Turvalliset etäyhteydet prosessin ohjaukseen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Valkeakosken kampus, sähkö- ja automaatiotekniikka, insinööri (AMK)

2020 Syksy

Tuukka Syrjänen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Sähkö- ja automaatiotekniikka
HAMK Valkeakoski

Tiivistelmä

Tekijä Tuukka Syrjänen

Vuosi 2020

Työn nimi Turvalliset etäyhteydet prosessin ohjaukseen

Ohjaajat Timo Viitala

TIIVISTELMÄ

Työn tavoitteena oli selvittää, löytyykö automaatiojärjestelmän etäohjaukseen järkevää ja turvallista ratkaisua. Työn tilaajana toimii Hämeen ammattikorkeakoulun tutkimusyksikkö HAMK Tech. Työn tuloksia esitetään sovellettavaksi HAMK:n VEneCT-tutkimusprojektiin. VEneCT-järjestelmä on hybridivoimalaitos, joka tuottaa energiaa vähäpäästöisesti aurinkovoimaa ja pelletinpolttoa hyödyntäen.

Työn alussa käydään läpi keskeisiä käsitteitä, ja esitellään VEneCT-järjestelmää. Etäyhteysmenetelmien käsittely on jaettu kahteen osaan: teknologioihin ja protokolliin sekä kaupallisiin järjestelmiin. luvussa kuusi kerrotaan tarkemmin protokollien tiedonsiirrosta ja tietoturvaominaisuuksista, kun seitsemännessä luvussa käsitellään enemmän toiminnallista puolta, hintaa ja saatavuutta.

Johtopäätöksissä esitetään käytettäväksi kolmea eri hintaista ratkaisua. Tähän malliin päädyttiin, koska huomattiin, että ainoastaan tietoturvallisuuden perusteella on hankala löytää ratkaisevaa eroa järjestelmien välillä. Selvityksen perusteella markkinoilta löytyi kolme eri hintaista järjestelmää, joita voidaan ehdottaa käytettäväksi tutkimusprojektissa. Haasteita loi lähinnä järjestelmien kulurakenteet – tilaajan puolelta toivottiin kertainvestointia, kun taas markkinoilla varsinkin halvempien järjestelmin osalta käytössä oli lähes poikkeuksetta kuukausittainen datan käyttöön perustuva laskutus.

Avainsanat Etäohjaus, tietoturva, VPN

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Electrical and automation technology
HAMK Valkeakoski

Abstract

Author Tuukka Syrjänen
Year 2020
Subject Safe remote access solutions for process controlling
Supervisors Timo Viitala

ABSTRACT

The subject of this thesis was to find out if there are reasonable and safe solutions to remotely control an automation system. This thesis was ordered by Häme university of applied sciences' research unit HAMK Tech. The outcome is supposed to be applicable to HAMK's VEneCT-research project. The VEneCT-system is a hybrid power plant that is driven by solar energy and burning pellet.

At first there are few chapters where the most important concepts will be discussed, also the VEneCT-system will be presented more closely. The actual remote controlling methods will be presented in two parts. In the sixth chapter technologies and protocols will be handled more closely and subjects like data transfer and information security will be discussed. The second part, chapter seven is mostly focused on more practical things such as usage, pricing and availability of solutions.

In the conclusion part, three different solutions will be suggested for HAMK's research project, with pricing being the main difference maker between them. This kind of structure was decided to be used after finding out that the security level between the solutions doesn't differ as much as predicted before. Three solutions with different price ranges were successfully found, but the challenge was to respond to the preferences set by the customer. The structure of expenses was hoped to be an investment without any running costs, but it turned out that the most low-end solutions are charged with monthly fees based on the data usage.

Keywords Information security, remote controlling, VPN

Sisällys

Kuvat, taulukot ja kaavat

1 JOHDANTO

Tässä opinnäytetyössä perehdytään automaatiojärjestelmän turvallisiin etäohjausmahdollisuuksiin. Selvityksen tarve on peräisin Hämeen ammattikorkeakoulun VEneCT-projektista. Kyseessä on prosessi, jossa pelletinpoltolla ja aurinkovoimalla toimiva hybridimoduuli tuottaa omavaraisesti ja vähäpäästöisesti energiaa. Tällä hetkellä kyseistä järjestelmää voidaan ohjata ja hallita ainoastaan koulun lähiverkosta käsin, ja työn tarkoituksena on antaa perusteltu ehdotus käytettävästä teknologiasta etäohjauksen mahdollistamiseksi.

Ennakkokäsityksenä ennen aiheeseen syventymistä on, että markkinoilta kyllä löytyy varteenotettava teknologia etäyhteyden mahdollistamiseksi turvallisesti. Raportissa pyritään ottamaan huomioon mahdollisimman hyvin toisistaan erilaiset ratkaisut ja vertailemaan niitä kriittisesti turvallisuuden ollessa keskeisenä arviointikriteerinä. Lähtökohtana on, että mikäli työn perusteella päädytään ehdottamaan tiettyä ratkaisua, se ei saa huonontaa järjestelmän tietoturvan tasoa.

Raportin alkuvaiheessa käsitellään tärkeimpiä aiheeseen liittyviä käsitteitä yleisellä tasolla. Luvussa kuusi kartoitetaan etäyhteyden mahdollistavia teknologioita. Seitsemännessä luvussa perehdytään markkinoilla oleviin ratkaisuihin, joissa hyödynnetään näitä teknologioita. Opinnäytetyön tavoitteena on paitsi ehdottaa käytettäväksi yhtä ratkaisua, myöskin antaa mahdollisimman laaja kuva muista mahdollisista teknologioista, jotta saadaan tarpeeksi kattava vertailupohja johtopäätösten tekemiseksi.

Kuten työn otsikko viittaa, tärkein yksittäinen aspekti teknologioita vertailtaessa on turvallisuus. Ratkaisussa pitää myös huomioida käyttöönottoon ja ylläpitoon vaadittava työ ja asiantuntijuus, koska paljon resursseja sitovat ratkaisut tulevat ajan kuluessa kertainvestointeja kalliimmaksi. Hinnalla on myös olennainen merkitys vertailun kannalta.

Toteutusvaiheessa keskusteltiin tilaajan edustajan kanssa tietoturvan lisäksi myös muista vertailukriteereistä. Tarve tilaajan lisätoiveiden kuulemiseen syntyi, kun selvitysvaiheessa

kaikki esitellyt teknologiat ja ratkaisut osoittautuivat tietoturvatasoltaan riittäviksi. Johtopäätökset keskustelusta olivat seuraavat:

- kulurakenteen tulisi olla kertainvestointi kuukausittaisen laskutuksen sijaan,
- suojattuja yhteyksiä pitäisi olla vähintään 6 kpl,
- ratkaisun tulisi mahtua 1000 € budjettiin, työssä voisi kuitenkin esittää kolme eri hintaista ratkaisua.

Budjetti ja kulurakenne tulevat aiheuttamaan haasteita sovittaa yhteen, koska halvimmat vaihtoehdot ovat yleensä jatkuvalla laskutuksella toimivia ratkaisuja. Seuraavissa kappaleissa esitetään kolme vaihtoehtoista ratkaisua, jotka eroavat toisiltaan hintansa osalta.

2 Automaatiojärjestelmä

2.1 Automaatiojärjestelmän tarkoitus ja osat

Automaatiojärjestelmän tarkoitus on automatisoida prosesseja. Järjestelmän toiminta perustuu sensoreiden tuottamaan mittausdataan, ohjainlaitteen sisällä pyörivään ohjelmaan, sekä toimilaitteiden toimintaan. Automaatiojärjestelmän tarkoitus on valvoa ja hallita prosessin toimintaa ja kuntoa. (Opetushallitus, automaatiojärjestelmä, n.d)

Nykyaikainen automaatioprosessi sisältää useita eri komponentteja ja rajapintoja. Pääpiirteittäin kuvattuna automaatioprosessiin kuuluu kenttälaitteet ja instrumentit, ohjauslaite tai -laitteisto, mahdollinen pilvipalvelin, sekä ns. valvomo (Control room tai SCADA), josta voidaan prosessista riippuen joko monitoroida tai operoida prosessia käyttöliittymän avulla. (Opetushallitus, automaatiojärjestelmä, n.d)

Laitteet ja instrumentit koostuvat muun muassa sensoreista sekä toimilaitteista, jotka lähettävät ja vastaanottavat tietoa ohjausyksiköltä. Sensoreilla voidaan mitata monia eri suureita eli kerätä mittausdataa, jonka perusteella ohjausyksikkö lähettää ohjaussignaaleja toimilaitteille. Ohjausyksikkönä toimii useimmiten PLC eli ohjelmoitava logiikka. Sensorit ja toimilaitteet ovat kytkettynä logiikkaan sen Input- ja Output-moduulien kautta. (Opetushallitus, automaatiojärjestelmä, n.d)

PLC:ltä on muodostettu yhteys valvomoon, joka voi olla sanan varsinaisen merkityksen mukaisesti fyysinen valvontahuone, mutta nykyään langattomien yhteyksien ansiosta myös esimerkiksi kannettava tietokone. Tässä raportissa automaatiojärjestelmästä puhuttaessa käytetään sanaa ”valvomo” kuvaamaan mitä tahansa prosessiin kytkettyä tietokonetta, jonka avulla prosessin toimintoja monitoroidaan ja ohjataan. (Opetushallitus, automaatiojärjestelmä, n.d)

2.2 Tiedonsiirto

Automaatiojärjestelmät ovat kehittyneet vauhdilla eteenpäin niiden olemassaolon alusta lähtien. Järjestelmien perusrakenne, jota käsiteltiin edellisessä kappaleessa, on kuitenkin pysynyt samankaltaisena. Tarvitaan ohjausyksikkö, joka vastaanottaa tietoa sensoreilta, ja joka lähettää tietoa edelleen toimilaitteille ja ohjaa niitä siihen ladatun ohjelman perusteella. Näiden komponenttien keskinäinen tiedonsiirto on kuitenkin muuttunut monellakin tavalla ja edelleen vaihtoehtoja tämän toteuttamiseen on useita. Jokainen sensori ja toimilaite voidaan kytkeä logiikkaan parikaapeleilla, joka on alkuperäinen ja käytännössä yksinkertaisin tapa. Asennus- ja ylläpitovaiheessa tämä kuitenkin aiheuttaa huomattavan määrän työtä, koska johtojen määrä on verrannollinen laitteiden määrään. (Opetushallitus, automaatiojärjestelmä, n.d)

Nykyään suositaan enemmän väyläteknologioita, jotka yhden väylän avulla muodostavat automaatiojärjestelmästä yhtenäisen verkon. Enää ei kytketä jokaista laitetta erikseen logiikkaan, vaan yhdistetään logiikalta lähtevään runkokaapeliin. Eri kenttäväyläjärjestelmiä on useita, joita kuitenkin yleensä voidaan yhdistää gateway-komponenttien avulla toisiinsa. Väyläjärjestelmää käytettäessä kaapelin määrä pienenee huomattavasti. Väyläteknologiat eroavat keskenään mm. tiedonsiirtonopeuden, kytkentätopologioiden ja laitteiden maksimimäärän osalta. (Opetushallitus, automaatiojärjestelmä, n.d)

Uusi trendi alalla on Internet of Things eli “IoT” ja Industrial Internet of Things eli “IIoT”. Internet of Things -käsite tarkoittaa järjestelmää, jossa laitteet muodostavat keskenään verkon ja jakavat sen välityksellä tietoa keskenään. Nimikin toki erottaa kaksi edellä mainittua termiä toisistaan, mutta mikä on konkreettinen ero niiden välillä? IoT-laitteet ovat käyttäjäkeskeisiä, koska niiden tarkoituksena on tuottaa lisäarvoa käyttäjälle. Normaalin IoT-

laitteen vikatila tai rikkoutuminen ei myöskään yleensä aiheuta mittavia vahinkoja. IIoT-laitteet taas ovat suunniteltuja toimimaan vaativissa olosuhteissa ja ohjaamaan mm. öljy- ja kaasuteollisuuden prosesseja, joissa laitteiden vioittumisesta tai rikkoutumisesta aiheutuvat riskit ovat huomattavasti suurempia. (Tran, 2019; Rouse, 2020)

IoT:n toiminta perustuu tiedon keruuseen ja sen älykkääseen käsittelyyn. Laitteiden lähettämä data kerätään talteen, ja PLC:n ohjelmoinnin yhteydessä määritellyt algoritmit optimoivat järjestelmän toimintaa. Teknologia yleistyy nopeasti, koska sekä tekninen kehitys fyysisten laitteiden osalta, että koneoppiminen ja koodaaminen kehittyvät jatkuvasti. Tarjolla on paljon avoimen lähdekoodin (open source) ratkaisuja, jotka ovat kaikkien nähtävillä ja sovellettavissa. (Tran, 2019; Rouse, 2020)

IIoT mahdollistaa automaatiojärjestelmän toiminnan huomattavasti aiempaa tehokkaammin, koska sen avulla laitteet voivat siirtää dataa keskenään reaaliajassa. Järjestelmä voidaan siis ohjelmoida suorittamaan mittauksia ja monitoroimaan prosessia apuohjelmien avulla, ja reagoimaan mittaustuloksiin halutulla tavalla. Tällä tavoin saadaan kasvatettua järjestelmän tehokkuutta. VEneCT-projektissa IIoT-teknologian kiistattomia hyötyjä ovat palamismateriaalin määrän monitorointi, energiantarpeen ennustaminen kiireisimpinä tunteina, sekä energiantarpeen kysyntäjousto eli tarpeen mukauttaminen energian saatavuuteen. Tutkimusprojektin kannalta myös datan kerääminen on välttämätöntä kehityksen ja analyysien kannalta. (Tran, 2019)

3 Tietoturva

3.1 Tietoturva käsitteenä

Tietoturva on nykyisin virallisin standardein säädelty käsite, jolla tarkoitetaan teknisiä ja hallinnollisia toimia, jotka varmistavat jollekin taholle – kuten yritykselle – kuuluvan tiedon luottamuksellisuuden, eheyden, sekä käytettävyyden. Toisin sanoen tiedon tulee olla vain määrättyjen henkilöiden saatavilla ilman, että sitä voi luvattomasti muuttaa tai hyödyntää, jotta tietoturva toteutuu. Yllämainitut ehdot täyttyvät, kun kaikki tietoliikennealan toimitusketjun osapuolet noudattavat niille asetettuja oikeuksia ja velvollisuuksia. Aivan kuten muillakin aloilla tilaajilla, välittäjillä ja toimittajilla ovat omat vastuunsa, joita

noudattamalla liiketoiminnan harjoittaminen on turvallista ja potentiaalisesti kannattavaa. (Kyberturvallisuuskeskus, 2020)

Huomioitakoon myös, että tietoturva ei koske pelkästään informaatioteknologiaa, vaan sen toteutumiseen vaikuttavat huomattavasti myös inhimilliset tekijät. Vaikka monesti tietoturva-termi yhdistetään vain digitaaliseen tekniikkaan, ja tietoturvariski tarkoittaa mielikuvissa lähinnä hakkeroiduksi joutumisen uhkaa, näin ei suinkaan ole. Edellä mainitut periaatteet – luottamuksellisuus, eheys ja käytettävyys – ovat liiketoiminnan mahdollistavia arvoja, vaikka yritys ei omistaisi yhtäkään tietokonetta. Tietojen luvaton lukeminen, salakuuntelu, varastaminen, sekä fyysiset murrot ovat yhtälailla tietoturvariskejä, kuin hakkeroinnit ja tietomurrotkin. (Suomen Standardisoimisliitto, 2016)

3.2 Tietoturvan merkitys automaatiossa

Automaatioteknologiassa tietoturva on keskeisessä roolissa, koska varsinkin langattomien teknologioiden yleistyessä järjestelmien haavoittuvuus kasvaa. Käytännössä jokainen verkkoon yhteydessä oleva laite on potentiaalinen portti järjestelmään tunkeutujalle. Riskejä voidaan hallita asianmukaisilla toimilla, joista suurin osa on lähes kaikkien tiedossa olevia perusasioita.

Asianmukainen salasanasuojaus (verkko sekä laitteet), kaikkien laitteiden käyttöjärjestelmien sekä sovellusten pitäminen ajan tasalla ja pääsyn salliminen vain sitä tarvitseville henkilöille ovat kaikki asioita, joita noudattamalla ulkopuolisen luvaton tunkeutuminen järjestelmään vaikeutuu huomattavasti. Yhteyksien ja järjestelmien asianmukainen valvonta edistää myös tietoturvaa, varsinkin jos useammilla ihmisillä on pääsy järjestelmän verkkoon. Valvontaa voidaan toteuttaa pitämällä yllä lokia järjestelmään kirjautuneiden käyttäjien istunnoista. Sovellus tästä löytyy tämän raportin kappaleesta seitsemän, jossa esitellään Secomea-etäkäyttöjärjestelmän toimintaa.

3.3 Esimerkkejä teollisuuden automaatiojärjestelmien tietomurroista

Vakava suhtautuminen tietoturvaan automaatiossa on ensiarvoisen tärkeää, koska motiiveja tietomurron tekemiselle on enemmän, kuin moni tulee ajatelleeksi. Tietojen varastus,

kiristys, ilkivalta ja jopa politiikka voivat olla tietomurron taustalla. Tekniikan maailman artikkelissa (Niemi, 2017) kerrotaan, kuinka tuntematon hakkeriryhmä hyökkäsi mahdollisesti Saudi-Arabiassa sijaitsevan voimalaitokseen, ja sai haltuunsa osan voimalaitoksen työasemista. Hyökkäys pysäytti voimalaitoksen toiminnan hetkellisesti. Tuntematonta hakkeriryhmää on epäilty valtiorahoitteiseksi, ja artikkelissa kerrotaan Yhdysvaltalaisen CyberX-yrityksen epäilevän Iranin valtiota osalliseksi hyökkäykseen.

TM:n artikkelissa mainitaan, että hyökkäykseen käytetty haittaohjelma on läheistä sukua Joulukuussa 2016 Ukrainassa tehtyyn voimalaitokseen kohdistuneeseen hyökkäykseen, joka aiheutti laajasti sähkökatkoksia osassa Ukrainaa. Reuters (Finkle, 2017) kertoo hyökkäykseen käytetty haittaohjelma ”Stuxnet” on kehitetty vuonna 2010, ja sitä on laajasti uskottu käytettävän Yhdysvaltain ja Israelin toimesta Iranin ydinaseohjelmaan kohdistuneisiin hyökkäyksiin. Artikkelin mukaan Stuxnetin kaltaiset haittaohjelmat ovat muokattavissa ja kehitettävissä, jolloin niitä voidaan soveltaa muihinkin prosessiteollisuuden laitoksiin, ja mikä tekee niiltä suojautumisen entistä vaikeammaksi.

Kahden edellä mainitun artikkelin ja esimerkin esiin tuomisen tarkoitus on alleviivata sitä faktaa, että oli kyseessä sitten yhden logiikan yksinkertainen järjestelmä, tai satojen tuhansien ihmisten ja kotitalouksien energiasta vastaava valtava laitos, järjestelmään on mahdollista hyökätä. Tässä raportissa käsiteltävän järjestelmän haavoittumattomuus on äärimmäisen tärkeää, koska monitoroinnin lisäksi järjestelmää halutaan myös ohjata etänä. Tämä tarkoittaa, että järjestelmään murtautuja voisi päästä mahdollisesti muuttamaan prosessin arvoja eli hallitsemaan sen toimintaa käyttöliittymän välityksellä.

4 Langattomat verkkoyhteydet

4.1 WLAN

WLAN eli lähiverkko (”wireless local area network”) tarkoittaa kansainvälisten standardien mukaisia tietokoneiden liityntäverkkoja. WLAN-verkon kaupallinen nimi on WI-FI, joka viittaa kyseisiin standardeihin. WLAN-verkot toimivat maailmanlaajuisesti pääosin kahdella taajuusalueella, 2,4GHz ja 5 GHz -radiotaajuusalueilla. Kyseiset taajuusalueet on vielä jaettu useiksi kanaviksi. Kanavilla on hieman aluekohtaisia eroja maailmalla, mutta kaikki WLAN-tuella varustetut laitteet toimivat kuitenkin kaikkialla maailmassa. WLAN-perustuu standardiryhmään IEEE 802.11. WLAN on maailmalla hyvin yleinen, koska se on edullinen ja lähes kaikissa nykyään myytävissä kannettavissa tietokoneissa ja älypuhelimissa on WLAN-tuki sisäänrakennettuna ominaisuutena. (Viestintävirasto, 2014)

4.1.1 WLAN – tietoturva

WLAN-verkkoja voi luoda vapaasti. Kun laite on kytketään WLAN-verkkoon, on hyvä varmistaa verkon turvallisuus. WLAN-verkkoa on helppo käyttää haittaohjelmien levittämiseen siihen kytkettyihin laitteisiin. Avoimet ja tuntemattomat verkot ovat riski, koska hyökkääjät luovat luotettavan oloisia verkkoja, jotta käyttäjät liittyisivät niihin ja levittävät sitä kautta haittaohjelmia kytketyille laitteille. (Viestintävirasto, 2014)

Kodin WLAN-verkko kannattaa pitää salasanasuojattuna, ja varmistaa, ettei ulkopuolisilla ole siihen pääsyä, koska muuten kodin laitteet ovat vaarassa. Nykypäivän älykodeissa tämä voi aiheuttaa mittaviakin ongelmia, mikäli kaikki kodinkoneet ja lämmitysjärjestelmä ovat verkkoon kytkettynä, mikä ei tänä päivänä ole enää harvinaista. Tämä koskee myös automaatiojärjestelmiä, koska myös niiden suunnittelussa suositaan langattomuutta. Jos siis esimerkiksi PLC on kytkettynä haavoittuvaan WLAN-verkkoon, tunkeutuja voi saada järjestelmän haltuunsa helpostikin. (Viestintävirasto, 2014)

WLAN-käyttäjän kannattaa pitää huolta, että laitteiden ja tukiaseman välinen yhteys on salattu, jolloin sen lukeminen ei onnistu helposti ei-toivotuilta tahoilta. Yleisesti suositeltu salausmenetelmä on WPA2, joka käyttää ”Advanced Encryption Standard” -algoritmia. (Viestintävirasto, 2014)

4.1.2 Käyttö automaatiojärjestelmässä

Edellä esitettyyn tietoon nojaten voidaan todeta, että WLAN-yhteyden käyttö ei merkittävästi heikennä automaatiojärjestelmän tietoturvaa, kunhan laitteet on konfiguroitu asianmukaisesti, ja käyttö on ohjeiden mukaista. Joka tapauksessa jokainen ylimääräinen rajapinta järjestelmän ja yleisen verkon välillä tarjoavat mahdollisuuden hyökkäyksen yrittämiseen ja yrityksen arvokkaan tiedon varastamiseen (Digipooli, 2020). Alleviivattakoon tähän, että raportissa on tarkoitus käsitellä tietoturvaa yleisellä tasolla, eikä ottaa kantaa henkisiin tekijöihin ja motiiveihin tietomurtojen taustalla. Tästä syystä automaatiojärjestelmien tietoturvaa käsitellään kriittiseen sävyyn, vaikka todellisuudessa ei ole missään sanottua, että automaatiojärjestelmän sisältämä data olisi automaattisesti rikollisille erityisen arvokasta. Hyökkäyksen mahdollisuuteen ja haavoittuvuuteen tulee suhtautua kriittisesti, oli siihen etukäteen pääteltävissä olevaa motiivia tai ei, sillä hyökkäyksessä voi olla kyse ainoastaan ilkivallasta.

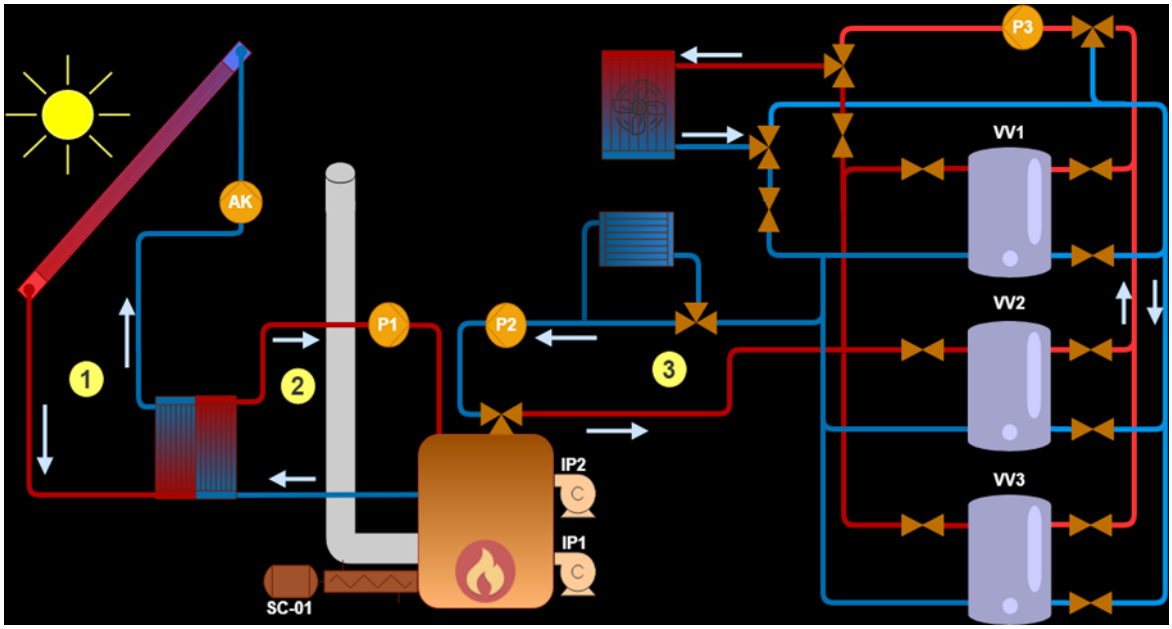
WLAN-yhteyden keskeinen etu automaatiojärjestelmän yhteydessä on langattomuus eli perinteisen kaapelilla kytketyn valvomon sijaan mahdollistetaan liikkuvuus verkon kantoalueella. Yrityksissä tämä ratkaisu onkin jo laajalti käytössä. Monet yritykset kuitenkin haluavat salata yhteytensä vielä tehokkaammin tai ohjata järjestelmää lähiverkon ulkopuolelta käsin, ja tämä voidaan mahdollistaa esimerkiksi VPN-yhteydellä, jota esitellään myöhemmin luvussa kuusi.

5 VEneCT-projekti

5.1 Yleisesti

VEneCT eli ”Vähähiilistä energiatehokkuutta mikro-CHP tekniikalla”, on Hämeen ammattikorkeakoulun tutkimusyksikön HAMK Techin tutkimusprojekti, jonka tarkoituksena on suunnitella ja rakentaa vähähiilisen biomassan palamisenergian sekä aurinkoenergian keräysprosessit optimoiva automaatiojärjestelmä. Järjestelmään on integroitu tietokanta tiedonkeruuta varten, sekä graafinen käyttöliittymä prosessien visualisointia ja etävalvontaa varten. Projektissa haluttiin hyödyntää nykyaikaista IoT-teknologiaa (Internet of Things) ja tästä nimenomaan teollisuuden käyttöön suunniteltua IIoT- eli (Industrial Internet of Things)-teknologiaa. Kuva 1. VEneCT-kaavio on laitoksen kaaviokuva, joka on poimittu järjestelmän web-applikaatiosta. (Tran, 2019)

Kuva 1. VEneCT-kaavio (Truong)

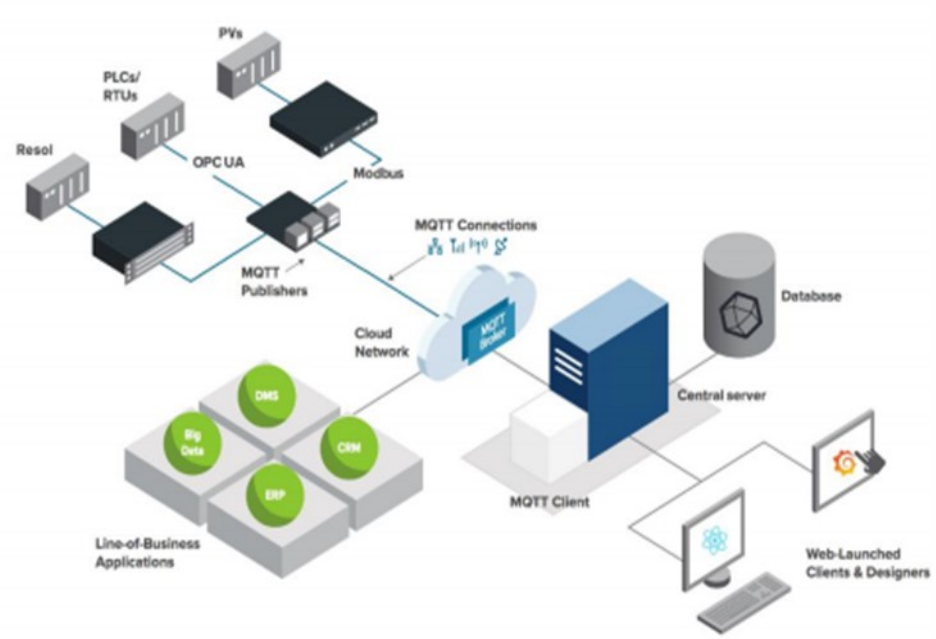


5.2 Järjestelmän rakenne

Automaatiojärjestelmä voidaan jakaa kolmeen eri tasoon, joita ovat kenttälaitteet, ohjaustaso, sekä valvontataso. Tasot ovat numeroitu pienestä suurimpaan edellä mainitussa järjestyksessä. Kenttälaitetasolle kuuluvat sensorit ja toimilaitteet, jotka siirtävät dataa

ohjaustasolle monitorointia ja analyysiä varten. Kuva 2 (Tran, 2019) nähdään kaavio automaatiojärjestelmän rakenteesta. Kuvan alkuperäinen lähde on Inductive Automation (2019). (Tran, 2019)

Kuva 2. Automaatiojärjestelmän rakenne (Tran, 2019)



Ohjaustasolle kuuluvat PLC, Resol sekä PV, joiden tehtävä on kerätä data kenttälaitteilta järjestelmään. Laitteet ovat kytketty toisiinsa Modbus-väylää, OPC UA:ta sekä MQTT-protokollaa (Message Queuing Telemetry Transport) käyttäen. Ohjaustason laitteistosta Resol ja PV keräävät dataa, kun taas PLC pyörittää itse ohjelmaa. PLC:n ohjelmaan on määritetty algoritmeja, joiden perusteella – mittausdataa hyödyntäen – PLC pyrkii maksimoimaan järjestelmän energiatehokkuutta. (Tran, 2019)

Palvelin ja sen sisältämät sovellukset kuuluvat kolmannelle- eli valvontatasolle. Kaikki järjestelmästä saatava data varastoidaan tietokantaan, ja siitä muodostetaan web-applikaatiossa nähtävät mittaustulokset. Käyttöliittymän avulla datasta voidaan muodostaa myös graafisia kuvaajia prosessin analysointia varten. Web-applikaatio on yksinkertaistettu graafinen kaavio järjestelmästä kokonaisuutena, jossa mittauspisteet on sijoiteltu totuudenmukaisesti eli oikeille paikoilleen. Näin ollen graafisesta käyttöliittymästä voidaan suoraan seurata prosessin toimintaa. (Tran, 2019)

6 Etäyhteysteknologiat

6.1 VPN

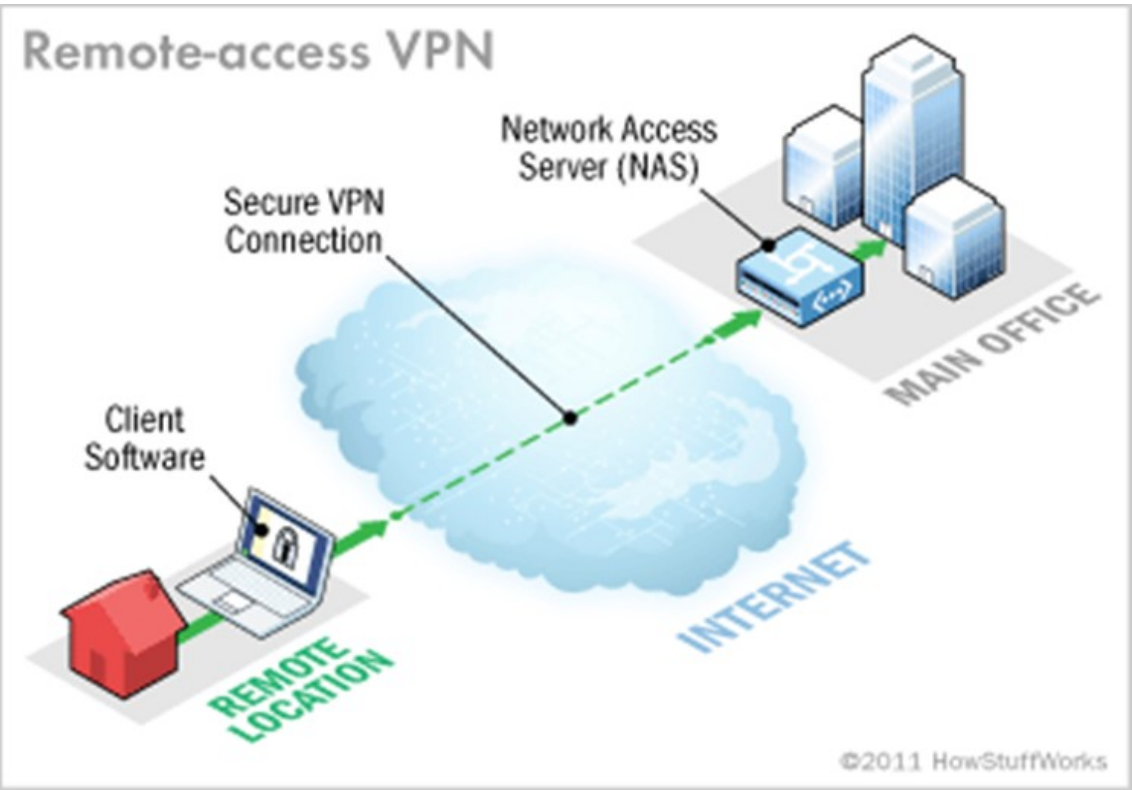
VPN eli ”Virtual Private Network” tarkoittaa verkkoyhteyttä, jonka avulla kuluttaja ei ole normaalin ISP:n (”Internet Service Provider”) serverin, vaan salatun VPN-serverin kautta yhteydessä internetiin. VPN-serverin kautta yhdistettäessä laitteen oma IP-osoite piilotetaan, ja internet-sivustoilla laitteen IP-osoite on piilotettu ja verkkosivustot näkevät ainoastaan VPN-serverin osoitteen. (Vpnyhteys, 2020)

VPN on alun perin luotu yrityksille mahdollistamaan etätyöntekijöiden työskentely yrityksen omassa verkossa, mutta nykyään sen käyttö on yleistynyt myös kuluttajien keskuudessa. Suurin VPN:n hyöty kuluttajalle on anonymiteetti verkossa, sekä tiettyjen verkkosivustojen tai palveluiden alueellisten käyttörajoitusten kiertomahdollisuus. Varsinkin ilmaisten palveluiden yhteydessä kannattaa pitää mielessä, että vaikka internet-palveluntarjoaja ei näe asiakkaan verkkoliikennettä servereidensä kautta, VPN-palveluntarjoajalla on mahdollisuus päästä dataan käsiksi. Joissakin Euroopan maissa, kuten esimerkiksi Iso-Britanniassa sekä Ranskassa, VPN-palveluntarjoajien on pidettävä rekisteriä asiakkaistansa ja heidän verkkoliikenteestään, minkä perusteena on terrorismin ehkäisy. Monesti siis aivan täydellinen yksityisyys verkossa jää saavuttamatta. (Vpnyhteys, 2020)

VPN:n toimintaa voidaan kuvainnollisesti verrata tunneliin. VPN-serveri luo turvallisen ”tunnelin” käyttäjän laitteen ja internetin välille, joka estää ulkopuolisia tahoja pääsemästä siirtämääsi dataan käsiksi. Monissa yhteyksissä tästä käytetänkin termiä VPN-tunneli. Suojatun väylän lisäksi VPN-palveluntarjoajan ohjelma laitteella salaa yhteyden laitteen ja VPN-serverin välillä eli jo ennen varsinaista VPN-tunnelia. VPN-palveluntarjoajien kesken tämän datan salaus- eli kryptausalgoritmeissa on hieman eroja. VPN-palveluntarjoajan valinnassa kannattaa siis huomioida palvelun hintalaatusuhde, jotta palvelu vastaa asiakkaan toiveita ja mielikuvia. Esimerkiksi ilmaisten VPN-palveluiden ”hinta” asiakkaalle on usein se, että selaustietoja myydään mainostajille, mikä mahdollistaa yritykselle kalliin VPN-serverin ylläpidon. (Marks, 2020)

Yrityksille järjestelmien etäohjaamista varten markkinoilla on kaksi erilaista VPN-ratkaisua: Pilvipohjainen ”hosted VPN”, sekä perinteinen ilman pilvipalvelua toimiva ”Self-hosted VPN”. Seuraavissa kappaleissa käsitellään näiden mallien keskeisiä eroja. Alapuolella Kuva 3 on yksinkertaistettu kaaviokuva havainnollistamassa VPN-yhteyden toimintaa. (Griffith, 2020)

Kuva 3. VPN-yhteys kaavio (Tyson ;Pollette;& Crawford, 2019)



6.1.1 Pilvipohjainen VPN

Pilvipohjainen ratkaisu eli hosted VPN on kahdesta vaihtoehdosta yksinkertaisempi ja halvempi, joskin se sisältää tiettyjä rajoituksia palvelun tilaajalle. Menetelmän yksinkertaisuus johtuu siitä, että se sisältää vähemmän fyysisiä laitteita sekä konfigurointia. Kun yritys ostaa palveluntarjoajalta reitittimen, siinä on valmiiksi yhteys pilvipalvelimeen, josta se hakee automaattisesti asetuksensa. Sen asentaminen ei edellytä muutoksia yritysverkon palomuuriin, eikä sen ylläpitäminen vaadi verkkoteknologioiden asiantuntijuutta. Palvelun hankkiminen ja käyttäminen on siis mahdollista, vaikka yrityksessä ei olisi IT-ammattilaisia vastaamassa siitä. (Griffith, 2020)

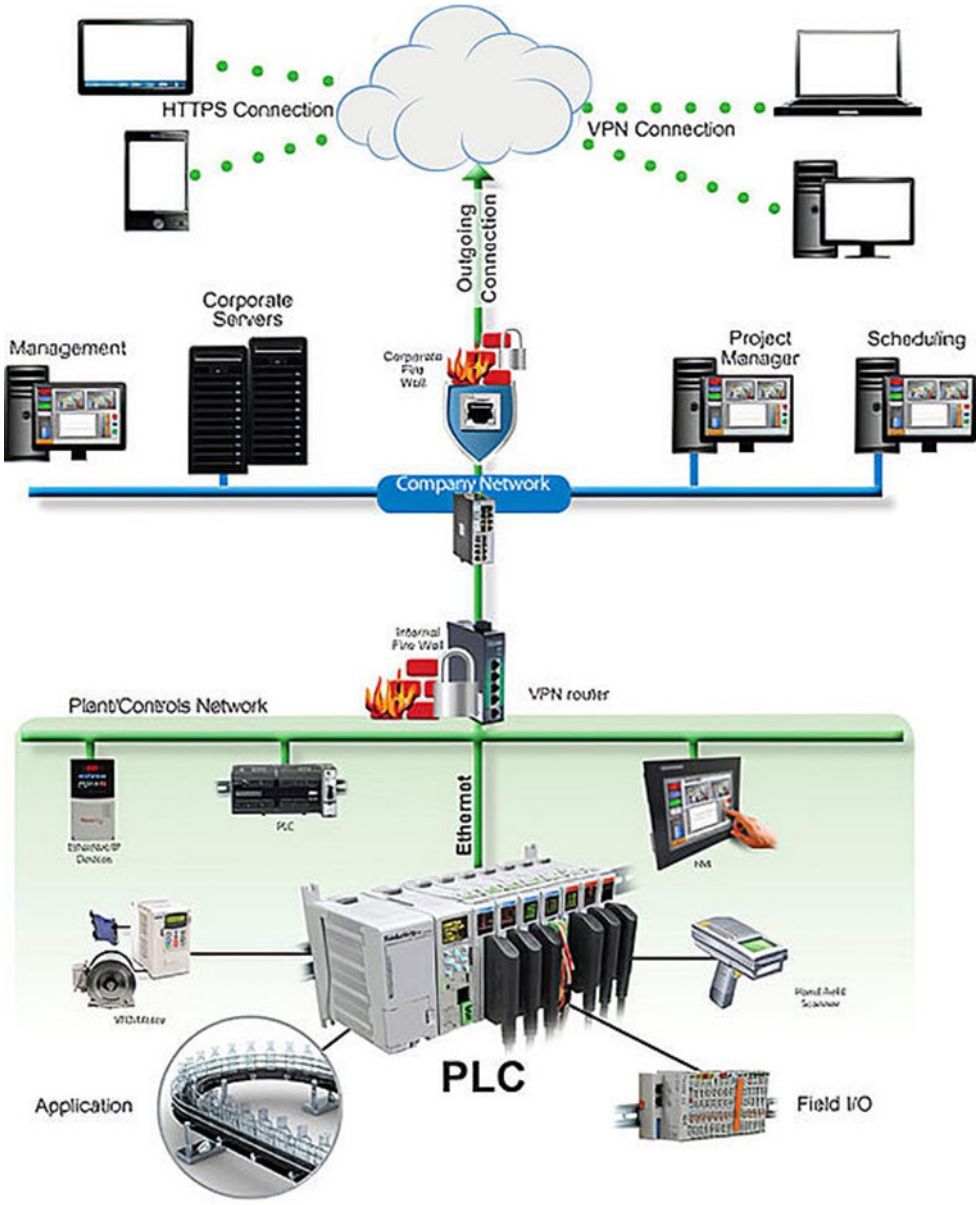
Pilvipohjaisen järjestelmän sisältämät rajoitteet puolestaan koostuvat siitä, että kaistanleveyttä ei yleensä ole rajattomasti. Palveluntarjoajat ovat porrastaneet hinnastonsa kuukausikohtaisen datan käyttömäärän mukaan eli mikäli järjestelmän kautta siirretään suuria määriä dataa, saattaa palvelun juoksevat kulut nousta korkeiksi. Esimerkiksi videonsiirto tai jatkuva monitorointi tarvitsevat kaistanleveyttä niin paljon, että perinteiseen vaihtoehtoon siirtyminen voi olla perusteltu investointi. (Griffith, 2020)

Hosted VPN-vaihtoehdossa reititin kytketään yritysverkon ja automaatiojärjestelmän väliin. Sen sisäinen palomuuri erottaa verkot toisistaan. Pilvipohjaisen VPN-yhteyden toiminta perustuu site-to-site-, sekä Internet Protocol security (IPsec) -tekniikoihin. site-to-site tarkoittaa kahta verkkoa, jotka ovat yhdistettynä toisiinsa virtuaalisesti. IPsec-protokollalla salataan verkkojen välillä kulkeva data, ja tällä tavoin muodostetaan täysin turvallinen VPN-tunneli. IPsec-protokollassa on kaksi eri tilaa: Kuljetus- ja tunnelointitila. Kuljetustilassa salataan verkkojen välisen datapaketin sisältö, kun taas tunnelointitilassa salataan koko datapaketti. (Griffith, 2020; Perimeter 81, 2020)

Client-tietokone on turvallisesti yhteydessä palvelimeen SSL/TLS ja TLS 1.2.-salausprotokollien avulla. TLS-kättely eli key exchange suoritetaan standardien mukaisilla 2048-bit RSA- ja SHA-256-salausalgoritmeilla. WLAN- sekä 4G LTE-tuen ansiosta verkkoon voi ottaa yhteyttä langattomasti eli ilman LAN-yhteyttä tietokoneen ja reitittimen välillä. Tämä mahdollistaa etäyhteyden käyttämisen yrityksen lähiverkon ulkopuolelta. (Griffith, 2020)

VPN-verkon sisäisten salaus- ja turvallisuusprotokollien lisäksi yrityksissä monesti käytetään mm. kaksivaiheista tunnistautumista tietoturvan lisäämiseksi. Kaksivaiheinen tunnistus toimii esimerkiksi siten, että käyttäjätunnuksen ja salasanan syötettyään, kirjautumista yrittävälle käyttäjälle lähetetään vahvistettuun matkapuhelinnumeroon tekstiviestillä varmennuskoodi, jonka syötettyään käyttäjä pääsee kirjautumaan verkkoon. Joissakin tapauksissa voidaan koodin sijaan käyttää biometrisia tunnisteita, esimerkiksi kasvojentunnistusta tai sormenjälkitunnistinta henkilöllisyyden varmentamiseksi. Kuva 4 alapuolella on kaavio yritysverkon rakenteesta, jossa pilvipohjainen VPN on kytkettynä. (Griffith, 2020)

Kuva 4. Pilvipohjainen VPN (Griffith, 2020)



6.1.2 Perinteinen VPN

Perinteisessä VPN-yhteydessä ei käytetä pilvipohjaista palvelua lainkaan, vaan yhteyden muodostamiseen tarvitaan kaksi reititintä. Sen muodostaminen ja konfigurointi vaatii enemmän työtä ja taloudellisia resursseja. Tämä menetelmä on käytössä lähinnä suurilla yrityksillä, joiden täytyy siirtää suuria määriä dataa verkon kautta. Menetelmä profiloituu

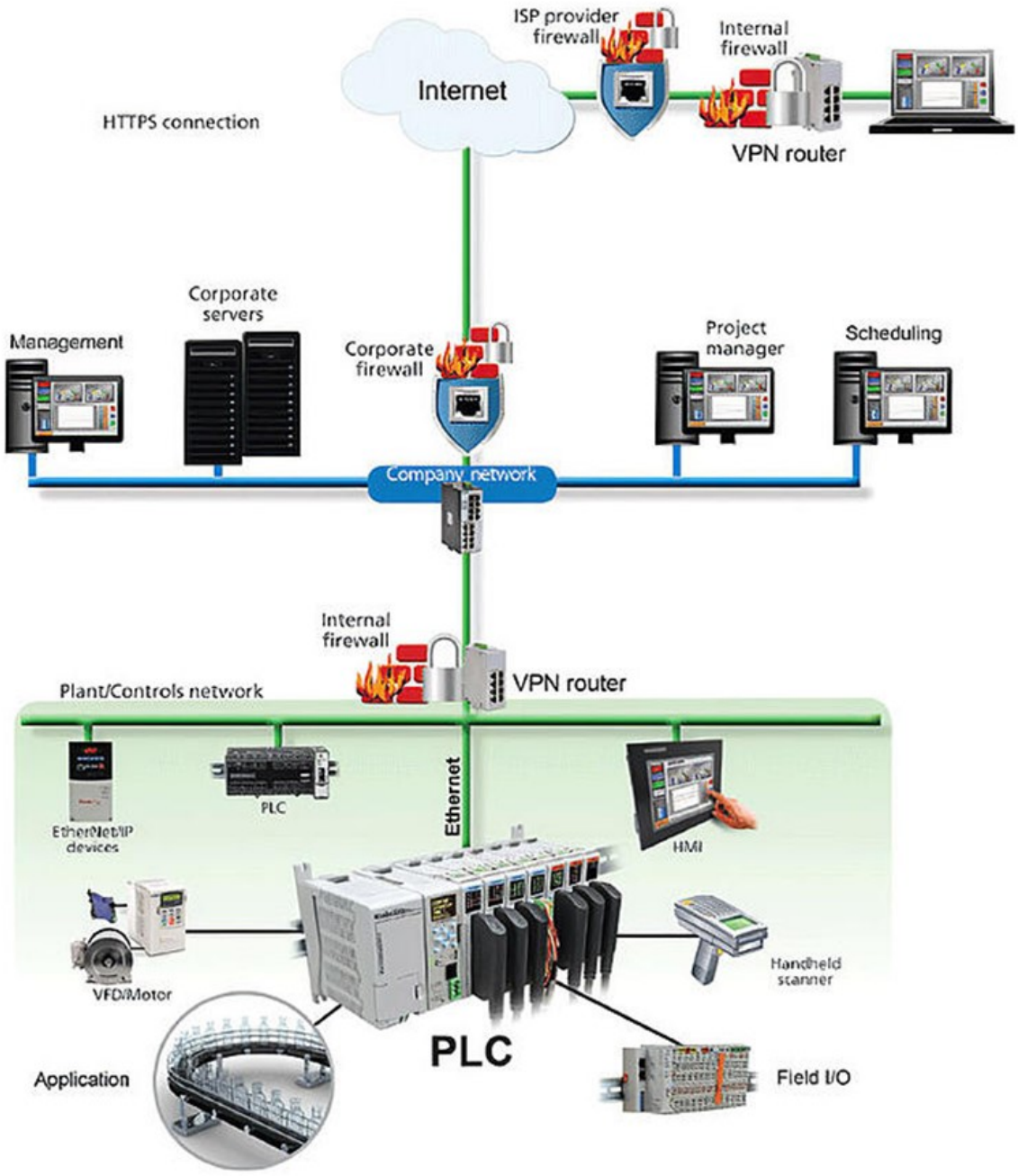
suurempien yritysten käyttöön myös siksi, että se vaatii oman IT-henkilöstön konfigurointiin ja ylläpitoon. (Griffith, 2020)

Laitekustannukset ja IT-henkilöstön kulut tekevät kyseisestä menetelmästä kalliin. Käyttökustannukset VPN-palveluntarjoajan osalta ovat pilvipohjaista VPN:ää pienemmät, koska yritystä ei laskuteta käytön ja datamäärän perusteella. Perinteisessä VPN-yhteydessä joudutaan konfiguroinnin yhteydessä avaamaan yritysverkon palomuuri, mikä tuottaa työtä. Kun verkkoon joudutaan luomaan ns. heikko kohta, sitä joudutaan suojaamaan ja valvomaan aktiivisesti, koska ei-toivotut tahot eivät tietenkään saa pystyä käyttämään porttia verkkoon murtautumiseen. (Griffith, 2020)

Yritysverkon palomuuriin tehtävät muutokset tuovat mukanaan lukuisia pakollisia toimenpiteitä, joista yrityksen täytyy itse pitää huolta. Toimenpiteet edellyttävät vahvaa tietoteknistä osaamista verkkoteknologioiden osalta, jotta etäyhteyttä voidaan käyttää turvallisesti. Jokainen client-tietokone täytyy konfiguroida erikseen, eli käytännössä IT-osaston palkkaaminen yritykseen tai sen olemassaolo on välttämätöntä. Kuva 5 on esitetty kaaviokuva perinteisestä VPN-yhteydestä. (Griffith, 2020)

Menetelmää kutsutaan perinteiseksi VPN:ksi, koska se oli ainoa turvallinen etäyhteysmenetelmä ennen pilvipohjaisten menetelmien keksimistä ja markkinoille tuomista. Tiivistetysti voidaan todeta, että se on paras tapa turvallisen etäyhteyden muodostamiseksi, jos sen kautta siirrettävä datamäärä edellyttää suurta kaistanleveyttä, ja jos yrityksellä on varaa ylläpitää IT-henkilöstöä sekä pääverkon, että sivuverkon luona. Tässä ratkaisumallissa ei myöskään tarvitse luottaa ulkoisen palveluntarjoajan tuottamaan ja ylläpitämään verkkoon. Kumpaakin menetelmää pidetään siitä huolimatta yhtä turvallisena ratkaisuna, koska onhan tietojen varastaminen, salakuuntelu tai luvaton käyttö rikollista toimintaa, josta joutuu vastuuseen. (Griffith, 2020)

Kuva 5. Perinteinen VPN (Griffith, 2020)



6.2 OPC UA

OPC UA on käyttöjärjestelmästä riippumaton standardi automaatioteollisuudessa, ja se on kehitetty eri informaatiojärjestelmien integroimiseksi. Se on OPC Foundationin kehittämä

IoT-ratkaisu eri valmistajien laitteiden, ohjelmistojen ja koneiden kommunikointiin yhteisen rajapinnan avulla. OPC Foundation -järjestössä ovat mukana kaikki automaatiotekniikan suurimmat toimijat, kuten esimerkiksi Siemens, ABB ja Beckhoff. Alkuperäinen OPC Classic kehitettiin vuonna 1996, mutta sen ongelmaksi muodostui ajan saatossa se, että se oli Windows-käyttöjärjestelmästä riippuvainen, eikä se pystynyt enää täyttämään automaatiotekniikan tietoturvavaatimuksia. OPC UA:n ensimmäinen versio julkaistiin vuonna 2008. OPC Classicin laajasta suosiosta ja yleisesti hyväksytystä teknologiasta johtuen OPC UA sisältää OPC Classicin toiminnot (Heikkilä, 2016, s. 7; OPC Foundation, Unified Architecture, n.d; OPC Foundation, What is OPC?, n.d)

Tällä hetkellä maailmassa on yli 22 000 laitetta 3 200 eri toimittajalta, jotka käyttävät OPC-standardia. OPC UA soveltuu eri tasojen tiedonsiirtoon automaatiotekniikassa, sillä sitä voi käyttää kenttälaitteiden ja automaatiojärjestelmän väliseen tiedonsiirtoon, mutta myös ylemmän tason kommunikointiin esimerkiksi kunnossapitojärjestelmien, valmistuksenohjausjärjestelmien ja toiminnanohjausjärjestelmien välille. OPC UA -sovelluksia voidaan kehittää Java-, ANSI C-, C++ ja .NET-ympäristöihin laitetoimittajista riippumatta. (Heikkilä, 2016, s. 11)

6.2.1 Ominaisuudet

OPC-standardin vanhin määrittely on OPC Data Access, jonka rajapintaa käytetään prosessissa datan lukemiseen, kirjoittamiseen ja monitorointiin. Tätä hyödynnetään pääasiassa tiedon reaaliaikaiseen siirtämiseen logiikoilta tai hajautetuista järjestelmistä paikallisiin käyttöliittymiin, sekä valvomosovelluksiin. OPC DA:n käyttäjä valitsee käyttöliittymässä luettavat muuttujat ja muodostaa yhteyden palvelimelle luomalla OPC-palvelin-olion. Kyseessä on ylimmän tason olio OPC:n hierarkiassa, jonka avulla osoiteavaruudesta voidaan paikantaa haluttu tietolähde. Tietolähde voi olla esimerkiksi kenttälaite, tai jokin tietty muistialue PLC:ssä. Asiakkaan on luotava OPC-ryhmäolioita tietolähteille päästäkseen dataan käsiksi. (Heikkilä, 2016, s. 8; OPC Foundation, Classic, n.d)

OPC Alarm and Events -rajapintaa käytetään prosessin ilmoitusten ja hälytysten vastaanottamiseen. Ilmoitukset voivat kertoa prosessissa määriteltyjen ehtojen täyttymisestä. Hälytykset taas kertovat muutoksista, esimerkiksi pinnankorkeuden ala- tai

ylärajan ylittymisestä. Hälytykset on mahdollista myös kuitata rajapinnan kautta. Hälytykset ovat määritelty itse prosessissa, esimerkiksi logiikassa, joten rajapinta ei itse tuota niitä, vaan välittää niitä eteenpäin. Rajapinnan käyttämiseksi OPC-asiakkaan on otettava yhteyttä palvelimelle ja tilattava hälytykset ja ilmoitukset. Käyttäjällä on mahdollisuus asettaa suodatuksia eli filttereitä ilmoituksille, jos hän haluaa vastaanottaa vain tiettyjä hälytyksiä. (Heikkilä, 2016, s. 9; OPC Foundation, Classic, n.d)

OPC Historical Data Access tarjoaa nimensä mukaisesti pääsyn vanhaan, varastoituun prosessidataan. Datavarastona voidaan käyttää SQL-kyselykieltä käyttäviä palvelintietokantoja, joita tarjoavat muun muassa Microsoft, Oracle ja IBM. OPC-asiakkaan on otettava yhteys palvelimelle luomalla OPCHDA-palvelin-olion, joka tarjoaa historiadatan lukemiseen tarvittavat rajapinnat ja metodit. Dataa voidaan lukea kolmella eri tavalla. Ensimmäinen tapa on kerätä dataa varastosta aika-alueen, jolta haluaa lukea yhden tai useamman muuttujan arvoja. Toinen tapa on lukea arvoja (yksi tai useampi muuttuja) tietyllä aikaleimalla. Kolmas tapa on kerätä arvoja ja suorittaa laskutoimituksia sen perusteella. Laskutoimituksia voi olla vaikkapa minimi-, maksimi- ja keskiarvojen määrittäminen. (Heikkilä, 2016, s. 10; OPC Foundation, Classic, n.d)

OPC Classicin aikana nämä rajapinnat olivat erillisiä määrittelyjä standardissa, mutta OPC UA:n julkaisussa rajapinnat olivat yhdistetty yhdeksi laajennetuksi määrittelyksi. (Heikkilä, 2016, s. 11; OPC Foundation, Classic, n.d)

6.2.2 Tiedonsiirtoprotokollat

Tiedonsiirtokerros voidaan toteuttaa tällä hetkellä joko OPC Foundationin määrittelemällä UA TCP-, HTTPS-, tai SOAP/HTTPS-protokollalla. UA TCP on binäärikoodattua dataa, joka lähetetään TCP/IP:n yli. SOAP/HTTPS (”Simple Object Access Protocol” / ”Hypertext Transfer Protocol Secure”) -protokolla on yleisesti käytössä web-palveluissa tietoturvaominaisuuksien, sekä palomuuriystävällisyyden vuoksi. SOAP/HTTPS-protokolla tarkoittaa SOAP-kommunikaatiota HTTPS:n yli. SOAP on tietoliikenneprotokolla, jonka avulla mahdollistetaan proseduurien etäkutsu ja järjestelmien välinen tiedonvaihto. HTTPS tarkoittaa HTTP-protokollaa, jonka yhteydessä käytetään TLS-salausta. TLS puolestaan on salausprotokolla, jolla salataan verkon yli tapahtuvaa tietoliikennettä. Vaikka

tiedonsiirtokerros ei kuitenkaan ole protokollariippuvainen, OPC UA:n kehittäjät ovat määritelleet kyseiset palvelut ja konseptit käytettäväksi, jotta voidaan taata yhteensopivuus eri tuotteiden välille ja säilyttää avoimuus tulevaisuuden teknologioille. (Heikkilä, 2016, s. 32; Tahvanainen & Aro, 2015)

Standardissa on määritelty kaksi tapaa datan koodaukselle: XML, sekä binääri. Siitä huolimatta standardissa on jätetty mahdollisuus käyttää muitakin tekniikoita tulevaisuudessa. Binääri-tekniikan etuna on nopea koodaus ja dekoodaus pienen viestikoon ansiosta. Koodauksessa käytetään primitiivisiä datatyyppejä (built-in data types) kummallakin tekniikalla. Esimerkkejä primitiivisistä tietotyypeistä ovat mm. liukuluvut ja kokonaisluvut. Binäärikoodaus toimii kääntämällä primitiiviset datatyypit binäärimuotoon jaksottaisesti binäärijonoiksi. XML WS eli Extensible Markup Language Web Services on merkintäkieli, joka on sekä ihmisen, että koneen luettavissa, ja joka mahdollistaa kommunikoinnin minkä tahansa web-palvelua tukevan järjestelmän kanssa. Formaatti auttaa laajojen tietomassojen jäsentelyssä. XML-formaatissa suurin osa datatyypeistä on koodattu noudattamalla yleisiä XML-spesifikaatioita W3C04a ja W3C04b, joitakin rajoituksia ja erikoistapauksia lukuun ottamatta. (Heikkilä, 2016, s. 32; Tahvanainen & Aro, 2015)

6.2.3 Suorituskyky

OPC UA käyttää eri siirtotekniikoita ja protokollia täyttääkseen mahdollisimman monet eri vaatimukset ja varmistaakseen standardin skaalautuvuuden. OPC UA:n kehityksessä oli tavoitteena oli parantaa suorituskykyä verrattuna OPC Classiciin. Suorituskyky tässä kontekstissa ei kuitenkaan tarkoita pelkästään tiedonsiirtonopeutta, vaan ennen kaikkea pienempää kuormaa ja resurssivaatimuksia käytössä olevalta järjestelmältä. Suorituskykyyn vaikuttaa muun muassa siirto- ja koodausmenetelmä, mutta myös moni muu asia. Sovelluskerros, sovelluksen integrointi UA-pinon kanssa, kommunikaation tietoturvataso sekä käytettävä laitteisto vaikuttavat suorituskykyyn, jonka voidaankin todeta oleva monen eri tekijän summa. OPC UA:n suorituskykyä on tutkittu akateemisesti muun muassa Saksalaisen Ostwesfalen-Lippe yliopiston Institute of Industrial IT-osaston, sekä Suomalaisen ohjelmistoyritys Prorys Oy:n toimesta. Edellä mainitun Saksalaisyliopiston tutkimuksessa tutkittiin OPC UA, CoAP ja MQTT -protokollien tiedonsiirtokäyttäytymistä emuloiduissa EDGE-, UMTS-. ja LTE-verkoissa. OPC UA käytti testissä vähiten aikaa tiedonsiirtoon kaikissa

tapauksissa, vaikka aiemmin OPC UA:n viestin oli todettu olevan yleiskustannukseltaan korkein, sen hyötykuorman lisäksi verkkoon aiheuttaman merkittävän lisäkuorman takia. Testissä ei kuitenkaan kerrottu, mitä tietoturvaprofiilia OPC UA:n tapauksessa käytettiin. Testi on referoitu Mikko Heikkilän Tampereen ammattikorkeakoululle tekemässä ylemmän AMK-tutkinnon opinnäytetyössä. Prosys Oy:n omassa testissä mielenkiintoisin aspekti on eri laitteiden välinen ero salausalgoritmien purkamisajoissa. Dell:n valmistama Intel Core i7 -prosessorilla varustettu kannettava tietokone osoittautui peräti 20 kertaa Raspberry Pi:tä nopeammaksi. (Heikkilä, 2016, ss. 40-44; Tahvanainen & Aro, 2015)

6.2.4 Tietoturva

Koska kyseessä on useilla järjestelmäalustoilla ja erilaisissa ympäristöissä käytettävä teknologia, tietoturva-arkkitehtuurin on oltava joustava ja yleiskäyttöinen. OPC UA:n tietoturvakonsepti perustuu käyttäjän tunnistukseen, käyttöoikeuksiin, sertifikaatteihin sekä sovellusten todentamiseen ja turvattuun tiedonsiirtokanavaan. Yleiskäyttöisyys ja tietoturvatason skaalautuvuus toteutetaan erilaisilla tietoturvaprofiileilla, jotka määrittelevät sovellusten välisen kommunikaation tietoturvatason. Profiileissa on määriteltynä erilaisia algoritmeja ja avaimia, joita kommunikoinnin salaamiseen käytetään. Profiileja on neljä, ja niitä ovat: None, Basic128RSA15, Basic256 ja Basic256SHA256. Esimerkiksi internetin yli kommunikoivien sovellusten kommunikoinnissa voidaan käyttää raskainta profiilia, jossa kaikki viestit allekirjoitetaan ja salataan. Vastapainoksi suljetun verkon sisällä kommunikoivien laitteiden väliset viestit voidaan hyvin toimittaa ilman salausta, tai pelkällä allekirjoituksella. Tämän avulla säästetään laitteiden resursseja, kun niiden ei tarvitse käyttää laskentatehoa raskaiden salausten purkuun. On olemassa myös laitteita, joiden prosessointiteho ei edes riittäisi salausten purkuun. (Heikkilä, 2016, ss. 45-61; Tahvanainen & Aro, 2015)

OPC UA-standardissa käytetään myös tietoturvasertifikaatteja, joita on kolmea eri tyyppiä: Sovellussertifikaatit, ohjelmistosertifikaatit, sekä käyttäjäsertifikaatti. Ensimmäiseksi mainittu on digitaalinen sertifikaatti, jota käytetään yksittäisten sovellusten tunnistamiseen, sekä myös viestien allekirjoitukseen ja salaukseen asymmetrisessä tietoturvamenettelyssä. Ohjelmistosertifikaatti tunnistaa kyseessä olevan tuotteen, ja se sisältää tiedot profiileista, joita sovellus tukee. Istunnon luomisvaiheessa sovellukset välittävät tiedot tuetuista

ominaisuuksista, joiden perusteella sovellukset päättelevät, voivatko ne kommunikoida keskenään asianmukaisesti. Mikäli asiakkaan sertifikaatti ei vastaa palvelimen vaatimuksia, palvelin voi kieltäytyä aktivoimasta istuntoa. Ohjelmistosertifikaatti toimitetaan tuotteen toimituksen yhteydessä. Käyttäjäsertifikaatin avulla tunnistetaan sovelluksen käyttäjä istunnon aktivoinnin yhteydessä. (Heikkilä, 2016; Tahvanainen & Aro, 2015)

Muita mahdollisuuksia tunnistamisen toteuttamiseksi ovat muun muassa käyttäjätunnus ja salasana tai Web-sovellusvaltuus. Mahdollista on myös käyttää sovellusta anonyymisti, eikä tässä tapauksessa käyttäjää tunnisteta. Sertifikaattien hallinnointijärjestelmä tulee valita järjestelmän laajuuksien ja vaatimusten perusteella. Esimerkiksi laajoissa järjestelmissä sertifikaatteja ei kannata ylläpitää manuaalisesti, koska se on työlästä ja kuluttavaa. Ylläpitäjän pitäisi kopioida palvelinten julkiset avaimet ja siirtää ne kaikkiin asiakassovelluksiin, joiden kanssa järjestelmän pitäisi kommunikoida ja toisinpäin. Sertifikaatit myös vanhenevat määrätyn ajan jälkeen, jolloin tämä proseduuri pitäisi aina toistaa. Tästä syystä ainoastaan pienissä, tarkoin määritellyissä järjestelmissä manuaalinen sertifikaattien ylläpitäminen voi olla perusteltua. (Heikkilä, 2016, ss. 45-61; Tahvanainen & Aro, 2015)

Kun tiedonsiirto toteutetaan binäärimuotoisesti, se perustuu OPC UA TCP -protokollaan. Tällöin tietoturva toteutetaan OPC UA Secure Conversation- eli UASC-protokollalla, joka on binäärinen versio web-sovellusten välisen liikenteen turvaamiseen käytettävästä Web Sercives Secure Conversation-spesifikaatiosta. UASC on koko OPC UA-standardin mukaisesti suunniteltu toimimaan eri tiedonsiirtoprotokollien ja rajoitetulla suorituskyvyllä varustettujen laitteiden kanssa. UASC pilkkoo lähetettävät viestit lohkoihin, joiden puskurikoot UASC:n käyttövaatimusten mukaan vähintään 8196-kilotavua, mutta jotka ovat pienempiä, kuin käytettävän protokollan määrittelyn mukaan. UASC-viesti koostuu kolmesta otsikosta: Runko-osasta, alatunnisteesta ja allekirjoituksesta. (Heikkilä, 2016, ss. 45-61)

Viestiotsikko on UASC-viestin ensimmäinen osa, joka on esimerkiksi pyyntö salatun tiedonsiirtokanavan avaamiseen, sulkemiseen tai sovellusten välisen istunnon luomiseen. Seuraavana viestissä on symmetrinen tai asymmetrinen tietoturvaotsikko. Asymmetrinen otsikko tarkoittaa sitä, että siihen sisältyy tieto viestin tietoturvamenettelyistä, joita ovat esimerkiksi salaus-algoritmit ja lähettäjän sertifikaatti. Lähettäjän sertifikaatin avulla

vastaanottaja voi purkaa ja varmentaa viestin. Asymmetrisiä salausalgoritmeja käytetään kuitenkin ainoastaan OpenSecureChannel-palvelupyyntöihin liittyvien viestien yhteydessä, koska ainoastaan kyseisen palvelun yhteydessä viestit turvataan julkisilla ja yksityisillä avaimilla. Symmetristä salausta käytetään kaikkeen liikenteeseen OpenSecureChannel-palveluita lukuun ottamatta. Symmetrisen salauksen tietoturvaotsikko sisältää ainoastaan tunnisteen, joka identifioi viestin salaus- ja allekirjoitusavaimet. (Heikkilä, 2016, ss. 45-61)

6.2.5 Yhteenveto

OPC UA on kasvavaan tarpeeseen kehitetty monipuolinen ja skaalautuva etähallintajärjestelmä. Tietoturva on selkeästi ollut kehittävän tahon eli OPC Foundationin prioriteettilistalla korkealla, mikä onkin järkevää. Luottamusta OPC UA-standardissa herättää se, että sitä kehitetään jatkuvasti ja ennen kaikkea se, että kehityksestä vastaa alan suurimmat toimijat. Vaikka ratkaisuja on kehitetty tietoturva edellä uusimpia salausalgoritmeja hyödyntäen, myöskään suorituskyvystä ei ole tingitty. Järjestelmän skaalautuvuus on toteutettu tietoturvaprofiileilla, joka mahdollistaa standardin hyödyntämisen kaiken kokoisissa automaatiojärjestelmissä.

OPC UA:n hyödyntäminen VEneCT-projektin etäohjauksessa saattaa kuitenkin olla työlästä. Sen sijaan, että OPC-verkko reititettäisiin uudelleen ja tarvittava määrä käyttäjiä lisättäisiin verkkoon, saattaa lähiverkkojen yhdistäminen reitittimien avulla tai ohjelmallisesti olla huomattavasti resursseja säästävämpää.

6.3 MQTT

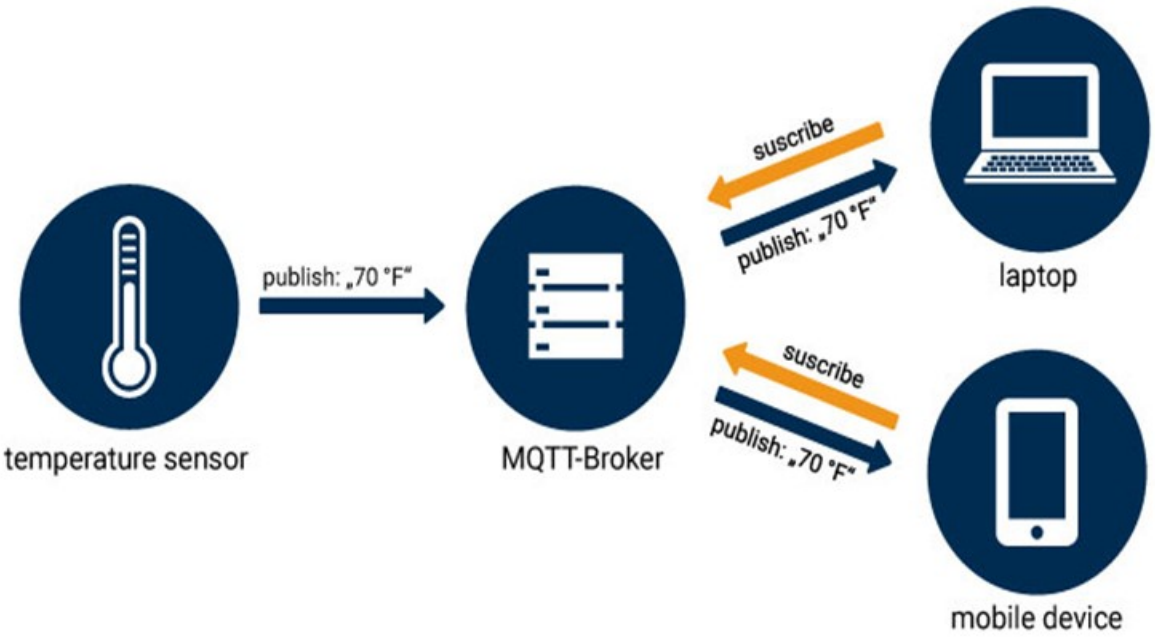
MQTT on vuonna 1999 kehitetty tiedonsiirtoprotokolla, jonka alkuperäinen käyttötarkoitus oli öljyputkien seuranta etänä satelliittiyhteyden kautta. MQTT onkin alkuperäisestä käyttötarkoituksestaan johtuen suunniteltu toimimaan hitaallakin internet-yhteydellä ja pienemmän kapasiteetin laitteilla. Tästä syystä MQTT on kevyt ja yksinkertainen tuottaja / tilaaja -protokolla (publish / subscribe). MQTT:stä on julkaistu versiot 3.1.1 ja 5. Nykyisin moni MQTT-välittäjä tukee MQTT 5:ttä, mutta IoT-pilvipalvelut edelleen lähinnä versiota 3.1.1. MQTT-verkkojen kehitystä ja visualisointia varten kehitettiin oma käyttöliittymä Node-RED. (Ojala, 2017, s. 31; HiveMQ, 2020)

6.3.1 Tiedonsiirto

MQTT-viesti sisältää kiinteämittaisen otsakkeen, jonka koko vaihtelee 2 ja 5 tavun välillä, ja tarvittaessa muuttuvamittaisen jatko-otsakkeen. Kiinteämittaisen otsakkeen pituudesta riippuen, viestin koko on 127 tavusta 256 megatavuun. Yhden mittaustuloksen lähettäminen tavallisen lähiverkon kehysrakennetta noudattaen vie 85 tavua eli 680 bittiä. IPv6-lähiverkossa tähän tarvitaan vähintään 26 tavua lisää eli yhteensä 111 tavua. Toimittaja / tilaaja -protokollan arkkitehtuuria havainnollistetaan alla kuvassa. (Ojala, 2017, s. 32)

MQTT-järjestelmä koostuu clienteista eli asiakkaista, sekä broker-laitteesta eli välittäjästä. MQTT:n kotisivuilla on ”software”-osio, josta löytyy listattuna broker- ja client-ohjelmistoja. Ohjelmistoja on saatavilla eri tekijöiltä, eri kielillä koodattuna ja eri MQTT-versioina (MQTT, n.d). Välittäjän vastuulla on lähettää MQTT-viestejä oikeille vastaanottajille. MQTT-asiakkaan lähettämästä viestistä julkaistaan otsikko, jolloin välittäjä tutkii, mitkä muut asiakkaat ovat tilanneet viestin kyseisellä otsikolla ja toimittaa sen oikeisiin osoitteisiin. Koska MQTT on alun perin suunniteltu toimimaan epävakaisellakin verkkoyhteydellä, välittäjän on mahdollista puskuroida viestejä, joita ei voida sillä hetkellä toimittaa asiakkaalle. Kuva 6 on yksinkertaistettu kaavio MQTT:n publish / subscribe -protokollan toimintaperiaatteesta. (HiveMQ, 2020)

Kuva 6. Publish / subscribe -tiedonsiirto (OPC Router, n.d)



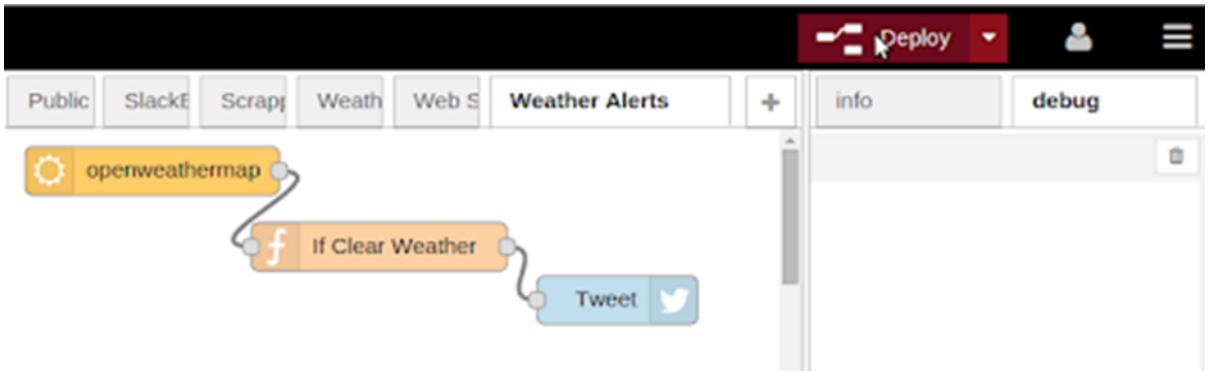
6.3.2 Node-RED

Node-RED on IBM:n ”Emerging Technology Services” -yksikön vuonna 2013 kehittämä vuokaavioihin perustuva selainpohjainen ohjelmointityökalu. Nykyisin Node-RED on osa JS Foundationia. Alun perin sivuprojektina kehitettyä ympäristöä oli tarkoitus käyttää MQTT-verkkojen visualisoimiseen ja muokkaamiseen. (Node-RED, about, n.d)

Vuokaaviopohjainen ohjelmointi on kehitetty 1970-luvulla kehittäjänään J. Paul Morrison. Vuokaavio-ohjelmoinnilla tarkoitetaan visuaalista ohjelmointiympäristöä, jossa ohjelma muodostetaan yhdistelemällä kytkentäpisteitä (Node). Kytkentäpisteitä on erilaisia eri tarkoituksiin, mutta pääperiaatteiltaan ne toimivat vastaanottamalla dataa, prosessoimalla sitä halutulla tavalla, ja lähettämällä eteenpäin. Kuva 7 on hyvin yksinkertainen ohjelmaesimerkki Node-RED:n omasta ohjelmointioppaasta. Kuvassa näkyvä ohjelma avaa ensin sääkartan ja tutkii onko sää selkeä ohjelman suoritushetkellä, ja mikäli näin on, ohjelma julkaisee tiedon Twitterissä. Tämä on tietysti varsinkin automaatiotekniikan mittakaavassa hyvin yksinkertaistettu esimerkki, mutta siitä voi tehdä oleelliset havainnot ohjelmointiympäristön toiminnasta. Kytkentäpisteitä klikkaamalla avautuu valikko, joka sisältää kyseiseen kytkentäpisteeseen liittyvät määrittelyt. Ohjelmointiperiaate on siis sama,

kuin missä tahansa ohjelmointikielessä tai -muodossa, mutta visuaalinen ohjelmointitapa mahdollistaa ohjelmoinnin ilman ohjelmointikielten tuntemusta – se siis tarjoaa mahdollisuuksia laajemmalle käyttäjäkunnalle ”tavalliseen” ohjelmointiympäristöön verrattuna. (Node-RED, about, n.d)

Kuva 7. Node-RED -esimerkki (Node-RED, programming guide, n.d)



Node-RED on hyvin yksinkertainen käyttää ja se toimii kokonaisuudessaan selaimessa. Ohjelmaa voidaan muokata Editorissa, josta voidaan yhdellä klikkauksella siirtyä käyttöliittymä-näkymään, jossa ohjelma toimii. Node-RED on hyvin monikäyttöinen ohjelmointiympäristö, koska sillä voidaan ohjelmoida ja luoda käyttöliittymiä melkeinpä mihin sovellukseen tahansa, esimerkkeinä mm. Raspberry PI, PLC:t, ja IoT-laitteet. Voidaan puhua hyvin skaalautuvasta ympäristöstä, sillä sen avulla onnistuvat niin pienet harrasteprojektit, kuin suurempienkin järjestelmien ohjelmointi. Node-RED on avoimen lähdekoodin järjestelmä, ja sillä on aktiivinen yhteisö, joka kehittää toiminnallisuuksia. ”Nodeja” eli kytkentäpisteitä on alkuperäisissä kirjastoissa jo monipuolisesti, mutta nimenomaan yhteisön kehittämiä kytkentäpisteitä on mahdollista ladata vakiokirjaston lisäksi. (Node-RED, about, n.d)

Edellisessä kappaleessa esitetty ohjelmaesimerkki ei sisällä ulkoisia prosessoreita, vaan ohjelma pyörii pelkästään tietokoneella. Kun halutaan ohjelmoida ja tehdä käyttöliittymiä ulkoiselle prosessorille, järjestelmä monimutkaistuu hieman. Kuten edellisessä kappaleessa mainitaan, ulkoisia prosessoreita voi olla vaikkapa Raspberry PI tai PLC. Ohjelmointiperiaate sinänsä on sama, mutta joudutaan avaamaan kommunikaatioväylä selaimen ja prosessorin välille. Esimerkiksi PuTTY-nimistä SSH-client -ohjelmaa voidaan käyttää yhteyden muodostamiseen. (Putty, n.d)

Node-RED:iin voidaan ottaa etäyhteys qbee.io-sovelluksen avulla. Qbee.io on IoT-sovellus, joka on kehitetty Linux-pohjaisten järjestelmien hallinnointiin, joihin Raspberry PI:kin kuuluu. Sovelluksen kerrotaan sopivan ennen kaikkea sulautettujen järjestelmien hallinnointiin, mutta verkkosivujen mukaan sitä voidaan käyttää myös muiden järjestelmien hallinnointiin. Qbee.io:n avulla voidaan ohjata myös useita järjestelmiä samaan aikaan. (qbee.io, n.d)

6.4 Etätyöpöytäohjelmat

Yrityksillä on etäkäyttöä varten käytössään myös ilman VPN:ää toimivia etätyöpöytäohjelmistoja. Tunnetuimmat ohjelmat lienevät Teamviewer ja Microsoftin Remote Desktop. Point-to-point VPN-yhteyteen verrattuna tämä ratkaisu edellyttää hiukan enemmän laitteita toimiakseen, koska ohjelmiston avulla yhdistetään laitteet keskenään ja VPN:llä taas itse verkot. (Teamviewer, n.d; Microsoft, 2018)

Järjestelmän käyttöönotto siis edellyttää, että automaatiojärjestelmän lähiverkossa on tietokone, johon voidaan ottaa yhteys. Käytännössä tällöin etäkäyttäjä voi avata etätyöpöytäohjelman tietokoneellaan, muodostaa suojatun yhteyden automaatiojärjestelmän lähiverkossa sijaitsevaan tietokoneeseen, ja tätä kautta saada pääsyn automaatiojärjestelmän ohjelmointi- ja monitorointirajapintoihin, vaikka todellisuudessa sijaitseekin lähiverkon ulkopuolella. (Teamviewer, n.d; Microsoft, 2018)

7 Kaupalliset ratkaisut

7.1 Secomea

Secomea on kansainvälinen automaatioalan yritys, joka tarjoaa nykyaikaisia ratkaisuja teollisuuteen yli 7000 asiakkaalle. Secomean verkkosivuilta käy ilmi, että maailmassa yli 300 000 tietokonetta ja PLC:tä on varustettu heidän ratkaisuillaan (Secomea, company, n.d). Yksi Secomean tarjoamista palveluista on teollisuuslaitosten etäohjaamiseen suunniteltu tuoteperhe, joka sisältää osat LinkManager, GateManager ja SiteManager. Suomessa Secomean palveluita myy Elkome (Elkome, n.d).

Secomea mainostaa tuoteperhettään erittäin turvalliseksi – jopa turvallisemmaksi etäyhteysjärjestelmäksi kuin VPN. Järjestelmä täyttääkin tiukimmatkin tietoturvastandardit, ja tarjoaa huomattavan kattavia turvallisuusominaisuuksia, joista esimerkkinä kaikkien etäyhteysistuntojen tietojen tallentaminen. Voidaan siis jälkikäteen tarkastella kuka on ollut yhteydessä mihinkin järjestelmän piirissä olevaan laitteeseen, ja milloin. On myös palvelun käyttäjän hallinnoitavissa, keille käyttäjille tai käyttäjäryhmille annetaan lupa yhdistää mihinkin järjestelmiin. (Elkome, n.d)

7.1.1 Järjestelmän rakenne

Secomea-järjestelmä koostuu kolmesta osasta, kuten edellisessä kappaleessa mainittiin. LinkManager on käyttäjän eli yleensä yrityksen työntekijän tai ulkopuolisen kunnossapidon valtuutetun henkilön tietokoneelle asennettava ohjelmisto, jonka avulla henkilö voi ottaa etäyhteyden hänelle sallittuihin järjestelmiin. Sen lisäksi, että sallittuja laitteita voidaan hallinnoida, on mahdollista määritellä myös sallitut yhteystavat. Käyttäjä tunnistetaan yksilöllisen sertifikaattitiedoston sekä salasanan avulla. (Elkome, n.d)

GateManager on hallintaportaali, jonka avulla hallinnoidaan IoT-järjestelmien tiedonkeruuta, sekä etäyhteyksien asetuksia. GateManagerin avulla siis hallinnoidaan, mitkä käyttäjät saavat LinkManagerin kautta olla yhteydessä mihinkin laitteeseen. GateManageriin tallennetaan myös lokitiedot jokaisesta etäyhteysistunnosta. GateManager on käytettävissä

pilvipalveluna, tai vaihtoehtoisesti se voidaan asentaa käyttäjän omalle tietokoneelle. (Elkome, n.d)

SiteManager on reititinlaite, joka asennetaan etäkohteeseen. Se sisältää 4G-tuen sekä tietysti kiinteän internet-yhteyden, joista kumman tahansa kautta voidaan muodostaa etäyhteys kohteeseen. SiteManageriin määritellään agentit, joiden avulla määräytyy laitteet ja yhteystavat, millä etäyhteys muodostetaan. Agentit ovat myös tietoturvan kannalta tärkeä ominaisuus, koska niiden avulla määritellään vain ne laitteet, joihin yhteys halutaan muodostaa, eikä näin ollen koko tehdasverkkoa tarvitse avata etäkäyttäjille. (Elkome, n.d)

7.1.2 Toimintaperiaate

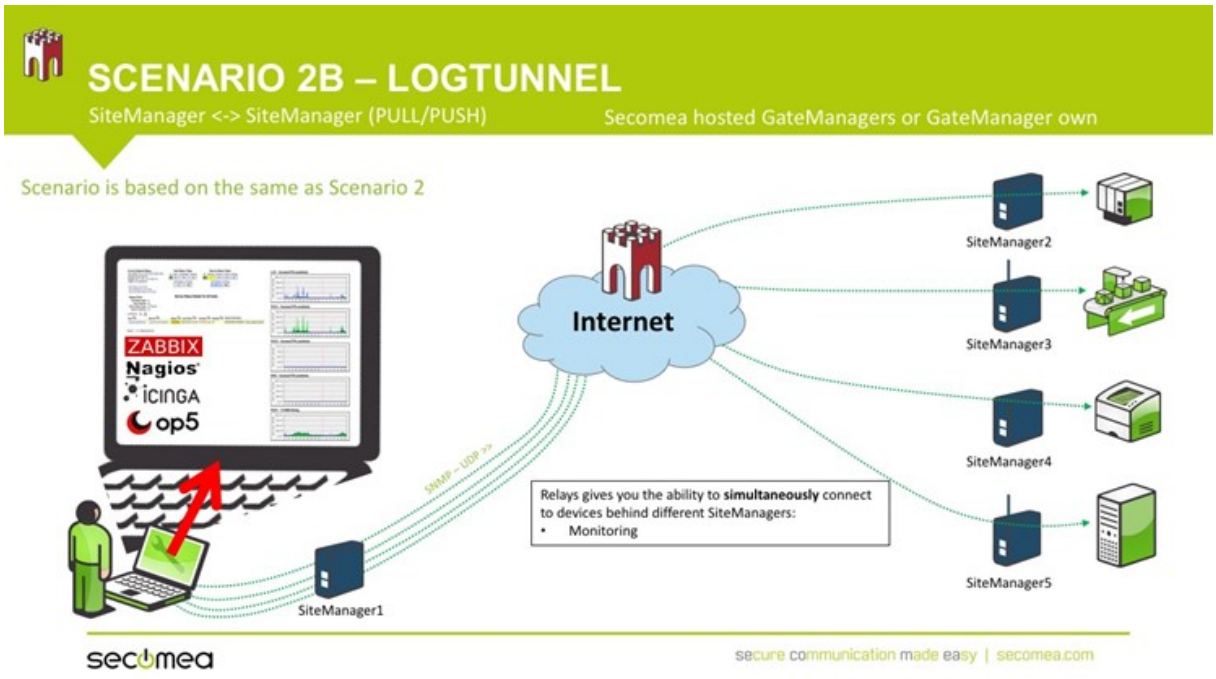
Järjestelmän toiminnan kannalta tärkein osa on Secomea SiteManager eli fyysinen reititinlaite, joita on tällä hetkellä tarjolla kahta eri sarjaa. Kumpikin mahdollistaa turvallisen etäyhteyden, mutta ne sisältävät eroavaisuuksiakin, lähinnä toimintojen laajuudessa. (Secomea, company, n.d)

SiteManager 15xx/35xx-sarjan reitittimiin voi yhdistää samanaikaisesti jopa 100 laitetta, ja yhdistämisvaihtoehtoja ovat Ethernet, USB- tai sarjaportti. Reititin myös tukee automaatiolaitteiston omia tiedonsiirtoprotokollia, kuten Modbusia, Profinetia, EtherCatia tai Ethnernet/IP:tä. Reititin sisältää moduulin, joka kerää dataa kytketyiltä laitteilta. Datan keräämiseen käytettäviä protokollia ovat Modbus, OPC UA, CIP tai S7. Datan keräämisen lisäksi moduuli lähettää tämän datan pilvipalvelimelle. Vaihtoehtoja käytettävälle pilvipalvelimelle ovat muun muassa Azure, AWS, EcoStruxure, Machine Advisor tai Secomea DCC. Reitittimessä on sisäänrakennettu flash-muisti, jotta RAM-pohjainen tietokanta säilyy myös internet-yhteyden katkosten, tai sähkökatkon aikana. Datan säilyvyyttä on mahdollista parantaa entisestään ulkoisella SD-kortilla. Reititin sisältää myös sisäänrakennettuna kolme DEV/LAN-porttia, jotka voidaan konfiguroida siltaan, tai hallita yksittäisinä portteina, joilla on erilliset DHCP-palvelimet. Reititin on yhteydessä internetiin hyödyntäen ennestään olemassa olevan verkon rakennetta, mikä tekee Secomea:sta erittäin palomuuriystävällisen ratkaisun. Secomea:n LogTunnel-ratkaisun avulla reititin muodostaa yhteyden valvomoon (SCADA). Yhteyttä voidaan kuvata staattiseksi tunneliksi. (Secomea, SiteManager 15xx/35xx, n.d)

SiteManager 11xx/33xx on hieman kevyempi ja toiminnoiltaan suppeampi versio edellisessä kappaleessa esitellystä mallista. Reitittimeen voidaan yhdistää korkeintaan 25 eri laitetta, jotka voidaan kytkeä samoilla menetelmillä kuin 15xx/35xx-mallissakin. Myös internetiin yhdistäminen sekä LogTunnel toimivat täysin samalla tavalla, kuin 15xx/35xx-sarjan reitittimissä. Eroina kattavampaan reititinmallistoon ovat muisti, kolmen DEV/LAN-portin puuttuminen, ja pieni ero datan keräysvaihtoehdoissa. Datalehtiä vertailtaessa kiinnittyy huomio siihen, että 15xx/35xx-sarjan lehdessä mainitaan datan keräämisen olevan älykästä - maininta puuttuu 11xx-33xx-sarjan datalehdestä, mutta kummassakaan lehdessä ei tätä avata tarkemmin. Erona on vain se, että 11xx-33xx-sarjan reitittimistä puuttuu Rockwell CIP-, ja Ethernet/IP-tuki. Muistin osalta tässä suppeammassa versiossa ei ole ulkoisen SD-kortin paikkaa, vaan ainoastaan 80MB sisäistä flash-muistia, joka vastaa myös 15xx-35xx-reitittimen sisäistä muistia. (Secomea, SiteManager 15xx/35xx, n.d; Secomea, SiteManager 11xx/33xx, n.d)

Opinnäytetyön aiheen kannalta mielenkiintoisin ja tärkein SiteManagerin ominaisuus on LogTunnel, jonka avulla luodaan etäyhteys valvomoon. Kuvassa alla on esitetty yksi vaihtoehto LogTunnel-ratkaisun hyödyntämisestä. Kuva 8 nähdään, kuinka SiteManager-reitittimien avulla useilla eri etäkohteilla (site) on yhteinen valvomo (SCADA). (Secomea, SiteManager 15xx/35xx, n.d; Secomea, SiteManager 11xx/33xx, n.d)

Kuva 8. Secomea, keskitetty SCADA (Secomea, n.d)



SiteManager:sta on myös saatavilla ohjelmallinen versio SiteManager Embedded. Se voidaan asentaa PC:lle, IPC:lle, tai HMI-paneeliin. SiteManager Embeddedin idea on tehdä alustastaan turvallinen ”access gateway”, joka toimii fyysisen SiteManager-reitittimen tapaan. Ohjelma tukee useita eri käyttöjärjestelmiä, ja se vaatii vain vähän resursseja alustaltaan. Ohjelmalle soveltuvia käyttöjärjestelmiä ovat muun muassa Windows 32/64 bit x86, Windows Embedded, Linux x86, Linux ARM Raspberry Pi ja VxWorks ARM. (Secomea, SiteManager Embedded, n.d)

SiteManager Embedded tukee samoja tiedonsiirtoprotokollia kuin fyysiset SiteManagerit. Siihen voidaan kytkeä kuitenkin maksimissaan vain 10 eri laitetta eli siinä suhteessa ero 15xx-35xx-sarjan reitittimeen on huomattava. SiteManager Embedded hyödyntää alustansa yhteysvaihtoehtoja, joita voivat olla muun muassa Ethernet, 4G ja WiFi. Käytettävän alustan palomuuri, sekä muut turvallisuusasetukset ohjaavat ohjelmiston toimintaa. Embedded-versio sisältää samat älykkäät datankeruumenetelmät kuin 15xx-35xx-sarjan fyysinen reititin. LogTunnel-ominaisuus on myös sisällytetty Embedded-versioon. Ohjelmisto sisältää sisäänrakennetun graafisen käyttöliittymän (GUI), sekä ohjelmointirajapinnan (API). (Secomea, SiteManager Embedded, n.d)

SiteManager-reitittimien hinnat vaihtelevat välillä $570 - $1,140.00. Ohjelmistot kustantavat noin $1000, mutta hintaan vaikuttaa mm. agenttien määrä. Mobile Access -ohjelmisto maksaa $185 eli mobiililaitteen yhdistämisen mahdollistava rajapintakin tuottaa lisäkuluja. Vaikka Secomea onkin ehkä suunniteltu silmälläpitäen suurempia tehtaita on todettava, ettei noin 2000 dollarin yhteishinta luotettavasta ja hyvin rakennetusta etäyhteysintegraatiosta ole mahdottoman korkea hinta – skaalautuvuutta tuntuu siis löytyvän myös hinnaston osalta. 10.12.2020 kurssin mukaan 2000 dollaria vastaa 1653,13 Euroa (Transferwise, 2020). (Industrialnetworking, n.d)

7.2 Qbee.io

Qbee.io on sovellus, joka muodostaa turvallisen etäyhteyden haluttuun palvelimeen. Qbee-agent -niminen sovellus asennetaan tietokoneelle, ja sen käyttäminen on yksinkertaista. Käyttäjä kirjautuu qbee-tunnuksillaan sovellukseen, jonka jälkeen hän voi käyttää sitä. Käyttäjän täytyy määritellä sovellukseen portit, joihin yhteys halutaan muodostaa. Esimerkkinä http-portti 80, https-portti 443 ja Node-RED -portti 1880. Tämän jälkeen määritellään paikallinen portti, jolloin sovellus muodostaa yhteyden edellä mainitun etäyhteys-portin ja paikallisen portin välille. Node-RED:iä voidaan käyttää selaimessa, kun yhteys on muodostettu. Node-RED:iin pääsee, kun kirjoittaa selaimen osoiteriville ”localhost:” ja paikallisen portin numero. (qbee.io, n.d)

Qbee.io muodostaa turvallisen yhteyden verkkoon, sillä sovellus ei avaa palomuurin portteja. Tämä on mahdollista, koska qbee.io:ssa on sisäänrakennettu turvallinen yhteydenmuodostusmekanismi (qbee.io, n.d). Verkkosivuilla mainitaankin, että sovellus toimii ikään kuin palomuurin ”takana”, jolloin portteja ei tarvitse avata. Palomuuriin avattu portti on huomattava turvallisuusriski, ja sitä joudutaan valvomaan jatkuvasti. Todellisuudessa qbee.io:ta voidaan käyttää huomattavasti laajemmin, mutta tässä kontekstissa olennaista on turvallisen etäyhteyden luominen, esimerkiksi juuri Node-RED:iin. qbee.io:n avulla voidaan myös muodostaa turvallinen tunneli laitteiden välille SSH- ja VPN-tekniikoilla (qbee.io, Using qbee as a relay for other devices (ssh port forwarding), n.d). Yksinkertaistettuna qbee-agentin avulla voidaan käyttää Node-RED:iä mistä päin tahansa, niin kuin oltaisiin lähiverkossa oikeasti. Qbee.io on myös hyvin kohtuullisen hintainen,

esimerkiksi kulta-tason palvelu maksaa 0,5 € / kk per laite. Tuki maksaa 179 € / kk eli ratkaisu tulisi kustantamaan noin 180 € / kk. (qbee.io, n.d)

Qbee.io ei yksinään tarjoa mahdollisuutta ohjata järjestelmää etänä, mutta se voidaan kuitenkin yhdistää soveltuvan UI- ja API-ohjelmiston kanssa, joten esimerkiksi Node-RED:n kanssa yhdessä ohjelma voisi tarjota järkevän ratkaisun. Ainakin kyseessä olisi helppo ja kustannustehokas ratkaisu. (qbee.io, n.d)

7.3 StrideLinx

StrideLinx on pilvipohjaisen VPN:n palveluntarjoaja. Toimintaperiaatteeltaan teknologia on täysin sama, kuin luvussa kuusi esiteltiin. StrideLinx:n pakettiin kuuluu käyttäjäystävällisellä käyttöliittymällä varustettu reititin, ja 5GB ilmaista dataa kuukaudessa. Käyttäjien määrää ei ole palvelussa rajoitettu. StrideLinx:n avulla on helppo yhdistää automaatiojärjestelmään mistä päin tahansa, millä laitteella vain. Lisämaksusta on saatavilla lisää kuukausikohtaista dataa. Mobiililaitteista StrideLinx tukee sekä Android-, että Apple-käyttöjärjestelmiä. (Automationdirect, StrideLinx: Industrial VPN Cloud - PLC Remote Access Solution, n.d)

StrideLinx käyttää TLS 1.2 ja ISO27001:2013 -standardeja tiedonsiirrossa taatakseen turvallisen yhteyden. Turvallisuusominaisuuksista myös kaksivaiheinen todennus on saatavilla järjestelmään. (Automationdirect, Stridelinx, 2020)

StrideLinx-reititin maksaa Automation Directin kaupassa hieman mallista riippuen 369 – 650 USD. Dataa voidaan ostaa tarpeen mukaan 5GB:stä (35 USD/kk) 50GB:n (190 USD/kk). Monitorointia varten myydään erikseen ohjelmallisia lisäominaisuuksia, joita ovat hälytykset ja ilmoitukset (210 USD) ja Cloud Logging eri resoluutioilla (15-85 USD). (Automationdirect, shop, 2020)

7.4 TOSIBOX

TOSIBOX on on patentoitu point-to-point VPN-ratkaisu, joka hyödyntää kahden reitittimen välille muodostettavaa niin sanottua perinteistä VPN-tunnelia. Toisin sanoen TOSIBOX ei sisällä pilvipalvelua, toisin kuin vaikkapa edellä mainittu Stridelinx. Palveluun kuitenkin

kuuluu ”Plug & Go”-ominaisuus, eli asennus on mahdollista tehdä ilman edistyneitä IT-taitoja. (TOSIBOX, n.d)

TOSIBOX on skaalautuva järjestelmä, johon muiden esiteltyjen järjestelmien tapaan on saatavilla ominaisuuksiltaan hieman eri tasoisia komponentteja. Kaikki komponentit ovat kuitenkin keskenään sopivia, mikäli järjestelmää halutaan laajentaa jälkeenpäin. TOSIBOX:n kotisivuilla mainitaankin, että laajennettavuus ja joustavuus on rajatonta. Key eli avain sisältää Client-ohjelman, jonka avulla päästään kirjautumaan verkkoon etänä. Tämä on mahdollista myös Mobile Client-sovelluksella, joka on vastaavaan tarkoitukseen kehitetty mobiiliapplikaatio. Key-laitteesta on saatavilla myös SoftKey-versio, joka toimii kuten Key, mutta ei sisällä fyysistä laitetta lainkaan, vaan on tietokoneelle asennettava ohjelma. (TOSIBOX, n.d)

TOSIBOX Lock on reititin, joita on saatavilla useita eri mallisia. Eri malliset reitittimet eroavat toisistaan ominaisuuksiltaan. Yhdistävä tekijä eri mallisissa reitittimissä on kuitenkin se, että käyttäjien client-sovellukset (Key, SoftKey, Mobile Client) ottavat yhteyttä Lock-reitittimiin, jolloin muodostuu turvallinen laitteidenvälinen VPN-tunneli. TOSIBOX Hub on yrityksen vastuuhenkilöille kehitetty alusta, jonka avulla voidaan helposti hallita verkkojen käyttöoikeuksia, mikä tulee ehdottomasti tarpeeseen kun puhutaan suuremmista yrityksistä. TOSIBOX MatchMaker on taustalla pyörivä palvelu, joka on koko järjestelmän tärkein osa. Palvelu etsii käyttäjille etäyhteyspisteitä eli Lock-reitittimiä, joihin heidän laitteillaan olevilla avaimilla (Key) on pääsyoikeus. Palvelun merkitys korostuu tietenkin siinä vaiheessa, jos suurella kansainvälisellä yrityksellä on vaikkapa satoja eri etäyhteyspisteitä, joihin ollaan yhteydessä eri puolilta maailmaa. (TOSIBOX, products, n.d)

Kuten sanottu, TOSIBOX on VPN:n perustuva teknologia, joka muodostaa VPN-tunnelin Key-avaimen ja Lock-reitittimen välille. VPN-tiedonsiirto salataan RSA-salauksella, sekä noudattamalla TLS-, Blowfish- ja AES-standardeja. Lisäksi käyttäjän todentaminen toteutetaan kaksivaiheisella tunnistautumisella. (TOSIBOX, 2017)

7.4.1 Saatavuus

TOSIBOX-tuotteet eroavat suurimmasta osasta teollisuusautomaatioon tarkoitetuista tuotteista siten, että niitä myydään Suomessakin elektroniikkakaupoissa. Verkkokauppa.com on yksi TOSIBOX:n jälleenmyyjistä, ja se myy tuoteperhettä laitepareina tai yksittäisinä laitteina. Referenssiksi TOSIBOX Lock 200 + Key -laitepari maksaa 859 €. Kuten sanottu, laitteet toimivat Plug & Go -periaatteen vuoksi keskenään ilman erillistä konfigurointia, ja pelkästään kyseinen laitepari tarjoaa runsaasti erilaisia käyttömahdollisuuksia. Järjestelmä nimittäin tukee kaikkia internetliittymätyyppejä, joten verkon protokollien tunteminen ei ole kriteerinä järjestelmän hankinnalle. Kyseisillä laitteilla maksimi tiedonsiirtonopeus on 15 Mbps ja järjestelmään sisältyy myös Mobile Client, joka tukee sekä Android-, että IOS-käyttöjärjestelmää. Vertailun vuoksi sanottakoon, että Lock 150 + Key -laitepari maksaa OVH-hinnaltaan 796,80 €, kun taas Lock 500-reititin yksin kustantaa 1047,90 €. Hinnan määrittäviä ominaisuuksia ovat yhtäaikaisten VPN-yhteyksien maksimimäärä, tiedonsiirtonopeus, ja sisäänrakennetut ominaisuudet. (Verkkokauppa.com, 2020)

Tämän opinnäytetyön aihetta silmällä pitäen Lock 150 + Key -laitepari voisi olla sopivin, vaikkakin avaimia tulee paketissa vain yksi kappale. Avaimet maksavat erikseen kappalehinnaltaan 239,90 €. Ohjelmallinen avain SoftKey maksaa kappalehinnaltaan 184,9 € ja viiden lisenssin paketilla on hintaa 863,9 €. Lock 150 sallii 10 samanaikaista VPN-yhteyttä, joten jos käyttöön tulee koko reitittimen kapasiteetti, laitekustannuksia tulee 3018,1 € Verkkokauppa.com:n kautta hankittuna. Hinnat ovat esitetty vain vertailupohjan vuoksi, jota voidaan hyödyntää johtopäätöksiä tehtäessä. (Verkkokauppa.com, 2020)

7.5 Teamviewer ja Remote Desktop

7.5.1 Teamviewer

Teamviewer on yksi suurimmista etätyöpöytäohjelmistojen palveluntarjoajista. Teamviewer mainostaa verkkosivuillaan nopeutta ja helppoutta verrattuna perinteiseen VPN-ratkaisuihin turvallisuudesta tinkimättä. Teamviewer käyttää 256-bittistä RSA-avainta päästä-päähän-salauksen toteuttamiseen, ja käyttäjä tunnistautuu salasanalla ennen etätyöpöytäistunnon

alkamista, joten salauksen ja tunnistautumisen osalta tietoturva on kunnossa. (Teamviewer, n.d)

Kulut Teamviewer-ohjelmiston käytöstä muodostuvat kuukausilaskutuksesta. Premium-lisenssi maksaa 57,90 € / kk ja se sisältää 15 käyttäjää, jotka voivat käyttää yhtä etäistuntoa samanaikaisesti. Halvemmat tilausvaihtoehdot ovat tähän käyttötarkoitukseen liian suppeita. Teamviewer on verrattain kallis sovellus, koska käyttöönoton yhteydessä joudutaan hankkimaan vielä etäkone, johon yhteys muodostetaan. Lisäpalveluna Teamvieweriin voi ostaa muun muassa tuen mobiililaitteille. (Teamviewer, n.d)

7.5.2 Microsoft Remote Desktop

Remote Desktop on Windows-käyttöjärjestelmien pro-versioihin sisältyvä etätyöpöytäsovellus, jonka avulla voidaan muodostaa verkkojen välinen salattu yhteys tietokoneesta toiseen. Yhteyden salaamiseksi Remote Desktop käyttää RSA:n RC4-salausta, joka on suunniteltu nimenomaan tähän käyttötarkoitukseen eli verkkojen väliseen turvalliseen yhteyteen. Ohjelma sisältää ominaisuuden, joka antaa haltijan (administrator) valita 56- tai 128-bittisen salausavaimen väliltä. Lisäksi tietoturvaa lisätään käyttäjätunnus / salasana -tunnistautumisella ennen etäyhteysistunnon aloittamista. (Microsoft, 2018)

Koska ohjelma sisältyy Windows-käyttöjärjestelmään, ja on ilmaiseksi ladattavissa myös mobiililaitteille sovelluskaupasta niin Android- kuin iOS-alustallakin, ei ohjelman käytöstä muodostu kustannuksia. Kustannuksilta ei kuitenkaan täysin voida välttyä, koska tarvitaan alusta, johon otetaan yhteys ja jolla voidaan käyttää automaatiojärjestelmän web-applikaatiota. (Microsoft, etätyöpöydän käyttäminen, n.d)

8 Johtopäätökset

8.1 Pohjustus

Sopivan etäkäyttöteknologian löytäminen VEneCT-järjestelmän hallintaan ei ollut itsestäänselvyys. Suurin osa markkinoilla olevista etäkäyttöjärjestelmistä on suunniteltu suurten yritysten tarpeisiin – ainakin järjestelmien markkinointi toimii kyseinen kulma edellä. Skaalautuvuus onkin pääprioriteetin eli turvallisuuden ohella yksi tärkeimmistä kriteereistä, koska kyseessä on pieni järjestelmä teollisuusautomaation mittakaavassa. Lisäksi markkinoilla olevat järjestelmät ovat usein ominaisuuksiltaan hyvin laajoja, ja sisältävät apuohjelmia mm. käytönvalvontaan. HAMK Techin tutkimusprojektissa tarve tällaisille apuohjelmille tuskin on erityisen suuri.

Myös itse toteutukseen on eri tulokulmia. Sama lopputulos voidaan saavuttaa joko reitittämällä OPC UA niin, että liittämällä sopiva reititin avataan uusi liityntärajapinta järjestelmään tai hyvin yksinkertaisesti hankkimalla plug & play -tyyppinen VPN-ratkaisu. Näiden ääripäiden välillä toki on lukuisia muitakin vaihtoehtoja. Valmiiden järjestelmien etuna on, että ne ovat usein laajalti käytössä olevia ratkaisuja eli niitä on testattu ja kehitetty. Niitä käytettäessä ei myöskään välttämättä tarvita verkkoteknologioiden asiantuntijuutta tai jatkuvaa valvontaa. Jos esimerkkinä käytetään luvussa seitsemän esiteltyä TOSIBOX-järjestelmää, sisältyy ratkaisuun myös käyttäjän vahva tunnistautuminen, mikä tämän kaltaisessa automaatiojärjestelmässä olisi äärimmäisen hyvä asia.

Tietoturvan kannalta tärkeimpiä ominaisuuksia ovat viestin salausominaisuudet sekä juuri käyttäjän tunnistusmenetelmät. Tietysti myös etäyhteyden muodostamiseen vaaditut toimenpiteet – jotka teknologiakohtaisesti jonkin verran eroavat – vaikuttavat tietoturvaan, kuten aikaisemmin raportissa jo viitattiinkin. Jos teknologian käyttöönotto edellyttää muutoksia palomuuriin, vaatii järjestelmän tietoturvallisuuden varmistaminen ja ylläpito huomattavasti enemmän tietotaitoa ja työtä, kuin mitä vaaditaan pilvipohjaisen, valmiin konfiguraation sisältävän järjestelmän osalta. Seuraavassa kappaleessa esitetään raportin perusteella sopivimmat etäyhteysteknologiat käytettäväksi tähän projektiin. Perusteluna näiden järjestelmien valikoitumiselle ovat käytettävyys ja turvallisuus omassa hintakategoriassaan.

8.2 Ratkaisut

8.2.1 Remote Desktop

Windows Remote Desktop on halvin ratkaisu ymmärrettävästä syystä: Ohjelma sisältyy tietokoneissa käytössä olevaan käyttöjärjestelmään, eikä vaadi kalliin reitittimen hankkimista. Ratkaisu edellyttää Windows 10 pro -käyttöjärjestelmällä varustettua host-tietokonetta, joka on jatkuvasti automaatiojärjestelmän verkossa liityntärajapintana etäyhteyttä varten. (Microsoft, 2018)

Koska host-tietokoneeseen muodostetaan yhteys lähiverkon ulkopuolelta, tarvitaan client-tietokoneeseen myös VPN-palvelu. Tässä tapauksessa kuitenkaan VPN-palvelun ei tarvitse olla site-to-site -tyyppinen kallis ja räätälöity ratkaisu, vaan riittää hyvin pelkkä ohjelmistopohjainen palvelu. Tällaisen yhteyden voi budjetoida maksamaan vuositasolla muutaman euron kuukaudessa käyttäjää kohti. Esimerkiksi Nord VPN Teams -palvelun perustaso maksaa tavallisesti noin $9 / kk per käyttäjä (NordVPN Teams, 2020). Markkinoilta löytyy myös ilmaisia VPN-palveluita, mutta niiden huonoja ominaisuuksia sivuttiin jo aiemmin tässä raportissa luvun 6 kappaleessa 1. On todennäköistä, että koululla on jo palvelusopimus jonkin VPN-palveluntarjoajan kanssa, jolloin vältyttäisiin juoksevilta kustannuksilta. (Microsoft, Allow access to your PC from outside your PC's network, 2018)

Remote desktop -ratkaisua puoltaa vahva oletus siitä, että tilaajalla on käytettävissään host-laitteeksi sopiva tietokone varastossa – onhan tilaajana ammattikorkeakoulun tutkimusyksikkö, eikä host-tietokoneella tässä tapauksessa ole erityisen korkeita järjestelmävaatimuksia. Tilaajan edustajalta ei kuitenkaan saatu vahvistusta asian varmistamiseksi. Kaikesta huolimatta ratkaisun kokonaishinta on edullinen, vaikka ylimääräinen laiteinvestointi jouduttaisiin tekemään. Juoksevia kustannuksia ratkaisulle tulisi 42 € / kk kuudelle käyttäjälle, kun hinta VPN-palveluiden hinta muutetaan Euroiksi. (Transferwise, 2020).

8.2.2 StrideLinx

Keskihintaisten tuotteiden kategoriassa StrideLinx herättää eniten luottamusta ja kiinnostusta. Pilvipohjainen VPN-järjestelmä tarvitsee reitittimen, johon otetaan client-tietokoneelta yhteys. Ratkaisu sisältää kertainvestoinnilla hankittavan reitittimen lisäksi joitakin juoksevia kuluja, jotka ovat kuitenkin maltillisia. Hyvä puoli kulurakenteessa on se, ettei laskutus ole käyttäjämäärään perustuva, vaan on porrastettu siirrettävän kuukausittaisen datamäärän mukaan. (Automationdirect, Stridelinx, 2020)

Järjestelmä on hyvin soveltuva tähän käyttötarkoitukseen, koska tarvitaan vain yksi reititin, mutta vähintään kuusi käyttäjää. Koska etäyhteys muodostetaan käyttäjän tietokoneelta ohjelmallisesti, eikä käyttäjämääriä ole rajoitettu, onnistuu uusien käyttäjien tai laitteiden lisääminen jälkeenpäin hyvin. Kaksiosaisen tunnistautumisen ansiosta riski ulkopuolisen henkilön järjestelmään tunkeutumiseen hukatun tai varastetun laitteen avulla on hyvin pieni. Tiedonsiirron salausmenetelmien, sekä jokaisessa reitittimessä olevan palomuurin ansiosta kokonaiskuva järjestelmän tietoturvallisuudesta on erittäin positiivinen. (Automationdirect, Stridelinx, 2020)

Verrattaessa edellisessä kappaleessa esiteltyyn Remote Desktop -ratkaisuun, korostuu StrideLinxin kompaktius ja yksinkertaisuus – kaikki ominaisuudet ovat integroitu yhteen järjestelmään, eikä näin ollen etäyhteyden muodostamiseen tarvitse käyttää useita palveluntarjoajia. Reitittimen edullisin hankintahinta $369 on kertainvestointina varsin kohtuullinen, joskin juoksevat kulut ovat hiukan suuremmat, kuin Remote Desktop -ratkaisussa. Siitä huolimatta, koska dataa ei tarvita suuria määriä, eikä hinta korreloi käyttäjämäärien kanssa (toisin kuin Remote Desktopiin tarvittavassa VPN:ssä) hintaero voi jäädä hyvin minimaaliseksi. VPN:n kautta siirrettävä datan määrä ei välttämättä kasva suureksi, koska sen kautta tarvitsee yhdistää ainoastaan hallitakseen automaatiojärjestelmää – monitorointi onnistuu myös lähiverkon ulkopuolelta. Jos datan määräksi riittää 5GB / kk, tulee juoksevia kustannuksia $35 / kk. Kokonaiskustannukset ratkaisulle olisivat $369 + $35 / kk. Hinnat käännettynä Euroiksi, halvimmalle reitittimelle jäisi hintaa 305 Euroa, ja kuukausittaiselle 5GB siirtorajalle noin 29 € (Transferwise, 2020). (Automationdirect, shop, 2020)

8.2.3 TOSIBOX

TOSIBOX on kallein esitettävä ratkaisuehdotus, jonka kokonaiskustannukset nousevat hieman yli toivotun rajan, mutta joka ei sisällä lainkaan juoksevia kustannuksia. Laatu- ja turvallisuusvaikutelmat kohtaavat myös hinnan kanssa hyvin, ja tässä tapauksessa hiukan kalliimmalla investoinnilla saa vastineeksi myös helppoutta ja yksinkertaisuutta. TOSIBOX ei sisällä pilveä, vaan se muodostaa suoran yhteyden avaimen ja reitittimen välille. (TOSIBOX, n.d)

Käyttötarkoitukseen sopiva ratkaisu olisi hankkia reititin + 5kpl paketti ohjelmallisia (SoftKey) avaimia, sekä yksi ylimääräinen avain. Järjestelmän saatavuus verrattuna halvempiin ratkaisuihin on ensiluokkainen – vaihtoehtona on joko tilata konsultaation kautta sopivat osat suoraan toimittajalta, tai hankkia jälleenmyyjältä, joka tässä tapauksessa on Verkkokauppa.com. Kuluttajahinnaltaan yhteensä 6 kpl SoftKey-avaimia kustantaa 1048,8 € ja lock 150 -reititin 556,90 €. Kokonaiskustannukset olisivat siis 1605,7 €. Kyseessä on kallein menetelmä, joka ylittää annetun budjetin, mutta tässä tapauksessa lisäinvestoinnilla saa turvallisuutta, huolettomuutta, sekä yksinkertaisuutta. Kuten sanottu, tässä kappaleessa mainitut hinnat ovat kuluttajahintoja ja sisältävät totta kai jälleenmyyjän katteen. Kokonaishintaa on mahdollista saada laskettua vielä, jos konsultaation yhteydessä ostaa laitteet suoraa valmistajalta. (Verkkokauppa.com, 2020)

8.3 Yhteenveto

Kaikki kolme työssä esitettyä ratkaisua ovat tietoturvaltaan hyvällä tasolla, ja eroavat teknologiansa ja hintansa puolesta. Selvityksen perusteella VPN:n suosio etähallintajärjestelmissä on erittäin suuri, mikä on helppo ymmärtää. VPN voidaan toteuttaa eri tavoilla riippuen hieman käyttötarkoituksesta, ja palveluntarjoajia on markkinoilla lukematon määrä. VPN:n tarjoama yksityisyys ja turvallisuus verkossa varmasti vaikuttaa sen suosioon.

Niin kuin raportista käy ilmi, on olemassa myös kattavampaa tietotaitoa vaativia ratkaisuja, mutta niiden käyttökohteet ovat ennemminkin suurten yritysten verkoissa, joiden rakentamiseen ja ylläpitoon on varattu huomattavia resursseja. Kyseisten järjestelmien

käyttö tulee kyseeseen myös, mikäli etäyhteyden välityksellä siirretään esimerkiksi videokuvaa tai muuta erityisen raskasta dataa.

Etähallintajärjestelmän luominen on mahdollista myös ilman VPN:ää, esimerkiksi reitittämällä OPC UA- tai MQTT-verkot uudelleen, ja tällä tavoin liittämällä etähallintaan tarkoitetut tietokoneet osaksi järjestelmän IoT-verkkoa. Kyseessä on kuitenkin ylläpidoltaan monimutkaisempi järjestelmä, joka sisältää tietoturva-aukkoja. Esimerkiksi OPC UA-verkon liittäminen suoraan internetiin vaatisi kaikista raskaimman tietoturvaprofiilin käyttöä, joka taas kuormittaisi kevyempiä käytössä olevia IoT-laitteita – kuten Raspberry PI:tä – huomattavasti. Lisäksi kahden lähiverkon yhdistäminen turvallisesti on tänä päivänä niin yksikertainen ja kohtuuhintaisesti toteutettava toimenpide, että tämän selvityksen pohjalta edellisen esimerkin kaltainen uudelleen reitittäminen ei olisi perusteltua.

Viimeisenä yhteenvetona todettakoon, että työn tekeminen onnistui hyvin. Taustakartoitusta varten löytyi hyvin paljon luotettavaa lähdemateriaalia eri julkaisujen artikkeleista, opinnäytetöistä, sekä valmistajien verkkosivuilta. Lisäksi työn aihe, eli etäohjaus on näkyvä trendi koko alalla – palveluntarjoajia eri protokollia hyödyntäville järjestelmille oli useita, joten vertailua oli helppo tehdä. Ratkaisujen hintahaarukka oli odotetun kaltainen, itseasiassa suuriin tehtaisiin tarkoitettujen järjestelmien skaalautuvuus jopa yllätti. Positiivinen yllätys oli myös se, että lähes kaikki palveluntarjoajat olivat tietoturvan suhteen hyvin läpinäkyviä. Salausalgoritmeista, käyttäjän tunnistusmenetelmistä sekä erilaisista tietoturvasertifikaateista kerrottiin hyvin näkyvästi valmistajien ja jälleenmyyjien omilla sivuilla, mikä on omiaan herättämään luottamusta. Tämä toki teki teknologioiden vertailun hieman hankalammaksi tietoturvan näkökulmasta, mutta tätä voi pitää positiivisena ongelmana. Nykypäivän markkinoilta löytyy useita tietoturvallisia automaatio- ja muiden erillisverkkojen etäohjaamiseen soveltuvia järjestelmiä.

Lähteet

Automationdirect, shop. (2020). Automationdirect. Haettu 30.11.2020 osoitteesta https://www.automationdirect.com/adc/shopping/catalog/communications/secure_remote_access_-_vpn

Automationdirect, Stridelinx. (2020). Automationdirect. Haettu osoitteesta https://www.automationdirect.com/stride/stridelinx

Automationdirect, StrideLinx: Industrial VPN Cloud - PLC Remote Access Solution. (n.d). Automationdirect. Haettu osoitteesta https://www.automationdirect.com/videos/video?videoToPlay=JX35JtToXcA

Digipooli. (2020). *Digipooli*. Haettu osoitteesta https://www.digipooli.fi/fi/ajankohtaista/oletteko-jo-keskustelleet-etatyovalineiden-tietoturvakovennuksista

Elkome. (n.d). *Secomea - Etäyhteys- ja IoT-järjestelmä*. Elkome. Haettu osoitteesta https://elkome.com/jarjestelmatuotteet/secomea-etayhteys-ja-iot-jarjestelma/

Finkle, J. (2017). Cyber firms warn of malware that could cause power outages. *Reuters*. Haettu osoitteesta: https://www.reuters.com/article/us-cyber-attack-utilities/cyber-firms-warn-of-malware-that-could-cause-power-outages-idUSKBN1931EG

Griffith, J. (2020). *International Society of Automation*. Haettu osoitteesta: https://blog.isa.org/how-to-implement-secure-remote-access-industrial-automation-system

Heikkilä, M. (2016). *OPC UA Automaation tiedonsiirrossa.* Tampere: Tampereen ammattikorkeakoulu. Haettu osoitteesta: https://www.theseus.fi/bitstream/handle/10024/114376/Heikkila_Mikko.pdf?sequence=1&isAllowed=y

HiveMQ. (2020). *Getting Started with MQTT*. HiveMQ. Haettu osoitteesta https://www.hivemq.com/blog/how-to-get-started-with-mqtt/

Industrialnetworking. (n.d). *Secomea*. Industrialnetworking. Haettu 13.10.2020 osoitteesta https://www.industrialnetworking.com/Secomea

Kyberturvallisuuskeskus. (2020). *Traficom*. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Marks, T. (2020). *VPNoverview*. Haettu osoitteesta https://vpnoverview.com/vpn-information/what-is-a-vpn/

Microsoft. (2018). *Documentation*. Microsoft. Haettu osoitteesta Remote Desktop Protocol: https://docs.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol

Microsoft, Allow access to your PC from outside your PC's network. (2018). Microsoft. Haettu osoitteesta https://docs.microsoft.com/fi-fi/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-outside-access

Microsoft, etäytyöpöydän käyttäminen. (n.d). Microsoft. Haettu osoitteesta https://support.microsoft.com/fi-fi/windows/et%C3%A4ty%C3%B6p%C3%B6yd%C3%A4n-k%C3%A4ytt%C3%A4minen-5fe128d5-8fb1-7a23-3b8a-41e636865e8c

MQTT. (n.d). *Software*. MQTT. Haettu osoitteesta https://mqtt.org/software/

Niemi, V. (2017). Hakkerit ottivat hallintaansa voimalaitoksen turvajärjestelmän – Hyökkäys ensimmäinen laatuaan. *Tekniikan maailma*. Haettu osoitteesta: https://tekniikanmaailma.fi/hakkerit-ottivat-hallintaansa-voimalaitoksen-turvajarjestelman-hyokkays-ensimmainen-laatuaan/

Node-RED, about. (n.d). Node-RED. Haettu osoitteesta https://nodered.org/about/

Node-RED, programming guide. (n.d). Node-RED. Haettu osoitteesta http://noderedguide.com/

NordVPN Teams. (2020). *Pricing*. NordVPN. Haettu 30.11.2020 osoitteesta https://nordvpnteams.com/pricing/

Ojala, R. (2017). *MQTT IoT-protokolla.* Jyväskylä: Jyväskylän ammattikorkeakoulu. Haettu osoitteesta: https://www.theseus.fi/bitstream/handle/10024/139798/Ojala_Rami.pdf?sequence=3

OPC Foundation, Classic. (n.d). OPC Foundation. Haettu osoitteesta https://opcfoundation.org/about/opc-technologies/opc-classic/

OPC Foundation, Unified Architecture. (n.d). OPC Foundation. Haettu osoitteesta https://opcfoundation.org/about/opc-technologies/opc-ua/

OPC Foundation, What is OPC? (n.d). OPC Foundation. Haettu osoitteesta https://opcfoundation.org/about/what-is-opc/

OPC Router. (n.d). *What is MQTT?* OPC Router. Haettu osoitteesta https://www.opc-router.com/what-is-mqtt/

Perimeter 81. (2020). *Perimeter 81*. Haettu osoitteesta https://www.perimeter81.com/resources/hosted-vpn-service

Putty. (n.d). *PuTTY.org*. Haettu osoitteesta https://www.putty.org/

qbee.io. (n.d). *Deploy and configure Node-RED*. Qbee.io. Haettu osoitteesta https://qbee.io/docs/qbee-node-red-deployment.html

qbee.io. (n.d). *Manage embedded Linux Devices*. Qbee.io Haettu osoitteesta https://qbee.io/#

qbee.io. (n.d). *Secure remote web server access (Node-RED)*. Qbee.io. Haettu osoitteesta https://qbee.io/docs/qbee-secure-web-server-access.html

qbee.io, Using qbee as a relay for other devices (ssh port forwarding). (n.d). Qbee.io. Haettu osoitteesta https://qbee.io/docs/using-qbee-as-a-relay-for-other-devices.html

Rouse, M. (2020). *TechTarget - industrial internet of things (IIoT)*. TechTarget.Haettu osoitteesta https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

Secomea. (n.d). *LogTunnel - Pull/Push Scenario 2B.* Secomea. Haettu osoitteesta https://kb.secomea.com/helpdesk/KB/View/24855533-logtunnel--pullpush-scenario-b

Secomea, company. (n.d). Secomea. Haettu osoitteesta https://www.secomea.com/company/

Secomea, SiteManager 11xx/33xx. (n.d). Secomea. Haettu osoitteesta https://www.secomea.com/wp-content/uploads/2020/08/SiteManager_11xx-33xx_180320_ENG.pdf

Secomea, SiteManager 15xx/35xx. (n.d). Secomea. Haettu osoitteesta https://www.secomea.com/wp-content/uploads/2020/08/Datasheet-SiteManager-15xx-35xx-ENG-1.pdf

Secomea, SiteManager Embedded. (n.d). Secomea. Haettu osoitteesta https://www.secomea.com/wp-content/uploads/2020/09/SiteManager_Embedded_2020.pdf

Suomen Standardisoimisliitto. (2016). *SFS*. Haettu osoitteesta https://www.sfs.fi/ajankohtaista/artikkelit/tietoturvallisuus_on_luottamusta?gclid=CjwKCAjwn9v7BRBqEiwAbq1Ey_VvwjcVdaUBSJZFaTg-wbffqenkDNKe3cr1AutiQHJNokGpfiBtlBoC4PgQAvD_BwE

Tahvanainen, H.;& Aro, J. (2015). OPC UA Enables Secure Data Transfer and System Integrations in Private and Public Networks. *Automaatioseura.* Haettu osoitteesta https://www.automaatioseura.fi/site/assets/files/1550/f2068.pdf

Teamviewer. (n.d). *ratkaisut*. Haettu 7.12.2020 osoitteesta: https://www.teamviewer.com/fi/ratkaisut/etakaytto/

TOSIBOX. (2017). *Youtube.* Haettu osoitteesta https://www.youtube.com/watch?v=G3yIU0hqqNw

TOSIBOX. (n.d). *tosibox/remote-access*. Haettu osoitteesta https://www.tosibox.com/remote-access/

TOSIBOX, products. (n.d). Haettu osoitteesta https://www.tosibox.com/products/

Tran, Q. B. (2019). *End-to-end IIoT Automation System Solution.* Valkeakoski: Hämeen ammattikorkeakoulu. Haettu osoitteesta: https://www.theseus.fi/bitstream/handle/10024/261678/Quoc-Bao%20Tran%20-%20Bachelor%27s%20thesis.pdf?sequence=2&isAllowed=y

Transferwise. (2020). Transferwise. Haettu 11.12.2020 osoitteesta https://transferwise.com/gb/currency-converter/usd-to-eur-rate

Truong, D. (ei pvm). VEneCT. Hämeen ammattikorkeakoulu, Valkeakoski.

Tyson , J.;Pollette, J.;& Crawford, S. (2019). *Howstuffwork.* Haettu osoitteesta https://computer.howstuffworks.com/vpn.htm

Verkkokauppa.com. (2020). *Verkkokauppa.com*. Haettu 25.11.2020 osoitteesta https://www.verkkokauppa.com/fi/product/25856/hxftr/Tosibox-Lukko-200-Avain-etayhteyslaite?gclid=Cj0KCQiA7qP9BRCLARIsABDaZziYJt64P8YTmqhI-rh0vLCZ593ayIv7mKiXREuQOCliKOhBDlpMEtEaAtMlEALw_wcB

Viestintävirasto. (2014). *Viestintävirasto.* Haettu osoitteesta Kyberturvallisuuskeskus: https://legacy.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Vpnyhteys. (2020). *vpnyhteys*. Haettu osoitteesta https://www.vpnyhteys.fi/