyttöön, esimerkiksi automaatiojärjestelmien tiedonsiirtoon. Tässä kappaleessa esitellään myös muutamia muita käytössä olevia tekniikoita, jotka soveltuvat voimalaitosympäristöön, mutta pääfokus on kahdessa edellä mainitussa standardiperheessä.

2.4 IEEE 802.11 standardiperhe, WLAN

IEEE 802.11-standardit ovat joukko määritelmiä langattoman lähiverkon (WLAN, wireless local area network) OSI-mallin[31] fyysisen- ja siirtokerrosten (MAC, media access control) implementointiin [6]. Standardin tavoitteena oli tarjota luotettava, nopea ja kustannustehokas langaton verkko. WLAN-termi käsittää myös muita vastaavia langattomia lähiverkkotekniikoita, mutta puhekielessä termi on pitkälti vakiintunut tarkoittamaan IEEE 802.11-pohjaisia verkkoja. Näitä verkkoja ja niitä hyödyntäviä laitteita markkinoidaan WiFi-tavaramerkin alla, jonka käyttö perustuu WiFi Alliancen [32] sertifiointiin. WiFi Alliance on vuonna 1999 perustettu kauppayhdistys, johon kuuluu tällä hetkellä noin 600 jäsenyritystä. Yhdistyksen tehtävänä on varmistaa eri valmistajien IEEE 802.11-pohjaisten laitteiden yhteensopivuus, sekä yleisesti edistää WiFi-sertifioidun tekniikan käyttöä. Kaikki IEEE 802.11-standardiin perustuvat laitteet eivät välttämättä ole WiFi-sertifioituja vaikka ne olisivatkin täysin yhteensopivia standardin ja muiden valmistajien laitteiden kanssa. Valmistajat voivat jättää laitteensa sertifioimatta esimerkiksi kustannussyistä, mutta tällöin laitteissa ei voi käyttää ”WiFi Certified” logoa. Tässä työssä IEEE 802.11-pohjaisista tekniikoista puhuttaessa käytetään termiä WLAN.

Ensimmäinen versio standardista, joka kykeni 1 ja 2Mbit/s nopeuksiin 2,4GHz-taajuusalueella, julkaistiin vuonna 1997 [33]. Standardi on ollut siitä

lähtien jatkuvassa kehityksessä, tavoitteena on ollut tarjota suurempia siirtonopeuksia pysyäkseen mukana käyttäjien vaatimuksissa [34]. Tärkeä osa standardin menestystä on jo alusta lähtien mukana ollut yhteensopivuus muiden IEEE 802-verkkojen kanssa [35], joista esimerkkinä voidaan mainita IEEE 802.3-pohjainen Ethernet lähiverkkoprotokolla. Yleisesti käytössä olevat 802.11-standardin versiot voi tunnistaa standardinumeron lopussa olevasta kirjainyhdistelmästä.

2.4.1 Verkon perusrakenne

WLAN-verkko koostuu kolmesta peruselementistä [36] [30]. Nämä elementit ovat asema (STA, station), tukiasema (AP, access point) ja jakelujärjestelmä (DS, distribution system). Asema on mikä tahansa standardin mukaisesti kommunikoiva laite, esimerkiksi kannettava tietokone, ryhmä asemia muodostaa peruspalveluryhmän (BSS, Basic Service Set). Tukiasema mahdollistaa tiedonsiirron asemien välillä, asemat eivät siis kommunikoi suoraan keskenään vaan kaikki liikenne kulkee tukiaseman välittämänä. Tukiasema ja siihen liittynet asemat muodostavat infrastruktuuri-peruspalveluryhmän (inf-BSS). Jakelujärjestelmä yhdistää nämä toisiinsa sekä ulkoiseen verkkoon. WLAN-verkko voidaan toteuttaa kahdella eri topologialla [30]. Ensimmäinen on itsenäinen peruspalveluryhmä (IBSS, independent basic service set), joka koostuu vain asemista jotka kaikki asemat ovat toistensa kantaman sisällä. Vain asemista koostuva verkko tunnetaan myös nimellä ad-hoc-verkko [34]. Toinen on laajennettu palveluryhmä (ESS, extended service set), joka koostuu tukiasemista, asemista ja jakelujärjestelmästä. Asemat ovat yhteydessä tukiasemiin, jotka on yhdistetty toisiinsa jakelujärjestelmän kautta.

2.4.2 Fyysinen kerros

Standardin fyysinen kerros määrittelee miten ylemmiltä kerroksilta tuleva tieto siirretään asemien välillä käyttäen radioaaltoja. Määritelmään kuuluvat käytettävät taajuudet, taajuusalueen kanavajako sekä määrittely kuinka tieto koodataan kantoaaltoon eli modulaatiotekniikka.

IEEE 802.11-standardiperhe määrittelee WLAN-verkkojen toiminnan sekä 2,4GHz, että 5GHz taajuusalueilla. Taajuusalueiden tarkempi kanavajako sekä ISM-taajuusalueet on esitetty kappaleessa 2.1, työn liitteistä selviää myös viranomaisten taajuusalueille asettamat rajoitukset. Muiden samalla taajuudella toimivien laitteiden ohella juuri viranomaismääräykset ovat langatonta tiedonsiirtoa rajoittavin tekijä. Tärkeimmät modulaatiotekniikat selviävät kappaleesta 2.4.4, joka käsittelee WLAN-standardiversioita.

2.4.3 Siirtokerros

Siirtokerroksella määritellään tavat, joilla siirtotietä käytetään. Tarkoituksena on jaetun siirtotien mahdollisimman tehokas ja tasapuolinen hyödyntäminen, kun siirtotiellä on useita samanaikaisia asemia. Langallisissa 802.x-verkoissa useimmiten käytössä CSMA/CD (Carrier Sense Multiple Access with Collision Detection)-tekniikka [34], jossa törmäys siirtotiellä havaitaan ja lyhyen ajan kuluttua tehdään uudelleenlähetys. Tämä on hyvin soveltuva nopeisiin langallisiin verkkoihin, mutta langattomat verkot ovat hitaampia ja siirtotie ruuhkaisempi. Langattomissa verkoissa on suotavampaa pyrkiä välttämään törmäys, jonka takia käytössä on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)-tekniikka [24], jossa törmäykset pyritään välttämään kokonaan lähettämällä tietoa vain silloin, kun siirtotie on havaittu vapaaksi. Siirtotielle pääsy on toteutettu käyttäen distributed coordination function (DCF) toimintoa [36]. DCF käyttää Binary Exponential Backoff-tekniikkaa määrittämään, mikä asema pääsee käyttämään vapaata siirtotietä. Jokainen siirtotielle haluava asema joutuu odottamaan satunnaisen, ja jokaisella epäonnistuneella yrityksellä kasvavan, ajan lähettämänsä tietokehyksen jälkeen. Asema, jonka odotusaika on pienin pääse ensimmäisenä käyttämään siirtotietä. Tällaisessa tekniikassa ongelmana on siirtotien epäoptimaalinen hyödyntäminen, jos samaan aikaan toimivia asemia on useita. Lisäksi tiedonsiirtokapasiteetti pienenee nopeammin kuin lineaarisesti asemien määrän kasvaessa.

Edellä mainitun lisäksi käytössä voi olla myös RTS/CTS (request to send/clear to send) tekniikkaa, jossa lähettäjä pyytää vastaanottajalta

lähetysluvan RTS-viestillä ja vastaanottaja kuittaa sen CTS-viestillä. Tätä ratkaisua käyttäen vältytään ongelmilta, joita esiintyy kahden samaan tukiasemaan yhteydessä olevan aseman ollessa toistensa kuulumattomissa. Tällaisessa tilanteessa pelkkää radiokanavaa tarkkailemalla kumpikin asema tulkitsisi kanavan olevan vapaa ja asemat voisivat pahimmassa tapauksessa lähettää tietoa tukiasemalle samaan aikaan jolloin tapahtuu yhteentörmäys.

2.4.4 Standardiversiot

Standardin merkittävimmät versiot aikajärjestyksessä ovat:

- **802.11-1997** [33]: Ensimmäinen versio standardista, 2400 – 2483,5MHz-taajuusalueella toimiva versio, jonka tiedonsiirtonopeus käytettävästä tekniikasta riippuen on joko 1 tai 2 Mbit/s [30]. Käytössä on joko taajuushyppely (frequency hopping) - tai suorasekventointi (direct sequence spread spectrum)-tekniikka. Taajuushyppelyssä tieto siirretään käyttäen jatkuvasti vaihtuvaa taajuutta, suorasekventoinnissa signaali levitetään matemaattisesti koko käytössä olevalle taajuusalueella. Alkuperäinen standardi ei ole enää käytössä, uudet laitteet pääasiassa enää tue tätä versiota.
- **802.11a-1999** [37]: Ensimmäinen laajennus standardiin. Määrittelee toiminnan 5GHz-taajuusalueella, käyttäen OFDM-tekniikkaa (monitaajuusmodulointi, Orthogonal frequency-division multiplexing), jossa tietoa siirretään usealla toisiaan häiritsemättömällä taajuuskanavalla samaan aikaan. Mahdollistaa parhaimmillaan 54 Mbit/s tiedonsiirtonopeudet. Tämä versio ei ole yhteensopiva alkuperäisen standardin kanssa.
- **802.11b-1999** [38]: Määrittelee parannuksia alkuperäiseen standardiin 2,4GHz-taajuusalueella. Käytössä on edelleen suorasekventointi, mutta kehittyneempänä versiona. Tällöin saavutetaan parhaimmillaan 11 Mbit/s tiedonsiirtonopeus. Tämä versio saavutti merkittävää suosiota markkinoilla, ja sitä käyttäviä laitteita oli laajasti saatavilla. Standardi on yhteensopiva alkuperäisen standardin kanssa, mutta

tällöin on käytettävä vanhempaa suorasekventointia, jolloin nopeus on alkuperäisen standardin mukainen 1 tai 2 Mbit/s.

- **802.11g-2003** [39]: Koska 802.11a-standardiversio ei ollut yhteensopiva alkuperäisen standardin kanssa, jäi sen rooli markkinoilla varsin pieneksi. 802.11g kehitettiin korjaamaan tätä puutetta. Se on yhteensopiva edellisen 802.11b-version kanssa ja se tuo 802.11a-version OFDM-modulaatiotekniikan 2,4GHz-taajuusalueelle. Tällöin saavutetaan parhaimmillaan 54 Mbit/s tiedonsiirtonopeus käytettäessä 64-QAM (Quadrature Amplitude Modulation)-modulaatiota. QAM-modulaatiossa sekä signaalin amplitudia, että vaihekulmaa moduloidaan samanaikaisesti toisistaan riippumatta. Yhteensopivuuden takaamiseksi 802.11g tukee myös edellisen version modulaatiotekniikoita. Jos käytetään samanaikaisesti molempien versioiden mukaisia laitteita, aiheutuu tästä hidastusta myös nopeammille laitteille. Parhaan suorituskyvyn saavuttamiseksi tulee käyttää vain 802.11g-version laitteita.
- **802.11-2007** [6]: Alkuperäisen 802.11-1997-version päivitys. Tässä versiossa standardi on päivitetty kaikilla siihen asti julkaistuilla lisäosilla, eli edellä mainitut sekä d, e, h, i ja j-versiot. Näistä tähän tarkasteluun kiinnostava on 802.11i-standardi, joka määrittelee tietoturvaan liittyvät tekijät. Tietoturvaan perehdytään omassa kappaleessaan.
- **802.11n-2009** [19]: Merkittävä päivitys standardiin. Standardi koskee sekä 2,4GHz- että 5GHz-taajuusalueita. Käytössä on edelleen samat edellisten versioiden modulaatiotekniikat. Aikaisemmissa versioissa käytettiin yksiantennitekniikka (SISO, Single-Input Single-Output), jossa tietoa siirretään yhdellä antennilla käyttäen yhtä datavirtaa(spatial stream) [18]. 802.11n-versio mahdollistaa moniantennitekniikan (MIMO Multiple-Input Multiple-Output)[18] käytön, jossa tietoa voidaan siirtää parhaimmillaan käyttäen neljää datavirtaa ja neljää antennia. Teoreettisesti tämä nelinkertaistaa tiedonsiirtonopeuden. Toinen parannus on jo edellä mainittu

tiedonsiirron jakaminen useampaan samanaikaiseen datavirtaan, jotka yhdistetään takaisin yhdeksi vastaanottajan päässä. Datavirrat lähetään samalla taajuudella käyttäen eri antenneja. Ajatuksena on siis hyödyntää aiemmin haitalliseksi nähty monitie-eteneminen [18]. MIMO-tekniikan lisäksi standardissa määritellään toinen tiedonsiirtoa nopeuttava laajennus, mahdollisuus käyttää leveämpiä kanavia. Tätä standardia käyttäessä on mahdollista yhdistää kaksi 20MHz kanavaa yhdeksi 40MHz kanavaksi. Edellisten lisäksi standardiin on lisätty määritelmä keilanmuodostuksesta (beamforming), jolla pyritään keskittämään lähetystehoa vastaanottajan suuntaan ja parantamaan signaalin kuuluvuutta [18]. Myös siirtokerrokseen on tehty parannuksia, joiden tarkoituksena on tehostaa kanavan käyttöä vähentämällä turhaa odottelua kanavalle pääsyssä ja tehostaa kanavan käyttöä esimerkiksi kasvattamalla kehyksen kokoa. Kaikkien näiden parannusten seurauksena teoreettinen maksimitiedonsiirtonopeus on 600 Mbit/s käyttäen neljää datavirtaa ja 40MHz kanavaleveyttä.

- **802.11ac-2013** [29]: Kirjoitushetkellä uusin julkaistu versio standardista. Muutokset koskevat vain 5GHz-taajuusaluetta [21]. Ensimmäinen muutos mahdollisuus käyttää joko 80MHz tai 160MHz (kaksi 80MHz kanavaa) kanavia. Tällä on tarkoitus kasvattaa tiedonsiirtokapasiteettia entisestään. Standardi lisää tuen monimutkaisemmalle 256-QAM-modulaatiolle. Standardi yksinkertaistaa keilanmuodostusta, edellisessä 802.11n-standardissa tuettiin useita erilaisia tekniikoita, 802.11ac-standardissa on käytössä vain yksi tekniikka, jonka tavoitteena on varmistaa yhteensopivuus eri valmistajien laitteiden välillä. Datavirtojen määrä on kasvatettu edellisen standardin neljästä kahdeksaan. Tämä määrä on kuitenkin käytössä vain tukiasemilla ja asemat käyttävät korkeintaan neljää datavirtaa. Siirtokerrokseen on myös tehty joitakin muutoksia, joiden tavoitteena on parantaa tukea korkeille tiedonsiirtonopeuksille.

Taulukko 1, IEEE 802.11 standardin versiot

Standardi	Maksiminopeus	Taajuusalue
802.11-1997	1 tai 2 Mbit/s	2,4GHz
802.11a-1999	54 Mbit/s	5GHz
802.11b-1999	11 Mbit/s	2,4GHz
802.11g-2003	54 Mbit/s	2,4GHz
802.11n-2009	600 Mbit/s	2,4GHz, 5GHz
802.11ac-2013	3,5 Gbit/s	5GHz

Edellä olevassa taulukossa on listattu eri standardit ja niiden teoreettiset maksimitiedonsiirtonopeudet ja toimintataajuudet. On hyvä huomata, että maksiminopeuksien saavuttaminen on lähinnä vain teoreettinen mahdollisuus varsinkin n- ja ac-standardien kohdalla. Niiden tapauksessa pitäisi olla käytössä maksimimäärä datavirtoja sekä häiriöttömät ja leveimmät mahdolliset kanavat. Käytännössä laitteet on vaikea suunnitella käyttämään riittävää määrää antenneja ja tosimaailmassa voi olla vaikeaa löytää vapaata ja häiriötöntä taajuuskaistaa.

Edellä mainittujen standardien lisäksi kehitystyötä on tekeillä WLAN-tekniikan standardoimiseksi muilla kuin 2,4GHz ja 5GHz taajuusalueilla. 802.11ad-standardi [40] määrittelee WLAN-verkkojen toiminnan 60GHz-taajuusalueella. Vasta kehitysvaiheessa oleva 802.11ah-standardi [41] pyrkii määrittelemään toiminnan perinteisesti TV-lähetyksille varatulla 54-790MHz-taajuusalueella käyttäen TV-kanavilta vapaaksi jääviä taajuuksia siten, että häiriöt muille tekniikoille olisivat mahdollisimman vähäiset. Vielä työn alla oleva 802.11ah-standardin tavoitteena on mahdollistaa WLAN-tiedonsiirto käyttäen alle 1 GHz taajuuksia [42]. Standardia kehittää IEEE:n Task Group ah (TGah)-työryhmä [43]. Standardin tavoitteena on hyödyntää matalampien taajuuksien parempaa kuuluvuutta ja siten parantaa WLAN-tekniikan käytettävyyttä esimerkiksi automaatiojärjestelmissä ja laitteiden välisessä (machine-to-machine, M2M) tiedonsiirrossa. Standardin fyysinen kerros perustuu

muokattuun 802.11ac-standardiin. Koska käytössä on uusi taajuusalue, ei standardin tarvitse olla taaksepäin yhteensopiva vanhempien versioiden kanssa. Tätä hyödyntäen siirtokerros on voitu suunnitella siten, että kehysten otsikkotiedot ovat mahdollisimmat lyhyet. Koska sovelluskohteisiin luetaan myös anturiverkot, on protokollasuunnittelussa keskitytty sekä virransäästöominaisuuksiin, että tukeen laajoille verkoille [42]. Standardin valmistuttua se voisikin tarjota sovellusmahdollisuuksia sekä voimalaitoksella, että koko konsernin tasolla.

IEEE 802.11 standardiperheen tarjoamat mahdollisuudet ovat pääasiassa sovelluksissa, joissa tarpeena on siirtää suuria tietomääriä nopeasti. Tälläkin tekniikalla on toki mahdollista toteuttaa toimintavarmuutta vaativaa tiedonsiirtoa, mutta standardin alkuperäinen ajatus on kuitenkin tarjota langaton korvaaja perinteiselle lähiverkkotekniikalle. Toisin kuin esimerkiksi anturiverkkojen tapauksessa virransaanti tukiasemille ei pitäisi olla ongelmallista, sillä laitteet asennetaan useimmiten kiinteästi. Kiinteässä asennuksessa voidaan hyödyntää IEEE 802.3af [44] ja 802.3at [45]-standardien mukaista Power over Ethernet-tekniikkaa, jossa virta tuodaan laitteelle datakaapelilla.

2.5 Anturiverkot ja IEEE802.15.4 standardiperhe

Teollisuuden tuotanto- ja prosessitekniikka on jo pitkään luottanut automaatiojärjestelmiin. Nämä järjestelmät ohjaavat tuotantolaitoksen toimintaa prosessista keräämänsä tiedon ja ohjelmointinsa perusteella. Perinteisesti mittaus- ja ohjaustiedot on siirretty käyttäen langoitettua tekniikkaa. Tänä päivänä tekniikan kehitys on mahdollistanut tämän tiedon kuljettamisen myös langattomasti [9] [46] [47] [48] [49] [50]. Tässä kappaleessa perehdytään tähän tarkoitukseen kehitettyyn anturiverkkotekniikkaan ja sen pohjana oleviin standardeihin.

2.5.1 Langattomat anturiverkot

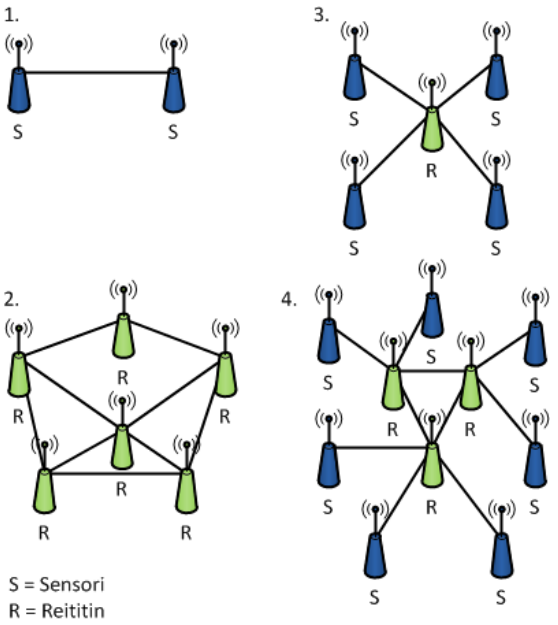
Anturiverkon perusajatus on, että anturisolmut siirtävät mittaustietoa keskittimelle, joka siirtää tiedon eteenpäin sinne missä sitä tarvitaan esimerkiksi prosessiautomaatiojärjestelmä. Anturiverkon solmujen tehtävä on kerätä ja siirtää mittaustietoa, ja ne voidaan jaotella kahteen ryhmään niiden toiminnallisuuden mukaan. Täyden toiminnallisuuden laitteet (full-function device, FFD) kykenevät toimimaan tavallisena anturisolmuna tai verkon koordinaattorina, jolloin ne kykenevät reitittämään muiden solmujen lähettämiä viestejä. Rajallisen toiminnallisuuden laitteet (reduced-function device, RFD) ovat yksinkertaisempia ja ne eivät pysty reitittämään muiden solmujen lähettämiä viestejä, vain lähettämään keräämäänsä tietoa eteenpäin.

Riippumatta käytetystä standardista anturiverkon solmut noudattavat tiettyä perusrakennetta [3] [46]:

- *Anturi:* muodostaa mitattavasta ilmiöistä sähköisen signaalin, signaalille tehdään tarvittaessa analogi-digitaalimuunnos
- *Prosessori:* käsittelee anturilta saamansa signaalin, tiedon prosessoinnilla voidaan vähentää verkossa siirrettävän tiedon määrää ja siten energiankulutusta
- *Kommunikaatio:* vastaa tiedonsiirrosta langattomasti muille anturisolmuille, kommunikaatiojärjestelmä koodaa tiedon radiosignaaliin käyttäen sovittua modulaatiota. Kommunikaatiojärjestelmän energiatehokkuutta voidaan parantaa suunnittelemalla tiedonsiirtoprotokolla, joka pystyy koordinoimaan tiedonsiirtoa koko verkon laajuisesti.
- *Energianhallinta:* vastaa anturin energiansaannista, tähän kuuluu sekä energianlähde, että mahdollinen energian välivarasto. Järjestelmä huolehtii energialähteen toiminnasta sekä energian siirtämisestä muille järjestelmille. Energianlähteenä voi olla kiinteä yhteys sähköverkkoon, akku tai jokin energiankerääjä kuten aurinkopaneeli.

Tämän kokonaisuuden toimintaa kontrolloi käyttöjärjestelmä. Anturiverkkoihin liittyy usein tarve anturisolmujen energiaomavaraisuudesta, jonka vuoksi energiatehokkuus ohjaa kaikkien osajärjestelmien suunnittelua. Anturisolmun energiansaanti asettaa reunaehdot suunnittelulle, saatavilla olevan energian määrä rajoittaa solmuun toteutettavaa toiminnallisuutta. Anturiverkkojen toimintaan kuuluu olennaisesti kyky muodostaa verkko ilman erillistä asennusta eli verkot ovat itseorganisoituvia (self-organizing). Tähän liittyen verkon tulee kyetä korjaaman itsensä yksittäisen solmun hajotessa täysin itsenäisesti. Energiantehokkuuden parantamiseksi solmut voivat myös sammuttaa itsensä väliaikaisesti joko kokonaan tai joidenkin järjestelmien osalta. Periaatteessa koko verkko voidaan synkronoida siirtämään tietoa vain ennalta sovituilla ajan hetkillä. Lisäksi reitityspäätöksissä voidaan ottaa huomioon tiedonsiirron etäisyys, lyhyemmillä etäisyyksillä tarvitaan pienempi lähetysteho joten useamman lyhyen linkin hyödyntäminen voi olla energiatehokkaampaa kuin yhden pitkän linkin.

Energiansaanti ohjaa pitkälle anturiverkon solmujen suunnittelua [3]. Sensoriverkon solmujen energiaomavaraisuus voidaan toteuttaa yleisesti seuraavilla tavoilla: anturin energiankerääjä, langaton teholähetin tai riittävän pitkäkestoinen paristo tai akku. Kaikki edelliset vaihtoehdot tarjoavat rajallisen energiansaannin joten langaton anturi tulee myös suunnitella energiatehokkaaksi. Yleensä energiakerääjän lisäksi tarvitaan energiavarasto (esim. akku tai superkondensaattori) anturin jatkuvan energiatarpeen täyttämiseksi tarpeen vaihdellessa. Energianlähteen ja energiavaraston lisäksi tarvitaan jokin ratkaisu energianhallintaan. Dynaaminen energian hallinta mahdollistaa anturisolmujen radiolaitteiden sammuttamisen sekä laskentayksiköiden kellotaajuuden muuttamisen laskentakuorman mukaan. Anturisolmussa tapahtuvalla laskennalla voidaan vähentää lähetettävän tiedon määrää, jolloin laskentaan käytetty energia voi olla suhteessa pienempi kuin suuren tietomäärän siirtoon tarvittava energia. Anturiverkossa voidaan käyttää akkukäyttöisiä laitteita, joiden akkukesto on vuosia. Pitkää akkukestoa voidaan hyödyntää ajoittamalla akkujen vaihto samaan muiden vuosittaisten huoltotoimenpiteiden kanssa.



Kuva 5, Anturiverkon topologiat

Anturiverkon yleisimmät topologiat [24] on esitetty kuvassa 5.

1. **point-to-point,** suora yhteys kahden laitteen välillä
2. **mesh-verkko,** jossa jokainen verkon solmu osallistuu verkonlaajuiseen tiedonsiirtoon
3. **tähti-verkko,** jossa yksi solmu toimii reitittimenä muille verkon solmuille välittäen niiden lähettämiä paketteja
4. **mesh- ja tähtiverkon hybridi,** jossa eri tähti-verkkojen reitittävät solmut muodostavat välilleen mesh-verkon

Sensori-laitteella (kuvassa merkintä S) ei ole reititysominaisuuksia, eli laite ainoa rooli on lähettää ja vastaanottaa tietoa. Reititin-laite (kuvassa merkintä R) välittää muilta verkon solmuilta saapuva tietoa reititysprotokollan määrittelemällä tavalla. Reititin voi toimia samalla myös sensorina ja sen laitteisto voikin olla täysin sama kuin sensori-laitteella. Laitteet, jotka muodostavat anturiverkon voivat olla kaikki fyysisesti samanlaisia, ja reitittimet erotetaan sensoreista vain ohjelmointinsa perusteella. Reitittävät solmut valitaan siten, että tiedonkulku on taattu myös vikatilanteessa. Vikasietoisuus saavutetaan luomalla tiedolle loogisesti ja fyysisesti erotetut vaihtoehtoiset reitit.

2.5.2 IEEE 802.15.4 standardiperhe

Langattomien anturiverkkojen kehityksen pohjana on käytetty IEEE802.15.4-standardiperheen langattomia likiverkkoja [3]. Näiden standardien perustalle on rakennettu WirelessHART-[11], ISA100.11a- [12]. ZigBeePRO- [13] ja

WIA-PA [51] verkkoteknologiat. Näihin standardeihin liittyen kehityksen kohteena on myös ISA100.12-standardi, jonka tarkoituksena parantaa WirelessHART:n ja ISA100.11a:n samanaikaista toimivuutta, sillä molemmat standardit käyttävät samaa 2,4GHz taajuusaluetta [3]. Edellä mainituista protokollista WirelessHART ja ISA100.11a ovat suorimmin suunnattu teollisuuskäyttöön ja siten oleellisimmat tämän työn kannalta. Molempien tiedonsiirto perustuu muokattuun IEEE 802.15.4-standardiin 2,4GHz-taajuusalueella ja yksinkertaistettuun OSI-malliin [17]. Kuten myös langattomien lähiverkkojen (WLAN) tapauksessa myös IEEE 802.15.4-standardiin perustuvat tekniikat ovat vain yksi monien erilaisten likiverkkoratkaisujen joukossa. WiFi Alliancen tapaan myös likiverkkostandardien taustalla ovat niiden käyttöä ja kehitystä edistävät yhdistykset. WirelessHART:n taustalla on HART Communication Foundation [52], ISA100.11a:n taustalla on The International Society of Automation eli ISA [53] ja ZigBee:n taustalla on ZigBee Alliance [54]. Nämä yhdistykset koostuvat alan yrityksistä ja organisaatioista.

Vaikka tässä työssä ei muuten perehdytä tarkemmin IEEE 802.15.4-standardiperheen eri versioihin, on tässä yhteydessä hyvä mainita standardin e-versio. IEEE 802.15.4e-versio pyrkii parantamaan standardin soveltuvuutta teollisuuskäyttöön lisäämällä siihen taajuushyppely (frequency hopping) toiminnallisuuden [55]. Näin pyritään parantamaan tiedonsiirron luotettavuutta ulkoisia häiriötekijöitä vastaan sekä vähentämään signaalin häipymisen vaikutuksia. Standardin määrittelemä taajuushyppely perustuu ajanjakson mukaan vaihtuvaan taajuuteen, aika jaetaan tiettyihin väleihin ja kullakin välillä käytettävä taajuus lasketaan standardin määrittelemällä yhtälöllä.

2.5.3 Fyysinen kerros

IEEE 802.15.4-standardin fyysinen kerros on suunniteltu käyttämään vapaita ISM-taajuusalueita, näistä Euroopassa ovat käytössä 868MHz-taajuusalue ja 2,4GHz-taajuusalue. Lisäksi joillain alueilla Euroopan ulkopuolella on

käytettävissä 915MHz-taajuusalue. Kuten IEEE 802.11-standardissa fyysisen kerroksen perustehtävä on lähettää ja vastaanottaa radiosignaaliin koodattua tietoa. Lisäksi fyysinen kerros vastaan radiolähettimen pois ja päälle kytkemisestä, radiokanavan laadun tarkkailemisesta ja kanavanvalinnasta [7]. Tiedonsiirto tapahtuu käyttäen suorasekventointi (Direct Sequence Spread Spectrum, DSSS), modulaatiotekniikka riippuu käytettävästä taajuudesta. Standardin alkuperäinen versio IEEE 802.15.4-2003 [56] määrittelee 868MHz-taajuusalueelle käytettäväksi binäärisen vaiheavainnuksen (Binary Phase-Shift Keying, BPSK), jolla saavutetaan 20 kbps tiedonsiirtonopeus. Vaihtoehtoisesti standardin uudempi IEEE 802.15.4-2006 [7] versio mahdollisuuden käyttää rinnakkaissekventointia (Parallel Sequence Spread Spectrum, PSSS) ja ASK (Amplitude Shift Keying) modulaatiota 868MHz-taajuusalueella, jolla saavutetaan 250 kbps tiedonsiirtonopeus. Toinen lisäys on mahdollisuus käyttää O-QPSK (Offset-Quadrature Phase Shift Keying)-modulaatiota samalla taajuusalueella, jolloin tiedonsiirtonopeus on korkeintaan 100 kbps. Tätä modulaatiota käytetään myös 2,4GHz-taajuusalueella, jolloin tiedonsiirtonopeus on korkeintaan 250 kbps.

IEEE 802.15.4-standardi jakaa taajuusalueet 27:ään kanavaan numeroituna 0-26, yksi kanava 868MHz-taajuusalueelle, kymmenen 915MHz-taajuusalueelle ja 16 kpl 2,4GHz-taajuusalueelle. Tässä työssä keskitytään 2,4GHz-taajuusalueelle, tämän alueen kanavajako on esitetty ISM-taajuuksia käsittelevässä kappaleessa.

Fyysisen kerroksen tehtävä on arvioida onko haluttu radiokanava vapaa tiedonsiirtoon. Tähän käytetään CCA (Clear Channel Assessment) mekanismia. Mekanismissa on kolme toimintamuotoa: CCA Mode 1, 2 ja 3. Mode 1 arvioi kanavalta mitattua energiaa, jos energia ylittää asetetun rajan oletetaan kanava varatuksi. Mode 2 pyrkii tunnistamaan kanavalta jonkin ennalta tunnetun modulaatio- tai hajautustekniikan, jos tällainen havaitaan, voidaan kanava olettaa varatuksi. Kanavalta mitattu energia ei vaikuta tähän päätökseen. Mode 3 yhdistää kaksi edellistä, eli siinä pyritään havaitsemaan

energiataso ja tunnettu signaali. CCA tekniikan hyödyntäminen on osa koeksistenssin varmistamista.

2.5.4 Siirtokerros

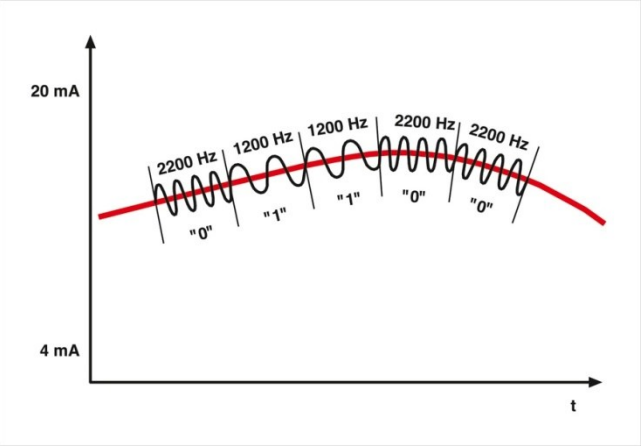
Protokollan siirtokerroksen vastuulla on hallita verkkoon liittymistä, verkosta poistumista ja koordinoida siirtotien tasaväkistä hyödyntämistä. IEEE 802.15.4-standardissa on IEEE 802.11-standardin tapaan käytössä CSMA/CA-tekniikka [24], mutta toisin kuin IEEE 802.11 se ei tue IEEE 802.1x kehyksiä. IEEE 802.15.4 kehykset on suunniteltu olemaan mahdollisimman yksinkertaisia ja kestäviä häiriöitä vastaan.

Siirtokerros määrittelee onko verkossa käytössä koordinaattorisolmu. Jos koordinaattoria ei käytetä, verkon solmut pyrkivät lähettämään tietoa heti sen saatuaan. Radiokanavan käyttö perustuu tavalliseen CSMA/CA-mekanismiin, jossa solmu odottaa satunnaisen aikavälin (backoff period). Tämän aikavälin jälkeen solmu kuuntelee radiokanavaa tarkistaakseen sen olevan vapaa. Jos kanavan havaitaan olevan vapaa, voidaan paketti lähettää vastaanottajalle. Jos kanava on varattu, odottaa solmu toisen satunnaisen pituisen aikavälin ja yrittää sen jälkeen lähetystä uudestaan. Uudelleenyritysten määrä on rajattu. Jos verkossa on koordinaattori, käytetään aikaväleihin jaettua CSMA/CA-tekniikkaa. Tällöin solmut kilpailevat pääsystä radiotielle ennalta määrätyillä ajan hetkillä. Näiden kahden vaihtoehdon lisäksi tiedonsiirto voi tapahtua ilman CSMA/CA:tä käyttäen aikaväleihin perustuvaa vuorottelua.

Kun verkossa on käytössä koordinaattori, protokolla täyttää myös reaaliaikaisen liikenteen vaatimukset tarjoamalla mahdollisuuden käyttää varattuja aikavälejä (guaranteed time slot, GTS). Tällä mekanismilla pyritään takaamaan pakettien oikea-aikainen toimitus, joka on erityisesti anturiverkkosovelluksissa tärkeää. Kun käytössä on aikaväleihin jaettu siirtotien varaus, voidaan osa aikaväleistä varata käyttöön ilman kilpavarausta. Nämä aikavälit jaetaan reaaliaikaista tiedonsiirtoa vaativille sovelluksille, eli niiden tulee siirtää tietoa aina ennalta määrätyllä ajan

hetkellä. Vastineeksi tiedonsiirto tapahtuu ilman kilpailua ja tasaisin aikavälein jolloin oikea-aikaisuudesta voidaan varmistua.

2.5.5 WirelessHART



Kuva 6, HART-protokollan taajuusmodulaatio

Alkuperäinen HART-protokolla mahdollistaa digitaalisen tiedonsiirron hyödyntäen yleisesti automaatiossa käytettyä 4-20mA analogisignaalia. Digitaalinen tieto on koodattu signaaliin käyttäen taajuusmodulaatiota (frequency shift keying, FSK), jossa 0- ja 1-bitit vastaavat eri taajuuksilla lähetettyjä pulsseja [57]. Periaate on havainnollistettu kuvassa 6. HART standardin 7. versiosta lähtien protokollaan on kuulunut myös mahdollisuus siirtää tietoa langattomasti laitteiden välillä. Tämä langaton tiedonsiirto tunnetaan nimellä WirelessHART, se mahdollistaa HART tiedonsiirron IEEE 802.15.4-pohjaisessa langattomassa anturiverkossa.

WirelessHART verkko koostuu seuraavista osista [11]:

- **Kenttälaite (Field Device),** johon kuuluu moduuli langattomaan tiedonsiirtoon
- **Adapteri (Adapter),** joka kytkeytyy langalliseen HART laitteeseen ja mahdollistaa sille WirelessHART tiedonsiirron
- **Kannettava laite (Handheld),** joka hoitaa kenttälaitteiden asetusten määrittelyn, diagnostiikan ja kalibroinnin
- **Yhdyskäytävä (Gateway),** joka yhdistää WirelessHART-verkon automaatiojärjestelmään
- **Verkon hallintalaite (Network Manager),** joka hallinnoi verkkoa ja laitteita
- **Tietoturvan hallintalaite (Security Manager),** joka vastaa verkossa käytettävien salausavainten luomisesta, varastoimisesta ja hallinnoinnista

Kolme viimeistä osaa yhdistetään usein yhteen laitteeseen, mutta ne voidaan myös eritellä toimintavarmuuden parantamiseksi. WirelessHART verkossa kaikki laitteet kykenevät reitittämään muiden laitteiden paketteja jolloin verkon topologia on mesh-tyyppinen, ks. kuva 5. WirelessHART käyttää 2,4GHz-taajuusalueella IEEE 802.15.4:n kanavia 11-25.

2.5.6 ISA100.11a

ISA100.11a-standardin tavoitteena on tarjota langatonta tiedonsiirtoa teollisuusautomaatio tarpeisiin. WirelessHART:n tavoin tiedonsiirto perustuu IEEE 802.15.4-pohjaiseen anturiverkkoon [58]. Toisin kuin WirelessHART ISA100.11a ei ole sidottu johonkin tiettyyn kenttäväylään, vaan sen tarkoituksena on kyetä siirtämään mitä tahansa tietoa.

ISA100.11a verkko koostuu seuraavista laitteista [12]:

- **Sisään-/ulostulo (Input/Output),** kenttälaite eli käytännössä joko anturi, joka tuottaa tietoa tai toimilaite, joka saa aikaan jonkin toiminnon vastaanottamansa tiedon perusteella
- **Reititin (Router),** joka kykenee reitittämään muilta laitteilta saamaansa tietoa
- **Valmistelu (Provisioning),** joka kykenee valmistelemaan toisen laitteen liittymään verkkoon
- **Runkoverkon reititin (Backbone router),** joka kykenee reitittämään tietoa runkoverkon ja anturiverkon välillä
- **Yhdyskäytävä (Gateway),** joka yhdistää ISA100.11a verkon muihin tietoverkkoihin
- **Järjestelmän hallintalaite (System manager),** joka hallinnoi verkkoa ja sen laitteita
- **Turvallisuuden hallintalaite (Security manager),** joka yhdessä järjestelmän hallintalaitteen kanssa varmistaa verkon turvallisen toiminnan

- **Järjestelmän aikalähde (System Time Source),** joka vastaa aikatiedon ylläpitämisestä koko verkolle

Verkon rakenne eroaa WirelessHART:n vastaavasta huomattavasti, mikä johtaa erilaisiin mahdollisiin verkkotopologioihin. Kenttälaitteet eivät välttämättä kykene reitittämään tietoa lainkaan jolloin verkon topologia on mesh- ja tähtiverkon hybridi, ks. kuva 5. ISA100.11a käyttää samoja 2,4GHz-taajuusalueen kanavia kuin WirelessHART, mutta myös kanavan 26 käyttö on mahdollista.

2.5.7 Wireless network for Industrial Automation-Process Automation WIA-PA

WIA-PA on Kiinassa kehitetty tiedonsiirtoprotokolla automaatiokäyttöön, joka perustuu WirelessHART:n ja ISA100.11a:n tavoin IEEE 802.15.4-standardin fyysiseen ja tiedonsiirtokerrokseen. WIA-PA ei ole sidonnainen mihinkään tiettyyn kenttäväylä standardiin, vaan verkko kykenee siirtämään mitä tahansa tietoa.

WIA-PA verkko koostuu seuraavista osista [59]:

- **Hallinnointi PC (Host computer),** josta käyttöhenkilökunta pystyy hyödyntämään WIA-PA verkon tarjoamaa tiedonsiirtomahdollisuutta
- **Yhdyskäytävä (Gateway [GW]),** joka yhdistää WIA-PA verkon muihin tietoverkkoihin
- **Reititin (Routing device),** joka reitittää muilta WIA-PA verkon laitteilta tulevaa liikennettä
- **Kenttälaite (Field device),** joka on suoraan liitetty prosessiin, esim. anturi tai toimilaite
- **Kannettava laite (Handheld device),** joka vastaa verkon laitteiden
- **Verkon hallintalaite (Network manager [NM]),** joka hallinnoi verkkoa, tiedonsiirtoa reitittimien välillä ja valvoo verkon suorituskykyä

- **Tietoturvan hallintalaite (Security manager [SM]),** joka vastaa verkossa käytettävistä avaimista ja verkkoon liittyvien kenttä- ja reititinlaitteiden todentamisesta

WIA-PA verkon mahdollisia topologioita ovat mesh- ja tähtiverkon hybridi sekä tähtiverkko. Radiokanavista käytössä ovat ISA100.11a:n tavoin 11-26. Tässä on ollut tarkoituksena lähinnä esitellä lyhyesti olemassa olevat anturiverkkoprotokollat, tarkemmat tiedot niiden toiminnasta löytyy protokollien standardointidokumenteista sekä protokollien välinen vertailu lähteistä [17] ja [59].

2.6 Langattomien verkkojen koeksistenssi

Koska siirtotie on kaikille yhteinen, vain yksi asema voi lähettää signaalia tietyllä ajanhetkellä jollakin tietyllä taajuuskaistalla häiriöttä. Käytettäessä useampia laitteita samalla taajuusalueella samanaikaisesti on vaarana, että laitteiden lähettämät signaalit häiritsevät muita samalla taajuusalueella toimivia laitteita. Häiriöiden minimoimiseksi ja mahdollisimman tehokkaan taajuuksien hyödyntämisen varmistamiseksi viranomaiset ovat määritelleet säännöt kuinka kullakin taajuusalueella toimivien radiolaitteiden tulee toimia [14] [15]. Säännöillä varmistetaan erilaisten radiostandardien koeksistenssi sekä siirtotien tasapuolinen käyttö samalla taajuusalueella. Mitä pienempi taajuusalue on käytettävissä ja mitä enemmän laitteita on jakamassa kyseistä taajuusaluetta, sitä todennäköisempää on, että signaalit häiritsevät toisiaan. Tässä työssä tarkastelluista taajuusalueista 2,4GHz-alue on ongelmallisin, sillä alue on suhteellisen pieni (2400MHz – 2483 MHz) ja sillä toimivia standardeja ja niihin perustuvia laitteita on paljon. Kuten ISM-taajuuksia käsittelevässä kappaleessa havaittiin, sekä IEEE 802.11, että IEEE 802.15.4 jakavat käyttämänsä taajuusalueen pienempiin kanaviin. Käytettäessä vain kolmea IEEE 802.1-pohjaista verkkoa 20MHz kaistanleveydellä on suurin osa 2,4GHz-taajuusalueesta käytössä ja IEEE 802.15.4-standardin kanavia jää vapaaksi vain kolme kuudestatoista mahdollisesta. Kanavat eivät myöskään ole täysin ortogonaalisia, eli signaali

vuotaa hieman kanavan viereisille taajuuksille. Käytettäessä IEEE 802.11n-standardin mukaisia 40MHz leveitä kanavia on tilanne vielä huonompi. Eri standardien välistä koeksistenssiä varmistamaan on perustettu IEEE:n toimesta kaksi työryhmää. Näistä ensimmäinen on IEEE 802.15 WPAN™ Task Group 2 (TG2) [60], joka keskittyi WLAN ja WPAN verkkojen väliseen koeksistenssiin, ryhmän toiminta on loppunut. Toinen ryhmä on IEEE 802.19 Wireless Coexistence Working Group (WG) [61], joka perehtyy yleisesti koeksistenssiin vapaasti käytettävillä taajuusalueilla. Ryhmien tehtävänä on tutkia sekä standardien väliseen yhteistyöhön perustuvaa koeksistenssiä, jonka toiminta perustuu standardien väliseen tiedonvaihtoon, että itsenäiseen toimintaan perustuvaa koeksistenssiä, joka perustuu radiotiellä olevien häiriöiden havaitsemiseen ja erotteluun.

IEEE 802.11 ja IEEE 802.15.4 standardien välistä koeksistenssiä on tutkittu alan kirjallisuudessa varsin paljon. Tutkimus keskittyy usein tilanteeseen, jossa IEEE 802.11-pohjainen verkko aiheuttaa häiriötä IEEE802.15.4 verkolle ja tapoihin, joilla häiriö pystytään havaitsemaan ja välttämään löytämällä vähemmän häiriöinen radiokanava [62] [63].

Uudet EN 300 328 V1.8.1-määräykset [64] asettavat tiukemmat rajoitukset laajakaistamodulaatiolle 2,4GHz taajuusalueella. Tavoitteena parantaa erilaisten teknologioiden koeksistenssiä vaatimalla laitteilta tuki taajuushyppelylle. Määräykset tulevat näillä näkymin vaikuttamaan vuoden 2014 jälkeen myytäviin laitteisiin. Yhteensopivuus tulee ottaa huomioon, jos halutaan käyttää samanaikaisesti uuden ja vanhan standardin laitteita. Käytännössä tämä aiheuttaa ongelmia lähinnä laitevalmistajille. Tässä yhteydessä on lähinnä hyvä tiedostaa, miten nopeasti teknologia ja siihen liittyvät määräykset kehittyvät. Nopea kehitys tarkoittaa käytännössä jatkuvaa tarvetta päivittää laitekantaa. Tähän liittyen kannattaa huomata, että 802.11-standardin uudemmat versiot sisältävät paljon tekniikkaa säilyttääkseen taaksepäin yhteensopivuuden standardin vanhempia versioita noudattavien laitteiden kanssa [18] [21]. Uudemmat standardit hyödyntävät taajuuskaistan

tehokkaammin ja ilman tarvetta taaksepäin yhteensopivuudelle voitaisiin ainakin teoriassa saavuttaa korkeampia siirtonopeuksia [65].

Langattoman teollisuusautomaatio kannalta koeksistenssiä ja sen hallintaa käsitellään IEC:n standardissa 62657-2 [51]. Standardi määrittelee koeksistenssin tärkeimmät tekijät sekä siihen liittyvän hallintaprosessin. Koeksistenssin saavuttamiseksi on ensin määriteltävä langattoman sovelluksen asettamat vaatimukset sekä koeksistenssiin liittyvät tekijät. Näiden perusteella voidaan tehdä tarvittavat suunnitelmat joita seurataan ja ylläpidetään. Olennainen tekijä on määrittää koeksistenssiin liittyviä tekijöitä hallinnoiva vastuuhenkilö. Vastuuhenkilön tukena on tarpeen mukaan radiotekniikan asiantuntijoita. Nykytilanteessa nyt tutkimuksen kohteena olevalla voimalaitoksella ei vielä tässä vaiheessa ole tarkoituksena toteuttaa useita rinnakkaisia langattomia järjestelmiä, mutta langattomien järjestelmien yleistyessä voi tarvetta olla tällaiselle vastuuhenkilölle.

Vaikka molemmissa standardeissa on käytössä mekanismeja itsenäiseen koeksistenssin varmistamiseen, on väistämätön tosiasia, että samalla taajuudella toimivat verkot aiheuttavat toisilleen häiriöitä [63] [66]. Järkevällä suunnittelulla voidaan tilannetta helpottaa jonkin verran valitsemalla kanavat siten, että kumpikaan standardi ei täytä suurta jatkuvaa aluetta taajuuskaistasta. Taajuuksien käytön suunnittelun lisäksi koeksistenssiä voidaan parantaa suunnittelemalla radioresurssien käyttöä ajan ja tilan suhteen [66]. Tiedonsiirto voidaan pyrkiä jaksottamaan ja signaalien törmäyksiä vähentämään esimerkiksi suunta-antennien käytöllä. Tässä työssä koeksistenssiin liittyviä ongelmia pyritään ratkaisemaan tutkimalla 5GHz-taajuusalueen soveltuvuutta voimalaitos ympäristöön. Jos IEEE 802.11-pohjaiset laitteet voidaan siirtää pääasiassa 5GHz-alueelle, voidaan mahdollinen IEEE 802.15.4 verkko suunnitella välttämään jo nyt alueella olevia 2,4GHz-alueen verkkoja.

2.8 Vaatimusmäärittely

2.8.1 Tekniset vaatimukset

Käyttötarkoitukseen soveltuvan langattoman ratkaisun valitsemiseen vaikuttaa joukko teknisiä tekijöitä. Nämä tekijät ohjaavat valintaa kohti tiettyä radioteknologiaa. Vaikka tässä työssä keskitytään pääasiassa WLAN- ja anturiverkkoihin, vaatimusmäärittelyssä laajennetaan tarkastelua hieman tämän rajauksen ulkopuolelle. Vaatimuksia läpikäydessä on tarkoitus aloittaa yleiseltä tasolta, vaatimuslistaa läpikäydessä voidaan valinta tarkentaa lopulta johonkin tiettyyn teknologiaan.

Tekniset vaatimukset ovat seuraavanlaisia:

- *Toimintaetäisyys*: ensimmäisenä on määriteltävä millä etäisyydellä tietoa halutaan siirtää. Vaikka monet teknologiat tarjoavat suuren skaalan toimintaetäisyyksiä, vaikuttaa haluttu etäisyys esimerkiksi tarvittaviin antenneihin, lähetystehoihin ja radiotaajuuteen. Kun toimintaetäisyys tiedetään, voidaan tarpeet arvioida karkeasti selvittämällä signaalin eteneminen ilman heijastuksia suoralla näköyhteydellä. Toimintaetäisyys vaikuttaa myös tarvittavaan lähetystehoon, jos laitteet säätävät lähetystehoa automaattisesti voi tällä olla vaikutus esimerkiksi langattoman anturisolmun akkukestoon.
- *Sovelluskohde*: sovelluskohde eli fyysinen tila, johon järjestelmä halutaan toteuttaa, liittyy läheisesti toimintaetäisyyteen, mutta tässä tarkastelussa perehdytään tarkemmin tilan rakenteeseen ja sen asettamiin vaatimuksiin. Toimintaetäisyyden perusteella valinta rajataan suoran näköyhteyden kantaman perusteella. Sovelluskohteen perusteella rajausta tarkennetaan entisestään tutkimalla signaalin etenemistä sovelluskohteessa. Tutkimus joudutaan useimmiten tekemään käytännön mittauksin, jos kohde sisältää esimerkiksi paljon radiosignaalia heijastavia pintoja tai vaimentavia rakenteita. Lisäksi sähkölaitteet ja liikkuvat esineet saattavat aiheuttaa aikariippuvaisia häiriöitä. Sovelluskohteen perusteella voidaan rajausta tarkentaa taajuuksien ja tarvittavien radiolaitteiden suhteen.

- *Taajuusalue*: kun toimintaetäisyys ja sovelluskohde on päätetty, ja tarvittavat tutkimukset tehty voidaan valita sopiva taajuusalue. On kuitenkin hyvä muistaa, että kaikki teknologiat eivät tarjoa suuria mahdollisuuksia vaikuttaa toimintataajuuteen. Myös viranomaisten määräykset vaikuttavat siihen miten milläkin taajuusalueella saa toimia, suurin osa radiotaajuuksista ei ole vapaasti käytettävissä [15]. Tämän työn laajuudessa valinta tapahtuu lähinnä eri ISM-taajuuksien välillä. Taajuusalueen valintaan vaikuttaa oleellisesti myös *koeksistenssi* muiden laitteiden kanssa. Samalla taajuudella toimivat laitteet vaikuttavat negatiivisesti kuuluvuusalueellaan olevien laitteiden toimintaan. Valinta tulisi tehdä mahdollisuuksien mukaan siten, että samalla taajuusalueella toimivia laitteita on toistensa lähellä mahdollisimman vähän.
- *Standardienmukaisuus*: Laitteiden olisi hyvä noudattaa yleisesti hyväksyttyjä standardeja, jolloin yhteensopivuus eri laitevalmistajien välillä voidaan varmistaa.
- *Loppukäyttäjille tarjottu palvelu*: tarjottujen palveluiden perusteella voidaan määritellä kuinka suuri tiedonsiirtokapasiteetti verkon tulee tarjota, ja mahdolliset vasteaikavaatimukset. Tiedonsiirtokapasiteetti vaikuttaa mahdolliseen langalliseen siirtoverkkoon, jonka kapasiteetin tulee olla riittävä [18] [21].
- *Laitteiden suojaus*: IP (Ingress Protection Rating tai International Protection Rating)-luokitus on standardoitu tapa ilmoittaa erilaisten laitteiden suojaus ympäristön likaa ja kosteutta vastaan. Luokitus löytyy standardista IEC 60529 [67]. Voimalaitosympäristössä useat tilat ovat sellaisia, missä syntyy laitteille haitallista likaa, esimerkiksi pölyä. Lisäksi joissain tiloissa laitteet voivat altistua eri määrille kosteutta. Riittävää suojaustasoa päättäessä myös liittimien suojaus on otettava huomioon. Luokitus tulee valita pahimman tapauksen mukaan, tämä saattaa tulla vastaan laitteita siirrettäessä tilasta toiseen. IP-luokitus koostuu IP-kirjaimista, kahdesta numerosta ja

vapaaehtoisista kirjaimista. Numeroiden merkitykset ovat seuraavat [67]:

IP-luokituksen ensimmäinen numero [68]:

Taulukko 2, IP-luokituksen ensimmäisen numeron merkitykset

Numero	Vaatimus	Suojaus lähestyvien osien varalta
0	Ei suojausta	Suojaamaton
1	Suojaus suurilta kappaleilta, halkaisija min. 50mm	Nyrkki, kädenselkä
2	Suojaus keskikokoisilta kappaleilta, halkaisija min. 12,5mm	Sormi
3	Suojaus pienilta kappaleilta, halkaisija min 2,5mm	Työkalu
4	Suojaus erittäin pieniltä kappaleilta, halkaisija min 1mm	Lanka
5	Suojaus pölyltä, ei täydellinen pölytiiveys, ei haitallinen pölykertymä sallittu	Johdinlanka
6	Täydellinen suojaus pölyltä	Johdinlanka

IP-luokituksen toinen numero[68]:

Taulukko 3, IP-luokituksen jälkimmäisen numeron merkitykset

Numero	Vaatimus	Suojaus vedeltä
0	Ei suojausta	Suojaamaton
1	Suojaus suoraan ylhäältä putoavalta vedeltä, osittainen sisääntunkeutuminen sallittu	Pystysuoraan putoava sadevesi
2	Suojaus ylhäältä putoavaa vettä vastaan, kappale kallistettu 15°, osittainen sisääntunkeutuminen sallittu	Maks. 15° pystysuorasta putoava vesi
3	Suojaus maks. 60° kulmassa putoavalta vedeltä, osittainen sisääntunkeutuminen sallittu	Rajoitettu satava vesi
4	Suojaus joka suunnasta tulevia roiskeita vastaan, osittainen sisääntunkeutuminen sallittu	Roiskevesi joka suunnasta
5	Suojaus joka suunnasta tulevaa vesiruiskua vastaan, osittainen sisääntunkeutuminen sallittu	Suihkutettu vesi joka suunnasta
6	Suojaus joka suunnasta tulevaa voimakasta vesisuihkua vastaan, osittainen sisääntunkeutuminen sallittu	Voimakkaasti suihkuava vesi joka suunnasta
7	Suojaus 15cm-1m upotusta vastaan	Lyhytaikainen upotus veteen
8	Suojaus pitkäaikaista upotusta vastaan	Jatkuva upotus veteen

- *Käyttölämpötila:* Prosessitilojen lämpötila voi olla korkea, asennuspaikasta riippuen laitteilta voidaan vaatia korkeaa toimintalämpötilaa.
- *Palo- ja räjähdysvaara:* Laitteita hankittaessa niiden tulee täyttää tarvittava ATEX-luokitus [69] [70]. ATEX-direktiivi koskee laitteita, joita käytetään normaali-ilmapaineisissa ilmaseoksissa tiloissa, joissa on syttymislähde [71]. Laitteiden tulee olla ATEX-tilaan sopivaksi luokiteltu tai laite tulee sijoittaa sopivaan suojakoteloon. Langattomien laitteiden tapauksessa tämä voi tarkoittaa laitteen sijoittamista koteloon, josta antennit on tuotu johdoilla kotelon ulkopuolelle.

- *Laiteasennus ja -huolto:* laitteet vaativat vähintään fyysisen asennuksen, mutta tämän lisäksi voidaan tarvita sähkö- tai datakaapelointi. WLAN-laitteille sähkö voidaan tuoda datakaapelin mukana Power over Ethernet (PoE)-tekniikalla, anturiverkkojen virransaantiin on perehdytty tarkemmin niitä käsittelevässä kappaleessa. Laitteet vaativat huoltamista tai rikkinäisten laitteiden vaihtamista, näiden on hyvä olla mahdollisimman pitkälle oman henkilökunnan hoidettavissa. Esimerkiksi akkukäyttöinen anturiverkon solmu voi vaatia akun vaihtamista kerran vuodessa.
- *Tietoturva:* koska kyseessä on tuotantovarmuuskriittinen voimalaitosympäristö, tulee langattomien järjestelmien tietoturvan olla riittävällä tasolla. Tietoturvaa voidaan arvioida eri tavoin ja näihin seikkoihin onkin perehdytty omassa kappaleessaan. Yleisesti voidaan kuitenkin sanoa, että tietoturvan tulee osoitetusti täyttää sille asetetut vaatimukset luottamuksellisuuden, eheyden ja saatavuuden suhteen.

2.8.2 Käyttö- ja taloudelliset vaatimukset

Oleellisimmat vaatimukset verkkoteknologian valinnalle tämän projektin kannalta ovat laitekustannukset, liitäntämahdollisuudet olemassa oleviin järjestelmiin sekä laitteiden helppokäyttöisyys. Jos laitteet on tarkoitus liittää prosessiverkkoon joten myös tietoturvan oltava erittäin hyvällä tasolla, sekä laitteiden on oltava mahdollisimman pitkälle laitoksen työntekijöiden hallittavissa. Ympäristö, johon verkot on tarkoitus toteuttaa asettavat myös joitakin rajoituksia, mutta näiden ratkaiseminen on enemmän tekninen haaste verkon toteutusvaiheessa kuin suoranaisesti teknologian valintaan liittyvä kysymys.

Tämänkaltaisessa projektissa, jossa varsinkin alkuvaiheessa kaivataan joustavuutta laitteiden suhteen, ei ole kannattavaa sitoutua suureen hankintaan. Vielä alun konseptivaiheessa kustannusten ei pitäisi nousta ongelmaksi, mutta jos järjestelmää halutaan laajentaa, tulee laajennuksen hinnan olla selvillä. Tämän takia peruskonseptin tulee olla tarkasti selvitetty,

jotta laajennusten toteutus olisi helppoa, ja kustannukset tiedossa. Jos järjestelmä todetaan toimivaksi ja hyödylliseksi, se voidaan ottaa käyttöön helposti myös yrityksen muilla laitoksilla toimivan peruskonseptin avulla. Konseptivaiheessa yksittäisten laitteiden kustannukset on hyvä pitää kohtuullisina, jolloin erilaisia laiteyhdistelmiä testatessa kustannukset pysyvät alhaisina. Järjestelmälle voi olla tarpeen selvittää myös jonkinlainen takaisinmaksuaika perustuen esimerkiksi mahdollisiin energiansäästöihin tai työtehon parannuksiin.

Laitteiden käyttöönotto, asetusten määrittely ja muuttaminen sekä mahdolliset huoltotoimenpiteet tulisi olla mahdollisimman pitkälle yrityksen omien työntekijöiden hoidettavissa.

Voimalaitoskäytössä on yleistä, että erilaisten järjestelmien kuten automaatiojärjestelmien käyttöikä on huomattavan pitkä, pisimmillään jopa 30-40 vuotta. Tämä asettaa odotuksia tilaajan ja käyttäjien suunnalta myös langattomien järjestelmien käyttöiälle. Tämä korostuu erityisesti jos langatonta teknologiaa hyödynnetään osana automaatiojärjestelmää, jolloin langattoman tekniikan päivittäminen teknologiakehityksen mukana voi olla haastavaa ja kallista. Tulee kuitenkin ymmärtää, että langaton teknologia kehittyy nopeasti, laitteiden elinkaari tulee todennäköisesti olemaan huomattavasti lyhyempi kuin automaatiojärjestelmillä.

Laitteiden elinkaarta on tärkeä tarkastella myös tietoturvan kannalta. Tietokoneiden laskentatehon kasvaessa jatkuvasti on mahdollista, että langaton salaus voidaan murtaa puhtaasti väsytystekniikalla (brute force tekniikka). Tämä tarkoittaa käytännössä kaikkien mahdollisten merkkiyhdistelmien laskemista kunnes salasanaa vastaava merkkijono löytyy. Nykyisillä kuluttajatietokoneilla tällainen hyökkäys ei ole vielä realistinen. Jos kuitenkin laskentatehon kehitys jatkuu nykytahtiin Mooren lain mukaan kaksinkertaistuen aina n. kahden vuoden välein, on tämäkin riski otettava huomioon. Salasanan pituus määrää tarvittavan laskenta-ajan, WPA2-standardi [72] määrittelee salasanan minimipituudeksi vähintään 8 merkkiä. Tämä korostaa myös fyysisen turvallisuuden merkitystä, jotta voidaan

varmistaa että mahdollisimman harva ulkopuolinen pääsee käsiksi langattomiin verkkoihin. Pahimmassa tapauksessa verkot voitaisiin joutua eristämään fyysisesti jotta ne eivät pääse ”vuotamaan” voimalaitoksen ulkopuolelle. Tässä tapauksessa yhteyksien toteuttaminen kaapeloidulla ratkaisulla olisi varmasti edullisempi ja helpompi toteuttaa. Ympäristön kohinatason myötä, kun samalla taajuudella toimivien laitteiden määrä kasvaa, tämä vaikuttaa pitkällä aikavälillä myös langattomien verkkojen toimintaan. Riskinä voi olla, että tulevaisuudessa langattomia laitteita joudutaan korvaamaan tehokkaammiksi tai herkemmiksi, jotta kommunikaatio olisi edelleen mahdollista kohinan kasvaessa.

Laitteiden/verkon hallinta, laitteiden oltava mahdollisimman pitkälle yrityksen työntekijöiden hallittavissa. Eduksi voidaan lukea mahdollisuus suorittaa perus huolto- ja korjaustoimenpiteet itse, ilman ulkopuolista henkilökuntaa esimerkiksi osana vuosihuoltoa.

3. Langattomuuden hyötyanalyysi

Tässä kappaleessa on tarkoituksena tarkastella sekä langattomien verkkoratkaisujen tuomia etuja, että sen asettamia haasteita ja ongelmia yleisellä tasolla. On tärkeää huomata, että jotkin seuraavista kohdista löytyvät sekä etujen, että haasteiden alta riippuen sovelluskohteesta. Tämän lisäksi vääränlainen toteutus voi siirtää mahdollisen edun haitaksi, äärimmäisenä esimerkkinä täysin langaton järjestelmä voi olla kustannuksiltaan kalliimpi, jos se epävarmuutensa vuoksi aiheuttaa tuotantoon keskeytyksiä. Langattomuus ei saa myöskään olla itsetarkoitus, vaan sen tulee palvella järjestelmää ja sen käyttäjiä. Langaton tiedonsiirto voidaankin ajatella yhtenä monista palveluista, jotka edistävät pääliiketoiminnan suoritusta. Langattomat verkot voivat palvella esimerkiksi suoraan loppukäyttäjää tai toisaalta ne voivat mahdollistaa muuten hankalan tiedonsiirron osana automaatiojärjestelmää.

3.1 Langattomuuden edut

Seuraavassa on listattu langattomien tekniikoiden tuomia mahdollisia etuja:

- *Asennus:* Kaapeleiden korvaaminen hankalissa asennuksissa langattomalla yhteydellä voi helpottaa sekä laitteen asennusta, että käyttöä [36]. Liikkuvissa laitteissa langaton yhteys voi olla erittäin yksinkertainen ja siten kustannustehokas ratkaisu laitteen ohjaamiseen. Verrattuna langallisiin mittauksiin anturiverkot mahdollistavat mittausten helpomman toteutuksen myös vaativissa olosuhteissa. Mittaus voidaan toteuttaa siten, että tieto siirretään monen anturisolmun kautta. Jos tähän yhdistetään vielä laitteisto, joka kykenee ottamaan toimintaenergiansa ympäristöstään, voidaan toteuttaa mittauksia sellaisissa paikoissa, joihin kaapelointi olisi kallista, vaikeaa tai jopa vaarallista. Anturiverkkojen käyttöönotto suuressa skaalassa voi olla langallista vaihtoehtoa helpompaa, jos laitteille saadaan energiaa riittävän helposti. Myös esimerkiksi yksittäisiä uusia mittauksia voi olla helpompaa toteuttaa langattomasti, jos esimerkiksi kenttäkoteloon ei ole enää mahdollista liittää lisää laitteita. Laitteiden

käyttöönotto on joustavampaa ja nopeampaa tarvittavan johdotuksen vähentyessä.

- *Joustavuus:* Langatonta järjestelmää on helpompi ja halvempi laajentaa ja muuttaa, kun laitteiden siirto ei vaadi uusien kaapelointi. Laitteet voidaan myös asentaa vähemmän ongelmallisiin paikkoihin radiosignaalin kuuluvuuden puitteissa. Anturiverkot voivat olla itseorganisoituvia, jolloin verkon ensiasennus ja mahdolliset muutokset eivät vaadi muuta kuin laitteiden sijoittamisen paikoilleen. Langaton tekniikka tuo joustavuutta myös automaatiojärjestelmän päähän helpottamalla järjestelmän laajentamista. Langoitetussa järjestelmässä tieto siirretään käyttäen automaatiojärjestelmän I/O-kortteja. Kortit on sijoitettu automaatiojärjestelmän kaappeihin ja niiden määrä on mitoitettu sisältämään nykyiset signaalit ja jonkin verran laajennusvaraa. Kaappeja ja siten kortteja voidaan asentaa vain jokin rajallinen määrä ja määrän täyttyessä muuttuu laajentaminen vaikeaksi. Langattomat anturiverkot voivat tarjota tähän tilanteeseen sopivan ratkaisun. Niiden avulla voidaan automaatiojärjestelmän kapasiteettia kasvattaa ilman automaatiokaappien laajennuksia. Anturiverkon kapasiteetin kasvattamiseen riittää uusien anturisolmujen käyttöönotto.
- *Kustannukset:* Kaapelit ja niiden liittimet ovat alttiita mekaaniselle hajoamiselle erityisesti jos niitä joudutaan kytkemään ja irrottamaan usein, tällaisessa tapauksessa langaton linkki voi olla hyvä ratkaisu jatkuvan kaapeleiden korjaamisen sijaan. Kaapelit voivat myös ikääntyessään haurastua ja hajota. Huoltotarpeen vähentyessä myös tuotannon keskeytyksistä johtuvat rahalliset menetykset vähenevät. Huoltokustannusten lisäksi myös asennus voi tulla halvemmaksi, kun vältytään mahdollisesti kalliilta kaapelinvedoilta. Erityisen hyödyllistä tämä voi olla tapauksissa, joissa tarvitaan lisää tiedonsiirtokapasiteettia aiemmin asennettuihin järjestelmiin jolloin yksittäisen kaapelin vetäminen voi olla suhteessa hyvin kallista. Edellä mainittu automaatiojärjestelmän kapasiteetin kasvattaminen on usein

myös hyvin kallista, varsinkin jos joudutaan asentamaan täysin uusia automaatiokaappeja ja kalustamaan ne. Langaton tekniikka voi tuoda tähänkin kustannussäästöjä.

- *Läpäisykyky:* Mahdollistaa asennukset hankaliinkin paikkoihin ilman kaapelinvetoa, jos käytetään akusta tai ympäristöstä energiansa saavia laitteita.
- *Kapasiteetti:* Langattoman verkon kapasiteettia on usein helpompaa ja siten myös kustannustehokkaampaa laajentaa, kuin kiinteän langoitetun verkon. Verkon peittoon voidaan vaikuttaa esimerkiksi vaihtamalla laitteiden antennit erilaisiin tai muuttamalla laitteiden asetuksia. Langoitetussa verkossa muutokset tarkoittavat useimmiten kaapelinvetoa.
- *Luotettavuus:* Langattomiin järjestelmiin voidaan rakentaa redundanttisuutta hyödyntämällä useaa vaihtoehtoista reittiä. Anturiverkot voivat reitittää liikenteen ongelmakohtien ympäri. WLAN-yhteys on mahdollista kahdentaa käyttäen 2,4GHz ja 5GHz taajuuksia samanaikaisesti. Kahdennus on usein vaatimuksena automaatiojärjestelmien kriittisimmissä osissa. Tällöin on kuitenkin huomioitava taajuuksien erilainen vaimeneminen ja eteneminen sillä yhteydet eivät ole välttämättä samanlaatuisia vaikka niiden signaalit kulkisivat samaa reittiä. Erityisesti akkukäyttöisten laitteiden tapauksessa vaihtoehtoisten tiedonsiirtoreittien toteutus on langallista vaihtoehtoa edullisempaa.
- *Huollettavuus:* Erityisesti langattomien anturiverkkojen tapauksessa yksittäisen solmun korvaaminen uudella on yksinkertainen operaatio. Itseorganisoituva verkko helpottaa tätä toimenpidettä entisestään.
- *Liikkuvuus:* Langattomat verkot mahdollistavat laitteiden, ja siten käyttäjien liikkumisen. Tieto voidaan pitää tallennettuna keskitetysti eikä työnteko ei sidottu johonkin tiettyyn työpisteeseen, tarvittavat tiedot ja dokumentaatiot ovat saatavilla missä tahansa langattoman verkon peiton alueella [36]. Tämä helpottaa tilannetta myös, jos laitteita pitää sijoittaa uudelleen esimerkiksi prosessimuutosten vuoksi.

- *Standardointi:* Erilaisia langoitettuja kenttäväylä (fieldbus) standardeja on huomattavan paljon, tähän verrattuna langattomia standardeja on vähemmän ja eri standardiperheet on suunnattu eri käyttötarkoituksiin. Yleisesti käytössä olevat avoimet standardit alentavat laitevalmistajien kynnystä tuoda uusia tuotteita markkinoille, joka alentaa hintoja kilpailun kautta. Tämä helpottaa ainakin teoriassa järjestelmän rakentamista, jos voidaan olla varmoja eri laitevalmistajien laitteiden yhteensopivuudesta. Tällöin vältytään myös ylimääräiseltä signaalien muuntamiselta.
- *Päivitettävyys:* Langattoman laitteen päivittäminen on helpompaa kuin langoitetun [73]. Parhaassa tapauksessa laite saa energiansa akusta tai ympäristöstä [46] ja uusi laite osaa liittyä suoraan osaksi valmista verkkoa vanhan laitteen tilalle. Siinäkin tapauksessa, että laite tarvitsisi virtakaapeloinnin, voidaan kaapelin kunnosta riippuen hyödyntää vanhan laitteen virtakaapelia.
- *Tuottavuus:* Langattomilla tekniikoilla voidaan tehostaa työn tuottavuutta, esimerkiksi saattamalla työntekoon tarvittava tieto helpommin työtekijöiden käyttöön kentällä. Lisäksi laitteiden ohjausta ja konfigurointia sekä tiedonkeruuta laitteista voidaan tehostaa. Lisäksi voidaan tehostaa tiedonsiirtoa kentältä esimerkiksi valvomoon tai automaatiojärjestelmään. Tästä esimerkkinä voidaan mainita langaton kameravalvonta, jolla voidaan helpottaa ja tehostaa hankalien kohteiden väliaikaista valvontaa.

3.2 Ongelmat ja haasteet

Seuraavassa on listattu langattomiin tekniikoihin liittyviä mahdollisia ongelmia ja haasteita:

- *Epävarmuus:* Langaton yhteys on käytännössä aina kaapelia epävarmempi johtuen radiotien muuttuvista olosuhteista eri ajanhetkillä. Radiotien toimivuutta on vaikea ennustaa testaamatta varsinkin, jos radioympäristö sisältää paljon erilaisia materiaaleja ja rakenteita. Tiedonsiirron toteutumisesta voidaan antaa ennalta vain

arvioita, ja käytännön toimivuus paljastuu vasta yhteyksiä testatessa. Radiotien satunnaisuus voi vaikeuttaa viive-vaatimusten täyttämistä ja järjestelmä voi olla tarpeen suunnitella huonoimman testeissä kohdatun tilanteen mukaan. Muutokset radiotiessä, kuten liikkuvat ihmiset tai esineet voivat aiheuttaa myös odottamatonta pakettien katoamista matkalla. Vaatimusten täyttämiseksi voi olla tarpeen esim. rakentaa mesh-tyyppinen verkko pakettien perillepääsyn takaamiseksi, joka monimutkaistaa myös tarvittavia verkkoprotokollia ja siten kasvattaa verkkosolmuilta vaadittavaa laskentakapasiteettia. Suurempi laskentakapasiteetti kasvattaa myös virrankulutusta, joka voi olla ongelma jos energiaa on vain rajallisesti saatavilla (WSN). Radiotien satunnaisuudesta johtuen myös pakettien saapumisajat voivat vaihdella huomattavasti, tätä kutsutaan jitteriksi. Saapumisaikojen vaihtelu johtuu pakettihukasta, törmäyksistä aiheutuvista uudelleenlähetyksistä sekä CSMA:han liittyvästä kanavalle pääsyviiveestä. Tämänkin ongelma tulee ottaa huomioon, jos langoitettuja yhteyksiä korvataan langattomilla.

- *Tietoturva:* Verrattuna kaapeloituun ratkaisuun aiheuttaa omat ongelmansa. Radioliikenne on ulkopuolisten kuunneltavissa, joka asetta tietoturvalle omat haasteensa, kun laitteiden pelkkä fyysinen turvaaminen ei enää riitä. Tietoturvaan langattomissa verkoissa perehdytään tarkemmin omassa kappaleessaan.
- *Häiriöalttius:* Langaton tiedonsiirto on altis ympäristön häiriöille. Häiriöt voivat johtua esimerkiksi muista langattomista laitteista tai sähkölaitteista joiden toiminnasta aiheutuu tietyntaajuista sähkömagneettista säteilyä. Monille jo varmasti entuudestaan tuttu esimerkki sähkölaitteiden aiheuttamasta häiriöstä ovat mikroaaltouunin WLAN-verkoille aiheuttama häiriö. Häiriö voi olla myös tahallisesti, palvelunestohyökkäys tarkoituksessa, aiheutettua.
- *Koeksistenssi (ks. kappale 2.6): S*amalla taajuusalueella toimivat eri standardien mukaiset laitteet aiheuttavat toisilleen häiriöitä. Kun käytetään samalla taajuusalueella useita eri laitteita, tulee niiden

häiriöttömään yhteistoimintaan kiinnittää huomiota. Radiokanavien käyttö tulee suunnitella siten, että kanavien päällekkäisyydet toisiaan lähellä olevien laitteiden välillä vältetään. On hyvä tiedostaa myös, että radiokanavat eivät ole täysin ortogonaalisia eli tiedonsiirto vierekkäisillä kanavilla aiheuttaa häiriötä.

- *Suunnittelu:* Langattomien järjestelmien toteuttaminen, erityisesti voimalaitosympäristössä, jossa signaalinen eteneminen on useimmiten tarpeen selvittää etukäteen testaamalla, voi vaatia huomattavan paljon suunnittelutyötä.
- *Monitie-eteneminen:* Radiosignaalien etenemistä on vaikea ennustaa voimalaitosympäristössä. Voimalaitosympäristö sisältää paljon metallisia rakenteita ja laitteita, jotka aiheuttavat radiosignaalien heijastumista. Erityisesti käytettäessä ympärisäteileviä antenneja signaali pääsee kulkemaan kahden pisteen välillä useaa reittiä. Tämä vaikeuttaa suunnittelua, sillä signaalin etenemistä on vaikea ennustaa ilman testausta. Jos sovellus mahdollistaa suunta-antennien käytön, on tämä varsin suositeltavaa. Suunta-antenneilla voidaan rajoittaa signaalin heijastumista kohdistamalla se suoraan vastaanottajaan.
- *Spektrinhallinta:* Koska käytössä on vain rajallinen taajuusalue, tulee myös spektrin käyttö suunnitella tarkasti. Laitteiden määrän kasvaessa tähän ongelmaan voidaan törmätä hyvin nopeasti.
- *Elinkaari:* Langattomien laitteiden elinkaari ei tekniikan nopean kehityksen vuoksi välttämättä ole yhtä pitkä kuin muilla teollisuuden laitteilla. Tämä asia tulee tiedostaa laitteita hankittaessa ja esimerkiksi laskettaessa mahdollista takaisinmaksuaikaa.
- *Standardointi:* Standardointitilanne on hieman parempi kuin langoitettujen kenttäväylien kohdalla, mutta ei kuitenkaan täysin ideaalinen jolloin jokaiseen käyttötarkoitukseen olisi yksi standardi, jota kaikki valmistajat noudattaisivat. Samaan käyttötarkoitukseen suunnattuja standardeja ovat esimerkiksi ISA100.11a [12] ja WirelessHART [11] perustuvat samaan 802.15.4-perusstandardiin, mutta eivät ole yhteensopivia keskenään.

4. Helsingin Energian Salmisaaren laitokset

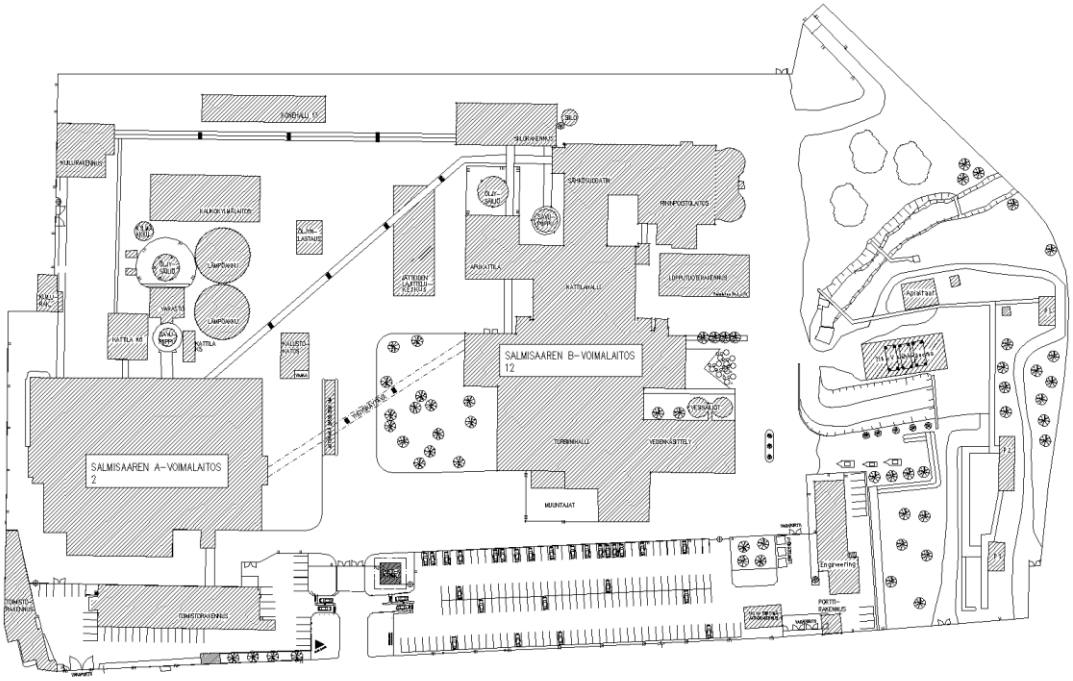
Tässä kappaleessa perehdytään Salmisaaren voimalaitosalueeseen, jossa työn kokeellinen osa suoritettiin. Tarkoituksena on antaa käsitys siitä, minkälainen ympäristö alue on erityisesti langattoman tiedonsiirron kannalta.

4.1 Yleisesti voimalaitoksista

Työssä keskitytään Helsingin Energian Salmisaaren laitoksille, mutta suurin osa selvitetyistä asioista on sovellettavissa myös muille Helsingin Energian laitoksille. Salmisaaren kivihiilivoimalaitos aloitti toimintansa 1953 ja nykyään päätuotantoyksikkönä toimiva Salmisaari B valmistui 1984. Salmisaaren voimalaitosalueilla sijaitsevat nykyään Salmisaaren A-voimalaitos ja Salmisaaren B-voimalaitos, rikinpoistolaitos, omakäyttöhöyrykattila K5, kaukolämpökattila K6, Kellosaaren kaasuturbiinilaitos, kaukojäähdytyslaitos, 2 lämpöakkua, Tammasaaren (Kellosaaren) hiilisatama, maanalainen hiilivarasto, maanalainen sähköasema, maanalainen kaukojäähdytyslaitos, maanalaiset raskas- ja kevytöljyvarastot sekä toimisto-, korjaamo- ja varastorakennukset. Laitosalueelta lähtevissä kaukolämpötunneleissa siirretään lämpöä sekä kantakaupungin että Lauttasaaren suuntiin. Voimalaitosalueen layout selviää kuvasta 7, tässä kuvassa ei näy Kellosaaren voimalaitosta tai hiilisatamaa.

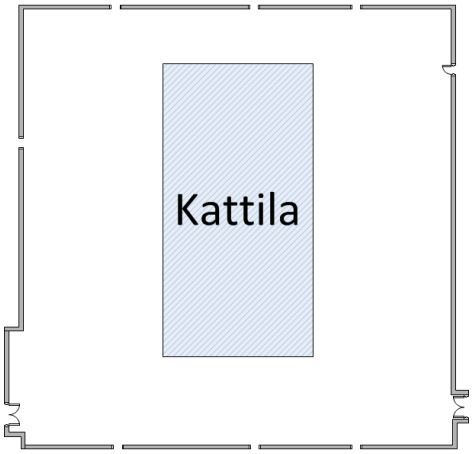
Salmisaaren voimalaitoksilla tuotetaan yhteistuotantona sähköä, kaukolämpöä ja kaukojäähdytystä. Tuotanto tapahtuu polttamalla kattilassa hiilipölyä, jolla kuumennetaan turbiinia pyörittävää höyryä. Höyryä käytetään tämän lisäksi kaukolämpöveden lämmittämiseen kaukolämmönvaihtimissa. Laitoksella aloitetaan pellettien poltto kivihiilen seassa vuonna 2014, joka

asettaa omat tekniset ja logistiset haasteensa.



Kuva 7, Salmisaaren voimalaitosalue

4.2 Prosessitila



Kuva 8, Salmisaari B voimalaitos, kattilahallin ylemmät kerrokset

Prosessitilalla tarkoitetaan tiloja, joihin on sijoitettu voimalaitosprosessiin liittyvät laitteet. Näitä tiloja ovat esimerkiksi kattilahalli, turbiinisali ja rikinpoistolaitos. Helsingin Energian Salmisaaren B-voimalaitoksen kattilahallin layout ilmenee kuvasta 8. Kyseessä monikerroksinen halli, joka on jaettu korkeussuunnassa n. 3m välein olevilla ritilätasoilla. Ritilätasot on valmistettu metallista ja ritilän aukot ovat kooltaan n. 2x6cm. Tasot kiertävät lähes koko hallin korkuista kattilaa. Hallin seinät ovat ylimmissä kerroksissa metallipintaiset joka sivulta ja alemmissa kerroksissa osa seinistä on betonia. Kuvasta selviävät vain hallin mittasuhteet, kattilan ympärillä on kerroksesta riippuen erilaisia esteitä.

Erilaiset putkistot ja kanavat voivat kulkea useamman kerroksen läpi eli ritilätasot eivät peitä kaikkea kattilalta vapaaksi jäänyttä tilaa. Tasoissa on myös aukkoja esimerkiksi tavarankuljetusta varten. Kuvissa 9 ja 10 on näkymät kuvassa 8 vasemmassa ja oikeassa alakulmassa näkyviltä ovilta.

Kuva 9, SaB kattilahalli

Kuva 10, SaB kattilahalli

Edellä on perehdytty yksityiskohtaisesti vain kattilahalliin, sillä tarkoituksena ei ole niinkään kuvata jokaisen tilan kaikkia yksityiskohtia, vaan antaa yleiskäsitys prosessitilasta. Esimerkiksi rikinpoistolaitos on tilana varsin samanlainen, joskin vapaata ilmatilaa on paikoitellen huomattavasti vähemmän. Kuten aiemmin mainittiin, parhaan mahdollisen radiotien saavuttamiseksi tulisi Fresnelin-alueen [27] olla mahdollisimman tyhjä, eli vapaata tilaa pitäisi olla riittävästi. Toinen varsin oleellinen erottava tekijä radiosignaalin etenemisen kannalta on seinien rakennusmateriaali, jonka suhteen esimerkiksi turbiinisali eroaa kattilahallista. Turbiinisalin seinät eivät ole metallia vaan tiiltä, joka ei heijasta radioaaltoja metallin tavoin. Tällä voi olla huomattava vaikutus radiosignaalin monitie-etenemiseen, sillä signaali ei heijastu tiiliseinästä läheskään yhtä voimakkaasti kuin metallista. Jos signaali ei heijastu, vaan kulkee väliaineen läpi, tapahtuu signaalin vaimenemista. Vaimeneminen on riippuvainen väliaineesta ja signaalin taajuudesta [26]. Jos radiosignaalin tielle sattuu jokin sopiva teräväreunainen esine, voi sopiva osuma esineen reunaan aiheuttaa signaalille suunnanmuutoksen [28].

Prosessitiloissa voi liikkua esimerkiksi laitoksen henkilökuntaa suorittamassa huoltotoimenpiteitä. Tilanteesta riippuen voi olla myös tarpeen kuljettaa varaosia vikaantuneille laitteille. Nämä tekijät voivat aiheuttaa häipymistä radiokanavassa. Vähintäänkin kannattaa tukiasemien sijoittelussa ottaa huomioon usein käytetyt kulkuväylät, jotta häipyminen saadaan minimoitua. Voimalaitoksen prosessin kehitys saattaa myös aiheuttaa muutoksia radioympäristöön. Esimerkiksi uudet putkistot voivat muuttaa radioympäristöä tai pahimmassa tapauksessa jopa katkaista kahden pisteen välillä olevan yhteyden. Langattomien järjestelmien ylläpitäjän tuleekin olla tietoinen tiloihin tehtävistä muutoksista ja varauduttava niiden aiheuttamiin ongelmiin.

Voimalaitosprosessi tuottaa hukkalämpöä prosessitiloihin, joka nostaa ympäristön lämpötilan tavallista huonelämpötilaa korkeammaksi. Lähellä esimerkiksi kattilaa tai putkistoja, joissa kuljetetaan kuumaa ainesta voi lämpötila nousta hyvinkin korkeaksi.

Toimistotiloissa kuuntelutilaan asetettu langaton USB-verkkosovitin havaitsi LinSSID-ohjelmalla [74] n. viikon tarkkailun aikana yhteensä 218 kpl langattomia WLAN-verkkoja 2,4 Hz taajuusalueella. Tämä ei suoranaisesti vaikuta prosessitilaan, mutta piha-alueella tällaiset häiriötekijät on otettava huomioon. Verkkojen lukumäärä saattaa kuulostaa suurelta, mutta on otettava huomioon, että verkkojen SSID-tunnusten voidaan päätellä suuren osan olevan ohikulkevia matkapuhelimia, joissa on käytössä tukiasema-tila. Tukiasema-tilassa matkapuhelin toimii WLAN-tukiasemana, joka mahdollistaa puhelimen Internet-yhteyden jakamisen muille laitteille, esimerkiksi kannettavalle tietokoneelle, langattomasti. Myöhemmissä testeissä havaittiin joidenkin lähistöllä olevien WLAN-tukiasemien kuuluvan alhaisella signaalinvoimakkuudella myös prosessitiloihin erityisesti ikkunoiden läheisyydessä.

4.3 Voimalaitosautomaatio ja tiedonsiirtoverkot

Voimalaitosympäristössä automaatiojärjestelmiä käytetään ohjaamaan energiantuotantoprosessia. Yksinkertaisesti ilmaistuna automaatiojärjestelmä kerää tietoa prosessista, jonka perusteella prosessin toimintaa säädetään. Käytännössä kyseessä on hyvin monimutkainen järjestelmä, jossa tietoa kerätään tuhansista mittapisteistä, joiden perusteella säädöt tehdään. Tavoitteena prosessin automatisoinnissa on yleensä tuotannon tehostaminen vähentämällä tarvittavaa työmäärää sekä parempi tiedonkeruu ja -hallinta. Voimalaitosta ohjataan ja tarkkaillaan valvomosta, jonne tuodaan oleellinen mittaustieto ja asetetaan halutut arvot prosessille. Automaatiojärjestelmä tekee tarvittavat säädöt tavoitearvojen saavuttamiseksi. Prosessiohjauksen lisäksi automaatiota hyödynnetään turvallisuuteen liittyvissä järjestelmissä (TLJ). Nämä järjestelmät on erotettu käyttöautomaatiosta ja niiden tehtävä on häiriö- tai vaaratilanteessa pysäyttää prosessi tai laite ja ohjata se turvalliseen tilaan. Järjestelmien toimintavarmuuden tulee olla erittäin korkealla tasolla. Tiukat varmuusvaatimukset rajoittavat tai jopa estävät langattoman tiedonsiirron hyödyntämisen näissä järjestelmissä.

Tuotantoprosessia ohjaavan pääautomaatiojärjestelmän lisäksi käytössä voi olla erillisiä osajärjestelmiä. Näiden järjestelmien tehtävänä voi olla ohjata jotakin osaa prosessista tai ohjata jotakin prosessia tukevaa järjestelmää. Lisäksi käytössä voi olla kiinteistöautomaatiojärjestelmiä, joita käytetään esimerkiksi kulunvalvontaan ja ilmanvaihdon ohjaukseen.

Perinteisesti tieto mittalaitteilta on siirretty automaatiojärjestelmään joko suoraan langoitettuna analogi- tai digitaalisignaalina tai käyttäen jotakin kenttäväylää. Nykyisin on kuitenkin mahdollista siirtää mittaus- ja ohjaustietoa myös langattomasti [11] [12] käyttäen esimerkiksi langatonta anturiverkkoa [9], tätä kautta myös automaatiojärjestelmät sisältyvät ainakin yleisellä tasolla myös tämän työn laajuuteen.

Voimalaitosalueen kaksi tärkeintä langallista tiedonsiirtoverkkoa ovat prosessitiedonsiirtoon tarkoitettu kuituverkko sekä toimistolaitteille tarkoitettu toimistoverkko. Näiden lisäksi langallista tiedonsiirtoa tapahtuu automaatiojärjestelmän ja kenttälaitteiden välillä. Toteutuksesta ja laitteesta riippuen tietoa voidaan tuoda suoraan erikseen langoitettuna tai kenttäväylää käyttäen.

Prosessitiedonsiirtoon tarkoitettu tiedonsiirtoverkko, ProLAN, on mahdollisimman toimintavarmaksi suunniteltu valokuituverkko[75]. Verkko on fyysisesti toteutettu kahdennetulla kuiturengasverkolla. Verkon tavoitteena on tarjota varmaa tiedonsiirtoa sekä prosessiautomaatiojärjestelmille, että eri toimipisteiden välille. Verkon suunnittelussa on myös huomioitu prosessijärjestelmien asettamat tietoturvavaatimukset hajauttamalla järjestelmät omiin kokonaisuuksiinsa ja eriyttämällä käyttäjien pääsy näihin järjestelmiin. Tällaista lähestymistapaa syvyyssuuntaiseksi puolustusstrategiaksi (defense-in-depth). Liitännät sekä prosessi-, että toimistoverkkoon tapahtuvat helpoiten kaapelitiloihin sijoitetuissa liitäntäpisteissä. Tämä on hyvä tiedostaa mahdollisia kaapelointeja suunniteltaessa.

Langallisten verkkojen lisäksi voimalaitos alueella on tiettyihin neuvottelutiloihin asennettu 2,4GHz-taajuusalueella toimivia WLAN-vieralijaverkkoja. Riippuen tilojen sijainnista voidaan nämä verkot havaita myös prosessitiloissa esimerkiksi ikkunoiden kohdalla. Vaikka tällä hetkellä WLAN-verkkoja on vain muutamissa neuvottelutiloissa, on todennäköistä että verkkoja tulla ottamaan käyttöön tulevaisuudessa yhä enemmän. Prosessitilojen paksuhkot seinät sekä metalliset ovet rajoittavat jossain määrin ulkopuolisten verkkojen signaalien kuulumista, mutta WLAN-verkkojen laajennukset on kuitenkin otettava huomioon. Tässä yhteydessä on hyvä tiedostaa, että laajennusta voi tapahtua myös prosessitiloissa toimivaksi havaitulla 5GHz-taajuusalueella. Automaatiojärjestelmissä Salmisaaren voimalaitoksilla tällä hetkellä ainoa langaton tiedonsiirtoyhteys on yksittäinen WirelessHART-linkki A-voimalaitoksen katolta meren rannassa sijaitsevaan merivesikanavaan. Vuosaaren voimalaitoksilla on käytössä 2,4GHz-taajuusaluella toimivia Bluetooth yhteydellä varustettuja säätö- ja sulkutoimilaitteita. Yhteyttä voidaan käyttää laitteiden parametrien lukemiseen ja kirjoittamiseen.

5. Tietoturva

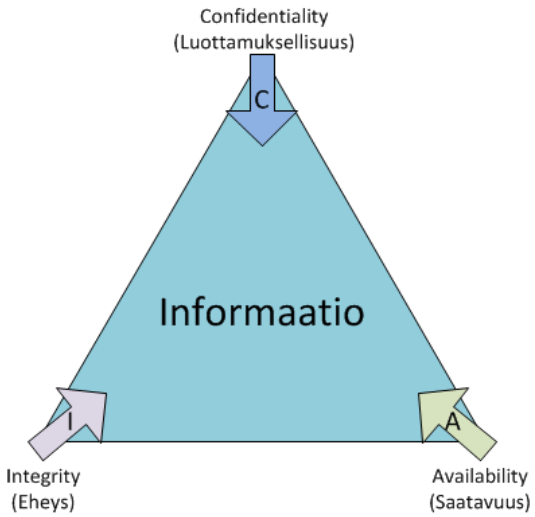
Tässä kappaleessa perehdytään tietoturvaan aluksi hieman yleisellä tasolla ja tämän jälkeen langattomien järjestelmien näkökulmasta. Tavoitteena on selvittää miten tietoturvan eri osa-alueet on otettu huomioon langattomissa järjestelmissä ja millä osa-alueilla on vielä mahdollisia ongelmia tai puutteita.

Tietoturvan perusajatus on tiedon eheyden, saatavuuden ja luottamuksellisuuden varmistamista. Tietoturva onkin nykyisin äärimmäisen tärkeä osa minkä tahansa tietojärjestelmän toteutusta [76]. Puutteellinen tietoturva voi altistaa järjestelmän ja sen käyttäjät vaaroille, jolla voi olla pahimmassa tapauksessa terveys-, turvallisuus tai ympäristöseuraamuksia (health, safety, environment, HSE) [77]. Tietoturvaa tarkasteltaessa on hyvä tiedostaa, että mikä tahansa järjestelmä on teoriassa mahdollista tehdä täysin tietoturvalliseksi, mutta tällöin järjestelmän saatavuus ja käytettävyys kärsivät huomattavasti. Tietoturvassa onkin pitkälle kyse tasapainon löytämisestä käytettävyyden ja turvallisuuden välillä sekä riskien järkevästä hallinnasta.

Tietoturva nähdään yhtenä tärkeimmistä haasteista langattomalle automaatiolle [78]. Tässä työssä perehdytäänkin teollisuuden tietoturvaan sekä perinteisen CIA-mallin, että IEC 62443-2-1-standardin [77] määrittelemän tietoturvajärjestelmän pohjalta. Vanhemmissa järjestelmissä tietoturva on perustunut lähinnä järjestelmän toiminnan salassapitoon (security through obscurity), eli olettamus on, että hyökkääjät eivät tunne kohdejärjestelmää ja tämän takia hyökkäys epäonnistuu [79].

Kehittyvä tekniikka parantaa tietoturvan teknistä puolta, mikä voi aiheuttaa hyökkäysten kohdistumista yhä enemmän käyttäjiin. Sosiaalisella manipulaatiolla (social engineering) [80] voidaan käyttäjät saada paljastamaan hakkerille oleellisia tietoja järjestelmästä tai tekemään jotakin joka vaarantaa järjestelmän tietoturvan. Hyvän teknisen tietoturvan lisäksi on siis varauduttava myös ihmisiin kohdistuviin tietoturvauhkiin. Tärkeässä roolissa tässä on käyttäjien koulutus ymmärtämään oma roolinsa osana järjestelmän tietoturvaa.

5.1 CIA-malli ja tietoturvajärjestelmä



Kuva 11, CIA-malli

CIA-malli [81], kuva 7, on tietoturvassa yleisesti käytetty konsepti, jonkin järjestelmän tietoturvan tarkasteluun. Mallissa jonkin informaation tietoturvaa tarkastellaan kolmen päätekijän suhteen. Nämä päätekijät, joista malli myös saa nimensä, ovat **C**onfidentiality eli Luottamuksellisuus, **I**ntegrity eli Eheys ja **A**vailability eli Saatavuus.

Pääpiirteittäin tekijöillä tarkoitetaan seuraavaa:

- *Luottamuksellisuudella* hallitaan sitä, että tieto pysyy salassa sellaisilta tahoilta, joille ei ole erikseen sallittu pääsyä kyseiseen tietoon. Luottamuksellisuus voidaan saavuttaa salaamalla tieto sitä siirrettäessä ja rajoittamalla pääsy tietoon vain tiettyihin sijainteihin tai tietyille käyttäjille. Pääsy voidaan rajoittaa esimerkiksi käyttämällä käyttäjä tunnuksia ja salasanoja. Esimerkiksi WLAN-verkoissa luottamuksellisuus voidaan saavuttaa salaamalla liikenne siten, että kommunikointi onnistuu vain, jos käyttäjällä on hallussaan tarvittava salasana.
- *Eheys* varmistaa, että tietoa ei voi muuttaa ilman riittäviä oikeuksia ja, että tieto ei pääse itsestään korruptoitumaan kenenkään huomaamatta. Eheyden varmistamiseen liittyy oleellisesti myös korruptoituneen tiedon korjaaminen tai esimerkiksi palauttaminen varmuuskopioista. Varmuuskopioinnin lisäksi eheydestä voidaan huolehtia tietoliikenne pakettien tai tiedostojen tarkistussummilla.

- *Saatavuudella* tarkoitetaan, että tiedon tulee olla helposti tietoon oikeutettujen tahojen saatavilla silloin kun sitä tarvitaan. Tällä tarkoitetaan, että tietoa suojaavien mekanismien ei tule kohtuuttomasti vaikeuttaa tietoon käsiksi pääsemistä. Vaatimus koskettaa sekä pääsyä rajoittavien järjestelmien suunnittelua, että koko järjestelmän suojausta esimerkiksi palvelunestohyökkäyksiä vastaan. Järjestelmä tulee suunnitella siten, että siinä on riittävä määrä redundanttisuutta sekä ylimääräistä kapasiteettia. Tämän lisäksi voidaan käyttää esimerkiksi palomuuria, joka kykenee suojelemaan palvelunestohyökkäykseltä. Saatavuudella arvioidaan myös kuinka helposti taho, jolla on riittävät käyttöoikeudet, pääsee käsiksi tietoon. Tällä arvioidaan siis kuinka hyvin tietoturva ja käytettävyys ovat tasapainossa keskenään. Pahimmassa tapauksessa liian aggressiiviset tietoturvajärjestelmät voivat vaikeuttaa tiedon hyödyntämistä yhtä pahasti kuin jokin ulkopuolinen hyökkäys.

CIA-mallia voidaan laajentaa sisällyttämällä siihen vielä tiedonsiirtoon osallistuvien tahojen todentaminen (authentication) sekä vastuuvelvollisuus (accountability) [81]. Todentaminen tarkoittaa tiedonsiirron osapuolten varmistumista toisen osapuolen olevan sitä mitä nämä väittävät. Vastuuvelvollisuus on vaatimus siitä, että kaikki toimenpiteet voidaan jäljittää takaisin suorittajaansa. Mallia laajennuksineen tullaan käyttämään tässä työssä pohjana tietoturvan arviointiin eri langattomissa sovelluksissa.

CIA-malli soveltuu tietoturvan arviointiin, lisäksi on tarpeen luoda jonkinlainen malli, jolla tietoturvaa hallitaan ja kehitetään käytännössä. Tällainen malli on yleensä osa yleisempää organisaation tietoturvapolitiikkaa. Tämänkaltainen politiikka on käytössä myös nyt tarkastelun kohteena olevassa organisaatiossa, lisäksi hankintoihin sovelletaan omaa vaatimuslistaa. Jos valmista mallia ei vielä ole, voidaan sen luomiseen soveltaa IEC 62443-2-1-standardia. Standardi määrittelee tietoturvan hallintajärjestelmään tarvittavat osat, ja antaa ohjeita jokaisen osa-alueen toteutukseen. Jakamalla tietoturvan asettama haaste pienempiin osa-alueisiin voidaan sen hallintaa

yksinkertaistaa. On hyvä huomata, että jako ei tapahdu siten, että eri osajärjestelmiä käsiteltäisiin itsenäisesti. Eri osa-alueet koskettavat kaikkia järjestelmiä. Standardin määrittelemä tietoturvajärjestelmä koostuu seuraavista osa-alueesta: *riskianalyysi*, *riskin käsittely* sekä *tietoturvajärjestelmän seuranta ja parantaminen*.

- Riskiarvioinnin tavoitteena on luokitella mahdolliset riskit ja selvittää minkälaisia tietoja mahdollinen tietomurto voi paljastaa sekä mitä ongelmia tiedonsiirtojärjestelmien toimimattomuus voi aiheuttaa. Riskiarvioinnin perusteella voidaan määritellä kunkin järjestelmän suojaustaso. Tässä kerätyn tiedon perusteella kehitetään järjestelmien muita osa-alueita. Olennainen osa riskianalyysia on löytää liiketoimintaperustelu tietototekniikan hyödyntämiselle teollisuusjärjestelmissä. Liiketoimintaperusteluun sisältyy arvio mahdollisista uhista, vaikutuksista liiketoimintaan sekä kustannuksista.
- Riskin käsittely tarjoaa ohjeita sopivan tietoturvaorganisaation luomiseen sisältäen henkilöstön, tietoturvapolitiikan ja tarvittavat suunnitelmat. Lisäksi tähän sisältyy määrittely tarvittavista toimenpiteistä tietoturvan takaamiseksi, kuten verkon suunnittelu, pääsyn- ja käyttäjienhallinta sekä yleinen henkilöstöön liittyvä tietoturva. Viimeinen osa riskien käsittelyä on itse toteutus, johon sisältyy riskien hallinnan toteutus, järjestelmän ylläpito, tiedonhallintaan liittyvät prosessit sekä häiriötilanteisiin varautuminen ja reagointi. Tässä kohdassa erityisen tärkeäksi tekijä on hyvin koulutettu henkilökunta, joka ymmärtää oman vastuunsa tietoturvan suhteen. Työn toteuttajina heillä onkin lopullinen vastuu tietoturvallisesta toiminnasta.
- Tietoturvajärjestelmän seurannalla ja parantamisella määritellään prosessit sekä järjestelmän noudattamisen valvontaan, että yleisesti järjestelmän katselmointiin, parantamiseen ja ylläpitoon.

On hyvä tiedostaa, että standardi ei suoraan määrittele tietoturvajärjestelmän toteutusta, vaan sen on tarkoitus luoda viitekehys, jonka pohjalta tietoturvajärjestelmä voidaan sovittaa kuhunkin sovellukseen.

Helsingin Energialla onkin edelliseen liittyen käytössä kattava määrittely tietoturvavaatimuksista, jota käytetään osana automaatiohankintoja. Nämä perustuvat COREQ-VE [82] vaatimusmäärittelyyn, joka on VTT:n, Huoltovarmuuskeskuksen ja CERT-FI:n yhteistyössä kehittämä tietoturvavaatimuskanta. Näiden vaatimusten perusteella pitäisi olla mahdollista toteuttaa automaatiojärjestelmiin liittyviä projekteja tietoturvallisesti.

5.2 Tietoturva langattomissa verkoissa

Verrattuna perinteiseen langalliseen verkkoon, langattoman verkon tietoturvaan liittyvät kysymykset ovat monella tavalla erilaisia. Tämä johtuu langattomien verkkojen avoimesta luonteesta. Langattomat verkot ja niissä tapahtuva tiedonsiirto ovat kenen tahansa sopivalla laitteistolla kuuntelevan havaittavissa sillä olettamuksella, että kuuntelija sijaitsee lähettävän langattoman aseman kantaman sisällä. Perinteisessä langallisessa tiedonsiirrossa tämä vastaisi periaatteessa sitä, että jonkin kolmas osapuoli pääsisi asentamaan oman kuuntelulaitteensa johonkin osaan verkkoa siten, että sitä ei voida verkon ylläpidon toimesta havaita. On hyvä myös muistaa, että toisin kuin langallisessa verkossa, laitteiden fyysinen paikantaminen on vaikeampaa. Nykyaikainen salaustekniikka tekee kuitenkin radioliikenteen sisällön paljastamisesta vaikeaa. Tämä nostaakin erilaiset palvelunestohyökkäykset merkittävimmäksi uhaksi langattomia järjestelmiä vastaan [30]. Erilaisista teknisistä tekijöistä huolimatta tietoturvaan voidaan perehtyä yleisellä tasolla samojen perusperiaatteiden kannalta, kuin langallisissakin järjestelmissä.

Langattomat verkot, toisin kuin langalliset, siirtävät tietoa avoimessa siirtotiessä. Tämä tarkoittaa, että siirrettävä tieto tulee suojata jollain keinolla

sen luottamuksellisuuden varmistamiseksi. Langattomissa verkoissa luottamuksellisuus saavutetaan salaamalla tieto jollakin salausalgoritmilla [30] [17]. Langallisen verkon tapaan tiedon eheys varmistetaan käyttämällä tarkistussummia. Isoin haaste langattoman tiedonsiirron tietoturvassa onkin saatavuuden varmistaminen. Erilaiset palvelunestohyökkäykset voivat haitata tai estää tiedonsiirron tämä korostaa fyysisen turvallisuuden merkitystä. Fyysisellä turvallisuudella rajoitetaan hyökkääjien mahdollisuuksia vaikuttaa tiedonsiirtoon. Käyttämällä riittävän tehokasta radiolaitteistoa voidaan hyökkäys toteuttaa pitkänkin etäisyyden päästä. Jos hyökkääjällä on yleinen käsitys esimerkiksi tukiaseman sijainnista, on tämän mahdollista lähettää voimakas radiosignaali kohti tukiasemaa. Tällöin tukiasema ja siihen yhteydessä olevat asemat eivät voi käyttää radiotietä omaan tiedonsiirtoonsa ja verkon toiminta häiriintyy. Tällainen hyökkäys ei vaadi langattoman verkon sijainnin lisäksi muuta tietoa kuin taajuusalueen, jolla verkko toimii. Riittävällä fyysisellä turvallisuudella voidaan lisätä minimietäisyyttä, jolle hyökkääjä voi päästä kohteestaan. Etäisyyden kasvaessa tarvitaan suurempaa lähetystehoa signaalin vaimenemisen välttämiseksi. Kun hyökkäykseen vaaditaan monimutkainen laitteisto ja suuri lähetysteho, on sen havaitseminen sekä fyysisesti, että radiotietä tarkkailemalla helppoa. Pääsy voimalaitosalueella on jo lähtökohtaisesti rajoitettu ja alueella on ympärivuorokautinen valvonta, tämä vaikeuttaa myös radiohäirinnän suorittamista. Jos voimalaitos sijaitsee kaupunkialueella, ei sen ympärillä oleva tyhjä tila kuitenkaan voi olla kovinkaan suuri tilankäytöllisistä syistä. Tällöin hyökkääjän on helpompi päästä lähelle laitosta, myös suuri määrä ohikulkevia ihmisiä ja liikennettä voi helpottaa hyökkääjää pysymään havaitsemattomissa.

Lisähuomiona voidaan mainita langattomien järjestelmien eristäminen kriittisistä järjestelmistä. Erityisesti automaatiojärjestelmien yhteydessä on tärkeää, että mahdollinen tietoturvan pettäminen ei aiheuta koko järjestelmän lamaantumista. Hyökkäyksen vaikutukset pitää pystyä rajoittamaan mahdollisimman pienelle alueelle ja järjestelmän tulee olla siinä määrin vikasietoinen, että jonkin osa-alueen toimimattomuus ei ole ongelma [83].

Tämä korostuu tapauksissa, joissa järjestelmiin lisätään langatonta tiedonsiirtoa. Langattoman tiedonsiirron yleistyessäkin kriittisimmät järjestelmät tulisi edelleen erottaa mahdollisimman pitkälle ulkopuolisista verkoista ja pyrkiä pitämään niiden hyökkäyspinta-ala mahdollisimman pienenä.

Laajalti uutisoitu Iranin ydinohjelman ohjelmoitaviin logiikoihin kohdistunut Stuxnet [84] [85] [86]-hyökkäys on nostanut uusia kysymyksiä liittyen teolliseen tietoturvaan ja tietoturvapolitiikkaan. Hyökkäys on tuonut esille aivan uudenlaisen vaaran tietoturvaan liittyen. Kyseessä on ns. edistynyt jatkuva uhka (Advanced Persistent Threat, ATP), joka soluttautuu järjestelmään aiheuttaakseen kohteena olevalle organisaatiolle jonkinlaista haittaa pitkällä aikavälillä. Tällainen uhka korostaa tarvetta varmistaa tietoturvan toimivuutta myös järjestelmän asennuksen jälkeen sekä mahdollisen hyökkäyspinta-alan pienentämistä. Uhan torjumiseen ja havaitsemiseen tarvitaan riittävän edistyneitä hyökkäyksenesto- (Intrusion Prevention System) ja havaitsemisjärjestelmiä (Intrusion Detection System). Hyökkäyspinta-alaan liittyen Aalto-yliopisto on tutkimuksen verkkoon liitetyistä avoimista automaatiolaitteista [87], joka tilanteessa olevan vielä parantamisen varaa monien organisaatioiden kohdalla. Onkin muistettava, että myös langattomat verkot kasvattavat hyökkäyspinta-alaa, eli niitä hyödyntäessä tulee varmistua tietoturvan riittävästä tasosta.

Stuxnet ja edistyneet jatkuvat uhat yleisesti nostava esille kysymyksen hyökkäysten motivaatiosta ja hyökkääjistä yleensä. On selvä, että tällaisen hyökkäyksen toteuttaminen vaatii huomattavia resursseja ja siten myös riittävän syyn. Eli on epätodennäköistä, että hyökkäyksen taustalla on perinteisesti hakkeriksi miellettäviä yksityishenkilöitä ilman selkeää motiivia. Mahdolliset hyökkääjät/uhat voidaan luokitella kykyjen, käytössä olevien resurssien ja motiivien perusteella seuraavasti [88]:

- **Kansallisvaltiot** kykenevät pitkäaikaiseen ja laajamittaiseen toimintaan sillä niillä on käytössään laaja henkilöstö ja rahalliset resurssit. Toiminta on pääasiassa sotilaallista tai vakoilua hyödyntäen

uusinta ja edistyneintä tekniikkaa. Toiminta on mahdollista poliittisen oikeutuksen sekä vahvan salassapidon kautta. Valtioiden motiivina on tiedonkeruu muiden valtioiden, mahdollisten terroristien tai rikollisten toimista sekä halu pysyä mahdollisten vihollisten kehityksen mukana. Valtioilla on käytössään laajin valikoima hyökkäystekniikoita.

- **Terroristit** käyttävät terroritekoja poliittisina mielenilmauksina tai välineenä poliittiseen muutokseen. Terroristeille verkkorikollisuus on tähän mennessä ollut lähinnä julkisuus- ja rahankeruutyökalu. Resurssit ja taidot hyökkäysten toteuttamiseen ovat rajalliset, mutta uuden terroristisukupolven kehittyessä voi tilanteeseen tulla muutos. On myös mahdollista, että kansallisvaltiot tukevat terroristiryhmien toimintaa tavoitteena vahingon aiheuttaminen yhteisille vihollisille. Vaikka onnistuneita hyökkäyksiä ei tähän mennessä ole tapahtunut, voidaan potentiaalisiksi kohteiksi laskea kriittisen infrastruktuurin osat niihin kohdistuvien hyökkäysten näkyvyyden vuoksi.
- **Rikollisjärjestöt** toimivat voittoa tavoitellen, eli verkkorikollisuutta käytetään tulonlähteenä ja edistämään muuta rikollista toimintaa. Kykyä tai halua ei välttämättä ole kehittää edistyneitä hyökkäyksiä, jotka voisivat vaarantaa kriittisen infrastruktuurin järjestelmiä. Rikollisjärjestöt ovat osoittautuneet haittaohjelmien ja bottiverkkojen aktiivisiksi käyttäjiksi.
- **Tyytymätön sisäpiiriläinen** ei ole riskinä samalla tavalla jatkuva kuin edellä mainitut, mutta vahinkopotentiaali on huomattava. Hyödyntämällä järjestelmien tuntemusta ja käyttöoikeuksiaan sisäpiiriläinen voi vaarantaa järjestelmän joko suoraan tai paljastamalla tietoja jollekin kolmannelle osapuolelle. Motivaatio tällaiselle toiminnalle vaihtelee tapauskohtaisesti, vaaran tunnistaminen ja ennaltaehkäiseminen edellyttää lähimmiltä esimiehiltä ja koko organisaatiolta tarkkaavaisuutta mahdollisten ongelmien havaitsemiseen jo etukäteen.
- **Haktivistit** on terminä yhdistelmä sanoista ja hakkeri ja aktivisti. Kyseessä on suhteellisen uusi ilmiö ja se on lähimpänä perinteistä

käsitystä hakkereista. Tämä ryhmä käsittää laajan kirjon ihmisiä ja siten sekä motivaatiot, että kyvyt vaihtelevat eri yksilöiden välillä suuresti. Yleisesti tavoitteena on saada aikaan muutosta yhteiskunnassa hyödyntäen tietoteknisiä apuvälineitä lain rajojen molemmin puolin. Toiminnan kohteena ovat usein helpot kohteet kuten järjestelmät, jotka sisältävät jonkin tunnetun haavoittuvuuden tai organisaatiot, joiden tietoturvakäytännöt ovat riittämättömiä. Kriittiseen infrastruktuuriin liittyvät järjestelmät eivät yleensä ole tällaisia helppoja kohteita ja tähän mennessä haktivistit eivät ole toteuttaneet niihin kohdistuneita onnistuneita hyökkäyksiä.

5.3 WLAN tietoturva

WLAN-verkkojen tietoturva on kehittynyt ajan myötä huomattavan paljon. Tämä onkin ollut tarpeen ensimmäisten tietoturvaratkaisuiden osoittautuessa riittämättömiksi. Standardin ensimmäisessä versiossa käytössä ollut WEP (Wired Equivalent Privacy) salaustekniikka oli murrettavissa siitä löytyneiden haavoittuvaisuuksien vuoksi. Ongelmaa korjaamaan aloitettiin 802.11i-standardin kehitystyö. Jo ennen standardin valmistumista tarjolle tuli standardin osin implementoiva WPA (Wi-Fi Protected Access)-standardi väliaikaisratkaisuksi huonoon tietoturvatilanteeseen. Tällä hetkellä käytössä oleva, standardin viimeisin versio, tunnetaan nimellä WPA2 (Wi-Fi Protected Access II). Se tarjoaa päivitetyt ratkaisut salaukseen, todennukseen, avaintenhallintaan ja eheydenvarmistukseen.

WPA2:ssa todentaminen voidaan hoitaa ennalta jaetulla avaimella (pre-shared key, PSK), jolloin avaimen muuttuessa muutokset tulee tehdä kaikkiin laitteisiin erikseen. Toinen vaihtoehto on hyödyntää myös Ethernet-verkoista tuttua 802.1X todennusta, jossa verkkoon lisätään todennuksesta vastaava taho esimerkiksi RADIUS (Remote Authentication Dial In User Service)-palvelin. Salauksesta ja eheydestä vastaa CCMP-protokolla. Salaukseen käytetään AES (Advanced Encryption Stadard)-algoritmia ja eheydestä MIC-

tarkistussumma. Näillä menetelmillä voidaan varmistua WLAN-verkon eheydestä ja luottamuksellisuudesta ulkopuolisia hyökkääjiä vastaan.

Vaikka WPA2:n salauksessa ei kirjoitushetkellä ole mitään tunnettuja, helposti hyväksikäytettäviä, haavoittuvaisuuksia tulee avaimeksi valita riittävän pitkä ja monimutkainen merkkijono. Yksinkertainen salasana voi teoriassa paljastua väsytystekniikalla. Hyökkääjä voi pyrkiä löytämään salasanan kaappaamalla tunnistuskehyksen. Tunnistuskehys sisältää salasanasta hajautusalgoritmilla (hash function) lasketun tiivisteen (hash). Jos käytetty hajautusalgoritmi on tiedossa ja salasana on jokin sanakirjan, tai muuten helposti arvattava, sana, voidaan salasana selvittää laskemalla. Kun hyökkääjällä on tunnistuskehys, voi tämä suorittaa tarvittavan laskennan ilman yhteyttä mihinkään ulkopuoliseen tahoon. Eli kun kehys on kaapattu, ei hyökkäystä voi enää havaita mitenkään. Hyökkääjä voi yrittää pakottaa asemat lähettämään tunnistuskehyksen tukiasemalle lähettämällä väärennetyn asemille tunnistuksen purkukehyksen. Tämä pakottaa asemat lähettämään tunnistuskehyksen uudestaan muodostaakseen yhteyden uudestaan tukiasemaan. Tällainen hyökkäys korostaa riittävän pitkän ja vaikeasti arvattavan salasanan merkitystä. Jos salasana on riittävän pitkä satunnainen merkkijono, muuttuu tällaisessa hyökkäyksessä tarvittava laskenta-aika nykytietokoneilla epäkäytännöllisen pitkäksi.

WLAN-verkon havaitsemista voidaan pyrkiä rajoittamaan poistamalla käytöstä SSID-tunnuksen lähetys. Normaalissa tapauksessa WLAN-tukiasema lähettää tasaisin väliajoin ympäristöönsä viestin, jossa se kertoo tarpeellisia tietoja verkostansa. Tästä viestistä voidaan poistaa SSID tieto, jolloin aseman on tiedettävä verkon SSID ennen liittymistä. SSID on kuitenkin selvitettävissä kuuntelemalla verkkoon liittyvien asemien liikennettä, sillä ne sisältävät SSID:n selkokielisenä tekstinä. Tiedon piilotus on siis lähinnä suoja satunnaista ohikulkijaa vastaan. Toinen, samalla tavalla lähinnä lisäturvaa tarjoava, mekanismi on rajoittaa pääsyä verkkoon MAC-osoitteiden suodatuksella. Jokaisella verkkolaitteella on uniikki, valmistajan määrittämä MAC-osoite, eli periaatteessa sen perusteella voidaan rajata pääsy verkkoon

vain tunnettuihin laitteisiin. Tämän hyödyllisyyttä rajoittaa se, että MAC-osoite lähetetään salaamattomana eli sen selvittäminen on varsin helppoa. Kun osoite tiedetään, on sen vaihtaminen ohjelmallisesti triviaalia.

WLAN-verkon, kuten minkä tahansa muun langattoman verkon, saatavuutta vastaan voidaan hyökätä palvelunestohyökkäyksellä. Palvelunestohyökkäykset perustuvat siirtotien häirintään ja ne voidaan jaotella tyhmään ja älykkääseen häirintään. Tyhmä häirintä pyrkii vain estämään radiotien käytön täyttämällä sen siten, että kaikkien muiden samalla alueella toimivien tiedonsiirto estyy. Älykäs häirintä pyrkii käyttämään protokollaviestejä huijaamaan kaikkia tai jotain yksittäistä asemaa siten, että asema luulee siirtotien olevan varattu. Häirintä voidaan jaotella tämän lisäksi myös ulkoiseen ja sisäiseen häirintään sen perusteella mistä häirintä tulee suhteessa verkkoon. Kaikissa tapauksissa kyseessä on kuitenkin aktiivinen hyökkäys, jossa hyökkääjä lähettää signaalia radiotielle. WLAN-protokolla ei valitettavasti sisällä mitään valmiuksia palvelunestohyökkäysten torjumiseen. Voimalaitosympäristön etuna tässä tilanteessa on alueen fyysinen turvallisuus, mikä rajoittaa hyökkääjän mahdollisuuksia päästä riittävän lähelle kohteenaan olevaa verkkoa.

5.4 Anturiverkkojen tietoturva

Tässä työssä tarkastellut WirelessHART ja ISA100.11a anturiverkot hyödyntävät salausta ja todennusta sekä yksittäisten solmujen välillä, että erikseen koko viestin kulkemalla reitillä [17]. Tällä varmistetaan tiedon luottamuksellisuus ja tiedonsiirron osapuolten autenttisuus. Tiedon eheys varmistetaan sisällyttämällä viestiin eheys koodi (message integrity code). Vertaamalla tätä koodia viestin sisällöstä laskettuun vastaavaan arvoon, on mahdollista havaita, jos viesti on muuttunut matkalla [89]. Verkon saatavuus on vaikeampi varmistaa, sillä langaton tiedonsiirto on aina altista samalla taajuudella tapahtuvalle häirinnälle. Anturiverkot eivät muiden langattomien verkkojen tapaan kykene suojautumaan täysin häirintään perustuvilta palvelunestohyökkäyksiltä. Hyökkäys voidaan lähinnä havaita, jonka jälkeen

verkon hallinnoijan tulee pyrkiä paikallistamaan häirinnän lähde ja tehdä vaadittavat toimenpiteet sen poistamiseksi.

Isoimmat riskit anturiverkkojen tietoturvassa liittyvät palvelunestohyökkäyksiin ja tietoturvapolitiikkaan [89]. Luottamuksellisuuteen ja eheyteen liittyvät uhat ovat lähinnä teoreettisia ja vaatisivat hyökkääjän olevan fyysisesti lähellä verkkoa ja erittäin tarkkaa tietoa verkon toiminnasta. Tiedon eheys ja luottamuksellisuus voi realistisesti vaarantua vain verkon sisältäpäin tulevassa hyökkäyksessä. Tämä korostaa tarvetta toimivalle tietoturvapolitiikalle, jolla varmistetaan asiattomien käyttäjien pysyminen verkon ulkopuolella. Isoin riski tässä tapauksessa ovat käyttäjät, joiden käyttöoikeuksia ei poisteta työsuhteen päättyessä. Anturiverkkojen tapauksessa palvelunestohyökkäys voi radioliikenteen lisäksi kohdistua myös itse laitteiden toimintaan, jos käytössä on akkukäyttöisiä anturisolmuja. Tämä voidaan luokitella älykkääksi häirinnäksi, joka vaatii jonkin tasoista tietoa hyökkäyksen kohteena olevista laitteista. Solmut voidaan pyrkiä pakottamaan käyttämään lisää energiaa ja siten tyhjentämään akkunsa ennenaikaisesti. Tämä voidaan toteuttaa esimerkiksi heikentämällä radioympäristöä siten, että solmut joutuvat nostamaan lähetystehoaan ja siten käyttämään lisää energiaa tai lähettämällä solmuille paketteja, jotka joko estävät niitä menemästä lepotilaan tai pakottavat ne joihinkin toimenpiteisiin. Sama lopputulos voidaan aiheuttaa, jos jokin anturiverkon solmu saadaan kaapattua ja siten luotua reitityssilmukka verkkoon [90].

Vaikka anturiverkkojen tietoturva on asiallisella tasolla, on aina muistettava, että langaton verkko voi tarjota hyökkääjille uuden mahdollisen hyökkäysreitin. Kriittisimmät järjestelmät tulisi edelleen erottaa ulkomaailmasta ja kuten viime aikoina on tullut ilmi [85], ei tämäkään välttämättä ole riittävää ilman toimivaa tietoturvapolitiikkaa.

5.5 Yhteenveto

Nykyiset tekniset ratkaisut ovat toistaiseksi riittäviä varmistamaan langattomien verkkojen luottamuksellisuuden ja eheyden. Saatavuuden varmistaminen on huomattavasti vaikeampaa. Palvelunestohyökkäyksiltä suojautuminen vaatii langattomien verkkojen fyysistä suojaamista ulkopuoliselta häirinnältä. Tätä ongelmaa lievittää ehkä hieman yllättävästi radiosignaaleille haasteellinen voimalaitosympäristö. Metalliseinäiset rakennukset estävät signaalin kuulumisen rakennuksen ulkopuolelle, ja toisaalta häiriöiden kuulumisen rakennuksen sisälle. Myös riittävän suuri voimalaitos alue vaikeuttaa sisätiloissa tapahtuvan tiedonsiirron häirintää, sillä hyökkääjän on vaikeaa päästä riittävän lähelle kohdettansa. Ongelmallista on myös, että samanlaista häirintää voi esiintyä vaikka kyseessä ei olisi suoranainen hyökkäys. Kaikki samalla taajuusalueella toimivat sähkö- ja radiolaitteet voivat häiritä radiosignaalia. Jos häiriösignaali on laittoman tehokas, voi siltä puolustautuminen olla vaikeaa ainakin lyhyellä aikavälillä.

6. Sovelluskohteet

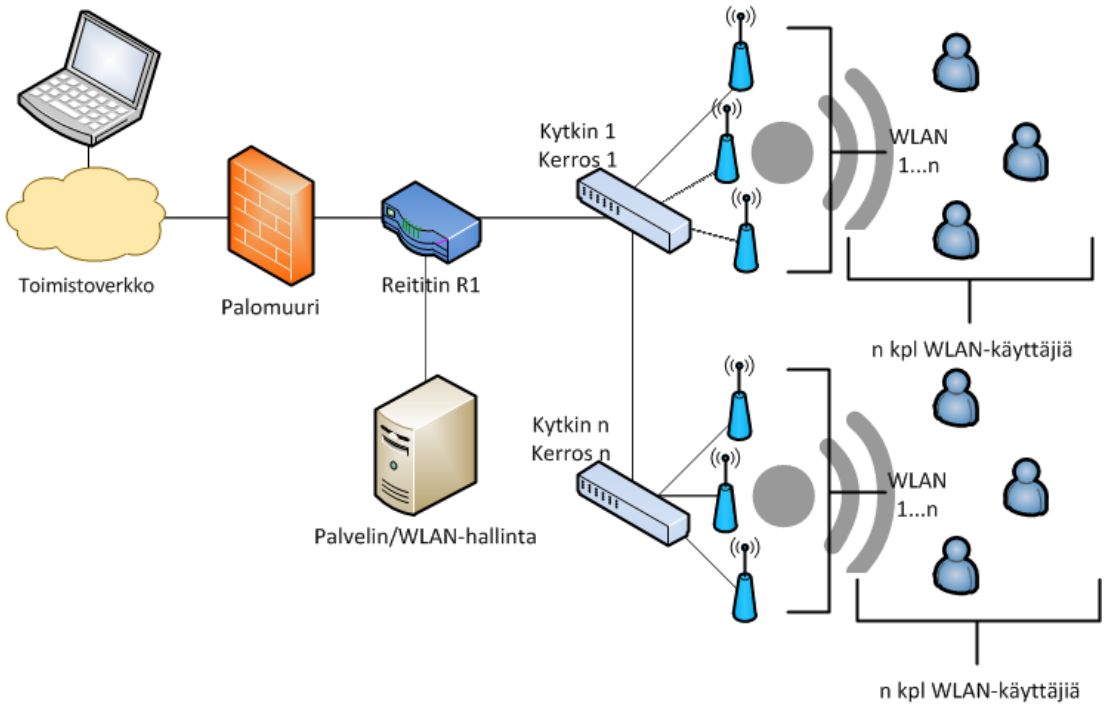
Tässä kappaleessa esitellään joitakin mahdollisia langattomien verkkojen sovelluskohteita voimalaitosympäristössä. Tässä esitetyt ideat ovat lähinnä suuntaa-antavia, joiden jalostaminen käytännön sovelluksiksi olisi hyvä jatkotutkimuksen kohde. Kuten aiemmin on jo mainittu, on hyvä tiedostaa, että langattomuuden ei tule olla itsetarkoitus. Langattomien järjestelmien, kuten kaiken teknologian tulee tarjota loppukäyttäjille jotakin lisäarvoa esimerkiksi kasvaneen työtehon muodossa

Mahdollisia sovelluksia voidaan arvioida ISA-SP100.11-luokittelun [91] perusteella. Luokittelu jakaa sovellukset kuuteen luokkaan niiden tiedonsiirron kriittisyyden perusteella. Luokat on lisäksi jaettu kolmeen kategoriaan sovelluskohteen mukaan. Luokittelun perusteella voidaan määritellä tiedonsiirrolle viivevaatimukset automaatiokäytössä. Luokittelu on esitetty tarkemmin taulukossa 4. Luokalla 0 on korkeimmat vaatimukset viestin vasteajalle ja ajantasaisuudelle, luokalla 5 pienimmät.

Taulukko 4, ISA-SP100.11-luokittelu

Kategoria	Luokka	Sovelluskohde	Kriittisyys
Turvallisuus	0	Turvallisuuteen liittyvät järjestelmät	Aina kriittinen
Ohjaus	1	Suljettu säätöpiiri, suora ohjaus	Usein kriittinen
	2	Suljettu säätöpiiri, epäsuora ohjaus	Yleensä ei-kriittinen
	3	Avoin säätöpiiri	Ihminen osana ohjausta
Valvonta	4	Hälytykset	Lyhyen aikavälin vaikutus operointiin
	5	Tapahtumien rekisteröinti, tiedonsiirto	Ei välittömiä vaikutuksia operointiin

6.1 Esimerkki 1: Prosessitilan WLAN-verkko



Kuva 12, monikerroksisen prosessitilan WLAN-verkko

Ensimmäinen sovellusmahdollisuus langattomille verkoille voimalaitos ympäristössä on prosessitiloihin rakennettava WLAN-verkko. Verkon peitto on korkeintaan voimalaitosalueen luokkaa. Tavoitteena olisi mahdollistaa langaton tiedonsiirto kentällä olevien päätelaitteiden ja voimalaitosalueen muiden tietoverkkojen välillä. Nämä tietoverkot voivat olla esimerkiksi toimistoverkko tai automaatiojärjestelmän prosessiverkko.

WLAN-verkon perusperiaate näkyy Kuvasta 7. Tukiasemia asennetaan kerroksiin tarvittava määrä (n kpl), jotta verkon peitto saadaan riittäväksi. Tällainen ratkaisu on sopiva prosessitiloihin, jotka ovat pystysuunnassa suuria rakennuksia. Vaikka työssä pääasiassa keskityttiin juuri prosessitiloihin, on hyvä muistaa, että voimalaitosalueella on myös muunlaisia ympäristöjä. Näistä maininnan arvoisia ovat maanalaiset hiililuolat, joissa tukiasemat asennettaisiin pitkiin tunneleihin. Niiden tapauksessa tukiasemat asennettaisiin joillekin tietyille väleille pitkin tunnelia. Tämä vaatisi oman selvityksensä sillä esimerkiksi ilmassa leijuva hiilipöly ja tunnelien seinämät vaikuttavat radiosignaaliin eri tavalla kuin prosessitilojen runsaat

metallirakenteet. Asennuspaikkoihin ja tiheyteen vaikuttaa myös tukiasemien sähköntarve. Tarvittavia sähköliitäntöjä ei välttämättä ole helposti tarjolla ja tukiasemat voidaan joutua asentamaan vähemmän optimaalisiin paikkoihin. Käytännön kokeissa havaittiin, että tukiasemia ei välttämättä tarvita jokaiseen kerrokseen, vaan sopivalla sijoittelulla ja antenneilla signaali on riittävä kattamaan useampia kerroksia. Tähän vaikuttaa luonnollisesti myös tavoiteltu palvelunlaatu. Tukiasemat liitetään kerroksittain kytkimiin, jotka voidaan ketjuttaa ja liittää reitittimeen. Reititin voidaan tällöin sijoittaa sopivaan paikkaan, esimerkiksi kaapelitilaan, jossa yhteys muihin verkkoihin on helppo toteuttaa. Kuvassa reitittimeen (R1) on liitetty myös hallintapalvelin WLAN-tukiasemille. Tällainen järjestely tulee kysymykseen tukiasemien määrän kasvaessa, jolloin niiden asetusten hallintaan tarvittava työmäärä kasvaa kohtuuttomaksi. WLAN-verkkokokonaisuus erotetaan vielä muista verkoista palomuurilla, jolla varmistetaan mahdollisuus valvoa ja hallita liikennettä tietoturvakriittisempiin verkkoihin. Vaikka kuvassa reititin, palomuuri ja WLAN-hallintapalvelin (WLAN-manager) on piirretty erillisiksi laitteiksi, voivat nämä kaikki kolme tai jokin yhdistelmä olla samassa laitteessa, esimerkiksi reititin voi toimia myös palomuurina. Palvelin voi sisältää myös 802.1X-standardin mukaisen todennuspalvelun, jolla tarjotaan keskitetty tietoturvaratkaisu koko verkolle.

Tämänkaltaisen järjestelmän, jonka päätarkoitus on tarjota vain yksinkertainen tiedonsiirtokanava, yhteydessä voidaan sovellusmahdollisuudet jaotella karkeasti kahteen kategoriaan. Ensimmäinen vaihtoehto on, että teknologia tarjoaa alustan ja loppukäyttäjät voivat hyödyntää sen tarjoamia mahdollisuuksia haluamallaan tavalla. Tämä edellyttää, että pääsy verkkoon ja sen käyttö ovat suhteellisen vapaita jolloin tietoturvakysymykset nousevat erittäin merkittäviksi. Toinen vaihtoehto on, että langaton verkko rakennetaan tarjoamaan jotakin hyvin tarkasti määriteltyä palvelua. Esimerkkeinä tarjotuista palveluista voivat olla yhteys automaatiojärjestelmään tai järjestelmä, jolla tuodaan voimalaitokseen liittyvää dokumentaatiota tarjolle kentällä. Jos tarkoituksena on tarjota jokin tarkasti rajattu palvelu, tämä mahdollistaa tiukemman rajauksen verkossa

siirrettävälle liikenteelle. Tämä taas rajoittaa mahdollisille hyökkääjille tarjoutuvaa hyökkäyspintaa.

6.1.1 Toteutuksen suunnittelu

Käytännön toteutuksen ensimmäinen askel on suunnitella verkko siten, että sekä signaalin kuuluvuus, että tiedonsiirtokapasiteetti ovat riittäviä mahdollisimman pienellä määrällä tukiasemia. Tähän työhön liittyen tehtyjen kokeiden perusteella voidaan sanoa olevan mahdollista tarjota perustason palvelu pienelle määrälle käyttäjiä (1-5) yhdellä n-nopeusluokan tukiasemalla n. 4 kerrosta korkealle alueelle kattilahallissa käyttäessä 5GHz-taajuusaluetta ja teollisuuskäyttöön suunniteltuja laitteita. 5GHz-taajuuksien teoriassa pienempi kuuluvuusalue ei osoittautunut rajoittavaksi tekijäksi. Perustason palvelulla tarkoitetaan tässä tapauksessa seuraavaa:

- Vähintään **10 Mbit/s** tiedonsiirtonopeutta pisimmällä etäisyydellä tukiasemasta
- Korkeintaan **100 ms** vasteaikaa
- Korkeintaan **5 %** pakettihäviö

Tällainen palvelutaso riittää esimerkiksi kevyeen Internet käyttöön, ei-aikakriittisen tiedon lukemiseen automaatiojärjestelmästä tai pakatun videokuvan siirtämiseen [21]. Erityisesti tiedonsiirtonopeus paranee moninkertaiseksi etäisyyden tukiasemaan pienentyessä. Myös vasteaika ja pakettihäviö paranevat jonkin verran etäisyyttä pienentämällä. Tässä työssä suoritetut kokeet kattavat vain muutaman erilaisen yhdistelmän erilaisia laitteita. On suositeltavaa myös selvittää erityisesti tukiasemaan liitettävien asemien toimivuus kuuluvuusalueen ulkoreunoilla. Varsinkin pienten kannettavien laitteiden kohdalla antennien kyky toimia heikolla signaalilla on selvittämisen arvoista. Käytännön mittausten perusteella voidaan arvioida millä etäisyydellä asetetut vaatimukset tiedonsiirtonopeuksille, vasteajalle ja pakettihäviölle täyttyvät. Asennustiheyttä suunnitellessa on selvitettävä verkkoon liitettävien laitteiden määrä ja jokaisen laitetyypin generoima liikenne. Kun kunkin laitteen tarvitsema kapasiteetti on tiedossa, voidaan nämä tiedot suhteuttaa tukiaseman todelliseen mitattuun kapasiteettiin.

Näissä laskelmissa ei tule käyttää teoreettisia valmistajien lupaamia tiedonsiirtonopeuksia. Kuten tämänkin työn puitteissa tehdyissä mittauksissa havaittiin jäävät käytännössä mitatut tiedonsiirtonopeudet jopa kertaluokkaa pienemmiksi.

Koska suurimpiin tiedonsiirtonopeuksiin päästään yksinkertaisimmin pienentämällä etäisyyttä tukiasemaan, vaatii WLAN-verkon kapasiteetin kasvattaminen luonnollisesti myös tukiasemien määrän kasvattamista. Tämä tarkoittaa myös tukiasemien sijoittamista lähemmäs toisiaan, jolloin eri tukiasemien kuuluvuusalueet ovat ainakin osittain toisensa päällä. Jotta tämä ei aiheuttaisi ongelmia, tulee WLAN-kanavien uudelleenkäyttöön kiinnittää huomiota. Tämä on erityisen tärkeää 2,4GHz-taajuusalueella, jolla samaan aikaan käytössä olevia täysin ei-päällekkäisiä kanavia on vain 3kpl. 5GHz-taajuusalueella ei-päällekkäisiä kanavia on käytössä 8kpl, joten ongelma ei ole yhtä huomattava. Ongelmaa helpottamaan tukiasemat tulee valita siten, että niiden ohjelmisto kykenee valitsemaan optimaalisimman kanavan ympäristöstään tekemien mittausten perusteella [18]. Kanavien uudelleenkäytön suunnittelu on vain osa verkon suunnittelua, varsikin voimalaitosympäristössä on tarpeen tehdä mittauksia kentällä ja selvittää siten signaalinen todellinen käyttökelpoinen kantama. Jos jo etukäteen on tiedossa muita samalla taajuusalueella toimivia verkkoja tai laitteita tulee myös tämä huomioida suunnittelemalla radiokanavien käyttö siten, että päällekkäisyyksiä muiden verkkojen kanssa vältetään mahdollisimman paljon. Kun lopulta tiedossa on sekä tarvittavien tukiasemien määrä, että tukiasemilla saavutettava todellinen signaalin kantama voidaan näiden tietojen perusteella valita tukiasemille optimaaliset asennuspaikat. Tässä yhteydessä on hyvä ottaa huomioon myös se, että samalla taajuudella toimivat tukiasemat vaikuttavat negatiivisesti toistensa tiedonsiirtokapasiteettiin. Jaetulla siirtotiellä tapahtuu hyvin todennäköisesti jossain vaiheessa törmäyksiä jolloin tiedonsiirto epäonnistuu. WLAN:n tapauksessa törmäys pakottaa osapuolet, joiden lähettämät paketit tuhoutuivat matkalla, odottamaan siirtotielle uudelleenpääsyä. Tästä johtuen samalla taajuudella toimivat tukiasemat aiheuttavat kapasiteetin

jakautumisen tukiasemien määrän funktiona, kapasiteetti laskee nopeammin kuin lineaarisesti. Eli tästäkin syystä taajuuskanavien uudelleenkäyttöön tulee kiinnittää paljon huomiota ja harkita esimerkiksi suunta-antennien käyttöä aina, kun se on mahdollista.

Jotkin sovellukset voivat tuottaa liikennettä vain tietyin aikavälein, jolloin on hyödyllistä pyrkiä porrastamaan tiedonsiirron ajankohtia mahdollisuuksien mukaan. Porrastaminen ei välttämättä ole kuitenkaan mahdollista, jos samanaikaisia käyttäjiä yksinkertaisesti on paljon joillain tietyillä ajanhetkillä. Tällaiset piikit osuvat todennäköisesti työpäivien aamu- ja iltapäiviin. Kun liikennemääristä on tehty arvio, voidaan sen perusteella päättää miten langaton järjestelmä liitetään osaksi muita tietoverkkoja. Jos liikennemäärä on huomattavan suuri, se voi aiheuttaa turhaa ruuhkaa prosessiverkossa. Erittäin kattava järjestelmä voi vaatia jopa oman siirtoverkon rakentamista, jolloin kustannukset voivat nousta huomattavan suuriksi.

Tietoturvan kannalta on oleellista hyödyntää uusinta WPA2-tekniikkaa. Näin voidaan varmistaa verkossa liikkuvan tiedon eheys ja luottamuksellisuus. WPA2 tarjoaa työkalut tiedon salaukseen ja käyttäjienhallintaan. Verkon koosta riippuen voidaan käyttää joko PSK (Pre-shared Key)-järjestelmää, jossa jokaiselle laitteelle tulee erikseen syöttää salasana verkkoon liittyäkseen tai 802.1X-standardin mukaista porttipohjaista pääsynhallintaa, jossa erillinen palvelin vastaa verkkoon liittyvien laitteiden hallinnasta. PSK on soveltuva pieniin verkkoihin, kun taas 802.1X-pohjainen järjestelmä suurempiin [30]. Verkkoon liittymiseen käytettyä avainta on suositeltavaa vaihtaa tietyin väliajoin esimerkiksi vähintään kerran vuodessa vuosihuollon yhteydessä. Lisäksi tulee soveltaa organisaation tietoturvaperiaatteita käyttäjien ja laitteiden hallinnointiin. On tarpeen määritellä henkilöt, joiden vastuulla on esimerkiksi tukiasemien hallinta sekä prosessit käyttäjien tunnistukseen. Koska järjestelmään voi kuulua kannettavia laitteita, on tarpeen määritellä myös niiden hallintaan liittyvät säännöt. Laitteiden käyttö tulee rajoittaa vain työkäyttöön ja ne tulee säilyttää voimalaitosalueella niille määritellyssä paikassa. Langaton verkko ja siihen liittyvä langallinen

runkoverkko tulee eriyttää siten, että niistä on pääsy vain käytön kannalta tarpeellisiin osiin muita verkkoja. Näin minimoidaan muihin järjestelmiin kohdistuva hyökkäyspinta-alan kasvu.

6.1.2 WLAN-tekniikan mahdollisia sovelluskohteita

Seuraavassa on listattu voimalaitosympäristössä joitakin mahdollisia sovelluskohteita WLAN-tekniikalle:

- **WLAN-yhteys osana automaatiojärjestelmän tiedonsiirtoa:** Kuten käytännön kokeet osoittivat, on WLAN-tekniikan soveltamista rajoittavin tekijä varsinkin hankalissa radio-olosuhteissa suhteellisen pitkä vasteaika (n. 100 ms) sekä tiedonsiirtokapasiteetin putoaminen (n. 10 Mbit/s). Tämä rajoittaa käyttöä nopeimmissa mittauskohteissa ja laitteiden määrää aivan verkon peiton ulkorajoilla. Lisäksi langattoman yhteyden toimivuutta ei voi taata samalla tasolla kuin langoitetun, joten nämä tekijät rajaavat käytön automaatio järjestelmän vähemmän kriittisiin kohteisiin. Tässä tapauksessa langatonta tiedonsiirtoa voitaisiin hyödyntää esimerkiksi jos on tarpeen toteuttaa yksittäinen mittaus johonkin vaikeapääsyiseen paikkaan. Tällöin vältytään korkeilta kaapelointi- ja asennuskustannuksilta ja voidaan lisäksi parantaa työturvallisuutta sellaisissa tapauksissa, joissa sama tieto on aiemmin pitänyt kerätä ihmisvoimin. Langaton yhteys voi myös olla käytössä langallisen yhteyden rinnalla varayhteytenä. Tämä voi olla hyödyllistä tapauksissa, joissa vaatimuksena on erotella tiedonsiirtoreitit fyysisesti toisistaan tai on tarve lisätä uusia yhteyksiä olemassa olevien rinnalle. Langaton yhteys ei myöskään ole altis tiedonsiirtokaapeleiden katkeamiselle, toiminta riippuu vain päätelaitteista ja siirtotiestä. Yhteys voi toki katketa, mutta lukuun ottamatta jotakin laajamittaista vahinkoa, ei kaapeleiden katkeamiseen johtanut tilanne välttämättä estä langatonta tiedonsiirtoa. Jos langaton yhteys muodostetaan ulkotiloihin, voidaan hyödyntää voimalaitosympäristöstä löytyviä korkeita rakenteita vapaan siirtotien takaamiseksi. Vaihtoehtoisesti toteutukseen voidaan käyttää IEEE

802.15.4-pohjaista ratkaisua, jos on tarpeen saavuttaa lyhyin mahdollinen vasteaika ja mahdollisesti parempi toimintavarmuus.

- **Langaton yhteys kentältä automaatiojärjestelmään:** Tämä sovellus hyödyntää WLAN-tekniikalla toteutettua verkkoa, joka kattaa esimerkiksi prosessitilat. Tarkoituksena on luoda langaton yhteys kannettavalta päätelaitteelta automaatiojärjestelmään. Tällä mahdollistetaan sekä mittalaitteiden keräämän tiedon tarkastelu, että mahdollisesti myös joidenkin asetusten muuttaminen käyttäjän sijainnista riippumatta. Tässäkin tapauksessa langattoman verkon suunnittelu riippuu pitkälti siitä, minkälaista tietoa päätelaitteen ja automaatiojärjestelmän välillä on tarkoitus siirtää. Erityisesti vasteaika on ratkaisevassa osassa, kokeissa havaittu huonoin tapaus eli n. 100 ms vasteaika ei välttämättä riitä nopeasti päivittyvien suureiden seurataan.
- **Langaton dokumentinhallinta:** WLAN-pohjainen järjestelmä, jossa laitoksen dokumentaatio on langattomasti tarkasteltavissa päätelaitteella kuten kannettavalla tietokoneella. Tarkoituksena on tuoda esimerkiksi piirustukset ja kunnossapitotietokanta työntekijöiden saataville suoraan kentällä. Tämän tavoitteena on varmistaa, että työn suorittajilla on heti saatavilla tarvitsemansa tiedot ja vähentää työn suoritukseen tarvittavaa esivalmistelua. Voimalaitosdokumentaatio voi sähköisessä muodossa vaatia suuren tallennustilan. Laitepiirustukset voivat olla kooltaan useita megatavuja. Tiedonsiirron kannalta tärkeimmäksi vaatimukseksi nousee siis riittävän nopea tiedonsiirto. Kuten käytännön kokeista havaittiin, on vasteaika riittävän pieni tähän käyttöön vielä koeverkon ulkoreunallakin, jossa tiedonsiirtonopeus on enää 10 Mbit/s. Tämä tiedonsiirtonopeus ei ole enää riittävä tarjoamaan sulavaa käyttökokemusta, jos on tarpeen siirtää satoja megatavuja tietoa lyhyessä ajassa. Tällainen tilanne voi tulla eteen tilanteessa, jossa joudutaan käymään läpi useita piirustuksia jonkin tietyn löytämiseksi. Käytännössä tämä tarkoittaa langattoman verkon liittämistä osaksi toimistoverkkoa, jossa tällaiset tiedot ovat saatavilla.

Langattoman järjestelmän tulee siis täyttää organisaation asettamat vaatimukset toimistoverkkoon liitettäville laitteille.

- **Langaton kameravalvonta:** WLAN-pohjainen järjestelmä, joka tarjoaa mahdollisuuden sijoittaa langattomia valvontakameroita väliaikaiseen tarkkailuun ympäri voimalaitosta. Näin voidaan tarkkailla jotakin häiriötilannetta ilman, että henkilökunnan tarvitsee olla jatkuvasti paikan päällä. Tällaisen järjestelmän suunnittelua ohjaa pitkälti kameroiden määrä ja kunkin kameran verkkoon tuottama liikenne. Yksittäisen kameran tuottama liikenne riippuu pitkälti halutusta kuvanlaadusta ja, joka koostuu valitusta videonpakkausalgoritmista, resoluutiosta ja ruudunpäivitysnopeudesta. Kuvanlaadun lisäksi tuotetun tiedon määrää vaihtelee kuvatun kohteen monimutkaisuus, yksinkertainen ja vähän muuttuva kohde tuottaa vähemmän siirrettävää tietoa. Lisäksi on huomioitava kuinka usein kamerat lähettävät tietoa, joka määräytyy sen perusteella kuinka usein kamerat on määritetty kuvaamaan ja perustuuko kuvauksen aloittaminen jonkin ehdon täyttymiseen. Näiden tietojen perusteella voidaan laskea tuotetun tiedon määrä sekuntia, tuntia tai päivää kohden[92]. Tiedon määrän perusteella voidaan mitoittaa tiedonsiirtokapasiteetti sekä mahdollinen tallennuskapasiteetti. Jotta verkon kapasiteetti voidaan määritellä oikein, tulee lisäksi ottaa huomioon eri protokollatasojen otsikkotiedot (header). Otsikkotietojen vuoksi hyötykuorma on pienimmillään n. 95 % [93], joka tulee ottaa huomioon laskelmissa.

  Käytännön kokeissa mitattu huonoin tilanne, eli n. 100ms vasteaika, 10Mbit/s tiedonsiirtonopeus ja 5 % pakettihäviö, tarjoaa edelleen mahdollisuuden käyttää yhtä tai useampaa kameraa riippuen kuvanlaadusta. Tässä tapauksessa tiedonsiirtonopeus muodostuu rajoittavaksi tekijäksi, sillä tarkoituksena ei ole valvoa nopeasti muuttuvia kohteita vaan lähinnä vapauttaa työntekijöitä valvontatehtävistä muihin työtehtäviin. Käyttäen H.264 videopakkausta, 352x288 resoluutiota, 5 kuvaa/sekunti ruudunpäivitysnopeutta on

tuotetun tiedon määrä n. 110Kbit/s[92]. Kun otetaan huomioon 95 % hyötykuorman osuus, on tarvittava tiedonsiirtonopeus kameraa kohden $\frac{110Kbit/s}{0,95} \approx 116Kbit/s$. Tämä edustaa heikointa mahdollista kuvanlaatua. Jos laatu nostetaan 704x576 resoluutioon ja 15 kuvaan sekunnissa käyttäen samaa pakkausalgoritmia on tuotetun tiedon määrä n. 600Kbit/s[92]. Tällöin tarvittava tiedonsiirtonopeus on $\frac{600Kbit/s}{0,95} \approx 632Kbit/s$. Tämä edustaa hieman keskitasoa parempaa kuvanlaatua. Parhaalla mahdollisella kuvanlaadulla käyttäen Motion JPEG pakkausta, 704x576 resoluutiota 15 kuvaa sekunnissa on tuotetun tiedon määrä 4800Kbit/s[92]. Tarvittava tiedonsiirtonopeus on tällöin $\frac{4800Kbit/s}{0,95} \approx 5050Kbit/s$. Tähän mennessä voimalaitoksella tehtyjen käyttökokeiluiden perusteella on tarvetta ollut käyttää samanaikaisesti yhtä tai kahta langatonta kameraa. Tällaisessa tilanteessa riittäisi siis yksi WLAN-tukiasema neljää kattilahallin kerrosta kohden tarjoamaan riittävän nopeantiedonsiirron yhdelle parhaalla kuvanlaadulla toimivalle kameralle tai lukuisille keskitason tai heikon kuvanlaadun kameralle. Tässäkin yhteydessä on muistettava, että tukiaseman kapasiteetti ei jakaudu lineaarisesti asemien määrän kasvaessa johtuen tavasta, jolla protokolla siirtokerros jakaa siirtotien asemien kesken.

6.2 Esimerkki 2: Langaton anturiverkko

Anturiverkkojen etuna WLAN-tekniikkaan on ainakin teoriassa varmempi tiedonsiirto sekä mahdollisuus monimuotoisempiin verkkotopologioihin ja siten parempaan toimintavarmuuteen. IEEE 802.15.4-standardiin perustuvat anturiverkon on myös suunniteltu suoraan teollisuuden käyttöön. Anturiverkoilla voidaan luoda toimintavarma langaton tiedonsiirtoverkko esimerkiksi automaatiojärjestelmän tarpeisiin. Toimintavarmuuden takaamiseksi tiedonsiirto voi hyödyntää useampia vaihtoehtoisia reittejä, kun käytössä on mesh-verkko tai sen hybridi. Anturiverkko koostuu jostakin määrästä anturisolmuja ja niitä hallinnoivasta laitteesta. Anturisolmut

keräävät tietoa ja välittävät sitä eteenpäin esimerkiksi automaatiojärjestelmään. Hallintalaitteen tehtävä on kontrolloida verkon toimintaa ja tietoturvaa, lisäksi se toimii usein yhdyskäytävänä muihin verkkoihin.

Vaikka pääfokus työssä on ollut 2,4GHz ja 5GHz ISM-taajuusalueella toimivissa laitteissa, voitaisiin tässä yhteydessä käyttää myös lupavapaalla [15] 868MHz-taajuusaluella toimivia laitteita. Tällöin siirrettävän liikenteen määrä olisi kuitenkin huomattavan rajoittunut, sillä kyseisellä taajuusalueella toimintasuhteen tulee olla alle 1 %. Tällaisia laitteita voitaisiinkin käyttää sellaisissa osissa verkkoa, joissa anturisolmut ovat vaikeasti saavutettavissa korkeammilla taajuuksilla heikomman läpäisykykynsä vuoksi. Lisäksi tulee huomioida, että WirelessHART [11] ja ISA100.11a [12] on suunniteltu toimimaan vain 2,4GHz-taajuuksilla.

6.2.1 Toteutuksen suunnittelu

Anturiverkkojen toimintaa ei tämän työn puitteissa päästy kokeilemaan käytännössä, joten tässä yhteydessä ei voida antaa suosituksia liittyen juuri kyseiseen ympäristöön. Anturiverkkostandardit on suunniteltu teollisuuskäyttöön eli niiden tiedonsiirron pitäisi ainakin teoriassa olla toimintavarmaa. Tämä yhdistettynä WLAN-verkoista saatuihin positiivisiin tuloksiin voidaan ennakoida anturiverkkojenkin toimivan vähintään kohtuullisesti prosessitiloissa. Tästä huolimatta ennen laajamittaista käyttöönottoa olisi kuitenkin suositeltavaa selvittää tekniikan toimivuus ainakin jollain tasolla käytännön mittauksin. Joka tapauksessa toimittaessa 2,4GHz-taajuusalueella tulee huomioida koeksistenssi muiden verkkojen kanssa. Radiokanavien valinta tulee mahdollisuuksien mukaan tehdä siten, että jo olemassa olevat verkot voidaan välttää. Lisäksi tulevaisuuden kannalta hyödyllistä on kerätä keskitetysti tieto anturiverkon käyttämistä radiokanavista helpottamaan mahdollisten muiden langattomien verkkojen suunnittelua.

Suurimmat uhat anturiverkon tietoturvalle liittyvät verkon sisältä tuleviin hyökkäyksiin sekä palvelunestohyökkäyksiin [89]. Toisin kuin IEEE 802.11-

pohjaisissa verkoissa WirelessHART tai ISA100.11a-verkoissa ei ole mahdollista käyttää vanhoja salaustekniikoita eli tilanne on tältä kannalta hyvä. Standardeja kehitetään kuitenkin edelleen eli laitteet on pidettävä ajan tasalla sitä mukaan, kun päivityksiä tulee. Kuten WLAN-verkon tapauksessakin, myös anturiverkossa salaukseen ja verkkoon liittymiseen käytettyjä avaimia tulisi vaihtaa tasaisin väliajoin. Sisäisiä hyökkäyksiä voidaan torjua toimivalla tietoturvapolitiikalla. Erityistä huomiota tulee kiinnittää käyttäjienhallintaan, vastuu verkon hallinnoinnista tulee olla vain siihen koulutetuilla tahoilla ja vanhojen tai väliaikaisten käyttäjien hallinnointi tehokasta. Palvelunestohyökkäyksiä vastaan voimalaitosympäristö tarjoaa fyysisen turvallisuuden muodossa turvaa pakottaen mahdolliset hyökkääjät kauemmas kohteestaan. Tilannetta voi parantaa myös valitsemalla sellaisia laitteita, jotka kykenevät valitsemaan käyttämänsä radiokanavan dynaamisesti. Tällöin hyökkäyksen tapahtuessa laitteet voivat vaihtaa vähemmän häiriöiselle kanavalle. Fyysisellä turvallisuudella suojellaan myös anturisolmuja. Jos solmu päätyy hyökkääjän haltuun, voidaan sitä käyttää vaarantamaan koko verkko [94].

6.2.2 Langattoman anturiverkon sovelluskohteita

Seuraavassa on listattu voimalaitosympäristössä joitakin mahdollisia sovelluskohteita anturiverkoille:

- **Langaton kunnonvalvontajärjestelmä (KVJ-järjestelmä):** Tämä sovelluskohde voi yhdistää sekä anturiverkkotekniikan, että WLAN-tekniikan. Anturiverkko kerää kunnonvalvontatiedon laitteilta, joka hallintalaitteelle. Tämä laite on kytketty WLAN-verkon kanssa samaan langalliseen verkkoon. Kattavan WLAN-verkon kautta tieto tuodaan kunnonvalvonnasta vastaavien työntekijöiden saataville suoraan kentällä. Näin voidaan laitteiden kunnonvalvontatiedon lukemisen lisäksi kuitata laite tarkistetuksi osana voimalaitoksen tarkastuskierrosta.
- **Anturiverkko energianhallintaan käyttäen energiaomavaraisia anturisolmuja** [95] [96]**:** Yksittäinen mittaus tai pieni anturiverkko,

jonka anturisolmut saavat toimintaenergiansa ympäristöstänsä tai pitkäkestoisista akuista. Mittalaite toimii täysin langattomasti jolloin sen asennuskustannukset ovat pienet ja asennus helppoa, sillä kaapelinvetoa ei tarvita lainkaan. Tällainen ratkaisu sopii hyvin tilanteeseen, jossa tietoa halutaan kerätä hankalapääsyisestä paikasta. Tätä konseptia voidaan laajentaa myös energiaomavaraiseen anturiverkkoon, jolla tarkkaillaan ja ohjataan jonkin esimerkiksi jonkin tilan lämmitystä tai ilmanvaihtoa. Mahdollinen käyttökohde voimalaitoksella voisi olla sähkö- ja automaatiotilat, joissa on tarpeen pitää yllä tiettyä lämpötilaa ja ilmanlaatua. Langattomalla anturiverkolla voidaan tuottaa tarkempaa mittaustietoa ilman kalliita asennuksia. Anturiverkon solmut voisivat saada energiansa pitkäkestoisista akuista. Yksittäinen anturisolmu voisi olla erittäin yksinkertainen ja siten energiatehokas. Yhden anturisolmun tarvitsisi mitata esimerkiksi vain yhtä ympäristön suuretta. Anturisolmujen akut voitaisiin huoltaa voimalaitoksen vuosihuollon yhteydessä. Jos jotkin verkon solmut joutuvat reitittämään suhteessa enemmän liikennettä, voidaan ne sijoittaa siten, että ne saavat energiansa kiinteästi asennettavalla virtakaapelilla.

Anturiverkon keräämän tiedon perusteella voidaan optimoida tilan ilmanvaihdon toimintaa. Optimoinnilla voidaan säästää tilojen ilmastointiin kuluvaa energiaa ja siten parantaa laitoksen energiatehokkuutta. Samalla voidaan tarkkailla esimerkiksi tiloihin kertyviä mahdollisia epäpuhtauksia, jotka voivat aiheuttaa sähkölaitteiden toimintahäiriöitä. Jos tällainen järjestelmä voidaan toteuttaa jokaiseen voimalaitoksen sähkötilaan, voi saavutettu energiansäästö olla hyvinkin merkittävä. Tällaisen järjestelmän ei tarvitse täyttää automaatiojärjestelmän tiukkoja toimintavarmuusvaatimuksia, joten käytettävät laitteet voivat olla yksinkertaisia ja siten hinnaltaan edullisempia. Kun anturiverkkoa ei liitetä osaksi automaatiojärjestelmää, vältytään samalla myös sen asettamilta tiukoilta tietoturva ja varmuusvaatimuksilta. Tarvittaessa

varmuutta järjestelmään voidaan rakentaa toteuttamalla verkko mesh-rakenteella. Järjestelmän toteutukseen soveltuvat ratkaisut löytyvät luultavimmin 802.15.4-standardiperheeseen perustuvista ratkaisuista. Tällaiselle ratkaisulle olisi tässä työssä esitetyistä helpoin laskea takaisinmaksuaika, sillä säästetylle energialle on helppo antaa rahallinen arvo. Tässä konseptissa vältytään myös asennuksilta radiosignaalien etenemisen kannalta vaikeaan prosessitilaan, jolloin radiosuunnittelu helpottuu. Tätä helpottavat myös suhteellisen lyhyet etäisyydet anturisolmujen välillä.

Jos kyseinen konsepti osoittautuu toimivaksi, voidaan samaa periaatetta laajentaa myös esimerkiksi toimistotiloihin ja niiden ilmastoinnin ja lämmityksen tarkempaan ohjaukseen. Samalla järjestelmällä voidaan myös löytää mahdollisia ongelmakohtia, kuten esimerkiksi vuotavia ikkunoita poikkeavien anturilukemien perusteella ja siten myös parantaa energiatehokkuutta. Lisäksi ohjausta voidaan laajentaa esimerkiksi valaistuksen ohjaukseen, jolla voidaan saavuttaa lisäsäästöjä.

7. Käytännön kokeet ja tulokset

Käytännön kokeiden tarkoituksena oli selvittää voimalaitoksen prosessitilojen radioympäristön soveltuvuutta langattomaan tiedonsiirtoon ISM-radiotaajuksia käyttävillä laitteilla. Kokeet suoritettiin 2,4GHz ja 5GHz taajuusalueilla. Radiosignaalien eteneminen prosessitiloissa ei ole intuitiivisesti selvää, varsinkaan jos radioasemien välillä ei ole suoraa näköyhteyttä, vaan todellinen tilanne on selvitettävä mittaamalla. Mittaukset osoittivatkin, että radiosignaali voidaan saada kuulumaan riittävän voimakkaasti yllättävissä paikoissa sekä päinvastoin signaali saattaa heikentyä käyttökelvottomaksi hyvin lähellä tukiasemaa.

7.1 Koejärjestelyt

Kokeet jaettiin kahteen vaiheeseen. Ensimmäisessä vaiheessa käytössä oli kaksi kannettavaa tietokonetta, ja niiden välillä langaton WLAN yhteys käyttäen kuluttaja-luokan laitteita. Toisessa vaiheessa kokeet suoritettiin teollisuus-luokan WLAN testilaitteistolla, joissa oli käytössä huomattavasti järeämmät antennit. Molemmat kokeet suoritettiin sekä 2,4GHz, että 5GHz taajuusalueilla. Koeympäristöiksi valittiin Salmisaaren voimalaitoksen eri prosessitilat, joista tarkastelun kohteeksi otettiin radiosignaalin etenemisen kannalta helpommaksi oletettu kattilahalli sekä vaikeaksi oletettu rikinpoistolaitos. Kokeissa mitattiin signaalin voimakkuutta, tiedonsiirtonopeutta, vasteaikaa ja pakettihäviöitä. Pakettihäviö mitattiin osana vasteaikamittausta. Tiedonsiirtonopeus mitattiin UDP- ja TCP-protokollia käyttäen.

Kaikkien edellä mainittujen arvojen perustasot mitattiin toimistotiloissa, sijoittamalla tukiasema ja asema pöydille n. 5m päähän toisistaan siten, että niiden välille jäi tyhjä tila. Valituilla radiokanavilla ei mittausten aikana kuulunut muita WLAN-verkkoja 2,4GHz- tai 5GHz-taajuusalueilla.

UDP-protokolla [97] on yhteydetön protokolla eli tieto siirretään laitteiden välillä ilman erillistä yhteydenmuodostusta tai pakettien kuittausta. Tällöin ei

tarvita erillistä alkukättelyä tai yhteydenpurkua ennen ja jälkeen tiedonsiirron. UDP-protokolla on toiminnaltaan hyvin kevyt ja yksinkertainen, paketilla on vain lyhyet otsikkotiedot eli siirrettävä hyötykuorma on suhteessa suurempi TCP-protokollaan verrattuna. Tietoa voidaan saada siirrettyä siis ainakin jonkin verran myös epävarmalla yhteydellä.

TCP-protokolla [98] on yhteydellinen protokolla eli tiedonsiirto vaatii aina erillisen yhteydenmuodostuksen sekä pakettien kuittauksen. Tiedonsiirto aloitetaan kolmitiekättelyllä, vastaanottaja kuittaa saamansa paketit ja yhteys puretaan nelitiekättelyllä. Tiedonsiirto on siis varmempaa kuin UDP-protokollalla, olettaen että yhteys saadaan muodostettua. Hyötykuorma jää pienemmäksi sillä otsikkotiedot ovat UDP-protokollaa suuremmat. Tämän lisäksi pakettien kuittaus ja yhteydenmuodostus kuluttavat ylimääräisiä resursseja, joka vähentää hyötykuorman määrää.

Nämä kaksi protokollaa ovat OSI-mallin [31] siirtokerroksen tavallisessa tiedonsiirrossa yleisimmin käytetyt protokollat. Tämän sekä testiohjelmiston saatavuuden vuoksi protokollat valittiin osaksi koejärjestelyä.

7.2 Kokeiden tavoitteet

Ensimmäisen vaiheen kokeilla oli tavoitteena selvittää jonkinlainen perustaso käyttäen yksinkertaisia ja halpoja kuluttajaluokan laitteita. Samalla tavoitteena oli selvittää sopivat mittauskohteet ja parhaiten toimivat koejärjestelyt, jotta toisen vaiheen kokeet saatiin suoritettua mahdollisimman sujuvasti.

Toisessa vaiheessa käytössä oli teollisuusympäristöön suunnitellut laitteet, joilla päästiin selvittämään erityisesti voimakkaammin vahvistavien antennien vaikutusta signaalin kuuluvuuteen.

Yleisesti kokeiden tavoitteena oli selvittää WLAN-teknologian toimivuutta kyseisessä voimalaitosympäristössä. Erityisesti 5GHz-taajuuksien toimivuus verrattuna jo varsin yleisesti käytössä olevaan 2,4GHz-taajuusalueeseen oli

kokeissa kiinnostuksenkohteena. Jos 5GHz-taajuusalue osoittautuisi käyttökelpoiseksi, voitaisiin sitä hyödyntää WLAN-verkkojen toteutuksessa ja jättää jo valmiiksi ruuhkainen 2,4GHz-taajuusalue vähemmän kaistanleveyttä vaativille anturiverkoille.

7.3 Koevaiheet

7.3.1 Ensimmäinen vaihe: USB WLAN-sovittimet

Kokeet jaettiin kahteen osaan, ensimmäinen koe suoritettiin 2,4GHz-taajuusalueella, toinen 5GHz-taajuusalueella. Molemmat kokeet suoritettiin sekä B-voimalaitoksen kattilahallissa, että rikinpoistolaitoksella. Kokeissa mitattiin tukiaseman signaalin voimakkuus, vasteaika sekä pakettihäviö lähettimeltä tukiasemalle ja tiedonsiirtonopeus käyttäen sekä UDP-, että TCP-protokollaa. Näillä laitteilla mittaukset tehtiin kattilahallissa vain kerrosta alempana tukiasemasta, sillä jo tällä etäisyydellä yhteys havaittiin liian epävakaaksi. Kuuluvuus kartta on piirretty vielä tästä yhtä kerrosta alempaa. Rikinpoistolaitoksella mittaukset tehtiin aina samassa kerroksessa kuin tukiasema, ensin ylimmässä kerroksessa ja sen jälkeen n. laitoksen puolivälissä olevalla tasolla.

1. *koe, 2,4GHz laitteet ja asetukset*: 2 kpl kannettavia tietokoneita, 2 kpl USB-väylään liitettäviä WLAN-sovittimia, jotka käyttävät MediaTek (aiemmin Ralink) RT3573-piirisarjaa [99]. Sovittimissa on käytössä kolme ympärisäteilevää antennia, eli nopeimmillaan käytössä on kolme yhteyttä tukiaseman ja lähettimen välillä. Tällöin teoreettinen maksiminopeus on 450MBit/s. Yksi prosessitilan langattoman järjestelmän tavoitteista on tarjota riittävä tiedonsiirtokapasiteetti mahdollisimman pienellä määrällä tukiasemia. Kapasiteetin maksimoimiseksi tukiasema asetettiin käyttämään kahta samanaikaista kanavaa (7 ja 11), jolloin käytössä on yhteensä 40MHz kaistanleveys. Molempien tietokoneiden käyttöjärjestelmä on Windows 7, johon on asennettu kaikki saatavilla olevat päivitykset (Service Pack

1 + päivitykset) ja kirjoitushetkellä uusin piirisarjavalmistajan ajuriversio 5.1.7.0 langattomille sovittimille. Molemmista tietokoneista otettiin Windowsin oma palomuuri pois käytöstä mahdollisten yhteysongelmien välttämiseksi. Tukiasemana toimiva tietokone oli sijoitettu kokeiden ajaksi joko n. 1m korkuiselle metalliselle työskentelytasolle tai metalliselle ritilätasolle lattiakorkeudelle. Tukiasema oli sijoitettu siten, että antennit olivat pystysuunnassa. Tällöin radiokenttä suuntautuu voimakkaimmin vaakatasossa tukiaseman ympärille.

2. *koe, 5GHz*: käytössä samat laitteet kuin 1. kokeessa, mutta nyt käyttäen 5GHz taajuuksia. Tässäkin kokeessa tukiasema asetettiin käyttämään kahta 20MHz kanavaa, jolloin käytössä on siis yhteensä 40MHz kaistanleveys. Käytettävät kanavat olivat 36 ja 40. Tukiaseman sijoittelu on sama kuin ensimmäisessä kokeessa.

Ohjelmisto testeissä 1 ja 2:

- *siirtonopeus:* iperf v2.0.5 (Win32)
- *vasteaika ja pakettihäviö:* hrPing v5.06.1143
- *signaalin voimakkuus:* Ekahau HeatMapper v1.1.4.39795

Iperf-testi ajettiin prosessitilassa seuraavilla asetuksilla, jolloin käytössä on TCP-protokolla:

```
iperf -c x.x.x.x -w 128k -i 1 -t 20
```

Perusnopeus toimistossa mitattiin komennolla:

```
iperf -c x.x.x.x -w 128k -i 30 -t 600
```

Siirtonopeus UDP-protokollalla mitattiin seuraavilla asetuksilla:

```
iperf -c x.x.x.x -w 128k -l 1470 -u
-b XM -i 1 -t 20
```

Perusnopeus toimistossa mitattiin komennolla:

```
iperf -c x.x.x.x -w 128k -l 1470 -u
-b XM -30 1 -t 600
```

Näissä x.x.x.x on palvelimena toimivan tietokoneen IP-osoite ja X on teoreettinen maksimi kaistanleveys. Kuluttajaluokan laitteilla X oli 450 eli teoreettinen maksimi on 450 Mbit/s ja teollisuusluokan tukiasemalla X oli 100 johtuen Ethernet-portin maksiminopeudesta. Laitteiden lähetystehot selviävät taulukosta 1, valmistaja ei ilmoita antennien vahvistusta. Vasteaika ja pakettihäviö mitattiin n. 30s aikavälillä.

Taulukko 5, USB WLAN-sovittimien lähetystehot eri 802.11 standardeja käyttäen [100]

Nopeusluokka	Lähetysteho
b	22dBm
g	19-22dBm
n	19-22dBm
a/n	18-21dBm

7.3.2 Toinen vaihe: Teollisuus-luokan testilaitteisto

Tässä vaiheessa tehtiin samanlaiset testit kuin kannettavilla, mutta käyttäen teollisuusluokan tukiasemaa. Tukiasema oli DIN-kiskoon asennettavaa mallia ja siinä oli 3 kpl. ulkoisia antenneja, jotka oli asennettu samaan kiskoon n. 10 cm päähän toisistaan. Kyseisten antennien vahvistus on 2,4GHz-taajuudella 2,5dBi ja 5GHz-taajuudella 5dBi. Tukiasema asetettiin käyttämään korkeinta mahdollista lähetystehoa 23dBm (EIRP). Asemana käytettiin samaa laitetta kuin ensimmäisessä vaiheessa. Näillä laitteilla kattilahallin mittaukset tehtiin kolme kerrosta alaspäin tukiasemasta verrattuna kuluttajaluokan laitteiden yhteen. Rikinpoistolaitoksella mittaukset tehtiin samalla tavalla kuin kuluttajaluokan laitteilla.

Toimistotiloissa mitattuja perustiedonsiirtonopeuksia tarkastellessa tulee ottaa huomioon, että tukiaseman Ethernet-portit ovat nopeudeltaan 10/100 Mbit/s, eli korkein mahdollinen käytännön tiedonsiirtonopeus portteihin liitetyille laitteille on hieman alle 100 Mbit/s. Mittausohjelmistoja suorittavat kannettavat tietokoneet oli liitetty kokeita suorittaessa kyseisiin portteihin.

7.3.3 Mittaustulokset 2,4GHz

Mittaustulokset toimistotilassa **kuluttajaluokan laitteilla**:

Taulukko 6, 2,4 GHz mittaustulokset toimistotilassa kuluttajaluokan laitteilla

Pakettihäviö (%)	Vasteaika min./kesk./maks. (ms)	Tiedonsiirtonopeus TCP/UDP (MBit/s)
0	1,90 / 2,98 / 6,49	101 / 156

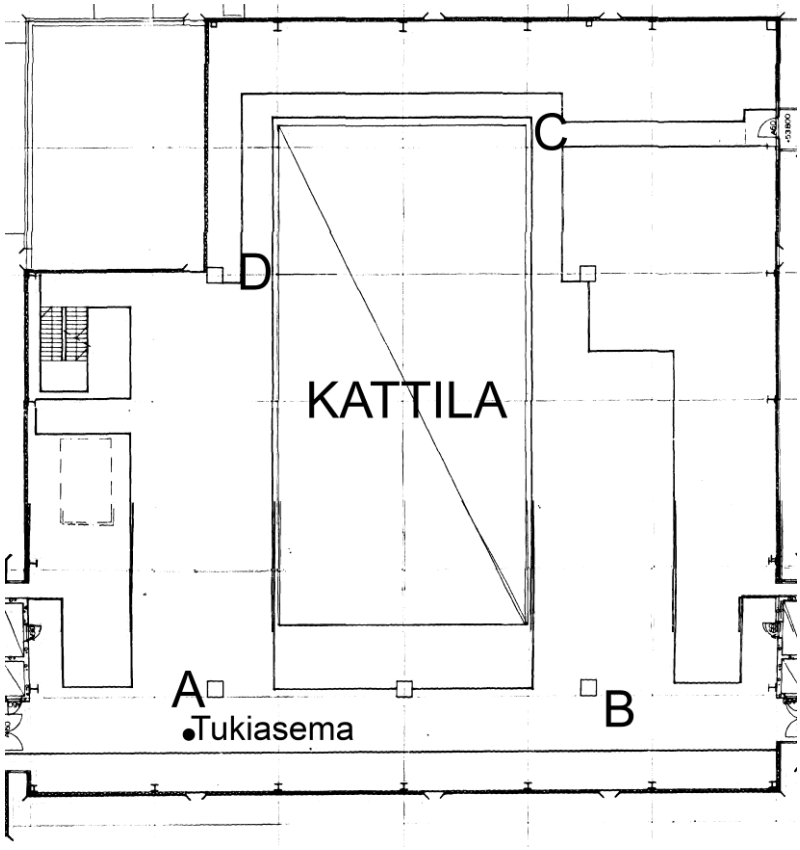
Mittaustulokset toimistotilassa **teollisuusluokan tukiasemalla:**

Taulukko 7, 5 GHz mittaustulokset toimistotilassa kuluttajaluokan laitteillak

Pakettihäviö (%)	Vasteaika min./kesk./maks. (ms)	Tiedonsiirtonopeus TCP/UDP (MBit/s)
0	1,86 / 2,57 / 6,03	68,7 / 98,3

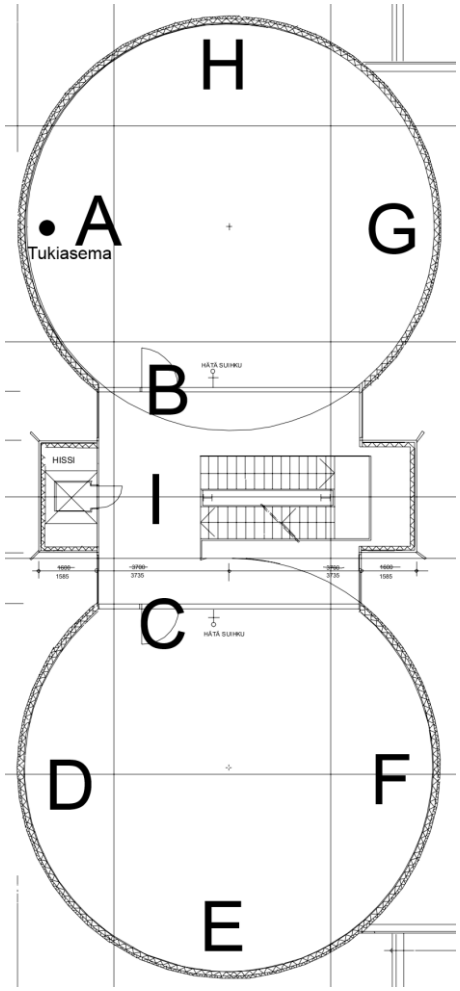
Laitoksen pohjapiirustus kerroksittain, johon on merkitty tukiaseman sijainti ja signaalinvoimakkuus eri etäisyyksillä ja eri kerroksissa kuin tukiasema löytyvät työn liitteistä (liitteet 2-23), metreinä esitetty lukema on tason korkeus merenpinnasta mitattuna. Värit kuvaavat vastaanotetun signaalin voimakkuutta (recieved signal strength indication, RSSI). Kuvat on piirretty automaattisesti Ekahau HeatMapper-ohjelmalla, joka päättelee tarkasteltavan tukiaseman sijainnin mittausten perusteella. Näihin kuviin on ohjelman toiminnasta johtuen piirretty myös muut samassa paikassa samaan aikaan kuuluvissa olleet tukiasemat, matalan signaalin voimakkuuden (alle 80dBm) vuoksi ne on piirretty kuvan reunaan. Tukiaseman todellinen sijainti kattilahallissa sekä tiedonsiirtonopeuksien ja vasteaikojen mittauspisteet

näkyvät kuvasta 13 ja vastaavat tiedot rikinpoistolaitokselle kuvissa 14 ja 15. Tukiasema sijoitettiin kattilahallin ylimpään kerrokseen ja mittaukset tehtiin vastaavissa pisteissä myös alemmissa kerroksissa. Rikinpoistolaitoksella tukiasema oli sijoitettu 5. kerroksessa n. 1m korkealle työtasolle ja 3. kerroksessa n. ½ kerrosta tason yläpuolella olevalle porrastasanteelle, jossa tukiasema sijoitettiin siten, että metallirakenteet olivat mahdollisimman vähän näköyhteyden tiellä. Tukiaseman sijainti on merkattu kuviin mustalla pallolla.



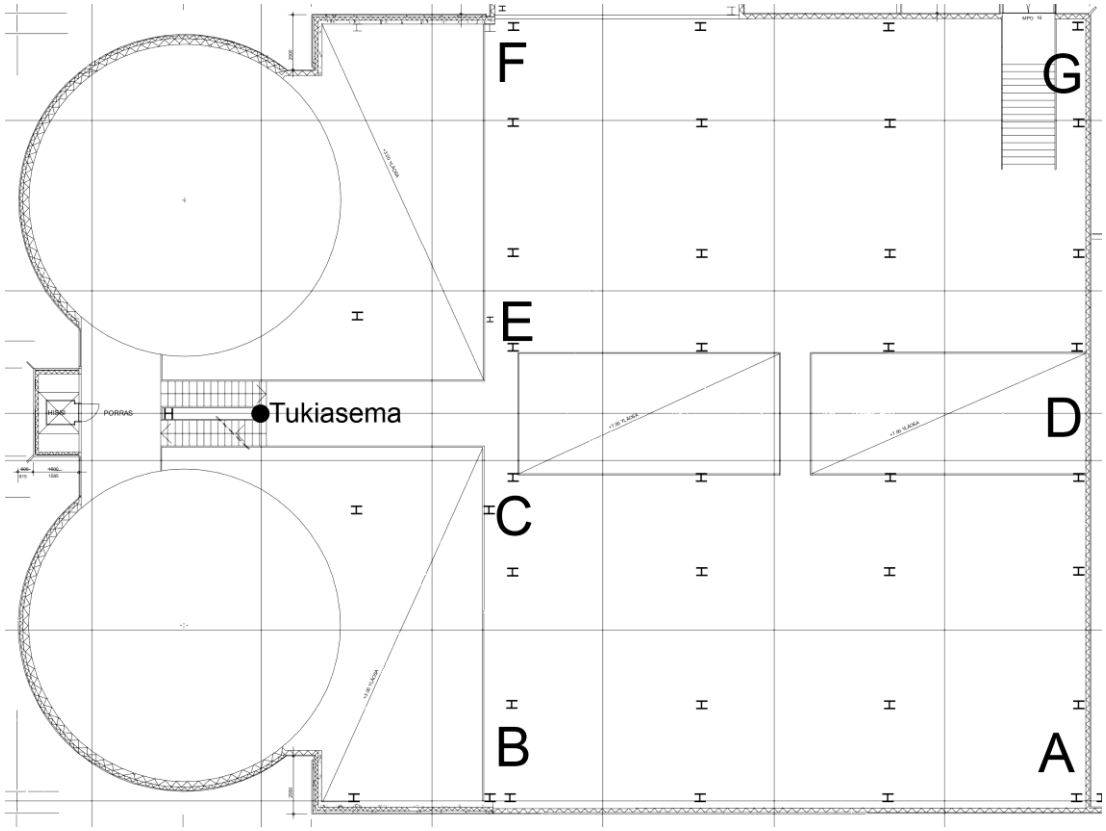
Kuva 13, Mittauspisteet ja tukiaseman sijainti kattilahallissa

Kattilahallin leveys on n. 38m (kuvassa 13 vasemmalta oikealle) ja syvyys n. 37m (kuvassa 13 alhaalta ylös), tukiaseman ja pisteen A välinen etäisyys on n. 2m, tukiaseman ja pisteen B n. 20,5m, tukiaseman ja pisteen C n. 34m, tukiaseman ja pisteen D n. 22m.



Kuva 14, Mittauspisteet ja tukiaseman sijainti rikinpoistolaitoksen ylimmässä kerroksessa

Kuvan 14 pyöreiden tilojen halkaisija on n. 11m ja niiden välinen etäisyys n. 3,5m, mittauspisteet on sijoitettu tilojen reunoille paitsi pisteet B ja C jotka ovat tiloihin johtavilla ovilla. Mittauspiste I on n. ½ kerrosta alemmalla porrastasanteella kuvassa näkyvällä kohdalla.



Kuva 15, Mittauspisteet ja tukiaseman sijainti rikinpoistolaitoksen 3. kerroksessa

Tukiasema on sijoitettu n. ½ kerrosta tasoa korkeammalle porrastasanteelle. Tilan leveys ja syvyys ovat n. 27m.

Liitteistä löytyvissä taulukoissa (liitteet 24-33) on esitetty mitatut vasteajat (minimi, keskiarvo, maksimi), vasteaikamittauksen pakettihäviö sekä tiedonsiirtonopeudet käyttäen TCP- ja UDP-protokollia. Tulokset on jaettu mittauspaikan (kattilahalli/rikinpoistolaitos) ja mittaustason mukaan. Taulukot ovat laskevassa numerojärjestyksessä ylimmästä kerroksesta alimpaan, eli järjestys on sama kuin missä mittaukset tehtiin.

7.3.4 Mittaustulokset 5GHz

Mittaustulokset toimistotilassa **kuluttajaluokan laitteilla**:

Taulukko 8, 2,4 GHz mittaustulokset toimistotilassa teollisuusluokan laitteilla

Pakettihäviö (%)	Vasteaika min./kesk./maks. (ms)	Tiedonsiirtonopeus TCP/UDP (MBit/s)
0	1,40 / 1,97 / 3,05	111 / 217

Mittaustulokset toimistotilassa **teollisuusluokan tukiasemalla:**

Taulukko 9, 5 GHz mittaustulokset toimistotilassa teollisuusluokan laitteilla

Pakettihäviö (%)	Vasteaika min./kesk./maks. (ms)	Tiedonsiirtonopeus TCP/UDP (MBit/s)
0	1,86 / 2,26 / 2,58	68,5 / 98,0

Prosessitiloissa tehtyjen mittausten tulokset löytyvät liitteistä (liitteet 34-43).

7.4 Havainnot ja päätelmät

Kuluttajaluokan laitteilla havaittiin jo alkuvaiheissa, että ympärisäteilevät antennit ovat ongelmallisia tiloissa, joissa signaali pääsee heijastumaan ja taittumaan erisuuntaisista pinnoista. Varsinkin 2,4GHz-taajuusalueella WLAN-laitteiden tiedonsiirtokykyä oli vaikea ennustaa etukäteen. 5GHz-taajuusaluetta käytettäessä signaalin kantama heikkeni nopeammin, mutta heikkeneminen oli paremmin ennalta arvattavaa kuin 2,4GHz-taajuusalueella. Näköyhteydestä huolimatta tiedonsiirto voi olla todella hidasta tai jopa täysin olematonta. Esimerkiksi kattilahallissa tukiaseman ollessa sijoitettuna hallin nurkkaan, voi tiedonsiirto toimia yhdellä hallin reunalla toimia täysin riittävällä nopeudella ja varmuudella, kun taas toisella reunalla signaali voi olla käyttökelvoton. Tämä siitä huolimatta, että molemmissa tapauksissa on suora näköyhteys tukiasemaan. Tässä kannattaa huomata sekä Fresnelin-alueen, että monitie-etenemisen vaikutus signaalin käyttökelpoisuuteen. Vaikka laitteiden välillä on näköyhteys, on hyvin mahdollista, että Fresnelin-alueella on esteitä. Suurimmassa osassa esimerkiksi kattilahallia kulkutasot eivät ole täysin tyhjiä. Tämän lisäksi myös monitie-eteneminen vaikuttaa signaalin etenemiseen, signaali heijastuu metallisista pinnoista ja saapuu vastaanottajalle useaa eri reittiä. Vaikka vastaanottava asema tukee MIMO-tekniikkaa, ei tällaista kuluttajaluokan laitetta ole suunniteltu teolliseen ympäristöön. Pienet lähekkäin sijoitetut antennit eivät kykene erottelemaan eri signaaliteitä riittävästi ja tällöin interferenssi on destruktiivista. On myös hyvä huomata ero aseman kuuleman signaalin ja käytännössä saavutetun tiedonsiirtonopeuden välillä. Kuuluvuuskartat näyttävät signaalin voimakkaana vielä kaksi kerrosta tukiasemasta alempana, mutta tiedonsiirto ei tällä etäisyydellä enää onnistunut. Rikinpoistolaitoksessa tiedonsiirto oli hankalaa jo samassa kerroksessa johtuen suuresta määrästä erilaisia metallisia rakenteita. Kuten aiemmin mainittiin tiedonsiirtonopeus- ja vasteaikamittaukset lopetettiin kattilahallissa jo yksi kerros tukiasemasta alaspäin, sillä tiedonsiirto kuluttajaluokan laitteilla havaittiin toimimattomaksi jo tällä etäisyydellä. Toimimattomuus varmistettiin vielä yksittäisillä mittauksilla alemmissa kerroksissa.

Teollisuusluokan laitteita käytettäessä havaittiin heti huomattava parannus erityisesti tiedonsiirron ennalta arvattavuuteen. Toisin kuin kuluttajille suunnatuilla laitteilla, ei mittauksissa havaittu lainkaan kohtia, joissa signaali olisi täysin kuulumattomissa tai tiedonsiirto olisi mahdotonta. Verrattuna kuluttajaluokan laitteisiin on todennäköistä, että tiedonsiirto olisi onnistunut vielä alemmillakin kerroksilla. Koealue rajattiin kuitenkin tähän, sillä tukiaseman palveleman alueen kasvaessa myös palveltavien asemien määrä kasvaa jolloin yksittäisen tukiaseman kapasiteetti voi ylittyä[18]. Tiedonsiirtonopeus laski myös varsin tasaisesti etäisyyden tukiasemaan kasvaessa ilman läheskään samanlaista nopeudenvaihtelua kuin kuluttajaluokan laitteilla.

Joissain mittapisteissä havaittiin tiedonsiirron onnistuvan vain käyttäen UDP-protokollaa. Samoissa pisteissä havaittiin korkeita pakettihäviöitä. On todennäköistä, että pakettihäviön ollessa useita kymmeniä prosentteja, ei TCP-protokolla kykene muodostamaan yhteyttä vastaanottajaan yhteydenmuodostuspakettien hävitessä matkalla. Koska UDP-protokolla on yhteydetön, saa se lähetettyä ainakin osan paketeista vastaanottajalle. Ilmiö havaittiin lähinnä kuluttajaluokan laitteilla. Käytännön hyöty havainnosta on lähinnä se, että vaikeissa olosuhteissa voidaan edelleen tarjota jonkin tasoinen yhteys sovelluksille, jotka eivät vaadi kaikkien pakettien saapumista vastaanottajalle. Tuotantokriittisiin järjestelmiin tällainen ei kuitenkaan ole hyväksyttävää. Protokollien välinen ero oli suurin kuluttajaluokan laitteita käytettäessä, teollisuuskäyttöön tarkoitetuilla laitteilla protokollien väliset erot tasaantuivat, eikä UDP-protokolla enää ollut välttämättä nopeampi jokaisessa mittauspisteessä. Syytä tähän ei voi yksiselitteisesti sanoa, mutta ero voi johtua esimerkiksi tavasta, jolla laitteet käsittelevät paketteja tai jostain muusta ohjelmisto- tai laite-erosta.

Kokeita suoritettaessa erityisesti 230V-verkkovirtaa tarvitsevien tukiasemien tapauksessa virransaanti oli hieman hankalaa ja vaati pitkiä väliaikaisia kaapeleita. Kiinteissä asennuksissa tätä ongelmaa ei kuitenkaan pitäisi olla. WLAN-tukiasemien fyysiseen asennukseen liittyvät merkittävimmät haasteet

ovat asetettujen tiedonsiirtovaatimusten täyttäminen ja näiden vaatimusten perusteella valituille asennuspaikoille tarvittava mahdollinen Ethernet-kaapelointi ja sähkösyöttö. Voimalaitosympäristössä on yleensä tarjolla eri jännitettä syöttäviä sähkökeskuksia joten sähkönsaanti ei pitäisi olla ongelma. Jos tukiasemien kanssa voidaan käyttää muuntajia, voidaan syöttöjännite valita lähimmän sähkökeskuksen mukaan ja siten alentaa kaapelointikustannuksia. Fyysinen asennus voidaan tehdä DIN-kiskoon, jolloin asennuspaikka voi olla esimerkiksi yhteinen automaatiolaitteiden kanssa. Fyysistä paikkaa valitessa tulee ottaa huomioon laitteiden käyttölämpötilat sekä IP-suojausluokat. Voimalaitoksessa on paikkoja, joissa ilman lämpötila on korkea tai ilmassa on paljon pölyä. Koska WLAN-verkko halutaan hyvin todennäköisesti liittää osaksi jotakin langallista verkkoa, tarvitaan ainakin osalle tukiasemista myös datakaapeli. Jos kaapelointia halutaan välttää, voidaan osa tukiasemista liittää verkkoon vain langattomasti, jolloin niille tarvitaan vain sähkösyöttö. Kaapeloinnin vähentämiseksi voidaan sähkösyöttö toteuttaa Power-over-Ethernet-tekniikalla, jolloin käyttöjännite tuodaan tukiasemalle käyttäen datakaapelia.

Koetulosten perusteella voidaan sanoa, että yhden tukiaseman kantama on niin suuri, että ainakin pienillä käyttäjämäärillä esimerkiksi kattilahallissa yksi tukiasema riittää palvelemaan neljää kerrosta neljästätoista. Tämä tarkoittaisi, että koko kattilahallin peittävä verkko voitaisiin toteuttaa vähimmillään neljällä tukiasemalla käyttäen 5GHz-taajuusaluetta. Tässä tapauksessa vielä pisimmälläkin etäisyydellä tukiasemasta saavutetaan yli 10Mbit/s tiedonsiirtonopeus ja alle 10ms vasteaika. Jos on tarpeen nostaa tiedonsiirtokapasiteettia, tulee tukiasemia asentaa tiheämmin jolloin radiokanavien uudelleenkäyttöön tulee kiinnittää huomiota. Tällöin voi olla tarpeen laskea tukiasemien lähetystehoa, jos samaa kanavaa käyttävät tukiasemat joudutaan asentamaan toistensa kuuluvuusalueille. Suurempi määrä tukiasemia ja niihin liittyneitä käyttäjiä kasvattaa tiedonsiirtovaatimuksia myös tukiasemien väliselle langalliselle runkoverkolle. Onkin hyvä tiedostaa tiedonsiirtokapasiteetin rajoitukset sekä langattomassa, että langallisessa verkossa mahdollisia sovelluskohteita suunnitellessa.

Tukiasemien määrän kasvaessa kasvavat myös asennuskustannukset lisäkaapeloinnista sekä mahdollisista päivitystarpeista langalliseen runkoverkkoon johtuen.

Lopullisena johtopäätöksenä käytännönkokeista voidaan sanoa WLAN-tekniikan soveltuvan tiedonsiirtoon voimalaitosympäristössä sekä 2,4GHz-, että 5GHz-taajuusalueilla teollisuuskäyttöön suunnitelluilla laitteilla. Näistä erityisesti jälkimmäinen on tulevaisuuden kannalta positiivinen lopputulos 2,4GHz-taajuusalueen ruuhkaisuudesta johtuen. 5GHz-taajuusaluetta käytettäessä joudutaan kokeiden perusteella tyytymään hieman pienempään kuuluvuusalueeseen ainakin vastaanotetun signaalin voimakkuuden perusteella mitattuna, mutta joissain tapauksissa tiedonsiirtonopeudet ovat jopa 2,4GHz-taajuuksia vakaampia. Tiedonsiirron vakaus ja ennustettavuus ovatkin erityisesti automaatiokäytössä tärkeitä ominaisuuksia. Edellä mainitut varaukset liittyvätkin juuri radiotien vaikeaan ennustettavuuteen verrattuna langalliseen tiedonsiirtoon. Ulkoiset tekijät voivat vaikuttaa heikentävästi tiedonsiirron onnistumiseen. Tässäkin kohdassa on vielä hyvä muistuttaa, että tietoturvan kannalta WLAN-verkot ovat kirjoitushetkellä luottamuksellisuutensa ja eheytensä kannalta hyvällä tasolla. Radiohäirintään perustuva hyökkäys voi kuitenkin vaarantaa WLAN-verkon saatavuuden. Tästä riskistä johtuen käytännössä mitään langatonta tiedonsiirtoa ei voi täysin varauksettomasti suositella ainoaksi ratkaisuksi kriittisten järjestelmien tiedonsiirtoon, varsinkaan tuotantovarmuuskriittisessä ympäristössä. WLAN-tekniikan sopivimmat sovelluskohteet löytyvät mielestäni ei-kriittisistä järjestelmistä, joiden tarkoitus on esimerkiksi tuoda tietoa langattomasti saataville työnteon tehostamiseksi tai tuoda jotakin ei-kriittistä tietoa kentältä esimerkiksi kamerakuvaa tai mittaustietoa.

8. Johtopäätökset ja tulevaisuuden näkymät

Tässä kappaleessa esitellään työn aikana kohdattuja langattomuuteen liittyviä ongelmia, haasteita ja lopullinen toteutuskonsepti. Lisäksi esitetään mahdollisia tulevaisuuden näkymiä.

8.1 Ongelmat ja haasteet

Työssä kohdatut ongelmat ja haasteet:

- Ensimmäinen haaste tavoiteltaessa suuria tiedonsiirtonopeuksia oli riittävän peiton saavuttaminen. Mittaustuloksista voidaan päätellä, että jos tavoitteena on esimerkiksi koko voimalaitoksen kattava langaton tiedonsiirtoverkko, on tarvittavien tukiasemien määrä varsin huomattava. Tukiasemien määrän kasvattaminen lisää asennuskustannuksia sekä runkoverkolta vaadittavaa tiedonsiirtokapasiteettia. Toisaalta yksittäisen ja yhtenäisen tilan kattavan verkon toteutus ei vaadi esimerkiksi koeympäristönä olleen kattilahallin tapauksessa kuin 4 tukiasemaa pienillä tiedonsiirtomäärillä.
- Odotuksista ehkä hieman poiketen signaalin heijastuminen tuntui aiheuttavan enemmän ongelmia prosessitiloissa kuin signaalin vaimeneminen. Toisaalta ilmeni myös tapauksia, joissa heijastumien avulla signaali saatiin kuulumaan yllättävän kaukana tukiasemasta. Tämä ongelma oli huomattavin kuluttajaluokan laitteilla ja siirtyminen teollisuusluokan laitteisiin ratkaisi kuuluvuusongelmat lähes täysin.
- Vaikka langattomien verkkojen tietoturva on muuten hyvällä tasolla luottamuksellisuuden ja eheyden kannalta, voi riittävän saatavuuden saavuttaminen olla ongelmallista. Ainakin teoriassa riittävän voimakas häiriösignaali voi estää kaiken langattoman tiedonsiirron tietyllä taajuusalueella, eli langallista tiedonsiirtoa täysin vastaavaa toimintavarmuutta ei voida saavuttaa. Tämä estää langattomien verkkojen käytön kriittisimmissä järjestelmissä.

8.2 Langattomien järjestelmien toteutuskonsepti

- Radiotekniikka ja taajuusalue valitaan käyttökohteen mukaan. Ennen lopullista valintaa olisi hyvä päästä tekemään mittauksia eri tekniikoilla. Vaikka yleisesti voidaan todeta radioaaltojen etenevän tietyllä tavalla eri taajuuksilla, tämän työn puitteissa tehdyissä mittauksissa havaittiin radioympäristön olevan suhteellisen vaikeasti ennustettava varsinkin pidemmillä etäisyyksillä. Tästä huolimatta WLAN-tekniikka havaittiin toimivaksi.
- Radioympäristö ja sen muutokset ajan myötä. Jatkuva tekniikan kehitys tuo markkinoille lisää langattomia laitteita. Tämä lisää liikennettä, ja siten myös häiriöitä, erityisesti lupavapailla taajuuksilla. Radioympäristöön liittyy oleellisesti myös koeksistenssi samaa taajuusaluetta käyttävien laitteiden välillä. Langattomia järjestelmiä suunnitellessa tulee huomioida, että toistensa kuuluvuusalueella olevat samaa taajuutta käyttävät verkot vaikuttavat toistensa toimintaan. Koeksistenssi eri standardien välillä ei ole täysin ratkaistu ongelma, joten samojen taajuuksien käyttöä tulisi välttää mahdollisuuksien mukaan.
- Verkon mitoitus tehdään sovelluskohteen mukaan. Tähän tarvitaan alustava selvitys siitä, mitä laitteita verkkoon on aikomus liittää ja kuinka paljon käyttäjiä verkolle on kaavailtu. Tämän perusteella voidaan laskea tarvittavien tukiasemien määrä ja suunnitella sen perusteella laitteiden asennuspaikat ottaen huomioon radiotaajuuksien uudelleenkäyttö. Tukiasemien määrän perusteella mitoitetaan myös tukiasemat toisiinsa liittävä runkoverkko.
- Liitännät muihin järjestelmiin ja verkkoihin selvitetään. Tähän tarvitaan selvitys siitä mihin tietoa halutaan viedä ja kuinka paljon.
- Tietoturva-analyysi, perusselvitys voidaan tehdä hieman laajennetun CIA-mallin perusteella. Kun perusasiat ovat selvillä, voidaan tietoturvaan perehtyä yksityiskohtaisemmin esimerkiksi teollisuuden tietoliikenneverkkojen tietoturvajärjestelmän määrittelevän IEC-standardin tai organisaation omien vaatimusten perusteella.

- Riskianalyysi tehdään mahdollisten tietoturvapoikkeamien pohjalta. On selvitettävä mitä tietoja voi paljastua mahdollisen tietomurron yhteydessä. Nykytilanteen valossa on otettava huomioon myös Stuxnet-tyylinen jatkuva edistynyt uhka (Advanced persistent threat, APT), jossa hyökkääjä pääsee toimimaan järjestelmissä pitkällä aikavälillä. Langattomissa järjestelmissä palvelunestohyökkäykset ovat täysin erilainen uhka verrattuna langoitettuihin verkkoihin. Langoitetussa verkossa uhka kohdistuu verkon ulkoreunaan eli siihen verkon osaan, joka on yhteydessä Internetiin. Prosessin toiminnan kannalta kriittistä prosessiverkkoa ei yleensä liitetä suoraan julkiseen Internetiin eli ongelma voidaan välttää kokonaan. Langattomia verkkoja vastaan voidaan kuitenkin teoriassa aina tehdä ns. tyhmä palvelunestohyökkäys. Radiosignaalia voidaan häiritä riittävän voimakkaalla lähettimellä siten, että tiedonkulku häiriintyy tai estyy kokonaan.
- Elinkaari, takaisinmaksuaika. Voimalaitosjärjestelmissä on totuttu pitkiin, jopa useiden vuosikymmenien mittaisiin, elinkaarien pituuksiin. Tietotekniikan nopea kehitys tarkoittaa kuitenkin sitä, että langattomia tekniikoita hyödyntäessä näin pitkiä elinkaaria tuskin tullaan saavuttamaan. Laitteiden elinkaari vaikuttaa suoraan kustannusten ja takaisinmaksuajan arviointiin. Lyhyempää elinkaarta tulee verrata mahdollisiin langattomuuden tuomiin kustannussäästöihin ja työtehon parannuksiin. Työtehon parannuksia voi tosin olla hankala arvioida suoraan rahallisesti, mutta suuntaa antavia arvioita voidaan tehdä esimerkiksi arvioimalla säästynyttä työaikaa.
- Hyötyanalyysi. Kuten työssä on jo todettu, ei langattomuuden tule olla itsetarkoitus. Mahdollisia käyttökohteita tutkittaessa tulee mahdolliset hyödyt punnita ongelmia vastaan. Erityisesti tietoturva on sellainen tekijä, joka puoltaa langallisia ratkaisuja langattomien sijasta. Koska verkon saatavuutta ei radiotien avoimen luonteen vuoksi voi täysin varmistaa, on kriittisimmät järjestelmät rajattava pois mahdollisista sovelluskohteista.

8.3 Tulevaisuuden kehitys- ja tutkimusmahdollisuuksia

Tietoturvan kannalta voisi olla hyödyllistä mitata signaalien läpäisy ulkoseinien suhteen, ja tarkastella kuinka pitkälle signaalit kantavat ulos voimalaitosalueelta. Käytännön kokeissa havaittiin ulkopuolisten WLAN-verkkojen kuuluvan erityisesti prosessitiloihin erityisesti ikkunoiden kohdilla. Tulevaisuudessa olisi myös mielenkiintoista tehdä vielä kattavampia mittauksia 5GHz-taajuusalueella nyt saatujen positiivisten tulosten innoittamana. Jos osa, tai jopa kaikki, liikenteestä voidaan siirtää pois 2,4GHz-taajuusalueelta voitaisiin koeksistenssi-ongelmia erityisesti 802.15.4-standardin laitteiden kanssa eliminoida lähes kokonaan. Tämä helpottaisi mahdollisimman kattavan järjestelmän toteuttamista, anturiverkot voisivat käyttää pääasiassa 2,4GHz-taajuuksia ja WLAN-verkot 5GHz-taajuuksia. Toki ulkopuoliset häiriöt varsinkin 2,4GHz-taajuusalueella olisi otettava huomioon, mutta tähän helpotusta tuo voimalaitoksen suhteellinen etäisyys laitosalueen ulkopuolisista häiriölähteistä sekä ulkopuolisia signaaleja vaimentavat rakenteet, erityisesti metalliset seinät. Jos tämäkään ei riitä, voidaan joitain yhteyksiä toteuttaa 433MHz- ja 868MHz-taajuuksia käyttävillä laitteilla. Näillä alueilla ei tämän työn puitteissa päästy tekemään käytännön mittauksia, mutta näillä alueilla ei ole samalla tavalla saatavilla kuluttajille suunnattuja laitteita. Viranomaiset ovat myös asettaneet tiukemmat rajoitukset lähetysteholle ja toiminta-ajalle, eli näillä taajuusalueilla ei pitäisi olla samalla tavalla ruuhkaa kuin 2,4GHz-taajuusalueella.

On kuitenkin hyvä huomata, että tässä vaiheessa ei voida vielä varmuudella arvioida mitä tulevaisuus tuo tullessaan 5GHz-taajuusalueelle. Näiden taajuuksien käyttö on yleistynyt valmistajien tuodessa markkinoille niitä tukevia laitteita. Toistaiseksi tukea 5GHz-taajuuksille ei löydy ainakaan hieman vanhemmista laitteista, mutta tilanne muuttuu kuitenkin koko ajan laitekannan päivittyessä. 2,4GHz-tuki löytyy käytännössä kaikista WLAN-yhteensopivista laitteista. 2,4GHz-taajuusalueen ruuhkaisuus voi kuitenkin kiihdyttää siirtymistä 5GHz-taajuusalueelle. Vaikka 5GHz-taajuusalueella onkin käytössä laajempi taajuusalue, voidaan samalla käyttää myös leveämpää kaistaa.

Työssä keskityttiin lähinnä vain WLAN- ja anturiverkkoteknologiaan, mutta työssä selvitetyt tekijät pätevät suuriltaosin myös muihin langattomiin tekniikoihin. Tulevaisuuden tutkimusta voisikin laajentaa käsittämään vasta tulossa olevia teknologioita, kuten viidennen sukupolven (5G, fifth generation) mobiiliverkot sekä uudet 60GHz-taajuusalueella toimivat WLAN-verkot. Varsinkin WLAN-verkkojen tapauksessa siirtyminen pois ruuhkaiselta 2,4GHz-taajuusalueelta olisi varsin suotavaa. Kuten työssä on mainittu nykyiset standardit tukevat toimintaa myös 5GHz-taajuusalueella, jossa mielestäni olisi paljon hyödyntämispotentiaalia. Mittaustulokset osoittivat 5GHz-taajuuksien toimivan joissain tapauksissa jopa paremmin kuin 2,4GHz-taajuudet. Potentiaali onkin suuri juuri prosessitiloissa, joissa signaali ei niinkään vaimene paksuihin rakenteisiin, vaan heijastuu metalliseinistä ja esineistä.

Vielä pitkälti kehitysvaiheessa oleva Internet of things (IoT) tai esineiden Internet-konsepti [101] voi myös tarjota hyödyntämismahdollisuuksia voimalaitosympäristössä. Konseptin ajatus on varustaa kaikki fysikaalisen maailman esineet yksilöllisellä tunnisteella, jonka perusteella niistä saadaan langattomasti tietoa. Mahdolliset sovelluskohteet kattavat useita eri aloja liikenteestä maanviljelyyn, mutta näitä yhdistävä tekijä on toiminnan tehostaminen laajamittaisen tiedonkeruun kautta sekä erilaisten verkkoteknologioiden yhtenäistäminen [102]. RFID-tekniikka nähtiin alun perin pohjana konseptille, jonka perusteella voidaan merkitä ja seurata sekä asioiden, että ihmisten sijaintia. Tiedonsiirto ja tunnistaminen eivät kuitenkaan ole suoraan sidottu RFID-tekniikkaan vaan molempiin voidaan hyödyntää muitakin teknisiä ratkaisuja. Tunnisteena voidaan käyttää IP-osoitteita ja tiedonsiirtoon mitä tahansa pienitehoisiin laitteisiin soveltuvaa tiedonsiirtoprotokollaa. Tällä hetkellä ei ole vielä yhtä yhteistä standardia tällaiselle IoT-tekniikalle, mutta kehityksen edetessä tilanne tulee varmasti muuttumaan. Jos konsepti saadaan standardoitua riittävän tietoturvalliseksi ja helposti käyttöönotettavaksi, voisi sen tarjoamille teknisille ratkaisuille olla käyttöä myös voimalaitosympäristössä. Sovelluskohteena ei välttämättä ole olla osana prosessia tai muuten tuotantokriittisessä roolissa, vaan tukemassa

ja tehostamassa työntekoa. Yhtenä mahdollisuutena voisi olla erittäin pitkälle hajautettu tiedonkeruu ympäristöstä käyttäen yksinkertaisia laitteita. Tämä tieto voisi palvella jotakin automaatiojärjestelmän osaa, esimerkiksi kiinteistöautomaatiota. Toisaalta pieniä langattomia tunnisteita voitaisiin hyödyntää varastotilanteen seurantaan tai omaisuudenhallintaan. Kappaleessa 2.4.4 mainittu IEEE 802.11ah-standardi voisi olla yksi mahdollinen tekninen ratkaisu IoT:n eteenpäin viemiseen. Sen tarkoituksena on tarjota pitkän kantaman langatonta tiedonsiirtoa pienitehoisille laitteille, aiempia WLAN standardeja matalammilla taajuusalueilla.

Enemmän teolliseen ympäristöön soveltuva konsepti voisi olla teollinen Internet, joka pyrkii yhdistämään koneoppimisen, big data-konseptin, M2M (machine-to-machine)-kommunikaation ja edellä mainitun esineiden Internetin ja siten tuottamaan ja hyödyntämään suuren määrän tietoa teollisuuden tarpeisiin. Tavoitteena on yhdistää suuri määrä ”tyhmiä” laitteita yhdeksi älykkääksi järjestelmäksi, jonka toimintaa voidaan optimoida tehokkaammin [103]. Järjestelmään sisältyvän älyn vuoksi teollinen Internet voidaan mieltää korkeamman tason konseptiksi kuin IoT, joka keskittyy enemmän tiedon tuottamiseen.

Viimeisenä voidaan mainita 5G (5th Generation) eli viidennen sukupolven matkapuhelinverkkoihin suunnitellut Machine Type Communications [104] ominaisuudet, joiden on tarkoitus parantaa matkapuhelinverkkojen soveltuvuutta laitteiden väliseen (machine-to-machine) tiedonsiirtoon. Tavoitteena on mahdollistaa useiden tuhansien laitteiden kytkeminen samaan langattomaan verkkoon ja siten yhtenäistää langatonta tiedonsiirtoa. Teknisesti toteutustapa voisi sisältää useita erilaisia tekniikoita (mobiili, WLAN, WPAN), jolloin radiokaista voitaisiin hyödyntää mahdollisimman tehokkaasti. Toteutuessaan nämä ominaisuudet voisivat tarjota sovellusmahdollisuuksia sekä automaatiokäytössä, että laajemmin Internet of Things-tyyppisessä konseptissa, johon sisältyy myös automaatiojärjestelmään kuulumattomia toimintoja ja järjestelmiä.

Lähdeluettelo

[1] P. Turunen, J. Uddfolk ja T. Viskari, ”Voimalaitosautomaatio,” tekijä: *Voimalaitosautomaation järjestelmät*, Suomen Automaatioseura ry, 2007, pp. 184 - 210.

[2] P. Radmand, A. Talevski, S. Petersen ja S. Carlsen, ”Comparison of Industrial WSN Standards,” tekijä: *4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010)*, 2011.

[3] W. Dargie ja C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, John Wiley & Sons, Inc., 2010.

[4] M. Paavola ja K. Leiviskä, ”Wireless Sensor Networks in Industrial Automation,” In-Tech, Vukovar, 2010.

[5] ITU-R, *SM.1896 : Frequency ranges for global or regional harmonization of short-range devices (SRDs),* 2011.

[6] IEEE, *802.11-2007 IEEE Standard for Information Technology - Specific Requirements - Part 11: Wireless Local Area Network Medium Access Control and Physical Layer 802.11,* 2007.

[7] IEEE, *IEEE Standard for Information Technology - Specific Requirements - Part 15.4: Wireless Medium Access Control and Physical Layer Specifications for Low Rate Personal Area Networks IEEE 802.15.4-2006,* 2006.

[8] M. Felser, ”The Fieldbus Standards: History and Structures,” University of Applied Science Berne, Bern.

[9] J. Nikunen, ”Langattomat tekniikat teollisuudessa,” *Automaatioväylä,* nro 3, pp. 8 - 10, 2011.

[10] A. Buda, V. Schuermann ja J. F. Wollert, ”Wireless Technologies in Factory Automation,” tekijä: *Factory Automation*, InTech, 2010, pp. 29-50.

[11] HART Communication Foundation, *HART Field Communication Protocol Specification, Revision 7.0,* 2007.

[12] ISA, *Wireless Systems for Industrial Automation: Process Control and Related Applications ISA-100.11a-2009 Standard,* 2009.

[13] ZigBee Alliance, *ZigBee PRO Specification,* 2007.

[14] Viestintävirasto, *Radiotaajuusmääräys 4 Q/2013 M,* Helsinki: Viestintävirasto, 2013.

[15] Viestintävirasto, *Taajuusjakotaulukko (liite määräykseen M4Q),* Helsinki: Viestintävirasto, 2013.

[16] ISO/IEC, *ISO/IEC 18000-7:2009 Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz,* 2010.

[17] S. Petersen ja S. Carlsen, ”WirelessHART Versus ISA100.11a - The Format War Hits the Factory Floor,” *IEEE Industrial Electronics Magazine,* pp. 23-34, 2011.

[18] M. S. Gast, 802.11n: A Survival Guide, O'Reilly Media Inc., 2012.

[19] IEEE, *802.11n IEEE Standard for Information Technology - Specific Requirements - Part 11: Wireless Local Area Network Medium Access Control and Physical Layer Specifications Amendment 5: Enhancements for Higher Throughput,* 2009.

[20] Cisco Systems Inc., ”802.11ac: The Fifth Generation of Wi-Fi - Technical White Paper,” Cisco Systems Inc., 2012.

[21] M. S. Gast, 802.11ac: A Survival Guide, O'Reilly Media Inc., 2013.

[22] Institute for Telecommunication Sciences, *Federal Standard 1037C, "Telecommunications: Glossary of Telecommunication Terms",* Boulder, Colorado, 1996.

[23] The Institute of Electrical and Electronics Engineers, ”IEEE Std. 100 The Authoritative Dictionary of IEEE Standards Terms, 7th Edition,” New York, 2000, p. 391.

[24] M. Johansson ja R. Jäntti, ”Networked Control Systems,” tekijä: *Wireless Networking for Control: Technologies and Models*, Lontoo, Springer London, 2010, pp. 31 - 74.

[25] H. T. Friis, ”A Note on a Simple Transmission Formula,” *Proceedings of the I.R.E. and Waves and Electrons,* pp. 254 - 256, 1946.

[26] T. S. Rappaport, Wireless communications principles and practices, Prentice-Hall, 2002.

[27] United States Department of Commerce National Telecommunications & Information Administration, *Federal Standard 1037C Telecommunications: Glossary of Telecommunication Terms: Fresnel zone,* 1996.

[28] United States Department of Commerce National Telecommunications & Information Administration, *Federal Standard 1037C: Telecommunications: Glossary of Telecommunication Terms: Knife-edge effect,* 1996.

[29] IEEE, *IEEE P802.11ac/D1.1,* 2011.

[30] S. Hallenberg, *Langattoman IEEE 802.11-lähiverkon tietoturva,* Helsinki: Helsingin Yliopisto, Tietojenkäsittelytieteen laitos, 2012.

[31] ISO/IEC, *ISO/IEC 7498-1 Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,* ISO/IEC, 1996.

[32] WiFi Alliance, ”WiFi Alliance,” [Online]. Available: http://www.wi-fi.org. [Haettu 3 Syyskuu 2014].

[33] IEEE, *802.11-1997 IEEE Standard for Information Technology - Specific Requirements - Part 11: Wireless Local Area Network Medium Access Control and Physical Layer 802.11,* 1997.

[34] J. Berg, ”The IEEE 802.11 Standardization Its History, Specifications, Implementations, and Future,” 2011.

[35] T. Alexander, ”Optimizing and Testing WLANs: Proven Techniques for Maximum Performance,” Newnes, 2007.

[36] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition, O'Reilly Media Inc., 2005.

[37] IEEE, *802.11a-1999 High speed Physical Layering the 5GHz band,* 1999.

[38] IEEE, *802.11b-1999 Supplement to IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical L,* 2000.

[39] IEEE, *802.11g-2003: Further Higher Data Rate Extension in the 2,4 GHz Band,* 2003.

[40] IEEE, *802.11ad-2012: Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band,* 2012.

[41] IEEE, *802.11ah: Amendment - Sub 1 GHz License-Exempt Operation,* 2010.

[42] S. Weiping, C. Munhwan ja C. Sunghyun, ”IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz,” Department of ECE and INMC, Seoul National University, Soul, 2013.

[43] IEEE, ”IEEE P802.11- TASK GROUP AH - MEETING UPDATE,” Toukokuu 2014. [Online]. Available: http://www.ieee802.org/11/Reports/tgah_update.htm. [Haettu 7 Heinäkuu 2014].

[44] IEEE, *802.3af-2003,* 2003.

[45] IEEE, *802.3at Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements,* 2009.

[46] H. Huovila, P. Pursula ja E. Strömmer, ”Miten energiaa langattomille antureille?,” *Automaatioväylä,* nro 3, pp. 18 - 21, 2011.

[47] A. Jaatinen, ”Langattomien teknologioiden käyttö kivenmurskauslaitoksen tehokkuuden ja turvallisuuden parantamiseen,” *Automaatioväylä,* nro 3, pp. 12 - 14, 2011.

[48] M. Paavola ja P. Koskela, ”European Sensor Network Architecture - projektissa perehdyttiin langattomien anturiverkkosovellusten kehittämiseen,” *Automaatioväylä,* nro 3, pp. 22 - 23, 2011.

[49] M. Hakonen, ”WirelessHART - tilanne tänään ja tulevaisuus,” *Automaatioväylä,* nro 3, pp. 34- 36, 2011.

[50] V. Pentikäinen, P. Tukeva, J. Hannuksela ja O. Silvén, ”Langatonta kunnonvalvontaa ja ennakoivaa kunnossapitoa vaativiin ympäristöihin,” *Automaatioväylä,* nro 3, pp. 28 - 29, 2011.

[51] IEC, ”IEC 62601 Industrial communication networks - Fieldbus specifications - WIA-PA communication network and communication profile,” IEC, 2011.

[52] HART Communication Foundation, ”HART Communication Protocol and Foundation - Home Page,” [Online]. Available: http://en.hartcomm.org. [Haettu 8 Syyskuu 2014].

[53] ISA, ”ISA | The International Society of Automation,” [Online]. Available: http://www.isa.org. [Haettu 8 Syyskuu 2014].

[54] ZigBee Alliance, ”ZigBee Alliance > Home,” [Online]. Available: http://www.zigbee.org. [Haettu 8 Syyskuu 2014].

[55] IEEE, ”802.15.4e-2012 - IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer,” IEEE, 2012.

[56] IEEE, *IEEE Standard for Information Technology - Specific Requirements - Part 15.4: Wireless Medium Access Control and Physical Layer Specifications for Low Rate Personal Area Networks IEEE 802.15.4-2003,* 2003.

[57] A. N. Kim, F. Hekland, S. Petersen ja P. Doyle, ”When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard,” tekijä: *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*, Hampuri, 2008.

[58] T. Hasegawa ja M. Matsuzaki, ”Reliable Radio with ISA100 for Wireless Industrial Automation,” tekijä: *Future of Instrumentation International Workshop (FIIW)*, Oak Ridge, TN, 2011.

[59] W. Liang, X. Zhang, Y. Xiao, F. Wang, P. Zeng ja H. Yu, ”Survey and experiments of WIA-PA specification of industrial wireless network,” *WIRELESS COMMUNICATIONS AND MOBILE COMPUTING,* vuosik.

2011, nro 11, pp. 1197 - 1212, 2010.

[60] IEEE, ”IEEE 802.15 WPAN™ Task Group 2 (TG2),” 2002. [Online]. Available: http://www.ieee802.org/15/pub/TG2.html. [Haettu 24 Kesäkuu 2014].

[61] IEEE, ”IEEE 802.19 Wireless Coexistence Working Group (WG),” 2014. [Online]. Available: http://www.ieee802.org/19/. [Haettu 6 Kesäkuu 2014].

[62] M. M. A. Hossian, A. Mahmood ja R. Jäntti, ”Channel Ranking Algorithms for Cognitive Coexistence of IEEE 802.15.4,” tekijä: *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, Tokio, 2009.

[63] H. Shariatmadari, ”Channel ranking scheme in wireless sensor networks based on packet delivery ratio estimation,” Aalto University School of Electrical Engineering, Espoo, 2012.

[64] ETSI, ”ETSI EN 300 328 V.1.8.1,” Huhtikuu 2012. [Online]. Available: http://www6.ietf.org/mail-archive/web/6tsch/current/pdfd3d1acPkgu.pdf. [Haettu 30 Tammikuu 2014].

[65] S. Lawson, ”Old-school Wi-Fi is slowing down networks, Cisco says,” 27 Tammikuu 2014. [Online]. Available: http://www.networkworld.com/news/2014/012714-old-school-wi-fi-is-slowing-down-278131.html. [Haettu 30 Tammikuu 2014].

[66] D. Yang, Y. Xu ja M. Gidlund, ”Wireless Coexistence between IEEE 802.11- and IEEE 802.15.4-based networks: A Survey,” *International Journal of Distributed Sensor Networks,* vuosik. 2011, 2011.

[67] IEC, *IEC 60529 ed2.2 Consol. with am1&2,* IEC, 2013.

[68] SESKO ry, ”IP-KOODI TAULUKKO,” [Online]. Available:

http://www.sesko.fi/attachments/testaa_tietosi/ip-taulukko.pdf. [Haettu 7 Helmikuu 2014].

[69] European Parliament, Council, *Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres,* European Parliament, Council, 1994.

[70] Turvallisuus- ja kemikaalivirasto (Tukes), ”ATEX - räjähdysvaarallisten tilojen laitteet,” 18 Lokakuu 2012. [Online]. Available: http://www.tukes.fi/fi/Toimialat/Sahko-ja-hissit/Sahkolaitteet1/Sahkolaitteiden-vaatimukset/ATEX---Rajahdysvaarallisten-tilojen-laitteet/. [Haettu 20 Tammikuu 2014].

[71] Turvallisuus- ja kemikaalivirasto (Tukes), ”Lisätietoa ATEX-direktiivistä,” 17 Syyskuu 2012. [Online]. Available: http://www.tukes.fi/fi/Toimialat/Sahko-ja-hissit/Sahkolaitteet1/Sahkolaitteiden-vaatimukset/ATEX---Rajahdysvaarallisten-tilojen-laitteet/Lisatietoa-ATEX-direktiivista/. [Haettu 21 Tammikuu 2014].

[72] IEEE, *IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements,* 2004.

[73] Industrial Wireless Workshop Participants, ”Industrial Wireless Technology for the 21st Century,” U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, 2002.

[74] wseverin, ”LinSSID,” 23 Kesäkuu 2013. [Online]. Available: http://sourceforge.net/projects/linssid/. [Haettu 11 Helmikuu 2014].

[75] M. Takala, *Tuotantokriittisen prosessiverkkoympäristön valvonta,* Espoo, 2012.

[76] ISO, *ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems - Overview and vocabulary,* ISO, 2014.

[77] Suomen Standardisoimisliitto SFS, *SFS-IEC 62443-2-1 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus.,* Helsinki: Suomen Standardisoimisliitto SFS, 2013.

[78] J. Morse, ”Wireless in industrial systems: Cautious enthusiasm,” Industrial Embedded Systems, 2006.

[79] R. Savola ja P. Ahonen, ”Information Security Challenges in Industrial Automation Systems,” tekijä: *Industrial Informatics, 2006 IEEE International Conference on*, Singapore, 2006.

[80] R. Anderson, ”Security Engineering: A Guide to Building Dependable Distributed Systems (Second Edition),” tekijä: *Chapter 2: Usability and Psychology*, Indianapolis, Wiley, 2008, p. 18.

[81] W. Stallings, Cryptography and Network Security - Principles and Practice, New York: Pearson Education Inc., 2011.

[82] T. Kauppinen ja P. Ahonen, ”Tietoturvaa Huoltovarmuuskriittisille Yrityksille,” Huoltovarmuuskeskus, Oulu, 2013.

[83] B. Zhu, A. Joseph ja S. Sastry, ”A Taxonomy of Cyber Attacks on SCADA Systems,” Department of Electrical Engineering and Computer Sciences University of California at Berkeley, CA, Berkeley, 2011.

[84] T. M. Chen ja S. Abu-Nimeh, ”Lessons from Stuxnet,” *Computer,* vuosik. 44, nro 4, pp. 91 - 93, 2011.

[85] R. Langner, ”Stuxnet: Dissecting a Cyberwarfare Weapon,” *Security & Privacy, IEEE,* vuosik. 9, nro 3, pp. 49 - 51, 2011.

[86] N. Falliere, L. O. Murchu ja E. Chien, ”W32.Stuxnet Dossier,” Symantec Corporation, 2011.

[87] S. Tiilikainen ja J. Manner, ”Suomen automaatioverkkojen haavoittuvuus - Raportti Internetissä julkisesti esillä olevista automaatiolaitteista,” Aalto-yliopisto Sähkötekniikan korkeakoulu, Espoo, 2013.

[88] J. B. Sheldon, ”State of the Art: Attackers and Targets in Cyberspace,” *Journal of Military and Strategic Studies,* vuosik. 14, nro 2, 2012.

[89] C. Alcaraz ja J. Lopez, ”A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems,” *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* vuosik. 40, nro 4, pp. 419 - 428, 2010.

[90] H. Chan ja A. Perrig, ”Security and Privacy in Sensor Networks,” *Computer,* vuosik. 36, nro 10, pp. 103 - 105, 2003.

[91] ISA, *ISA-SP100.11 Call for Proposal Wireless for Industrial Process Measurement and Control,* ISA, 2006.

[92] Axis Communications, ”Bandwidth and storage considerations,” [Online]. Available: http://www.axis.com/products/video/about_networkvideo/bandwidth.htm. [Haettu 21 Toukokuu 2014].

[93] P. Dykstra, ”Protocol Overhead,” Syyskuu 2013. [Online]. Available: http://sd.wareonearth.com/~phil/net/overhead/. [Haettu 22 Toukokuu 2014].

[94] S. Raza, A. Slabbert ja T. Voigt, ”Security Considerations for the WirelessHART Protocol,” tekijä: *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, Mallorca, 2009.

[95] S. Nethi, M. Pohjola, L. Ericsson ja R. Jäntti, ”Simulation case studies of wireless control systems,” tekijä: *Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, 2007.

[96] G. C. Bell, ”Wireless Sensors Improve Data Center Energy Efficiency,” U.S. Department of Energy, 2010.

[97] J. Postel, ”RFC 768 - User Datagram Protocol,” 28 Elokuu 1980. [Online]. Available: http://tools.ietf.org/html/rfc768. [Haettu 28 Tammikuu 2014].

[98] Information Sciences Institute University of Southern California, ”RFC793 - Transmission Control Protocol,” Syyskuu 1981. [Online]. Available: http://tools.ietf.org/html/rfc793. [Haettu 28 Tammikuu 2014].

[99] Wikidevi, ”ASUS USB-N66 - Wikidevi,” 2 Marraskuu 2013. [Online]. Available: http://wikidevi.com/wiki/ASUS_USB-N66. [Haettu 15 Tammikuu 2014].

[100] ASUSTEK COMPUTER INC., ”ASUS USB-N66 Specifications,” [Online]. Available: http://www.asus.com/Networking/USBN66/#specifications. [Haettu 9 Tammikuu 2014].

[101] K. Ashton, ”That 'Internet of Things' Thing,” *RFID Journal,* p. 1, 2009.

[102] J. Arkko ja J. Höller, ”Standards for embedded devices in the networked society,” *Internet of Things Finland,* nro 1, pp. 6 - 9, 2013.

[103] J. Bruner, ”Defining the industrial Internet,” 11 Tammikuu 2013. [Online]. Available: http://radar.oreilly.com/2013/01/defining-the-

industrial-internet.html. [Haettu 7 Heinäkuu 2014].

[104] O. Dementev, ”Machine-Type Communications as Part of LTE-Advanced Technology in Beyond-4G Networks,” tekijä: *Proceeding of the 14th Conference of FRUCT Association*, Tampere, 2013.

[105] IEC, ”IEC 62657-2 ed1.0 Industrial communication networks - Wireless communication networks - Part 2: Coexistence management,” IEC, 2013.

Liitteet

Liite 1, viestintäviraston määräykset luvasta vapautetuille taajuusalueille.

- 433MHz taajuusalue (433,050 – 434,790MHz)
    - 433,050 – 434,790MHz
        - Lähetysteho: korkeintaan 25mW ERP
        - Ei rajoituksia tehotiheydelle
        - Toiminta-aika: <10 %
    - 433,050 – 434,790MHz
        - Lähetysteho: korkeintaan 1mW ERP
        - Tehotiheys: korkeintaan -13dBm/10kHz
        - Ei rajoituksia toiminta-ajan suhteen
    - 434,040 – 434,790MHz
        - Lähetysteho: korkeintaan 10mW ERP
        - Ei rajoituksia tehotiheydelle
        - Ei rajoituksia toiminta-ajan suhteen, ei audio- ja videosovelluksille
        - Muuta: kanavaväli enintään 25kHz
- 868MHz taajuusalue (868MHz – 890MHz)
    - 868,000 – 868,600MHz
        - Lähetysteho: korkeintaan 25mW ERP
        - Ei rajoituksia tehotiheydelle
        - Toiminta-aika: <1 % tai käytössä on soveltuva liikennöintiprotokolla
        - Muuta: Taajuusalueella 868,150 – 868,650 ennen 31.21.1998 luvasta vapautettuja lyhyen kantaman radiolähettimiä, joiden lähetysteho on korkeintaan 500mW
    - 868,600 – 868,700MHz
        - Lähetysteho: korkeintaan 10mW ERP
        - Ei rajoituksia tehotiheydelle
        - Toiminta-aika: <1 %
        - Muuta: käyttötarkoitus pienitehoiset valvonta- ja hälytyslaitteet sekä turvapuhelimet

- 868,700 – 869.200MHz
    - Lähetysteho: 25mW ERP
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <0,1 % tai käytössä on soveltuva liikennöintiprotokolla
- 869,200 – 869,250MHz
    - Lähetysteho: 10mW ERP
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <0,1 %
    - Muuta: ainoastaan turvapuhelimet
- 869,250 – 869,400MHz
    - Lähetysteho: 10mW ERP
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <0,1 %
    - Muuta: käyttötarkoitus pienitehoiset valvonta- ja hälytyslaitteet sekä turvapuhelimet
- 869,400 – 869,650MHz
    - Lähetysteho: 500mW ERP
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <10 % tai käytössä on soveltuva liikennöintiprotokolla
- 869,650 – 869,700MHz
    - Lähetysteho: 25mW ERP
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <10 %
    - Muuta: käyttötarkoitus pienitehoiset valvonta- ja hälytyslaitteet sekä turvapuhelimet
- 869,700 – 870,000MHz
    - Lähetysteho: 5mW ERP tai 25mW, jos toiminta-aika on <1 % tai käytössä on soveltuva liikennöintiprotokolla
    - Ei rajoituksia tehotiheydelle
    - Toiminta-aika: <1 % lähetystehon ollessa 25mW

- 2,4GHz taajuusalue (2400,00 – 2483,500Mhz):
    - Lähetysteho: korkeintaan 100mW EIRP
    - Ei rajoituksia tehotiheydelle

    - Ei rajoituksia toiminta-ajan suhteen
- 5GHz taajuusalue
    - 5150 – 5250MHz (sallittu vain sisätiloissa)
        - Lähetysteho: korkeintaan 200mW ERP
        - Tehotiheys: korkeintaan 10mW/1MHz
        - Ei rajoituksia toiminta-ajan suhteen
    - 5250 – 5350MHz
        - Lähetysteho: korkeintaan 200mW ERP
        - Tehotiheys: korkeintaan 10mW/1MHz
        - Ei rajoituksia toiminta-ajan suhteen
    - 5470 – 5725MHz
        - Lähetysteho: korkeintaan 1W EIRP
        - Tehotiheys: korkeintaan 50mW/1MHz
        - Ei rajoituksia toiminta-ajan suhteen
    - Lisäksi taajuusalueilla 5250 – 5250Mhz ja 5470 – 5725MHz toimivissa laitteissa on käytettävä lähettimen tehonsäätöä, jonka häiriönlieventämiskerroin on vähintään 3 dB järjestelmän suurimalla lähtöteholla. Jos tehonsäätö ei ole käytössä, tulee näillä alueilla vähentää suurimman keskimääräistä EIRP:n ja vastaavan keskimääräisen EIRP:n tiheyden rajoituksia vähennetään 3dB:llä. Näillä taajuuksilla on myös käytettävä häiriönlieventämistekniikoita, jotka antavat vähintään EN 301 893-standardin mukaisen suojan [15].

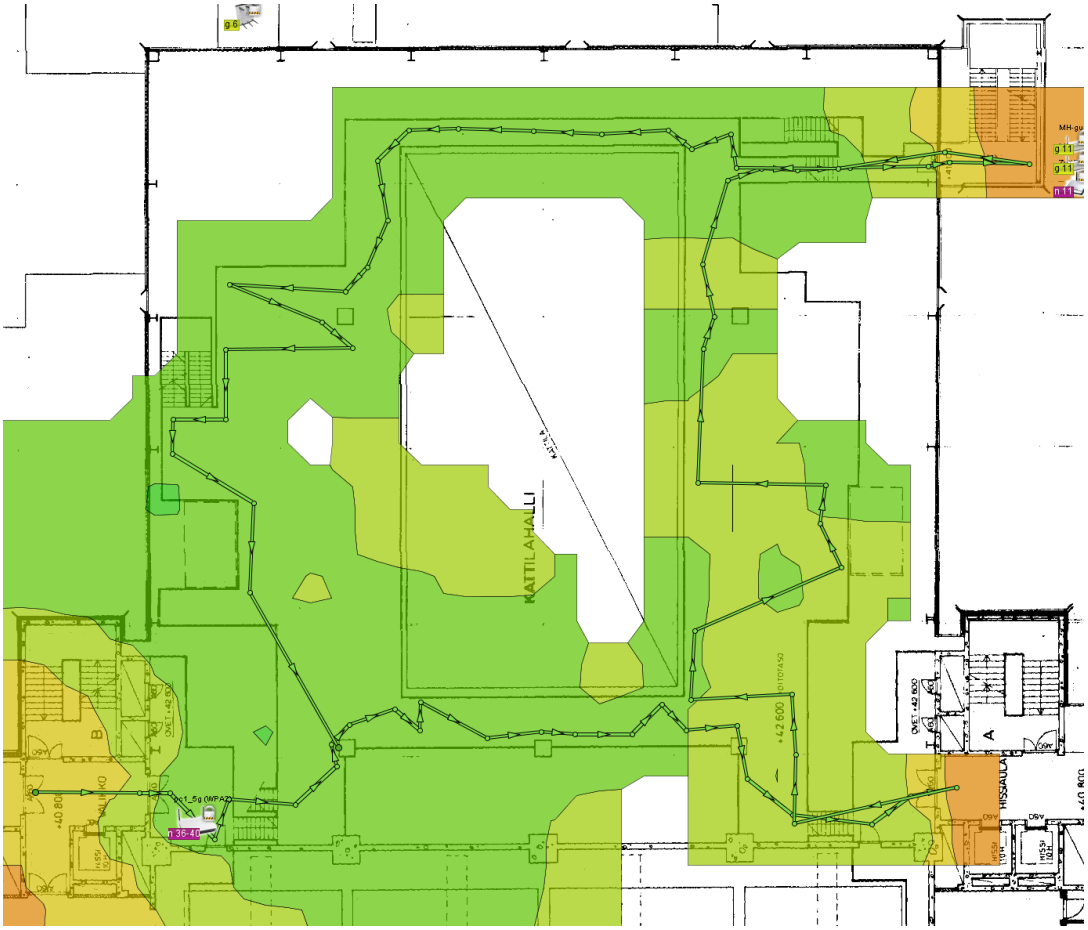
Liite 2, Kuva 16, Kuluttajaluokan laite: Kattilahalli taso 14 (+50,80 m), 2,4GHz kuuluvuus

Liite 3, Kuva 17, Kuluttajaluokan laite: Kattilahalli taso 13 (+46,90 m), 2,4GHz kuuluvuus

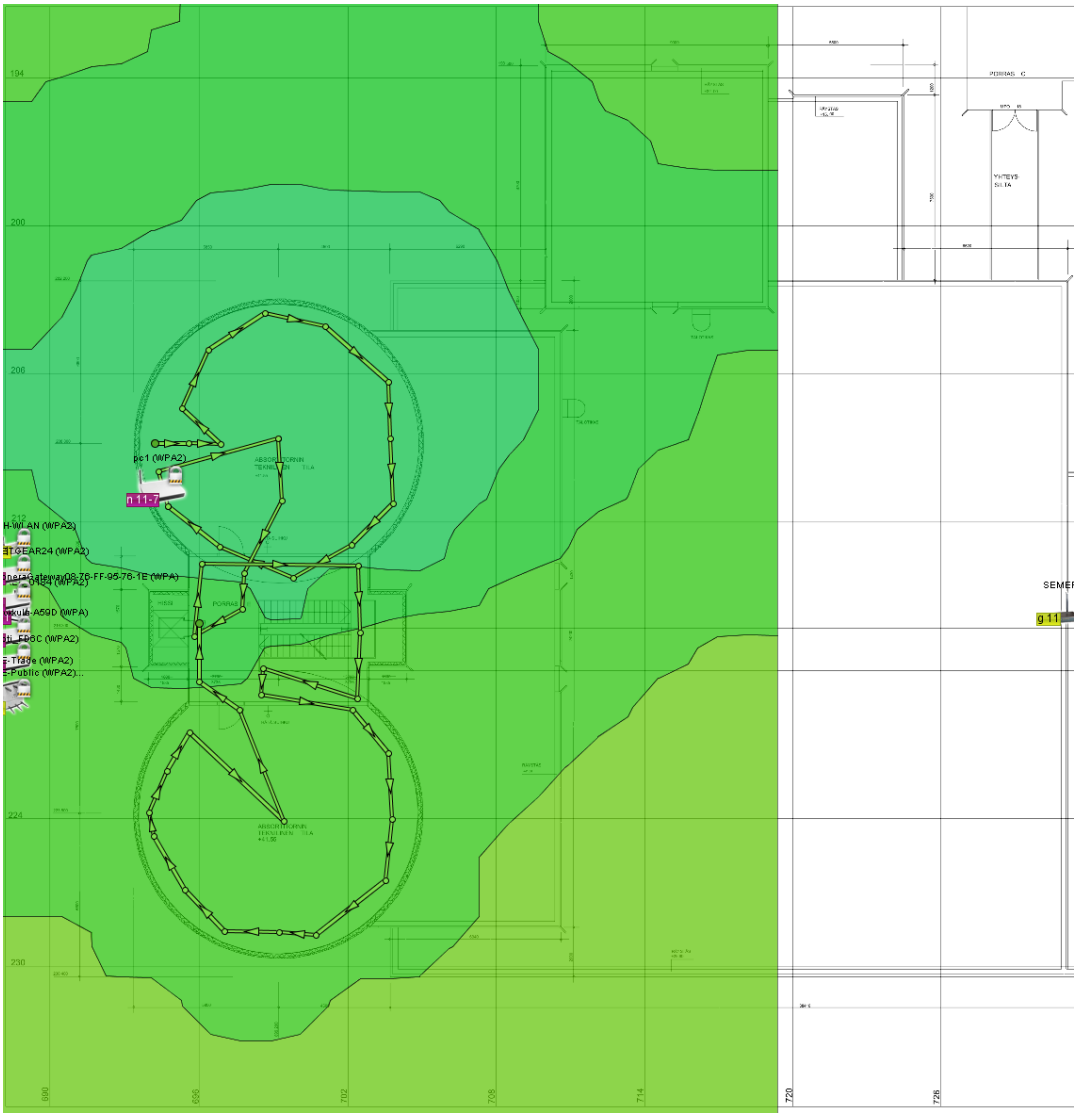
Liite 4, Kuva 18, Kuluttajaluokan laite: Kattilahalli taso 12 (+40,80 m), 2,4GHz kuuluvuus

Liite 5, Kuva 19, Kuluttajaluokan laite: Kattilahalli taso 14 (+50,80 m), 5GHz kuuluvuus

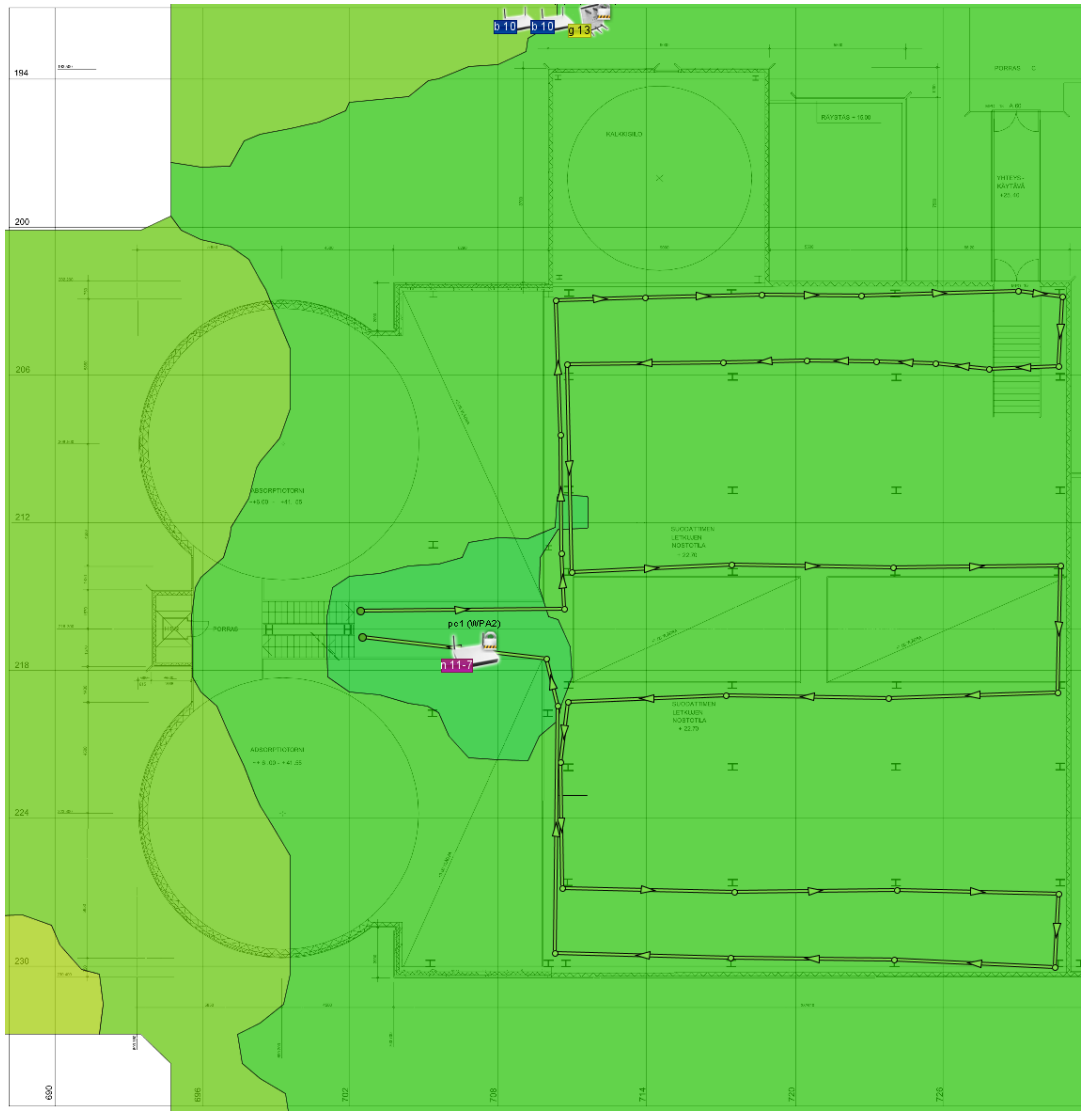
Liite 6, Kuva 20, Kuluttajaluokan laite: Kattilahalli taso 13 (+46,90 m), 5GHz kuuluvuus



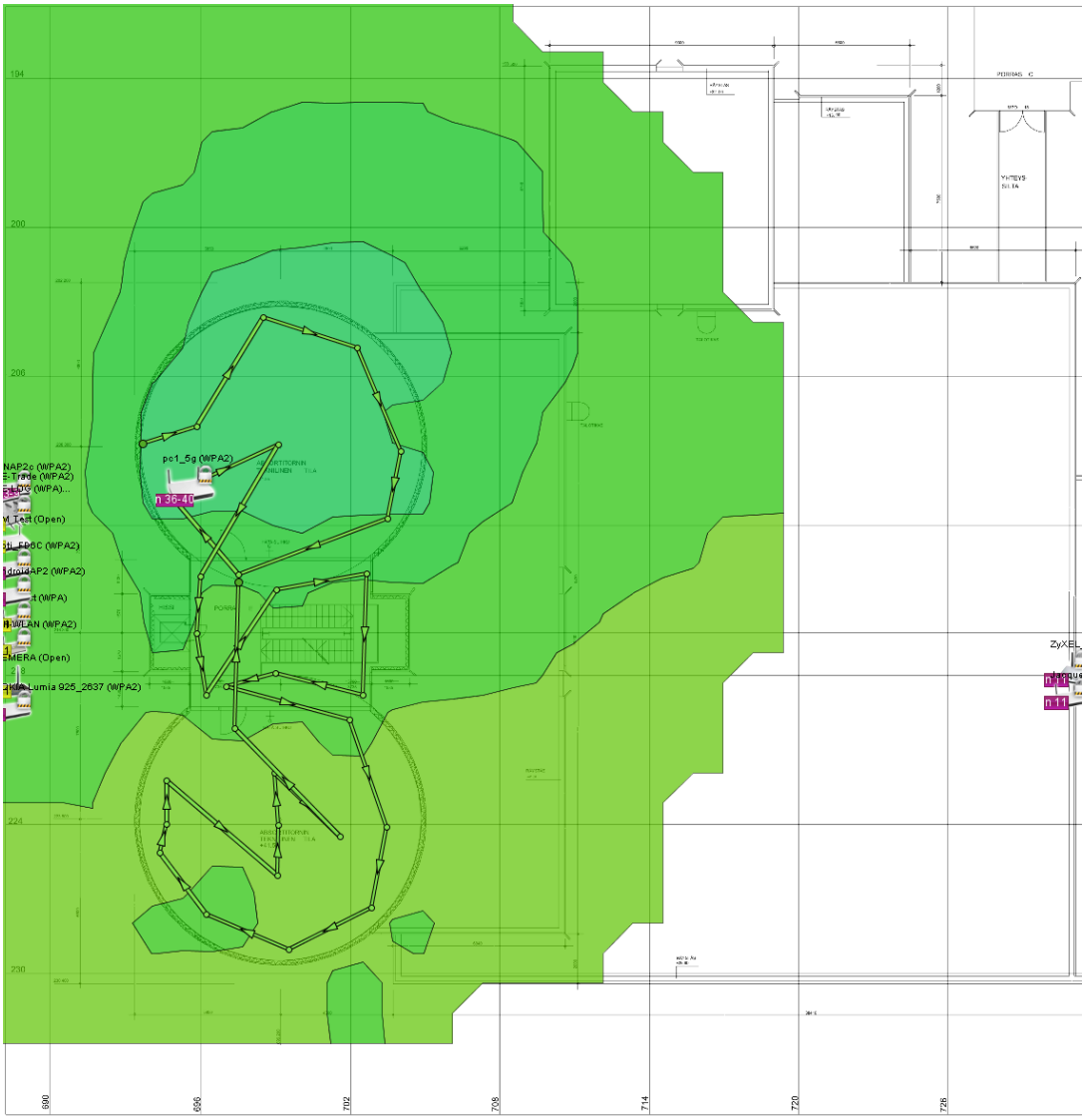
Liite 7, Kuva 21, Kuluttajaluokan laite: Kattilahalli taso 12 (+40,80 m), 5GHz kuuluvuus



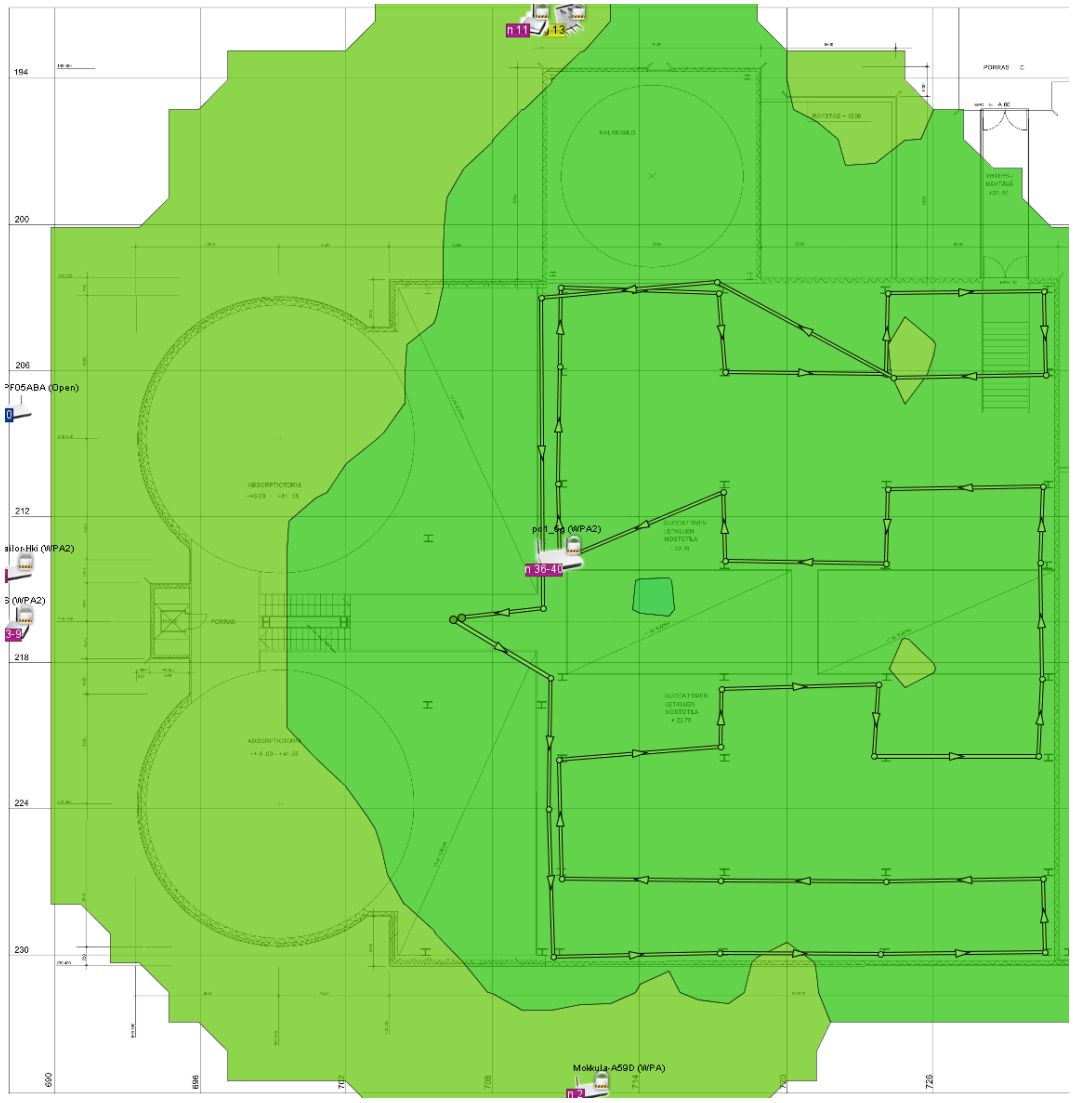
Liite 8, Kuva 22, Kuluttajaluokan laite: Rikinpoistolaitos taso 5 (+41,55 m), 2,4GHz kuuluvuus



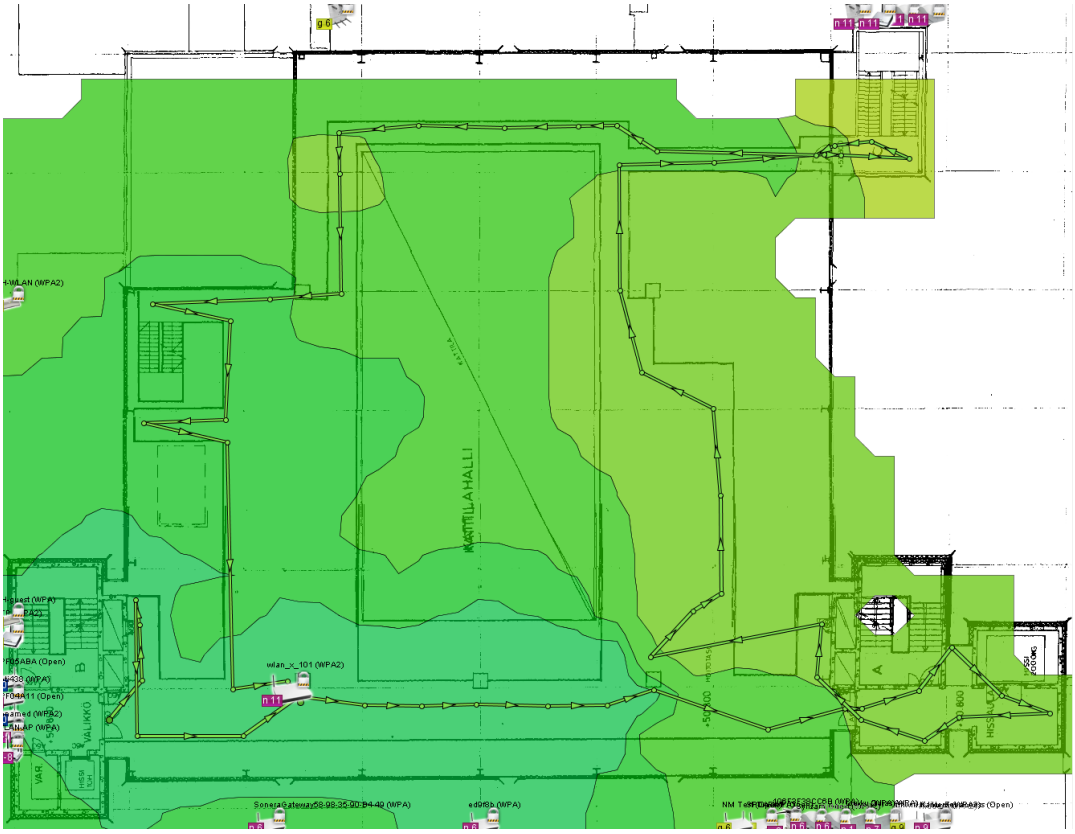
Liite 9, Kuva 23, Kuluttajaluokan laite: Rikinpoistolaitos taso 3 (+22,70 m), 2,4GHz kuuluvuus



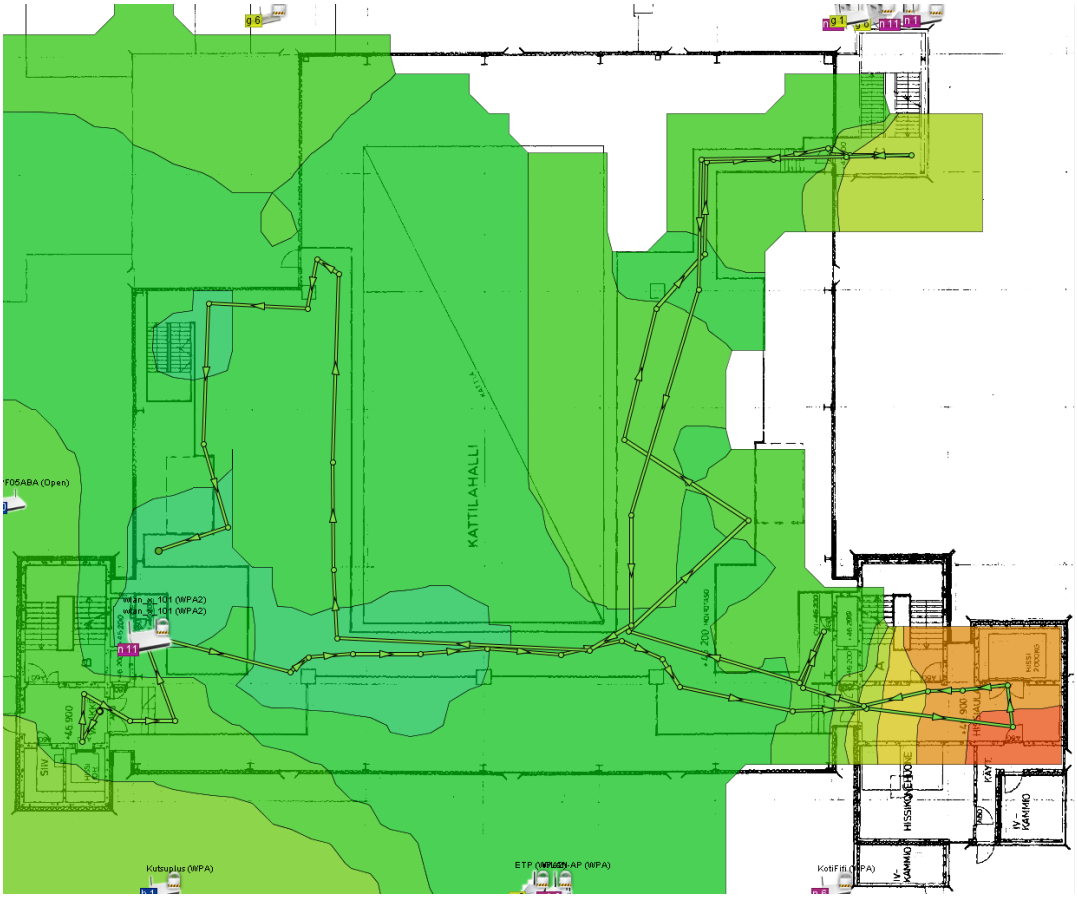
Liite 10, Kuva 24, Kuluttajaluokan laite: Rikinpoistolaitos taso 5 (+41,55 m), 5GHz kuuluvuus



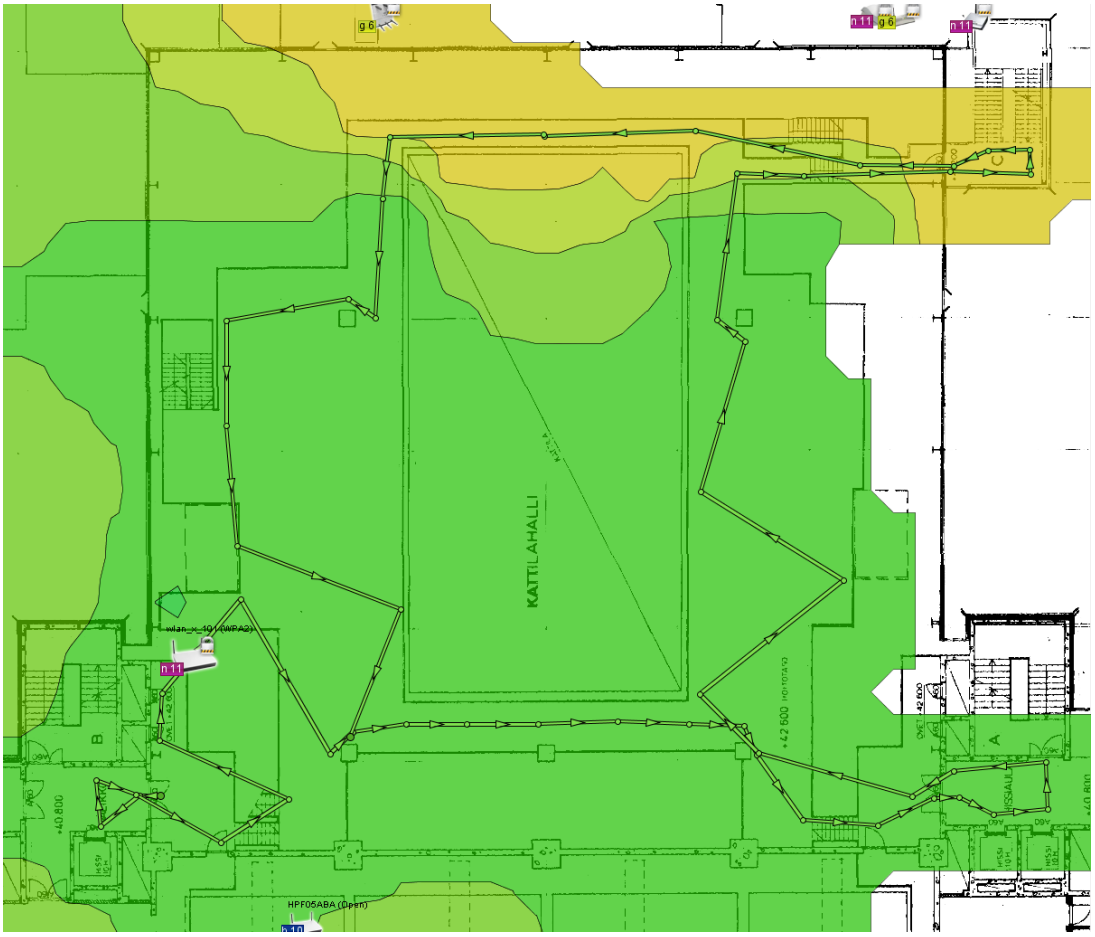
Liite 11, Kuva 25, Kuluttajaluokan laite: Rikinpoistolaitos taso 3 (+22,70 m), 5GHz kuuluvuus



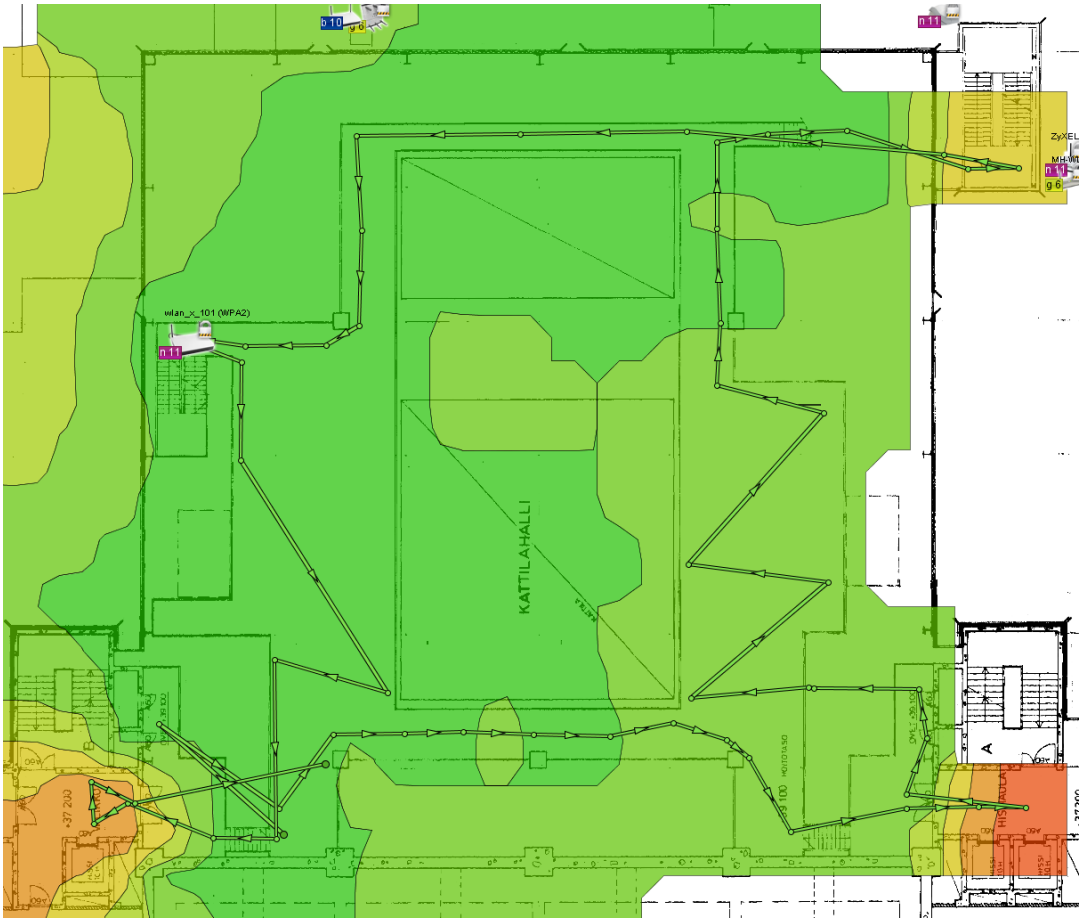
Liite 12, Kuva 26, Teollisuusluokan laite: Kattilahalli taso 14 (+50,80 m), 2,4GHz kuuluvuus



Liite 13, Kuva 27, Teollisuusluokan laite: Kattilahalli taso 13 (+46,90 m), 2,4GHz kuuluvuus



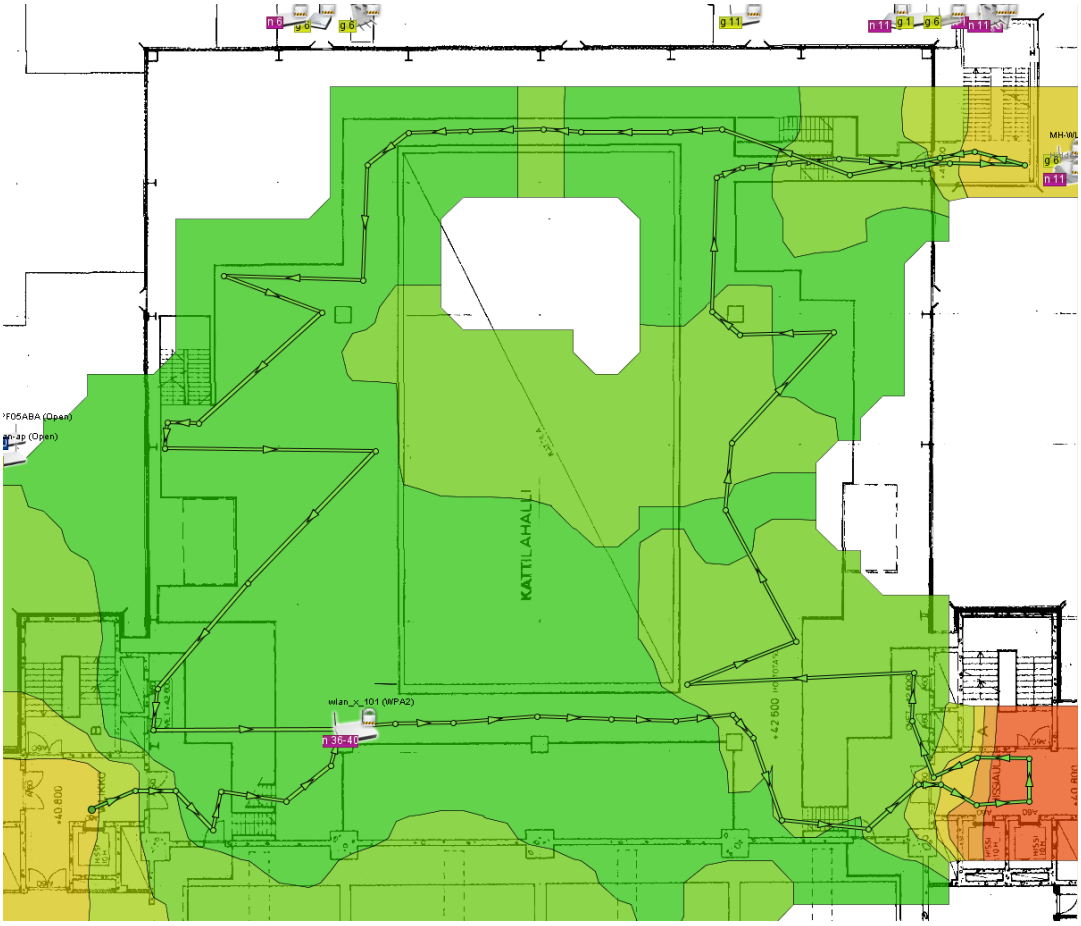
Liite 14, Kuva 28, Teollisuusluokan laite: Kattilahalli taso 12 (+40,80 m), 2,4GHz kuuluvuus



Liite 15, Kuva 29, Teollisuusluokan laite: Kattilahalli taso 11 (+37,20 m), 2,4GHz kuuluvuus

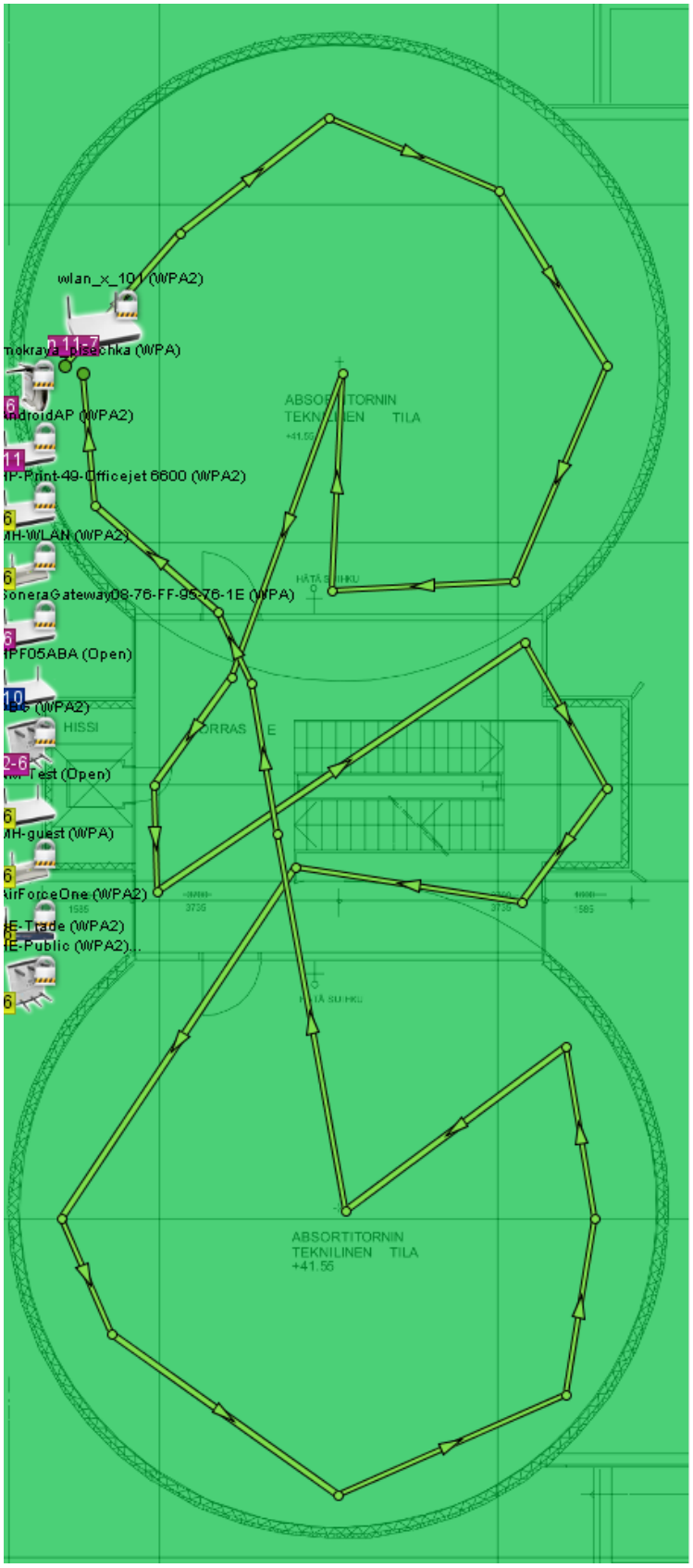
Liite 16, Kuva 30, Teollisuusluokan laite: Kattilahalli taso 14 (+50,80 m), 5GHz kuuluvuus

Liite 17, Kuva 31, Teollisuusluokan laite: Kattilahalli taso 13 (+46,90 m), 5GHz kuuluvuus

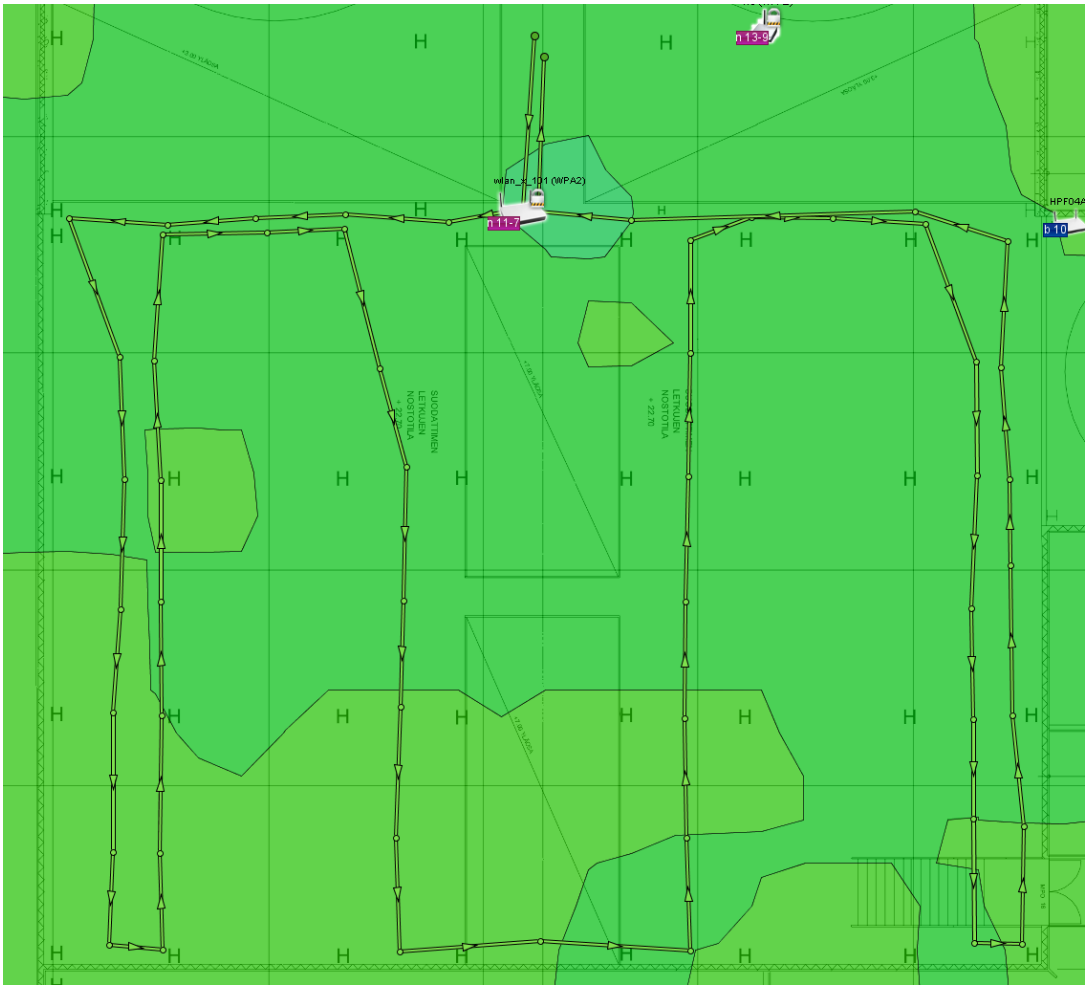


Liite 18, Kuva 32, Teollisuusluokan laite: Kattilahalli taso 12 (+40,80 m), 5GHz kuuluvuus

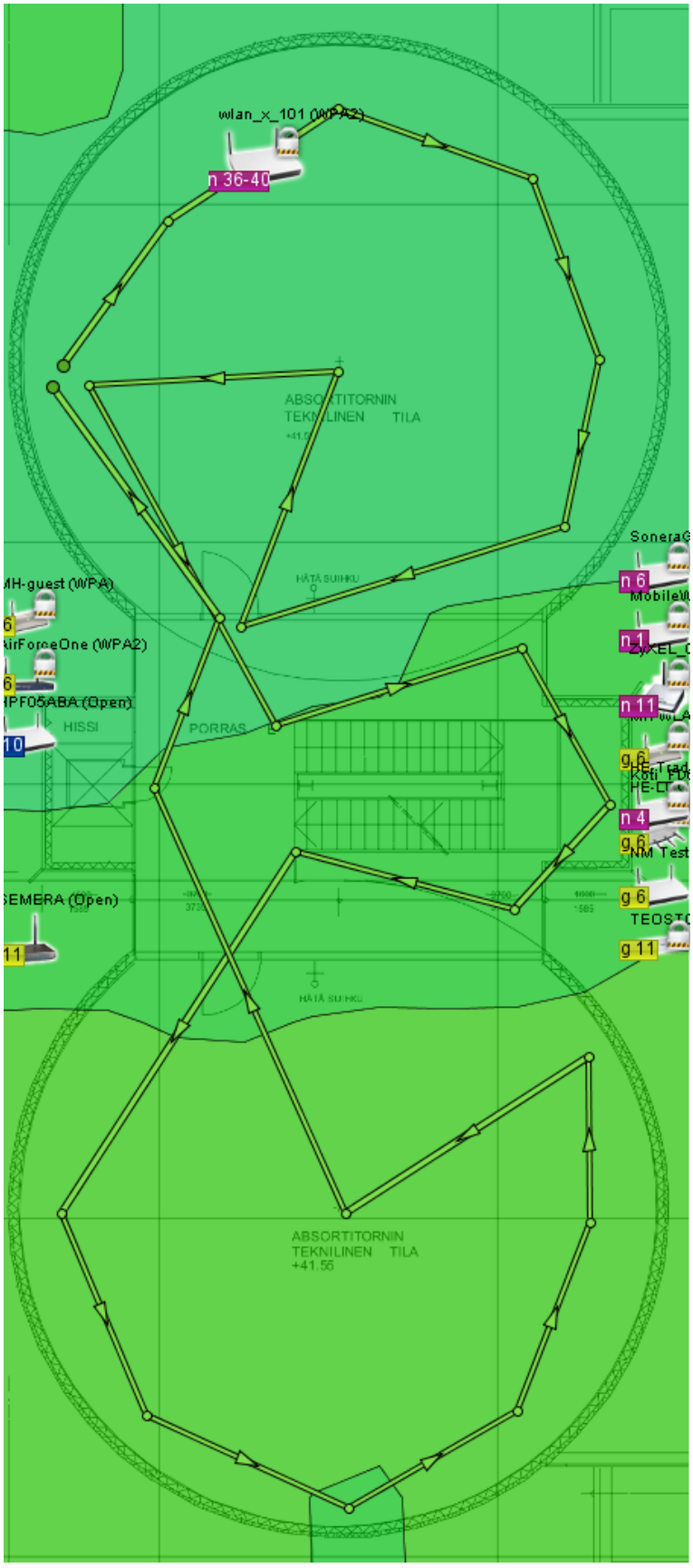
Liite 19, Kuva 33, Teollisuusluokan laite: Kattilahalli taso 11 (+37,20 m), 5GHz kuuluvuus



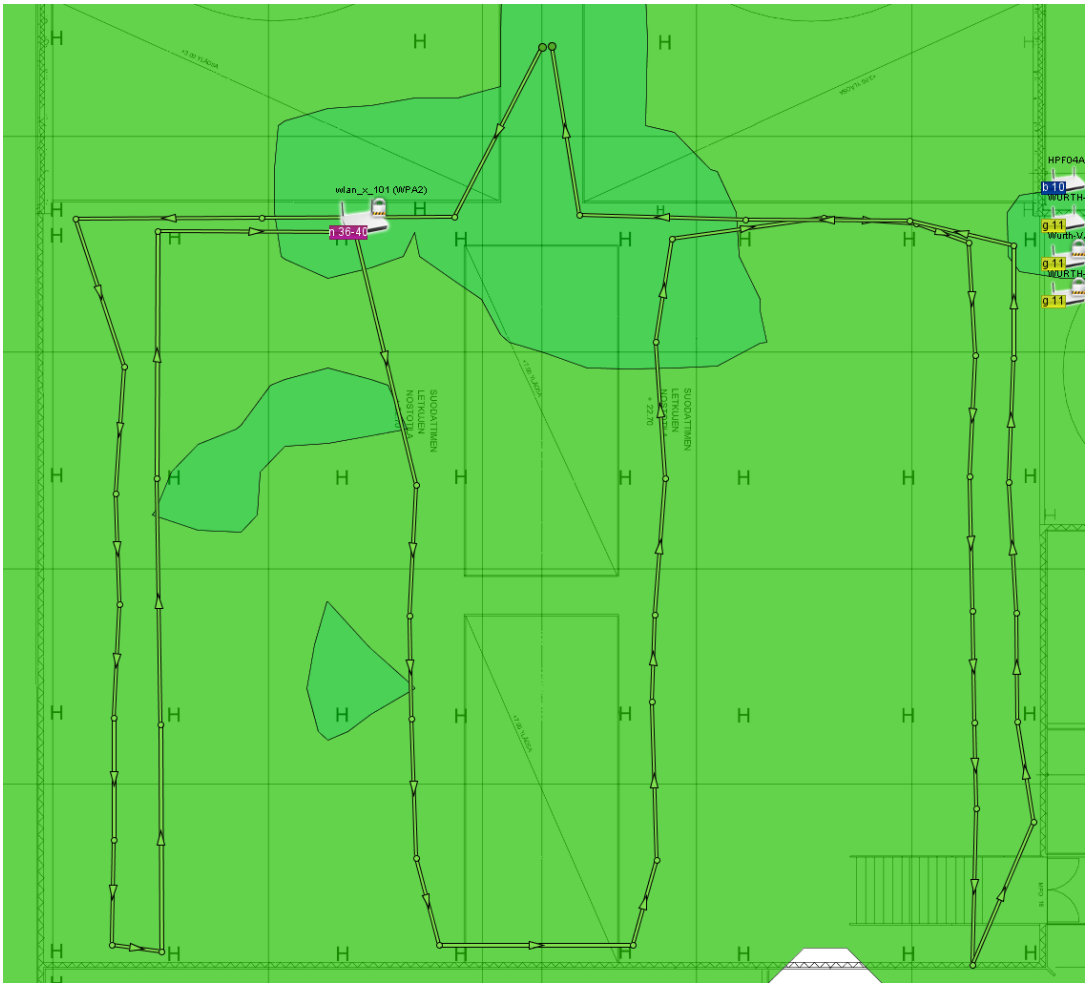
Liite 20, Kuva 34, Teollisuusluokan laite: Rikinpoistolaitos taso 5 (+41,55 m), 2,4GHz kuuluvuus



Liite 21, Kuva 35, Teollisuusluokan laite: Rikinpoistolaitos taso 3 (+22,70 m), 2,4GHz kuuluvuus



Liite 22, Kuva 36, Teollisuusluokan laite: Rikinpoistolaitos taso 5 (+41,55 m), 5GHz kuuluvuus



Liite 23, Kuva 37, Teollisuusluokan laite: Rikinpoistolaitos taso 3 (+22,70 m), 5GHz kuuluvuus

Kuluttajaluokan laitteet kattilahallissa 2,4GHz-taajuusalueella:

Taso 14:

Liite 24, Taulukko 10, kuluttajaluokka 2,4GHz KH taso 14

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,37 / 4,05 / 6,01 ms	0 %	72,7 / 75,1 Mbit/s
B	5,36 / 150 / 993 ms	47,0 %	4,00 / 30,7 Mbit/s
C	5,35 / 154 / 359 ms	45,4 %	0,00 / 17,5 Mbit/s
D	4,04 / 25,9 / 194 ms	12,0 %	1,41 / 10,8 Mbit/s

Taso 13:

Liite 25, Taulukko 11, kuluttajaluokka 2,4GHz KH taso 13

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,73 / 39,7 / 466 ms	15,5 %	7,05 / 41,8 Mbit/s
B	3,72 / 48,9 / 466 ms	13,5 %	0,92 / 25,1 Mbit/s
C	5,66 / 68,9 / 384 ms	26,6 %	0,00 / 2,80 Mbit/s
D	3,66 / 20,9 / 201 ms	5,70 %	38,5 / 40,5 Mbit/s

Teollisuusluokan laitteet kattilahallissa 2,4GHz-taajuusalueella:

Taso 14:

Liite 26, Taulukko 12, teollisuusluokka 2,4GHz KH taso 14

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,25 / 15,1 / 417 ms	2,50 %	49,3 / 57,0 Mbit/s
B	3,10 / 10,6 / 67,3 ms	0 %	19,3 / 14,3 Mbit/s
C	3,797 / 17,4 / 526 ms	0 %	4,82 / 9,22 Mbit/s
D	3,21 / 23,0 / 514 ms	0 %	7,33 / 14,5 Mbit/s

Taso 13:

Liite 27, Taulukko 13, teollisuusluokka 2,4GHz KH taso 13

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,18 / 26,3 / 515 ms	3,20 %	23,5 / 14,3 Mbit/s
B	3,94 / 50,4 / 375 ms	20 %	6,74 / 15,1 Mbit/s
C	4,86 / 44,1 / 138 ms	54,8 %	4,28 / 7,60 Mbit/s
D	2,99 / 8,28 / 104 ms	0 %	21,2 / 16,5 Mbit/s

Taso 12:

Liite 28, Taulukko 14, teollisuusluokka 2,4GHz KH taso 12

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,42 / 29,2 / 514 ms	0 %	11,9 / 20,8 Mbit/s
B	3,23 / 15,1 / 475 ms	0 %	7,27 / 15,8 Mbit/s
C	3,32 / 14,4 / 113 ms	12,0 %	2,33 / 11,9 Mbit/s
D	3,82 / 176 / 1930 ms	0 %	6,08 / 4,18 Mbit/s

Taso 11:

Liite 29, Taulukko 15, teollisuusluokka 2,4GHz KH taso 11

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,36 / 26,1 / 520 ms	0 %	23,4 / 17,7 Mbit/s
B	3,93 / 69,5 / 513 ms	5,20 %	5,58 / 9,53 Mbit/s
C	3,47 / 4,77 / 7,76 ms	0 %	5,59 / 10,2 Mbit/s
D	3,54 / 176 / 1830 ms	0 %	5,62 / 66,7 Mbit/s

Kuluttajaluokan laitteet rikinpoistolaitoksessa 2,4GHz-taajuusalueella:

Taso 5:

Liite 30, Taulukko 16, kuluttajaluokka 2,4GHz RP taso 5

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,40 / 32,6 / 138 ms	0 %	9,16 / 81,2 Mbit/s
B	4,15 / 28,6 / 168 ms	0 %	5,70 / 21,0 Mbit/s
C	4,42 / 23,8 / 191 ms	4,70 %	5,76 / 25,9 Mbit/s
D	5,44 / 291 / 914 ms	48,7 %	0 / 6,68 Mbit/s
E	5,52 / 609 / 1575 ms	58,3 %	0 / 14,5 Mbit/s
F	6,35 / 133 / 447 ms	26,0 %	0 / 12,2 Mbit/s
G	4,21 / 28,7 / 214 ms	4,50 %	9,54 / 38,9 Mbit/s
H	3,96 / 57,3 / 286 ms	17,2 %	1,15 / 26,2 Mbit/s
I	4,31 / 59,2 / 410 ms	11,0 %	2,43 / 14,6 Mbit/s

Taso 3:

Liite 31, Taulukko 17, kuluttajaluokka 2,4GHz RP taso 3

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	4,56 / 128 / 394 ms	37,8 %	0 / 10,1 Mbit/s
B	4,29 / 24,5 / 119 ms	7,40 %	4,36 / 23,4 Mbit/s
C	3,93 / 16,4 / 139 ms	0 %	3,63 / 27,3 Mbit/s
D	5,10 / 187 / 756 ms	35,2 %	0 / 20,3 Mbit/s
E	4,24 / 43,1 / 264 ms	7,40 %	14,6 / 33,8 Mbit/s
F	8,14 / 283 / 860 ms	29,6 %	0 / 7,25 Mbit/s
G	4,86 / 14,0 / 157 ms	5,20 %	0,303 / 30,0 Mbit/s

Teollisuusluokan laitteet rikinpoistolaitoksessa 2,4GHz-taajuusalueella:

Taso 5:

Liite 32, Taulukko 18, teollisuusluokka 2,4GHz RP taso 5

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,61 / 18,1 / 511 ms	0 %	63,3 / 34,4 Mbit/s
B	2,61 / 20,1 / 517 ms	0 %	54,2 / 45,7 Mbit/s
C	2,64 / 4,84 / 16,8 ms	0 %	40,1 / 41,4 Mbit/s
D	4,40 / 62,2 / 1070 ms	5,10 %	4,98 / 11,3 Mbit/s
E	3,56 / 59,3 / 512 ms	0 %	6,61 / 10,9 Mbit/s
F	3,01 / 7,99 / 104 ms	5,50 %	8,21 / 26,4 Mbit/s
G	2,84 / 19,6 / 513 ms	0 %	37,8 / 36,7 Mbit/s
H	2,67 / 3,78 / 14,1 ms	0 %	32,3 / 43,4 Mbit/s
I	3,70 / 9,10 / 34,4 ms	7,40 %	13,5 / 37,8 Mbit/s

Taso 3:

Liite 33, Taulukko 19, teollisuusluokka 2,4GHz RP taso 3

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,06 / 22,1 / 516 ms	2,80 %	5,40 / 41,2 Mbit/s
B	2,91 / 20,0 / 507 ms	0 %	49,4 / 42,1 Mbit/s
C	2,75 / 6,27 / 105 ms	2,60 %	50,7 / 34,6 Mbit/s
D	3,20 / 15,4 / 147 ms	2,70 %	18,1 / 37,6 Mbit/s
E	2,82 / 19,7 / 514 ms	0 %	38,1 / 69,1 Mbit/s
F	2,80 / 18,9 / 516 ms	0 %	25,3 / 50,6 Mbit/s
G	3,09 / 20,4 / 510 ms	2,50 %	15,1 / 47,0 Mbit/s

Kuluttajaluokan laitteet kattilahallissa 5GHz-taajuusalueella:

Taso 14:

Liite 34, Taulukko 20, kuluttajaluokka 5GHz KH taso 14

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	1,84 / 2,41 / 2,87 ms	0 %	80,9 / 180 Mbit/s
B	4,34 / 5,08 / 7,49 ms	0 %	27,3 / 23,4 Mbit/s
C	5,12 / 9,57 / 28,2 ms	0 %	12,5 / 11,9 Mbit/s
D	4,15 / 88,1 / 421 ms	32,1 %	0 / 22,8 Mbit/s

Taso 13:

Liite 35, Taulukko 21, kuluttajaluokka 5GHz KH taso 13

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,93 / 9,94 / 27,8 ms	0 %	1,66 / 63,1 Mbit/s
B	4,58 / 90,0 / 305 ms	28,5 %	0,00 / 22,9 Mbit/s
C	5,29 / 71,4 / 695 ms	15,0 %	0,00 / 16,1 Mbit/s
D	4,09 / 5,15 / 6,61 ms	0 %	24,0 / 53,3 Mbit/s

Teollisuusluokan laitteet kattilahallissa 5GHz-taajuusalueella:

Taso 14:

Liite 36, Taulukko 22, teollisuusluokka 5GHz KH taso 14

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,30 / 2,87 / 3,77 ms	0 %	66,6 / 88,0 Mbit/s
B	3,23 / 3,79 / 5,21 ms	0 %	17,0 / 28,8 Mbit/s
C	3,02 / 6,97 / 68,1 ms	0 %	14,2 / 19,7 Mbit/s
D	2,84 / 5,13 / 24,0 ms	0 %	30,2 / 42,9 Mbit/s

Taso 13:

Liite 37, Taulukko 23, teollisuusluokka 5GHz KH taso 13

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,57 / 3,78 / 7,98 ms	0 %	55,6 / 37,0 Mbit/s
B	3,06 / 4,09 / 6,07 ms	0 %	22,9 / 33,2 Mbit/s
C	3,30 / 9,90 / 65,6 ms	2,70 %	14,5 / 19,6 Mbit/s
D	3,09 / 7,34 / 103 ms	2,60 %	26,2 / 39,4 Mbit/s

Taso 12:

Liite 38, Taulukko 24, teollisuusluokka 5GHz KH taso 12

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,70 / 3,87 / 18,8 ms	0 %	48,0 / 53,1 Mbit/s
B	3,24 / 4,55 / 7,82 ms	0 %	27,6 / 33,6 Mbit/s
C	3,31 / 12,1 / 105 ms	11,6 %	21,7 / 12,6 Mbit/s
D	3,12 / 11,2 / 104 ms	6,60 %	22,3 / 21,6 Mbit/s

Taso 11:

Liite 39, Taulukko 25, teollisuusluokka 5GHz KH taso 11

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,96 / 3,74 / 4,61 ms	0 %	48,2 / 53,6 Mbit/s
B	2,76 / 3,93 / 6,58 ms	2,30 %	29,9 / 31,2 Mbit/s
C	3,28 / 9,16 / 104 ms	3,00 %	16,6 / 21,2 Mbit/s
D	3,03 / 9,70 / 103 ms	5,20 %	21,7 / 26,7 Mbit/s

Kuluttajaluokan laitteet rikinpoistolaitoksessa 5GHz-taajuusalueella:
Taso 5:

Liite 40, Taulukko 26, kuluttajaluokka 5GHz RP taso 5

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	3,31 / 3,70 / 4,27 ms	0 %	42,9 / 56,0 Mbit/s
B	4,76 / 8,10 / 20,5 ms	0 %	10,5 / 24,5 Mbit/s
C	4,37 / 37,2 / 186 ms	9,00 %	0 / 24,4 Mbit/s
D	4,87 / 226 / 765 ms	51,4 %	0 / 15,5 Mbit/s
E	5,36 / 73,3 / 282 ms	19,2 %	0 / 13,5 Mbit/s
F	4,70 / 94,5 / 486 ms	11,1 %	0 / 13,2 Mbit/s
G	3,91 / 94,0 / 862 ms	12,5 %	1,36 / 34,6 Mbit/s
H	3,54 / 4,78 / 12,2 ms	0 %	27,0 / 46,5 Mbit/s
I	4,54 / 12,0 / 101 ms	0 %	0,449 / 25,6 Mbit/s

Taso 3:

Liite 41, Taulukko 27, kuluttajaluokka 5GHz RP taso 3

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	4,60 / 44,2 / 167 ms	19,3 %	0,300 / 22,3 Mbit/s
B	4,32 / 20,0 / 183 ms	4,10 %	6,03 / 29,6 Mbit/s
C	4,34 / 13,3 / 199 ms	3,80 %	18,7 / 37,2 Mbit/s
D	4,96 / 25,2 / 154 ms	9,30 %	12,4 / 29,8 Mbit/s
E	4,49 / 7,14 / 19,6 ms	0 %	10,8 / 28,7 Mbit/s
F	4,50 / 12,3 / 132 ms	0 %	16,7 / 31,3 Mbit/s
G	4,43 / 38,0 / 204 ms	17,8 %	0,583 / 31,4 Mbit/s

Teollisuusluokan laitteet rikinpoistolaitoksessa 5GHz-taajuusalueella:

Taso 5:

Liite 42, Taulukko 28, teollisuusluokka 5GHz RP taso 5

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,41 / 19,8 / 503 ms	0 %	45,5 / 48,9 Mbit/s
B	2,99 / 30,4 / 508 ms	0 %	43,6 / 33,8 Mbit/s
C	2,87 / 7,36 / 40,6 ms	4,70 %	17,8 / 30,1 Mbit/s
D	3,15 / 19,3 / 518 ms	0 %	17,1 / 13,5 Mbit/s
E	2.93 / 17,2 / 511 ms	0 %	15,2 / 18,1 Mbit/s
F	2,90 / 6,17 / 35,3 ms	0 %	18,6 / 22,9 Mbit/s
G	2,84 / 16,9 / 505 ms	0 %	41,2 / 59,3 Mbit/s
H	2,66 / 16,3 / 510 ms	0 %	38,1 / 46,1 Mbit/s
I	2,89 / 5,30 / 24,2 ms	0 %	26,7 / 27,6 Mbit/s

Taso 3:

Liite 43, Taulukko 29, teollisuusluokka 5GHz RP taso 3

Piste	Vasteaika min./kesk./maks. (ms)	Pakettihäviö (%)	Tiedonsiirtonopeus TCP/UDP (Mbit/s)
A	2,94 / 4,30 / 13,8 ms	0 %	25,1 / 7,66 Mbit/s
B	2,66 / 10,9 / 198 ms	0 %	36,2 / 61,6 Mbit/s
C	2,80 / 4,62 / 13,7 ms	0 %	35,7 / 35,9 Mbit/s
D	2,75 / 7,09 / 106 ms	2,60 %	39,3 / 35,8 Mbit/s
E	2,62 / 4,63 / 38,4 ms	0 %	35,1 / 32,4 Mbit/s
F	2,74 / 3,52 / 6,30 ms	0 %	44,9 / 47,4 Mbit/s
G	2,92 / 8,07 / 103 ms	2,50 %	33,8 / 27,7 Mbit/s