



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Jere Rahikainen

# Keskitetty etäyhteysjärjestelmä eriko- koisiin teollisen internetin sovelluksiin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

24.8.2020

Tekijä Otsikko Sivumäärä Aika	Jere Rahikainen Keskitetty etäyhteysjärjestelmä erikokoisiin teollisen internetin sovelluksiin 31 sivua 24.8.2020
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	sähkö- ja automaatiotekniikka
Ammatillinen pääaine	automaatio
Ohjaajat	Johtaja Pasi Torenius Lehtori Reijo Leinonen
<p>Teollinen internet, IIoT, on voimakkaasti kehittyvä teollisuuden ilmiö, ja palveluntarjoajia on lukuisia. Usein yritysten kiinnostusta teollista internetiä kohtaan haittaavat tietoturvariskien pelko sekä eri aikakausien laitteiden integroinnin hankaluus. Oikeanlaisilla laitteilla nämä ongelmat on mahdollista minimoida.</p> <p>Sarlinin edustamat tietoturvalliset VPN-reitittimet sekä monipuoliset protokollamuunninimet helpottavat osaltaan näiden yleisimpien esteiden purkamista. Tämän työn tarkoituksena oli tutkia niiden soveltuvuutta erilaisiin IIoT-ratkaisuihin. Työ tehtiin luomalla simuloitu tiedonkeruusovellus automaatioverkosta pilvipalveluun käyttäen Sarlinin edustamia ja maahan tuomia tuotteita. Datalähteenä käytettiin Red Lion DA30D -protokollamuunninta, jolla datan kerääminen eri aikakausien laitteista ja eri protokollilla käy helposti. Data luettiin DA30D:stä MB Connect Linen tietoturvallisella mbNET-reitittimellä, jota on jo pitkään käytetty muun muassa useissa eri etähuolto- ja etävalvontakohteissa. Reitittimeen asennettiin mbEDGE-lisäohjelmisto, joka laajentaa reitittimen käyttömahdollisuuksia IoT- ja IIoT-sovelluksissa.</p> <p>Data luettiin DA30D:stä Modbus TCP -protokollaa käyttäen, käsiteltiin mbEDGE:n Node-RED-ympäristössä ja lähetettiin Microsoftin Azure-pilvipalveluun, jossa se visualisoitiin käyttäen Azureen sisältyvää Time Series Insightsia. Myös MB Connect Linen tarjoamalle omalle pilvilustalle tehtiin yksinkertainen datan visualisointi, samoin kuin Node-REDin omaa mitaristoa käyttäen.</p> <p>Työssä tehdyn kokeen perusteella laitteet soveltuvat erilaisiin teollisen internetin kohteisiin, ja niiden käyttöönotto on vaivatonta. Työ rajattiin IO-määrältään pieneen ja yksinkertaiseen testisovellukseen, mutta konsepti skaalautunee erikokoisiin tarpeisiin.</p> <p>Loppupäätelmänä voidaan sanoa, että mbNET ja mbEDGE tarjoavat kiinnostavia mahdollisuuksia teollisessa internetissä.</p>	
Avainsanat	Teollinen internet, IIoT, IoT, reunalaskenta

Author Title Number of Pages Date	Jere Rahikainen A Centralized Remote Connection System for IIoT Applications of Various Sizes 31 pages 24 <sup>th</sup> August 2020
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Technology
Instructors	Pasi Torenus, Director Reijo Leinonen, Lecturer
<p>Industrial internet is a strongly growing phenomenon in industry. Often companies' interest in IIoT is hindered by fear of security threats and the difficulty in integrating devices of different eras. With the right kind of devices, these problems can be minimized.</p> <p>The cyber secure VPN routers and versatile protocol converters in Sarlin's representation can be used to help clear some of these obstacles. The aim of this study was to investigate their suitability in various IIoT solutions. The work was done by creating a simulated data collection application from an automation network to a cloud service using products that Sarlin represents and imports. The data source used was Red Lion DA30D protocol converter, which makes collecting data from devices of different eras with various protocols easy. The data was read using MB Connect Line's mbNET router, which has already long been used in several different remote service and remote monitoring cases. The router was equipped with the mbEDGE suite, which further expands the router's capabilities in IoT and IIoT solutions.</p> <p>The data was read using Modbus TCP protocol, edited in mbEDGE's Node-RED environment and sent to a Microsoft Azure cloud service, where it was then visualized using the Time Series Insights included in Azure. A simple visualization was also made in the cloud service provided by MB Connect Line, as well as using Node-RED's own dashboard.</p> <p>According to the test done in the work, the devices are well suited for various use cases in Industrial Internet and they are easily commissioned. The work was limited to a simple test application with only a few IOs, but the concept should be well scalable for needs of various scopes.</p> <p>As a conclusion it can be said that mbNET and mbEDGE offer interesting possibilities for industrial internet.</p>	
Keywords	Industrial internet, IIoT, IoT, edge computing

# Sisällys

## Lyhenteet

1	Johdanto	1
1.1	Opinnäytetyön tausta, tavoitteet ja menetelmät	1
1.2	Sarlin Oy Ab	2
2	Teollinen internet	3
2.1	Automaatioverkko	4
2.2	IoT-reunayhdyskäytävä	4
2.3	Pilvipalvelut	5
2.4	MQTT	7
2.5	JSON	7
2.6	Node-RED	8
2.7	Tietoturva	9
3	MB Connect Line	10
3.1	Reitittimet	10
3.2	Datadiodit	13
3.3	mbEDGE	14
3.4	Palvelinvaihtoehdot	15
4	IIoT-sovellusesimerkki Sarlinin tarjoamilla tuotteilla	15
4.1	Red Lion DA30D	16
4.2	DA30D-protokollamuuntimen konfigurointi	16
4.3	Visualisointi ja yhteydet pilvipalveluihin	19
4.4	Azure IoT Hub	21
4.5	mbEDGE:n käyttöönotto	21
4.6	mbEDGE:n konfigurointi	22
4.7	Azure Time Series Insights	26
5	Yhteenveto	28
	Lähteet	29

## Lyhenteet

EDA	Event-driven architecture, tapahtumapohjainen arkkitehtuuri.
DDoS	Distributed Denial of Service, hajautettu palvelinestohyökkäys.
FTP	File Transfer Protocol, tiedostonsiirtomenetelmä kahden tietokoneen välille.
IaaS	Infrastructure as a Service, infrastruktuuri palveluna.
IIoT	Industrial Internet of Things, teollinen internet.
IoT	Internet of Things, esineiden/asioiden Internet.
JSON	JavaScript Open Notation. IoT:ssä usein hyödynnetty tiedostomuoto.
LAN	Local Area Network, lähiverkko.
MQTT	Message Queuing Telemetry Transport, eräs IoT:ssä ja M2M:ssä hyödynnetty tiedonsiirtoprotokolla.
M2M	Machine to machine, laitteiden välinen suora yhteys.
NAT	Network Address Translation, osoitteenmuunnos.
OPC	Open Platform Communications. Alun perin sanoista OLE (Object Linking and Embedding) for Process Control. Joukko teollisuusautomaatiossa käytettäviä tiedonsiirron standardeja.
OPC-UA	OPC Unified Architecture. OPC Foundationin kehittämä tietoliikenneprotokolla teollisuusautomaatioon.
PaaS	Platform as a Service, sovellusalusta palveluna.
PLC	Programmable Logic Controller, ohjelmoitava logiikka.

SaaS	Software as a Service, ohjelmisto palveluna.
SFTP	SSH File Transfer Protocol. Tiedonsiirtoprotokolla SSH-yhteyden yli.
SHA	Secure Hash Algorithm. Kryptografinen tiivistefunktio.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
WAN	Wide Area Network, ulkoverkko.
WLAN	Wireless Local Area Network, langaton lähiverkko.

# 1 Johdanto

## 1.1 Opinnäytetyön tausta, tavoitteet ja menetelmät

Teollinen internet, IIoT, on jo pitkään ollut alan puhutuimpia ilmiöitä. Siitä on lupailtu jopa seuraavaa teollista vallankumousta, ja tähän on myös hyvät perusteet. Kuluttajamarkkinoilla esineiden internet on otettu innokkaasti vastaan, mutta teollisuudessa kasvu ei ole täysin vastannut odotuksia. Suurimpana esteenä tähän on yleensä nähty huoli tietoturvasta. Tietoturva onkin syytä ottaa vakavasti, mutta toisaalta useissa teollisuusyrityksissä on suuria tietoturvariskejä riippumatta siitä, onko niissä käytössä IIoT:hen laskettavia ratkaisuja. Kun IIoT:tä rakennetaan asianmukaisilla laitteilla ja asiantuntevan kumppanin avustamana, voidaan tietoturvariskit pitää minimaalisina. [1.]

Tässä opinnäytetyössä on tavoitteena tutkia, miten teollisen internetin kaikenkattavia sovelluksia voidaan toteuttaa Sarlinin edustamilla tuotteilla. Erityisesti keskiössä on MB Connect Linen äskettäin julkaisema mbEDGE-ohjelmisto, jolla kyseisen valmistajan etäyhteysreitittimien käytettävyyttä voidaan laajentaa kattamaan teollisen internetin tarpeita. Yhdistettynä reitittimen mahdollistamaan VPN-yhteyteen sekä protokollamuuntimen tuomiin liityntämahdollisuuksiin saadaan näin yhdellä laitekokonaisuudella katettua niin etähuolto ja -valvonta kuin tiedonsiirto pilvisovelluksiin.

Työssä käydään läpi teollisen internetin peruskäsitteitä sekä sitä, mitä vaatimuksia teolliseen internetiin kytkeytyvien laitteiden on täytettävä.

Työ suoritetaan tekemällä simuloitu tiedonkeruuesimerkki automaatioverkosta pilvipalveluun. Työssä käytettävät laitteet ovat kaikki Sarlinin edustuksessa olevia tuotteita, ja niiden toimintaa tarkastellaan teollisen internetin näkökulmasta. Lopuksi työhön sisällytetään pohdintaa tämänkaltaisen järjestelmän tuomista mahdollisuuksista teollisuudessa toimivalle yritykselle.

## 1.2 Sarlin Oy Ab

Sarlin Oy Ab on vuonna 1932 perustettu suomalainen perheyhtiö, joka tuottaa teknisiä tuotteita, ratkaisuja ja palveluja teollisuudelle ja kunnille. Se on osa Sarlin Group -konsernia, johon kuuluu Sarlinin lisäksi Pietarsaaressa toimiva Beamex Oy, joka on kansainvälisesti tunnettu kalibrointilaitteiden valmistaja. Sarlinin pääkonttorilla Vantaan Kai-vokselassa työskentelee noin 80 henkilöä, minkä lisäksi toimipisteitä ja työntekijöitä on useissa kaupungeissa eri puolilla Suomea, muun muassa huolto- ja asennustehtävissä. Yhteensä henkilöstöä on noin 100.

Sarlinin osaamisalueita teollisuudessa ovat automaatio, kaasus- ja energiatekniikka sekä paineilma. Automaatioratkaisuihin Sarlin on rakentanut valmistajariippumattoman ja kattavan edustusvalikoiman eri alueiden johtavien valmistajien kanssa. Sen edustus kattaa koko IIoT-sovellukseen tarvittavan pinon mittauksista tiedonsiirtoon ja datan käsittelyyn aina sovellusohjelmistoihin saakka. Laitteiden osalta tähän sisältyvät muun muassa erilaiset anturit, prosessiteollisuuden instrumentointi, koneturvallisuus, etäyhteysjärjestelmät ja -reitittimet, tietoturva, protokollamuuntimet ja näyttöpaneelit.

Kaasu- ja energiatekniikan alueella Sarlin tarjoaa muun muassa mikroturbiinilaitoksia, moottorivoimalaitoksia, kaasus- ja LNG-järjestelmiä, maa- ja biokaasun tankkausasemia, biokaasun jalostuslaitoksia sekä ORC-järjestelmiä hukkalämmön hyödyntämiseen. Yli 80% biokaasulla tuotetusta sähköstä Suomessa tehdään Sarlinin toimittamilla moottori- ja turbiinilaitoksilla. Lisäksi suurin osa Suomen kaasutankkausasemista on Sarlinin toimittamia.

Paineilmasta Sarlinilla on kokemusta jo monen vuosikymmenen ajalta. Sarlin toimittaa paineilman tuottamiseen tarvittavat kompressorit ja jälkikäsittelylaitteet sekä kokonaiset paineilmajärjestelmät teollisen ja lääkkeellisen paineilman sekä hengitysilman tuottamiseen. Usein paineilmaa ostetaan myös ulkoistettuna palveluna, jolloin laitteet ja järjestelmät pysyvät Sarlinin omistuksessa. Sarlin tarjoaa myös paineilmajärjestelmien analysointipalveluja, vuotojen kartoitusta ja paineilman tuoton optimointia. Sarlinin paineilmapalveluille on myönnetty Avainlippuputunnus. [2.]

Omana tuotteenaan on Sarlinilla kehitetty Sarlin Balance -ohjausjärjestelmä paineilma-verkoille. Sen avulla paineilmajärjestelmän tilaa pystytään seuraamaan reaaliaikaisesti



etäyhteyden päästä, ja järjestelmä optimoi ja tasaa paineilman tuottoa verkossa. Näin voidaan luopua yleisesti paineilmajärjestelmissä käytetystä ylimääräisestä paineesta kulutuspiikkien varalta, ja saavuttaa jopa 30% säästö paineilman tuottamiseen käytettävässä energiassa. [3.]

## 2 Teollinen internet

Teollinen internet, IIoT, on nimensä mukaisesti teollisuudessa sovellettava alakäsite laajemmasta käsitteestä esineiden internet, IoT. Esineiden internet (joskus myös asioiden internet) tarkoittaa lyhyesti ilmaistuna tietoverkon yli kommunikoivia laitteita ja näiden muodostamaa infrastruktuuria. Laite voi tässä yhteydessä olla myös virtuaalinen eli yksinkertainen sovellus. IoT käsitetään yleisesti kuluttajille suunnatuksi, ja se sisältää sellaisia tuotteita kuin älykäs jääkaappi, internetiin kytketty valaistusjärjestelmä tai erilaisia puettavia älylaitteita, joiden sanotaan tekevän arjesta helpompaa ja mukavampaa. Käytännön hyöty voidaan kuitenkin usein kyseenalaistaa, ja IoT saakin osakseen paljon aiheellistakin kritiikkiä muun muassa tietoturva-aukkojen luomisesta ilman merkittävää lisäarvoa käyttäjän elämään. [4; 5.]

Teollinen internet voidaan määritellä yhdistelmänä älykkäitä koneita, ihmisiä ja prosesseja. Se sisältää yleensä analytiikkaa jossakin muodossa sekä takaisinkytkentää prosessin alkupäähän. Sen tarkoituksena voi olla luoda lisäarvoa tehostamalla prosesseja, mutta se voi myös mahdollistaa täysin uudenlaisia liiketoimintamalleja. IIoT:n ansiosta huolto- ja kunnossapitotoimissa voidaan siirtyä ennakoivaan malliin sen sijaan, että odotettaisiin vikojen ilmaantumista koneissa ja laitteissa tai tehtäisiin huoltotoimenpiteet aikataulun mukaan riippumatta todellisesta tarpeesta. Sitä voidaan myös käyttää suuntaamaan resursseja sinne, missä niistä on eniten hyötyä.

Yhtenä teollisen internetin piirteenä on älyn siirtyminen pilvestä sen reunalle. Kun nykyisin suurin osa datan käsittelystä tapahtuu keskitetysti pilvipalveluissa, on ennustettu, että tulevaisuudessa datamäärien yhä kasvaessa entistä suurempi osa käsittelystä tehdään jo ”pilven reunalla”, kentälaitteiden ja internetin välissä, jolloin lähetettävän datan määrä saadaan pienennettyä. Myös internet on muuttumassa niin sanotusti sumumaiseksi, mikä tarkoittaa, että älykkäät toiminnot pirstaloituvat siellä pienempiin yksiköihin. [6.]

Seuraavissa luvuissa käsitellään teolliseen internetiin läheisesti liittyviä käsitteitä ja rakenteita.

## 2.1 Automaatioverkko

Teollisuusautomaation varhaisina aikoina automaatioverkot olivat merkittävästi erilaisia rakenteeltaan ja toiminnaltaan kuin IT-verkko, eikä automaatioverkkoa yleisesti itse asiassa edes pidetty verkkona – nimitys kenttäväylä onkin peräisin näiltä ajoilta. [7.] Varhaisimmissa automaatiojärjestelmissä anturit ja toimilaitteet oli kytketty ohjainlaitteisiin suorilla point-to-point-yhteyksillä. Kenttäväylä kehitettiin yksinkertaistamaan kytkentöjä ja sen avulla saavutetaan merkittäviä säästöjä asennuskustannuksissa ja vähennetään asennusten vikaherkkyttä. Kenttäväylää käytettäessä myös automaatiojärjestelmän laajentaminen on huomattavasti helpompaa. [8.]

Nykyaikaisessa automaatioverkossa digitalisoidut kenttälaitteet kykenevät kommunikoidaan keskenään paikallisesti. Anturit ja toimilaitteet ovat yhä useammin ”älykkäitä”, mikä tarkoittaa, että ne voivat normaalin mittausdatan lisäksi välittää esimerkiksi tietoja tilastaan, vastaanottaa asetusparametreja verkon välityksellä, ja vikaantuessaan välittää parametrit uudelle laitteelle. Tällaisten laitteiden asennus, kunnossapito ja vaihtaminen on perinteiseen anturiin tai toimilaitteeseen verrattuna helppoa eikä vaadi erityisosaamista. [9.]

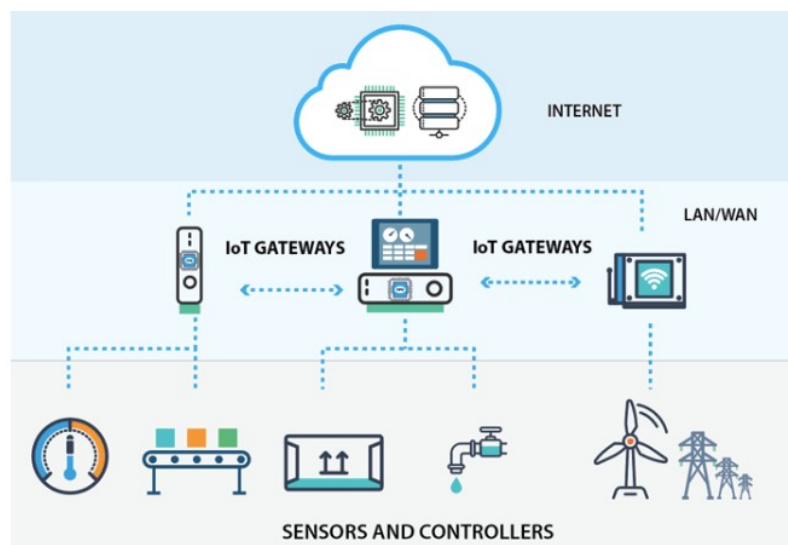
Automaatioverkon laitteiden ei normaalisti ole syytä olla suoraan yhteydessä internetiin. Kuitenkin vuonna 2013 tehdyssä kartoituksessa löytyi Suomesta tuhansia laitteita, jotka esimerkiksi laitevalmistajan, tuotenimikkeen tai käytetyn protokollan perusteella kuuluvat teollisuuden automaatiojärjestelmiin, rakennusautomaatioon, sähkönhallintaan tai järjestelmien etäkäyttöön. [10.]

## 2.2 IoT-reunayhdyskäytävä

Teollisen internetin laajentuessa nousee entistä useammin tarve yhdistää keskenään erilaisia laitteita ja protokollia eri aikakausilta vaihtelevin liitettävyyssominaisuuksin. Iot-reunayhdyskäytävät (IoT gateway tai edge gateway) tarjoavat mahdollisuuden luotettavan verkon rakentamiseen ja reunalaskentaominaisuuksien hyödyntämiseen.

Tyypillisesti IoT-reunayhdyskäytävä on laite, joka sisältää sovellusohjelmiston datan siirtämiseksi laitteesta toiseen laitteeseen tai pilvipalvelimeen. Se voi myös suorittaa edistyneempiä toimenpiteitä, kuten datan suodatusta, puskurointia, aggregointia, visualisointia, analysointia, verkon tietoturvatoteutuksia, käyttäjähallintaa ja järjestelmän diagnostiikkaa.

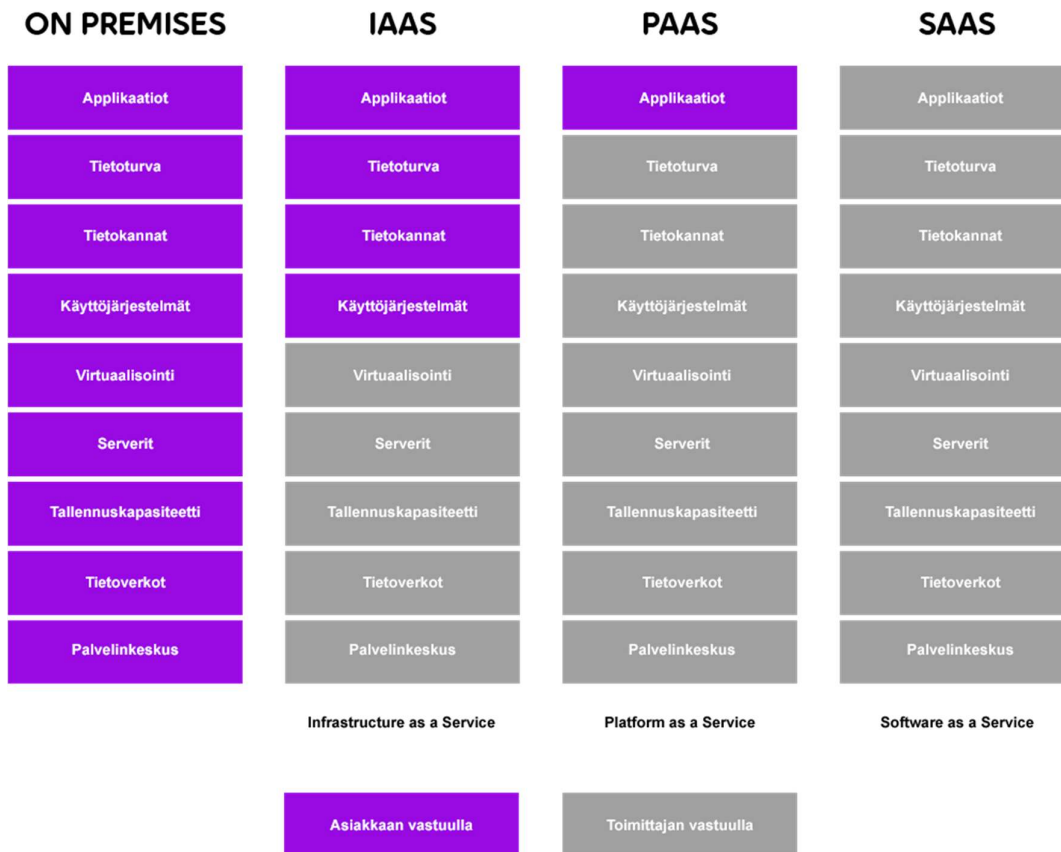
Datan esikäsittely verkon reunalla ennen pilveen lähettämistä on tullut yhä tärkeämmäksi. Sen sijaan, että siirrettäisiin suuria määriä raakadataa, ainoastaan määrättyt arvot lähetetään pilveen. Tämä säästää kaistatilaa ja mahdollistaa reaaliaikaisemman yhteyden. [11.]



Kuva 1. IoT-reunayhdyskäytävä [12.]

### 2.3 Pilvipalvelut

Pilvipalveluilla tarkoitetaan useita erilaisia internetin välityksellä tarjottavia palveluja. Perinteisesti ne jaetaan kolmeen malliin: IaaS eli infrastruktuuri palveluna, PaaS eli sovelluslusta palveluna ja SaaS eli ohjelmisto palveluna. Kuvassa 2 hahmotetaan toimintojen jakautumista toimittajan ja asiakkaan vastuulle eri palveluvaihtoehtoissa.



Kuva 2. Pilvipalvelumallit. [13.]

IaaS on palvelu, jossa tarjoaja vastaa ainoastaan infrastruktuurista, eli palvelun vaatimista tiloista ja laitteista, näiden ylläpidosta sekä tarvittavasta henkilöstöstä. Asiakkaan vastuulle jää kaikki muu: palvelimien asennukset ja konfigurointi, asennukset, ohjelmistojen asennukset ja hallinnointi sekä palvelimen tietoturva palomureineen.

PaaS-mallissa tarjotaan edellisen lisäksi sovellusalusta, jonka avulla yritys voi esimerkiksi kehittää mobiilisovelluksia tai tietokantapalveluja loppuasiakkaan käyttöön. Palveluun sisältyy sovellusten kehittämiseen, testaamiseen ja julkaisemiseen tarvittavat ohjel-

mistot, sekä usein myös suorat FTP-, SFTP- tai SSH-yhteydet palvelimiin, komentorivityökaluja sekä API-rajapinta. Asiakkaan tehtävä on huolehtia sovellustason tietoturvasta ja päivityksistä.

SaaS on pilvipalveluista useimpien tuntema malli. Siinä toimittaja tarjoaa valmiin sovelluksen ostajan käyttöön, ja palvelusta maksetaan tyypillisesti ainoastaan käytön mukaan. Palvelun tuottaja vastaa kokonaisuudessaan ohjelmistosta, ja päivitykset ja lisenssit kuuluvat palvelun hintaan. SaaS-tyyppistä palvelua käytetään tyypillisesti web-selaimen kautta; esimerkkinä tästä käy sähköpostipalvelu. [13; 14.]

## 2.4 MQTT

MQTT (Message Queuing Telemetry Transport) on M2M- ja IoT-sovelluksissa usein hyödynnetty tiedonsiirtoprotokolla, joka toimii publish/subscribe-periaatteella. MQTT:tä käytettäessä asiakkaat eivät kommunikoi suoraan keskenään, vaan niiden välille vaaditaan välittäjä, broker. Broker on palvelin, joka vastaanottaa kaikki asiakkaiden lähettämät viestit ja jakaa ne eteenpäin toisille asiakkaille. Viesteissä ei määritellä vastaanottajan osoitetta, vaan niihin on liitetty aihe (topic-kenttä), jonka perusteella mikä tahansa asiakas voi vastaanottaa viestin. [15.]

MQTT:tä käyttävien asiakkaiden ei tarvitse erikseen pyytää dataa, vaan broker välittää sen automaattisesti, kun sen sisältö muuttuu. Asiakkailla on siis jatkuva TCP-yhteys brokeriin. MQTT:n TCP-portit ovat tavallisesti 1883 suojaamattomalle yhteydelle ja 8883 suojatulle yhteydelle. [16.]

## 2.5 JSON

JSON (JavaScript Object Notation) on tekstimuotoinen formaatti strukturoidun datan ilmaisuun. Nimensä mukaisesti se pohjautuu JavaScriptin objektisyntaksiin, mutta ei kuitenkaan ole riippuvainen käytetystä kielestä, ja monet ohjelmointiympäristöt tarjoavat työkaluja JSON-syntaksin lukemiseen ja kirjoittamiseen.

JSON-muotoinen data tallennettuna .json-päätteiseen tekstitiedostoon on yleisesti käytetty tapa siirtää dataa web-sovellusten välillä. Kevyen rakenteensa takia se on myös suosittu formaatti IoT-sovelluksissa. JSON-formaatissa data on tallennettu ihmisen luettavaan muotoon, mikä myös puoltaa sen käyttöä etenkin yksinkertaisissa IoT-sovelluksissa. [17.]

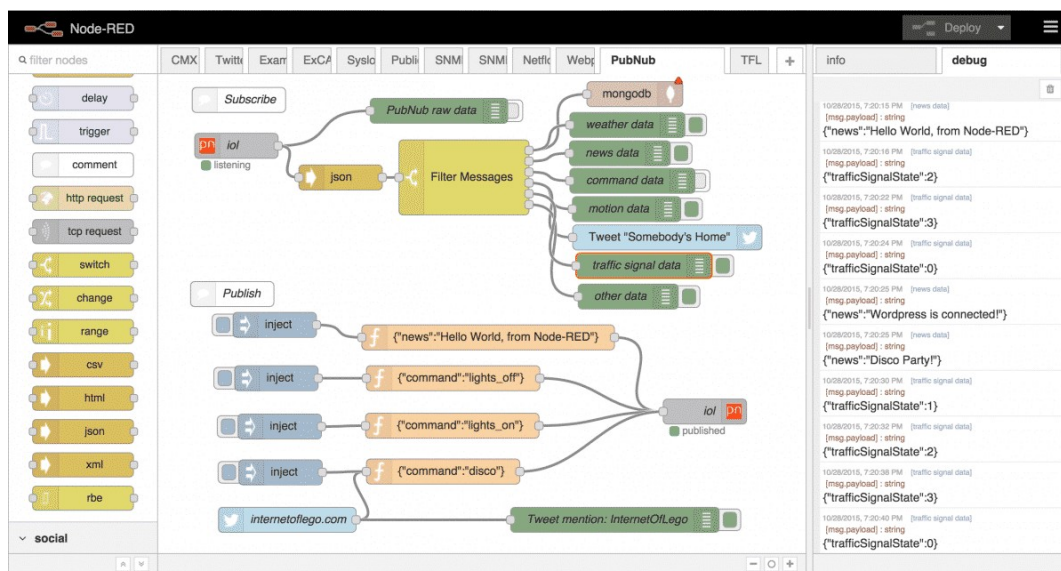
## 2.6 Node-RED

Node-RED on IBM:n kehittämä ohjelmointityökalu, joka tarjoaa helppokäyttöisen, selainpohjaisen käyttöliittymän IoT-rajapintojen ohjelmointiin Drag and drop -menetelmällä. Se pystyy esimerkiksi lukemaan PLC:ltä dataa ja tallentamaan sekä jakamaan sitä eri alustoille internetissä. Node-RED tukee yleisimpiä teollisuudessa käytettyjä tiedonsiirtoprotokollia, kuten MQTT, OPC-UA, ModBus ja S7.

Node-RED on Node.js-suoritusympäristön päälle rakennettu graafinen ohjelmointityökalu. Node.js on tapahtumapohjaiseen arkkitehtuuriin (EDA) perustuva suoritusympäristö, joka on tarkoitettu verkkosivujen palvelinpuolen ohjelmointiin. Siinä javascript-pohjaiset komennot on tehtävä kirjoitettuna koodina, ja tätä helpottamaan kehitettiin Node-REDin graafinen ympäristö, jossa ohjelmakoodi on paketoitu solmuihin (node). Solmuja voi yhdistää toisiinsa vetämällä niiden väliin ”johdon”, jolloin yhden solmun käsittelemä viesti välittyy ”johdon” toisessa päässä olevaan solmuun. Yksi solmu voi olla yhteydessä useaan solmuun samanaikaisesti. [18.]

Data siirtyy solmusta toiseen viestipakettina, jotka ovat yksinkertaisia javascript-objekteja. Niillä voi olla mitä vain ominaisuuksia eli avaimia, tyyppillisesti vähintään ”payload”-avain. Node-RED lisää objekteihin lisäksi ”\_msgid”-avaimen, jonka avulla viestin etenemistä virrassa voidaan seurata. Objektien syntaksi on muotoa ”msg.avain”; esimerkiksi viestin ”payload”-avaimeen viitataan osoitteella ”msg.payload”.

Kun Node-RED sovellus on käynnistetty, sitä pääsee konfiguroimaan verkkoselaimella osoitteesta 127.0.0.1:1880 (tai localhost:1880).



Kuva 3. Node-RED. [18.]

Käytettävissä olevien solmujen ”palettia” voi tarpeen mukaan rajata, ja lisää solmuja voi vapaasti ladata esimerkiksi Github-sivustolta. Node-RED sisältää hakutyökalun solmujen lataamiseen. Solmuja voi myös tarvittaessa luoda itse, jos ei valmiista tarjonnasta löydy soveltuvaa solmua.

## 2.7 Tietoturva

Kun internetiin yhdistettyjen laitteiden ja pilvipalvelujen määrä kasvaa, nousee myös riski tietomurroille ja hajautetuille hyökkäyksille (DDoS) niiden kautta. Yleensä murtautujien varsinainen kiinnostus kohdistuu muihin kohteisiin kuin IIoT-laitteisiin itseensä, ja näitä käytetään vain hyökkäyksen apuvälineinä. Teollisen internetin markkinoilla toimivan laitevalmistajan on huomioitava kasvanut kyberuhka ja panostettava suunnittelussaan tietoturvaan vakuuttaakseen asiakkaansa ja erottuakseen kuluttajamarkkinoiden IoT-laitevalmistajista.

Maailman talousfoorumi suosittelee koko teollisuudenalan kattavia standardeja tietoturvan toteuttamiseksi parhailla käytännöillä. Se on tutkimuksessaan määrittellyt neljä haastetta, joihin laitevalmistajien on pureuduttava: tiukan ohjelmistokehityssyklin noudattaminen, riskienarviointimallit, laitteiston integriteetti ja salaus. [19.]

Kuten edellä mainittiin, myös automaatioverkon laitteet ovat usein tarpeettomasti ja tietoturvan kannalta puutteellisesti liitettynä internetiin. Jokainen internetiin kytketty laite on potentiaalinen kyberhyökkäyksen kohde, ja erityisen haavoittuvaisia ovat sellaiset laitteet, joiden käyttäjä ei edes tiedä niiden olevan kytketty julkiseen verkkoon. Hyökkääjät käyttävät hyväkseen tunnettuja haavoittuvuuksia esimerkiksi yleisimmin käytetyissä ohjelmoitavissa logiikoissa, ja joitakin automaatioverkkoon tarkoitettuja ohjainlaitteita ei ole lainkaan suojattu tunkeutumista vastaan. [10.] Tämän takia minkä tahansa laitteen, joka yhdistää automaatioverkon julkiseen verkkoon, täytyy itsessään sisältää riittävä suoja, jottei se altista takanaan olevia laitteita hyökkäyksille.

### 3 MB Connect Line

MB Connect Line on saksalainen laitevalmistaja, joka ydinosaaamisalueellaan keskittyy etäyhteysreitittimien, tiedonkeruu- ja palomuurilaitteiden sekä näiden hallintaan tarkoitettujen palveluratkaisujen kehittämiseen ja valmistukseen. Sen toiminnan lähtökohtana ovat korkeat turvallisuusvaatimukset, ja tuotteet täyttävät nykyaikaisten määritysten mukaisen korkean turvallisuustason. Tuotekehitys seuraa turvallisuusmäärityksiä ja esimerkiksi laitteiden firmware-päivityksiä julkaistaan säännöllisesti. Sarlin on MB Connect Linen virallinen edustaja ja maahantuojaja Suomessa. Järjestelmä on hyväksytetty eri tietoturvasertifikaatteja myöntävien toimijoiden kanssa, mukaan lukien kotimainen Nixu sekä saksalainen Secuvera.

#### 3.1 Reitittimet

mbNET on MB Connect Linen tietoturallinen etäyhteysreititin, joka on saatavilla erilaisilla liitäntöillä ja yhteystekniikoilla varustettuna. Tietoturvaa parantavat muun muassa sisäänrakennettu palomuuuri sekä kovakoodattu laiteohjelmisto, joka estää ulkopuolisia tahoja korruptoimasta laitetta omilla ohjelmistoillaan. Kunkin laitteen web-käyttöliittymän oletussalasana on myös uniikki, mikä estää murtautumiset tunnettua tai yleistä salasanaa käyttäen (tyhjä kenttä, "admin", "password" tms.). Etäyhteyksien muodostamiseen reitittimissä käytetään openVPN-protokollaa.



mbNET-reitittimestä on saatavilla tarpeen mukaan vaihtoehtoja esimerkiksi erilaisilla modeemeilla, WLAN-yhteydellä, WAN-liitännöillä sekä kenttäväylä- ja sarjaliikenneporteilla. Modeemilla varustetuissa malleissa on kaksi SIM-korttipaikkaa, mistä on hyötyä esimerkiksi ajoneuvokäytössä, kun ylitetään säännöllisesti maarajoja. Korkeaa saatavuutta vaativissa voidaan käyttää toista vaihtoehtoista operaattoria varayhteytenä. Lisäksi kaikissa malleissa on digitaalisia tuloja ja lähtöjä. Tulojen avulla laite voidaan ohjelmoida esimerkiksi muodostamaan yhteys tai lähettämään hälytyksiä ulkopuolisten herätesignaalien mukaan. Digitaalisia lähtöjä puolestaan voidaan käyttää esimerkiksi muiden laitteiden etäkäynnistykseen tai -sammutukseen. Muita ominaisuuksia reitittimissä ovat muun muassa Lua-skriptien ajaminen ja helppo yhteensovittaminen yleisimpien PLC-tyyppien kanssa, kuten Siemens S7.

Reitittimien prosessorina toimii 32-bittinen ARM Cortex-A8, ja keskusmuistia siinä on 512 megatavua. Laite on koteloitu jämäkkään teräskoteloon.

Yhtenä uusimmista variaatioista mbNET-reitittimistä on julkaistu mbNET.rokey (kuva 4), jossa fyysisellä avainkytkimellä voidaan valita kolmen tilan välillä:

- OFF: VPN-yhteys estetty, internetyhteys estetty
- ONL: VPN- ja internetyhteydet käytettävissä
- REM: VPN- ja internetyhteydet käytettävissä, mukaan lukien reititykset LAN-puolelle. (Mahdollistaa huoltoyhteydet.)

Lisäksi laite voidaan palauttaa tehdasasetuksiin kääntämällä avainkytkin hetkeksi RST-asentoon uudelleenkäynnistyksen yhteydessä.



Kuva 4. mbNET.rokey RKH210

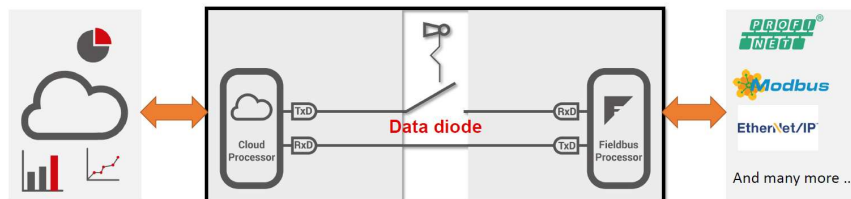
Sisäänrakennetulle palomuurille on valittavissa kolme esiasetusvaihtoehtoa:

- korkein turvallisuustaso
  - kaikki sisääntulevat paketit (internetistä tuleva data) hylätään
  - kaikki uloslähtevät paketit (LAN-verkosta lähtevä data) hylätään, paitsi DNS, FTP, IMAP, POP3, SMTP, HTTP, HTTPS, Telnet, NTP
- korjaus turvallisuustaso
  - kaikki sisääntulevat paketit hylätään
  - kaikki uloslähtevät paketit hyväksytään
- matalin turvallisuustaso
  - kaikki sisääntulevat ja uloslähtevät paketit hyväksytään.

Tehdasasetuksena palomuurilla on korkein turvallisuustaso. Lisäksi palomuurille voidaan määritellä portti-, protokolla- ja osoitekohtaisia sääntöjä sekä tunnelointi- ja NAT-sääntöjä.

### 3.2 Datadiodit

mbXLINK on MB Connect Linen laitesarja, jonka tiedonkeruulaitteet pohjautuvat data-diodiin. Datadiodilla tarkoitetaan elementtiä, jonka kautta data pääsee liikkumaan ainoastaan yhteen suuntaan, tässä tapauksessa kenttäväylästä tai automaatioverkosta pilveen (kuva 5).



Kuva 5. Datadiodin toimintaperiaate.

Monissa tapauksissa datadiodi on toteutettu ohjelmallisesti, minkä takia osaavan hakkerin on mahdollista ohittaa se. mbXLINKin (kuva 6) datadiodi on toteutettu fyysisellä erotuksella, joten minkäänlainen tietomurto internetin puolelta ei ole mahdollista, kun sisään tulokäytävää ei yksinkertaisesti ole. Datadiodin päälle- ja pois kytkeminen tapahtuu fyysisellä avainkytkimellä, mikä lisää käyttövarmuutta ja hallinnan tunnetta loppukäyttäjällä.



Kuva 6. mbXLINK.

### 3.3 mbEDGE

mbEDGE on Linux-pohjainen ohjelmistopaketti, joka laajentaa mbNET- tai mbNET.ro-key-reitittimen tai mbXLINK-datadiodin IoT-reunayhdyskäytäväksi, joka kerää dataa paikallisesti, prosessoi sitä ja siirtää sen eteenpäin pilvisovellukseen. mbEDGE tukee useita pilvialustoja kuten mbCONNECT24, Azure ja AWS sekä nykyaikaisia tiedonsiirtoprotokollia kuten OPC-UA ja MQTT.

mbEDGEstä on saatavilla start- ja advanced-versiot. Start-versio sisältää pelkän Node-RED-Dockerin. Advanced-versiossa on esiasennetun Node-REDin lisäksi mahdollisuus asentaa useita säiliöitä käytettäväksi käyttäjän omiin Docker-sovelluksiin. [20.]

mbEDGE toimitetaan 8 gigatavun teollisuus-SD-kortilla (kuva 7), jonka sisältämä data on salattu 256-bittisellä SHA-funktiolla. Kortin sallittu käyttölämpötila-alue on  $-40 \dots 85^{\circ}\text{C}$ , ja sen lukunopeus on 90 MB/s ja kirjoitusnopeus 20 MB/s.



Kuva 7. SD-kortti, jolla mbEDGE toimitetaan.

Dockereita hallitaan mbEDGEssä Portainer.io-työkalulla. Portainer on vapaan lähdekoodin ohjelma Docker-ympäristöjen hallintaan. Se koostuu yhdestä Dockerista, jota voidaan ajaa millä tahansa Docker Enginellä. [21.]

### 3.4 Palvelinvaihtoehdot

MB Connect Linen reitittimien ja muiden laitteiden hallinta on helpointa tehdä keskitetysti yhdeltä palvelimelta. Palvelimen portaalista käsin luodaan reititinkonfiguraatiot, hallitaan käyttäjiä ja näiden pääsyoikeuksia, muodostetaan etäyhteydet reitittimiin, valvotaan yhteyksiä sekä hoidetaan tiedonkeruu ja hälytykset. Myös mbEDGE:n asetukset ja ohjelmointi voidaan tehdä palvelimen kautta.

mymbCONNECT24.virtual-palvelin toimii VMware-pohjaisena virtuaalikoneena. Se on yksinkertainen asentaa ja ylläpitää. Halutessaan voi käyttää myös valmistajan tarjoamaa julkista palvelinta mymbCONNECT24, johon tilin voi luoda veloitusetta. Palvelimen tietoturvan ovat testanneet ja hyväksyneet muun muassa Nixu ja Secuvera.

Palvelinta voi käyttää web-selaimella, tai siihen voi muodostaa yhteyden mbDIALUP-ohjelmalla. Palvelimen kautta muodostetaan VPN-yhteydet reitittimiin, ja sieltä käsin voidaan myös avata suora linkki reitittimen ja sen takana olevien laitteiden web-käyttöliittymiin.

## 4 IIoT-sovellusesimerkki Sarlinin tarjoamilla tuotteilla

Tässä työssä tehtiin yksinkertainen simuloitu tiedonkeruuesimerkki automaatioverkosta Sarlinin tuotevalikoimaan kuuluvilla laitteilla pilvipalvelimelle. Kuvitteellisessa automaatioverkossa prosessista mitataan lämpötilaa ja painetta.

Red Lion DA30D -protokollamuuntimelle määriteltiin kaksi kokonaislukumuuttujaa, joista yksi saa arvoja välillä 200–210 ja toinen välillä 100–120 yhden sekunnin välein. Näiden muuttujien arvot luettiin Modbus TCP -protokollaa käyttäen mbEDGEllä ja lähetettiin edelleen Microsoft Azure-pilvipalveluun, jossa data visualisoitiin ja tallennettiin tietokantaan.

mbEDGE asennettiin mbNET MDH849 -reitittimeen, jonka ominaisuuksiin kuuluvat muun muassa Ethernet WAN -portti, neljä Ethernet LAN -porttia, LTE-modeemi kahdella SIM-korttipaikalla sekä SD-korttipaikka.

#### 4.1 Red Lion DA30D

Red Lion on yhdysvaltalainen laitevalmistaja, jonka tuotevalikoima käsittää muun muassa teollisuuskäyttöisiä verkkolaiteratkaisuja, paneelimittareita, protokollamuuntimia ja kosketusnäyttöpaneeleita. Sarlin on Red Lionin virallinen edustaja ja maahantuoja Suomessa.

Red Lion DA30D (kuva 8) on teollisuuskäyttöön tarkoitettu protokollamuunnin, jossa on sisäänrakennettuna muun muassa dataloggeri, verkkopalvelin ja virtuaalinen HMI. Laitteessa on valittavissa tällä hetkellä yli 300 eri tiedonsiirtoprotokollaa, mikä mahdollistaa eri valmistajien ja eri aikakausilta olevien laitteiden keskittämisen yhteen pisteeseen. Tästä keskitetystä pisteestä voidaan data siirtää laitteen sisäisellä valmiiksi sovitetulla MQTT-protokollalla yleisimpiin pilvipalveluihin: AWS, Azure, Google Cloud ja Sparkplug. Fyysisinä liityntöinä laitteessa on Ethernet-, USB-, RS232- ja RS485-portit. Erillisellä lisämoduulilla voidaan laite kytkeä myös esimerkiksi CAN- tai Profibus-väylään. [22.]



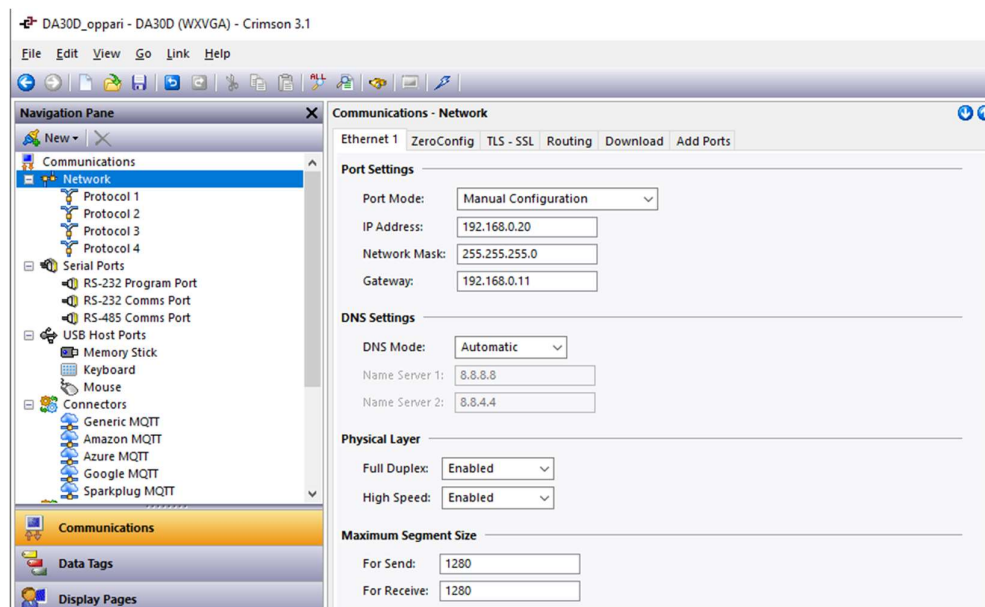
Kuva 8. Red Lion DA30D.

#### 4.2 DA30D-protokollamuuntimen konfigurointi

DA30D:n konfigurointi tapahtuu Crimson 3.1 -ohjelmalla, joka on ladattavissa ilmaiseksi valmistajan verkkosivuilta. Data Tags -valikon kautta päästään määrittelemään laitteen

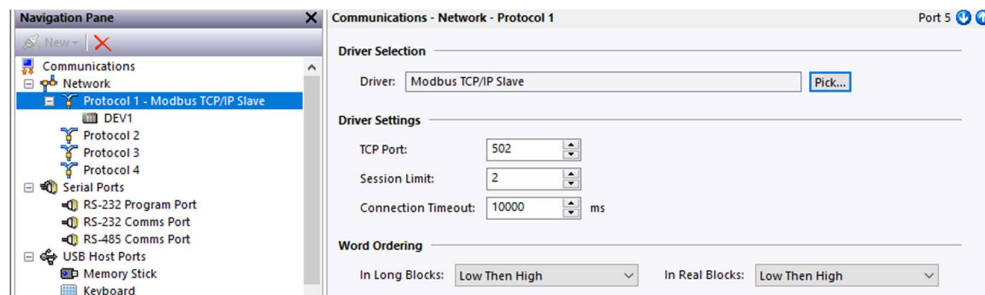
sisäiset datapisteet, joita tässä tapauksessa luotiin kaksi, tyyppiä Int. Datapisteiden nimiksi annettiin Temp1 ja PSI1. Nämä asetettiin saamaan satunnaisia arvoja välillä 200–210 ja 100–120 yhden sekunnin välein.

Dataliikenne mbEDGE:n suuntaan tapahtuu Modbus TCP -protokollalla, ja sitä varten määriteltiin laitteen Ethernet-portin asetukset (kuva 9). IP-osoite määriteltiin manuaalisesti, ja osoitteeksi asetettiin 192.168.0.20, aliverkon maski 255.255.255.0. Oletusyhdyskäytäväksi asetettiin mbNETin LAN-portin osoite 192.168.0.11. Muut asetukset jätettiin oletusarvoihinsa.



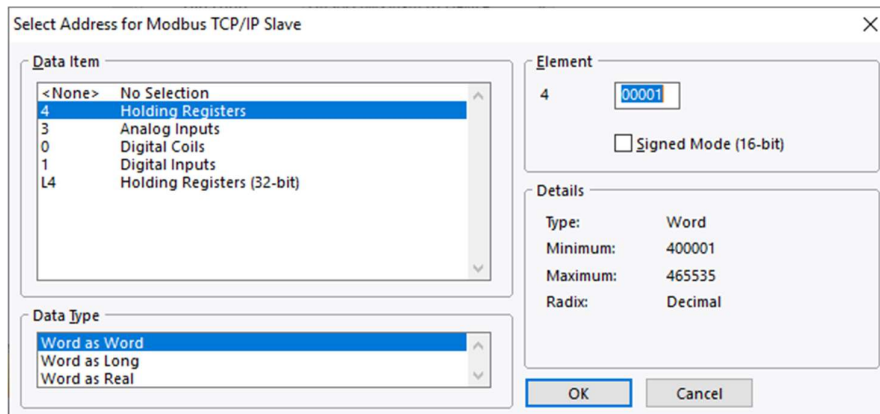
Kuva 9. DA30D:n Ethernet-portin asetukset.

Seuraavaksi porttiin määriteltiin Modbus TCP/IP Slave -ajuri (kuva 10). Ajurin asetukset pidettiin oletusarvoissaan.

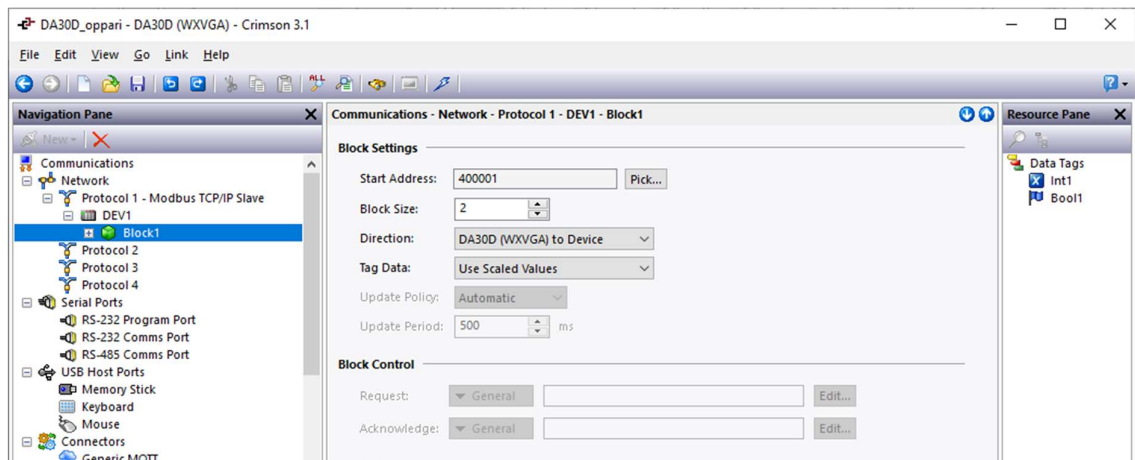


Kuva 10. DA30D:n Modbus Slave -ajurin asetukset.

Modbus TCP/IP Slave -ajurin alle muodostuu laite DEV1, joka tässä tapauksessa kuvaa DA30D-laitetta itsessään. Laitteen nimeä klikkaamalla avautuu näkymä, josta datapisteitä varten voidaan luoda blokkeja (gateway block). Datapistettä varten luotiin kahden muuttujan kokoinen blokki, joka alkaa osoitteesta 400001 (kuvat 11 ja 12).



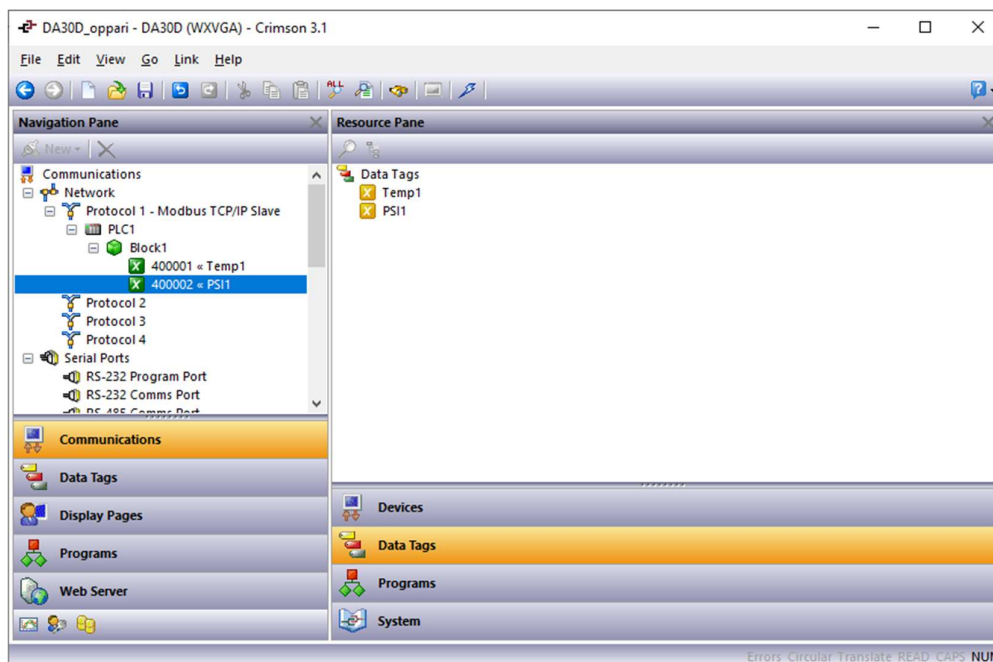
Kuva 11. Datablokin määrittely.



Kuva 12. Datablokin asetukset.

Lopuksi blokkiin liitettiin aiemmin luodut datapisteet Temp1 ja PSI1 (kuva 13).





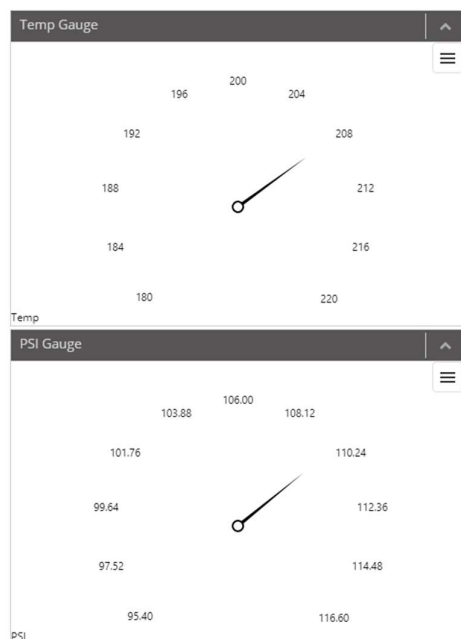
Kuva 13. Datapisteiden yhdistäminen blokkiin.

DA30D-laitteeseen on näin määritelty Modbus TCP/IP Slave -laite, jonka holding register -osoitteista 4:00001 ja 4:00002 löytyvät kokonaislukumuuttujat Temp1 ja PSI1.

#### 4.3 Visualisointi ja yhteydet pilvipalveluihin

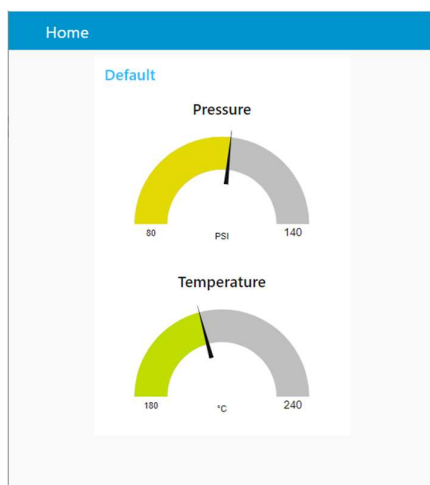
mbEDGE voi lähettää dataa eri pilvipalveluihin. Yksi sellainen on reitittimen konfiguroinnissakin käytettävä mymbCONNECT24.virtual-portaali, johon pystyy luomaan esimerkiksi yksinkertaisia visualisointeja luettavalle datalle.

Esimerkin vuoksi tässä työssä luotiin palvelimelle visuaalinen mittaristo, jolla näytetään luettujen muuttujien arvo mittareissa (kuva 14). Näitä varten palvelimelle luotiin omat datapisteet, joihin data voidaan Node-REDissä lähettää. Datapisteiden luomisen jälkeen kummallekin luotiin ensin Gauge-tyypin widgetit, jotka sitten sijoitettiin mittaristoon.



Kuva 14. mymbCONNECT24.virtual-palvelimelle luotu mittaristo.

Node-RED sisältää itsessään myös pohjan mittaristolle, jossa data voidaan visualisoida (kuva 15). Verrattuna mymbCONNECT24.virtual-portaalin mittaristoon se on varsin rajoittainen muokattavuudeltaan ja esimerkiksi eri käyttäjien pääsyoikeuksia ei pysty siinä määrittelemään. Se on kuitenkin vasteajaltaan huomattavasti nopeampi.



Kuva 15. Node-REDin mittaristo.

Varsinaisia IIoT-sovelluksia varten on tarpeen hyödyntää niitä varten kehitettyjä täysimittaisia pilvipalveluita, kuten Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud tai Oracle Cloud. Tässä työssä alustaksi valittiin Microsoft Azure.

#### 4.4 Azure IoT Hub

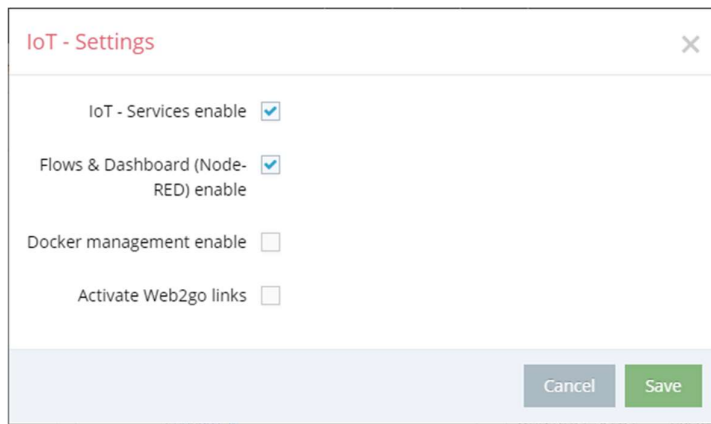
IoT Hub on Azuren hallinnoitu palvelu, joka toimii keskitettynä kaksisuuntaisena viestikeskukseksi IoT-palveluiden ja niissä hallinnoitujen laitteiden välillä. Sen tukemia viestintämuotoja ovat esimerkiksi mittausdatan lähetys laitteesta pilveen, tiedostojen lähetys laitteilta ja pyyntö–vastaus-tyyppiset metodit laitteiden hallintaan pilvestä. [23.]

Tätä työtä varten luotiin Azure IoT Hub, jolle annettiin nimeksi Inssihubi. Tämän jälkeen luotiin hubiin laite-ID mbEDGEä varten klikkaamalla ”IoT devices” ja ”New”, ja täytettiin tarvittavat tiedot.

Kommunikaatioon käytettiin MQTT-protokollaa. Azure IoT Hub ei ole varsinainen MQTT Broker, mutta se pystyy suorittamaan sille olennaisesti kuuluvat tehtävät.

#### 4.5 mbEDGE:n käyttöönotto

mbEDGE vaatii toimiakseen mbXLINK-, mbNET- tai mbNET.rokey-laitteen hardwareversion 03 tai uudemman, ja laitteen IoT-toiminnot on ensin otettava käyttöön web-käyttöliittymän tai palvelinportaalin kautta (kuva 16). SD-kortti asennetaan laitteen pohjasta löytyvään korttipaikkaan, jonka jälkeen laite tunnistaa kortin automaattisesti. Laitteen tilaa ilmaiseva ledi Fc4 vilkkuu ensin nopeasti, mikä tarkoittaa, että mbEDGE:n Dockereita käynnistetään. Kun Fc4 vilkkuu hitaasti, on mbEDGE toiminnassa.

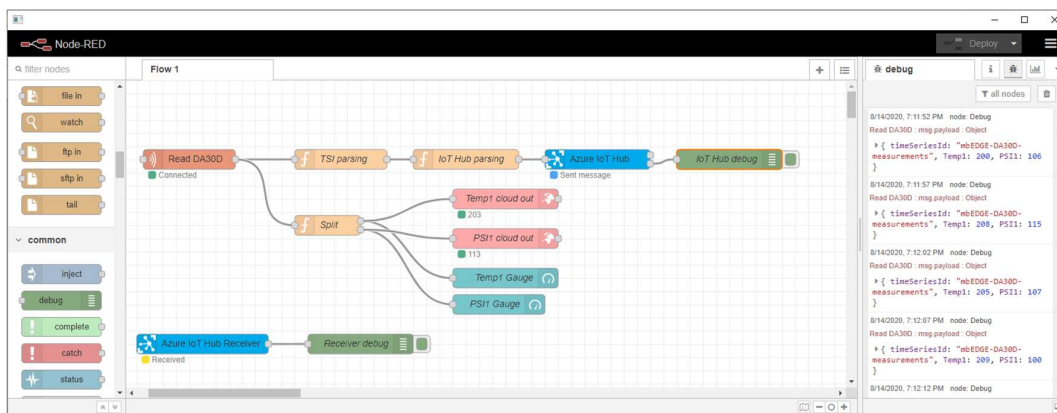


Kuva 16. IoT-toimintojen aktivointi mymbCONNECT24-portaalissa.

Kortin sisältö on salattu, ja kortissa on muistipaikat kolmelle purkuavaimelle. Kaksi näistä on tyhjiä, ja yhteen on tallennettu oletusavaimena kortin sarjanumero. Ensimmäisellä käyttökerralla laite lukee avaimen ensimmäisestä muistipaikasta ja avaa kortin sisällön. Tämän jälkeen laite muodostaa uniikin avaimen, kirjoittaa sen toiseen muistipaikkaan ja tyhjentää avaimen ensimmäisestä muistipaikasta. Näin korttia on tästedes mahdollista käyttää ainoastaan kyseisessä laitteessa. Jos laitetta halutaan vaihtaa, on ensin tällä laitteella luotava kortin kolmanteen muistipaikkaan vara-avain, jota voidaan käyttää toisessa laitteessa. Tämä estää kortin luvattoman käytön eri laitteessa.

#### 4.6 mbEDGEEn konfigurointi

Tiedonkeruussa käytettiin mbEDGEEn esiasennettua Node-REDiä (kuva 17). Tätä varten lisättiin mbEDGEEn palomuurisääntöihin pääsy porttiin 1880. Node-RED voidaan avata reitittimen web-käyttöliittymästä tai mymbCONNECT24-portaalista mbDIALUP-ohjelmalla.



Kuva 17. Node-REDin konfiguraatio.

Modbus TCP/IP -datapisteiden lukemiseen on mbEDGE:n Node-RED-ympäristöön asennettu valmiiksi solmu modbustcp (kuva 18). Modbus Read -solmulla luettiin DA30D:n holding-rekistereistä kaksi rekisteriä alkaen osoitteesta 4:00001 (tässä 3:00000 johtuen erilaisesta osoitteiden nimeämisestä).

**Edit modbustcp node**

---

**Properties**

Name:

Topic:

FC:

Address:

Quantity:

Poll Rate:

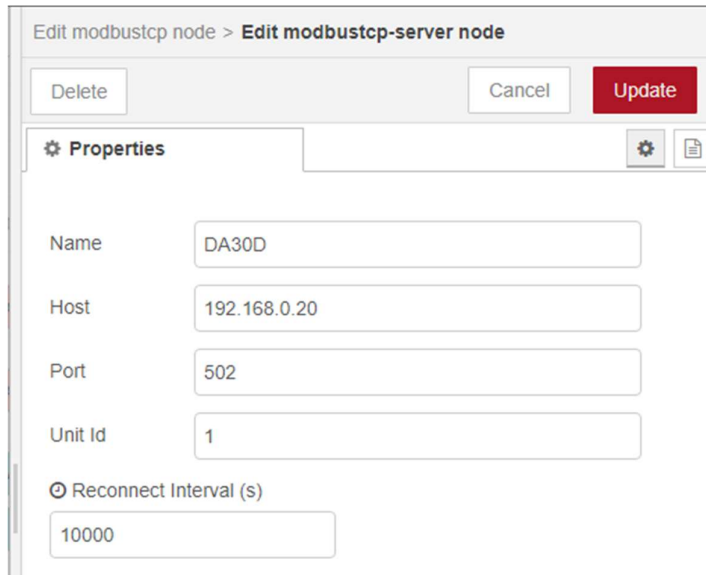
Server:

IEEE-754 # Type:

Endian:

Kuva 18. modbustcp-solmun asetukset.

Saman solmun Server-kohdasta päästään määrittelemään käytettävä Modbus TCP -palvelin (kuva 19). Tähän täytettiin aiemmin määritellyt DA30D:n Modbus TCP slave -ajurin asetukset.



Edit modbustcp node > Edit modbustcp-server node

Delete Cancel Update

⚙️ Properties 📄

Name DA30D

Host 192.168.0.20

Port 502

Unit Id 1

⊙ Reconnect Interval (s)

10000

Kuva 19. Modbus TCP -palvelimen asetukset.

Luettu data on nyt viestin payload-avaimessa taulukkona. Seuraavaksi data jäsenneltiin javascript-objektiksi niin, että mittausdata on siinä avain-arvo-pareina. Lisäksi viestiin sisällytettiin avain "timeSeriesId", jota tarvitaan myöhemmin datan visualisoinnissa. Jäsennely tehtiin function-solmulla, joka nimettiin "TSI parsing" (kuva 20).

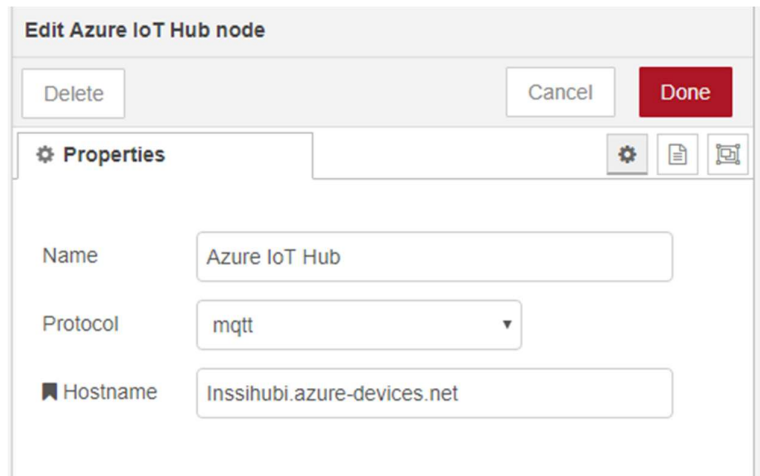


🔧 Function 📄

```
1 msg.payload = {
2   "timeSeriesId": "mbEDGE-DA30D-measurements",
3   "Temp1": msg.payload[0],
4   "PSI1": msg.payload[1]
5 };
6 return msg;
```

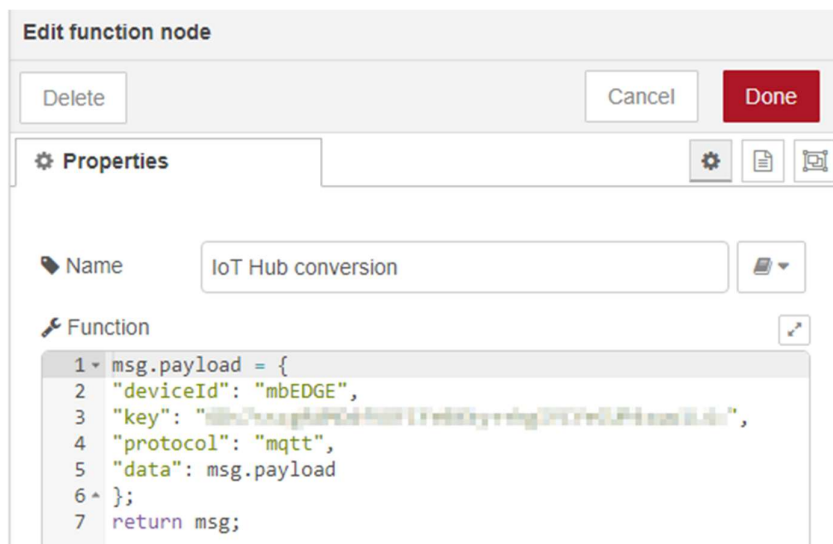
Kuva 20. TSI parsing -solmu.

Datan lähettämiseksi Azure IoT Hubiin asennettiin Node-REDiin solmupaketti node-red-contrib-azure-iot-hub. [24.] Datan lähettämiseksi käytettiin Azure IoT Hub -solmua. Tämän konfiguroinnissa määritellään käytettävä protokolla, tässä tapauksessa MQTT, sekä aiemmin määritellyn Azure IoT Hubin Hostname (kuva 21).



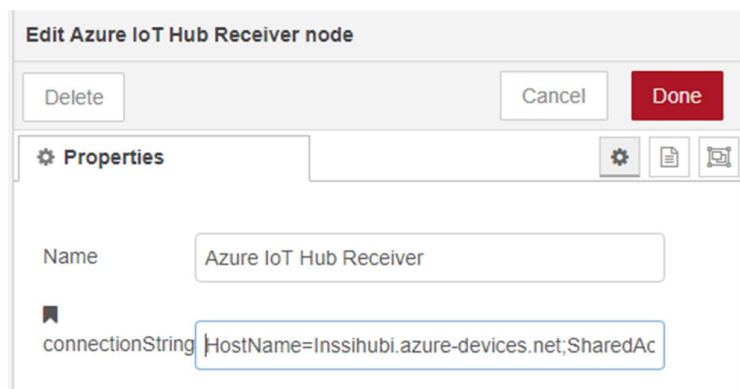
Kuva 21. Azure IoT Hub -solmu.

Kyseiselle solmulle lähetettävä data on ensin jäseneltävä niin, että sieltä löytyvät IoT Hubin vaatimina parametreina avaimet "deviceId", "key", "protocol" ja "data", sekä näiden perässä kaksoispisteen jälkeen vastaavat sisällöt. Avaimen "data" sisältämä tieto voi olla yksittäinen merkkijono tai javascript-objekti. [25.] Datan jäsentelyä varten solmun eteen lisättiin function-solmu, jossa datan jäsentely suoritetaan (kuva 22). Funktiossa "deviceId"-parametriksi määriteltiin "mbEDGE", "key"-parametriksi Azure IoT Hubista laitteen tiedoista löytyvä SharedAccessKey-avain, "protocol"-parametriksi "mqtt" ja "data"-parametriksi msg.payload, eli funktiosolmun TSI-parsing -solmulta vastaanottama javascript-objekti.



Kuva 22. Function-solmu.

Azure IoT Hubin vastaanottamaa dataa voidaan seurata Azure IoT Hub Receiver -solmulla (kuva 23). Tämän konfigurointiin vaaditaan ainoastaan Azure IoT Hubin Connection string -käskyjono, joka löytyy IoT Hubin "Shared access policies"-valikosta.



Kuva 23. Azure IoT Hub Receiver -solmu.

#### 4.7 Azure Time Series Insights

Azure Time Series Insights on työkalu aikasarjapohjaisen datan säilömiseen, visualisointiin, analysointiin ja etsimiseen. Se integroituu helposti Azure IoT Hubiin ja jäsentelee



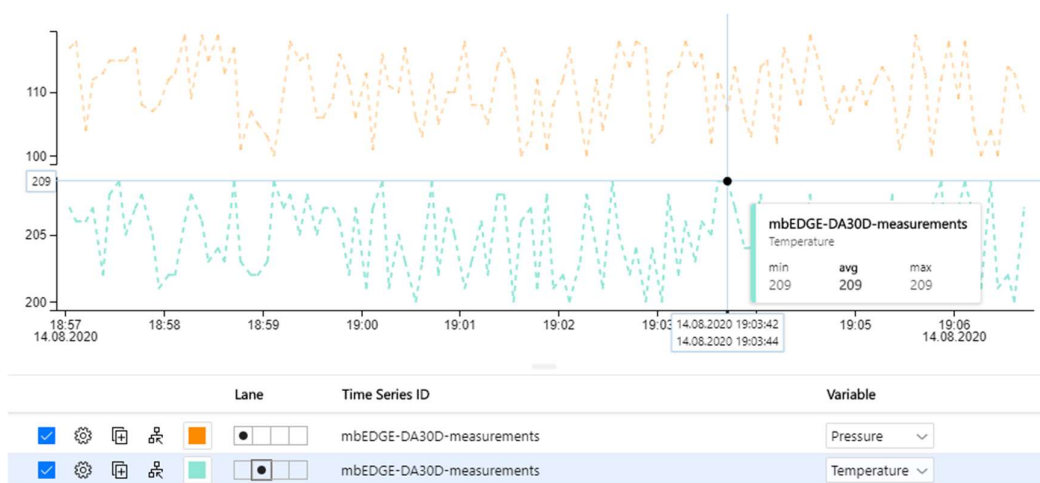
JSON-muotoista dataa viesteistä. Se liittää mittausdataan metadataa ja tallentaa datan taulukkomuodossa. [26.]

Kuvassa 24 on ote Time Series Insightsin tallentamasta datasta, jonka se on vastaanottanut Azure IoT Hubista. Dataan on sisällytetty aikaleima, ja se on jäsennelty automaattisesti avain–arvo-parien mukaan. Avain ”timeSeriesId” määriteltiin Time Series Insights -ympäristöä luodessa, ja sen avulla mittausdataa voidaan ohjata kuvaajassa eri instansseihin. Tässä yhteydessä käytettiin ainoastaan arvoa ”mbEDGE-DA30D-measurements”.

Events		22 events								
<input checked="" type="checkbox"/> All Columns		timestamp (\$ts)	timestamp (UTC+03:00) Local - Europe/Helsinki: EEST	Temp1	#	PSI1	#	timeSeriesId	abc	
<input checked="" type="checkbox"/> timestamp (\$ts)		14.08.2020 16:04:57.257	08/14/2020 19:04:57.257	203	107			mbEDGE-DA30D-measurements		
<input checked="" type="checkbox"/> timestamp (UTC+0... only)		14.08.2020 16:05:02.351	08/14/2020 19:05:02.351	204	112			mbEDGE-DA30D-measurements		
<input checked="" type="checkbox"/> # Temp1		14.08.2020 16:05:07.242	08/14/2020 19:05:07.242	200	108			mbEDGE-DA30D-measurements		
<input checked="" type="checkbox"/> # PSI1		14.08.2020 16:05:12.336	08/14/2020 19:05:12.336	207	112			mbEDGE-DA30D-measurements		
<input checked="" type="checkbox"/> abc timeSeriesId		14.08.2020 16:05:17.446	08/14/2020 19:05:17.446	202	114			mbEDGE-DA30D-measurements		
		14.08.2020 16:05:22.337	08/14/2020 19:05:22.337	208	111			mbEDGE-DA30D-measurements		
		14.08.2020 16:05:27.431	08/14/2020 19:05:27.431	200	101			mbEDGE-DA30D-measurements		
		14.08.2020 16:05:32.323	08/14/2020 19:05:32.323	206	107			mbEDGE-DA30D-measurements		
		14.08.2020 16:05:37.418	08/14/2020 19:05:37.418	207	119			mbEDGE-DA30D-measurements		
		14.08.2020 16:05:42.309	08/14/2020 19:05:42.309	203	113			mbEDGE-DA30D-measurements		

Kuva 24. Time Series Insightsin tallentamaa dataa taulukkomuodossa.

Datan visualisointi Time Series Insightsissa on suhteellisen yksinkertaista. Kuvassa 25 on ote visualisoidusta datasta.



Kuva 25. mbEDGen lähettämä mittausdata kuvaajana Time Series Insightsissa.

## 5 Yhteenveto

Simulaatiokokeen perusteella mbEDGE soveltuu hyvin perustaksi IIoT-sovellusten rakentamiseen. Yhdessä Red Lion DA30D:n tai muiden protokollamuuntimien kanssa sen avulla saadaan eri aikakausien automaatiolaitteita kytkettyä helposti samaan järjestelmään ja tekemään niiden keräämällä datalla moderneihin sovelluksiin tarvittavia toimenpiteitä. Tämä kokonaisuus tarjoaa helposti pystytettävän ja skaalautuvan järjestelmän kaikenkokoisia IIoT-sovelluksia varten.

Laitteiden ohjelmointi on vaivatonta eikä vaadi juurikaan erityistä tietoteknistä osaamista. Ohjelmointiin tarjotut työkalut on suunniteltu automaatioinsinöörin käyttöön, joten kokemus perinteisten automaatiolaitteiden parissa riittää hyvin niiden hallintaan.

mbEDGE:n vapaat Docker-säiliöt laajentavat sen käytettävyyttä entisestään. Reitittimen suorituskyvyn rajoissa niihin voidaan asentaa sovelluksia hyvin erilaisiin tarpeisiin, joko valmiista tarjonnasta tai itse ohjelmoituina. Tulevissa reititinversiossa laitteiden suorituskykyä parannetaan nykyisestä, jolloin myös laajennusmahdollisuudet paranevat.

MB Connect Linen laitteiden tietoturva ajantasainen ja kattava, ja sen perusteella niiden valinta IIoT-sovelluksiin voidaan tehdä luottavaisin mielin ajankohtaisiin tietoturvalle asetettuihin määräyksiin perustuen.

Yhdistämällä perinteisen automaatioverkon laitteita IoT-reunayhdyskäytävän avulla pilvipalveluihin saadaan niitä hyödynnettyä aivan uudella tavalla. Näin myös melko vanhoillekin automaatiolaitteille voidaan löytää uutta käyttöä modernissa tietoverkossa.

Työ oli kokonaisuudessaan mielenkiintoinen ja opetti paljon Sarlinin edustamien laitteiden toiminnasta kuten myös Azuren ominaisuuksista. Työ edistää helposti toteutettavien ja tietoturvallisten IIoT-pohjaisten sovellusten tarjoamista suomalaisten yritysten eri tarpeisiin uusien liiketoimintamahdollisuuksien kehittämiseksi ja kilpailukykyyn parantamiseksi.

## Lähteet

- 1 Kayla Matthews, 2019. The IIoT, Its Challenges And Why It's Important (blogikirjoitus) <<https://blog.robotiq.com/the-iiot-its-challenges-and-why-its-important>> (luettu 17.7.2020).
- 2 Sarlin Oy Ab (verkkoaineisto) <<https://www.sarlin.com/tietoa-sarlinista/>> (luettu 18.7.2020).
- 3 Sarlin Balance (verkkoaineisto) <<https://www.sarlinbalance.com/solutions/>> (luettu 18.7.2020).
- 4 Kent Mundle. Home Smart IoT Home: Domesticating the Internet of Things (verkkoaineisto) <<https://www.toptal.com/designers/interactive/smart-home-domestic-internet-of-things>> (luettu 5.12.2019).
- 5 Helsingin Sanomat, 29.10.2017. Esineiden internet on rikki, ja siellä leviää taas uusi kiusa – saastuneilla laitteilla tehty hyökkäys voisi lamauttaa nettiliikenteen (Artikkeli) <<https://www.hs.fi/teknologia/art-2000005428462.html>> (luettu 31.12.2019).
- 6 Taneli Tikka, 2015. Teollinen internet – mikä se on? (blogikirjoitus) <<https://www.tivi.fi/kumppaniblogit/tieto/teollinen-internet-mika-se-on/7527cb6f-715b-314e-b5ed-420e57214b54>> (luettu 5.12.2019).
- 7 Dick Caro, 2016. Automation Network Selection: A Reference Manual.
- 8 Verwer Training and Consultancy Ltd., 2020. Tutorial – Introduction to Fieldbus (verkkoaineisto) <<http://verwertraining.com/tutorials/tutorial-introduction-to-fieldbus-and-profibus/>> (luettu 1.6.2020).
- 9 Seppo Pyyskänen, 2013. Teollisuuden automaatio- ja ohjausjärjestelmät – Standardien valinta ja käyttö (verkkokirja) <<https://www.automatioseura.fi/site/assets/files/1367/standardikirja.pdf>> (luettu 27.12.2019).
- 10 Seppo Tiilikainen, Jukka Manner, 2013. Suomen automaatioverkkojen haavoittuvuus – Raportti Internetissä julkisesti avoimista automaatiolaitteista (raportti) Aalto-yliopisto, Sähkötekniikan korkeakoulu.
- 11 Open Automation Software. What is an IoT Gateway? (verkkoaineisto) <<https://openautomationsoftware.com/blog/what-is-an-iiot-gateway/>> (luettu 31.12.2019).
- 12 iotbyhvm.ooo. IoT Gateway (verkkoaineisto) <<https://iotbyhvm.ooo/iiot-gateway/>> (luettu 8.1.2020).

- 13 Telia Inmics-Nebula, 2018. Pilven monet kasvot – IaaS, PaaS ja SaaS (verkkoaineisto) <<https://www.inmicsnebula.fi/fi/blogi/pilven-monet-kasvot-iaas-paas-ja-saas>> (luettu 9.11.2019).
- 14 Heidi Eronen, 2016. IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi (blogikirjoitus) <<https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/>> (luettu 16.7.2020).
- 15 The HiveMQ Team, 2015. Publish & Subscribe - MQTT Essentials: Part 2 (verkkoaineisto) <<https://www.hivemq.com/blog/mqtt-essentials-part2-publish-subscribe/>> (luettu 18.5.2020).
- 16 The HiveMQ Team, 2019. Getting Started with MQTT (verkkoaineisto) <<https://www.hivemq.com/blog/how-to-get-started-with-mqtt/>> (luettu 1.6.2020).
- 17 MDN Web Docs, 2020. Working with JSON (verkkotutoriaali) <<https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Objects/JSON>> (luettu 17.7.2020).
- 18 TechDesign, 2017. Get Started with IoT Visual Wiring Tool – Node-RED (verkkoaineisto) <<https://blog.techdesign.com/get-started-with-iot-visual-wiring-tool-node-red/>> (luettu 9.11.2019).
- 19 Red Alert Labs, 2018. Industrial IoT: Security Challenges and Expectations (blogikirjoitus) <<https://www.redalertlabs.com/blog/industrial-iot-security-challenges-and-expectations>> (luettu 1.6.2020).
- 20 mbEDGE – Your IoT Upgrade for Remote Access (verkkoaineisto) <<https://www.mbconnectline.com/en/products/mbedge.html>> (luettu 31.12.2019).
- 21 github.com. portainer.io (verkkoaineisto) <<https://github.com/portainer/portainer>> (luettu 1.6.2020).
- 22 Red Lion. DA30D High Performance Protocol Converter and Data Acquisition System with Data Logger, Web Server and Virtual HMI (verkkoaineisto) <<https://www.redlion.net/product/da30d-high-performance-protocol-converter-and-data-acquisition-system-data-logger-web-server>> (luettu 10.8.2020).
- 23 Microsoft, 2019. What is Azure IoT Hub? (verkkoaineisto) <<https://docs.microsoft.com/en-us/azure/iot-hub/about-iot-hub>> (luettu 15.6.2020).
- 24 node-red-contrib-azure-iot-hub (verkkoaineisto) <<https://www.npmjs.com/package/node-red-contrib-azure-iot-hub>> (luettu 29.5.2020).
- 25 National Control Instruments, 2019. Using Node-RED to Send Sensor Data to Azure (verkkoaineisto) <<https://ncd.io/using-node-red-to-send-sensor-data-to-azure/>> (luettu 29.5.2020).

- 26 Microsoft, 2020. What is Azure Time Series Insights Gen1? (verkkoaineisto) <<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-overview>> (luettu 23.7.2020).