



VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Johanna Kauppi

SIEMENS MINDSPHEREN VERTAILU
MUIHIN IOT-PALVELUIHIN VEO OY:
LLE

Tekniikka
2019

TIIVISTELMÄ

Tekijä	Johanna Kauppi
Opinnäytetyön nimi	Siemens MindSpheren vertailu muihin IoT-palveluihin VEO Oy:lle
Vuosi	2019
Kieli	suomi
Sivumäärä	37
Ohjaaja	Timo Kankaanpää

Insinöörityön tarkoituksena on saada kokonaiskuva Siemensin MindSpheren toiminnasta. Tutkitaan mitä hyötyä MindSpherestä on VEO:lle sekä minkälaista lisäarvoa VEO voisi sen avulla tarjota asiakkailleen. Työssä tullaan vertaamaan erilaisia IoT-ratkaisuja sekä rakentamaan testausympäristö MindSpheren avulla. Koska asiakkaan data on pysyttävä turvassa eri tilanteissa, kyberturvallisuutta käsitellään työssä soveltuvien osien.

IoT-palveluiden vertailu suoritettiin työpöytävertailuna eri valmistajien liitännäismahdollisuuksista sekä millä eri teknologioilla pilvipalvelu liittyy prosessiin, esimerkiksi Profibus, OPC DA ja OPC UA. Tietoja kerättiin pääosin valmistajien kotisivuilta sekä esitteistä. Vertailtavaia IoT-valmistajia olivat Wapice IOT-ticket, Digi Connect Sensor+, Tosibox sekä Secomea. Siemens MindSphereen perehdyttiin syvällisemmin myös Siemensin järjestämässä koulutuksessa. Tutkimusosiossa tehtiin proto, jonka avulla voidaan testata, miten valitut toiminnot toimivat. Siemens MindConnect Nano liitettiin Simatic S7-1500:een, mittausta varten luotiin TIA 15:sta kuvan erilaisia lämpötilanmittaus lohkoja. Arvoja muuttamalla Fleet managerin käyriin saatiin muutoksia aikaan.

Vertailun perusteella selvisi, että IoT-laitteiden ja -valmistajien välillä on runsaasti samankaltaisuuksia, mutta myöskin eroja löytyy hyvin paljon. Käyttäjä löytää varmasti tarpeilleen sopivan laitteen, mutta vaivannäköä se vaatii. Laittevalmistajan valintatilanteessa kannattaakin testata ja tutustua useampiin merkkeihin ja malleihin, että tietää mikä on omaan käyttöön sopivin.

Lukuisien vastoinkäymisten jälkeen dataa saatiin näkyviin vaikkakaan ei sieltä alun perin oli tarkoitus. Mielestäni MindSpheressä samoja asioita lisättiin turhan moniin paikkoihin, ennen kuin tietoa saatiin siirrettyä. Ajanpuutteen vuoksi datan jatkokäsittely sekä yhdistäminen muualta tuotuun dataan jäi tekemättä. Mieli-kuvaani vahvisti näiden vastoinkäymisten jälkeen, että Siemens toimii parhaiten muiden Siemens laitteiden kanssa, koska muista laitteista datan keräys ei onnistunut.

ABSTRACT

Author	Johanna Kauppi
Title	Comparison of Siemens MindSphere to Other IoT Services for VEO Oy
Year	2019
Language	Finnish
Pages	37
Name of Supervisor	Timo Kankaanpää

The purpose of this Bachelor's thesis is to get an overall view of Siemens MindSphere's operations. The aim is to investigate the benefits of MindSphere to VEO and what added value VEO could offer to its customers. The thesis will compare different IoT solutions and build a testing environment with MindSphere. Because customer data must remain secure in different situations, cyber security is dealt with where applicable.

The comparison of IoT services was performed as a desktop comparison of the connectivity options of different manufacturers and with which technologies the cloud service is related to the process, for example, Profibus, OPC DA and OPC UA. Data was collected mainly from the manufacturers' websites and brochures. The IoT manufacturers compared were Wapice IOT ticket, Digi Connect Sensor +, Tosibox and Secomea. Siemens MindSphere was also more in-depth with the training organized by Siemens. In the research section, a prototype was made to test how the selected functions work. Siemens MindConnect Nano was connected to the Simatic S7-1500, with different temperature measurement blocks created from TIA 15 for measurement. Changing the values on the Fleet Manager curves resulted in changes.

The comparison found that IoT has a lot of similarities between devices and manufacturers, but there are also a lot of differences. The user will certainly find a device that suits their needs, but it requires effort. When choosing a device manufacturer, it is advisable to test and get acquainted with more brands and models to know what is most suitable for the purpose.

After problems, the data was displayed although not from where it was originally intended. The conclusion is that the same things were added to many places in MindSphere before the information was transferred. Due to the lack of time, further processing of the data and connection to the data imported from elsewhere was not done. After these adversities, it is fair to say that Siemens works best with other Siemens devices, because data collection from other devices failed.

Keywords	cloud, IoT, Siemens and MindSphere
----------	------------------------------------

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVALUETTELO

LYHENTEET

1	JOHDANTO.....	8
1.1	Työn tavoitteet.....	8
1.2	Työn rakenne.....	8
1.3	Teollinen internet.....	9
1.4	IoT (Internet of Things).....	9
1.5	VEO.....	10
2	SIEMENS MINDSPHERE.....	11
2.1	Pilvipalvelu.....	11
2.2	Yhteydet.....	12
2.3	Laitteet.....	12
2.3.1	MindConnect Nano.....	13
2.3.2	MindConnet IoT2040.....	14
2.3.3	MindSphere AWS MindConnect API.....	14
2.3.4	MindSphere AWS MindConnect LIB.....	15
2.3.5	MindSphere AWS MindConnect IoT Extension.....	15
3	VERTAILU.....	16
3.1	IoT Ticket.....	16
3.1.1	Yhteydet.....	17
3.1.2	Tietoturva.....	17
3.1.3	Ohjelmointi.....	17
3.1.4	Laitteet.....	17
3.2	Digi Connect Sensor+.....	18
3.2.1	Ohjelmat ja sovellukset.....	18
3.2.2	Liitännät.....	19
3.3	Tosibox.....	20
3.3.1	Lock 100.....	20
3.3.2	Lock 200.....	21

3.3.3	Lock 500	22
3.4	Secomea	22
3.4.1	Secomea LinkManager	23
3.4.2	Secomea GateManager	23
3.4.3	Secomea SiteManager	23
3.4.4	Etäyhteys Siemens S7 -logiikkaan	24
3.4.5	Yhteystavat	24
4	TIETOTURVA	25
4.1	Teollisuuden tietoturva	25
4.2	VEO	26
4.3	Siemens Mindsphere	28
4.3.1	Yhdistämisvaihe	28
5	TESTAUS	30
5.1	Käyttäjätili	30
5.2	Laitteen käyttöönotto	30
5.3	Fleet Manager	35
6	LOPPUPÄÄTELMÄT	36
	LÄHTEET	37

KUVALUETTELO

Kuva 1.	MindConnect Nano	s.10
Kuva 2.	MindConnect IoT2040	s.11
Kuva 3.	IoT-Ticket	s.13
Kuva 4.	Wapice WRM 247+	s.15
Kuva 5.	Digi Connect Sensor+	s.16
Kuva 6.	Älykäs avain	s.17
Kuva 7.	Lock 100	s.17
Kuva 8.	Lock 200	s.18
Kuva 9.	Lock 500	s.19
Kuva 10.	Secomea	s.19
Kuva 11.	USB-tikun liittäminen Nanoon	s.27
Kuva 12.	MindSphere Launchpad	s.27
Kuva 13.	Mittapisteiden luoti	s.28
Kuva 14.	Asetukset	s.28
Kuva 15.	Datamappings	s.29
Kuva 16.	Tia 15	s.30
Kuva 17.	Fleet Manager	s.31

LYHENTEET

IaaS	Infrastructure as a Service, web-pohjainen hallintaliittymä
IoT	Internet of Things, teollinen internet
OPC DA	Open process control data access, avoin prosessiohjaustietojen käyttö
OPC UA	Open process control unified architecture, avoin prosessiohjaus, yhtenäinen arkkitehtuuri
PaaS	Platform as a Service, avoin ohjelmistoalusta
SaaS	Software as a Service, pilvessä sijaitseva ohjelmisto

1 JOHDANTO

MindSphere on Siemensin pilvipohjainen avoin IoT-käyttäjärjestelmä, joka yhdistää koneita ja laitteita digitaaliseen maailmaan ja mahdollistaa tehokkaat teolliset sovellukset ja digitaaliset palvelut liiketoiminnan menestymiseen. Pilvipalvelu auttaa hyödyntämään koneiden sisältämää dataa, jonka avulla voidaan optimoida tuotantoa, vähentää tuotannon keskeytyksiä sekä varmistaa parhaan mahdollisen käytettävyyden.

Työssä tullaan vertaamaan erilaisia IoT-ratkaisuja, rakentamaan testausympäristö sekä tutkimaan kerättyä dataa. Selvitetään, miten onnistuu muualta tuodun datan yhdistäminen MindSpheren datan kanssa. Koska asiakkaan data on pysyvä turvassa eri tilanteissa, kyberturvallisuutta käsitellään työssä soveltuvin osin. Näiden jälkeen testataan kuinka palvelu toimii käytännössä.

1.1 Työn tavoitteet

Insinööritöiden tarkoituksena on saada kokonaiskuva Siemensin MindSpheren toiminnasta. Tutkitaan mitä hyötyä MindSpherestä on VEO:lle sekä minkälaista lisäarvoa VEO voisi sen avulla tarjota asiakkailleen.

Tavoitteena on muun muassa tehdä työpöytävertailua eri IoT-teknologioiden liittä-mähdollisuuksista, dokumentoida millä teknologioilla pilvipalvelu liittyy prosessiin, esimerkiksi Profibus, OPC DA ja OPC UA. Yhtenä osana työtä suoritetaan vertailua muiden valmistajien välillä muun muassa Wapice IOT-ticket, Digi Connect Sensor+, Tosibox sekä Secomea. Viimeisenä tullaan tekemään proto, jonka avulla voidaan testata, miten valitut toiminnot toimivat.

1.2 Työn rakenne

Luvussa yksi käsitellään työn taustaa ja tavoitteita sekä esitellään yritys, johon työ on tehty. Luvussa kaksi kerrotaan Siemens MindSpherestä tarkemmin sekä siihen

liittyvistä palveluista ja laitteista. Luvussa kolme tutustutaan valittuihin IoT-alustoihin. Alustoista tutkitaan eri ominaisuuksia, kuten yhteyksiä, tietoturvaa, tietokantamahdollisuuksia, ohjelmointia sekä laitteita. Luvussa neljä käsitellään IoT-palveluita tietoturvan näkökulmasta. Luvussa viisi käsitellään simulaatiotestauksen tuloksia. Luvussa kuusi on yhteenveto tehdystä työstä ja tuloksista.

1.3 Teollinen internet

Internet Of Thingsillä eli teollisella internetillä tarkoitetaan erilaisia laitteita ja järjestelmiä, jotka voidaan yhdistää toisiinsa tiedonkeruu tarkoituksessa. Laitteet ovat yhdistettävissä internetiin tai toisiinsa. Teollisen internetin avulla pyritään parantamaan tuotantoprosesseja ja tehostamaan liiketoimintaa. Tavoitteena on mahdollistaa esimerkiksi yrityksille etähallintaa, lisätä ennakoitavuutta sekä autonomisuutta. IoT laitteet tuottavat dataa, jota yritykset pyrkivät toiminnassaan hyödyntämään. (Collin 2016, 25–27.)

Yritykset hyötyvät laitteiden keräämästä datasta, koska tällöin tietoa pystytään analysoimaan paremmin ja seuraamaan esimerkiksi huoltojen tarvetta. (Plattonen 2015.) Koska internet on saatavilla lähes joka paikassa ja anturit kehittyvät toiminnallisesti, datan tallennus helpottuu. Tallennus on helppoa myös siitä syystä, että iso määrä tietoa mahtuu todella pieneen fyysiseen kokoon. (Collin 2016, 35.)

1.4 IoT (Internet of Things)

Internet of Things, eli esineiden internetillä tarkoitetaan verkon laajentumista laitteisiin, jotka eivät ole aiemmin olleet yhteydessä internetiin. Laitteet yhdistetään internetiin lisäämällä niihin verkkoyhteys ja antureita. Antureiden ja verkkoyhteyden avulla laite voi kerätä tietoa laitteen käytöstä tai laitteen ympärillä olevasta ilmastosta ja lähettää kerätty tieto verkkoyhteyden avulla, esimerkiksi pilvipalveluun tai muihin laitteisiin. (Taanila, 2016)

Kerättyä tietoa voidaan analysoida eri tarkoituksiin. Analysointi voi tapahtua esimerkiksi internetistä selaimen avulla, jonka avulla pääsee käsiksi web-sovellukseen, johon laite on kytketty, tai sovellus voi itse analysoida datan ja erinäisten laskelmien avulla päätellä esimerkiksi laitteen huollon tarvetta. (Taanila, 2016)

1.5 VEO

Vaasa Engineering Oy perustettiin itsenäisyyspäivänä 6. joulukuuta 1989. Perustajina olivat Harri Niemelä ja Mauri Holma. Vaasa Engineering Oy oli ensimmäinen energiateknologiyritys Runsorissa Vaasassa. Vaasa Engineering nimestä luovuttiin vuonna 2012, kun tytäryhtiöt Vaasa Kojeistot, joka vastaa suur- ja pienjännitekojeistojen sekä moottorikeskusten kokoonpanosta sekä Vaasa Service, joka on erikoistunut automaatio- ja sähköistysjärjestelmien asennukseen ja kunnossapitoon, fuusioitiin emoyhtiöön, jolloin VEO virallistettiin yhtiön uudeksi nimeksi. (Sippola, 2017, 96–97, 109)

VEOn palveluksessa on noin 340 työntekijää ja vuoden 2016 liikevaihto oli 75,6 miljoonaa euroa. Päätoimipiste on Vaasassa, jossa tuotanto myös sijaitsee. Lisäksi muita toimipaikkoja on Seinäjoella, Paimiossa ja Lahdessa sekä VEOlla on konttoreita eri puolilla Suomea ja sen lisäksi myyntikonttorit Norjassa, Ruotsissa ja Venäjällä. (Sippola, 2017, 124–127)

VEO tarjoaa automaatio- ja sähköistysratkaisuja energian tuotantoon, siirtoon, jakeluun ja käyttöön sekä kotimaassa että vientimarkkinoilla avaimet käteen-periaatteella. Toimituksiin kuuluu kokonaisprojekteja tai niiden osia sisältäen suunnittelun, hankinnan, projektinjohtamisen, asennukset, käyttöönoton ja koulutuksen. (Sippola, 2017)

Jakelujärjestelmiä valmistetaan lähinnä raskaan teollisuuden asiakkaille, kuten paperitehtaille ja voimalaitoksille. VEO valmistaa räätälöityjä itsenäisiä, linja- ja järjestelmäasemia vaativille teollisuus-, offshore- ja laivasovelluksille. Ilma- ja neste-mäiset jäähdytysratkaisut toteutetaan asiakkaan vaatimusten ja standardien mukaisesti. (Sippola, 2017)

2 SIEMENS MINDSPHERE

MindSphere on Siemensin pilvipohjainen avoin IoT-käyttöjärjestelmä, joka yhdistää todellisia asioita digitaaliseen maailmaan. MindSpheressä analysoitu data voidaan takaisinkytkä tuotteen ja tuotannon digitaaliseen kaksoseen, jolloin simulointi ja mallinnus voidaan toteuttaa kerätyllä datalla. Alusta on avoin, Platform as a Service (PaaS). Siemensin Mindsphere pilvipalvelu tarjoaa hallintaliittymän ja alustan lisäksi ohjelmiston, joka on muokattavissa asiakkaan tarpeiden mukaan. (Siemens 2019)

MindSphere voidaan ottaa käyttöön kolmannen osapuolen palveluntarjoajien isännöimissä julkisissa pilvissä ja tulevaisuudessa myös yksityisissä pilvissä, jotka on rakennettu yksinomaan yksittäiselle yritykselle. Asiakkaat voivat valita pilvipalvelut, jotka parhaiten vastaavat kustannuksia, valvontaa, konfiguroitavuutta, skaalautuvuutta, sijaintia ja turvallisuutta koskevia vaatimuksia. (Siemens 2019)

2.1 Pilvipalvelu

Pilvipalvelun käyttö mahdollistaa tietokoneen kapasiteetin sovelluksien tai palvelujen saatavuuden nopeasti mistä tahansa. Sovellusmalleja on neljä erilaista. Yksityinen pilvipalvelu eli Private cloud on varattu yhdelle organisaatiolle ja sitä voidaan käyttää rakennuksen sisältä tai ulkoa. Julkista pilvipalvelua eli Public cloudia voi käyttää kuka tahansa. Hybrid cloud on palvelu, joka sisältää yksityisen, julkisen ja yhteisöjen pilvipalvelun, tällöin laitteita ja ohjelmistoja voidaan käyttää yhdessä ja erikseen palveluista riippuen. Virtual private cloud eli virtuaalinen yksityinen pilvipalvelu mahdollistaa yksityisen pilvipalvelun käytön julkisessa pilvipalvelussa. (Mindsphere White Paper, 2019)

Palvelumalleista löytyy kolme vaihtoehtoa. Yksinkertaisimpana palvelunkäyttäjän näkökulmasta on Software as a Service (SaaS), joka tarjoaa kokonaisen ohjelmiston. Se sallii pääsyn ohjelmistotiedostoihin ja sovelluksiin. Malliin kuuluvat ohjelmistopäivitykset, uusimmat versiot ja lisenssit. (Mindsphere White Paper, 2019)

Platform as a Service (PaaS) on avoin ohjelmistoalusta, joka sallii mukautuvan ympäristön uusien sovellusten kehittämiseen ja tuottamiseen. Käyttäjän vastuulla on sovelluksen tietoturvasta ja päivityksistä huolehtiminen. (Mindsphere White Paper, 2019)

Infrastructure as a Service (IaaS) on web-pohjainen hallintaliittymä, joka sallii pääsyn virtuaaliseen tietojenkäsittelyyn, kuten tietoverkkoihin tai muistipaikkoihin. Asiakas voi tällä alustalla luoda omia palvelimia ja hallinnoida niitä. Palvelunkäyttäjältä tämä alusta vaatii eniten hallinnointia ja palvelimien hoitoa. Tämä soveltuu niille yrityksille, joilla on oma IT-osasto tai muuten osaavaa henkilökuntaa. (Mindsphere White Paper, 2019)

2.2 Yhteydet

Yhteys voidaan muodostaa MindSphereen joko yhdyskäytävälaitteella tai ohjelmistokirjaston avulla. Yhdyskäytävälaitteita ovat Mindconnect Nano ja IoT2040. Siemens S7 -logiikoille on kehitetty myös oma kirjastonsa Mindconnect-FB, joka mahdollistaa suoran yhteyden MindSphereen ilman yhdyskäytävälaitetta. Saatavilla on myös Mindconnect LIB -lähdekoodi, jonka avulla kehittäjät voivat yhdistää oman ohjelmistonsa MindSphereen. (MindSphere White Paper 2019)

Mindconnect Nano sekä IoT2040 käyttävät HTTPS-protokollaa portin 443 kautta yhdistääkseen MindSphereen. Nanossa ja IoT2040-laitteessa ei ole yhtään porttia auki sisään tulevalle liikenteelle, vaan ne tekevät ainoastaan yhteyspyynnön MindSphereen. Molemmat laitteet keräävät dataa käyttämällä OPC UA -protokollaa tai keräävät tarvittavan tiedon suoraan Siemensin ohjelmoitavalta logiikalta (MindConnect Nano Datasheet 2018).

2.3 Laitteet

Asiakas voi ajaa Mindsphere-sovelluksia muun muassa Amazon Web Service-, Microsoft Azure-, SAP Cloud Platform- ja Atos Canopy -pilvipalveluissa. OPC UA – standardin takia, MindSphereen voidaan liittää muitakin kuin Siemensin laitteita.

Siemensin laitteiden yhdistäminen onnistuu asettamalla Nanon asetuksiin PLC:n IP-osoite sekä halutut muistipaikat. Mindconnect-ohjelmisto sallii lähes kaikkien laitteiden yhdistämisen MindSphereen erilaisten laajennuksien avulla. Järjestelmän avulla käyttäjät voivat pilvipalvelussa kehittää, luoda ja käyttää omia ja muiden toteuttamia palveluita. MindAppien luominen ja kehittäminen onnistuvat pilvipalvelussa. (Mindsphere White Paper 2019)

2.3.1 MindConnect Nano

MindConnect Nano on teollisuustietokone tietojen keräämiseen eri protokollilla ja tietojen siirtämiseen MindSphere-laitteeseen (**Kuva 1.**). Laite tukee tiedonsiirtoa turvallisen Internet-yhteyden kautta pilvipohjaisten sovellusten ja palvelujen mahdollistamiseksi. Käyttölämpötila voi olla 0 °C – 60 °C. Sinetöity metallikotelo kestää hyvin ankarissakin olosuhteissa. Kotelo ehkäisee myös tärinää sekä iskuja. (MindConnect Nano Datasheet 2018).



Kuva 1. MindConnect Nano

MindConnect Nanon hyötyjä ovat muun muassa nopea ja helppo teollisuuskoneiden ja automaatiojärjestelmien liitettävyyys MindSphere-järjestelmään sekä se, että tiedonkeruu onnistuu tavanomaisilla teollisuusprotokollilla. Ohjelmistopäivitysten hallinta on helppo, rakenne kestävä ja huoltovapaa. Laite sisältää enintään 500 Mt:n paikallisen datapuskurin, eli jos internetyhteys katkeaa, Nano aloittaa datan varastoimisen sisäänrakennettuun puskuriin. Yhteyden palaututtua Nano lähettää

puskuroidun datan MindSphereen. Tietojen käsittelyjakso laitteella on enintään 250 datapistettä / sekunti sekä tiedonsiirtosykli 10 sekunnin välein. (MindConnect Nano Datasheet 2018).

Käytettäviä protokollia ovat Siemens S7 (tietojen keräämiseen S7-3xx / S7-4xx / ET-200s PLC: ltä), OPC UA (tietojen keräämiseksi kaikista tietolähteistä, jotka voivat toimittaa tietoja OPC UA -palvelimen kautta); MindSphere Nano tukee dataa OPC UA -määrityksen (Data Access) 8 osan kanssa (MindConnect Nano Datasheet 2018).

2.3.2 MindConnet IoT2040

MindConnect IoT2040 on laite tietojen keräämiseksi eri protokollilla ja tietojen siirtäminen MindSphere-laitteeseen (**Kuva 2.**). Laite tukee tiedonsiirtoa turvallisen Internetyhteyden kautta pilvipohjaisten sovellusten ja palvelujen mahdollistamiseksi. Muuten hyvin samanlainen laite kuin Nano, erona tietojen käsittelyjakso: Enintään 30 datapistettä / sekunti sekä tiedonsiirtosykli: 10 sekunnin välein. (Siemens 2019)



Kuva 2. MindConnect IoT2040

2.3.3 MindSphere AWS MindConnect API

MindConnect API on palomuuriystävällinen RESTful-sovellusliittymä, jonka avulla voi muodostaa yhteyden MindSphere-laitteeseen ilman erillistä laitteistoa tai

ohjelmistoa. Se tukee agentin käyttöönottoa, turvallista Internet-yhteyttä salatulla tiedostojen siirrolla, tapahtumia, aikasarjoja tai mukautettuja tietoja MindSphereille. Se mahdollistaa pilvipohjaiset sovellukset ja palvelut. API mahdollistaa yhteyden lähes jokaiseen laitteeseen sekä palomuuuriystävällisen viestinnän RESTfull API:n kautta. Turvallinen yhteys paikallisesta laitteesta MindSphere-alustalle, suojausprofiilit voidaan valita jaetusta salaisuudesta tai RSA3072: sta. Tietolähteen konfigurointi kenttätasolta mahdollista aikasarjaa varten. (Siemens 2019)

2.3.4 MindSphere AWS MindConnect LIB

MindConnect Lib on C-lähdekoodikirjasto, jonka avulla voi käyttää MindSphere-yhteyksiä omien agenttinsa kanssa, esim. sulautettuja laitteita, ohjelmoitavia ohjaimia tai Linux-/ Windows-tietokoneita. Se kapseloi MindConnect API:n näihin laitteisiin ja käsittelee salatun paikan päällä olevien tietojen siirtämisen MindSphere-verkkoon turvallisen internet-yhteyden kautta, jotta pilvipohjaiset sovellukset ja palvelut voidaan ottaa käyttöön. Tietojen käsittelyjakso alustavan laitteen suorituskyvystä riippuen voi olla enintään 250 datapistettä / sekunti. Tiedon siirtosykli on 10 sekunnin välein. (Siemens 2019)

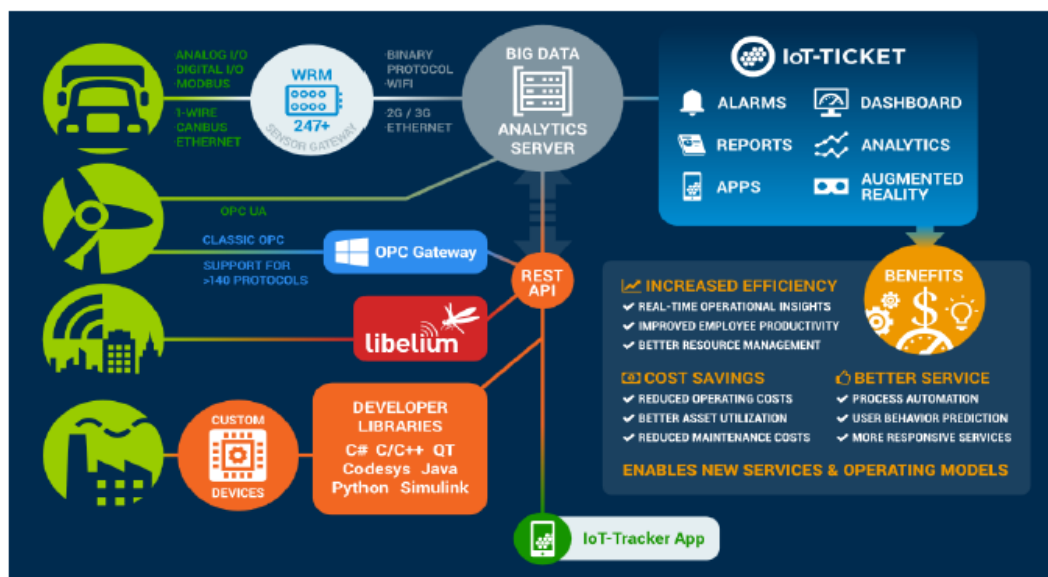
2.3.5 MindSphere AWS MindConnect IoT Extension

MindConnect IoT Extension on liitântäkerros, joka laajentaa protokollien määrää, jotka voivat kommunikoida suoraan MindSpheren kanssa. Erilaisia kenttäväyläprotokollia tuetaan yhdessä lisääntyneen laitteistoyhteysagenttien valikoiman kanssa, jotka luovat suoran yhteyden varoihin tuotantoympäristössä. MindConnect IoT Extension on mukana MindAccess IoT -arvosuunnitelmassa ja kehittäjäsuunnitelmassa, jossa on päivityksiä, jotka mahdollistavat tiedonsiirron lisäämisen ratkaisuvaatimusten perusteella. (Siemens 2019)

3 VERTAILU

3.1 IoT Ticket

IoT-Ticket on alusta joka kattaa datan keruun, raportoinnin, web-käyttöliittymän ja analytiikan. Alusta tukee valvottua seuranta, etähallintaa, automatisointia ja edistysellistä raportointia (**Kuva 3.**). IoT-Ticket on liitettävissä Matlab+ Simulink-ohjelmointiympäristöön ja se tukee myös mm. OPC-UA-, Modbus-, Ethernet- ja Can-protokollia. Laitteita voidaan myös etäohjata IoT-Ticketin avulla. (IoT-Ticket 2019)



Kuva 3. IoT-Ticket

IoT-Ticketin Dashboard on verkkopohjainen käyttöliittymä, jolla käyttäjä voi olla turvatussa yhteydessä etälaitteisiin, esimerkiksi tarkistamalla niiden tilan, selaamalla raportteja tai pyytäen lisätietoja sen hetkisestä toimintatehokkuudesta. Interface Desingnerin avulla voi luoda uusia elementtejä, lisätä kuvia, mittareita, painikkeita, taulukoita suoraan Dashboardiin (IoT-Ticket 2019).

Raporttien luominen tapahtuu raporttisovelluksessa. IoT-Ticketissä raportit voidaan luoda verkkoselaimessa ja niiden sisältö voi olla sekä dynaamista että staattista (IoT-Ticket 2019).

3.1.1 Yhteydet

IoT-Ticketin yhdistäminen on mahdollista käyttäen Wapicen tarjoamia REST-rajapintoja. Rajapintoja käyttämällä on mahdollista luoda laitteita, poistaa, lukea sekä kirjoittaa. Saatavana on myös laiteratkaisu, jonka ansiosta laitteen liittäminen on mahdollista ilman API-rajapinnan käyttöä. Wapice tarjoaa myös yli 140 protokollaa yhdistämiseen. Mukana on ohjelmoitavia logiikoita sekä yleisimpiä teollisuuden protokollia, muun muassa OPC UA. (IoT-Ticket)

3.1.2 Tietoturva

Kaikki pyynnöt tehdään HTTPS-protokollaa käyttäen, joten se on suojattu wiretappingiltä sekä man-in-the-middle-hyökkäyksiltä. Datan lähettäminen suojataan basic HTTP -suojauksella. (IoT-Ticket api user manual)

3.1.3 Ohjelmointi

IoT-Ticketin API on tarjolla käyttäjälle ja Wapice tarjoaa siihen esimerkkiohjelmia: C# REST Client, Java REST Client, Linux C++ Client. Käyttöliittymien ja raporttien ohjelmointi tapahtuu Web-pohjaisella Dataflow-editorilla, joka on visuaalinen ohjelmointityökalu (IoT-Ticket 2019).

3.1.4 Laitteet

Wapicella on myös oma kustomoitavissa oleva laite nimeltään WRM 247+ (**Kuva 4**). Laitetta voidaan käyttää etähallintaan, mittaukseen ja ohjaukseen. Wapice tarjoaa laitteelle myös kattavat räätälöintimahdollisuudet käsittäen PCB-suunnittelun, ohjelmistosuunnittelun sekä protokollien käyttöönoton. (IoT-Ticket alusta).



Kuva 4. Wapice WRM 247+

WRM 247+ sisältää muun muassa seuraavat moduulit, kiihtyvyys, CAN Data, ModBus Server, ISO11783 Monitor, Modbus TCP, OBD. (IoT-Ticket 2019)

3.2 Digi Connect Sensor+

Digi Connect -anturi on täysin integroitu, akkukäyttöinen solukkoväylä, jossa on I / O-liitäntä moniin ulkoisiin antureihin. Connect Sensor on suunniteltu toimimaan kestävässä teollisuusympäristöissä. Paikallisprotokollatuki mahdollistaa Connect-anturin kommunikoinnin Modbus-antureiden kanssa sekä tällöin antaa käyttäjille mahdollisuuden seurata paitsi tietojaan myös diagnosoida etäyhteyden antureidensa kuntoa. Akun kestoikä on 2-3 vuotta. Lämpötila jossa laitteistoa voi käyttää, on -35 °C – +70 °C välillä. (Digi Connect Sensor+ 2019)

3.2.1 Ohjelmat ja sovellukset

Digi Connect -anturi hyödyntää Digi Remote Manager® -ohjelmaa, jonka avulla asiakkaat, jotka seuraavat suuria määriä antureita, voivat integroida nämä tiedot helposti olemassa oleviin sovelluksiin tai käyttää kolmansien osapuolten sovelluksia (**Kuva 5.**). (Digi Connect Sensor+ 2019)

Digi Connect Sensor toimii Digi Connect Wizardin kanssa. Edellä mainittu älypuhelinsovellus on uusi innovaatio akkukäyttöiselle yhdyskäytävälle. Se antaa paikallisille asentajille, tekniikoille tai ajureille välittömästi palautetta anturin arvoista Bluetoothin kautta. Laite toimii 2G- ja 3G-verkkossa. Laite sisältää yhden standardikokoisen SIM-korttipaikan. Yhteys voidaan muodostaa myös Bluetoothin kautta. (Digi Connect Sensor+ 2019)



Kuva 5. Digi Connect Sensor+

3.2.2 Liitännät

Digi Connect Sensor+ -etäyhteysjärjestelmään on mahdollista liittää Hart 5,7- ja Modbus-liitännällä olevia antureita. Siinä on neljä analogiasisääntuloa ja kaikki ovat erikseen konfiguroitavissa 4 – 20 mA:n virtatuloksi tai 0 – 10 VDC jännitetuloksi. Tulot sisältävät 12-bittiset A/D-muuntimet (Digi Connect Sensor+ 2019).

Laitteeseen on valittavissa yksi digitaalinen I/O- tai pulssilaskurisisääntulo. Sisääntulo laitteelle voi olla jännitetietona 0 – 0.6 VDC tai 2.2 – 30 VDC. Laitteessa on yksi digitaalinen ulostulo, viisi jänniteulostuloa, 3,3 VDC, 5 VDC, 15 VDC, 24 VDC. Maksimivirta ulostulolle on 200 mA (Digi Connect Sensor+ 2019).

3.3 Tosibox

Tosibox on suomalainen tuote, jolla on mahdollista saada etäyhteys laitteiden välille. Helppokäyttöinen, laitteistopohjainen etäyhteysjärjestelmä, jolla yhteyksien luominen onnistuu muutamassa minuutissa. Tosibox on rajattomasti skaalautuva järjestelmä, mutta se ei ole pilvipalvelupohjainen ratkaisu, vaan se luo suoran VPN-yhteyden laitteiden välille.

Mikäli tietoon halutaan päästä käsiksi, tarvitaan salasana ja älykäs avain (**Kuva 6.**). Käyttäjiä ja avaimia voidaan hallinnoida yhdestä paikasta. RSA-avain liitetään tietokoneeseen USB 2.0 -liitännän avulla. Toimintalämpötila avaimelle on 0 – +70 °C ja avain sisältää yhden lisenssin. (Tosibox 2019)



Kuva 6. Älykäs avain

3.3.1 Lock 100

Tosibox Lock 100 ei tarvitse erillistä ohjelmistojen asennusta (**Kuva 7.**). Etäkäytettävät laitteet liitetään Tosiboxiin langattomasti tai verkkokaapelin avulla. (Tosibox 2019)



Kuva 7. Lock 100

3.3.2 Lock 200

Tosibox Lock 200 on etäyhteyslaite, joka on suunniteltu teolliseen käyttöön (**Kuva 8.**). Laite on vankempaa tekoa kuin Lock 100 ja se on mahdollista asentaa myös DIN-kiskoon. Etäkäytettävät laitteet liitetään Tosiboxiin langattomasti tai verkko-kaapelin avulla. (Tosibox 2019)



Kuva 8. Lock 200

3.3.3 Lock 500

Tosibox Lock 500 on tehty vaativan teollisuuden käyttötarpeita ajatellen (**Kuva 9.**). Laitteessa on mahdollisuus jopa 50 samanaikaiseen VPN-yhteyteen. Laitteen teknisiä ominaisuuksia ovat: integroitu Wifi, 2 digitaalista sisääntuloa (virtaraja 5 mA, jännite 0–32 V), 2 digitaalista ulostuloa (24 VDC, 50 mA), 24 VDC ulostulo. (Tosibox 2019)



Kuva 9. Lock 500

3.4 Secomea

Secomean järjestelmällä hallitaan etäkohteita ja – käyttäjiä. GateManager on hallintaportaali, jossa määritellään sallitut yhteydet kohteessa oleviin järjestelmiin protokolla- ja laitetasolla (**Kuva 10.**). Secomea Data Collection Module (DMC) kerää tietoja Modbus TCP- ja OPC UA -pohjaisilta laitteilta ja siirtää tiedot IoT-pilvipalveluun (Elokome 2019).



Kuva 10. Secomea

3.4.1 Secomea LinkManager

LinkManager on työasemalle asennettava etäyhteysohjelmisto. LinkManagerin avulla saadaan yhteys laitteisiin, jotka ovat käyttäjälle sallittuja. Käyttäjille voidaan määritellä oikeudet laitteen ja yhteystavan tarkkuudella. Etäkäyttäjän tunnistautuminen tapahtuu tietoturvallisesti käyttäjäkohtaisen sertifikaattitiedoston ja salasanan avulla (Elokome 2019).

3.4.2 Secomea GateManager

GateManager on etäyhteyksien ja IoT-tiedonkeruun hallintaan ja ylläpitoon tarkoitettu hallintaportaali. Hallintaportaaliin määritellään etäkohteet sekä luodaan ja hallitaan käyttäjiä. Portaaliin tallentuu loki muodostetuista yhteyksistä ja yhteydenottotavoista. GateManageria voidaan käyttää tietoturvallisena pilvipalveluna tai se on asennettavissa asiakkaan omalle palvelimelle (Elokome 2019).

3.4.3 Secomea SiteManager

SiteManager on etäkohteeseen asennettava reititinlaite. Etäyhteys kohteeseen on mahdollista 4G-mobiiliverkon tai kiinteän Internet-yhteyden kautta. SiteManageriin määriteltävät agentit määrittävät kohteessa olevan laitteen ja yhteystavan, johon etäyhteys on tarkoitus ottaa. Agenttien avulla etäyhteydet pystytään sallimaan vain haluttuihin laitteisiin, eikä koko tehdasverkkoa avata etäkäyttäjälle. (Elokome 2019)

3.4.4 Etäyhteys Siemens S7 -logiikkaan

Automaatiojärjestelmän kanssa samaan lähiverkkoon asennettavassa SiteManager-etäyhteysreitittimessä on valmiina agentti Siemens S7 -logiikoita varten. Agentti määrittelee etäyhteysasetukset ja yhteystavan, joten tietoturvallisen yhteyden muodostaminen suljetussa tehdasverkossa olevaan logiikkaan on mahdollista. Etäyhteys Siemens S7 -logiikkaan otetaan ohjelmoijan tietokoneelle asennetulla TIA- tai Step7-ohjelmalla. Koska tietokone on eri verkossa kuin logiikka, pitää tietokoneeseen asentaa Secomean LinkManager -etäyhteysohjelma. (Elokome 2019)

3.4.5 Yhteystavat

Secomea-etäyhteysjärjestelmä perustuu SiteManager-reititinlaitteeseen tai -ohjelmistoon määriteltäviin agentteihin. Agenttien käyttäminen mahdollistaa sen, että käyttäjille voidaan antaa erilaisia oikeuksia etäyhteyden muodostamiseen. Tietyille käyttäjäryhmälle voidaan antaa oikeus etäkohteessa olevien tietojen katselemiseen www-selaimella. Tietylle asiantuntijalle taas voidaan sallia Remote Desktop -yhteys palvelimeen. Jos tietokoneella ajetaan jo jotain ohjelmaa, jonka käyttöliittymää halutaan seurata, kannattaa yhteys muodostaa VNC:llä tai TeamViewerillä Secomean tietoturvallisen yhteyden kautta. (Elokome 2019)

4 TIETOTURVA

Tietoturvallisuudella tarkoitetaan tietoliikenne-, laitteisto-, ohjelmisto- ja tietoi-
neistotoiminnan turvallisuutta, joilla turvataan verkkojen ja palvelujen eheys, luot-
tamuksellisuus ja käytettävyys. Kyberturvallisuus on tietoturvan osa-alue, jolla py-
ritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. (IBM 2015.)

IoT-laitteisiin kohdistuu uhkia, kuten laitteen hallitseminen ulkopuolisen toimesta
tai tiedon varastaminen. Heikosti suunnitellut IoT-kommunikaatioverkot ja IoT-so-
velluksiin liittyvät tietoturva-aukot ovat isoja uhkia tiedon varastamisen kannalta
IoT-järjestelmissä. Tietoturva on vakavasti uhattuna, jos nämä osa-alueet järjeste-
tään huonosti. (IBM 2015.)

VPN eli virtual private network on väylä, jolla yksityinen verkko voidaan laajentaa
julkisen verkon yli ns. tunnelilla. Edellä mainitulla tunnelilla voidaan toteuttaa eri-
laisia tietokantoja tai toimintajärjestelmiä joihin vaaditaan salauksia. Tällöin pysty-
tään luomaan salattu yhteys IoT-laitteeseen ja keräämään laitteesta dataa pilvipal-
veluun analysoitavaksi turvallisesti. (Collin 2016, 56.)

Useat yhteiskunnan kriittiset toiminnot, esimerkiksi rahaliikenne, energiantuotanto
ja lennonjohto ovat riippuvaisia tietojärjestelmien ja verkkojen toimivuudesta.
Näitä toimintoja tukeviin järjestelmiin ja verkkoihin kohdistuvien häiriöiden syy
voi olla tietoturvakysymyksissä, kuten haittaohjelmissä tai vikaantuvissa laitteissa,
mutta häiriön vaikutus yhteiskunnan näkökulmasta tarkasteltuna muodostaa kyber-
turvallisuusuhkan. Olennaista kyberturvallisuusuhkien tarkastelussa on fyysisen
maailman vaikutusten tarkastelu erona tietojärjestelmävaikutuksiin. (Collin 2016,
56.)

4.1 Teollisuuden tietoturva

Nykypäivän ongelmia kyberturvallisuuden osalta on, että hakkeri saattaa murtautua
henkilön tietokoneelle, jolloin ongelmista yleensä selvittää ilman ihmisvahinkoja,

mutta tilanne muuttuu, kun rikollinen löytää tiensä auton tai voimalaitoksen järjestelmiin. Escrypt GmbH:n Key Account Manager Claus Jürgen Dobler vastasi kyberturvallisuutta koskeviin kysymyksiin Bosch Connected World -tapahtumassa toukokuussa 2019. Hänen mukaansa auton hakkerointi on nykypäivänä melko epätodennäköistä, mutta mahdollista esimerkiksi varastamistarkoituksessa. Kyberhyökkäykset teollisuuslaitoksia vastaan lisääntyvät ja saavat uusia muotoja. Hyökkäyksiltä ei vältty myöskään laivaliikenne (Hakala 2019).

Deloitte Cyber Secure Manufacturing in 2021 tutkimuksen mukaan kyberturvauhat lisääntyvät valmistavassa teollisuudessa. Tutkimuksessa selviää myös, että suomalaiset teollisuusyritykset arvioivat lähivuosien suurimmiksi kyberturvauhiksi esineiden internetiin (IoT) ja teollisuuden digitalisaatioon liittyvät riskit (Tero Mellin, Deloitte). Viestintäviraston 2018 vuoden tietoturvanäkymissä IoT-laitteet listataan sijalle kaksi, koska tietoturvattomat verkkoon kytketyt IoT-laitteet toimivat heikosti. Verkkoon jääneitä käyttämättömiä laitteita saatetaan kaapata haittakäyttöä varten. (Viestintävirasto 2019)

Viestintäviraston tutkimuksen mukaan keväällä 2017 suomalaisista verkoista löytyy lukuisia suojaamattomia automaatiolaitteita. Tarkastelun kohteena ovat olleet erityisesti teollisuusautomaatioon, kriittiseen infrastruktuuriin ja rakennusautomaatioon liittyvät järjestelmät (Viestintävirasto 2019).

4.2 VEO

Kyberhyökkäykset aiheuttavat merkittävän riskin voimalaitoksen kriittiselle infrastruktuurille sekä sähköjakelujärjestelmille ja teollisuudelle. Veon asiantuntijat pystyvät torjumaan näitä riskejä monella tavalla ja monella tasolla. Kaikki toimet perustuvat alustavaan raporttiin, joka sisältää yksityiskohtaisen kartoituksen asiakkaan nykyisestä suojaustilasta. Se on eräänlainen järjestelmän terveystarkastus, joka osoittaa, missä heikko osa on, ja mitä muutoksia tai parannuksia pitäisi tehdä näiden heikkouksien korjaamiseksi. (Veo 2019)

Veon tietoverkkoturvapalvelujen laajuus voi tarkoittaa esimerkiksi asetusten muuttamista tai mahdollisesti vanhojen laitteiden päivittämistä. Palveluihin voi sisältyä myös turvallisuuskoulutus ja – neuvonta. Veon asiantuntijapalvelut voivat tarjota myös nimetyn kyberturvallisuusasiantuntijan, joka on asiakkaan palveluksessa sovittun ajan. Tämä henkilö voi toimia kyberturvallisuusasiantuntijana asiakkaan puolesta ja olla vastuussa kaikista kyberturvallisuuteen liittyvistä asioista, esim. suojella etujasi kehitys- ja toimitusprojekteissa, arvioida tavarantoimittajien kyberturvallisuusosaamista ja auttaa määrittämään kyberturvallisuuteen liittyvät velvollisuudet sekä sisäisesti että tavarantoimittajien kanssa. (Veo 2019)

Veon etäkäyttö- ja neuvontapalvelut ovat nopein ja kustannustehokkain tapa saada apua odottamattomassa kunnossapidossa ja seurannassa. Turvallisen yhteyden kautta asiantuntijat voivat käyttää laitoksen sähköistys- ja automaatiojärjestelmiä maantieteellisestä sijainnista riippumatta. Palvelua voidaan käyttää joko maksamalla kuukausimaksun sekä palvelusta että etäkäyttölaitteista tai mahdollisuuksien mukaan käyttämällä laitoksen nykyistä etäkäyttöoikeutta. (Veo 2019)

Nykyään paljon enemmän voidaan tehdä etäkäytön kautta: vian havaitseminen, tietojen lataaminen vian analysointiin, valvontaan ja automaatiojärjestelmien muutoksiin sekä suojausreleen säätöihin. Myös kaikki tarvittavat hotfix-korjaukset, kuten järjestelmäpäivitykset, versiopäivitykset sekä ohjausasemien tietoturvapäivitykset tehdään nopeasti ja sujuvasti. (Veo 2019)

VPN-yhteyden ohjaamisen lisäksi muita järjestelmän etuja ovat muun muassa:

- luotettavat ja salatut kanavat, joissa käytetään IPSEC- ja SSL-VPN-protokollia
- asiakkaan VPN-kirjautumisprosessi, jossa käytetään vahvaa todennusta
- modernit palomuurit
- SSL VPN -portaali, jossa käytetään vahvaa todennusta

- tunnistusominaisuudet: NGFW-palomuurien tuottamat syslog-tiedot käsitellään koneen oppimisen poikkeaman havaitsemisella

Korkean ja jatkuvan tietoturvatason varmistamiseksi etäkäyttötoiminnot testataan säännöllisin väliajoin ja laitteet pidetään ajan tasalla. (Veo 2019)

4.3 Siemens Mindsphere

MindSphere-asiakas on tietojen omistaja ja valvoo valtuutustasoja. MindSphere tarjoaa erittäin turvallisen tietojenkäsittelyympäristön, joka mahdollistaa datan omistajan suorittavan täyden valvonnan tiedonsiirron todentamistasoilla. Tiedot tallennetaan erittäin turvallisiin infrastruktuureihin, joita johtavat pilvitietokeskuspartnerit (IaaS) tarjoavat. Nämä ammattimaiset IaaS-palveluntarjoajat voivat tarjota paljon korkeampia tietoturvamalleja kuin tavallisessa paikassa ja paikallisessa tietovarastossa. Lisäksi tiedonsiirto-oikeuksia hallitaan tiukasti erillisten vuokralaisten kautta, mikä teknisesti sallii vain tietojen käyttöoikeuden vuokralaisen (tiedon omistajan) osoittamalle omistajalle. (Siemens 2019)

4.3.1 Yhdistämisvaihe

MindSphere yhdistetään Mindconnect Nanoon. Jokaisella Nano-yhdyskätävällä on yksikäsitteinen tunnistenumero, joka on sulautettu järjestelmään. Tunnistenumeroa käytetään USB-käyttöavaimen luontiin. Käyttöavain liitetään MindConnect Nanoon, jolloin laitteet saadaan liitettyä yhteen. Näin varmistutaan siitä, että vain Siemensin Nano-boxit voidaan yhdistää MindSphereen. (MindConnect Nano Quick Start)

Mindconnect Nanon tietoturvaominaisuudet ovat seuraavat:

- Vain uloslähteviä HTTPS-yhteyksiä.
- Kaksi erillistä verkkokorttia, joista toinen yhdistyy automaatiolaitteiden verkkoon ja toinen ulkomaailman verkkoon.

- Lukuoikeus automaatiolaitteisiin.
- SSL/TLS-salaus. (MindConnect Nano getting started)

5 TESTAUS

Testausvaiheessa tarkoituksena oli konfiguroida Nano vastaanottamaan dataa Veon ilmanvaihtokonehuoneen laitteilta ja saada se eteenpäin Mindsphereen visualisointia varten. Tuntemattomasta syystä tämä ei yrityksistä huolimatta onnistunut. Toisena yrityksenä luotiin testausympäristö Nanoboxille Simatic S7-1500 sekä Modicom M580 kanssa.

5.1 Käyttäjätili

Kun laitteistosta kerättyä dataa halutaan liittää Mindsphereen, asiakkaalle luodaan tenant-tili, johon tieto siirretään. Siemensillä on saatavilla kolmea eri tilityyppiä, jotka ovat:

- käyttäjätili, joka mahdollistaa laitteiden liittämisen ja niiden tietojen tallennuksen ja visualisoinnin sekä halutessa kaupallisten lisäsovellusten appien oston
- kehittäjätili, jossa sovelluskehittäjät voivat testata ja luoda sovelluksia
- operaattoritili, jonka haltijat voivat julkaista kaupallisia sovelluksia Mindsphere Storessa.

Kun tenant on luotu, asiakas saa tililleen tunnuksen ja salasanan. Sisään kirjautumisen jälkeen Mindspheren etusivulta löytyvät käytettävissä olevat toiminnallisuudet. Osa toiminnallisuuksista on vakioita ja perushintaan kuuluvia, osa on asiakkaan tarpeisiin valittuja lisähintaisia toiminnallisuuksia, kuten erilaiset sovellukset, appsit. (Metsälä, Samuli 2019)

5.2 Laitteen käyttöönotto

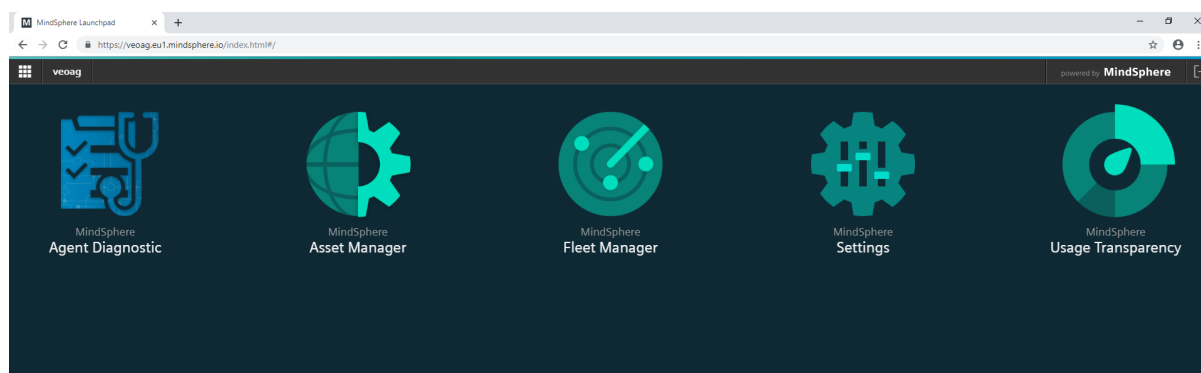
Ensimmäiseksi aseteltiin IP-asetukset tehtaan verkkoon sekä IP-asetukset internetiin yhdistämiseksi. Asetusten jälkeen Mindsphereltä tallennetaan tiedosto USB-tikulle, joka sisältää asetukset Nanolle. Seuraavaksi USB-tikku liitetään Nanon X63-

porttiin (**Kuva 11.**) USB-tikun liittämisen jälkeen Nano asettaa asetukset ja käynnistää itsensä uudelleen. Nanon kaksi ensimmäistä valoa syttyvät vihreäksi ja Nano tulee näkyviin Mindsphere-alustaan, jos asetukset tallentuivat onnistuneesti. (Siemens Nano Quick start)



Kuva 11. Usb-tikun liittäminen Nanoon

Kuvassa 12 näkyy MindSpheren ns. päävalikkosivu. Asset Manager-kohdasta avautuu valikko, josta luodaan Assets, Types sekä Aspects. Assetit ovat Mindspheressä teollisuusprosessiyksikön digitaalisia vastineita, esimerkiksi koneita tai yksittäisiä komponentteja ja aspektit ovat näihin asetteihin liittyvää dataa, joka kuvaa kyseistä teollisuusprosessia. Types- ja aspects-kohdissa luodaan halutut mittapisteet datakeräystä varten. Datan käsittelyä ja analysointia varten kerätyt tiedot liitetään haluttuihin asetteihin ja aspekteihin (Metsälä, Samuli 2019).



Kuva 12. MindSphere Launchpad

Kun pisteet on luotu, Asset-välilehdeltä määritellään Nanon mittaukset yhdistämällä mittapisteeet laittelle. Aspect-sivulla määritellään mittaukset, niiden datatyyppit sekä unitit (**Kuva 13.**).

The screenshot shows the 'Asset Manager' interface with the 'Mittaus' aspect selected. The left sidebar lists various aspects, and the main panel displays the configuration for 'Mittaus'.

Mittaus
Dynamic, 5 Variables

veoag.Mittaus ID	Mittaus Name	Description

Variables

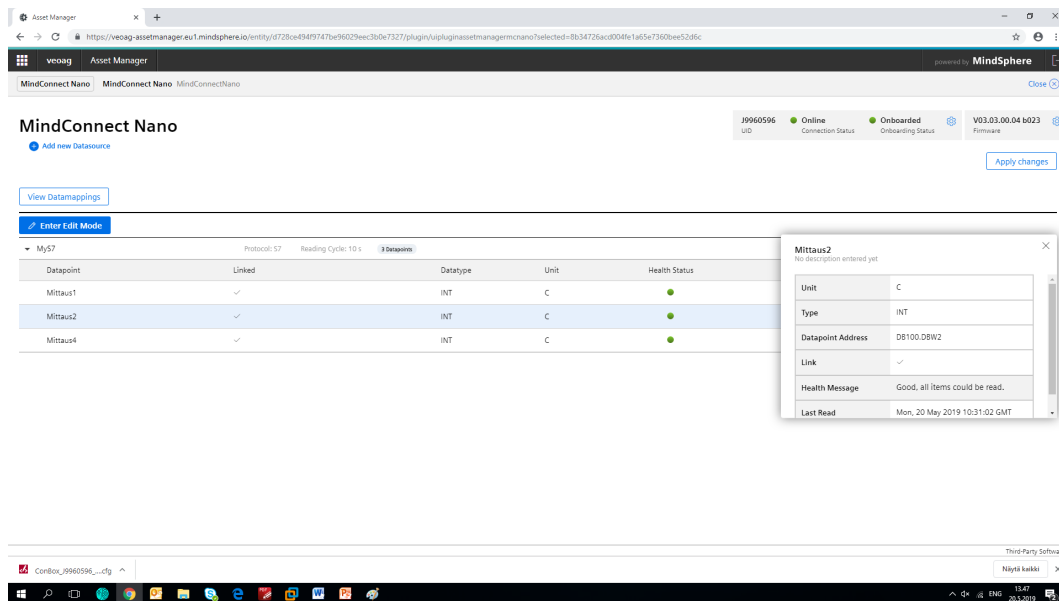
Name	Data type	Unit	Max. length	Value
mittaus1	INT	C	-	-
Mittaus2	INT	C	-	-
Mittaus3	DOUBLE	C	-	-
Mittaus4	INT	C	-	-
Mittaus5	INT	C	-	-

Defined on the following types

Name	Type ID
Testi	veoag.Testi

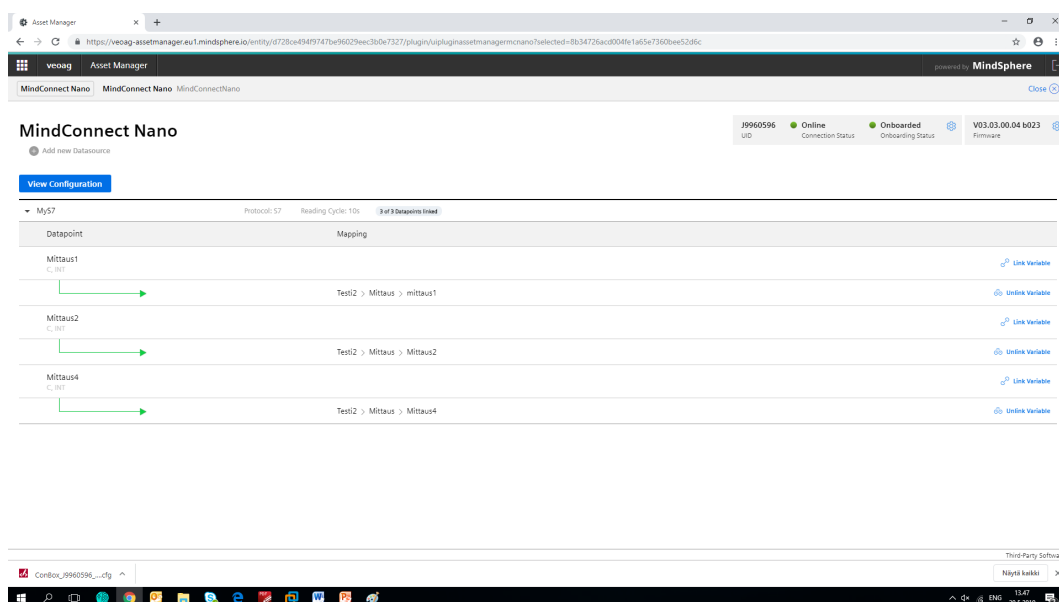
Kuva 13. Mittapisteiden luoti

Kuvan 14 oikeassa yläreunassa näkyy J-alkuinen koodi, joka on Nanoboxin laite-tunnus, Online näyttää internetyhteyden toimivuutta, Onboarding kertoo, että laite on yhteydessä MindSphereen. Enter edit moden kautta luodaan mittaukselle tarvittavat osoitteet, tyyppit ja lajit.



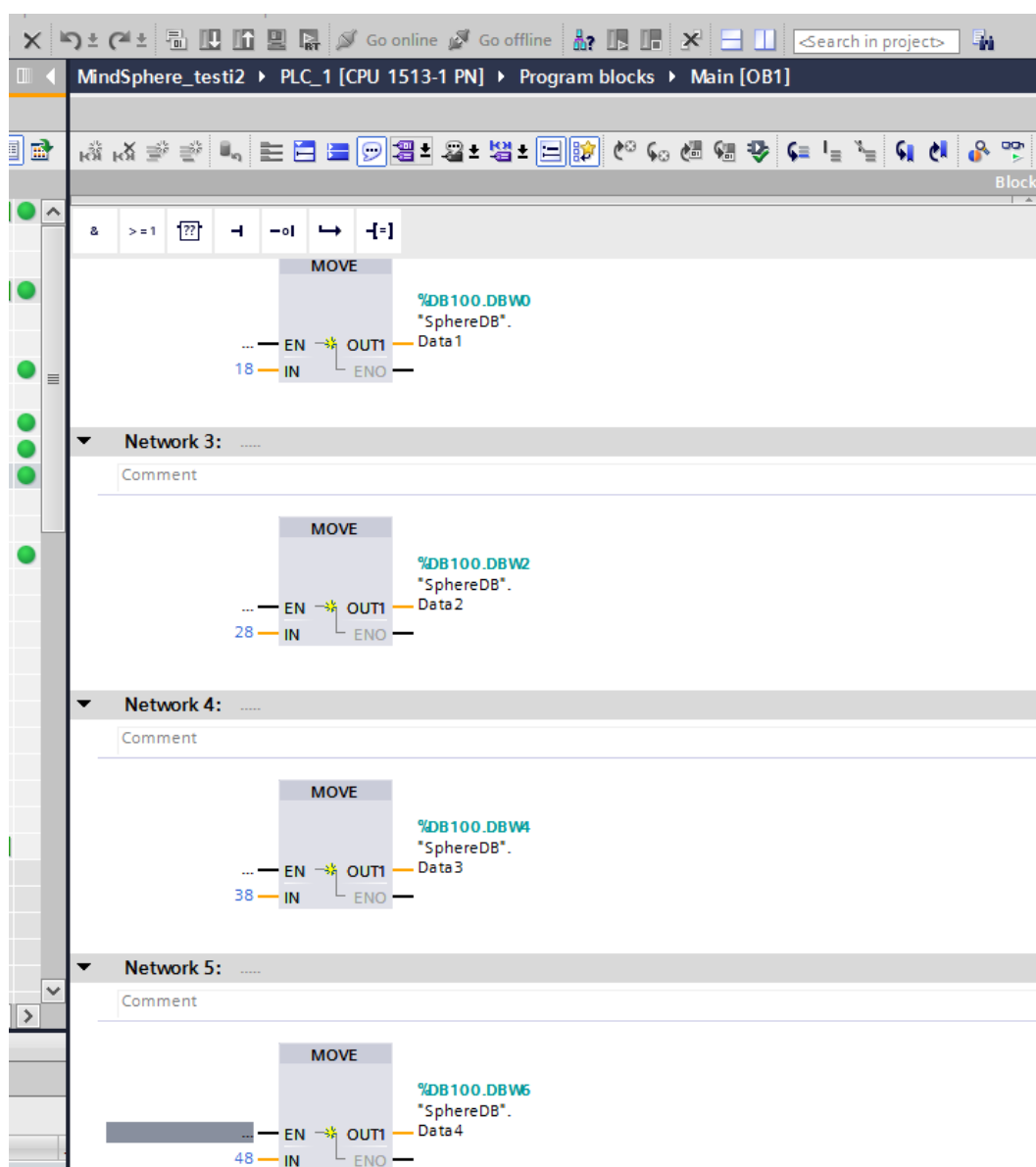
Kuva 14. Asetukset

Kuvassa 15 näkyy miten mittaukset on linkitetty toisiinsa. Klikkaamalla kohdasta link variable luodaan linkki oikeaan mittaukseen. Linkin poistaminen onnistuu klikkaamalla unlink variable. Vihreä nuoli kertoo linkityksen toimivuudesta, punainen nuoli taas siitä, että linkki on viallinen.



Kuva 15. Datamappings

Siemensin mukaan viimeisimmän päivityksen olisi pitänyt tuoda Nanolle myös Modbus liitettävyyden mahdolliseksi. Valikoista Modbus löytyi, mutta yhdistäminen Fidelixin järjestelmään IV-konehuoneessa sekä Modiconin M580:llä ei tuntemattomasta syystä kuitenkaan onnistunut. Simatic S7-1500 yhdistäminen onnistui. Mittausta varten luotiin TIA 15:sta kuvan 16 mukaiset lohkot. Arvoja muuttamalla Fleet managerin käyriin saatiin muutoksia aikaan (**Kuva 17**).

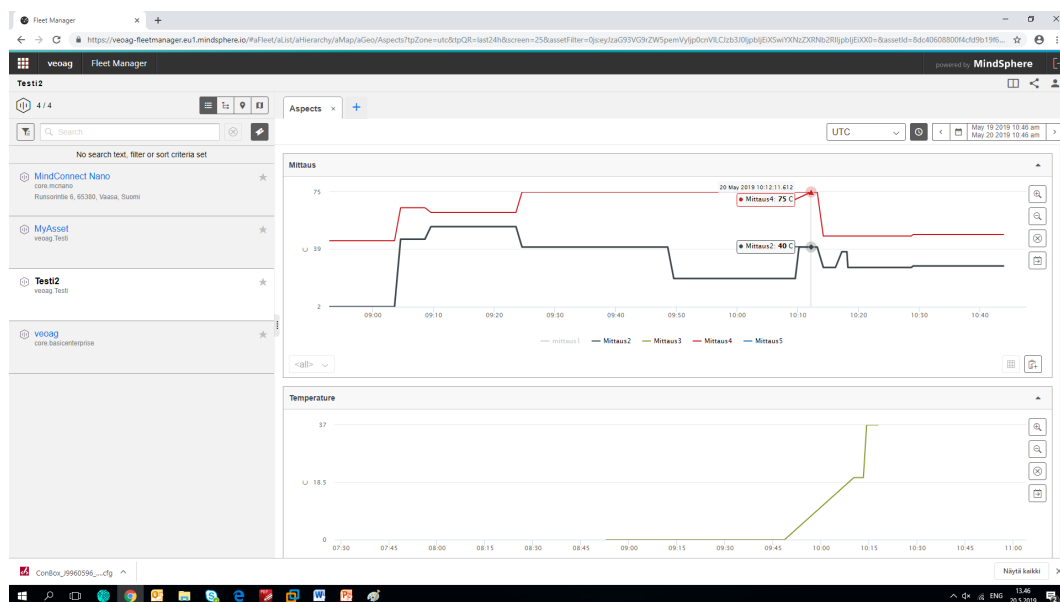


Kuva 16. Tia 15

5.3 Fleet Manager

Fleet Manager on paikka, jossa kerättyä dataa voidaan hallita, visualisoida ja yhdistää analysointia varten. Siellä voidaan muun muassa hallita ympäri maailmaa hajautettujen asettien tietoja. Fleet Managerissa voidaan myös luoda erilaisia hakuja tietokannoista sekä sääntöjä. Tällöin voidaan luoda erilaisia hälytyksiä tai muita tapahtumia. (Metsälä, Samuli 2019)

Fleet Managerista löytyy Rules-lisäosa, josta voidaan määritellä erilaisia rajoituksia ja sääntöjä, jolloin esimerkiksi raja-arvojen ylityksien seuranta helpottuu. Tällöin luodaan aikasarjalle tapahtuma, jonka vakavuusluokka voidaan määritellä toimintaohjeiden lähettämisen esimerkiksi sähköpostilla tai tekstiviestinä (Metsälä, Samuli 2019). TIA 15:sta lohkojen arvojen muutokset aiheuttivat käyrille kuvan 17 mukaisia muutoksia.



Kuva 17. Fleet Manager

6 LOPPUPÄÄTELMÄT

Internet of Things on lisääntymässä ihmisten arjessa niin vapaa-ajalla kuin työssä. Kotia ohjataan puhelimien avulla, teollisuudessa saadaan ennakoitua koneiden huollon tarvetta, autoja voi ohjata, listaa voisi jatkaa pidemmällekin. Päätös siitä, mitä todella tarvitaan käyttöön, tekee kuluttaja. Mielestäni edellä mainituilla ratkaisuilla saadaan tehostettua monia teollisuuden tarpeita sekä parannettua liiketoimintaa. Yritykset saavat tarjottua asiakkaalle lisäarvoa sillä, kun voidaan esimerkiksi seurata mittauksia puhelimen tai tabletin avulla, saada hälytykset heti, kun aiheutta syntyy. IoT-laitteilta vaaditaan kestävyyttä erilaisissa olosuhteissa, mutta myös erityisen tärkeää on se, miten helppoa on laitteiden pitäminen ajan tasalla. Uusimmat päivitykset tulisi olla helposti saatavilla ja asennettavissa.

Opinnäytetyön tekeminen opetti ja syvensi tietoaani IoT-ratkaisuista sekä eri valmistajista. Aihe oli laaja ja asiaa olisi voinut tutkia lähes mistä näkökulmasta tahansa. Opinnäytetyön tavoitteissa yhtenä osana määriteltiin tutustua tarkemmin Siemens MindSphereen sekä tehdä työpöytävertailua muiden valmistajien vastaaviin laitteisiin. Viiteen laitevalmistajaan tutustuneena sanoisin, että valinnanvaraa IoT-laitteista löytyy, käyttäjä löytää varmasti tarpeilleen sopivan laitteen, mutta vaivannäköä se vaatii. Valmistajien sivuilta löytyy paljon tietoa, kaikki kuvaavat laitteitaan helppokäyttöisiksi ja tehokkaiksi. Laitevalmistajan valintatilanteessa kannattaakin testata ja tutustua useampiin merkkeihin ja malleihin, että tietää mikä on omaan käyttöön sopivin.

Toisena osana opinnäytetyötäni oli testata miten MindSphereen saadaan dataa ja tutkia miten sitä voidaan hyödyntää jatkossa. Lukuisien vastoinkäymisten jälkeen dataa saatiin näkyviin vaikkakaan ei sieltä mistä alun perin oli tarkoitus. Mielestäni MindSpheressä samoja asioita lisättiin turhan moniin paikkoihin, ennen kuin tietoa saatiin siirrettyä. Ajanpuutteen vuoksi datan jatkokäsittely sekä yhdistäminen muualta tuotuun dataan jäi tekemättä. Mielikuvaani vahvisti näiden vastoinkäymisten jälkeen, että Siemens toimii parhaiten muiden Siemens-laitteiden kanssa, koska muista laitteista datan keräys ei onnistunut.

LÄHTEET

Collin, J & Saarelainen, A. 2016. Teollinen internet. Helsinki. Talentum.

Hakala, R. Tekniikan maailma. Viitattu 18.5.2019. <https://tekniikanmaailma.fi/asiantuntija-esittaa-uhkakuvan-tietokoneista-tutut-kiristysohjelmat-voivat-tulla-autoihinkin-ja-pahempaakin-on-luvassa/>

Digi Connect Sensor+ verkkosivut. Viitattu 9.5.2019. <https://www.digi.com/products/networking/gateways/digi-connect-sensor#resources>

Elkomen verkkosivut. Viitattu 9.5.2019. <https://elkome.com/jarjestelmatuotteet/secomea-etayhteys-ja-iot-jarjestelma/>

IBM 2015. IBM point of view: Internet of things security. Viitattu 10.4.2019. <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&info-type=SA&html-fid=RAW14382USEN&attachment=RAW14382USEN.PDF>

Mellin, T. Deloitte. Viitattu 18.5.2019. <https://www2.deloitte.com/fi/fi/pages/risk/articles/kyberturvallisuus-suomalaisen-teollisuuden-tulevaisuudessa.html>

Metsälä, S. Siemens-koulutus Veolla, 2.5.2019.

Mindsphere White Paper. Viitattu 2.5.2019 <https://new.siemens.com/fi/fi/tuotteet/ohjelmistot/mindsphere.html>

Plattonen, J. 2015. IoT-datan käsittely ja ennustaminen. Viitattu 10.4.2019. <http://iotfinland.fi/iot-datan-kasittely-ja-ennustaminen/>

Siemens verkkosivut. Viitattu 15.4.2019 <https://new.siemens.com/fi/fi/tuotteet/ohjelmistot/mindsphere.html>

Siemens verkkosivut. Viitattu 15.4.2019 <https://documentation.mindsphere.io>

Siemens verkkosivut. Viitattu 15.4.2019 <https://developer.mindsphere.io>

Sippola, H. 2017. Energiakesittymän ytimessä –VEOn tarina. VEO. Waasa Graphics Oy.

Taanila, I. 2016. Internet of Things (IoT). Viitattu 22.3.2019. <http://iotfinland.fi/internet-of-things-iot/>

Tosiboxin verkkosivut. Viitattu 20.4.2019 <https://www.tosibox.com/fi/>

VEOn verkkosivut. Viitattu 22.3.2019. <https://www.veo.fi>

Viestintävirasto. Viitattu 18.5.2019. <https://www.uusiteknologia.fi/2018/02/01/viestintavirasto-huolissaan-iot-laitteista-verkkotestit-alkoivat/>