Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Mikko Patronen

Automaation etäyhteydet

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikan tutkinto-ohjelma

Insinöörityö

25.5.2021

Tekijä Otsikko Sivumäärä Aika	Mikko Patronen Automaation etäyhteydet 23 sivua 25.5.2021
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	sähkö- ja automaatiotekniikan insinööri
Ammatillinen pääaine	automaatiotekniikka
Ohjaajat	lehtori Timo Kasurinen

Tämän opinnäytetyön tavoitteena on esitellä erilaisia tapoja muodostaa yhteys automaatiojärjestelmään etäältä.

Hyödynsin työn tekemisessä aiemmissa opinnoissani ja työkokemuksen myötä karttunutta asiantuntemusta. Osa ratkaisuista on kaupallisia, osa vapaan lähdekoodin ratkaisuja. Osa ratkaisuista vaatii toimiakseen työaseman yhteyden molempiin päihin, osa toteutetaan verkon aktiivilaitteilla, viimeisenä esiteltävä ratkaisu perustuu Microsoftin Azure -pilvipalveluun.

Työn loppupuolella on esitelty kaksi erilaista esimerkkiä, joista ensimmäinen on toteutettu Raspberry Pin ja Linux-työaseman yhdistelmällä. Toinen on tehty Raspberry Pin ja Microsoft Azuren yhdistelmällä.

Tutkielmassa ei oteta kantaa eri ratkaisuiden paremmuudesta, vaan jokaisella toteutuksella on oma paikkansa kulloisenkin tarpeen ja resurssien mukaan.

Automaation etäyhteydet ovat kuitenkin nykypäivänä helpohkosti järjestettävissä, lähes joka tapaukseen löytyy kustannustehokas ja toimiva ratkaisu.

Avainsanat	automaatio, etäyhteys

Author	Mikko Patronen
Title	Remote Connections of Automation Systems
Number of Pages	23
Date	May 25, 2021
Degree	Bachelor of Engineering
Degree Programme	Electrical and automation engineer
Professional Major	Automation engineering
Instructors	Timo Kasurinen, Senior Lecturer

The aim of this thesis is to introduce a variety of ways to connect to the automation systems remotely.
Expertise gained in my previous studies and work experience were utilized in the work. Some presented solutions are commercial, some open source projects. Some of the solutions require a workstation on both ends of a connection, some require active networking devices, and the last presented solution is implemented on Microsoft's Azure cloud service.

At the end of the work, there are two different demos presented. The first was implemented with a Raspberry PI and a Linux workstation. The second was implemented with Raspberry PI and Microsoft Azure combination.

Thesis does not consider the superiority of different solutions; each implementation has its place depending on the respective needs and resources.

The result of this thesis work is information on ways to connect to the automation systems remotely. As a conclusion, the work shows that remote connections to the automation systems are quite easy to set up, and a cost-effective and efficient solution can be found in almost every case.

Keywords	automation, remote connection

Sisällys

Lyhenteet

PLC	Programmable logic controller. -relational mapping. Ohjelmoitava logiikka.
PC	Personal computer. Henkilökohtainen tietokone.
VNC	Virtual Network Computing. Protokolla tietokoneen graafisen käyttöliittymän etäkäyttöön.
VPN	Virtual Private Network. Virtuaalinen erillisverkko.
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla.
OPC-UA	Open Platform Communication Unified Architecture. Koneiden välinen tiedonsiirtoprotokolla.
M2M	Machine to machine. Tiedonsiirtoa koneelta koneelle.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla tietokoneiden väliseen luotettavaan tiedonsiirtoon.
SOAP	Simple Object Access Protocol. Sovellusohjelmien välinen viestipohjainen tietoliikenneprotokolla.
HTTP	Hypertext Transfer Protocol. Sovellustason tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure. Sovellustason salattu tiedonsiirtoprotokolla.
HMI	Human machine interface. Käyttöliittymä laitteeseen.
IoT	Internet of Things. Esineiden internet.

1 Johdanto

Toisinaan on tarvetta ottaa automaatiojärjestelmään etäyhteys datan lukemiseksi tai asetusten muuttamista varten. Etäyhteys voidaan toteuttaa lukuisilla tavoilla riippuen tarpeesta, käytetystä automaatiojärjestelmästä ja käytössä olevista resursseista.

Etäkohteella tarkoitetaan tässä dokumentissa paikkaa, jossa automaatiojärjestelmä sijaitsee. Etäkohde saattaa olla esimerkiksi tehdaskiinteistö, josta on verkkoyhteydet ulkomaailmaan ja sisäinen lähiverkko tai vaikkapa jokin anturi, jolle on järjestetty jonkinlainen yhteys internetiin.

Paikalliskohteella tarkoitetaan paikkaa, jossa käyttäjä on ja ottaa yhteyden etäkohteeseen ja tarkastelee automaatiojärjestelmää tai tekee sen toimintaan tarvitsemiaan muutoksia.

Tässä opinnäytetyössäni esittelen erilaisia tapoja muodostaa yhteys automaatiojärjestelmään etäältä. Osa ratkaisuista on kaupallisia, osa vapaan lähdekoodin ratkaisuja. Osa ratkaisuista vaatii toimiakseen työaseman yhteyden molempiin päihin, osa toteutetaan verkon aktiivilaitteilla ja viimeisenä esiteltävä ratkaisu perustuu Microsoftin Azure -pilvipalveluun.

Työn loppupuolella on esitelty kaksi erilaista esimerkkiä, joista ensimmäinen on toteutettu Raspberry Pin ja Linux-työaseman yhdistelmällä. Toinen on tehty Raspberry Pin ja Microsoft Azuren -yhdistelmällä.

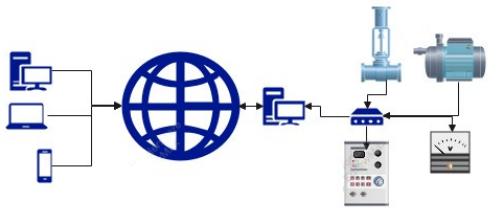
Tutkielmassa ei oteta kantaa eri ratkaisuiden paremmuudesta. Jokaisella toteutuksella on oma paikkansa kulloisenkin tarpeen ja resurssien mukaan. Työssä ei esitellä tietoliikenteen reititystä tai konfigurointia erityisen tarkasti ja tietoliikenteen salausta käsitellään yleisellä tasolla.

Työllä ei ollut toimeksiantajaa, eikä sitä tehty erikseen millekään tietylle kohderyhmälle tai projektille.

2 Yleinen kuvaus etäyhteyksistä

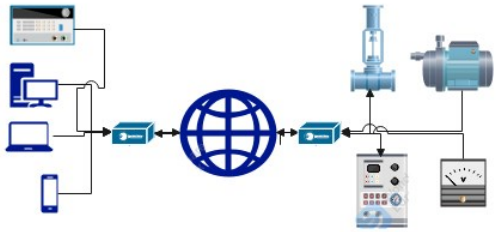
Etäyhteys voidaan muodostaa kolmella erilaisella tavalla, joilla kullakin on useita toteutustapoja, tietoteknisiä ratkaisuja, sovelluksia ja laitevalmistajia. Automaatiojärjestelmää ohjaava PLC voi ratkaisusta riippuen olla paikallis- tai etäkohteessa.

Luvussa kolme esitellään etätyöpöytäyhteyksiä, joissa työasemalla tai päätelaitteella otetaan kuvan 1 mukaisesti yhteys etäkohteessa olevaan työasemaan. PLC on tällaisessa tapauksessa etäkohteessa.



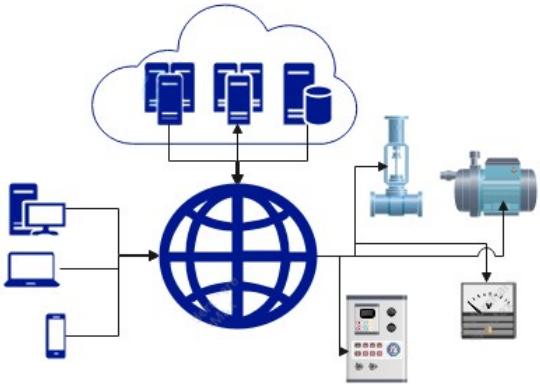
Kuva 1. Etätyöpöytäyhteys

Luvussa neljä esitellään virtuaalisia erillisverkkoyhteyksiä (VPN), joissa luodaan verkon aktiivilaitteilla tai VPN-ohjelmistolla kuvan 2 mukainen erillinen, salattu verkko, jolloin PLC voi olla etä- tai pakalliskohteessa.



Kuva 2. Virtuaalinen erillisverkkoyhteys (VPN)

Luvussa kuusi esitellään pilvipalvelun kautta toteutettua etäyhteyttä automaatiojärjestelmään kuvan 3 mukaisella konfiguraatiolla. PLC on tällaisissa tapauksissa joko etäkohteessa, tai pilvipalvelu voi toimia PLC:nä.



Kuva 3. Pilvipalvelun kautta toteutettu etäyhteys

3 Etätyöpöytäyhteydet

Etätyöpöytäyhteydellä tarkoitetaan yhteyttä, jolla saadaan samanlainen näkymä etäyhteyden takana olevan työaseman työpöydälle kuin istuisi kohteena olevan koneen ääressä. Useimmat käyttöjärjestelmät tarjoavat kuvatun yhteyden jo vakiona, jolloin mitään ylimääräisiä ohjelmistoja ei tarvitse asentaa. Vaihtoehtoisesti voidaan käyttää kaupallisia tai avoimen lähdekoodin ohjelmistoja. Kaupallisista ohjelmistoista tulee mahdollisesti kustannuksia, ja data saattaa kulkea ohjelmiston tarjoajan kautta.

Etätyöpöytäyhteys on kätevä automaatiolaitteiston hallintaan silloin, kun etäyhteyden takana on PC, jonka kautta automaatiojärjestelmää käytetään.

3.1 Microsoft Remote Desktop Connection

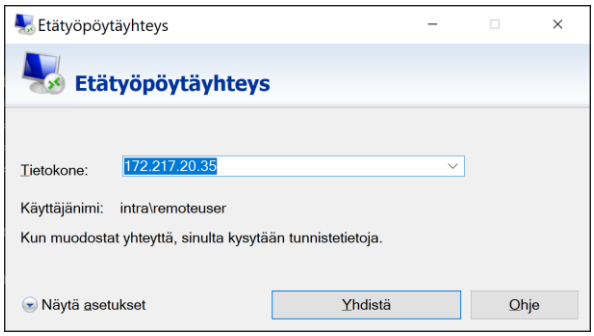
Microsoft Windows -käyttöjärjestelmän mukana tulee Microsoft Remote Desktop Connection -niminen ohjelma, jolla voidaan ottaa etätyöpöytäyhteys toisaalla sijaitsevalle työasemalle ja käyttää sitä kuten istuisi ko. koneen äärellä. Koska kyseinen ohjelma tulee käyttöjärjestelmän mukana, niin sen hankkimisesta ei aiheudu ylimääräisiä kustannuksia.

Yhteys muodostetaan seuraavasti:

1. Kohdepään palomuurista avataan jokin sopiva portti ja uudelleenohjataan sen liikenne lähiverkossa halutulle työasemalle.

2. Työaseman palomuurista avataan portti ja sallitaan Remote Desktop-ohjelman käyttö ja mahdollisesti luodaan etäkäyttäjälle käyttäjätunnus tai sallitaan nykyisen käyttäjän etätyöpöydän käyttö.

3. Etätyöasemalta käynnistetään Remote Desktop-ohjelma ja otetaan yhteys kohteen julkiseen IP-osoitteeseen ja annetaan kysyttäessä kirjautumistiedot.



Kuva 4. Windows-käyttöjärjestelmän suomenkielisen version etätyöpöytäyhteys ohjelman kirjautumisikkuna.

Microsoft Remote Desktop Connection käyttää tietoliikenteen salaamiseen Secure Sockets Layeria (SSL), ja yhteys on mahdollista konfiguroida suhteellisen turvalliseksi, mutta varsinkin oletusportti (3388) on usein tunkeutujien kohteena. Se on ainakin syytä vaihtaa johonkin, jota ei voi arvata.

3.2 TeamViewer

TeamViewer on saksalaisen TeamViewer Germany GmbH:n kehittämä ja myymä kaupallinen etätyöpöytäohjelmisto. TeamViewer Corporate -lisenssi maksaa (vuonna 2021) 1500 €/vuosi.

TeamViewer on perustoiminnaltaan vastaava kuin Remote Desktop eli etätyöpöytäohjelmisto, mutta siinä on joitakin eroavaisuuksia, kuten esimerkiksi se, että etätyöpöytä on etäkohteessa näkyvillä, eli siellä nähdään, mitä etäkäyttäjä tekee ja sessioon voi osallistua etäkohteen näppäimistöllä ja hiirellä. Tämä saattaa olla tietoturvariski, mutta ko. toiminnon voi kuitenkin estää. Toinen eroava ominaisuus on se, että TeamViewerillä voi siirtää tiedostoja etäkohteeseen.

TeamViewerin käyttöönotto on helppoa; etäyhteyden molempiin päihin asennetaan ja käynnistetään TeamViewer-ohjelmisto. Ohjelmisto tarjoaa käyttäjätunnuksia ja salasanoja, tai ne voi luoda itse. Näiden avulla yhteys voidaan muodostaa ilman palomuurin tai reitittimen porttien säätämistä. TeamViewer käyttää oletuksen porttia 5938, mutta mikäli edellä mainittu portti ei ole saatavilla, niin liikennettä saatetaan ohjata porteista 80 (HTTP) ja 443 (SSL). Ohjelmistot käyttävät TeamViewer.com-domainia yhteyteen. TeamViewer sanoo kryptaavansa liikenteen niin, etteivät edes he näe sisältöä, mutta tästä on ajoittain ollut havaintoja, että liikenne ei ole täysin salattua (1). TeamViewer on erittäin suosittu ohjelmisto ja antaa paljon oikeuksia etäkäyttäjälle ja on siten mielenkiintoinen kohde verkkorikollisille. Vuosien saatossa onkin löydetty joitakin haittaohjelmistoja, jotka hyökkäävät TeamVieweriä vastaan, kuten esim. vuonna 2013 löydetty TeamSpy(2).

Automaation tarpeisiin on tarjolla TeamViewer IoT -niminen tuote, jolla valmistajan mukaan voidaan tehdä mm. seuraavia asioita:

- ennakoiva kunnossapito
- PLC:n täysi etäyhteys
- MaaS (Machine-as-a-Service) eli laitteen tarjoaminen asiakkaalle palveluna
- DigitalTwin eli fyysisen laitteen digitaalinen kopio jolla voi tehdä testauksia ja simulaatioita
- Retrofit jolla vanhempia laitteita voidaan käyttää Industry 4.0 -ympäristössä.

3.3 VNC

Alun perin Olivetti & Oracle Research Lab:n kehittämä VNC on etätyöpöytä systeemi, johon on saatavilla eri valmistajien kaupallisia ja vapaan lähdekoodin ilmaisia ohjelmistoja.

VNC-konfiguraatiossa etäpäähän asennetaan VNC-palvelinohjelmisto, johon otetaan etätyöpöytäyhteys VNC-client-ohjelmistolla. Yhteen VNC-palvelimeen voi ottaa useita samanaikaisia yhteyksiä samaan aikaan. Yhteyden muodostamisen jälkeen etäyhteyden käyttö on samankaltaista kuin aiemmin esitellyissä Remote Desktop- ja TeamViewer-ratkaisuissa.

Tunnettuja VNC-ohjelmistojen tarjoajia ovat mm. englantilainen RealVNC, joka ohjelmisto on edullinen (3) yrityskäytössäkin ja tarjoaa sovelluksensa erittäin laajalle valikoimalle käyttöjärjestelmiä. Ilmaisia ohjelmistoja tarjoaa mm. TightVNC ja UltraVNC.

4 Virtuaaliset erillisverkkoyhteydet eli VPN-yhteydet

VPN (Virtual Private Network) eli virtuaalinen yksityinen verkko on tapa, jolla kaksi tai useampi verkkoa voidaan yhdistää julkisen verkon yli muodostaen yksityisen verkon. Nykyisin VPN-määritelmä on laajennettu koskemaan myös yksittäisten työasemien tai mobiililaitteiden liittämistä yrityksen verkkoon.

Yleisin tapa luoda VPN-yhteys on sellainen, jossa toisessa päässä on VPN-palvelin, johon VPN-client ottaa yhteyden. VPN-palvelimena voi toimia verkon aktiivilaite esim. reititin tai palomuuri tai erillinen VPN-laite. VPN-server-ohjelmiston voi myös ottaa käyttöön tietokoneessa. VPN-clientinä toimii työasema tai mobiililaite.

VPN-yhteyttä käytettäessä tietoliikenne salataan eli kryptataan, jotta vain halutut osapuolet voivat lukea niitä. Salaus ei estä viestin sieppaamista, vaan sen lukemisen. Salausjärjestelmä muuttaa viestin tai tiedon tekstin ”sekamelskaksi” salausalgoritmia käyttäen. Oikean sisällön voi tämän jälkeen lukea vain, jos salatekstin salaus puretaan.

4.1 Salausprotokollat

VPN-yhteyden salaukseen voidaan käyttää melkein mitä tahansa tunnelointiprotokollaa, joista julkisesti standardoidut vaihtoehdot ovat:

- IPsec-protokollaa voi käyttää niin lähiverkkojen yhdistämiseen kuin etäyhteyksien muodostamiseen.
- L2TP-tunnelointiprotokollaa voi käyttää ainoastaan etäyhteyksien muodostamiseen. L2TP:ssä ole omaa salausta, vaan sen kanssa käytetään IPsec:a liikenteen salaukseen.
- L2F-tunnelointiprotokollaa voi käyttää vain lähiverkkojen yhdistämiseen. L2F käyttää PPP:n Point-to-point Encryption Protocol (ECP) -protokollaa salaukseen.
- PPTP-etäkäyttöprotokolla voi käyttää Microsoft Point-to-Point Encryption (MPPE) -protokollaa salaukseen.

Automaatiojärjestelmien käyttöön edellisiä paremmin saattaa sopia edellisistä jonkin verran poikkeava ratkaisu Virtual Private Network VPN, jossa mahdollistetaan pääsy yrityksen tietojärjestelmiin salatun liikenteen kautta, mutta varsinaista pakettiliikennettä ei päästetä yrityksen verkkoihin, jolloin esimerkiksi automaatiojärjestelmän käyttö onnistuu, mutta yhteyden ollessa päällä ei ole pääsyä julkiseen internetiin.

4.2 VPN-yhteys

VPN-yhteys muodostetaan joko päätelaiteessa, tai se on automaattisesti päällä, mikäli kyseessä on ns. site-to-site-yhteys (esim. verkon aktiivilaitteiden kiinteästi muodostama yhteys). Kun VPN-yhteys on muodostettu, niin työasema tai päätelaite on samassa verkossa kuin etäkohde, vaikka fyysisesti onkin toisaalla, jolloin automaatiojärjestelmän käyttö on yhtä vaivatonta kuin työaseman ollessa etäkohteessa.

4.3 VPN-yhteyden edut ja haitat

Oikein konfiguroitu VPN-yhteys on erittäin turvallinen. Haittoja ei juurikaan ole, ellei kyseessä ole SSL VPN -tyyppinen toteutus, jolloin yhteyden ollessa päällä ei työasemalta pääse lainkaan internetiin, jolloin esim. sähköposti ei toimi. VPN-yhteyden salaus hidastaa jonkin verran tietoliikennettä, ja mahdollinen etäverkon hitaus saattaa tehdä käytön

mahdottomaksi esimerkiksi tilanteessa, jossa toimilaite on käynnistettävä juuri oikeaan aikaan.

VPN-yhteys ei välttämättä aiheuta mitään kustannuksia, sillä kaikissa käyttöjärjestelmissä on valmiita ratkaisuja sen toteuttamiseen. Kustannuksia saattaa tulla, mikäli käytetään verkkolaitevalmistajien tiettyjä ratkaisuja, jotka vaativat etäkäyttäjiltä maksullisia lisenssejä. Toisaalta tarjolla on ilmaisia ratkaisuja järeämpiinkin tarpeisiin, kuten esimerkiksi OpenVPN, jolla voi pystyttää oma VPN-palvelimen.

5 OPC-UA-tiedonsiirtostandardi

OPC Unified Architecture (OPC UA) on seuraavan sukupolven tiedonsiirtostandardi koneiden väliseen (M2M) ja anturista pilveen tiedonsiirtoon. Open Platform Communication Unified Architecture (OPC UA) on alustasta riippumaton, laajennettavissa ja turvallinen. OPC UA tarjoaa yhteensopivuuden useiden toimittajien laitteiden kanssa, on täysin skaalautuva ja joustavuutensa ansiosta laajasti käytössä useilla toimialoilla.

OPC UA -standardia ohjaa voittoa tavoittelematon organisaatio OPC Foundation, jonka tavoitteena on helpottaa monen toimittajan, monen alustan, turvallista ja luotettavaa yhteensopivuutta.

5.1 OPC UA -tietomalli

Industry 4.0 -sovellukset edellyttävät monimutkaisten ja monikerroksisten rakenteiden mallintamista (tarvitaan tiedon, ei pelkästään datan esittämistä), mikä on mahdollista OPC UA:n ja sen tietomallinnuskehyksen olio-ominaisuuksilla. OPC UA määrittelee useita yleisiä tietomalleja, joita voidaan soveltaa monilla teollisuudenaloilla. Skenaarioissa, joissa yleiset mallit eivät ole riittäviä, voidaan luoda asiakas- ja toimialakohtaisia tietomalleja.

OPC UA:n tietomallin vakiomekanismit ovat:

- Selataan malliesimerkkejä ja niiden viitteitä.
- Lue / kirjoita nykyisiä ja historiallisia tietoja.
- Ilmoita tietojen muutoksista ja tapahtumista.
- Suorita menetelmät.

5.2 OPC UA Client Server

OPC UA -palvelin vastaanottaa pyyntöjä OPC UA -asiakkaalta, käsittelee nämä pyynnöt ja lähettää vastauksen tuloksineen takaisin asiakkaalle. On huomattava, että Client - Server -tiedonsiirto on resursseja kuluttava ja sopii parhaiten yksittäisiin määrityksiin, diagnostiikkaan tai matalien taajuuksien käyttötarkoituksiin.

5.3 OPC UA -tiedonsiirto

OPC UA tukee kahta tiedonsiirtosiirtoprotokollaa, joista toinen on TCP:n binääriprotokolla ja toinen Web Service (SOAP) -protokolla. Binaariprotokolla tarjoaa parhaan suorituskyvyn ja vaatii vähiten resursseja, joka on tärkeää sulatetuille laitteille. Web Service (SOAP) -protokollaa tuetaan parhaiten Java- tai .NET-ympäristöissä, ja sitä on helppo käsitellä palomuureissa ja reitittimissä käyttämällä tavallisia HTTP- tai HTTPS-portteja.

5.4 OPC UA Tietoturva

OPC UA:ssa on sisäänrakennettu tietoturva, ja se tukee istunnon salausta eri salaustasoilla, viestien allekirjoittamista viestien alkuperän ja eheyden varmistamiseksi sekä pakettien sekvensointia, jolla suojataan viestejä toistohyökkäyksiltä. OPC UA tukee myös todennusta UA-clientilla ja palvelimella (sovellus- / järjestelmätasolla). Lisäksi kaikki käyttäjän, sovelluksen ja järjestelmän toiminnot voidaan kirjata tarkastusvaatimuksia varten.

5.5 OPC UA -palvelin Raspberry Pi -minitietokoneessa

Seuraavana toteutetaan esimerkki, jossa luodaan OPC UA -palvelin ja otetaan siihen yhteys OPC UA -clientillä. Tässä esimerkissä käytetään Raspberry Pi -minitietokonetta OPC UA -palvelimena teollisen PLC:n sijaan. Raspberry Pi on yhden piirilevyn minitietokone, jonka on kehittänyt Raspberry PI Foundation yhdessä Broadcomin kanssa. Raspberry Pi -projektin tarkoitus oli alun perin edistää tietotekniikan opetusta kouluissa ja kehitysmaissa. Raspberry Pi -tietokone ei sisällä valmista käyttöjärjestelmää tai tallennusmuistia. Siihen on tarjolla useita Linux-pohjaisia käyttöjärjestelmäversioita. Tallennusmuistina käytetään microSD-muistikorttia.

Erillisessä Linux-tietokoneessa käytetään OPC UA client -ohjelmistoa HMI:nä teollisen käyttöliittymän sijasta. Sitä käytetään yhteyden muodostamiseen OPC UA -palvelimeen ja sen tietomallin selaamiseen. Tässä esimerkissä Linux-tietokone liitetään Raspberry Pi -laitteeseen Ethernet-yhteyden kautta, mutta vastaavan yhteyden voi luoda aiemmin selitetyillä tavoilla esimerkiksi VPN-yhteyden kautta. Tässä esimerkissä käytettiin asiakasohjelmistona ilmaista FreeOPCUA Client -ohjelmistoa, mutta mitä tahansa OPC UA -standardinmukaista ohjelmaa olisi voinut käyttää ihan yhtä hyvin.

5.5.1 Valmistellaan laitteet

- Tarvitaan Raspberry Pi V3 tai uudempi, johon on asennettu Raspbian Buster OS.
- Tarvitaan Linux-tietokone, johon on asennettu Ubuntu 18.04 -käyttöjärjestelmä.

Tämän esimerkin voi toteuttaa myös niin, että käytössä on vain Raspberry Pi tai Linux-työasema, mutta silloin ei voi tietenkään ottaa etäyhteyttä vaan silloin sekä Client- että Server-ohjelmisto toimii samalla koneella.

5.5.2 Asennetaan ohjelmat

Molempiin tietokoneisiin asennetaan tarvittavat ohjelmat ja kirjastot. Lähes kaikki tarvittava saadaan helposti asennettua antamalla kaksi alla olevaa komentoa.

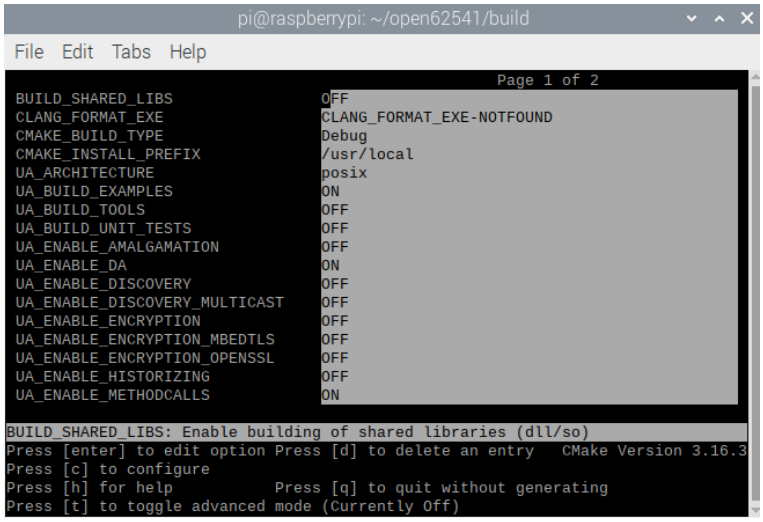
```
sudo apt-get install git cmake cmake-curses-gui build-essential gcc python3-
pip qttools5-dev python3-pyqt5 libmbedtls-dev check libsubunit-dev python-
sphinx graphviz python-sphinx-rtd-theme

sudo pip3 install opcua-client
```

Tässä esimerkissä käytetään open62541-palvelinohjelmistoa, joka on avoimen lähdekoodin toteutus OPC UA -palvelimesta. Asennetaan OPC UA -palvelin open62541 antamalla seuraavat komennot.

```
git clone https://github.com/open62541/open62541.git
cd open62541
mkdir build
cd build
cmake ..
ccmake ..
```

Otetaan cmake-määritysvaiheessa käyttöön UA_BUILD_EXAMPLES-vaihtoehto (kuva 5), jotta saadaan valmiita esimerkkejä heti käyttöön.



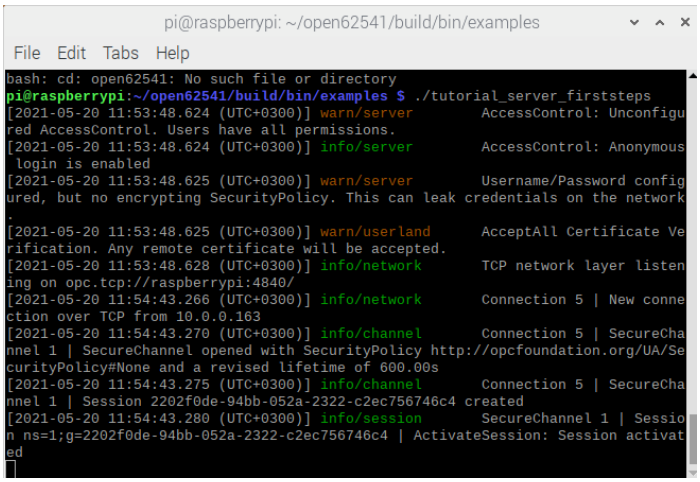
Kuva 5. Otetaan esimerkkidata käyttöön.

5.5.3 Käynnistetään OPC UA -palvelin.

OPC UA -palvelin käynnistetään antamalla seuraavat komennot.

```
make
cd bin/examples
./tutorial_server_firststeps
```

OPC UA -palvelin on nyt käynnissä, ja se kuuntelee TCP-porttia 4840. Se avaa uuden ikkunan (kuva 6), josta näkee muodostetut yhteydet ja mahdolliset varoitukset.



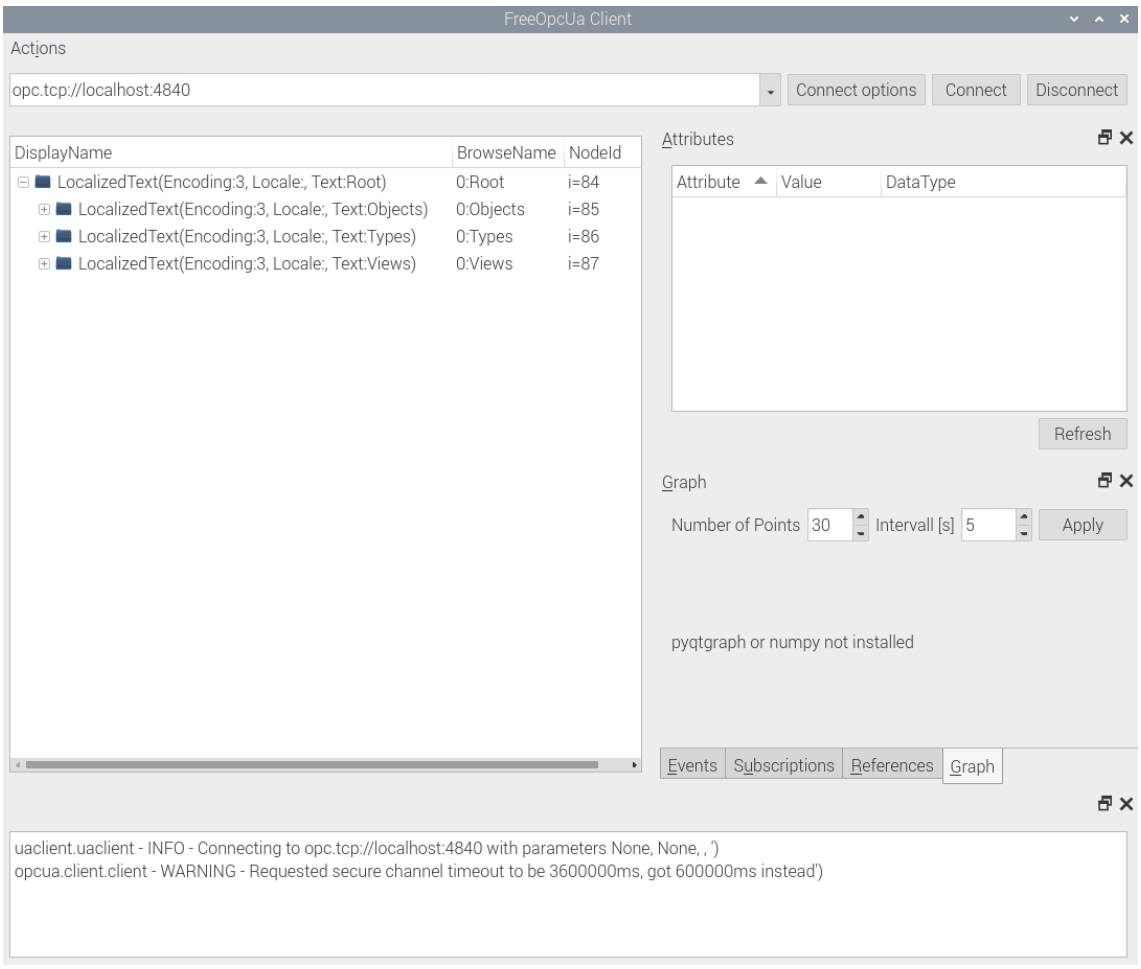
Kuva 6. OPC UA -palvelimen tilaikkuna

5.5.4 Otetaan yhteys OPC UA -palvelimeen

FreeOpcUa OPC UA -asiakasohjelman voi suorittaa samalla Raspberry Pi:llä, jossa palvelinohjelmisto pyörii tai Linux-tietokoneella. Molemmissa tapauksissa voi käyttää samaa komentoa, kun se käynnistetään sen pääteikkunasta.

```
opcua-client
```

Tämän komennon jälkeen avautuu käyttöliittymän ikkuna (kuva 7).



Kuva 7. FreeOpc Clientin käyttöliittymä

Mikäli yhteys otetaan samasta Raspberrystä, jossa palvelinohjelmisto toimii, niin osoitteeksi laitetaan opc.tcp://localhost:4840 ja painetaan Connect. Mikäli yhteys otetaan toiselta tietokoneelta, korvataan sana localhost Raspberryn osoitteella.

Jos yhteys on muodostettu onnistuneesti, FreeOpcUa-asiakasohjelman vasemmassa näyttöosiossa on luettelo OPC UA -palvelimen tietomallinäkymästä, jota voi selata.

5.5.5 Esimerkkitapauksen yhteenveto

Asennus Raspberry Pi -tietokoneeseen sujui ongelmitta. Tätä esimerkkiä varten asennettu Linux-työasema sen sijaan vaati hieman ylimääräistä säätämistä, joka johtui uuden Ubuntu-jakelun muutoksista. Kun Linux-työasema oli valmis, niin yhteydenotto OPC UA -palvelimeen sujui ongelmitta ja haluttuja arvoja pystyi muuttamaan vaivatta.

6 Etäyhteys pilvipalvelun kautta

Pilvipalvelulla tarkoitetaan tietoteknisten palveluiden toimittamista internetin välityksellä. Yleisimmät pilvipalvelut ovat tallennustila tai virtuaalikone, mutta tarjolla on myös tuhansia sovelluksia ja palveluita. Sen sijaan että kuluttaja tai yritys ostaisi lisenssejä tai laitteistoja, niin pilvipalveluista vuokrataan palveluita tai kapasiteettia ja niistä maksetaan käytön mukaan.

> Pilvipalvelua voi verrata hajautettuun ympäristöön (vrt. klusteri (tietotekniikka)). Käsitteenä se kuvaa paradigman muutosta, jonka tuloksena palvelu tarjotaan ”pilvessä”, jonka teknisiä yksityiskohtia palvelun käyttäjät eivät voi nähdä tai hallita. Pilvipalvelu kuvaa uutta tietoteknisten palveluiden tuottamisen, käyttämisen ja toimittamisen mallia, johon liittyy internetin yli palveluna tarjottuja dynaamisesti skaalautuvia ja virtuaalisia resursseja (4).

Suurimpia pilvipalveluiden tarjoajia tällä hetkellä ovat Microsoft ja Amazon. Tässä työssä esitellään hieman erästä Microsoftin ratkaisua ja toteutetaan sillä pieni esimerkki.

6.1 Azure IoT Hub

IoT, Internet of Things (suomeksi esineiden internet) -termillä tarkoitetaan laitteita, jotka on kytketty internet-verkkoon ja joita voidaan hallita tai valvoa etäältä. Yksinkertaisimmillaan esimerkiksi vaikkapa lämpötila-anturi, johon on liitetty jonkinlainen tiedonsiirtolaite, joka lähettää annetuin väliajoin tai pyydettäessä lämpötila-arvon etäkohteeseen.

> Microsoft Azure on Microsoftin julkinen pilvipalvelu. Azurea voidaan käyttää sekä virtuaalipalvelinten alustana (Infrastructure as a Service, IaaS) että kehittäjille tarkoitettuna kehitysalustana (Platform as a Service, PaaS). Microsoft Azure tarjoaa myös erilaisia valmiita pilvipalvelukomponentteja esimerkiksi mobiililaitteiden hallintaan (Microsoft Intune), dokumenttien suojaamiseen (Azure Rights Management Service), suurten datamassojen analysointiin (Big Data) ja koneoppimiseen (Azure Machine Learning). Lisäksi Azure toimii monen Microsoftin oman pilvisovelluksen, kuten esimerkiksi Dynamics CRM Onlinen alustana. (5.)

Azure IoT Hub on pilvipalvelu, johon IoT-laitteita voidaan liittää ja niitä voidaan hallita keskitetysti selainkäyttöliittymän avulla etäkohteesta. Iot-toteutuksissa dataa saattaa tulla erittäin paljon esimerkiksi tilanteessa, jossa on kymmeniä antureita, jotka lähettävät

sekunnin välein arvon. Azure IoT Hub ratkaisee tämän ongelman toimimalla rajapintana kaikille laitteille, jotta yhteyden voi muodostaa luotettavasti ja turvallisesti. Azure IoT Hub:ssa on useita valmiita tapoja koostaa data niin, ettei jokaista yksittäistä arvoa tarvitse katsoa, vaan aineisto esitetään vaikkapa trendeinä tai vain raja-arvojen poikkeamat näytetään tai niistä näytetään hälytys.

Eräs etu pilvipalveluiden käyttämisessä on se, että pilvipalvelu on aina samassa osoitteessa ja siihen voi helposti ottaa yhteyden riippumatta siitä, missä etäkäyttäjä on. Toisin sanoen etäkäyttäjän yhteyttä ei erikseen tarvitse konfiguroida mitenkään. Pilvipalveluita käytetään pääsääntöisesti selaimilla, joten etäkäyttäjän päätelaitettakaan ei tarvitse konfiguroida erikseen.

Azure IoT Hub:n hintaa hankala arvioida etukäteen. Hinta perustuu IoT-viestien ja Hub:ien määrään. Jo Microsoftin perushinnastossa kuukausihinta vaihtelee välillä 8 – 2100 €/kk (6). Lisäksi palvelusta saattaa joutua tilaamaan erikseen lisäpalveluita, kuten esimerkiksi levytilaa tai laskentatehoa.

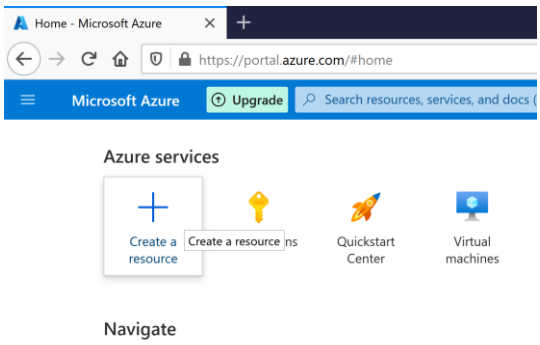
Azure IoT Edge on palvelu, joka on rakennettu Azure IoT Hubiin. Tilanteissa, joissa dataa tulee todella paljon saattaa olla käytännöllistä ottaa käyttöön pakallisesti erillinen laite, joka hoitaa osan IoT Hub:n toiminnoista paikallisesti lähellä IoT-laitteita. Tällaisella toteutuksella laitteet kuluttavat vähemmän aikaa yhteydenpitoon pilven kanssa, reagoivat nopeammin paikallisiin muutoksiin ja toimivat luotettavasti myös pitkiä offline-aikoja.

6.2 Raspberry Pi -esimerkin käyttöönotto Azure IoT Hub:n kanssa

Seuraavana toteutetaan esimerkki, jossa avataan Azure-tili, määritetään se ja konfiguroidaan Raspberry Pi lähettämään testidataa Azure IoT Hub -palveluun ja luetaan tiedot sieltä käyttämällä Visual Studio -ohjelmistoa Windows-työasemassa.

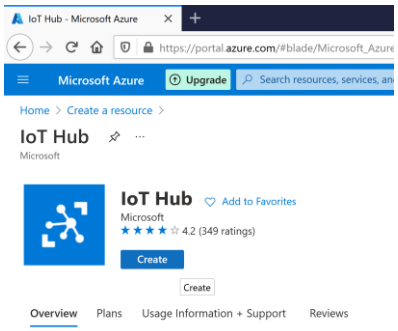
6.2.1 Azure-tilin avaaminen

Azure-tili avataan Azure-verkkosivustolla. Kun tili on avattu, siirrytään kotisivun valikkoon ja napsautetaan Luo resurssi tai Create resource, kuten kuvassa 8 esitetään.



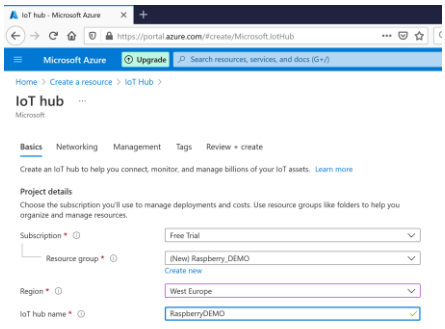
Kuva 8. Resurssin luominen

Resurssiluettelosta etsitään ja valitaan IoT Hub ja napsautetaan Create-painiketta (kuva 9).



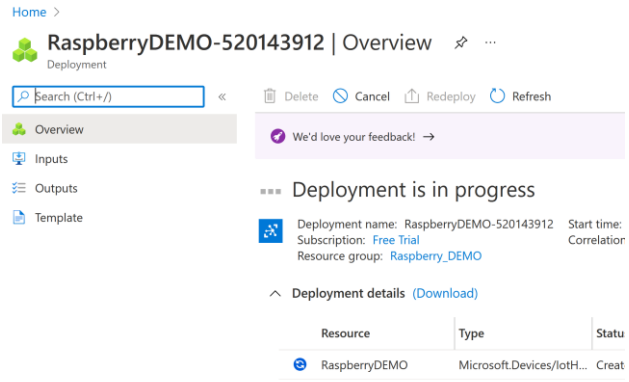
Kuva 9. IoT Hub -resurssin luominen

Tämän jälkeen avautuu lomake, jossa kysytään mm. haluttua Iot-keskuksen sijaintia ja pyydetään nimeämään luotava resurssi. Alueeksi kannattaa valita maantieteellisesti lähin palvelinkeskus.

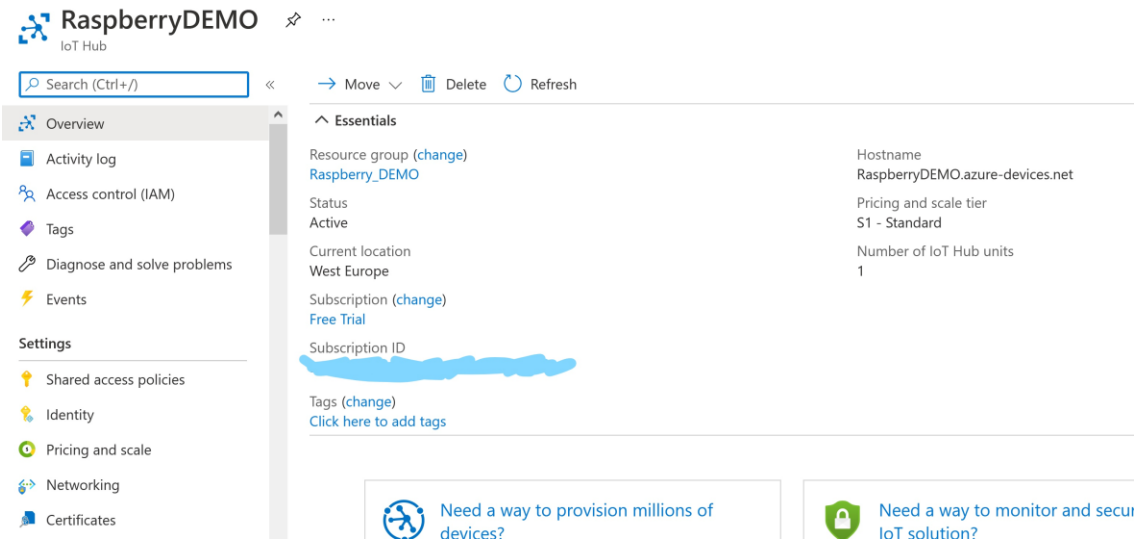


Kuva 10. IoT Hub -projeksin määrityksiä

Uuden Azure IoT Hub -resurssin luominen kestää muutaman minuutin (kuva 11), jonka jälkeen voi nähdä resurssin hallintapaneelin (kuva 12) ja pääsee käyttämään järjestelmää.



Kuva 11. Azure IoT Hub -resurssin luonti



Kuva 12. Azure IoT Hub -resurssin hallintapaneeli

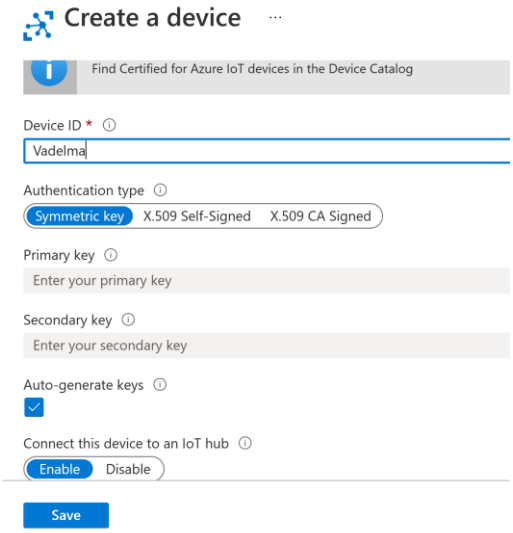
6.2.2 Asennetaan Raspberry Pi

Raspbian Pi valmistellaan asentamalla Buster-käyttöjärjestelmä ja asennuksen valmistuttua liitetään se WiFi-verkkoon.

6.2.3 Laitteen luominen Azure IoT Hubiin

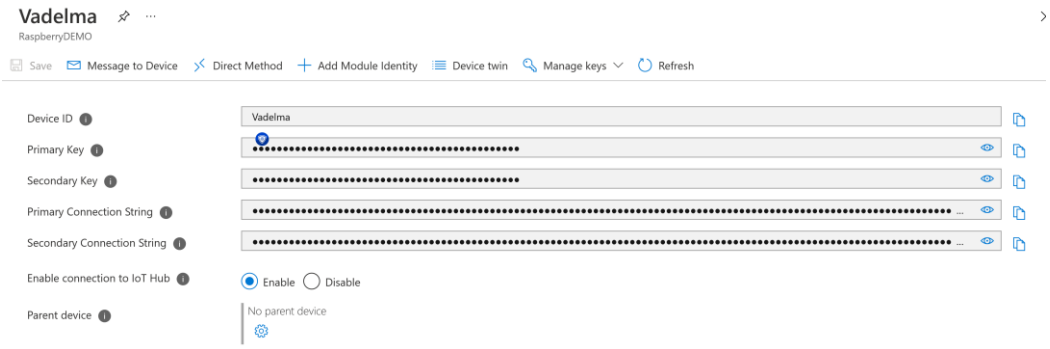
Seuraavaksi luodaan uusi laite Azure IoT Hubiin.

- Palataan Azure-portaaliin ja napsautetaan IoT-laitteita Azure IoT Hub -resurssisivulla. Luodaan uusi laite napsauttamalla + NEW
- Kirjoitetaan Laitetunnus (tunnistettava nimi), jätetään muut kentät oletusarvoihin (kuva 13) ja napsautetaan Tallenna-nappulaa



Kuva 13. Laitteen luominen Azure IoT Hubiin

- Napsautetaan laitetta ja kopioidaan ensisijainen yhteysmerkkijono, Primary Connection String (kuva 14)



Kuva 14. Yhteysmerkkijonon kopiointi

6.2.4 Ohjelmistokoodin käyttöönotto

Otetaan ohjelmistokoodi käyttöön Raspberry Pi:llä. Microsoft on julkaissut mallikoodin ja oppaat GitHubissa, jotta IoT Hub -projektit voidaan aloittaa nopeasti. Hyödynnämme niitä tässä antamalla Raspberryssä komennon:

```
git clone  https://github.com/Azure-Samples/azure-iot-samples-node.git
cd azure-iot-samples-node/iot-hub/Tutorials/RaspberryPiApp
npm install
```

6.2.5 Muodostetaan yhteys Azure IoT Hubiin

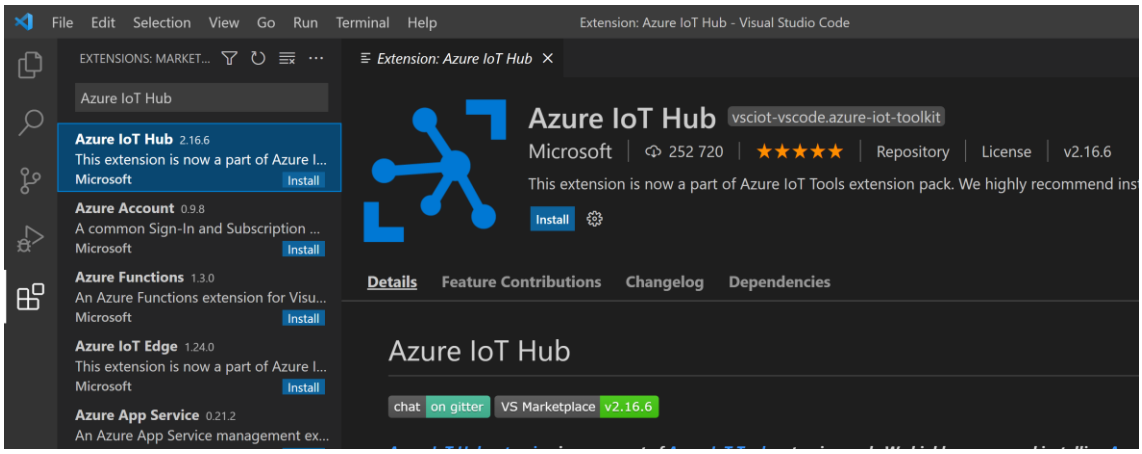
Seuraavaksi määritämme sovelluksen lähettämään simuloidut lämpötilatiedot Azure IoT Hubiin. Se tapahtuu antamalla Raspberry Pi:ssä seuraava komento.

```
sudo node index.js 'Tähän aiemmin kopioitu laitteen yhteysmerkkijono'
```

6.2.6 Tarkastelemme telemetriatietoja Azure IoT Hubissa

Tarkastelemme Azure IoT Hubiin vastaanotettuja telemetriatietoja käyttämällä Visual Studio -koodia.

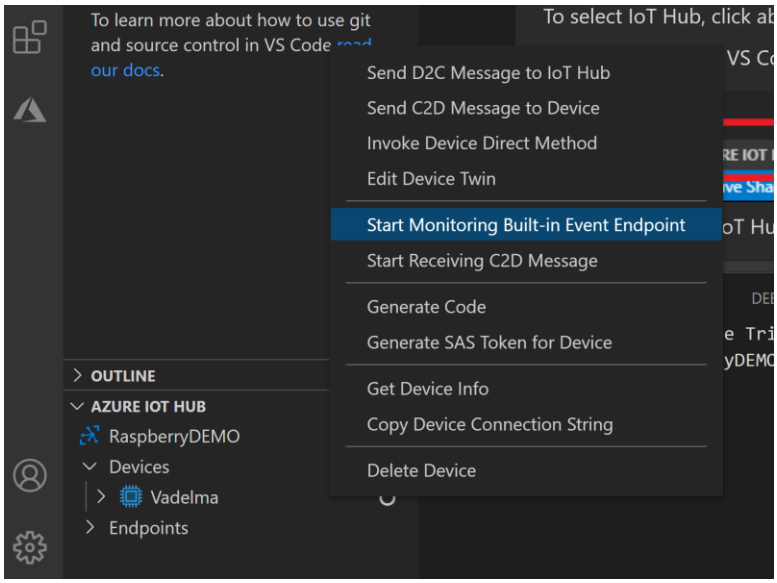
Avataan Visual Studio Code napsauttamalla Extensions. Etsitään ja asennetaan Azure IoT Hub -laajennus (kuva 15).



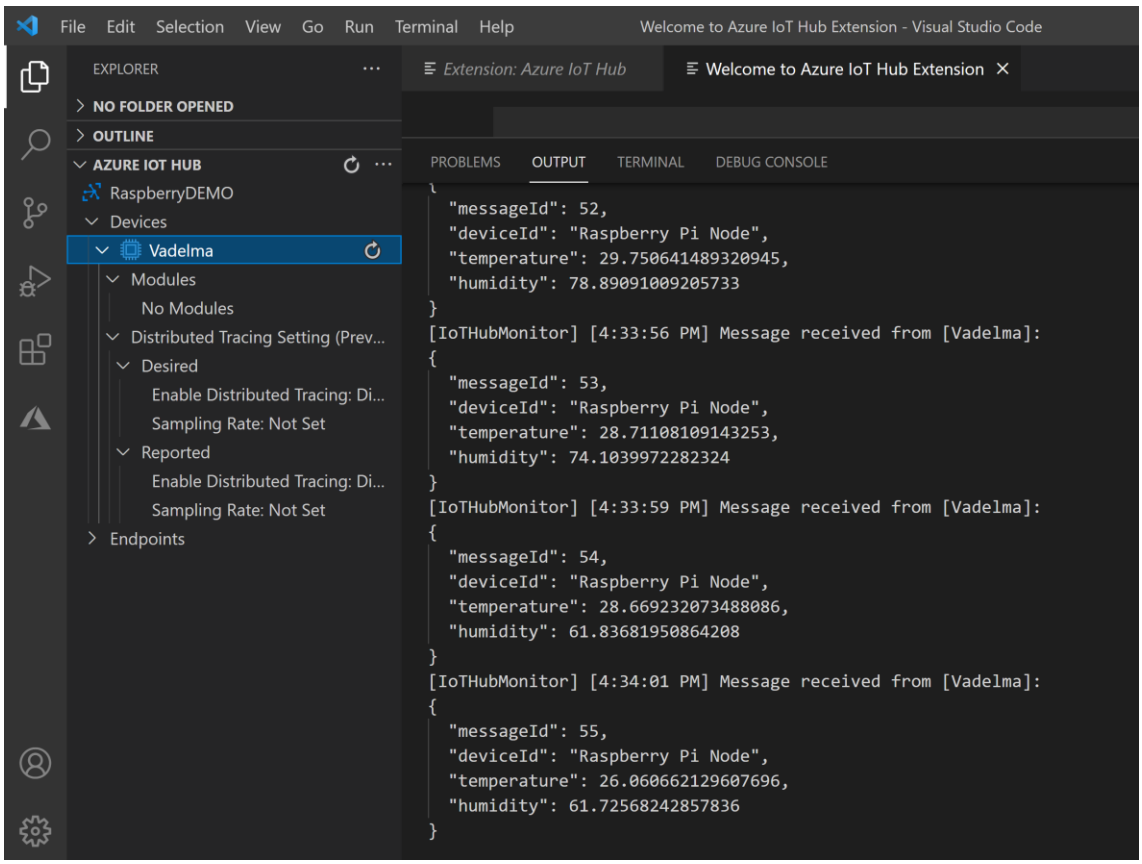
Kuva 15. Azure IoT Hub -laajennuksen asennus

Kun laajennus on asennettu, napsautetaan Azure IoT Hubia Explorerissa. Se pyytää käyttäjää kirjautumaan sisään Azure-portaaliin ja näyttää sitten Azure IoT Hub -resurssin ja Raspberry Pi -laitteen

Napsautetaan Raspberry-laitetta hiiren kakkospainikkeella ja napsautetaan Start Monitoring Built-in Event Endpoint (kuva 16), jolla käynnistetään tapahtuman seuranta. Tämän jälkeen alkaa näkymään Raspberry Pi:ltä vastaanotetut telemetriatiedot (kuva 17).



Kuva 16. Tapahtuman seurannan käynnistäminen



Kuva 17. Raspberry Pi:ltä vastaanotetut telemetriatiedot näkyvät ikkunan oikeassa puoliskossa

6.2.7 Esimerkkitapauksen yhteenveto

Asennukset sujuivat ongelmitta RaspBerry Pi:ssä, Azure IoT Hubissa ja Windowsissa. Kun RaspBerry Pi oli saatu lähettämään testidataa Iot Hub:iin niin tiedot pystyi lukemaan helposti tavoitellulla tavalla.

7 Yhteenveto

Etäyhteyden automaatiojärjestelmään voi ottaa lukuisilla tavoilla. Erityistä huomiota tulee kiinnittää tarvittavaan tietoturvan tasoon. Etäluettava lämpötila-anturi ei vaadi erityistä tietoturvaa. Pahin skenaario mahdollisen tietomurtautujan päästessä on anturi antaa väärän lämpötila-arvon tai ei anna arvoa ollenkaan. Tilanne tietysti muuttuu, mikäli kyseisen anturin arvolla säädetään jotain toimilaitetta tai lämpötilalukemalla on tärkeä merkitys, jolloin tietoturva pitää olla merkittävästi paremmalla tasolla.

Noudattamalla tietoliikenteen hyväksi havaittuja ja testattuja menetelmiä on automaation etäyhteyksiin suhteellisen vaivatonta saada tarvittava tietoturva. Kaikkiin kaupallisiin ratkaisuihin sellainen on jo oletuksena tarjolla.

Tietoturvan lisäksi etäyhteyksiä tulee tarkastella tietoliikenteen näkökulmasta. Kuinka luotettava ja nopea yhteys tarvitaan? Joihinkin tapauksiin langaton yhteys on varsin riittävä, joihinkin kriittisiin järjestelmiin tarvitaan kiinteä yhteys, tai jopa moninkertaistettu. Nopeuden lisäksi joissain tapauksissa yhteyden viive on myös merkittävä. Lisäpohdintaa aiheuttaa myös datan määrä, jolloin saattaa tulla kyseeseen osan toimintojen vieminen lähemmäs laitteita edge computing -tyyppisillä ratkaisuilla.

Automaation etäyhteydet ovat kuitenkin nykypäivänä helpohkosti järjestettävissä, ja lähes joka tapaukseen löytyy kustannustehokas ja toimiva ratkaisu.

Lähteet

1 Awake security. Verkkoaineisto. https://awakesecurity.com/blog/analyzing-team-viewer/. Luettu 13.3.2021.

2 Korhonen, Suvi. 2013. TeamSpy vakoilee TeamViewer-etähallinnan kautta https://www.tivi.fi/uutiset/teamspy-vakoilee-teamviewer-etahallinnan-kautta/1fc2a143-c8d0-3e1d-8da2-7f511fa90e4e. Luettu 14.4.2021.

3 RealVNC. Verkkoaineisto. https://www.realvnc.com/en/connect/pricing/. Luettu 21.5.2021.

4 Wikipedia Pilvipalvelu. Verkkoaineisto. https://fi.wikipedia.org/wiki/Pilvipalvelu. Luettu 20.5.2021.

5 Wikipedia Microsoft Azure. Verkkoaineisto. https://fi.wikipedia.org/wiki/Microsoft_Azure. Luettu 20.5.2021.

6 Microsoft. Verkkoaineisto. https://azure.microsoft.com/en-us/pricing/details/iot-hub/#pricing. Luettu 20.5.2021.