Kari Sipilä

TULEVAISUUDEN AUTOMAATIOJÄRJESTELMÄT

OPC UA:n tietoturva ja pilvipalvelut

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Sähkö- ja automaatiotekniikan koulutusohjelma
Huhtikuu 2019

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Huhtikuu 2019	**Tekijä/tekijät** Kari Sipilä
Koulutusohjelma Sähkö- ja automaatiotekniikka		
Työn nimi TULEVAISUUDEN AUTOMAATIOJÄRJESTELMÄT. OPC UA:n tietoturva ja pilvipalvelut		
Työn ohjaaja FM Joni Jämsä		**Sivumäärä** 30
Työelämäohjaaja FM Joni Jämsä		

Automaation järjestelmäintegraatio halutaan laajentaa vertikaalisesti ulottumaan jokaiselle tuotannon tasolle, mutta myös horisontaalisesti laitteelta toiselle. Pilvipalvelut tuovat mahdollisuuden jopa usean tehtaan integrointiin toisiinsa. Tähän tarvitaan tietoturvallinen tiedonsiirron standardi, sillä integrointi muodostaa valtavan tietoturvariskin paitsi yrityksen taloudelle, myös työ- ja ympäristöturvallisuuteen.

OPC oli ollut jo useita vuosia automaatioteollisuuden viestintäprotokollana. Sillä päästiin eroon toimittajariippuvaisista automaatiojärjestelmistä sekä laitevalmistajien valtavista työmääristä erilaisten laitekombinaatioiden ajuriviidakoista. OPC:n uusin määrittely OPC UA julkaistiin vuonna 2006, ja siinä oli kaikki OPC Classicin hyödyt, mutta se oli myös alustariippumaton. Näin toteutettiin turvallinen, avoin ja luotettava kommunikointitapa palvelimien sekä asiakasohjelmien välillä.

Tässä opinnäytetyössä perehdyttiin tulevaisuuden automaatiojärjestelmiin erityisesti viestintäprotokollan näkökannalta tietoturvallisuus huomioiden. Työssä tutkittiin OPC UA:n toteutustapaa sekä käyttötarkoitusta ja käsiteltiin niitä tietoturvan näkökulmasta. Työssä perehdyttiin myös OPC UA:n toimintamalleihin erilaisia tietoturvauhkia vastaan sekä UA:n käyttämiseen pilvipalveluissa. Työssä tutkittiin myös UA:n julkaisija/tilaaja–mallia sekä TSN:ää, jonka avulla saadaan aikaan tietoturvallinen sekä reaaliaikainen tiedonsiirto. Lopuksi esitettiin muutama käytännön esimerkki OPC UA:n käytöstä.

Asiasanat
Automaatio, OPC, OPC UA, pilvipalvelut, Publish/Subscribe, tietoturva, TSN

Centria
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Centria University of Applied Sciences	**Date** April 2019	**Author** Kari Sipilä
Degree programme Electrical and Automation Engineering		
Name of thesis FUTURE OF AUTOMATION. The security of OPC UA and cloud services		
Instructor M. Sc. Joni Jämsä		**Pages** 30
Supervisor M. Sc. Joni Jämsä		

Companies want to integrate their automation systems vertically from top-level ERP to low-level sensors and actuators. In addition, companies seek for horizontal integration of machines. Cloud services have enabled integrating factories. A secure way to connect these integrations is necessary.

OPC has been used as a standard communication protocol for several years. It specified the communication between control devices from different manufacturers. OPC had some disadvantages such as a large amount of work in making drivers for every combination of manufacturers and devices. In addition, Windows-requirement caused problems in reliability and security. A solution for this was OPC UA, which was first released in 2006. It had every advantage from OPC but it was also independent of the platform. OPC UA was an open, reliable, secure and scalable transfer protocol between servers and clients.

Modern automation systems are connected to cloud services from every level. This is a major risk in a company's security. The ways to protect companies from these risks while using OPC UA were studied in this thesis. Moreover, PubSub and TSN technologies were discussed. At the end some examples of how OPC UA is used in real life are presented.

Key words
Automation, cloud services, OPC, OPC UA, Publish/Subscribe, security, TSN

KÄSITTEIDEN MÄÄRITTELY

COM	Component Object Model. Microsoftin apuohjelma, joka mahdollistaa ohjelmistojen välisen tiedonsiirron.
DCOM	Distributed COM. Microsoft Windows –verkossa toimivien sovellusten välinen tiedonsiirtomenetelmä.
ERP	Enterprise Resource Planning. Yrityksen toiminnanohjausjärjestelmä.
HMI	Human Machine Interface. Käyttöliittymä käyttäjän ja laitteen välillä.
HTTP	Hypertext Transfer Protocol. Verkkopalveluiden ja -selainten protokolla.
IaaS	Infrastructure as a Service. Pilvipalvelutyyppi, jossa infrastruktuuri on palveluna.
IIoT	Industrial Internet of Things. Teollinen esineiden internet.
IoT	Internet Of Things. Esineiden internet.
MES	Manufacturing Execution System. Tuotannonohjausjärjestelmä.
M2M	Machine to Machine. Koneiden välinen viestintä.
OLE	Object Linking and Embedding. Microsoftin kehittämä teknologia, joka mahdollistaa objektien linkittämisen ja upottamisen.
OPC	OLE for Process Control. OLE prosessin ohjaukseen.
OPC UA	OPC Unified Architecture.
PaaS	Platform as a Service. Pilvipalvelutyyppi, jossa alusta on palveluna.
PLC	Programmable Logic Controller. Ohjelmoitava logiikka.
TCP	Transmission Control Protocol. Tiedonsiirtoprotokolla, jolla luodaan yhteyksiä tietokoneiden välille.
SaaS	Software as a Service. Pilvipalvelutyyppi, jossa ohjelmisto on palveluna.
SCADA	Supervisory Control And Data Acquisition. Valvomo-ohjelmisto.
SOAP	Simple Object Access Protocol. Protokolla XML viestien välitykseen.

TSN	Time-Sensitive Networking. Tosiaikaiset sovellukset mahdollistava IEEE 208-standardin laajennus.
XML	Extensible Markup Language. Standardoitu rakenteellinen kuvauskieli.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO

Automaatioteollisuus on suuren kehitysaskeleen äärellä uuden teollisen sukupolven saapuessa Teollinen Internet 4.0:n myötä. Automaation järjestelmäintegraatiota halutaan kasvattaa vertikaalisesti ulottumaan jokaiselle tuotannon tasolle, mutta myös horisontaalisesti laitteelta toiselle. Pilvipalvelut tuovat mahdollisuuden jopa usean tehtaan integroinnin toisiinsa. Tähän tarvitaan tietoturvallinen tiedonsiirron standardi.

OPC, OLE for Process Control on ollut jo useita vuosia automaatioteollisuuden viestintäprotokollana. Sillä päästiin eroon toimittajariippuvaisista automaatiojärjestelmistä sekä laitevalmistajien valtavista työmääristä erilaisten laitekombinaatioiden ajuriviidakoista. OPC saavuttikin pian teollisuusstandardin aseman. Siinä oli kuitenkin omat puutteensa Windows-riippuvuutensa myötä, mikä johtui Microsoftin silloisesta monopoliasemasta käyttöjärjestelmien valmistajana. Windows-riippuvuutensa ansiosta OPC:ta pidettiin osittain epäluotettavana ja haavoittuvana protokollana. Tähän vastaus oli OPC UA, Unified Architecture, jonka ensijulkaisu oli vuonna 2006. OPC UA:ssa on kaikki OPC:n ominaisuudet, mutta se on myös alustariippumaton. Tällöin voidaan toteuttaa turvallinen, avoin, skaalautuva ja luotettava kommunikointitapa palvelimien sekä asiakasohjelmien välillä.

Nykyaikainen automaatiojärjestelmä on yhdistetty jokaiselta toimintatasoltaan toiminnanohjausjärjestelmästä aina antureihin saakka pilvipalveluun. Tämä tuo valtavan tietoturvariskin paitsi yrityksen taloudelle, myös työ- ja ympäristöturvallisuuteen. Tietoturva on ollut UA:n kehityksessä mukana alusta saakka, joten se vaikuttaisi oleva yhteensopiva nykypäivän vaatimuksiin.

Tässä opinnäytetyössä perehdytään tulevaisuuden automaatiojärjestelmiin erityisesti viestintäprotokollan näkökannalta tietoturvallisuus huomioiden. Työssä tutkitaan OPC UA:n toteutustapaa sekä käyttötarkoitusta ja käsitellään niitä tietoturvan näkökulmasta. Tutkitaan myös UA:n toimintamalleja erilaisia tietoturvauhkia vastaan sekä OPC UA:n käyttämistä pilvipalveluissa. Työssä käytettiin lähteinä dokumentteja OPC-säätiön määrittelyistä, erityisesti turvallisuusasioita käsittelevää 2. osaa. Lähteinä toimivat myös muut raportit OPC UA:sta sekä eri valmistajien ja asiantuntijoiden internet-sivut.

2 TEOLLISUUDEN JÄRJESTELMÄTASOT

Joustavien ja avointen tuotantoautomaatiojärjestelmien merkitys kasvaa voimakkaasti yritysten tavoitellessa entistä kannattavampaa liiketoimintaa. Tuotantoketjua integroidaan siirtämällä dataa tuotantolaitteiden ja toiminnanohjausjärjestelmien välillä. Yritykset haluavat yhä enemmän reaaliaikaista tietoa tuotantonsa tilasta, mutta myös siirtää tietoa suoraan tuotantolaitteiden ohjausjärjestelmiin sekä mittausdataa kenttätasolta analysoitavaksi. Liikennöinti tuotantoketjun eri tasojen välillä vaatii standardoidun tiedonsiirtoprotokollan, joka helpottaa myös pienempien yritysten integraatiota. Kuvassa 1 on esitetty teollisuuden järjestelmätasot eli automaatiopyramidi, mitä integroidaan sekä vertikaalisesti, että horisontaalisesti.

2.1 Anturit ja toimilaitteet

Alimmalla tasolla kuvan 1 automaatiopyramidissa ovat anturit ja toimilaitteet. Nämä ovat yksittäisiä laitteita, jotka liitetään kenttäväylään. Kenttäväylällä esiintyy vielä vanhempiakin ratkaisuja, kuten Fieldbus sekä Profibus. Myös kenttäväylässä on alkanut yleistymään kommunikointiprotokolla OPC UA, jonka avulla anturit voivat kommunikoida suoraan tuotantopyramidin ylemmille tasoille. Tästä johtuen kuvassa 1 esitetyn automaatiopyramidin eri tasojen rajat alkavat häipymään. (Pyyskänen)

2.2 PLC

PLC eli ohjelmoitavat logiikat tai joissain tapauksissa PC-pohjaiset ohjaimet muodostavat ohjausjärjestelmätason. Tältä tasolta ohjataan alemman tason toimilaitteita ylempien tasojen reseptien mukaan sekä luetaan antureiden tietoa ja välitetään se edelleen ylemmille tasoille. (Pyyskänen)

2.3 SCADA

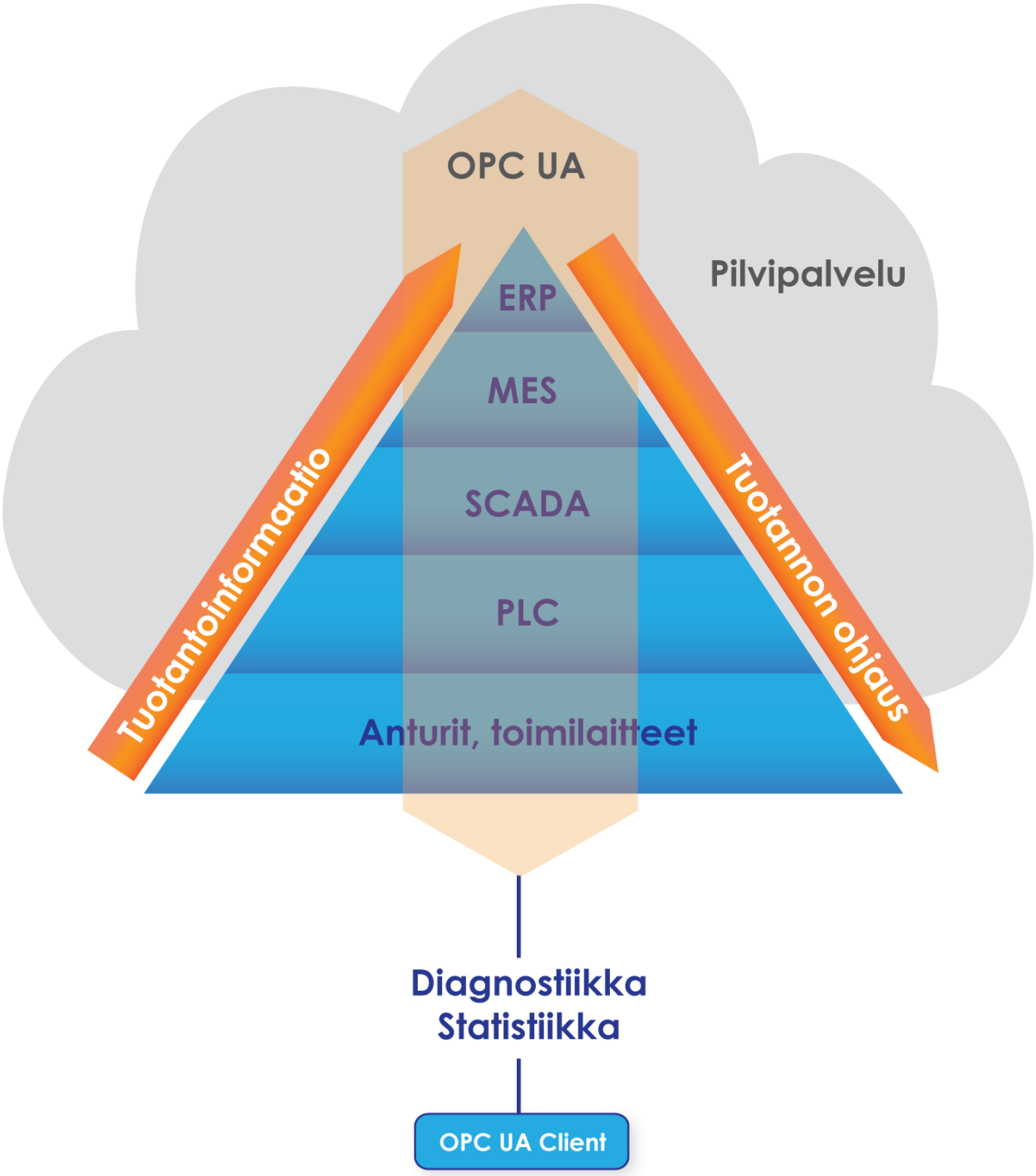
SCADA-järjestelmä on prosessin tai tuotannon valvontaohjelmisto, jota voidaan käyttää paikallisesti tai myös etänä. SCADA-järjestelmä kommunikoi eri laitteiden ohjausjärjestelmien kanssa ja esittää tiedot graafisesti näyttöpäätteillä. Niiltä valvotaan prosessien käyttäytymistä, tehdään ohjauksia sekä seurataan trenditietoja. Myös kaikki hälytystiedot välittyvät SCADA:an. (Inductive automation, 2018)

2.4 MES

MES-järjestelmät eli tuotannonohjausjärjestelmät ovat lyhyen aikavälin tuotannonohjaukseen sekä -suunnitteluun soveltuvia järjestelmiä. Tuotannonohjausjärjestelmä saa toiminnanohjaustasolta tilaukset, joiden valmistusjärjestystä MES-järjestelmä voi optimoida ja siirtää ne tuotantoon. Tuotannosta kerätään takaisin tietoja tuotantomääristä, laadunvalvonnasta sekä raaka-aineiden kulutuksesta. (Pyyskänen)

2.5 ERP

Toiminnanohjaustaso, eli ERP on korkein taso kuvan 1 automaatiopyramidissa. ERP-tasolla käsitellään yrityksen hallinnoimiseen ja johtamiseen liittyvät asiat. Näitä ovat esimerkiksi varaston hallinta, tilaustenhallinta, henkilöstösuunnittelu, laadunhallinta, laskutus sekä asiakastiedot. Myös ERP-tasolle siirtyy dataa tuotannosta. (Pyyskänen)



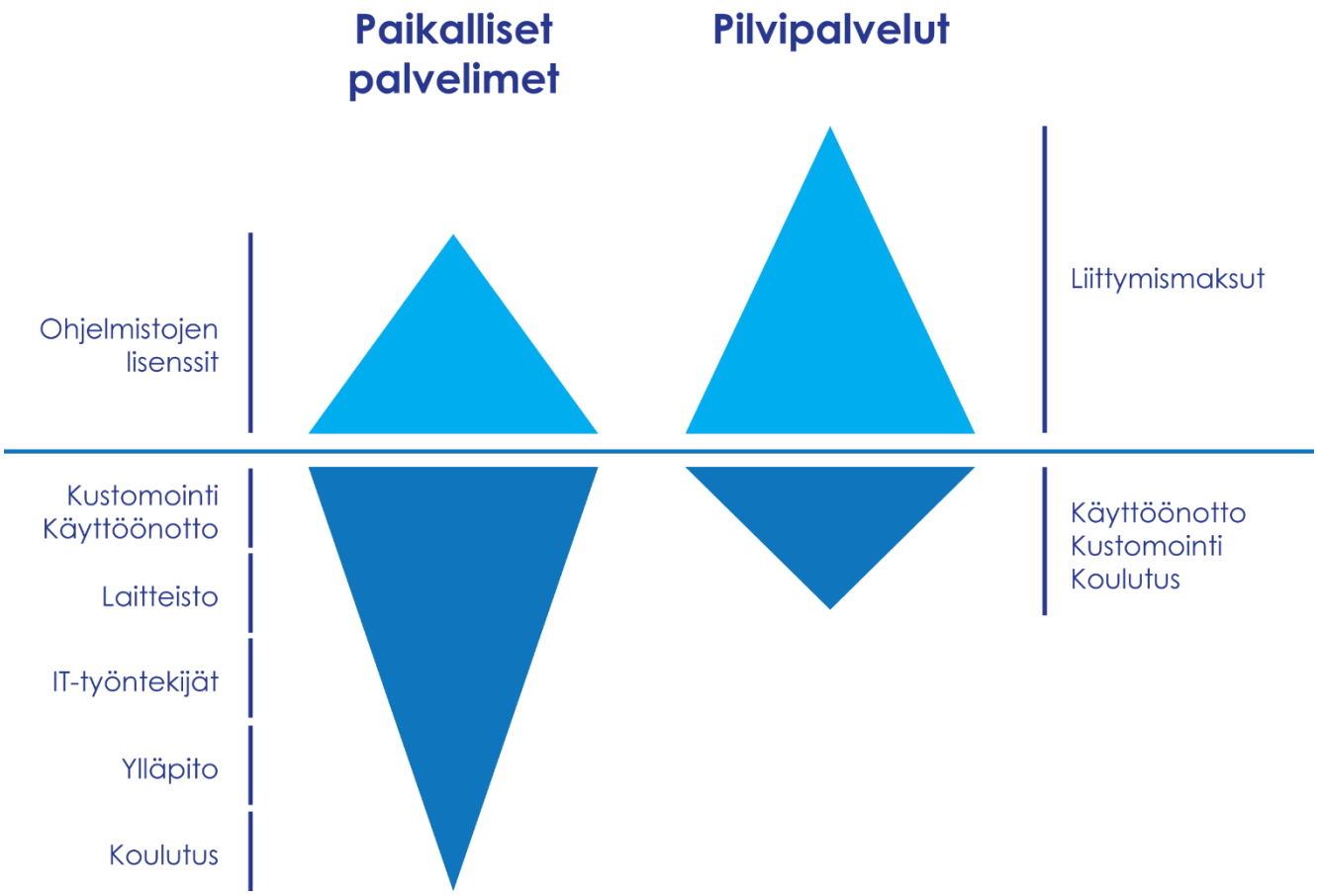
KUVA 1. Teollisuuden järjestelmätasojen eli automaatiopyramidin tiedonkulkumalli (mukaillen Microsoft Azure)

2.6 Pilvipalvelut

Tehostaakseen IT-resurssejaan yritykset ovat alkaneet käyttää perinteisen palvelinhuoneen sijaan pilvipalveluita. Pilvialustat ovat palveluiden tarjoajia, joiden palvelut voidaan ostaa internetin yli. Sisältönä palveluissa voivat olla palvelimet, tallennustilat, tietokannat, ohjelmistot sekä analytiikat. Hinnoittelu perustuu yleensä minuutti-, tunti- tai kuukausiveloitukseen. (Microsoft Azure)

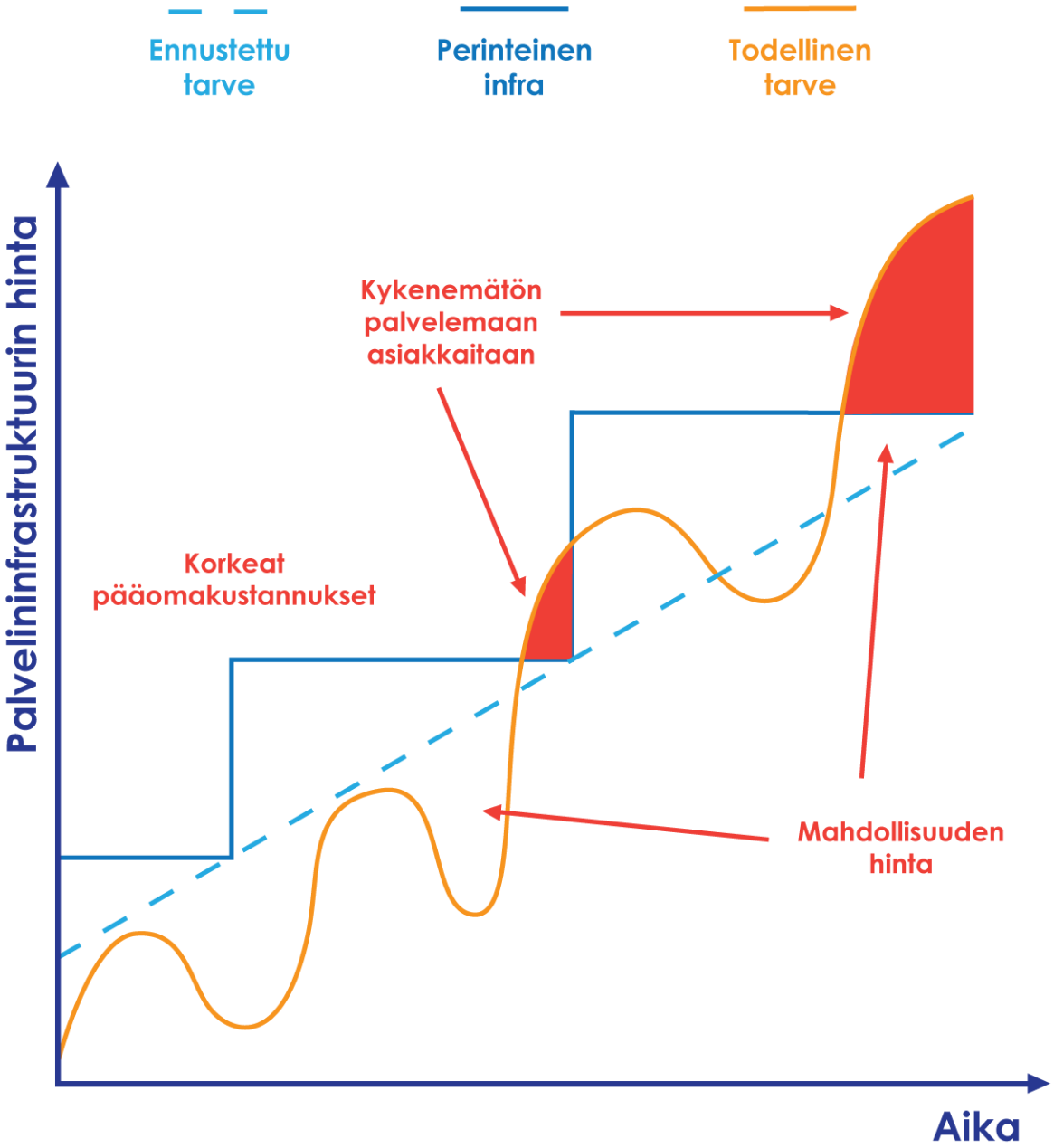
2.6.1 Pilvipalveluiden edut

Pilvipalveluiden ostaminen ulkopuoliselta toimijalta vähentää pääomakustannuksia, sekä kiinteitä kuluja kuvan 2 osoittamalla tavalla. Palvelimia ja tallennustilaa ei tarvitse hankkia yrityksen kasvaessa lisää, jolloin vältytään monimutkaisilta ratkaisuilta. Palvelinhuoneet myös tarvitsevat ympärivuotisen jäähdytyksen, sähkönkulutuksen sekä huolto- ja ylläpitotyön. Pilvipalvelua voidaan mukauttaa erittäin nopeasti yrityksen tarpeen mukaan. Tällöin ei tarvitse investoida kauas tulevaisuuteen, mikä olisi taas pois yrityksen muista hankinnoista. Ohjelmistojen sekä laitteistojen päivitys- ja korjaustöistä aiheutuneet tuotantokatkokset ovat kalliita yrityksille. Pilvipalveluiden ansiosta katkoksia ei esiinny sen toiminta-alueen osalta. Pilvipalveluiden tarjoajilla on myös nopeasti kehittyvien laitteiden viimeisin teknologia sekä ajan tasalla oleva asiantuntijuus tietoturva-asioissa. Kuten kuvasta 2 voidaan havaita, suorat kustannukset ovat hieman suuremmat pilvipalveluissa, mutta epäsuorat kulut jäävät huomattavasti pienemmiksi perinteiseen palvelininfrastruktuuriin verrattuna. Pilvipalveluissa käyttäjien tiedot ovat myös turvassa toisessa sijainnissa, jolloin käyttäjän laitteen rikkoontuminen ei hävitä tärkeitä tietoja. Lisäksi tallennustila on varmuuskopioitu ja hajautettu usealle eri palvelimelle. (Karimi, 2018)



KUVA 2. Pilvipalveluiden taloudelliset edut (mukaillen Karimi, 2018)

Pilvipalvelut ovat ratkaisu monimutkaisesti kehittyvään liiketoimintaympäristöön. Ne skaalautuvat välittömästi yrityksen tarpeeseen paitsi kasvussa, mutta myös palvelintarpeen vähentyessä ja näin saadaan aikaan säästöjä. Yritykset hyötyvät myös mahdollisuudesta ottaa käyttöön uusia palveluita nopeasti ja helposti, mitkä skaalautuvat myös tarpeen mukaan kuvan 3 mukaisesti. Perinteisessä palvelininfrassa yritykselle tulee suuret pääomakustannukset palvelinten hankinnassa ja varallisuutta on koko ajan liikaa sidottu palvelinlaitteistoon. Mikäli todellinen tarve ylittää palvelinkapasiteetin, on yritys kykenemätön palvelemaan asiakkaitaan ja ollaan taas tilanteessa, jossa joudutaan suuriin investointeihin. Todellisen tarpeen mukaan toteutuvassa pilvipalvelimessa investointi ikään kuin jakaantuu suuremmalle aikavälille eikä siitä koidu yritykselle korkokuluja. Pilvipalvelut mahdollistavat myös kokeilun erilaisille ratkaisuille ja palveluille. Palvelussa voi rohkeasti kokeilla uuden palvelun toimivuutta ilman lisäinvestointeja ja sen osoittautuessa toimivaksi, voidaan palvelimet skaalauttaa välittömästi vastaamaan tarvetta uudelle palvelulle. Mikäli kokeilu osoittautuu epäonnistuneeksi, voidaan se vain hylätä ja sulkea pilvipalvelinpalveluista. (Lassila, 2019)

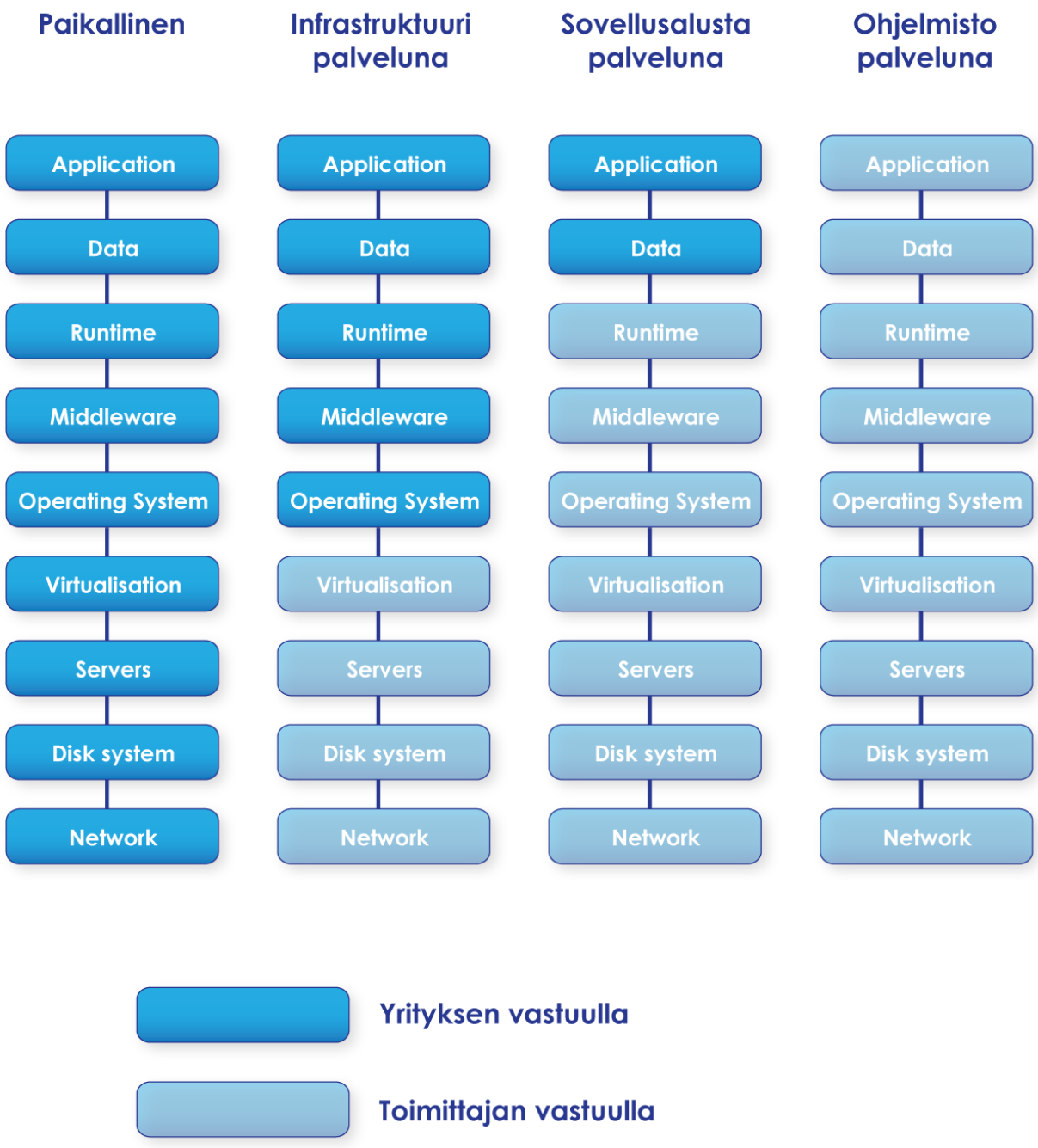


KUVA 3. Pilvipalveluiden edut yrityksille (mukaillen Lassila, 2019)

2.6.2 Pilvipalveluiden tyypit

Pilvipalveluita on tarjolla useita eri tyyppejä, jolloin jokaiselle yritykselle löytyy tarpeeseen sopiva palvelu. Pilvipalvelun arkkitehtuurin tyyppejä ovat julkinen, paikallinen sekä näiden yhdistelmä.

Julkisessa pilvessä palveluita sekä laitteita ylläpitää ja omistaa kolmas osapuoli, kuten esimerkiksi Microsoft Azure, AWS ja Google. Paikallisissa palvelimissa kaikki yrityksen itsensä tarjoamat palvelinpalvelut ovat vain yrityksen omassa käytössä. Hybridi-palvelussa kummatkin edellä mainitut ovat käytössä ja ne osaavat myös hyödyntää toisiaan. Julkisten pilvipalveluiden tarjoamat palvelut voidaan jakaa kolmeen eri malliin, joita ovat infrastruktuuri palveluna IaaS, sovellusalusta palveluna PaaS sekä ohjelmisto palveluna SaaS. Paikallisessa palvelimessa yrityksen vastuulla on koko palvelinketjun hoitaminen. Alla olevassa kuvassa 4 on havainnollistettu vastuualueiden jakaantuminen eri palvelutyyppien välillä. (Microsoft Azure)



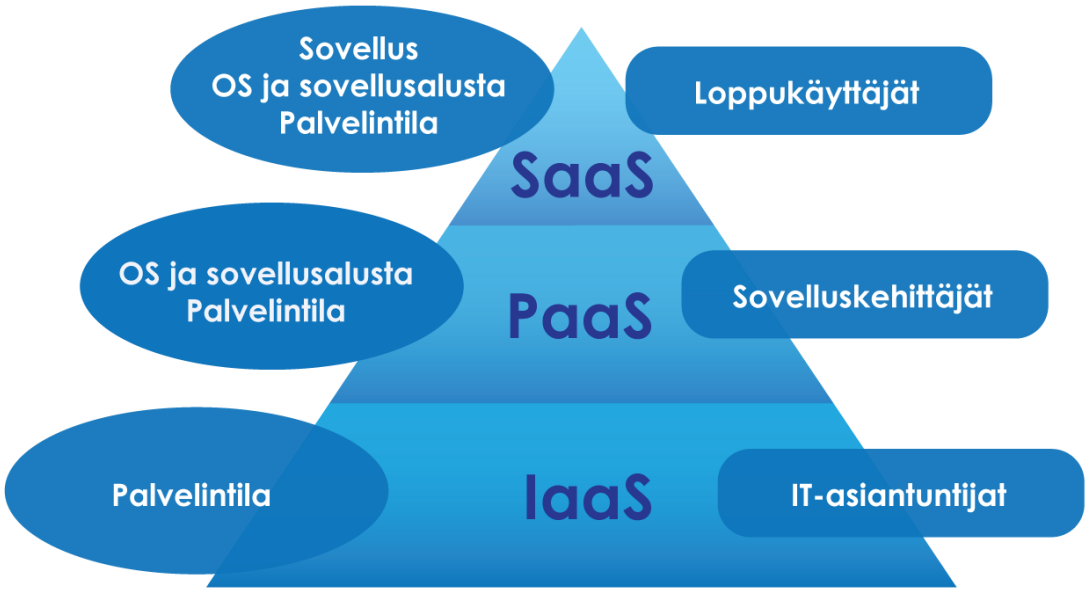
KUVA 4. Eri pilvipalvelumallien vastuualueet (mukaillen Lassila, 2019)

IaaS, infrastruktuuri palveluna on kuvan 5 alimman tason pilvipalvelu, jossa palveluntarjoaja tarjoaa asiakkaalleen virtualisoituja palvelimen resursseja. Käyttäjä voi asentaa haluamansa käyttöjärjestelmän ja sovellukset palvelimelleen. Palveluntarjoaja ylläpitää laitteita, joita yritys käyttää virtuaalisena palvelimenaan. Sen etuja ovat pääomakustannusten pienentäminen laitteiston osalta sekä palvelun koon

mukautuvuus tarpeen mukaan. Tällainen ratkaisu toimii parhaiten yritykselle, jolla on korkea tietotekninen osaaminen sekä halu mukauttaa palvelintaan omiin tarpeisiinsa sopivaksi. Tämä ratkaisu vaatii yritykseltä työpanosta myös palvelun ylläpitoon sekä tietoturva-asioihin. (Solomon, 2018)

PaaS, sovellusalusta palveluna on viety hieman IaaS:ia pidemmälle. Laitteiston lisäksi palveluntarjoajalta tulee valmiit työkalut sovelluksen toteuttamiseksi. Yleisimmin PaaS soveltuu parhaiten yrityksille, jotka testaavat ja kehittävät pilviratkaisuja tietyille ohjelmistoille. Näin yritykset voivat vain siirtää sovelluksensa ostetulle alustalle. Palveluntarjoaja ylläpitää käyttöjärjestelmää ja lisäohjelmistoja, jolloin ostaja huolehtii vain sovelluksensa ylläpidosta. Yrityksen ei tarvitse huolehtia laitteistonsa tai ohjelmistojensa hankinnoista ja päivityksistä. (Solomon, 2018)

SaaS, ohjelmisto palveluna on sovellus, jossa palveluntarjoaja tarjoaa myös ohjelmiston internetin yli esimerkiksi selaimella käytettäväksi. Tässä palvelussa palveluntarjoajan vastuulla on koko pilvipalvelun ylläpito, jolloin ostajayritykselle jää pelkästään palvelun käyttö. Tämä ratkaisu sopii erityisesti pienemmille yrityksille, joilla ei ole erikseen IT-henkilöstöä eikä ymmärrystä tietoturva-asioista. SaaS:n etuina ovat nopea skaalautuvuus jokaisella osa-alueella. Tällöin yritys maksaa vain siitä, mitä se tarvitsee kuvan 3 oranssia kuvaajaa seuraten. Palvelun käyttöön tarvitaan vain verkkoyhteys ja internetselain. (Solomon, 2018)



KUVA 5. Pilvipalveluiden palvelutyypit (mukaillen Fu, 2017)

3 OPC UA

Automaation tiedonsiirrossa on jo vuosikymmeniä käytetty OPC-tiedonsiirtoprotokollaa, jonka avulla on voitu lukea mittaustietoja muihin kuvan 1 automaatiopyramidin järjestelmiin. OPC:ta hyödyntäen saadaan erilaisia tilatietoja, hälytys- sekä tapahtumaviestejä, joita voidaan hyödyntää kunnossapidossa sekä tuotantoprosessin reaaliaikaisessa seurannassa myös ERP- ja MES-järjestelmissä. OPC:n jäljempänä esitettyjen ongelmien vuoksi siitä on kehitetty myös uudempi versio OPC UA, jota ollaan ottamassa yleisesti käyttöön automaatiojärjestelmissä. OPC UA:n avulla voidaan liittää tietoturvallisesti eri valmistajien tuotteet ja järjestelmät toisiinsa. (Prosys)

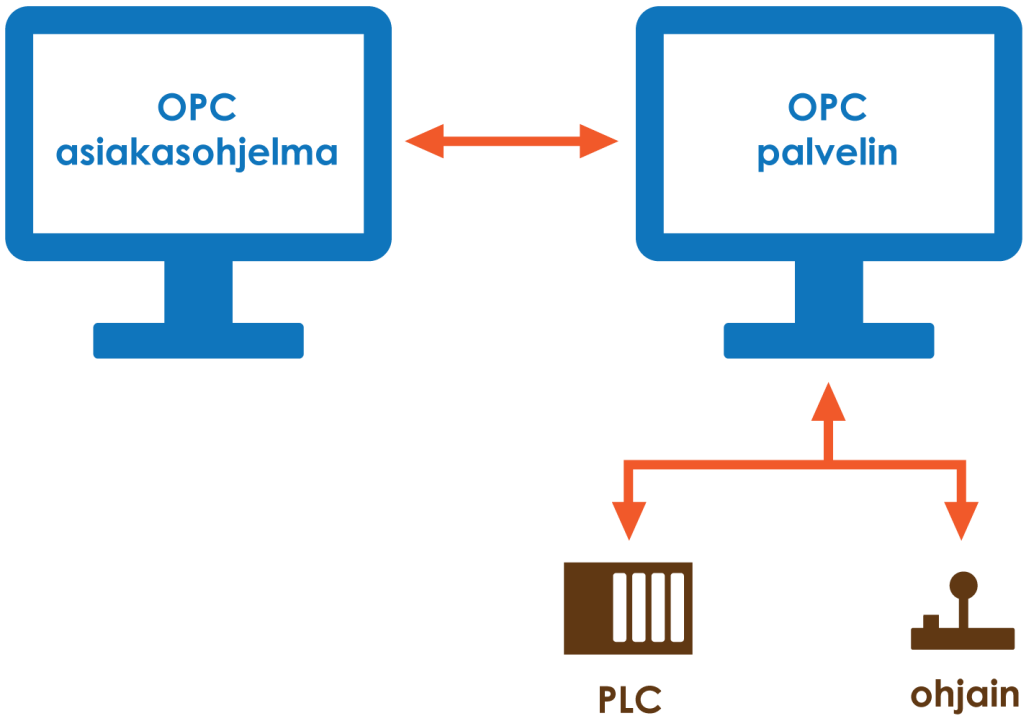
3.1 OPC:n historia

1990-luvulla oli markkinoilla monen automaatiojärjestelmiä ja väyläratkaisuja toimittavien yritysten tuotteita. Näistä jokainen vaati oman ajurinsa järjestelmää tukeville laitteille. Ohjelmistotoimittajien tuodessa uusia automaatio-ohjelmia myyntiin, joutuivat he tekemään ajureita sadoittain eri järjestelmien laitteille. Ajureiden valmistaminen työllisti yrityksiä valtavasti eikä muulle kehitystyölle jäänyt riittävästi aikaa. Muutamat automaatioalan yritykset perustivat OPC-työryhmän selvittääkseen keinoja päästä eroon ajureiden ylityöllistävästä vaikutuksesta. Mukana työryhmässä oli myös Microsoftin edustaja antamassa teknistä tukea tuolloisen monopoliasemansa vuoksi tietokoneiden käyttöjärjestelmissä. Microsoftilla oli valmiiksi COM- ja DCOM-teknologiat tiedon jakamiseen tietokoneiden ja Windows-käyttöjärjestelmien välillä. Samaan aikaan tietokoneet halpenivat ja jotkin yritykset halusivatkin Windows-pohjaisia tietokoneita automaatioteollisuuteen kalliiden ohjelmoitavien logiikoiden tilalle. OPC-työryhmän olikin luontevaa käyttää olemassa olevaa teknologiaa OPC:n tiedonsiirtoprotokollaksi. (OPCConnect)

OPC-työryhmä perusti voittoa tavoittelemattoman ja riippumattoman OPC-säätiön, johon liittyivät pian lähes kaikki automaatioalan toimittajat. Säätiön tehtävänä on muokata määrittelyitä puolueettomasti yritysten toiveiden mukaisiksi sekä luoda ja ylläpitää teknisiä tietoja. Se myös tukee jäseniään OPC:n käytössä. Säätiö on laatinut testauskäytännön, jolla varmistetaan OPC-sertifioitujen laitteiden yhteensopivuus. (OPC Foundation)

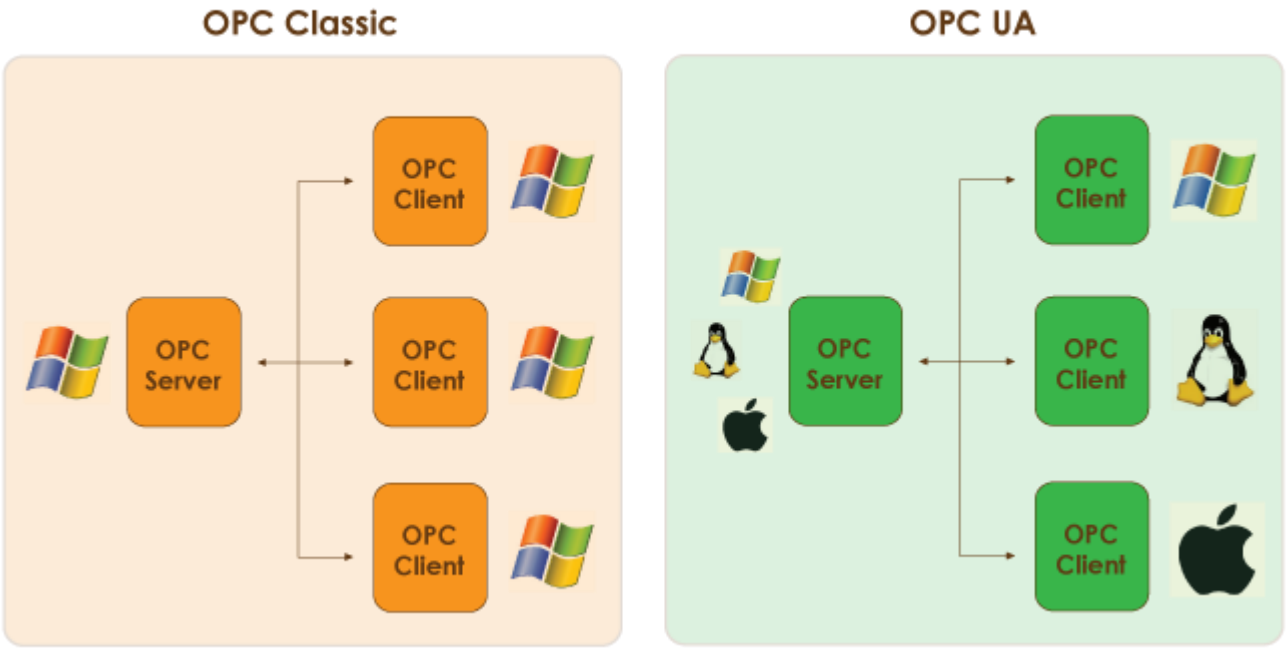
Vuoden 1996 julkaisun jälkeen OPC on ollut yksi käytetyimmistä kommunikointitavoista automaatioalalla. Siitä muodostui vallankumouksellinen teknologia automaatioalalla. Mikä tahansa

Microsoftin COM:ia tukeva ohjelma pystyi kommunikoimaan antureiden sekä toimilaitteiden kanssa kuvan 6 osoittamalla tavalla, eikä ajureiden kehitys enää vienyt sovelluskehittäjien kaikkea työaikaa. OPC mahdollisti kaiken teollisuudessa kulkevan tiedonsiirron OPC-yhteensopivien laitteiden välillä. Nämä asiat yhdessä auttoivat tietokoneiden tuloa automaatioteollisuuteen. Vuosien aikana OPC on kehittynyt erilaisiin protokolliin, kuten esimerkiksi Data Access, Alarms & Events sekä Data eXchange. Näistä käytetään usein yhteisnimitystä OPC Classic. OPC voi toimia joko pollaavana, jolloin asiakasohjelma pyytää tietoa palvelimelta tai tapahtumapohjaisena, jolloin palvelin lähettää tiedot asiakasohjelmalle muutoksen tapahtuessa. (Novotek)



KUVA 6. OPC:n toimintamalli (mukaillen Novotek)

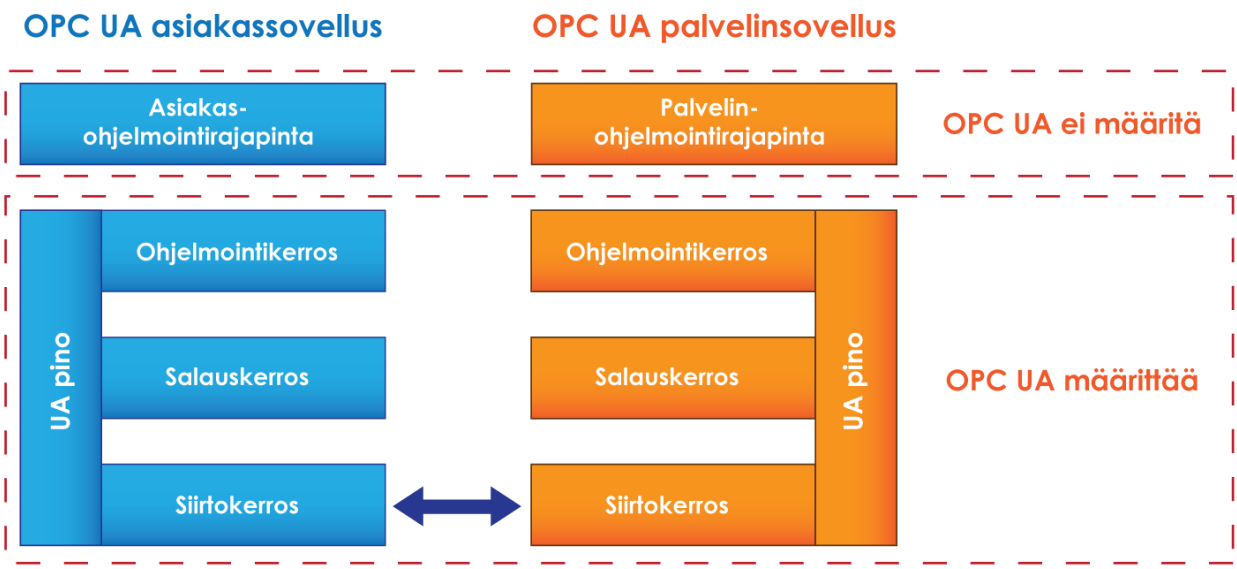
OPC:ta käytettiin monilla teollisuuden aloilla useisiin käyttötarkoituksiin. OPC Classicilla oli kuitenkin rajoituksensa sen Windows-riippuvuudesta johtuen. Kaikkien OPC:ta hyödyntävien laitteiden täytyi olla Windows-pohjaisia, jolloin sen luotettavuus sekä turvallisuus oli kyseenalaista. OPC UA oli tähän ratkaisu, minkä ensijulkaisu oli vuonna 2006. Siinä oli kaikki OPC Classicin ominaisuudet, mutta se oli myös alustariippumaton kuten kuva 7 osoittaa. Tällöin voitiin toteuttaa turvallinen, avoin ja luotettava kommunikointitapa palvelimien sekä asiakasohjelmien välillä. (National Instruments, 2017)



KUVA 7. OPC Classicin ja OPC UA:n alustariippuvuuserot (mukaillen National Instruments, 2017)

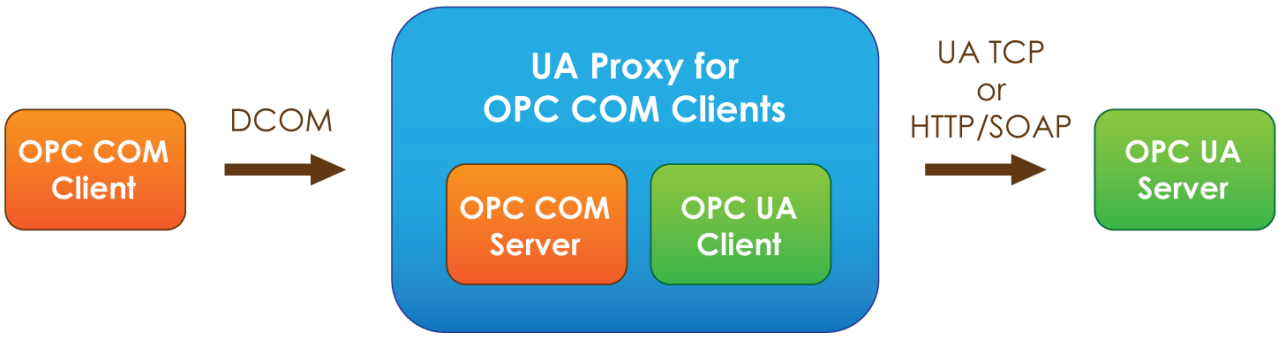
3.2 OPC UA

OPC UA on ensimmäinen menetelmä tiedonsiirtoon, mitä voidaan käyttää jokaisessa ympäristössä läpäisten palomuurit sekä muut tietoturvaesteet. Se on suunniteltu tietokantojen, ERP-järjestelmien, analytiikkatyökalujen sekä muiden tietojärjestelmien ympäristöihin. Näissä ympäristöissä anturit, kenttälaitteet, kytkimet sekä muut valvontajärjestelmien laitteet kommunikoivat keskenään pilvipalvelun välityksellä. Tällöin OPC UA:lla voidaan toteuttaa tiedonsiirtomenetelmä koko tuotantopyramidin jokaiselle osa-alueelle kuten kuvassa 1. OPC UA hyödyntää skaalautuvuutta sekä älykästä tiedonsiirtomallia tuottaakseen mahdollisimman pienen tietomäärän avoimeen palvelinsovellusten verkkoon. Sen avulla voidaan siirtää pientä tilatietoa, mutta myös valtavaa tietokompleksia koko tehtaan tilasta. Sitä voidaan siis hyödyntää kaiken kokoisissa käyttökohteissa. OPC UA:han liittäminen sekä sulautetuissa- että yritysympäristöissä on varmistettu käyttämällä standardiliikennöintiä ja salausta. UA ei määritä asiakas- tai palvelinohjelmointirajapintaa kuten kuva 8 ilmaisee. (Real Time Automation)



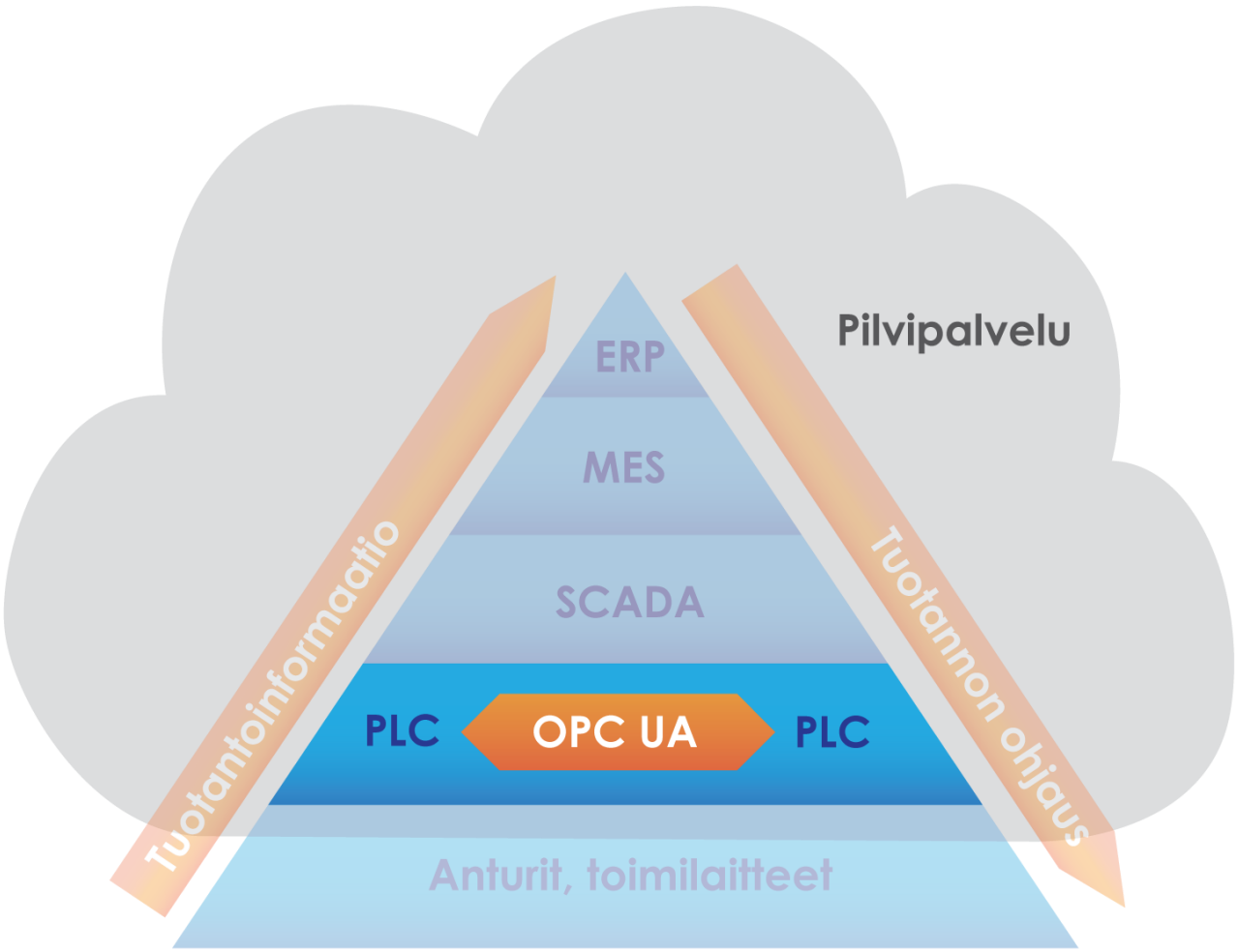
KUVA 8. OPC UA ei määritä asiakas- tai palvelinohjelmointirajapintaa. (mukaillen OPC Foundation, 2018)

Standardisoidun turvamallin vuoksi OPC UA voi kommunikoida minkä tahansa HTTP- tai TCP-portin välityksellä. Tällöin lisäkustannuksiakaan ei koidu, kun voidaan käyttää olemassa olevaa tietoliikenneverkkoa. OPC UA ei ole suoraan yhteensopiva OPC Classicin kanssa, vaan se vaatii tietyn Gateway-ohjelmiston muodostaakseen OPC UA tunnelin kuvan 9 mukaisesti. (National Instruments, 2017)



KUVA 9. OPC Classicin ja OPC UA:n yhteensovittaminen onnistuu sovittimien avulla (mukaillen National Instruments, 2017)

OPC UA on täysin uusi tapa toteuttaa kommunikointi koko teollisuusautomaatioketjussa turvallisesti. Sillä voidaan toteuttaa vertikaalinen yhteys toiminnanohjausjärjestelmästä tuotannonohjaukseen ja sieltä aina lattiatason antureihin ja toimilaitteisiin saakka täysin alustariippumattomasti jopa palomuurien yli. Horisontaalinen liikennöinti voidaan myös toteuttaa OPC UA:lla kuvan 10 mukaisesti älylaitteilta toiselle ilman tietokoneita. Näin automaatiopyramidin eri tasojen rajatkin alkavat häipyä, kun laitteet voivat keskustella suoraan toisilleen ilman ylempien tasojen ohjauskomentoja. Tämä kaikki voi tapahtua myös pilven yli, jolloin laitteet voivat sijaita eri tehtaissa. (National Instruments, 2017)



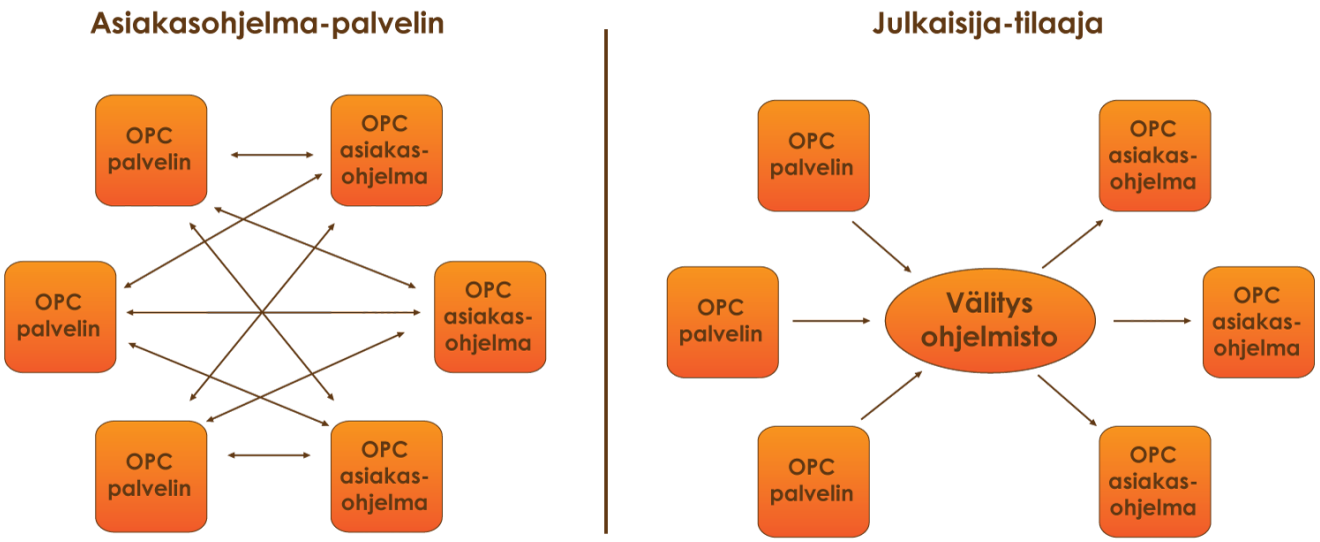
KUVA 10. OPC UA:ta voidaan käyttää laajasti koko teollisuusautomaatioketjussa myös horisontaalisesti (mukaillen National Instruments, 2017)

OPC UA:n tuleminen markkinoille on niin valtava harppaus teknologian kehityksessä, että sen tarjoamia mahdollisuuksia on vielä vaikea ymmärtääkään. Tuottamalla lisää dataa se mahdollistaa uusia

käyttötapoja ja toiminnallisuuksia mutta myös parantaa laatua, lisää tuottavuutta sekä pienentää kuluja. Lisädata antaa juuri oikealla hetkellä tietoa myös tuotantoon, kunnossapitoon sekä IT-järjestelmiin. OPC UA:n perustana toimii objekti, joka voi olla yksittäinen tieto tai prosessi, mutta myös vaikka kokonainen tehdas. Se voi myös olla yhdistelmä dataa ja metadataa. Objekteihin voi viitata myös muissa objekteissa tai datamuuttujien tietotyypeissä, jotka voivat olla muualla arkkitehtuurissa tai vaikka muualla internetissä. (Peltokangas, 2017)

3.3 OPC UA Pub-Sub

OPC UA:n rajoitteena ovat olleet laajat asiakasohjelma-palvelinjärjestelmät, joissa jokainen laite kysyy dataa palvelimilta erikseen kuvan 11 mukaisesti. Tämän tyyppinen malli soveltuu heikosti pilvipalveluiden toteuttamiseen sekä suurien järjestelmien palveluiden kehittämiseen. OPC-säätiö julkaisi vuonna 2016 Publish/Subscribe-laajennuksen korjatakseen tämän ongelman. Tässä julkaisija/tilaaja-mallissa UA-palvelin lähettää tiedot välitysohjelmistolle tietämättä, mitkä asiakasohjelmat haluavat kyseistä tietoa. Asiakasohjelmat ilmoittavat välitysohjelmistolle tiedon, mitä viestejä ne haluavat vastaanottaa. Näin siirrettävän datan määrä pienenee huomattavasti kuten kuvan 11 nuolien määrästä voidaan päätellä ja resursseja säästyy muihin toimenpiteisiin. (OPC Foundation, 2016)



KUVA 11. OPC:n julkaisija/tilaaja-malli vähentää liikennöintiä huomattavasti (mukaillen B&R Industrial Automation, 2015)

Julkaisija/tilaaja–malli parantaa erityisesti käytettävyyttä tulevaisuuden IoT-verkoissa sekä M2M-ratkaisuissa. PubSub:a voidaan käyttää paikallisen LAN-verkon yli, jolloin data lähetetään UDP-protokollaa käyttäen. Julkaisija lähettää viestin ja suuri joukko valtuutettuja tilaajia voi vastaanottaa viestin. PubSub:a voidaan käyttää myös julkisen WAN-verkon tai pilven yli, jolloin suuri joukko julkaisijoita voi lähettää viestin suurelle joukolle tilaajia. Tällä tavalla saavutetaan turvallinen, skaalautuva keino datan jakamiseen monimutkaisenkin verkkotopologian yli. Mikäli automaatiojärjestelmän halutaan toimivan täysin reaaliaikaisesti, tarvitsee PubSub-malli tuekseen TSN-laajennuksen. (OPC Foundation, 2018)

3.4 OPC UA ja TSN

Tulevaisuuden monimutkaisissa prosesseissa on vaatimuksensa tiedon kulkemiseen ERP-tasolta kenttätasolle reaaliaikaisesti, missä OPC UA:lla on omat rajoituksensa. Riittävä reaaliaikaisuus on toistaiseksi saatu aikaan erilaisilla protokollilla, mikä aiheuttaa valtavasti lisätyötä yhteensovittamiseen. Usean automaatiotoimittajan muodostama ryhmä on kehittänyt tähän ratkaisuna TSN:n. Time Sensitive Networkingia on kehitetty yleisenä rajapintana teollisten sovellusten sekä pilvipalveluiden väliin. Pyrkimyksenä on avoin, standardisoitu, yhtenäistetty sekä IIoT-yhteensopiva ratkaisu, jolla voidaan reaaliaikaisesti keskustella ylimmältä ERP-tasolta aina kenttätasolle saakka tai suoraan laitteelta laitteelle. (B&R Industrial Automation, 2015)

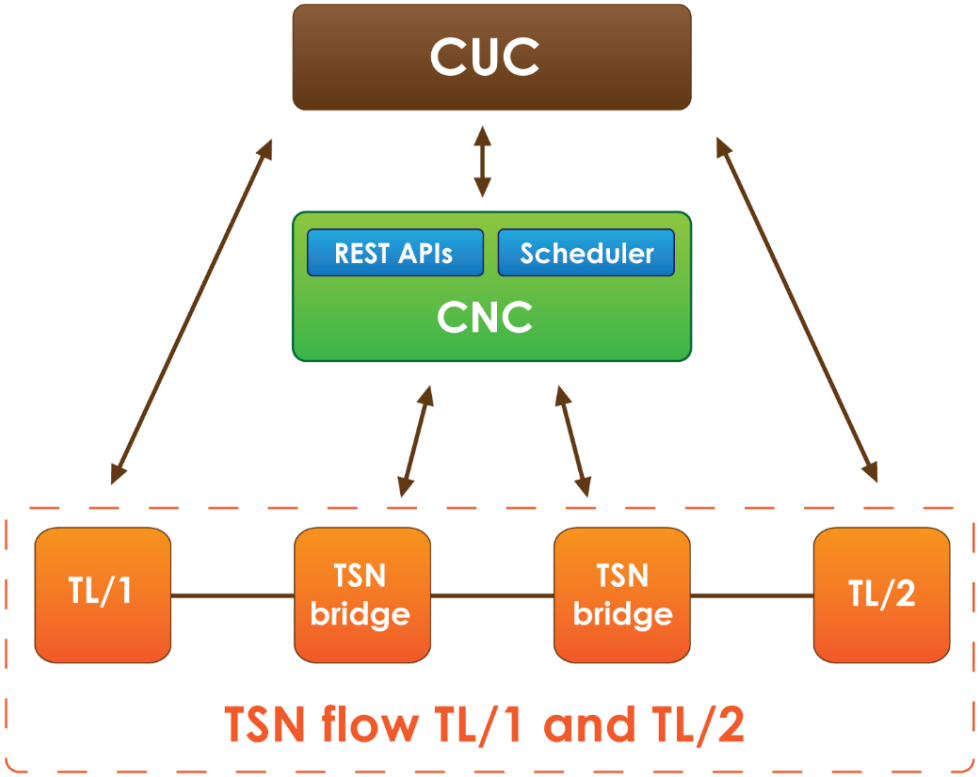
Nopeissa paikallisissa LAN-verkoissa voidaan julkaisija/tilaaja–mallia hyödyntäen saavuttaa reaaliaikainen tiedonsiirto TSN. Viestien täytyy olla vakiopituisia, -sisältöisiä ja sen tiedonsiirron täytyy kestää täsmälleen yhtä pitkän ajanjakson verkon jokaisessa solmukohdassa. Jokaisen TSN-verkon laitteen täytyy olla keskenään synkronoitu sekä niiden täytyy pystyä toimittamaan viesti lopulliselle vastaanottajalle. TSN mahdollistaa eri laitteiden reaaliaikaisen vuorovaikutuksen toistensa kanssa, joten se on tärkeä teknologia tulevaisuuden Teollinen Internet 4.0- ja IIoT-ratkaisuissa. (OPC Foundation, 2018)

B&R Industrial Automation on tuonut jo markkinoille TSN-väyläohjaimen, jonka avulla mikä tahansa OPC UA –asiakasohjelma voi ottaa reaaliaikaista dataa sen kautta. Valmistajille on tulevaisuudessa tärkeää, että koneiden kyky toteuttaa tietty prosessi ei rajoitu sen omiin ratkaisuihin, vaan myös muiden laitteiden reaaliaikaisiin tietoihin. B&R Industrial Automationin asiantuntijoiden mukaan on

maksimaalisen tuottavuuden kannalta tärkeää, että robotit, koneet ja kuljetinhihnat osaavat keskustella toistensa kanssa reaaliajassa. TSN on kehitteillä oleva joukko laajennuksia, jotka sisällytetään tulevaisuudessa Ethernet-standardiin IEEE 802.1. Tällä tavoitellaan mahdollisuutta reaaliaikaiseen tiedonsiirtoon Ethernetin kautta. TSN on jo käytössä moderneissa ajoneuvoissa, esimerkiksi välittämällä peruutuskameran kuvan Ethernetin välityksellä reaaliajassa. Autoteollisuuden mukaan tulo TSN:n käytössä on erinomainen asia, sillä näin komponentit ovat saatavilla nopeammin ja edullisemmin, mikä on ainakin kyseisen laitevalmistajan mieleen. Reaaliaikainen tieto teollisuusautomaatiossa tarjoaa riittävän tarkkuuden perustoimintojen ohjaukseen sekä jopa kuljetinhihnan toimintaan. (B&R Industrial Automation, 2015)

3.5 Cisco TSN Solution

Ciscon valmistama TSN-järjestelmä muodostuu sen IE-4000 –sarjasta, joka mahdollistaa satojen TSN-yhteyksien muodostamisen. Siihen kuuluvat kuvan 12 mukaisesti CUC (Centralized User Configuration), CNC (Central Network Controller) sekä kytkimet (bridge) ja päätelaitteet (TalkerListener, TL). Jokaiselle tiedonsiirrolle on tiukat aikataulutukset, joita verkkolaitteet noudattavat. CUC on ohjelmisto, joka kommunikoi CNC:n ja päätelaitteiden kanssa. CUC antaa komennon CNC:lle, joka tekee aikataulun ja reitin tiettyjen kytkimien kautta ja varaa liikennöintivuoron Ethernetistä. CNC muodostaa yksilöllisen tunnisteen jokaiselle TSN-yhteydelle (TSN flow) ja siirtää liikennöintitiedot tarvittaville kytkimille. Lähettäjä, Talker saa 13µs aikaikkunan, jonka aikana viesti lähetetään valmiiksi lasketun kytkinreitin kautta vastaanottajalle, Listenerille. Laitteen käyttäjä käyttää vain CUC:tä tietämättä edes CNC:n tai kytkimien toiminnasta kuten kuva 12 osoittaa. (Cisco)



KUVA 12. Ciscon esimerkki TSN-topologiasta (mukaillen Cisco)

3.6 OPC UA ja pilvipalvelut

Vuorovaikutus tietotekniikan ja automaatioteollisuuden välillä ei ole vallankumouksellisen uusi asia, vaan se perustuu pitkällä aikavälillä vakiintuneeseen kuvan 1 tuotantopyramidiin, jossa tieto kulkee kerroksesta seuraavaan. Teollinen Internet 4.0:n myötä nämä rajat alkavat häipyä ja sekoittua keskenään. Älykkäissä verkoissa jokainen laite tai palvelu voi itsenäisesti keskustella muiden palveluiden kanssa. Useiden ohjainvalmistajien muodostama PLC-open -järjestö yhteistyössä OPC-säätiön kanssa on kehitellyt OPC UA asiakassovellukselle oman ratkaisunsa. Siinä ohjain voi olla myös johtavassa roolissa tavanomaisen roolijaon lisäksi. Ohjain voi vaihtaa monimutkaista dataa horisontaalisesti muiden ohjainten kanssa, mutta myös keskustella OPC UA –palvelimen kanssa pyytääkseen MES- tai ERP-järjestelmältä uutta tilausta tai kirjoittaa tietoja pilveen. Tämä mahdollistaa tuotantolinjan itsenäistymisen, joka yhdessä OPC UA:n tietoturvan kanssa on avaintekijä Teollinen Internet 4.0:n tulevaisuudessa. (OPC Foundation, 2018)

Tietotekniikan näkökulmasta OPC UA on yhdistetyn tehtaan ohjelmointirajapinta. Se paitsi tarjoaa yhdyskäytävän pilvipalveluille, myös mahdollistaa tietojen ja laitteiden hallinnan sekä koneoppimisen sellaisille laitteille, joille se ei ole sisäänrakennettuna. Pilvipalvelut mahdollistavat maailmanlaajuiset, toimialakohtaiset SaaS-ratkaisut yrityksille, missä OPC UA toimii yhdyskäytävänä koko yrityksen tiedonsiirrolle. (OPC Foundation, 2018)

4 OPC UA ja tietoturva

Liiketoiminnan digitalisoituminen on tehnyt tietoturvasta entistä tärkeämmän turvallisessa kaupankäynnissä. Tietoturvallisessa ympäristössä laitteistot, ohjelmistot, tietoliikenneyhteydet sekä tiedot on suojattu fyysisesti, teknisesti ja toiminnallisesti. Tällaisessa tilanteessa uhat eivät aiheuta merkittävää riskiä liiketoiminnalle. Tietoliikenneyhteyksien vikaantuessa yrityksille aiheutuu merkittäviä haittoja, joten se asettaa yrityksille korkeat tavoitteet turvallisuutensa varmistamiseksi. Tietoturvan tarkoituksena on pyrkiä ehkäisemään erilaisten tietoturvauhkien aiheuttamat ongelmat. (Nykänen, 2014)

4.1 Tietoturvan osa-alueet

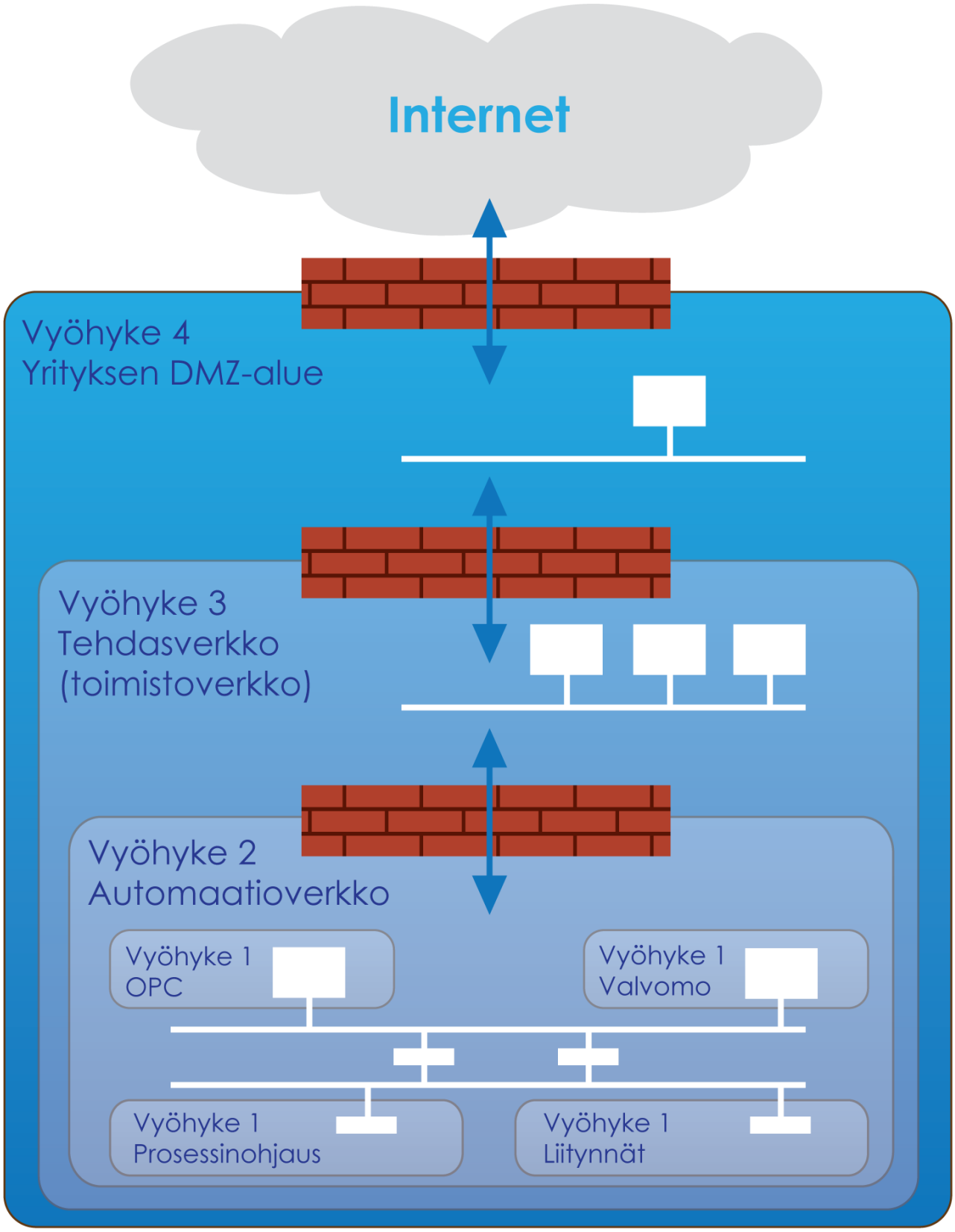
Tietoturvan tavoitteina voidaan pitää Suomen Automaatioseuran julkaisun mukaan luottamuksellisuutta, eheyttä, saatavuutta, kiistämättömyyttä ja seurantaa (Suomen Automaatioseura ry, 2010). Nykänen laajentaa tätä ajattelumallia seitsemään eri osa-alueeseen, joiden täyttyessä tietoturvallisuus toteutuu. Siihen vaaditaan luottamuksellisuutta, jolloin tietoja voivat käyttää vain siihen oikeutetut tahot. Eheyden toteutuessa tiedot pysyvät muuttumattomana syötön, käsittelyn ja tiedonsiirron aikana eivätkä ne saa hävitä missään tilanteessa. Todennuksella varmistetaan, että käyttäjät, tiedot sekä tapahtumat ovat niitä, joita sanovat olevansa. Kiistämättömyydellä tarkoitetaan sitä, että henkilö, laite tai tapahtuma ei voi kiistää tekemiään toimenpiteitä. Pääsynvalvonnassa rajoitetaan ja valvotaan käyttäjien pääsyä järjestelmiin. Saatavuuden saavuttamiseksi tiedot pitää olla helposti sekä viiveettä käyttäjiensä käytettävissä. Kaikki tapahtumat pitää myös olla jäljitettävissä, jotta pystytään selvittämään, mitä järjestelmässä on milloinkin tapahtunut ja kenen toimesta. (Nykänen, 2014)

4.2 Tietoturvallisuus teollisuusautomaatiossa

Perinteisemmät teollisuuden automaatiojärjestelmät on toteutettu suljetussa verkkoympäristössä, joten tietoturva ei ole ollut kovinkaan tärkeä asia yrityksille. Teollisuudessa verkottuminen yleistyy ja automaatiojärjestelmissä on alettu käyttää enemmän standardisoituja Ethernet-verkkoja. Standardiverkkojen sekä IP-teknologioiden lisääntyneen käytön ansiosta eri järjestelmät voivat integroitua huomattavasti helpommin. Samalla tietoturvariskit kasvavat, mihin yritysten olisi syytä kiinnittää aiempaa enemmän huomiota. (Suomen Automaatioseura ry, 2010)

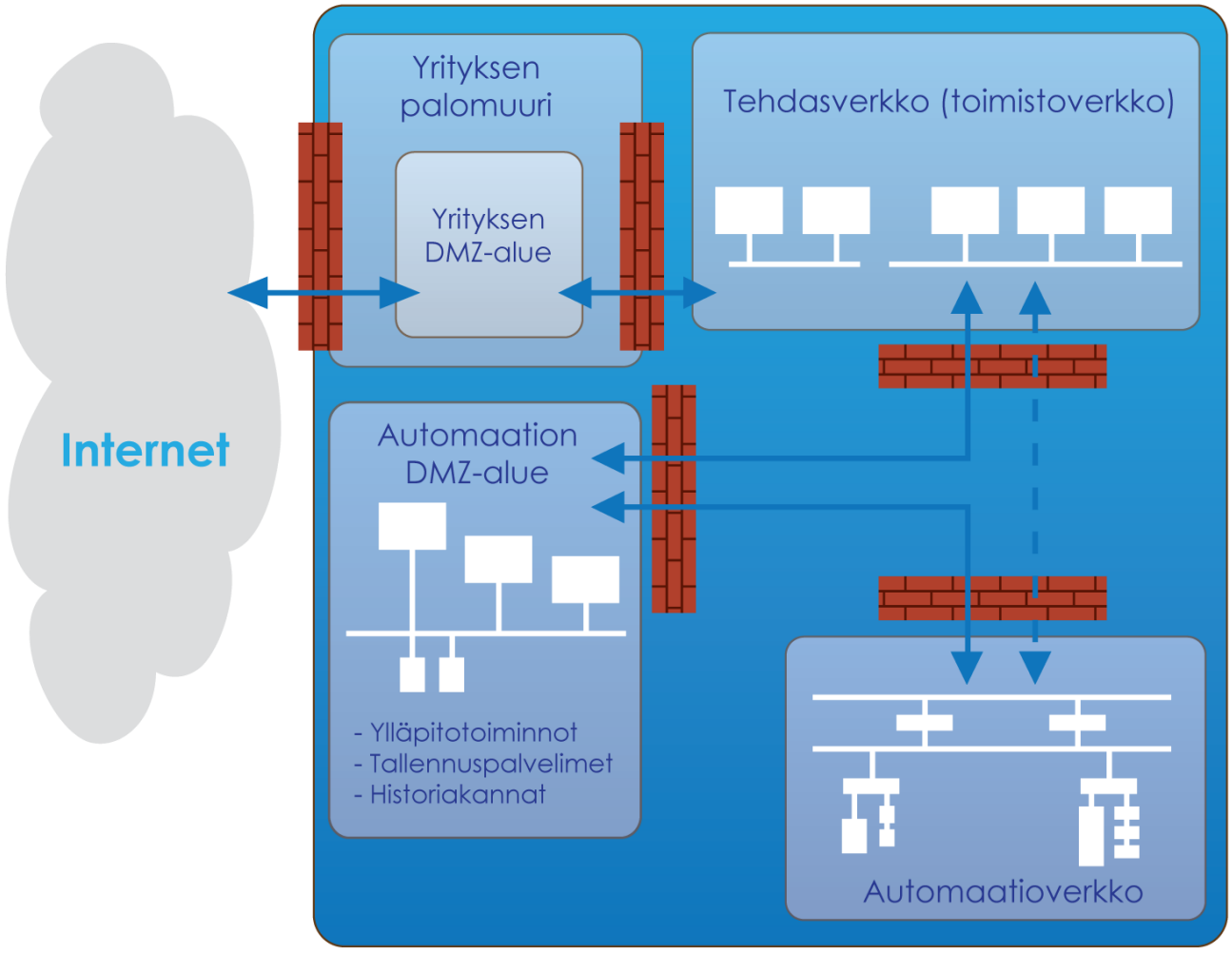
Automaatioverkko on vertikaalisen integraation vuoksi osa yrityksen koko verkkoa, jonka kautta avautuu mahdollisuus päästä käsiksi koko automaatiojärjestelmään. Erilaiset haittaohjelmat voivat haitata myös automaatiojärjestelmää aivan kuten perinteisemmin uhanalaiseksi luokiteltavaa toimiston lähiverkkoakin. Näin koko yrityksen tietoturva on uhattuna. Haavoittuvuus automaatiojärjestelmässä saattaa olla paljon vaarallisempi uhka liiketoiminnalle, ympäristöön tai jopa ihmisen terveydelle. Tämän päivän teollisuusautomaation vaatimukset suoraan pilveen yhdistettäville toimilaitteille sekä laitteiden reaaliaikaiseen keskinäiseen vuorovaikutukseen kasvattavat tietoturvariskiä entisestään. (Suomen Automaatioseura ry, 2010)

Teollisuusautomaatioverkon perushaasteina ovat toimistoverkon tavoin tietoturvan kannalta jatkuva ylläpito sekä muuttuvat tietoturvauhat. Tietoturvan hoitaminen voidaan jakaa ennalta ehkäisevään sekä tietoturvahäiriöiden hallintaan ja korjaamiseen. Ennalta ehkäisyn suurin mahdollisuus on hyvin tehdyssä järjestelmän suunnittelussa. Automaatiojärjestelmän täytyy havaita ja sietää mahdollisimman hyvin virhetoimintoja ja toipua nopeasti. Hyökkäykset voivat olla hyvin erilaisia, jopa tahattomia käyttäjävirheitä joten niiden aiheuttamat vahingot on syytä rajata mahdollisimman pienelle alueelle. Automaatioverkkojen suojaus tapahtuu perinteisiä menetelmiä soveltaen. Automaatioverkko voidaan esimerkiksi erottaa yrityksen muusta verkosta palomuurin avulla. Tällä tapaa voidaan ehkäistä toimistoverkon häiriön leviäminen ja eristää se automaatioverkosta. Syvyyssuuntaisessa suojauksessa saadaan tehostettua tietoturvaa jakamalla eri osa-alueet vyöhykkeisiin. Jokainen vyöhyke suojataan erikseen kuvan 13 mukaisesti. Toimenpiteet voivat olla teknisiä ratkaisuja, mutta myös prosesseja, ohjeita sekä koulutuksia, jotka edesauttavat tietoturvaa. (Suomen Automaatioseura ry, 2010)



KUVA 13. Syvyyssuuntaisessa suojauksessa käytetään useita suojausvyöhykkeitä (mukaillen Suomen Automaatioseura ry, 2010)

Tärkeimpiä asioita automaatioverkon suunnittelussa ovat segmentointi ja liikenteen rajoitus. Automaatioverkko täytyy erottaa omaksi verkkosegmentikseen muusta yrityksen verkosta tehokkaasti ja turvallisesti. Automaatio- ja tehdasverkon välinen liikenne tulisi tapahtua vain yhtä reittiä pitkin. Näin pystytään tehokkaasti valvomaan liikennettä eri segmenttien välillä. Kuvassa 14 demilitarisoitu alue, DMZ on fyysinen tai looginen aliverkko, joka muodostaa turvallisen alueen tiettyjen verkon segmenttien välille. DMZ on ylimääräinen tietoturvataso, jonka yli laitteet eivät voi muodostaa suoraa yhteyttä toisiinsa. Mikäli hyökkäys tehdasverkkoon onnistuisi, yhteys muihin segmentteihin katkeaisi. Näin tehtaan muu toiminta jatkuisi ennallaan. (Suomen Automaatioseura ry, 2010)



KUVA 14. Verkon segmentointi on yksi tietoturvallisuuden tärkeimmistä asioista (mukaillen Suomen Automaatioseura ry, 2010)

4.3 Turvallisuusuhat

OPC UA:a käytetään yrityksen tietojärjestelmien kaikilla tasoilla mukaan lukien pilvipalvelut, jolloin se on otollinen väylä tietoturvahyökkäyksille. OPC UA:ssa on tiettyjä menetelmiä, joilla tietoturva täyttyy kaikilla Nykäsen aiemmin mainituilla seitsemällä osa-alueella. Tiedon luotettavuus saavutetaan salaamalla tiedonsiirto ja eheys digitaalisella allekirjoituksella. Tietoturvamurtoja ja kuormitushyökkäyksiä estetään käyttäjien ja UA-sovellusten tunnistamisella sekä rajoittamalla käyttöoikeuksien avulla pääsy tietokantoihin. OPC UA –sovellukset keräävät tietoja tapahtumista, jolloin voidaan varmistaa tapahtumien kiistämättömyys ja tarkistaa UA-sovelluksen toiminta. Jo OPC UA:a määriteltäessä on tietoturva ollut tärkeässä roolissa, jolloin kaiken tyyppisiin tietoturvauhkiin on määritetty vastatoimenpide kuvan 15 mukaisesti. OPC Foundation on määritellyt tietoturvan osa-alueet vielä hieman eri tavalla Nykäseen verrattuna. (OPC Foundation, 2018)

	Todennus	Pääsynvalvonta	Luottamuksellisuus	Eheys	Varmennettavuus	Saatavuus	Kiistämättömyys
Palvelunesto-hyökkäys						✓	
Salakuuntelu	✓	✓	✓				
Viestihuijaus		✓					
Viestin muuntaminen	✓	✓		✓	✓		✓
Viestin toisto	✓	✓					
Epämuodostuneet viestit						✓	
Palvelimen profilointi	✓	✓	✓	✓	✓	✓	✓
Järjestelmän kaappaus	✓	✓	✓	✓	✓	✓	✓
Väärennetty palvelin	✓	✓	✓		✓	✓	
Käyttäjätietojen kaappaaminen	✓	✓	✓				
Kiistäminen							✓

KUVA 15. Vastatoimenpiteet eri tyyppisille tietoturvauhille (mukaillen OPC Foundation, 2018)

4.3.1 Kuormitushyökkäys

Kuormitushyökkäyksessä (Message flooding) kohteeseen lähetetään useita viestejä peräkkäin tai yksi useita pyyntöjä sisältävä viesti. Sen tarkoituksena on ylikuormittaa hyökkäyksen kohdetta kuluttamalla sen tarvitsemia resursseja, kuten prosessoria, tiedosto- tai käyttöjärjestelmää. Hyökkääjä voi esimerkiksi lähettää viestin kohteelle ja väärentää lähettäjän IP-osoitteen. Hyökkäyksen kohdepalvelin yrittää vastata väärään IP-osoitteeseen useita kertoja sitä koskaan saavuttamatta, jolloin palvelimen muisti voi täyttyä ja verkkoliikenne tukkiutua. OPC UA minimoi viestien prosessointia ennen autentikointia varmistaakseen tietojen saatavuuden. Ennen autentikointia suoritetaan vain vähän resursseja kuluttava GetEndPoints-palvelu sekä hieman enemmän suorituskykyä kuormittava OpenSecureChannel-palvelu. Siinä palvelinta kuormitetaan allekirjoitus- sekä salaustoimenpiteillä. Palvelin suojautuu tältä, kun se on saanut tietyn verran epäkelpoja OpenSecureChannel-pyyntöjä sekä lähettää hälytysviestin hyökkäysyrityksestä. Julkaisija/tilaaja–mallissa tilaaja suodattaa sellaiset viestit pois, minkä otsikkotiedot eivät ole kunnossa. Myös allekirjoitus tarkistetaan viesteistä, jolloin hyvin muodostetut, mutta SecurityGroupiin kuulumattomien lähettäjien viestit hylätään. (OPC Foundation, 2018)

4.3.2 Viestin muuntaminen

Viestin muuntamisessa (Message alteration) yleensä salakuuntelun ohessa hyökkääjä kaappaa viestin, muokkaa sitä ja lähettää sen OPC UA –asiakassovellukselle tai –palvelimelle. Tällä pyritään saamaan esimerkiksi pääsy palvelimelle tai lisätietoja sovelluksesta. OPC UA:ssa on mahdollista allekirjoittaa viestit, jotka kulkevat asiakasohjelman ja palvelimen välillä. Allekirjoituksen tarkistus havaitsee viestiin tehdyt muutokset ja hylkää sen, mikäli se ei ole säilyttänyt viestin eheyttä. (OPC Foundation, 2018)

4.3.3 Viestihuijaus

Viestihuijauksessa (Message spoofing) hyökkääjä lähettää väärennetyn viestin hyökättävään kohteeseen. Hyökkääjä voi myös muokata aiemmin kaappaamaansa viestiä hyökkäyksen uhrille sopivaan muotoon esimerkiksi esiintymällä toisena henkilönä. OPC UA:ssa tämä ehkäistään allekirjoittamalla viestit sekä niiden mukana kulkevien tunnistetietojen avulla. Tunnistetietojen mukana siirtyy tiedot käytetystä istunnosta, kanavasta sekä palvelupyynnöstä. On tärkeää, että tunnistetiedoista istunnon tunnus, SessionId valitaan satunnaisesti, eikä sitä aseteta nollaan tai muuhun helposti

arvattavaan numeroon. Myös julkaisija/tilaaja–mallissa käytetään viestien allekirjoitusta sekä erilaisia tunnistetietoja viestihuijauksien ehkäisemiseksi. (OPC Foundation, 2018)

4.3.4 Viestin toisto

Viestin toistossa (Message replay) alkuperäistä viestiä ei muuteta, vaan se lähetetään uudelleen alkuperäisenä. Tällaisen hyökkäyksen tarkoituksena on sekoittaa jonkin järjestelmän toiminto. Esimerkiksi robotin tietyn liikkeen toistaminen monta kertaa peräkkäin saattaa aiheuttaa vakavia haittoja. OPC UA:ssa viestin allekirjoituksen sekä tunnistetietojen tulkinnan avulla tämä on tehty lähes mahdottomaksi. Julkaisija/tilaaja–mallissa ei koskaan tulisi ottaa viestistä kenttiä pois käytöstä, kuten aikaleimaa tai viestin numeroa, vaikka se mahdollista onkin. (OPC Foundation, 2018)

4.3.5 Epämuodostunut viesti

Hyökkääjä voi lähettää epämuodostuneen viestin (Malformed message), jolla yritetään häiritä kohteen järjestelmän toimintaa. Viesti voi olla epämuodostunut XML- tai SOAP-viesti, jolloin vastaanottaja voi tulkita sen suorittavan laittomia operaatioita. Hyökkäyksen kohde voi näin kuluttaa ylimääräisiä resursseja viestin tulkitsemiseen ja palvelin saattaa jopa kaatua. Määrittelyiden mukaisesti OPC UA -palvelimet ja asiakasohjelmat tulisi rakentaa siten, että viestien muoto sekä parametrien laillisuus tarkistettaisiin mahdollisimman aikaisessa vaiheessa. (OPC Foundation, 2018)

4.3.6 Palvelimen profilointi

Hyökkääjä voi myös yrittää profiloida kohdesovellusta, jotta selviäisi sille ominaiset tietoturva-aukot. Palvelimen profilointia (Server profiling) saattaa auttaa esimerkiksi tieto kohdesovelluksen versiosta, tyypistä tai myyjästä. OPC UA -palvelimissa rajoitetaan tunnistamattomille asiakkaille lähetetyn tiedon määrä. Näin vain tunnistetut käyttäjät ja sovellukset pääsevät käsiksi sovelluksen tietoihin. (OPC Foundation, 2018)

4.3.7 Väärennetty palvelin tai julkaisija

Hyökkääjä voi myös toimia jonkin järjestelmän väärennettynä palvelimena tai julkaisijana (Rogue server of publisher) ja selvittää tietoja kommunikoivista käyttäjistä ja asiakasohjelmista. Hyökkääjä voi saada selville myös käyttäjätunnuksia ja salasanoja. Kommunikoivat OPC UA –sovellukset käyttävät sovellusten tunnistamiseen varmennettavia sertifikaatteja. Väärennetyn palvelimen tai julkaisijan käyttäessä omaa sertifikaattiaan, sitä ei voida varmentaa ja asiakasohjelma katkaisee yhteyden. Sertifikaattiin liittyy myös yksityinen avain, joten väärennetty palvelin ei voi käyttää luotetun UA-palvelimen sertifikaattia. Tästä johtuen se ei voi allekirjoittaa viestejään eikä myöskään tulkita niitä. Julkaisija/tilaaja–mallissa tilaajasovellukset vahvistavat julkaisijan tarkistamalla allekirjoituksen. (OPC Foundation, 2018)

4.3.8 Käyttäjätietojen kaappaaminen

Hyökkääjä voi yrittää myös saada selville jonkin sovelluksen tai järjestelmän käyttäjätunnuksia (Compromising user credentials), salasanoja tai muita salaisia tietoja. Näitä tietoja voidaan yrittää saada kaappaamalla palvelimen ja asiakassovelluksen välisiä viestejä. Vaikka viesti saataisiin kaapattua, OPC UA:ssa viestit voidaan salata, jolloin käyttäjätietoja ei saada selvitettyä viestistä. (OPC Foundation, 2018)

4.3.9 Salakuuntelu

Hyökkääjä voi yrittää poimia verkon yli tapahtuvasta liikenteestä viestejä salakuuntelemalla (Eavesdropping), mistä ilmenisi luottamuksellista tietoa yrityksestä. OPC UA:ssa liikennöinti voidaan salata symmetrisillä tai asymmetrisillä salaustekniikoilla, jolloin viestien tulkitseminen vaikeutuu. (OPC Foundation, 2018)

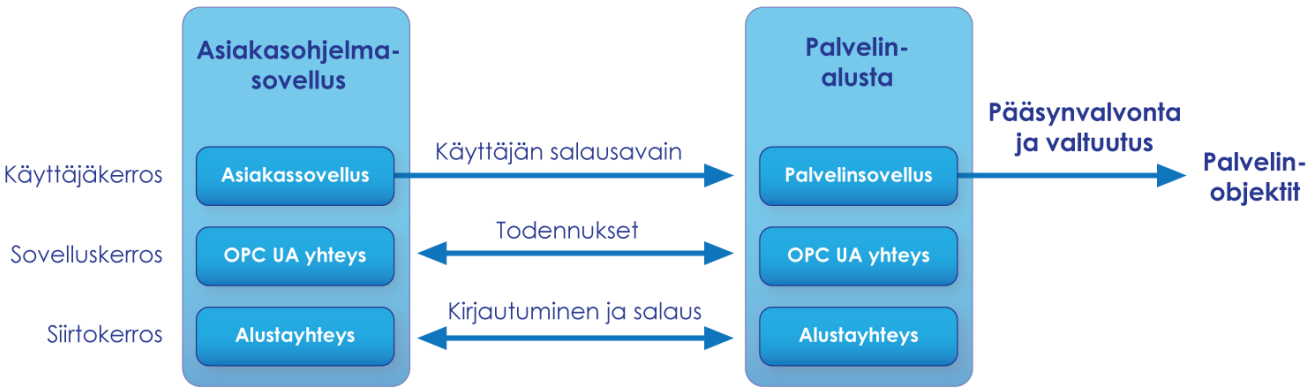
4.3.10 Istunnon kaappaaminen

Kahden OPC UA –sovelluksen välinen istunto voidaan myös yrittää kaapata (Session hijacking) hyödyntäen aikaisemmin saatuja tietoja, kuten UA-sovellusten välillä kulkevia viestejä. Hyökkääjä

pyrkii lisäämään istuntoon kelvollisia viestejä, joiden avulla hyökkääjä voisi kaapata istunnon. Kaappauksen onnistuttua hyökkääjä pääsisi käsiksi palvelimen tarjoamiin tietoihin sekä suorittamaan UA-palvelimen tarjoamia palveluita. OPC UA -istunnon viestit voidaan kuitenkin kuljettaa salattuna tietoturvattua kanavaa pitkin. Tästä johtuen hyökkääjä tarvitsisi koko OPC UA –tietoturvakontekstin kaapatakseen istunnon. (OPC Foundation, 2018)

4.4 Tietoturvan toteutus OPC UA:ssa

Tietoturva oli OPC UA:n perusvaatimus, joten se otettiin mukaan jo toteutusvaiheessa. Turvamekanismeiksi valittiin suojautumiskeinot jokaiselle tietoturvan osa-alueelle. OPC UA voidaan jakaa kolmeen suojauskerrokseen kuvan 16 osoittamalla tavalla, mikä on yhteneväinen muiden internet-pohjaisten alustojen kanssa. Käyttäjä-kerroksessa turvatoimet aloitetaan istunnon alkaessa. UA-asiakassovellus lähettää salatun suojausavaimen, jonka avulla käyttäjä tunnistetaan UA-palvelimella ja se antaa luvan käyttäjälle tarkoituksenmukaisiin objekteihin. Sovellus-kerroksessa siirtyvät digitaaliset allekirjoitukset ja sillä todennetaan asiakassovellukset, palvelimet sekä viestit. Siirtokerroksessa voidaan varmistaa eheys viestien allekirjoituksesta sekä luottamuksellisuus viestin salauksesta. Tällä estetään viestien salakuuntelut sekä väärennökset. OPC UA:n turvamekanismit on toteutettu osana OPC UA –pinoja, joten ne ovat käytettävissä suoraan UA-palvelimissa sekä -asiakassovelluksissa. Turvamekanismit käyttävät laitteiston resursseja, joten se saattaa vaikuttaa järjestelmän suorituskykyyn. OPC UA:ssa määritellään eri suojaustasot, joten toimittajat voivat valmistaa eri suorituskykyisiä laitteita. UA-asiakasohjelmat voidaan myös ohjelmoida käyttämään vain tietyn suojatason päätepisteitä, jotta arkaluontoiset tiedot siirtyvät turvallisesti. (OPC Foundation, 2018)



KUVA 16. OPC UA:n suojauskerrokset (mukaillen OPC Foundation, 2018)

5 JOHTOPÄÄTÖKSET

OPC UA soveltuu mainiosti ohjainten, laitteiden sekä automaatiojärjestelmien väliseen kommunikointiin. Se taipuu myös mobiiliympäristöön sekä globaaliin verkkojen ja tehtaiden väliseen tiedonsiirtoon. OPC UA on yhteistyön taidonnäyte, kun toimialan eri valmistajat luovat yhdessä standardeihin perustuvan kommunikointiprotokollan. Tällä on saatu aikaan avoin, tietoturvallinen ja skaalautuva protokolla. Tietoturvallisuus tulee olemaan tulevaisuuden pilveen kytkettyjen älykkäiden laitteiden suurimpia haasteita. OPC UA:n jo alusta asti mukana kehitetty tietoturvamalli on vahva vastine erilaisille uhille, mutta se vaatii myös asiantuntijuutta toimiakseen suunnitellulla tavalla. Pelkästään tietoturvan laaja-alaisuus tekee UA:sta monimutkaisen, joten sen käyttöönoton haasteita ei pidä väheksyä. OPC UA yleistyy tulevaisuudessa myös sen skaalautuvuuden ja avoimuuden ansiosta. Kommunikointi turvallisesti suoraan eri laitteiden välillä tuo mielenkiintoisia mahdollisuuksia tulevaisuuden älykkäisiin tehtaisiin.

Vaikka UA julkaistiinkin ensimmäisen kerran jo vuonna 2006, kehittyy se edelleen tarpeiden mukaan. Mielenkiintoista on nähdä, mitä julkaisija/tilaaja–malli yhdessä TSN:n kanssa mahdollistaa, kun reaaliaikainen tiedonsiirto toteutuu.

LÄHTEET

B&R Industrial Automation. 2015. TSN – A turbo charge for OPC UA? Saatavissa: https://www.br-automation.com/en-us/about-us/customer-magazine/2015/201511/tsn-a-turbo-charge-for-opc-ua/. Viitattu 27.2.2019.

Cisco. Time-Sensitive Networking: A Technical Introduction. Saatavissa: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-c11-738950.pdf. Viitattu 19.3.2019.

Fu, Arron. 7 Different Types of Cloud Computing Structures. Julkaistu 3.3.2017. Saatavissa: https://www.uniprint.net/en/7-types-cloud-computing-structures/. Viitattu 16.3.2019.

Inductive automation. What is SCADA? Julkaistu 12.9.2018. Saatavissa: https://inductiveautomation.com/resources/article/what-is-scada. Viitattu 18.3.2019.

Karimi, S. What Is Cloud Computing, In Simple Terms? Julkaistu 17.6.2018. Saatavissa: http://didarc.com/en/news/what-is-cloud-computing%2Cin-simple-terms%3F. Viitattu 2.3.2019.

Lassila, T. 2019. Pilvialustojen selvitys. Savonia.

Microsoft Azure. What is cloud computing? Saatavissa: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/. Viitattu 2.3.2019.

National Instruments. Why OPC UA Matters. Julkaistu 19.5.2017. Saatavissa http://www.ni.com/white-paper/13843/en/. Viitattu 27.2.2019.

Novotek. OPC ja OPC UA. Saatavissa: https://www.novotek.com/fi/ratkaisut/kepware-kommunikointialusta/opc-ja-opc-ua. Viitattu 27.2.2019.

Nykänen, Pirkko. Tietoturva – tietosuoja tietojärjestelmien suunnittelussa. Sovelluskehityksen tietoturvaohje. Valtiovarainministeriö. Julkaistu 17.3.2014. Saatavissa: http://www.uta.fi/sis/tie/tjsum/index/TJSUM_Luento6_2014_PirkkoNyk%C3%A4nen.pdf. Viitattu 28.3.2019.

OPC Foundation. Saatavissa: https://opcfoundation.org/. Viitattu 16.3.2019.

OPC Foundation. Interoperability for Industrie 4.0 and the Internet of Things. 2018. Saatavissa: https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf. Viitattu 29.3.2019.

OPC Foundation. OPC Foundation Announces support of Publish / Subscribe for OPC UA. Julkaistu 4.6.2016 Saatavissa: https://opcfoundation.org/news/opc-foun-dation-news/opc-foundation-announces-support-of-publish-subscribe-for-opc-ua/. Viitattu 17.3.2019.

OPC UA Specification Part 2: Security Model. Päivitetty 3.8.2018

OPCConnect. History of OPC. Saatavissa: https://www.opcconnect.com/history.php. Viitattu 16.3.2019.

Peltokangas, T. & Känsäkoski, J. 2017. OPC UA -arkkitehtuurin toteutus ja testaus teollisuusautomaatiossa. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/140754/ISBN%20978-952-7173-31-2.pdf?sequence=1&isAllowed=y. Viitattu 27.2.2019.

Prosys. OPC UA turvallisempaan ja helpompaan järjestelmäintegraatioon. Saatavissa: https://prosys.fi/brochures/proMaint1204.pdf. Viitattu 17.3.2019.

Pyyskänen, Seppo. Teollisuuden automaatio- ja ohjausjärjestelmät. Saatavissa: https://www.automaatioseura.fi/site/assets/files/1367/standardikirja.pdf. Viitattu 18.3.2019.

Real Time Automation. OPC UA Overview. Saatavissa: http://www.rtautomation.com/technologies/opcua/. Viitattu 27.2.2019.

Solomon, John. Understanding different types of cloud computing and their benefits. Julkaistu 25.5.2018. Saatavissa: https://www.chargebee.com/blog/understanding-types-cloud-computing/. Viitattu 2.3.2019.

Suomen Automaatioseura ry. 2010. Teollisuusautomaation tietoturva - Verkottumisen riskit ja niiden hallinta. Helsinki.