



samk

Satakunnan ammattikorkeakoulu  
Satakunta University of Applied Sciences

SAMI RISTOLAINEN

**Miten OPC UA protokollaa voidaan hyödyntää datan keruun ja systemien tiedonsiirron välillä laivassa.**

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN TUTKINTO-  
OHJELMA  
2024

## TIIVISTELMÄ

Ristolainen, Sami: Miten OPC UA protokollaa voidaan hyödyntää datan keruun ja systeemien tiedonsiirron välillä laivassa.

Opinnäytetyö, AMK

Sähkö- ja automaatiotekniikka

Tammikuu 2024

Sivumäärä: 44

Opinnäytetyön tarkoitus on kuvailla, miten OPC UA protokollaa voidaan hyödyntää datan keruussa ja tiedonsiirrossa laivassa. Tarve opinnäytetyön käsittelemään aiheeseen on tullut laivojen järjestelmien kehittymisen ja kyberturvallisuuden lisääntyessä. Lähdeaineistona ja tiedon hankintaan käytettiin sähköalan lakeja, standardeja, laitevalmistajan ohjeita, virallisia nettisivuja ja tutkimuksia aiheesta sekä sisäisiä ohjeita. Työn toimeksiantajana toimii Meyer Turku Oy.

OPC UA on tietoliikenneprotokolla, joka on avoimen lähdekoodin standardi tiedonsiirtoon teollisuudessa automaatioissa. Opinnäytetyössä käydään läpi OPC UA:n keskeiset käsitteet ja miten sitä voidaan hyödyntää datan keruussa ja tiedonsiirrossa laivassa. Esimerkkeinä on käytetty verkosta löytyneitä tutkimuksia, joita ovat suorittaneet laivanrakennusalan ammattilaiset. Testien ja teorian perusteella voidaan tehdä johtopäätös, että OPC UA on toimiva viestintäprotokolla laivoissa käytettävään datan keruuseen ja tiedonsiirtoon eri järjestelmien välillä.

OPC UA:n käyttö laivassa tulee tulevaisuudessa lisääntymään. Useat yritykset, jotka toimivat laivateollisuudessa, kuten ABB, Schneider Electric, Valmet, Siemens ja CISCO ajavat OPC UA:n käyttöä TSN yleisenä rajapintana ja ovat mukana protokollan kehittämisessä. Toisaalta vaikka OPC UA on teoriassa toimiva ja osittain testattu protokolla laivan tiedonsiirron ja datan keruun parantamiseen, siihen liittyy riskejä. Esimerkiksi onko rahallinen tuotto tarpeeksi investointiin nähden, jos viestintäprotokollaa muutettaisiin OPC UA:n spesifi-kaatioksi.

Avainsanat: OPC UA, Viestintäprotokolla, Data, Tiedonsiirto

## ABSTRACT

Ristolainen, Sami: How the OPC UA protocol can be utilized between data collection and system data transfer on ships.

Bachelor's thesis

Electrical and automation engineering

January 2024

Number of pages: 44

The purpose of the thesis is to describe how the OPC UA protocol can be used in data collection and data transfer on board. The need for the subject discussed in the thesis has come with the development of ship systems and the increase in cyber security. Electricity industry laws, standards, equipment manufacturer's instructions, official websites and studies on the subject, as well as internal instructions were used as source material and for the acquisition of information. The client of the work is Meyer Turku Oy.

OPC UA is a communication protocol that is an open source standard for data transfer in industrial automation. The thesis examines the key concepts of OPC UA and how it can be used in data collection and data transfer on board. As examples, studies found on the web, which have been carried out by professionals in the shipbuilding and manufacturing industry, have been used. Based on tests and theory, it can be concluded that OPC UA is a functional communication protocol for data collection and data transfer between different systems used in ships.

The use of OPC UA on board will increase in the future. Several companies that operate in the shipping industry, such as ABB, Schneider Electric, Valmet, Siemens and CISCO, promote the use of OPC UA as a common interface to TSN and are involved in the development of the protocol. On the other hand, although OPC UA is a theoretically functional and partially tested protocol for improving ship communication and data collection, there are risks associated with it. For example, is the financial return enough compared to the investment, if the communication protocol were to be changed to the OPC UA specification.

Keywords: OPC UA, Communication protocol, Data, Data transfer

# SISÄLLYS

1 JOHDANTO .....	6
1.1 Tutkielman tausta .....	7
1.2 Meyer Turku Oy.....	8
2 OPC UA .....	9
2.1 OPC Classic .....	10
2.2 OPC UA:n arkkitehtuuri .....	11
2.2.1 Tietomalli .....	14
2.2.2 Osoiteavaruus.....	16
2.3 Kyberturvallisuus .....	18
2.3.1 Kyberturvallisuuden arkkitehtuuri.....	20
3 OPC UA EDUT .....	22
3.1 Keskeiset ominaisuudet.....	23
3.2 Mikä erottaa OPC UA:n kilpailijoista .....	25
4 TIEDONSIIRTO SYSTEEMIEN VÄLILLÄ LAIVOISSA.....	26
4.1 OPC UA tiedonsiirto eri valmistajien välillä.....	27
4.2 Kyberturvallisuus tiedonsiirrossa .....	29
4.3 Verkkoratkaisut.....	29
5 DATAN KERÄÄMINEN LAIVASSA.....	30
5.1 Esimerkkejä OPC UA:n käytöstä datan keruussa laivoissa.....	33
5.1.1 Meyer Turku ja Semantum .....	33
5.1.2 MSC Cruises.....	37
6 YHTEENVETO.....	38
LÄHTEET .....	40

## LYHENNELUETTELO

<b>AE</b>	Alarms and Events
<b>AMQP</b>	Advanced Message Queuing Protocol
<b>COM</b>	Component Object Model
<b>CPMT</b>	Cyber-Physical Machine Tools
<b>DA</b>	Data Access
<b>DCOM</b>	Distributed Component Object Model
<b>DCS</b>	Distributed Control System
<b>ERP</b>	Enterprise Resource Planning
<b>HDA</b>	Historical Data Access
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IACS</b>	International Association of Classification Societies
<b>IEC</b>	International Electrotechnical Commission
<b>IMO</b>	International Maritime Organization
<b>IO</b>	Input/Output
<b>IDPS</b>	Intrusion Detection Prevention System
<b>IDS</b>	Intrusion Detection System
<b>IPS</b>	Intrusion Prevention System
<b>ISA</b>	International Safety of Automation
<b>IIoT</b>	Industrial Internet of Things
<b>JSON</b>	JavaScript Object Notation
<b>MES</b>	Manufacturing Execution System
<b>MQTT</b>	Message Queuing Telemetry Transport
<b>PLC</b>	Programmable Logic Controller
<b>SOAP</b>	Simple Object Access Protocol
<b>SOLAS</b>	International Convention for the Safety of Life at Sea
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TSN</b>	Time-Sensitive Networking
<b>UA</b>	Unified Architecture
<b>WLAN</b>	Wireless Local Area Network
<b>XML</b>	Extensible Markup Language

## 1 JOHDANTO

Opinnäytetyö on tehty Meyer Turku Oy:lle. Meyer Turku on yksi maailman suurimmista ja modernimmista telakoista maailmassa. Telakalla rakennetaan maailman uudenaikaisempia, innovatiivisimpia ja ympäristöystävällisimpiä risteilyaluksia, autolauttoja ja erikoisaluksia. Meyer Turku Oy:n osuus maailman risteilyrakentamisesta on noin 15 prosenttia, ja tilauskanta ulottuu vuoteen 2026 opinnäytetyötä tehtäessä. Meyer Turku Oy työllistää noin 2 000 työntekijää ja rakennettuja aluksia on Turun telakan historian aikana tehty 1 300 (Meyer Turku Oy, 2023).

Opinnäytetyön aihe on syntynyt kehitysideana, miten OPC UA protokollaa voidaan hyödyntää laivassa datan keruun ja systeemien tiedonsiirron välillä. Kehitysideana on luoda tutkielma, miten OPC UA protokollaa voidaan käyttää laivassa ja miten se vaikuttaa suunnittelutyöhön, tuotannon käyttöönottoon – etenkin ajallisesti – ja parantaa kyberturvallisuutta laivassa. Tutkielman tarkoituksena on antaa järjestelmien suunnittelijoille yleinen kuvaus OPC UA:sta ja miten sen käyttöä voidaan soveltaa laivassa datan keruussa ja tiedonsiirrossa.

Aihe on erittäin laaja, joten aihe on rajattu käsittelevän pääosin tiedonsiirtoa ja datan keruuta järjestelmien välillä, ja mitä hyötyjä sillä on kyberturvallisuuteen. Vaikka opinnäytetyö on tarkoitettu avuksi suunnittelutyössä, se ei kuitenkaan ole työohje, vaan yleinen kuvaus suunnittelijan vastuusta OPC UA protokollan käytöstä laivan verkkoratkaisuiden osana.

## 1.1 Tutkielman tausta

Meyer Turun telakalla pyritään pysymään kilpailijoiden edellä korkean teknologian osaamisen avulla ja OPC UA protokolla edes auttaa tavoitteessa. Tutkielman tarkoituksena on saada valmiiksi dokumentti, jossa käsitellään järjestelmä suunnitelman kannalta välttämättömät lait, standardit, määräykset ja vaatimukset eri laitteiden ja järjestelmien välillä.

## 1.2 Meyer Turku Oy

Meyer Turku Oy on osa Meyer Groupia, jossa on mukana 20 partneriyritystä. Meyer Turku Oy toimii Turun telakalla, jossa on valmistettu laivoja vuodesta 1737. Meyer Turku Oy:lla on kolme tytär yritystä: hyttitehdas Piikkiö Works Oy, laivanrakennus- ja offshore-alan suunnitteluyritys ENG´nD Oy ja kokonaistoimituksia laivojen yleisiin tiloihin tarjoava Shipbuilding Completion Oy. Meyer Group valmistaa ja suunnittelee maailman esityksellisimpiä risteilyaluksia, jorkilaivoja ja matkustaja autolauttoja, jotka räätälöidään vastaamaan asiakkaiden tarpeisiin (Meyer Turku Oy, 2023).

Meyer Group on perheyritys, joka on toiminut vuodesta 1795 Willm Rolf Meyer perusti Meyer Werft –telakan Papenburgiin, Saksaan. Meyer Group osti yhdessä Suomen valtion kanssa Turun telakan vuonna 2014 korealaiselta STX:ltä (Pietiläinen, 2014).

## 2 OPC UA

Teollisuus ja automaatio kehittyvät jatkuvasti. Siirtyminen teollisuusautomaatiosta (Teollisuus 3.0) teolliseen internetiin (Teollisuus 4.0) ja teollisen esineiden internettiin (IIoT) ovat tuottaneet haasteita, joihin perinteiset viestintäprotokollat eivät pysty vastaamaan. Teollisuus 4.0 kehityksen myötä automaatiotekniikassa on kehittynyt keskeinen haaste taata turvallinen ja standardoitu tiedonsiirto koneiden ja palveluiden välillä. OPC UA on suunniteltu vastaamaan tähän haasteeseen. OPC UA on standardoitu IEC 62541 –standardin mukaisesti, mikä muuttui huhtikuussa 2015 suositukseksi viestintäkerroksen toteuttamiseen. IEC eli International Electrotechnical Commission on kansainvälinen sähköalan standardointiorganisaatio. Sen tarkoituksena on taata elektroniikka- ja sähkölaitteiden turvallisuus ja hyötysuhde mahdollisimman hyväksi. IEC:llä on yli 10 000 standardia ja yli 170 maata mukana organisaatiossaan (beckhoff.com, 2023; epicor.com, 2023; Jasperneite & Lohveg, 2018, s. 232; IEC.ch, 2024).

OPC UA eli Open Platform Communications Unified Architecture on vuonna 2008 julkaistu alustariippumaton palvelukeskeinen arkkitehtuuri, joka yhdistää OPC Classic –määritysten toiminnot yhdeksi kehikseksi. OPC Foundation julkaisi standardinsa ensimmäistä kertaa vuonna 1996. Sillä oli tarkoituksena tiivistää PLC –spesifiset protokollat, kuten Modbus, standardoiduksi rajapinnaksi (opcfoundation.com, 2023).

## 2.1 OPC Classic

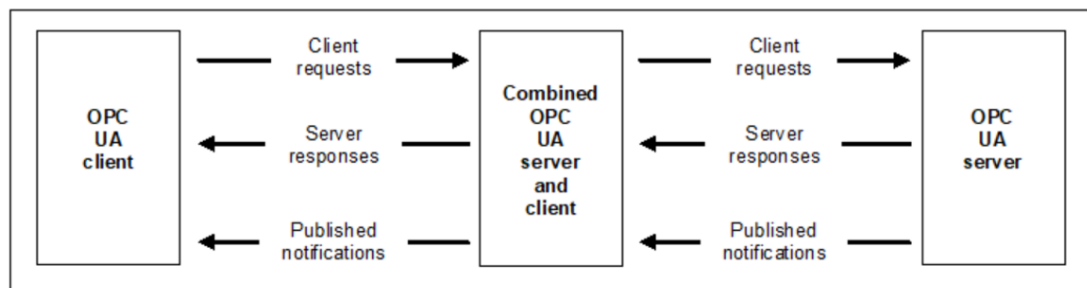
OPC Classic spesifikaatiot perustuvat Microsoft Windows –tekniikkaan. Se käyttää COM/DCOM –tekniikkaa tietojen vaihtoon ohjelmistokomponenttien välillä. OPC Classicin spesifikaatio määrittelee erilaiset määritelmät prosessidatan, hälytyksien ja historian tietojen käsittelylle. Lyhyesti nämä kolme spesifikaatiota ovat järjestyksessä OPC DA (Data Access), OPC AE (Alarms and Events) ja OPC HDA (Historical Data Access). OPC DA –spesifikaatio määrittää tiedon vaihdon, mukaan lukien arvot, aika- ja laatutiedot. OPC DA toimii perusprotokollana, joka siirtää tiedot ohjausjärjestelmistä muihin järjestelmiin. OPC AE –spesifikaatio määrittelee hälytys- ja tapahtumatyyppeviestien tietojen vaihdon sekä muuttuvien tilojen ja tilanhallinnan. Se eroaa OPC DA:sta siten, että tapahtumilla ei ole nykyistä arvoa. Käytännössä protokolla on aina palvelu, jossa asiakas saa kaikki tapahtumat tietoonsa. OPC HDA –spesifikaatio määrittelee kyselymenetelmät, analytiikan, joita voidaan soveltaa historiaan ja aikaleimattuihin tietoihin. Ero muihin spesifikaatioihin on, että OPC HDA sisältää historiallisia tietoja ja voi käsitellä suurempaa määrää tietoja kerralla (opcfoundation.org, 2023).

OPC-standardia käytetään yleisesti PC –valvomoiden ja ohjelmoitavien logiikoiden välillä. Standardi on alan toimijoiden, kuten toimittajien, loppukäyttäjien ja ohjelmistokehittäjien spesifikaatiosarja. Spesifikaatiosarja määrittelee asiakkaiden ja palvelimien välisen rajapinnan (opcfoundation.org, 2023).

## 2.2 OPC UA:n arkkitehtuuri

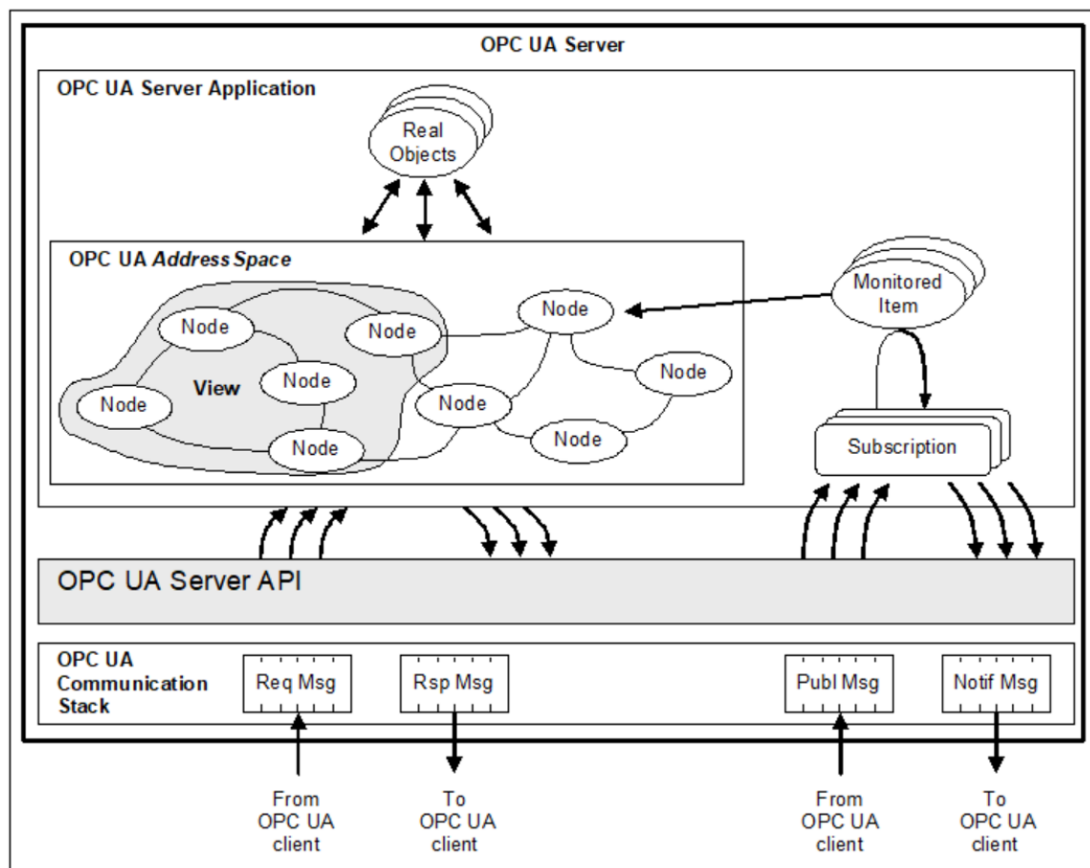
OPC UA protokollan peruseriaate on integroida ja automatisoida monimutkaisia järjestelmiä eri teollisuuden aloilla ja standardisoida kommunikaatio protokolla yhteiseksi. OPC UA käyttää joustavaa, laajennettavaa tietomallia, ja skaalautuvaa, turvallista ja luotettavaa siirtomenetelmää yhteensopivuuden helpottamiseksi eri valmistajien laitteiden ja järjestelmien välillä. Tietomallin avulla OPC UA pystyy ilmaisemaan laajan valikoiman tietotyyppejä ja rakenteita, kuten prosessidataa, laitetietoja ja ohjaukaskäskyjä. Siirtomekanismi varmistaa siirrettyjen tietojen eheyden ja salassapitoisuuden suojattujen viestintä- ja tietoliikennekanavien avulla. OPC UA:n komponentit sisältävät kuljetusmekanismeja, jotka tukevat yksi-yhteen, yksi-moneen ja moni-moneen –viestintää. Tietomallinnus määrittelee säännöt ja rakennuspalikat, jotka vaaditaan hallitun datan paljastamiseksi. (Jasperneite & Lohveg, 2018, s. 238, opc7.com, 2023).

OPC UA arkkitehtuuri mallintaa asiakasta (Client) ja palvelimia (Server) vuorovaikutteisina kumppaneina. Jokainen järjestelmä voi sisältää useita asiakkaita ja palvelimia. Asiakas voi olla vuorovaikutuksessa samanaikaisesti yhden tai useamman palvelimen kanssa ja jokainen palvelin voi tehdä saman useiden eri asiakkaiden kanssa. Sovellus voi tällöin yhdistää palvelimen ja asiakkaan komponentteja vuorovaikutukseen muiden palvelimien ja asiakkaiden kanssa (opcfoundation.org, 2023).



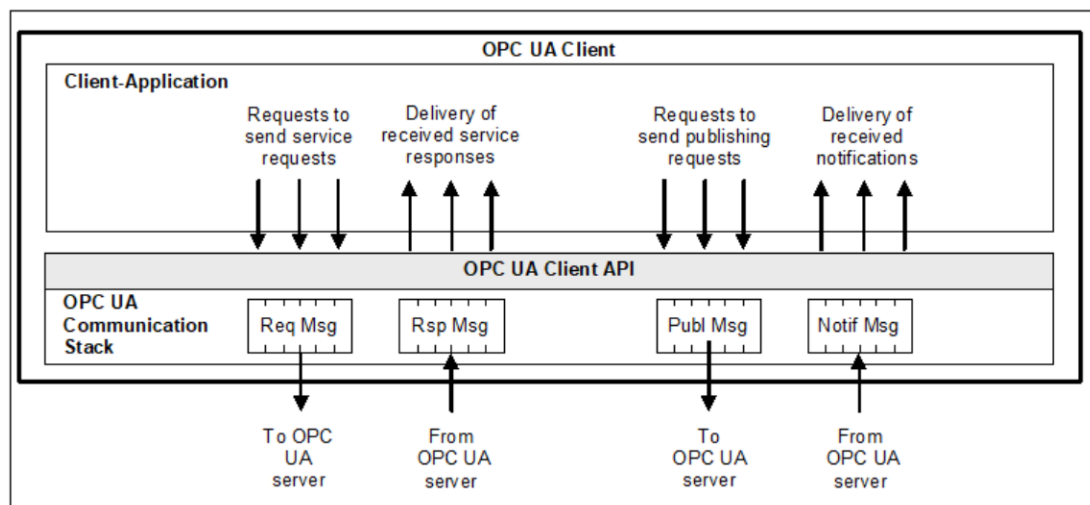
Kuva 1. OPC UA arkkitehtuuri (opcfoundation.com, 2023)

OPC UA –viestinnän perusta on OPC UA –palvelin. Palvelin on ohjelmisto, joka toteuttaa OPC UA –standardin ja tarjoaa siten standardoidut OPC UA –rajapinnat ulkomaailmaan. OPC UA:n perusideana on, että laitteiston valmistaja tarjoaa palvelimen järjestelmälleen ja mahdollistaa siten pääsyn. Palvelin voidaan toimittaa erillisenä ohjelmistona tai sulautettuna palvelimena laitteeseen tai koneen ohjaimiin. OPC UA:n viestintä on myös mahdollista lisätä järjestelmiin erillisenä itsenäisenä OPC UA –palvelimena, jos valmistaja ei tarjoa valmiiksi omaa palvelinta. Palveluntarjoajalta hankittu itsenäinen OPC UA-palvelin antaa laajemman viestintäprotokollan tuen ja joissain tapauksissa yksinkertaisempaa käyttöä, enemmän toimintoja ja parempaa vakautta verrattuna valmistajan suoraan tarjoamaan palvelimeen (opc-router.com, 2023).



Kuva 2. OPC UA palvelimen arkkitehtuuri (opcfoundation.com, 2023)

OPC UA –asiakas on OPC UA –palvelimen looginen vastine. OPC UA –palvelin voidaan yhdistää OPC UA –asiakkaan kanssa, jonka avulla voidaan lukea palvelimen toimittamat tiedot. Asiakas voi OPC UA –asiakkaan avulla käyttää mitä tahansa OPC –palvelinta, sillä palvelimet toteuttavat standardin ennalta määritellyt rajapinnat. OPC UA –asiakas on tyypillisesti asiakkaille, jotka ovat riippuvaisia tiedonvaihdosta teollisten järjestelmien välillä (opc-router.com, 2023).

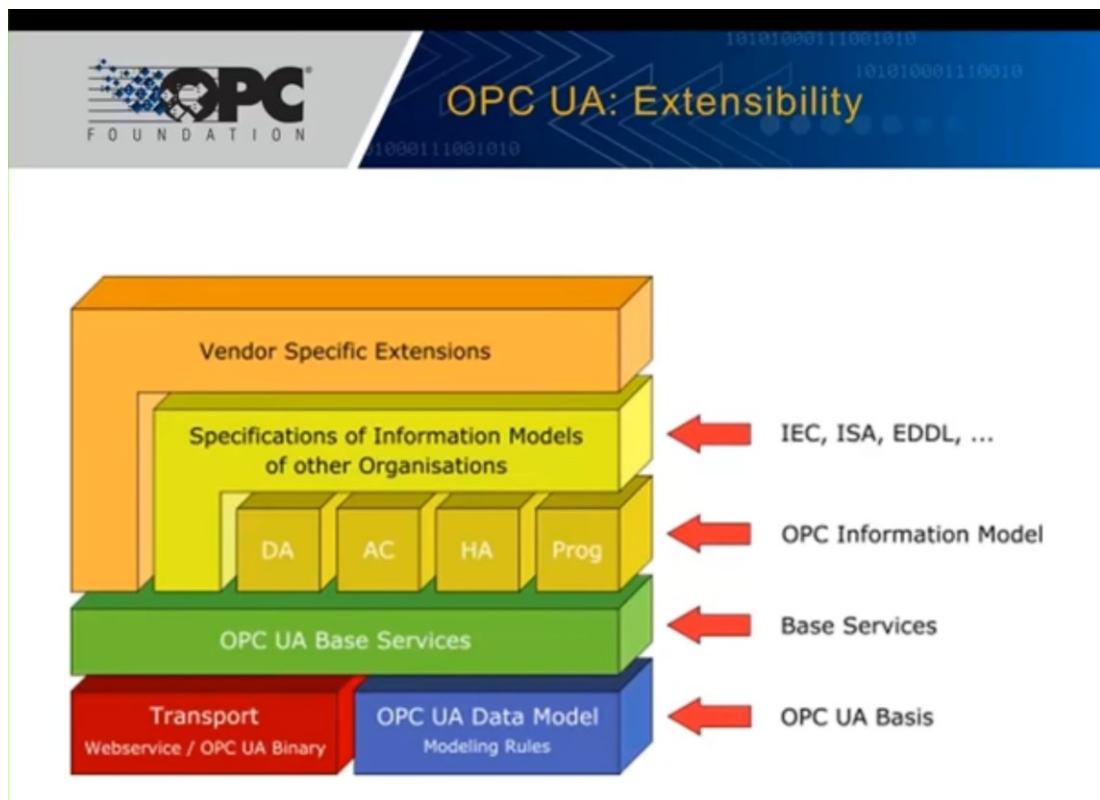


Kuva 3. OPC UA Client arkkitehtuuri (opcfoundation.com, 2023)

Kuva 3 havainnollistaa tyypillisen OPC UA –asiakkaan tärkeimpiä elementtejä ja niiden välistä yhteyttä. Kuvassa Client-Application on koodi, joka toteuttaa asiakkaan toiminnon. Se käyttää OPC UA Client API:ta palvelupyyntöjen ja vastausten lähettämiseen ja vastaanottamiseen palvelimelle. Kuvassa esitetty OPC UA Client API on sisäinen liitäntä, jonka tarkoituksena on eristää OPC UA:n asiakaskoodi viestintäpinosta. OPC UA Communications Stack muuttaa Client API:n kutsun viestiksi, jonka se lähettää edelleen viestintäyksikön kautta palvelimelle asiakkaan pyynnöstä (opcfoundation, 2023).

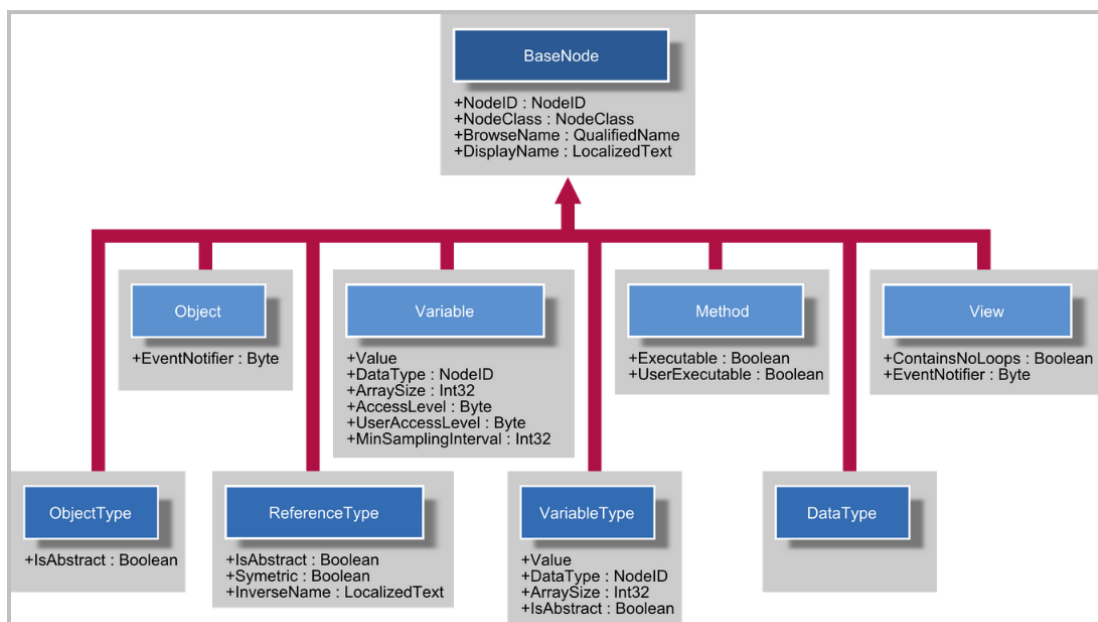
### 2.2.1 Tietomalli

OPC UA:n tietomalli erottaa sen kilpailijoistaan. OPC UA käyttää solmuja peruskäsitteenä edustamaan taustalla olevan järjestelmän tietoja ja käyttäytymistä. Classicin käytössä on ollut vain puhdas data, esimerkiksi anturilta tullut tieto ja sisällön ymmärtämiseen vaadittu tunnistenimi ja yksikkö. OPC UA pysyy edellä mainittujen lisäksi paljastamaan anturin tyyppin ja mitä laitetta se tukee. Vaikka tietomalli tarjoaa pelkän infrastruktuurin tietojen mallinnukseen, on se muokattavissa eri tarkoituksiin kolmansien osapuolien kautta. Esimerkiksi laitevalmistajat voivat laajentaa OPC UA:n tietomallin sopivaksi omaan käyttötarkoitukseen (Jasperneite & Lohveg, 2018, s. 239; Heikkilä, 2016, s. 14).



Kuva 4. OPC UA tietomalli (InduSoft OPC Webinar, 2012)

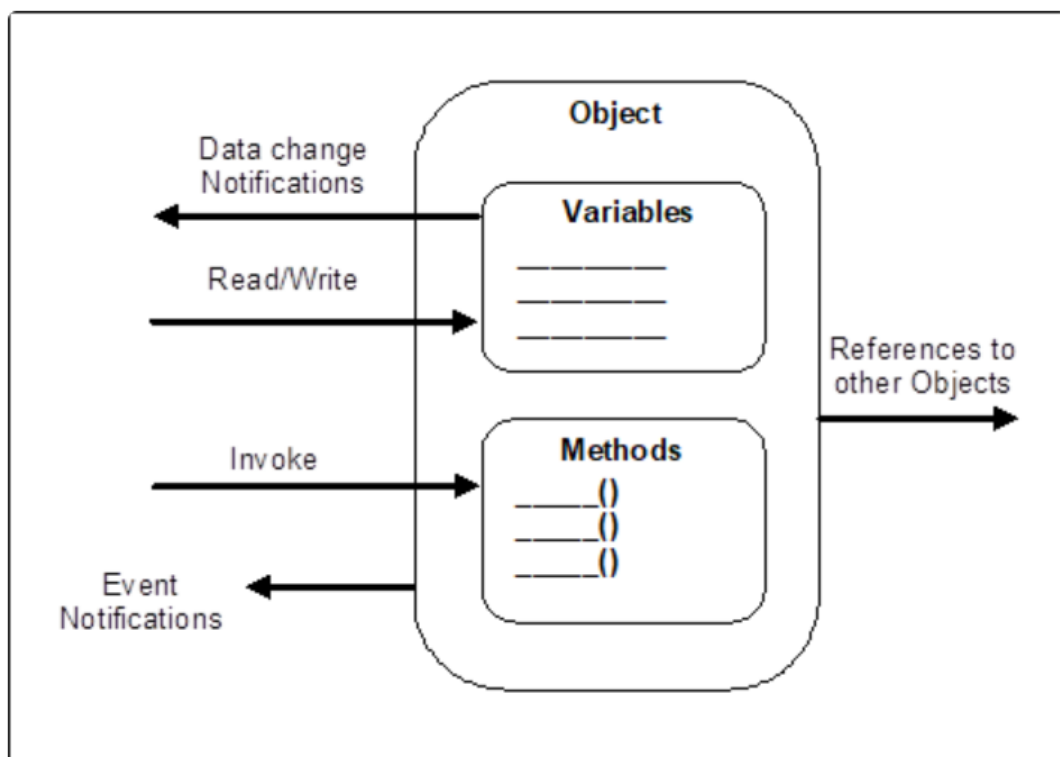
Kuvassa 4 havainnollistetaan OPC UA:n tietomalli. Tietomallin perusta on eri loogisilla tasoilla. Punainen laatikko "Transport" kertoo protokollista, jota OPC UA sisältää. Protokollat ovat verkko- ja binääripohjaisia protokollia, jota voidaan hyödyntää tarpeen mukaan, esimerkkinä verkkopohjaisesta protokollasta JSON, ja binääripohjaisesta OPC –binary transport. Sininen laatikko on datamalli, jossa kaikkien objektien tyypit on määritelty (kuva 5). Perus datamalli pystyy tarjoamaan muuttuja- ja objektityypit sekä tieto- ja viitetyypit, jonka perusteella OPC UA voi edustaa kaikenlaista dataa ja lisäksi metadataa sekä semantiikkaa. Vihreä laatikko kuvaa funktioiden määrittelyä, kuten tilauksia. Sen avulla OPC UA määrittää kiinteän joukon palveluita. Ne on määritelty tarkoin parametreilla ja käyttäytymisellä. Tämä vaikuttaa esimerkiksi ominaisuuksien ja tietojen lukemiseen, joka onnistuu yhdestä paikasta. Ennen OPC UA:ta esimerkiksi historian ja hälytystietojen hakeminen piti tehdä erikseen. Kirjain yhdistelmät DA, AC, HA ja Prog kuvaavat OPC Classicin protokollia. Ne on OPC UA protokollaan yhdistetty, jotta datan kerääminen olisi mahdollisimman helppoa ja käytännöllistä. Lyhenteet tarkoittavat Data Accessia, Alarms & Conditionsia, Historical dataa ja Programsia. Programs täydentää muita UA-palveluita ja objektityyppejä, joka helpottaa palvelimen ja asiakkaan toimintaa automaatioympäristössä. "L" laatikot kuvaavat muokkautuvuutta OPC UA:ssa, jota voi myös itse muokata eri standardien, kuten IEC:n ja SOLAS:n mukaan (InduSoft OPC Webinar, 2012; ascolab.com, 2024; opcfoundation, 2024).



Kuva 5. Esimerkki OPC UA Datamallin rakenteesta (Ascolab.com, 2024).

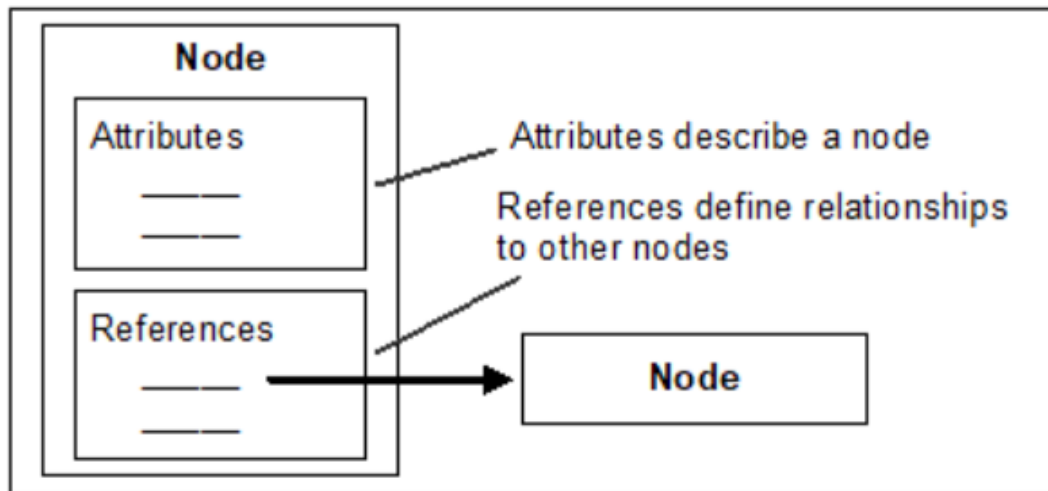
### 2.2.2 Osoiteavaruus

OPC UA:n osoiteavaruus (Address Space) koostuu kolmesta osasta: objektimallista (object model), solmumallista (node model) ja referenssimallista (reference model). Objektimallin tavoite on tarjota palvelimille tavallinen tapa edustaa objekteja asiakkaille. Se määrittää objektit muuttujien ja menetelmien avulla ja mahdollistaa myös suhteiden ilmaisemisen muihin objekteihin. Kuva 5 havainnoi OPC UA:n osoiteavaruuden objektimallia (opcfoundation.org, 2023).



Kuva 6. OPC UA objektimalli (opcfoundation, 2023).

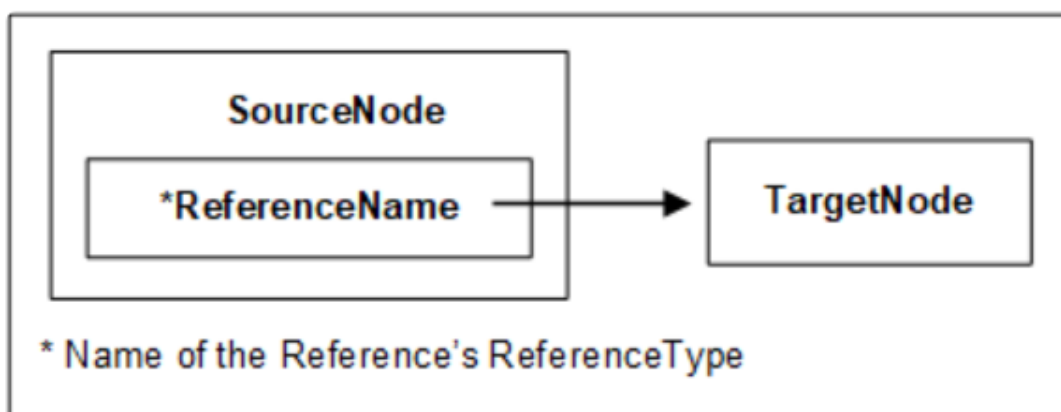
Solmumalli esittää objektit ja niiden komponentit solmujoukkona. Ne kuvataan attribuuttien avulla, jotka on yhdistetty toisiinsa referensseillä. Kuva 6 havainnollistaa solmumallin toimintaa (opcfoundation.com, 2023).



Kuva 7. OPC UA solmumalli (opcfoundation.com, 2023).

Osoiteavaruuden metadata on niin kutsuttu solmuluokka. Solmuluokat määritellään attribuuttien ja referenssien avulla, jotka on ilmennettävä – eli lisätä annetut arvot – kun solmut määritellään osoiteavaruudessa. Attribuutit ovat tietoelementtejä, jotka kuvaavat solmuja. Ne ovat solmuluokkien peruskomponentteja. Referenssit taas yhdistävät solmut toisiinsa. Niiden määrittely tapahtuu samalla tavalla kuin attribuuteissa, eli ne ovat solmujen peruskomponentteja. Solmu, joka sisältää referenssin, kutsutaan lähdesolmuksi ja solmua, jota referoidaan, kutsutaan kohdesolmuksi. OPC UA –palvelut käyttävät tätä viitteiden yksilöimiseen (opcfoundation.com, 2023).

SourceNode, ReferenceType ja TargetNode yhdistelmää käytetään OPC UA –palveluissa viitteiden yksilöimiseen. Täten kukin solmu voi viitata toiseen solmuun vain kerran samalla viitetyypillä (opcfoundation, 2023).



Kuva 8. OPC UA Referenssimalli (opcfoundation, 2023).

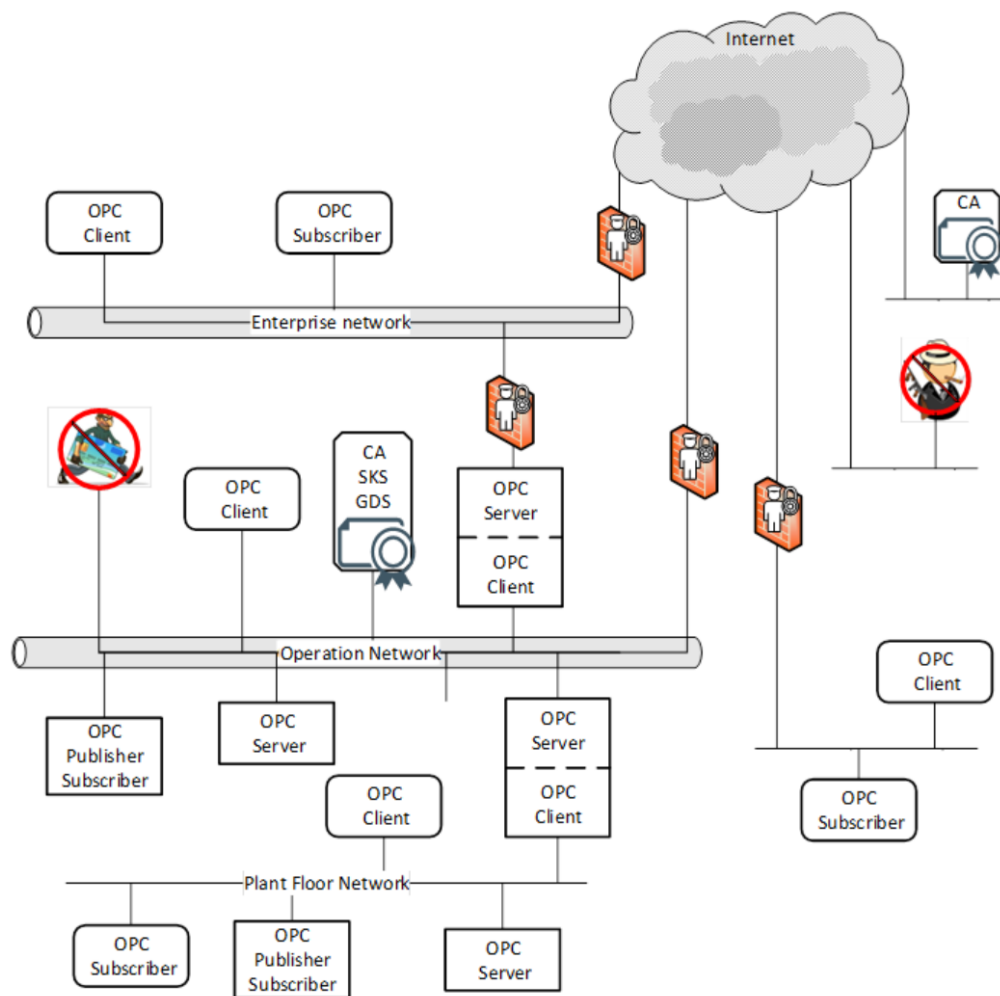
## 2.3 Kyberturvallisuus

Kyberturvallisuus tarkoittaa lyhyesti suojautumista kyberhyökkäyksiä ja niiden vaikutuksia vastaan, sekä toteutetaan tarvittavia vastatoimenpiteitä varustamon ja aluksen kyberympäristön tukemiseksi. IMO (International Maritime Organization) hyväksyi 98. istunnossaan päätöslauselman, jonka mukaan varustamoiden kyberriskien tarkastelu tulee olla tehtynä vuosiauditoinnissa. Telakoiden on otettava huomioon kyberturvallisuus tulevaisuudessa risteilijöissä jo aikaisessa vaiheessa, sillä rakennusvaiheessa kyberturvallisuus on helpompi huomioida. IACS:n (International Association of Classification Societies) sääntöihin perustuen on käytössä luokkamerkki, joka on vaade nykyristeilijöille. Vaikka luokkamerkki perustuu IACS:n sääntöihin jokaisella luokalla asia on toteutettu hieman eri tavalla. Nykyiset risteilyalukset varustetaan pääsääntöisesti ”Cyber secure class notation” –merkinnällä. IACS määrittelee myös uuden säännön (IEC 62443-3-3), joka astuu voimaan vuonna 2025 eteenpäin. OPC UA vastaa IACS:n säännön vaatimukseen ja se on osittain syy miksi OPC UA:ta halutaan telakalla tutkia ja käyttää (traficom.fi, 2020; IACS, 2023).

OPC UA:n käyttö teollisuuslaitosten toiminnassa on usein monikerroksista eli se toimii esimerkiksi yritys- ja toimintaverkon välissä, mikä tekee siitä todennäköisen kohteen sabotaasille. OPC UA:ta käytetään erilaisissa toimintaympäristöissä erilaisilla uhkilla ja saavuttavuudella olevilla oletuksilla sekä erilaisilla täytöntöönpanojärjestelmillä ja turvallisuusmääräyksillä. Tästä syystä OPC UA tarjoaa joustavan joukon turvamekanismeja, kuten suojatun kanavan muodostaminen palvelimen ja asiakkaan välillä sekä onko käyttäjällä oikeus käydä keskustelua palvelimen ja asiakkaan välillä. (opcfoundation.com, 2023).

ISA/IEC 62443 määrittelee strategiat uhkien hallintaan jakamalla operatiivinen verkko segmentteihin, jotka on kytketty toisiinsa tiettyjen liitoskohtien, putkien kautta. Nämä putket voidaan varustaa tunkeutumisen havainnointijärjestelmillä (IDS) tai tunkeutumisen estojärjestelmillä (IPS tai IDPS). Nämä havaitsevat tai estävät eri haittaohjelmien pääsyn laivan tai tehdasverkon haavoittuviin osiin. ISA/IEC 61662-460 määrittelee laivojen navigoinnin ja tietoliikenteen

korkean standardin suurien ulkoisten uhkien varalle tai verkon eheyden parantamiseksi (Suomen Automaatioseura, 2015; IEC, 2018).

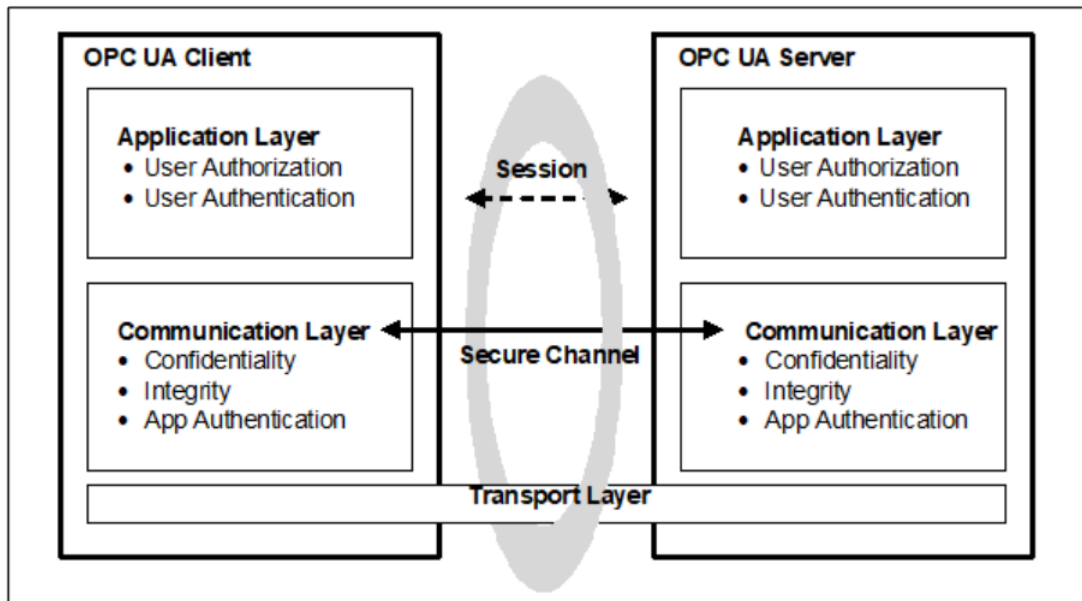


Kuva 8. OPC UA esimerkki tietoverkon rakenteesta (opcfoundation, 2023).

Kuva 8 on esimerkki OPC UA tietoverkon rakenteesta, joka esittää aiemmin mainitun ympäristön. Osa OPC UA –sovelluksista saattaa olla saman hostin eli isännän alla, joten ne on helppo suojata ulkoisilta hyökkäyksiltä, mutta osa voi olla eri hostin alla samassa verkossa, jossa ne suojataan esimerkiksi suojattu turvarajojen suojauksilla, jotka erottavat toimintaverkon ulkoisista yhteyksistä. OPC UA tarjoaa myös mahdollisuuden useille eri protokollille ja viestintätekniikoille, jotka saattavat vaatia erilaisia suojaustasoja ja erilaista kyberinfrastruktuuria (opcfoundation.com, 2023).

### 2.3.1 Kyberturvallisuuden arkkitehtuuri

OPC UA:n kyberturvallisuusarkkitehtuuri mahdollistaa vaadittujen turvaominaisuuksien toteuttamisen eri paikoissa OPC UA:n sovellusarkkitehtuurissa. Client/server viestintä on arkkitehtuuriltaan rakennettu niin, että sovellus- ja siirtokerros ovat viestintäkerroksen päällä. Alla olevat kuvat ovat esimerkkejä client/server kyberturvallisuusarkkitehtuureista.



Kuva 9. OPC UA Asiakas/Palvelin kyberturvallisuusarkkitehtuuri (opcfoundation, 2023).

OPC UA:n kyberturvallisuuden peruspilarina on tietoturva, eikä vain tietojen eheysyistä vaan myös palvelujen saatavuuteen. Kuva 9 kuvaakin OPC UA:n tekniset tiedot turvallisuuden kolmella painopisteellä: Todennus asiakas- ja palvelinsovellusten välillä, mahdollisuus määrittää, onko käyttäjällä lupa muodostaa yhteys ja suorittaa pyydetty toiminto sekä viestinnän luottamuksellisuus ja eheys (opcfoundation.com, 2021).

Transport layer on ensimmäinen kerros kyberhyökkäyksiä vastaan. Kerros löytää koneen oikean IP-osoitteen, jota sovellus kuuntelee. Kerros voi sisältää suojaustoimintoja, jotka eivät kuulu OPC UA:n piiriin, kuten pääsynhallintaluetelun ja palomuuureja. Tämä edes auttaa siihen, että transport layer voi hylätä yhteyden ennen kuin se on koskaan muodostettu sabotaasin aikana.

Communication layer on suurin osa OPC UA:n kyberturvallisuutta. Kun client muodostaa serveriin yhteyden, muodostuu suojattu kanava, jossa varmenteiden vaihto tapahtuu. Varmennetta ei käytetä vain yhteyksien luovien sovellusten ja hostien todentamiseen, vaan myös lähettyvien viestien salaamiseen ja allekirjoittamiseen. OPC UA –sovellus voi hylätä yhteysyrityksen, mikäli palvelimen sertifikaattiin ei luoteta.

Application layer on kerros, jossa on todennus ja OPC UA:n komentotodennus. Tällä tasolla on jo varmaa, että host ja sovellus ovat luotettuja ja OPC UA:n serverin ja clientin välinen keskustelu on suojattu. Viimeinen tarkistettava asia on, että onko sovelluksen kanssa oikeus käyttää sen kyseisiä resursseja (opcfoundation.com, 2021).

### 3 OPC UA EDUT

Teknologioiden, kuten monipolttoainekäyttöisten propulsiojärjestelmien, ympäristöystävällisten laivojen ja sähkökäyttöisten propulsioalusten kehittyessä IoT-sovellusten laajuus merenkulussa suurenee. Tämä lisää valvontatekijöiden monimutkaisuutta. OPC UA on suunniteltu edes auttamaan kyseisissä ongelmissa. Se muuttaa suunnittelua, rakentamista ja materiaalien hallintaa tehokkaammaksi ja sitä kautta myös kannattavammaksi (encyclopedia.com, 2023).

OPC UA mahdollistaa eri valmistajien laitteiden ja järjestelmien välisen kommunikoinnin. Sen joustavuus, yhteentoimivuus ja turvallisuus ovat mahdollistaneet protokollan yleistymisen eri teollisuudenaloille. Erityisesti joustavuuksensa ansiosta OPC UA:ta voidaan jatkuvasti parantaa, mikä tekee siitä tulevaisuuden kestävä. Se on yksi teollisen esineiden internetin tärkeimmistä viestintästandardeista (Process Genius, 2023).

Huomioitavaa on kuitenkin, ettei kaikki OPC UA:n palvelimet eivät tue itsessään kaikkia mahdollisia ominaisuuksia. Esimerkiksi hälytysten käsittely tai historian datan tallennus saattaa puuttua palvelimesta. Nämä ovat kuitenkin yleisiä ominaisuuksia useille eri OPC UA –palvelimelle (opcfoundation.com, 2024).

OPC UA:n ottaminen käyttöön telakalle on suuri investointi. Liian suuret muutokset aiheuttavat valtavia kustannuksia ja riskejä. Kuitenkin muutos – jo kyberturvallisuutta ajatellen – on vääjäämätön. Oikealla aikataululla, suunnitellulla ja riskien minimoimisella OPC UA:n käyttöönotto telakalle ja laivoihin maksaisi itsensä takaisin laadukkaamman datan ja turvallisuuden kautta. Operaattorin on mahdollista tehdä parempia päätöksiä ja raportteja, jonka avulla säästöä tehtäisiin (opcfoundation, 2017).

### 3.1 Keskeiset ominaisuudet

OPC UA protokolla on kuusi keskeistä ominaisuutta, jotka voidaan jakaa alustariippumattomuuteen, turvallisuuteen, skaalautuvuuteen, tietojen mallintamiseen, hälytyksiin ja tapahtumiin, sekä historiatietojen käyttöön (Process Genius, 2023).

Alustariippumattomuuden ansiosta OPC UA protokolla toimii useilla eri laitteistoalustoilla ja käyttöjärjestelmissä, kuten perinteisillä PC -laitteistoilla – esimerkiksi Windowsilla, Apple OS:llä ja linuxilla – pilvipohjaisilla palvelimilla ja PLC:lla (opcfoundation.org, 2023).

OPC UA tukee erilaisia tietoturvaominaisuuksia, kuten salausta ja digitaalisia allekirjoituksia, joilla varmistetaan eheyden luottamuksellisuuden ja todennuksen suojaus. Protokolla siis varmistaa itse turvallisen tiedonsiirron, jolla estetään luvaton pääsy verkkoon (Process Genius, 2023).

OPC UA tukee myös useita viestintämalleja, jotka takaavat skaalautumisen suurien ja pienien järjestelmien välillä. Esimerkiksi point-to-point ja multi-node kuuluvat OPC UA protokollan tukemiin viestintämalleihin. Tämä mahdollistaa eri valmistajien laitteiden ja järjestelmien välisen kommunikoinnin verkossa (Process Genius, 2023).

Tietojen mallinnuksessa OPC UA mahdollistaa joustavan ja laajennettavissa olevan tietomallikehityksen, jonka avulla käyttäjät voivat itse määrittää tietorakenteita, objektityyppejä ja menetelmiä (Process Genius, 2023).

OPC UA sisältää erilaisia mekanismeja tunnistaa ja käsitellä hälytyksiä ja tapahtumia. OPC UA mahdollistaa reaaliaikaisen raportoinnin ja ajantasaiset ilmoitukset kriittisistä tapahtumista, kuten vioista. Tämä edesauttaa kunnossapitoa ja vianmäärittystä (Process Genius, 2023).

Teollisuusjärjestelmiin tallennettujen historiatietojen hyödyntäminen on OPC UA protokollan avulla mahdollista. OPC UA pystyy hakemaan järjestelmien historiatietoja hälytyksistä tapahtumista ja prosessiarvoista. Se mahdollistaa trendien analysoinnin ja visualisoinnin (Process Genius, 2023).

Nämä keskeiset ominaisuudet luovat loistavan pohjan protokollan kehittämiseen myös tulevaisuudessa. Koska OPC UA protokollaa kehittää useat eri toimijat eri aloilta, kehitetään sitä laajasti IIoT:n haasteisiin sopivaksi. Esimerkkinä Yhdysvaltalainen ohjelmistoalan yritys Microsoft, joka on sitoutunut tukemaan OPC UA:ta ja sen kehitystä. Microsoft on pyrkinyt kehittämään OPC UA:ta tekoälyn, sekoitetun todellisuuden ja digitaalisten kaksosten kanssa toimiviksi niin, että näihin perustuvat järjestelmät mahdollistettaisiin tehdaskeroksissa (opcfoundation, 2023, s. 12).

### 3.2 Mikä erottaa OPC UA:n kilpailijoista

OPC UA protokolla on kehitetty yhteistyössä useiden eri laitevalmistajien ja tutkijoiden kanssa, jotta protokolla tukisi mahdollisimman laadukkaasti automaatioteollisuuden muutosta. Yhteensopivuuden puute laitteiden ja järjestelmien välillä on yksi merkittävimmistä esteistä automaatioteollisuudessa. Eri valmistajien omat viestintäprotokollat vaikeuttavat valmistajien eri laitteiden yhteyden muodostamista toisiinsa. Suunnittelun kannalta tämä on erittäin haitallista, sillä integroimisen vaikeus erilaisten järjestelmien ja laitteiden välillä on raskasta ja vaikeaa, mikä vähentää tuottavuutta ja tehokkuutta. OPC UA ratkaisee ongelman tarjoamalla oman standardikielen, jonka avulla laitteet voivat kommunikoida keskenään. Standardikieli määrittää kokoelman rajapintoja ja protokollia, joiden avulla laitteet voivat viestiä tietoja johdonmukaisesti toisilleen. Yhteen toimivuus ongelmien ratkaisun lisäksi OPC UA tarjoaa laitteille turvallisen ja luotettavan menetelmän tiedonsiirtoon. Se sisältää salauksen ja todennuksen tietojen turvallisuuden ja eheyden varmistamiseksi (opc7.com, 2023; opcfoundation.org, 2023).

Koska OPC UA:n idean taustana on objekti eli yksittäinen tieto tai prosessi, järjestelmä tai kokonainen tuotantolaitos, voi sen avulla kerätä dataa eri määriä. Tuottamalla eri tyyppistä dataa ja laajempaa dataa kuin aikaisemmat TCP/IP –verkot, voi sen avulla leikata kustannuksia esimerkiksi kunnossapidosta ja IT –järjestelmistä. Suurin ero on siis datan määrässä ja laadussa. Se on reaaliaikaista ja räätälöityä juuri asiakkaan omaan tarkoitukseen. OPC UA järjesteelele automaatioteollisuuden järjestelmiä, prosesseja ja tietoja ainutlaatuisella tavalla (Tomi Peltokangas & Janne Känsäkoski, 2017, s. 10).

## 4 TIEDONSIIRTO SYSTEEMIEN VÄLILLÄ LAIVOISSA

Risteilylaivat kehittyvät nopeaa tahtia. Sähkö- ja väylätekniikoiden kehityksen myötä laivojen sisällä on moninainen verkko erilaisia tiedonsiirto väyliä mahdollistamassa kommunikaatiota järjestelmien välillä. Järjestelmien määrä laivassa on niin suuri, että väylien määrittely on erittäin vaivalloista. Lisäksi erilaiset turvallisuus määräykset ovat risteilijöissä erittäin tarkat. Näitä määräyksiä ja lakeja määritellään kansainvälisissä sopimuksissa kuten SOLAS ja IEC:n päätöksissä. SOLAS (International Convention for the Safety of Life at Sea) on kansainvälinen meriturvallisuutta käsittelevä sopimus, joka muutoksia hallinnoi IMO (International Maritime Organization). Näitä valvovat eri maiden viranomaiset (Leino, 2022).

Integroidut väyläprotokollat ovat usein myös eri valmistajilta. Protokollat eivät ole yhteensopivia toistensa kanssa ja vaativat erityistoimenpiteitä, kuten protokollamuuntimia tai ohjelmisto päivityksiä, voidakseen kommunikoida toistensa kanssa. Standardien puute laivanrakennuksessa mahdollistaa jokaisen järjestelmän toimittajan oman spesifikaation eikä toimittajien ole kannattavaa suunnitella järjestelmiään uudelleen telakan hetkellisten tarpeiden mukaisiksi. Siksi telakan tulee suunnitella eri toimittajien järjestelmät yhteensopiviksi (Leino, 2022).

Näistä syistä laivanrakennuksessa on hankalaa muuttaa asioita vain sattumanvaraisesti uudeksi. Laivojen automaatiojärjestelmät muodostavat yhdessä suuren kokonaisuuden, jossa järjestelmien määrä riippuu laivan koosta, tyypistä ja käyttötarkoituksesta. Siksi koko toiminnan ja laitoksen ohjausjärjestelmän muuttamiseen kerralla liittyy liikaa riskejä, seisokkikustannuksia ja suunnittelua. Asioiden luonnollinen tila on, että löydämme eri ikäisiä ja tasoisia ohjelmistoja, standardeja ja järjestelmiä, jotka toimivat yhdessä. Haaste onkin, miten uudet järjestelmät saadaan toimimaan vanhojen järjestelmien kanssa. Näistä asioista johtuen telakan täytyy jo alusta asti olla ohjaamassa minkälaista väyläprotokollaa laivassa tulisi käyttää ja mitä muita standardeja noudatetaan, jotta varmistetaan, että eri automaatiotoimittajat puhuvat samaa kieltä.

OPC UA:n alustariippumattomuus ja skaalautuvuus antavat mahdollisuuden näiden ongelmien helpottamiseksi. (opcfoundation.com, 2017; Leino, 2022).

#### 4.1 OPC UA tiedonsiirto eri valmistajien välillä

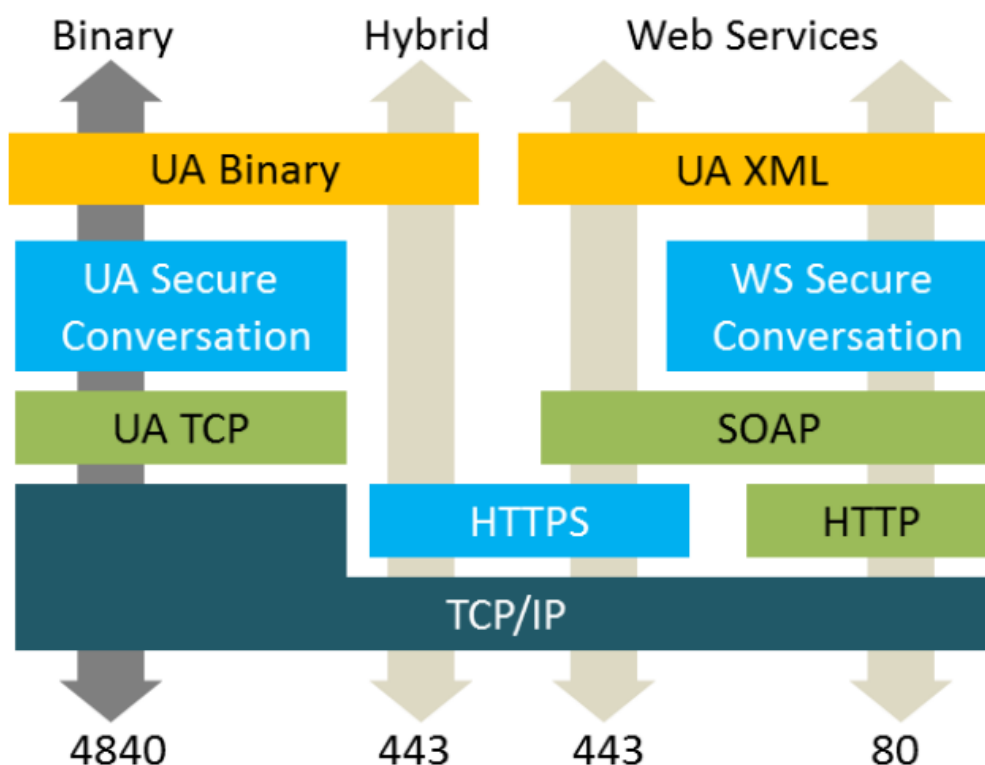
OPC UA mahdollistaa tiedonsiirron eri valmistajien välillä noudattamalla standardoituja protokollia, joita ovat esimerkiksi HTTP/HTTPS, TCP/IP, MQTT ja AMQP. Tämä mahdollistaa eri valmistajien laitteiden ja järjestelmien integroinnin, koska kaikki noudattavat samaa kommunikaatioprotokollaa.

Käytännössä tiedonsiirto OPC UA:n protokollan kanssa voidaan jakaa eri vaiheisiin. Yksi laite tai ohjelmisto toimii OPC UA –palvelimena ja toinen toimii OPC UA –asiakkaana. Asiakas muodostaa turvallisen yhteyden palvelimeen standardoidulla protokolalla. Kun yhteys on muodostettu asiakas voi pyytää tai lähettää tietoa palvelimelle turvallisesti vahvalla salauksella ja käyttäjän tunnistuksella. Datan rakenne, joka on usein XML- tai binäärimuodossa, noudattaen OPC UA:n määritelmiä tiedon mallinnussääntöjä (opcfoundation.com, 2023).

OPC UA:n käyttäminen tiedonsiirtoprotokollana esimerkiksi laivanrakennuksessa telakka voisi hyötyä taloudellisesti. Se virtaviivaistaa viestintää ja integraatiota ja sen avulla yritykset voivat vastaanottaa laadukkaampaa dataa. Tämä auttaa telakkaa saamaan parempaa tietoa järjestelmistä ja niiden kunnosta. OPC UA datan keruu antaa mahdollisuuden telakalle tehdä datalähtöisiä päätöksiä prosessien optimoimiseksi ja ennakoivien kunnossapitostrategioiden toteuttamiseksi ja hyödyntää näitä koko laivan elinkaaren aikana (Anybus, 2023).

OPC UA perustuu TCP/IP:hen, mutta siirtokanavaa voidaan vaihtaa joustavasti UA-, binääri-, HTTPS- ja SOAP-protokollien välillä. TCP/IP on lyhykäisyydessään sarja viestintäprotokollia, joita käytetään verkkolaitteiden yhdistämiseen internetissä. Tämän skaalautuvuuden ansiosta se on myös avoin tule-

ville protokollavaihtoehtoille. Jokainen näistä protokollista mahdollistaa täyden suojauksen sovellusten ja käyttäjien todennukselle ja tietojen salaukselle (Suomen Automaatioseura, 2015).



*Kuva 10. OPC UA tiedonsiirto-protokollien vaihtoehdot. Kuvassa numerot tarkoittavat vakio IP-porttinumeroita, jotka on määritellyt vastaaville protokollille. OPC UA –sovellukset käyttävät erilaisia porttinumeroita, jossa vain yhtä porttia käytetään tiedonsiirto sovellus- ja protokollakohtaisesti. (Suomen Automaatioseura, 2015).*

OPC UA:n käyttö avaa siis suuremmat markkinat ja vaihtoehdot valmistajille. Ja koska OPC UA mahdollistaa yhtenäiset rajapinnat ja toimintamallit, ei toimijan roolilla ole väliä. Samalla – riippumatta teollisuuden alasta – tuotantolaitoksen automaatiojärjestelmät, laitteet ja ohjelmistot voidaan integroida MES ja ERP järjestelmään turvallisesti. Diagnoosien ja raporttien tekeminen OPC UA:n avulla on myös mahdollista internet- ja pilvipohjaisilla järjestelmillä (Tomi Peltokangas & Janne Käsäkoski, s.11-12).

## 4.2 Kyberturvallisuus tiedonsiirrossa

Teollisuuden järjestelmien kannalta kriittisiä ominaisuuksia ovat ohjausjärjestelmien ja kaiken niihin liittyvän tiedonsiirron suojaus. OPC UA tarjoaa nykyaikaisen suojatun viestintäprotokollan, joka mahdollistaa useimpien laitteiden hallinnan nykyaikaisiin laivoihin ja tuotantolaitoksiin kohdistuvia turvallisuusuhkia. Vaikka OPC UA tarjoaa viestintäkanavaan vahvan suojan ulkoisille hyökkäyksille, suojaa se silti nimenomaan viestintäkanavaa. Kyberturvallisuuden takaamiseksi on edelleen käytettävä perinteisiä turvatoimia isäntätietokoneissa. Esimerkiksi haittaohjelmat voivat päästä verkkoon monin eri tavoin, joten turvatoimia ei voi heikentää hyvän viestintäsuojauksen takia. Tulevaisuudessa yhä useampi laite tulee olemaan avoimessa verkossa, jossa tietoturvan tärkeys korostuu tekijän tietojen, yksityisyyden ja luottamuksellisuuden varmistamiseksi (Suomen Automaatioseura, 2015).

## 4.3 Verkkoratkaisut

OPC UA tarjoaa useita verkkoratkaisuja tiedonsiirtoon. Yleisiä verkkoratkaisuja, jotka hyödyntävät OPC UA protokollaa ovat esimerkiksi: Ethernet-verkko, langattomat verkot (WLAN), IoT-sovellukset – kuten älykkäät anturit, joilla ohjata älykästä valaistusta – ja pilvipalvelut.

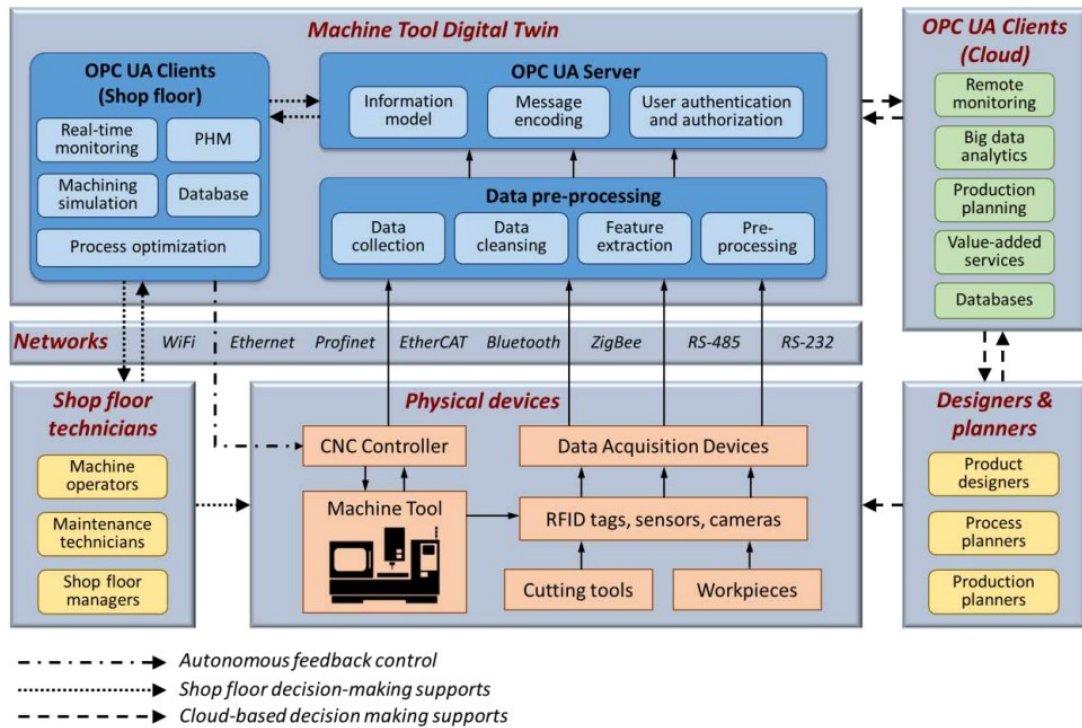
On olemassa siis useita tapoja siirtää tietoja asiakkaalle. Protokollan yksi ehdottomista eduista onkin, ettei palvelimen ja asiakkaan tarvitse olla kytköksissä toisiinsa fyysisesti, jotta dataa voidaan lähettää turvallisesti ja laajasti toistensa välillä. Verkkoratkaisuissa on kuitenkin asioita joita OPC UA ei pysty tekemään. Vaikka OPC UA on erittäin skaalautuva ja pystyy tukemaan erilaisia koodauksia, takaa turvajärjestelmän, läpäisee palomuurit, tukee yhdistettyjä viestintäkanavia ja on saatavilla julkisessa, yksityisessä ja hybridipilvessä, se ei kuitenkaan tarjoa lähtevää yhteyttä. Tämän ongelman voi kiertää välityspalvelimien avulla, joissa on asiakasyhteys tehtäseen ja pilveen. Usein näissä ratkaisuissa on käytössä OPC UA/MQTT –yhdykäytäviä (real time automation, 2018).

## 5 DATAN KERÄÄMINEN LAIVASSA

Laivojen automaatio, sähkö- ja propulsiojärjestelmät, anturit ja robotiikka ovat muutamia luokkia, jotka vaativat reaaliaikaista dataa, jotta yritykset voivat suorittaa nopeita toimintapäätöksiä. Tiedon analysointia ja laitteiden kunnosta saatava reaaliaikainen tieto pohjautuu mahdollisimman laajaan dataan, joka on selkeä ymmärtää ja paikantaa (Smart Ship Technology, 2016).

Hyvän ja reaaliaikaisen datan kerääminen laivan järjestelmistä on erittäin tärkeää omistajalle. Huolto ja ylläpitokustannukset ovat suuri menoerä yrityksille. Häiriöt vaikuttavat tuotteiden laatuun, tuotantokustannuksiin, terveyteen, turvallisuuteen ja ympäristöön. Kunnossapidon strategisena näkökulmana yritysorganisaatiossa turvallisuuden korostaminen, ympäristölainsäädäntö ja polttoainetehokkuuden parantaminen sekä päästöjen vähentäminen (Smart Ship Technology, 2016).

Datan analysoinnista tekee risteilyaluksissa hankalaa niiden järjestelmien määrä ja laitteiden valtava kirjo. Seos vanhoista ja uusista laitteista sekä erilaisista verkoista ja toimittajien tuotteista vaikeuttaa datan keräämistä jokaisesta laitteesta ja verkosta. Tämän lisäksi sovellusten, jotka analysoivat ja visualisoivat datan vaativat käyttöönottoa, joka on erittäin vaivalloista. Mahdollisuus kerätä tietoja automaatiojärjestelmistä korkealla resoluutiolla keskeytyksettä on avain tehokkaiden ja luotettavien toimintojen varmistamiseen. Laivojen elinkaaren aikana huolto- ja kunnossapitoinsinöörit joutuvat lisäämään signaaleja elinkaaren aikana, jotta automaatiojärjestelmä pysyy turvallisena. OPC UA:n avulla näitä toimenpiteitä ei tarvitse tehdä. Se esimerkiksi ratkaisee jännitteen aluksen tehokkuuden ja toiminnan lisäämiseen tietotarpeen ja korkean kyberturvallisuuden välillä. Lisäksi OPC UA tarjoaa nopeamman ja paremman integraation mihin tahansa tiloissa käytettävään analytiikkaan skaalautuvan koneen datan turvalliseen suoratoistamiseen laivan automaatiojärjestelmästä. Esimerkiksi Wärtsilällä on Nacos Platinum OPC UA käyttöliittymä, joka on luotu laivojen automaatiojärjestelmien turvallisen ja tehokkaan datan keräämisen ratkaisuksi (wartisila.com, 2024).



Kuva 11. OPC UA pohjainen arkkitehtuuri yleisestä CPMT:stä (Cardiff University, 2019).

Viime vuosina OPC UA:n integrointia on kehitetty prosessien seurantaan ja valvontaan paremmin sopivaksi. Kehityksessä on pyritty ottamaan käyttöön kokonaisvaltainen lähestyminen, joka huomioi etenkin Teollisuus 4.0 ympäristön. Tästä syystä se sopii loistavasti risteilijäaluksen datan keräämiseen. Rakentamismielessä risteilijäalusta haastavampaa laitosta on vaikea etsiä. OPC UA:n kommunikaatio pilvipohjaisten yhdyskäytävien kautta, CPPS arkkitehtuurin kehitys, jonka avulla päästään käsiksi laitetietoihin laajasti automaatiojärjestelmissä ja nanopalvelin, joka mahdollistaa integroinnin pienen muistin sisältäviin laitteisiin (University of Auckland, 2019).

Datan kerääminen voi tapahtua laivassa ja muussa teollisuusympäristössä OPC UA:n avulla useilla eri verkkoratkaisuilla. Esimerkkinä Ethernet, Wifi, Profinet ja Bluetooth ovat yleisesti käytössä olevia verkkotekniikoita, joita OPC UA tukee. OPC UA:n keräämän datan saa räätälöityä omaan tarkoitukseen esikäsitteilyllä, kuten esimerkiksi reuna- ja sumulaskennalla. Reunalaskelmassa IoT-laitteiden tuottama datan analysointi ja tallennus tapahtuvat lähellä sen keräyspistettä. Sumulaskenta asettaa tapahtumat ja resurssit verkon reunaan. Sumulaskenta tarkoittaa siis toimintaa verkon päissä, eikä toimi keskitetystä pilvipalvelusta käsin. Esikäsitteily vähentää OPC UA-palvelimen saamaa reaaliaikaisen datan määrää siten, että vain hyödyllinen data esimerkiksi anturilta toimitetaan OPC UA-palvelimelle. Tämä on OPC UA:n tietomallin loogisen rakenteen tarkoitus. Tiedot korreloidaan osoiteavaruuden solmujen kanssa ja niiden vastaavat komponentit ryhmitetään tietomallissa, jonka avulla palvelin koodaa vaaditut tiedot standardoiduksi viestiksi ja lähettää ne asiakkaalle. Paikalliset OPC UA-asiakkaat tarjoavat paikallisen verkon avulla paremman reaaliaikaisen suorituskyvyn. OPC UA-asiakkaat voivat pyytää palvelimelta tietoja, joita ne analysoivat ja käsittelevät niitä mukauttamalla algoritmeja ja tätä kautta tarjoavat apuja prosessien, kuten valvonnan päätöksen tekoon (Univeristy of Auckland, 2019; EC Council, 2023).

## 5.1 Esimerkkejä OPC UA:n käytöstä datan keruussa laivoissa

### 5.1.1 Meyer Turku ja Semantum

Meyer Turku panostaa myös energiatehokkaisiin ja vähäpäästöisiin ratkaisuihin niin telakalla, kuin laivoissaan. Meyer Turku on ottanut tavoitteeksi rakentaa hiilineutraalitelakka vuoteen 2030 mennessä. Tavoitteen saavuttamiseksi on tehty useita merkittäviä tekoja, kuten kaukolämmön käyttöönotto ja päästöneutraalia sähkön käyttö telakalla. Kamiinoissa, joilla laivaa lämmitetään rakennusvaiheessa, on siirrytty käyttämään HVO:ta (Hydroted Vegetable Oil) polttoöljyn sijasta. Vuoteen 2025 mennessä Meyer Turku tavoittelee 7,5%:n energiakulutuksen säästöä. Laivanrakennuksessa on mahdollista konkreettisilla teoilla, kuten materiaali- ja polttoainevalinnoissa saada merkittävästi pienennettyä alan päästöjä (turku.fi, 2023).

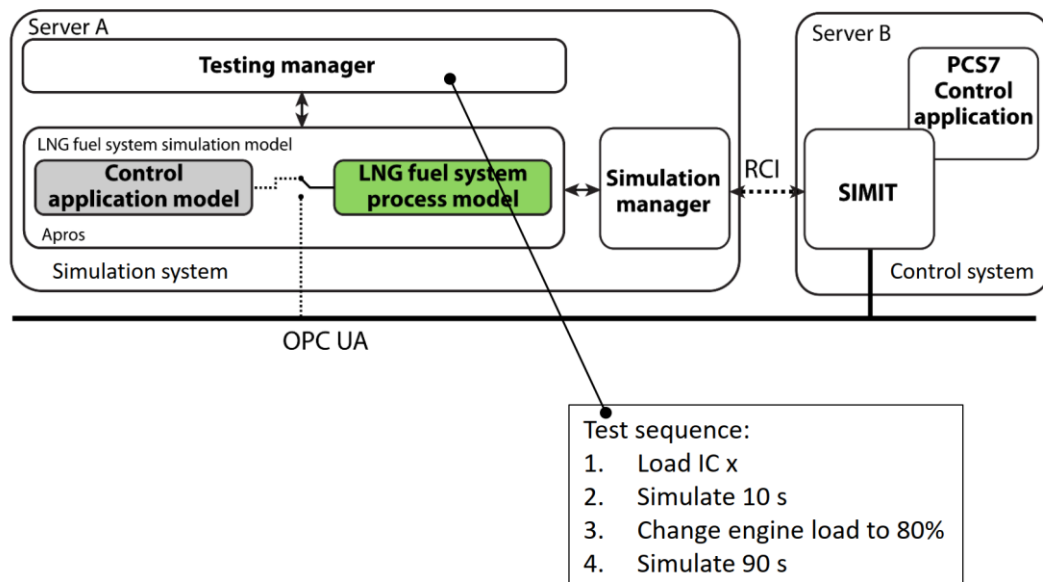
Risteilijäalukset modernisoituvat ja vaativat enemmän automaatiota. Uusien teknologioiden kehittyessä myös datan kerääminen lisääntyy ja monimutkaistuu. Meyer Turku pyrkii rakentamaan laivat mahdollisimman vähäpäästöisesti ja vähäpäästöisiksi. Varustamot vaativat myös eri ratkaisuja polttoaineisiin ja materiaalien käyttöön laivoissa, jotta niistä saataisiin mahdollisimman vähäpäästöisiä ja tätä kautta vastaamaan nykyisiä ja tulevia määräyksiä ja standardeja. Esimerkiksi Meyer Turun rakentamassa Icon Of the Seas laivassa on LNG:n (liquefied natural gas) käyttöön pääasiallisena polttoaineena.

LNG on suomeksi nesteytettyä maakaasua, joka jäähdytetään noin -160 °C pysyäkseen nesteenä, jonka seurauksena se tiivistyy 600-kertaisesti. Tällöin sen varastoiminen on helpompaa ja käyttö mahdollista risteilyaluksien polttoaineena. LNG:n käyttö on huomattu hyväksi vaihtoehdoksi erilaisiin laivatyyppeihin, kuten risteilijäaluksiin. Meyer Turun telakalla on rakennettu ja ollaan rakentamassa useita LNG:llä toimivia laivoja (Suomen Automaatioseura, 2021).

Yhdellä suurella risteilijällä simuloitiin OPC UA –pohjainen avustettu automaatiotestaus ympäristö risteilyaluksen LNG –järjestelmästä. Testaus suoritettiin Meyer Turun ja Semantumin yhteistyössä ja tarkoituksena oli selvittää LNG –järjestelmän toimintaa merenkulussa (Suomen Automaatioseura, 2021).

Simulaatiotestissä käytettiin MIL/SIL konfiguraatiota. MIL/SIL (Model-in-the-Loop/Software-in-the-Loop) ovat yleisiä simulointimenetelmiä, jossa MIL takaa tarkkuuden ja hyväksyttävyyden käyttämällä ohjausalgoritmin laitosmallia ja SIL tarkistaa luodun koodin käyttäytymisen hyväksymisen. Kyseisessä testissä MIL/SIL konfiguraatioita käytettiin LNG polttoainejärjestelmän suunnittelu prosessin tarkistamiseen, analysoi polttoainejärjestelmän käyttäytymistä erilaisissa olosuhteissa, arvioi ohimenevää vaikutusta polttoaineeseen ja yhteisen toiminnan apujärjestelmien ehtoihin, stabiloivien ohjaussilmukoiden käyttäytymiseen ja ohjaimen turvatoimintojen tarkistamiseen.

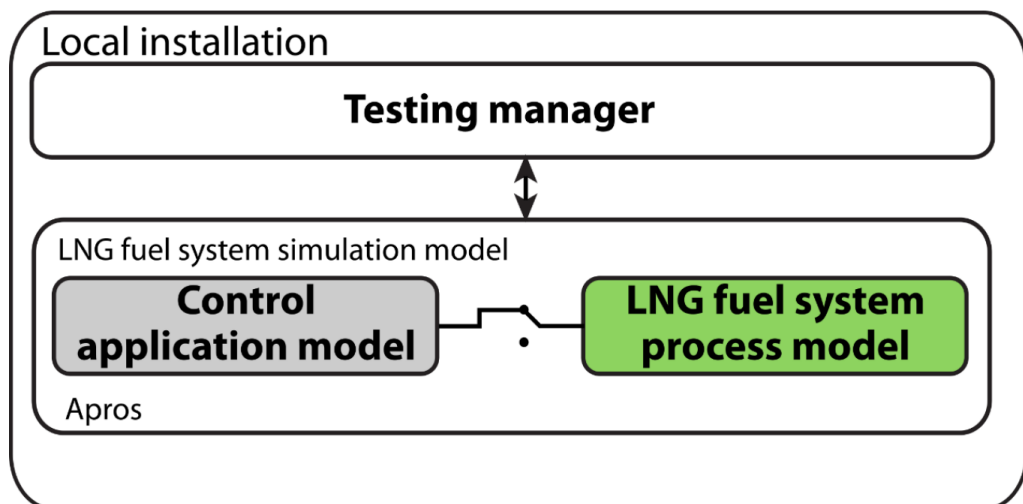
### MIL/SIL OPC UA-based testing environment architecture



Kuva 12. OPC UA pohjainen simulaatioympäristö MIL/SIL testausta varten (Suomen Automaatioseura, 2021).

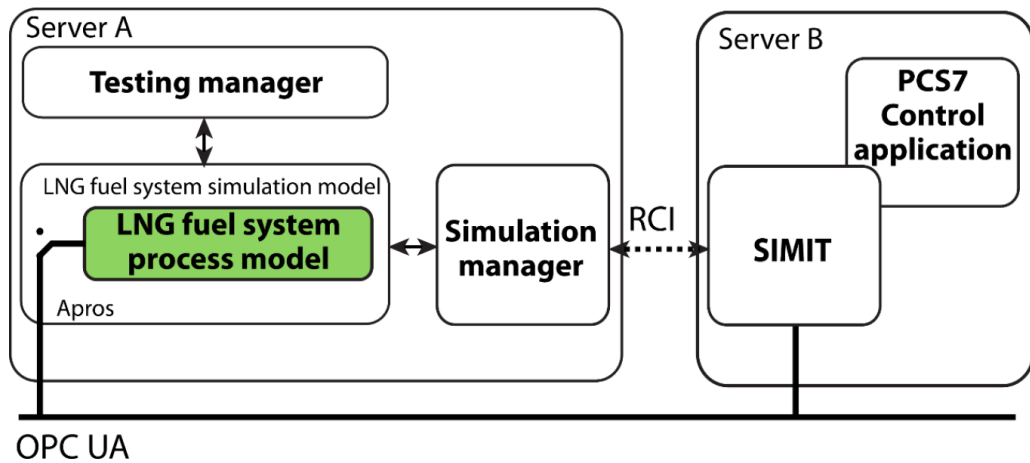
Simulointiympäristö sisälsi muun muassa OPC UA Clientin, LNG polttoainejärjestelmä prosessisimulaatiomallin, jossa malli voidaan liittää OPC UA:n kautta. Simulaation hallintana käytettiin Aprosin laajennusta, joka tarvittiin synkronoinnin hallintaan simulaation ja DCS –järjestelmien välillä. Ohjaussovellus on konfiguroitu käyttäen Siemensin PCS7:ää. OPC UA serverinä oli Siemensin SIMIT OPC UA, jonka avulla kommunikointiin MIL/SIL testauksen aikana ulkoisten järjestelmien kanssa. SIMIT osoiteavaruus paljasti kaikki tunnisteet, jotka olivat saatavana PCS7 ohjaussovelluksesta.

## MIL configuration



Kuva 13. MIL konfigurointi OPC UA pohjaisessa simulaatioympäristössä (Suomen Automaatioseura, 2021)

## SIL configuration



Kuva 14. SIL konfigurointi OPC UA pohjaisessa simulaatioympäristössä (Suomen Automaatioseura, 2021)

Kuvissa 13 ja 14 on havainne kuva MIL ja SIL konfiguraation arkkitehtuureista. Kuvissa esitetään OPC UA:han liittyvät toteutustiedot, jossa SIMIT OPC UA serveri paljastaa ohjaussovelluksen osoitetilan AproS clientille. Sen lisäksi tietoliikenne tapahtuu yli 200 tunnisteiden välillä, missä OPC UA:ta käytetään prosessi- ja ohjausmuuttujien vaihtoon ohjaussovelluksen ja prosessimallin välillä.

MIL/SIL testauksen lopputuloksena oli, että OPC UA pohjainen arkkitehtuuri on kehitetty tätä tarkoitusta varten. Se onnistuu käsittelemään onnistuneesti prosessien ja automaation muuttujien arvot, mutta jäljelle jäi silti simulaatio-synkronoinnin käsittelyn tarve erilaisella viestintä mekanismilla (Suomen automaatioseura, 2021).

### 5.1.2 MSC Cruises

MSC Cruises – joka on maailman neljänneksi suurin risteilyvarustamo maailmassa – käytti MSC Meraviglia laivassaan valvonta- ja ohjausjärjestelmänä ICONICS GENESIS64 –ohjelmistoa. Sillä on laivassa noin 6 000 fyysistä I/O- (tulo/lähtö) pistettä, sekä lisäksi noin 15 000 tietoliikenteen I/O- pistettä, jotka on kytketty järjestelmän kautta (opcfoundation, 2017).

ICONICS tuotti laivaan OPC UA sertifioidun HMI/SCADA –ohjelmiston, GENESIS64:n. ICONICS GENESIS64 –ohjelmisto perustuu ICONICSin alustapalveluihin, jotka sisältävät yleisen liitettävyyden OPC UA:han ja useisiin muihin tietoliikenneprotokolliin. Genesis64 tekee OPC UA –rajapinnan kautta helppoksi visualisoida kaikki laitteet, prosessit, toiminnot tai liiketoiminnot. Siksi OPC UA:n asiakkaat voivat laivassa käyttää turvallisesti tietoja muun muassa laitteiden huoltotiedoista, energiatiedoista, tilaustiedoista mistä tahansa ERP-järjestelmästä sekä rekistereistä ja tiedoista käytännössä mistä tahansa PLC- tai DSC- järjestelmästä (opcfoundation, 2017).

OPC UA:n viestintäprotokollan avulla voitiin tarjota kriittisille automaatiojärjestelmille turvallinen datan kerääminen. OPC UA:n toteutus laivassa tarjosi useita suojakerroksia, kuten käyttäjien ja auktoriteetin luoman varmenteen valtuutuksen, symmetrisin salauksen ja allekirjoitukset kaikessa viestinnässä, joka takaa tiukan käyttäjän todennuksen (opcfoundation, 2017).

## 6 YHTEENVETO

OPC UA on viestintäprotokollana yksi käytetyimmistä ja yleisimmistä teollisuusautomaation viestintäprotokollista. Sen käyttäminen laivoissa viestintäprotokollana vähentäisi suunnittelutyötä, tuotannonkustannuksia ja parantaisi kyberturvallisuutta. Se läpäisee kaikki vaadittavat sertifikaatit ja säädökset, jopa risteilijöissä, joissa on erittäin tarkat säädökset ja lait. Sen skaalautuva, käyttöjärjestelmästä riippumaton ja palvelukeskeinen arkkitehtuuri soveltuu niin datan keräämiseen kuin tiedonsiirtoon laivoissa.

Vaikka OPC UA:n julkaisusta on aikaa, sitä kehitetään jatkuvasti paremmaksi. Sertifikaatti on suunniteltu turvalliseksi kyberhyökkäyksiä vastaan ja alustariippumattomuus sekä ainutlaatuinen tietomalli antavat OPC UA:lle suuren valikoiman käyttömahdollisuuksista laivoissa.

Protokollan positiiviset puolet ovat mittavat ja soveltuvat hyvin risteilijäalukien automaatiojärjestelmien käyttöön. Mutta OPC UA:n käyttäminen vaatii kuitenkin suuria investointeja, mikäli protokolla vaihdetaan suureksi osaksi laivanjärjestelmien välistä tiedonsiirtoa liian nopeasti. Kuitenkin on huomioitavaa että, OPC UA protokollaa on käytetty datan keruussa ja tiedonsiirrossa moderneissa laivoissa ja sen näytöt ovat positiivisia.

OPC UA:n käyttö tulee lisääntymään tulevaisuudessa. Suuret alan yritykset ovat mukana kehittämässä OPC UA:n ympäristöä monipuolisemmaksi ja turvallisemmaksi. OPC Foundation järjestöön, joka kehittää OPC UA protokollaa kuuluu yli 900 yritystä eri teollisuuden aloilta ja heillä on OPC –yhteensopivia tuotteita useita tuhansia. OPC UA:n tulevaisuus näyttää siis hyvältä ja kehityskohteina ovat laajennukset koskien IloT:a ja kyberturvallisuutta. Kuitenkin tärkein kehityssuunta on parempi skaalautuvuus erilaisten järjestelmien ja systeemien välillä. Myös käyttöönottoa pyritään kehittämään käyttökokemuksien parantamiseksi, lisäämällä esimerkiksi toimittajia, automaattista käyttöönottoa ja analytiikan kehittämistä.

Opinnäytetyötä tehdessäni tutustuin ensikertaa OPC UA:han. Lopputuloksesta tuli hyvä ja työn toteutus sujui hyvin ja aikataulussa. Näkisin, että työlle on mahdollista keksiä jatkotutkimuksia aiheesta.

## LÄHTEET

Meyer Turku Oy. Yritys. Verkkoaineisto. Viitattu: 8.12.2023.

<https://www.meyerturku.fi/fi/yritys/index.jsp>

Pietiläinen T. 4.8.2014. Turun telakka on myyty valtiolle ja saksalaisille – uusi omistaja lupaa työpaikkojen säilyvän. Helsingin Sanomat. Viitattu: 8.12.2023.

<https://www.hs.fi/talous/art-2000002750803.html>

OPC Foundation. What is OPC? Verkkoaineisto. Viitattu: 8.12.2023.

<https://opcfoundation.org/about/what-is-opc/>

OPC Foundation. Unified Architecture. Verkkoaineisto. Viitattu: 8.12.2023.

<https://opcfoundation.org/about/opc-technologies/opc-ua/>

Process Genius. Mikä on OPC UA ja miksi se on tärkeä digitaaliselle kakso-  
selle. Verkkoaineisto. Viitattu: 8.12.2023

<https://shorturl.at/flrPT>

OPC Router. What is OPC UA. Verkkoaineisto. Viitattu 12.12.2023.

<https://www.opc-router.com/what-is-opc-ua/>

OPC7.com. What is OPC UA. Verkkoaineisto. Viitattu 12.12.2023.

<https://www.opc7.com/what-is-opc-ua/>

Beckhoff Suomi, OPC Unified Architecture (UA). Verkkoaineisto Viitattu  
12.12.2023.

<https://www.beckhoff.com/fi-fi/products/automation/opc-ua/>

Epicor. What is Industry 4.0—the Industrial Internet of Things (IIoT)?  
Verkkoaineisto. Viitattu: 12.12.2023.

<https://www.epicor.com/en/blog/what-is-industry-4-0/>

Jürgen Jasperneite & Volker Lohweg (2018), Kommunikation und Bildverarbeitung in der Automation, Springer Vieweg.

Heikkilä, M. (2016). OPC UA AUTOMAATION TIEDON-SIIRROSSA [YAMK-opinnäytetyö, Tampereen Ammattikorkeakoulu]  
<https://urn.fi/URN:NBN:fi:amk-2016061713162>

OPC Foundation. UA Part 1, Version 1.04. Verkkoaineisto. Viitattu: 14.12.2023.  
<https://reference.opcfoundation.org/Core/Part1/v104/docs/#>

InduSoftVideo. 26.4.2012. InduSoft OPC Webinar [video]. Youtube.  
<https://www.youtube.com/watch?v=gsHaJpnjv28&t=1172s>

OPC Foundation. UA Part 3, Version 1.05.03. Verkkoaineisto. Viitattu: 19.12.2023.  
<https://reference.opcfoundation.org/Core/Part3/v104/docs/4>

OPC Foundation. UA Part 15, Version 1.05.03. Verkkoaineisto. Viitattu: 19.12.2023.  
<https://reference.opcfoundation.org/Core/Part2/v105/docs/4>

Dataexel. Modbus RTU vs. Modbus TCP: What Are The Differences? Verkkoaineisto. Viitattu: 4.1.2024.  
<https://www.datexel.com/modbus-rtu-vs-modbus-tcp-what-are-the-differences.html>

Opc7. OPC UA vs. Modbus. Verkkoaineisto. Viitattu: 4.1.2024.  
<https://www.opc7.com/opc-ua-vs-modbus/>

Leino, V. (2022). Tiedonsiirtotavat ja yhteyksien määrittely laivojen integroidussa automaatiojärjestelmässä. [AMK-opinnäytetyö, Satakunnan Ammattikorkeakoulu].  
<https://urn.fi/URN:NBN:fi:amk-2022091420156>

Encyclopedia. Ship Automation System and Ship Data Collection. Verkkoaineisto. Viitattu: 9.1.2024.

<https://encyclopedia.pub/entry/51758>

Turku. 5 kysymystä ilmastoteoista: Hiilineutraali telakka 2030. Verkkoaineisto. Viitattu: 9.1.2024.

[https://www.turku.fi/uutinen/2023-11-29\\_5-kysymysta-ilmastoteosta-hiilineutraali-telakka-2030](https://www.turku.fi/uutinen/2023-11-29_5-kysymysta-ilmastoteosta-hiilineutraali-telakka-2030)

OPC Foundation. Breaking Down Your System's Obstacles to OPC UA Adoption. Verkkoaineisto. Viitattu 9.1.2024.

<https://opconnect.opcfoundation.org/2017/10/breaking-down-your-systems-obstacles-to-opc-ua-adoption/>

Anybus. Exploring OPC UA's use cases and benefits in industrial environments. Verkkoaineisto. Viitattu: 9.1.2024

<https://www.anybus.com/about-us/news/2023/07/11/exploring-opc-ua%27s-use-case-and-benefits-in-industrial-environments>

Traficom. Kyberturvallisuus ISM & ISPS. Verkkoaineisto. Viitattu: 9.1.2024.

[https://www.traficom.fi/sites/default/files/media/file/1.%20Kyberturvallisuus%20ISM%20%26%20ISPS\\_JW.pdf](https://www.traficom.fi/sites/default/files/media/file/1.%20Kyberturvallisuus%20ISM%20%26%20ISPS_JW.pdf)

OPC Foundation. Exploring Cybersecurity and OPC UA for a Secure System Architecture. Verkkoaineisto. Viitattu: 10.1.2023.

<https://opconnect.opcfoundation.org/2021/12/exploring-cybersecurity-and-opc-ua-for-a-secure-system-architecture/>

Smart Ship Technology. Ship sensors data collection and analysis for condition monitoring of ship structures and machinery systems. Verkkoaineisto. Viitattu: 10.1.2024.

<https://strathprints.strath.ac.uk/57271/>

Suomen Automaatioseura. OPC UA Enables Secure Data Transfer and System Integrations in Private and Public Networks. Verkkoaineisto. Viitattu: 11.1.2023

<https://www.automaatioseura.fi/site/assets/files/1550/f2068.pdf>

IEC. Homepage. Verkkoaineisto. Viitattu 11.1.2024.

<https://www.iec.ch/homepage>

Real time automation. OPC UA and the Internet. Verkkoaineisto. Viitattu: 16.1.2024.

<https://www.rtautomation.com/rtas-blog/opc-ua-and-the-internet/>

MathLabSolutions. What is MIL SIL? Why do we compare MIL and SIL performance of a Simulink (MATLAB) model? Verkkoaineisto. Viitattu: 16.1.2024.

<https://www.matlabsolutions.com/matlab/what-is-mil-sil-why-do-we-compare-mil-and-sil-performance-of-a-simulink-matlab-model.php>

Wärtsilä. NACOS Platinum OPC UA. Verkkoaineisto. Viitattu: 18.1.2024.

<https://www.wartsila.com/voyage/integrated-vessel-control-systems/automation/opcua>

IEC. IEC 61162-460:2018. Verkkoaineisto. Viitattu: 18.1.2024.

<https://webstore.iec.ch/publication/32322>

Tomi Peltokangas & Janne Käsäkoski (2017). OPC UA –arkkitehtuurin toteutus ja testaus teollisuusautomaatiossa. Viitattu: 23.1.2024.

<https://urn.fi/URN:ISBN:978-952-7173-31-2>

University of Auckland. Chao Liu, Hrishikesh Vengayil, Yuagian Lu & Xun Xu. A Cyber-Physical Machine Tools Platform using OPC UA and MTConnect. Verkkoaineisto. Viitattu: 30.1.2024

<https://doi.org/10.1016/j.jmsy.2019.04.006>

OPC Foundation. Part 11, Version 5.4.2. Verkkoaineisto. Viitattu: 5.2.2024.

<https://reference.opcfoundation.org/Core/Part11/v104/docs/5.4.2>

EC Council. What is Fog Computing. Verkkoaineisto. Viitattu: 13.2.2024.

<https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/fog-computing-everything-to-know/>

OPC Foundation. Interoperability for Industrie 4.0 and the Internet of Things, 2023. s. 13. Verkkoaineisto. Viitattu: 21.2.2024.

<https://rb.gy/wx1q0k>

Ascolab. OPC UA Data Model. Verkkoaineisto. Viitattu: 21.2.2024.

<https://www.ascolab.com/technology-unified-architecture/meta-model.html?lang=en>

OPC Foundation. Part 10, Version 1.05.00. Verkkoaineisto. Viitattu 21.2.2024.

<https://reference.opcfoundation.org/Core/Part10/v104/docs/4.1>

IACS. UR E27 REV1 CLN. Verkkoaineisto. Viitattu 27.2.2024.

<https://iacs.org.uk/resolutions/unified-requirements/ur-e>