Aleksi Koskela

Teollisuuden automaatioverkot

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Sähkö- ja automaatiotekniikka
Insinöörityö
4.5.2023

Tiivistelmä

Tekijä:	Aleksi Koskela
Otsikko:	Teollisuuden automaatioverkot
Sivumäärä:	29 sivua
Aika:	4.5.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Automaatiotekniikka
Ohjaajat:	Jarno Pispala, vanhempi suunnittelija Reijo Leinonen, lehtori

---

Tämä insinöörityö toteutettiin Tervakoski Oy:lle, joka on osa Delfortgroup AG -konsernia. Insinöörityön yhteydessä luotiin Tervakosken tehtaalle uusi automaatio- ja tietoliikenneverkkojen dokumentaatiojärjestelmä tukemaan verkkojen laajentamista ja kunnossapitoa.

Insinöörityön teoriaosassa perehdytään automaatioverkkojen rakenteeseen, toimintaan ja osiin. Tämän lisäksi työssä käsitellään OPC- ja OPC UA -rajapintoja, niiden tietoturvaa sekä perehdytään Microsoft DCOM -tietoturvakovennukseen, sen taustoihin ja sen vaikutuksiin OPC-rajapintoihin.

Työn lopputuloksena saatiin tuotettua tehtaalle toimiva dokumentaatiojärjestelmä, joka tukee eri osastojen toimintoja tulevaisuudessa. Projektin myötä tehtaalle syntyi oma monialainen työryhmä edistämään tietoliikenneverkkojen ja niiden dokumentaation kehitystä vielä projektin päätyttyä.

Avainsanat: Automaatioverkko, DCOM, OPC

Abstract

Author:	Aleksi Koskela
Title:	Industrial Automation Networks
Number of Pages:	29 pages
Date:	4 May 2023
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and Automation Engineering
Professional Major:	Automation Engineering
Supervisors:	Jarno Pispala, Senior Planning Engineer
	Reijo Leinonen, Senior Lecturer

This thesis work was commissioned by the paper manufacturing company Tervakoski Oy, which is a subsidiary of Delfortgroup AG. The goal of the thesis project was to create and implement a new documentation system for IT and automation networks for the Tervakoski factory. The new documentation system was created to support the design and maintenance of the factory's industrial networks.

The theoretical part of the thesis deals with the structure, operation, and different parts of industrial automation networks. In addition, the thesis deals with OPC and OPC UA interfaces, their security, as well as Microsoft DCOM security hardening and its impacts on OPC interfaces.

As a result of the thesis work, a new documentation system was created for the factory and a new multidisciplinary working group was set up to promote the development of industrial IT- and automation networks and their documentation even after the project has been completed.

Keywords: Automation network, DCOM, OPC, DCOM Hardening

Sisällys

Lyhenteet

1 Johdanto 1

2 Teollisuuden automaatioverkot 2

2.1 Automaatioverkon laitteet 2
2.2 Automaatioverkon tietoturvatasot 2
2.3 Automaatioverkkojen tiedonsiirto 7
2.4 Ethernet 7
2.5 Valokuidut 7
2.6 Tiedonsiirtostandardit 9
2.6.1 OSI-malli 9
2.6.2 Modbus 10

3 OPC 11

3.1 OPC Classic 12
3.1.1 OPC Data Access 12
3.1.2 OPC Alarms & Events 13
3.1.3 OPC Historical Data Access 13
3.2 Microsoft Component Object Model 13
3.3 OPC UA - Unified Architecture 18
3.4 OPC UA:n Tietoturva 19

4 Automaatio- ja tietoliikenneverkkojen dokumentointi 21

4.1 Dokumentaatio 21
4.2 Dokumentaation kehittäminen 21
4.2.1 Dokumentaation sähköistäminen 22
4.2.2 Tietokanta 22
4.2.3 Fyysinen dokumentaatio 23
4.2.4 Yhteyskartta 24

5 Yhteenveto 25

Lähteet 27

Lyhenteet

DCS *Distributed Control System* eli hajautettu ohjausjärjestelmä on tietokonepohjainen automaation ohjausjärjestelmä.

HMI *Human-Machine Interface.* Paikallinen käyttöliittymä, jolla voidaan seurata ja ohjata jotain prosessin osaa.

I/O *Input/Output.* Ohjelmoitavan logiikan tulo- ja lähtömoduuli, jonka avulla logiikka liitetään kenttälaitteisiin.

LAN *Local Area Network.* Paikallisverkko eli pienen alueen kattava tietoliikenneverkko, esim. tehtaan tai kodin tietoliikenneverkko.

OLE *Object Linking and Embedding* on Microsoftin kehittämä teknologia, joka mahdollistaa objektien linkittämisen ja upottamisen kohdesovellukseen.

PLC *Programmable Logic Controller* eli ohjelmoitava logiikkaohjain. Automaatiossa käytetty tietokone, jolla ohjataan teollisia prosesseja.

RTU *Remote Terminal Unit.* Teollisuusautomaatiossa käytetty laite, joka yhdistää kenttälaitteet DCS- tai SCADA-järjestelmään.

SCADA *Supervisory Control And Data Acquisition.* Valvomo-ohjelmisto, jolla seurataan ja ohjataan prosessia keskitetysti.

WAN *Wide Area Network.* Laajaverkko tai suuralueverkko. Tietoliikenneverkko, joka kattaa suuria maantieteellisiä alueita.

1 Johdanto

Digitalisaation myötä automaatiojärjestelmien tiedonsiirron tarve on moninkertaistunut 2000-luvulla eikä näytä hidastumisen merkkejä. Informaatioajan jatkuvasti kehittyvät vaatimukset tuovat haasteita teollisuudelle. Luotettava ja turvallinen automaatio vaatii koko ajan laajempia ja monimutkaisempia tietoliikenneverkkoja tehokkaan tuotannon takaamiseksi.

Tämä insinöörityö tehdään tukemaan Tervakoski Oy:n toteuttamaa automaatioverkkojen laajennus- ja uusimisprojektia. Projektiin taustalla ovat automaation tietoliikenneverkkojen laajeneminen, kasvavat tietoturvavaatimukset ja Microsoft DCOM-tietoturvakovennuksen takia suoritettavat OPC-rajapintojen uusinnat. Insinöörityön teoriaosiossa käydään läpi automaatioverkkoja ja niiden tietoturvan teoriaa sekä perehdytään OPC-rajapintoihin. Työn yhteydessä luotiin Tervakoski Oy:lle uusi tietokantapohjainen tietoliikenneverkkojen dokumentaatiojärjestelmä. Järjestelmän taustoihin ja työprosessiin perehdytään työn lopussa.

Tervakoski Oy on paperitehdas, jolla on pitkä ja värikäs historia. Tehdas perustettiin 1818, jolloin lumppupaperia alettiin valmistamaan käsin. Tehtaalle hankittiin ensimmäinen paperikone 1850-luvulla. Ajan myötä tehdas kasvoi, ja sen ympärille muodostui kylä. Tervakoski tunnettiin aikanaan erityisesti savuke- ja rahapainopaperin valmistuksesta. Tehdas on historiansa aikana ollut mm. Suomen Pankin ja Stora Enson omistuksessa. [1.] Tehtaan pitkä ikä on merkittävässä osassa työarkea, sillä tehtaalla on rakennuksia ja tekniikkaa kahden vuosisadan ajalta, joka aiheuttaa ajoittain haasteita tehtaan kunnossapidolle. Tervakosken tehtaalla sijaitsee Suomen vanhin edelleen tuotantokäytössä oleva paperikone, PK3, joka on ollut tuotantokäytössä jo vuodesta 1905.

Nykyään Tervakoski Oy on osa itävaltalaista Delfortgroup AG -konsernia ja on yksi maailman johtavia erikoispaperien, kuten kaapelieristepaperien ja elintarvikepaperien valmistajia. Tehtaalla on tuotantokäytössä neljä paperikonetta ja yksi koepaperikone, jolla tehdään tutkimustyötä myös ulkopuolisille tahoille.

Tehdas työllistää nykypäivänä yli 340 työntekijää. Tehtaan tuotannosta yli 90 prosenttia menee vientiin. Tervakoski Oy:n liikevaihto vuonna 2021 oli noin 156 miljoonaa euroa.

2 Teollisuuden automaatioverkot

Automaatioverkko on teollisen prosessin ohjaus- ja valvontajärjestelmien välinen tietoliikenneverkko. Se on osa tuotantolaitoksen laajempaa tehdasverkkoa, joka tyypillisesti kattaa tehtaan kaikki tietotekniset toiminnot. Automaatioverkko haarautuu tehdasverkosta omaksi itsenäiseksi alaverkokseen. Automaatioverkko on tarkasti varjeltu osa verkkoa, jonka sisäistä tietoliikennettä suojellaan ja tietoliikenne verkon ulkopuolelle on tarkkaan säädeltyä ja liikennöintiä valvotaan palomuureilla. Verkon sisäiset toiminnot on segmentoitu ja eroteltu toisistaan toimintojen perusteella. Verkko koostuu useista erilaisista laitteista, laitekokonaisuuksista ja järjestelmistä.

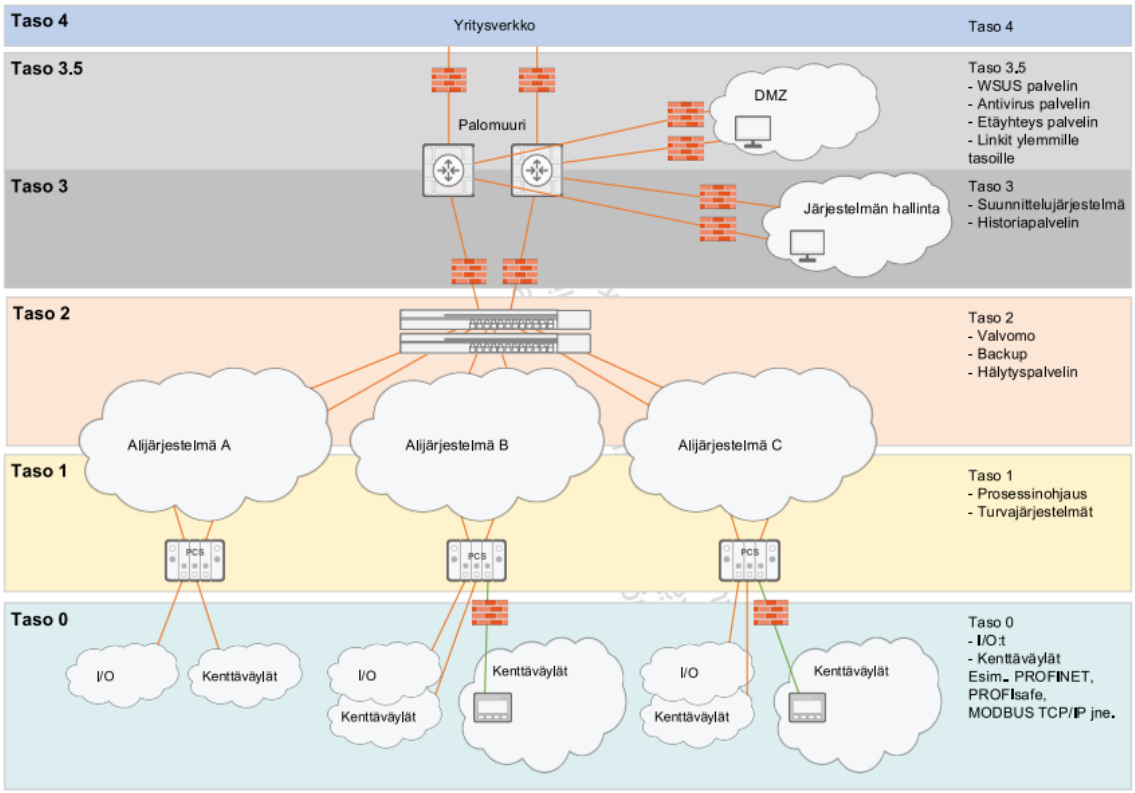
2.1 Automaatioverkon laitteet

Automaatioverkko koostuu yleisistä verkkolaitteista, joita kohtaa lähes kaikissa tietoliikenneverkoista kuten esimerkiksi palvelimista, kytkimistä, reitittimistä ja palomuureista. Tämän lisäksi automaatioverkoissa on automaatiolaitteita ja -järjestelmiä, joilla ohjataan ja valvotaan prosesseja, kuten ohjelmoitavia logiikkaohjaimia (PLC), prosessitietokoneita, prosessilaitteita, ohjausyksiköitä ja alaasemia.

2.2 Automaatioverkon tietoturvatasot

Turvallista automaatioverkon verkkoarkkitehtuuria määritellessä tulee lähteä siitä, että taataan tuotannon ja jakelun häiriöttömyys. Turvallinen ja luotettava arkkitehtuuri sisältää erilaisilla suojausratkaisuilla eroteltavia luottamustasoja. Luottamustasojen välille luodaan suojaus estämään paikallisten häiriöiden eteneminen eri luottamustasojen verkkoihin, laitteistoihin ja järjestelmiin. Automaatioverkon jako voidaan toteuttaa IEC-62443-standardin mukaisen

tietoturvavyöhykejaon avulla. IEC-62443-standardi jakaa automaatioverkon toiminnot ja järjestelmät viidelle eri luottamustasolle. Kuva 1 havainnollistaa automaatioverkon esimerkkiarkkitehtuuria (Valmet DNA), jonka tasot vastaavat IEC-62443-standardin luottamustasojen jakoa. [2. s. 103.]



Kuva 1. IEC-62443:ta mukaileva automaatioverkon esimerkkiarkkitehtuuri. [2. s. 104]

Standardin ylimmällä tasolla, tasolla 4, sijaitsee yritysverkko. Yritysverkko pitää sisällään kaikki yrityksen tietoliikenteen järjestelmät ja laitteistot. Yritysverkko liittyy automaatioverkkoon tasolla 3. Kuvassa 1 on luottamustaso 3 jaoteltu kahteen.

Taso 3.5 on eteisverkko, joka pitää sisällään palomuureja ja niin kutsutun ”demilitarisoidun alueen” (DMZ). DMZ on alaverkko, joka estää suorat yhteydet verkon muihin järjestelmiin. Eteisverkon tasolle sijoitetaan useasti myös etäyhteyspalvelin, joka mahdollistaa sisäverkon ulkopuolisten etäyhteyksien muodostamisen prosessitasolle. Tasolla 3 sijaitsevat laadunvarmistukseen,

tuotannonhallintaan ja työnkulkuun liittyvät järjestelmät, kuten historiatietokanta, tuotannon raportointi ja aikataulutus sekä hallinta- ja ohjaussovellukset.

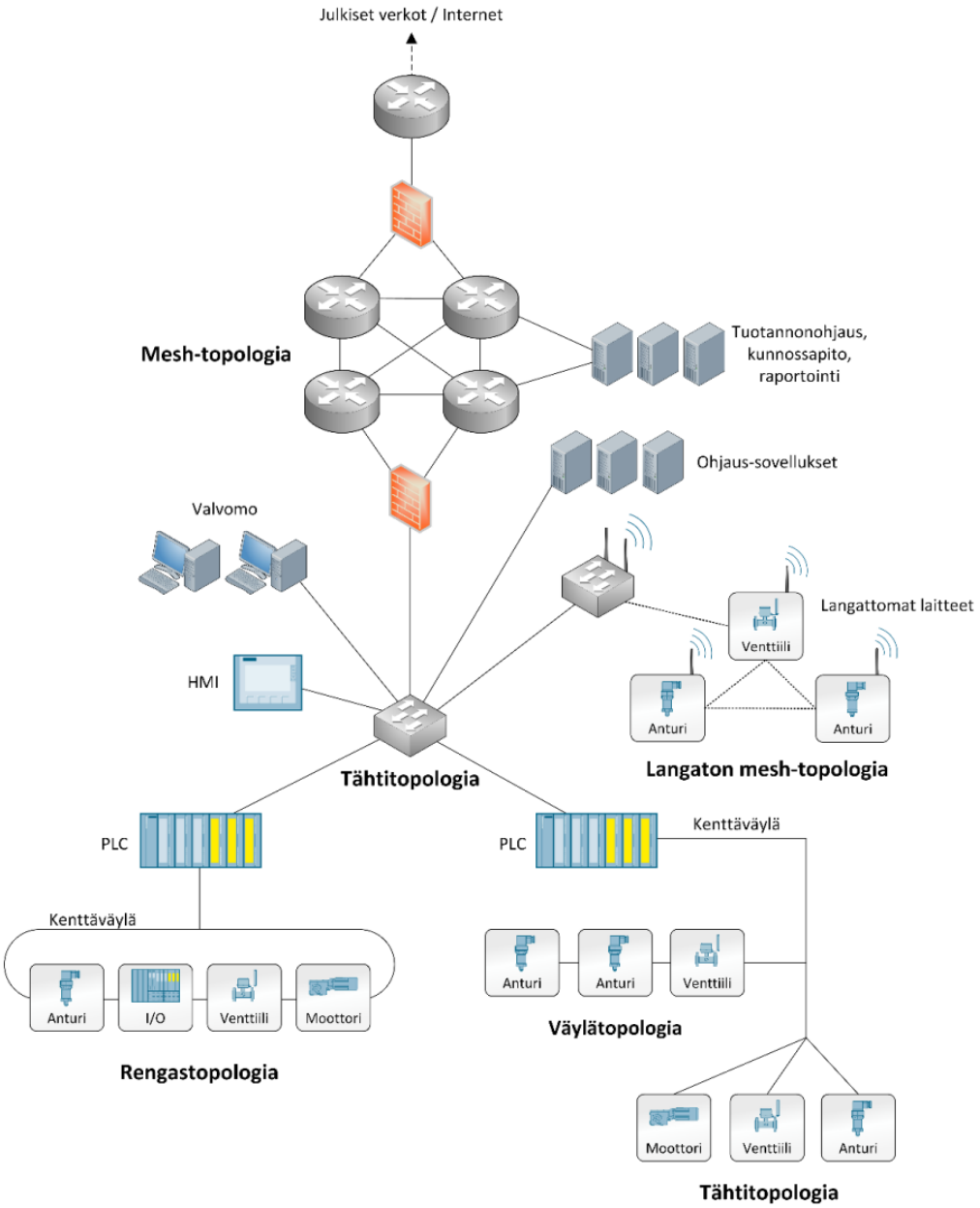
Tasolla 2 eli ”valvomotasolla” sijaitsevat prosessia ohjaavat sovellukset ja toiminnot. Tälle tasolle sijoittuvat valvomojärjestelmät eli SCADA-järjestelmät, prosessin paikalliset ohjausasemat eli HMI:t sekä hälytysjärjestelmät.

Taso 1 pitää sisällään automaatiojärjestelmän prosessia ohjaavat ja säätävät laitteet, kuten ohjelmoitavat logiikkaohjaimet (PLC) ja kaukokäytön ala-asemat (RTU). Tason 1 tehtävä on ohjata prosessia Tason 2 asettamien parametrien ja tason 0 tuottaman prosessidatan mukaan.

Taso 0 eli kenttätaso sisältää automaation kenttälaitteet, kuten anturit, toimitaitteet ja moottorit sekä automaatiojärjestelmien I/O:t. Kommunikaatio laitteiden ja järjestelmien välillä tapahtuu kenttäväylien välityksellä. Taso 0 kerää antureilla prosessidataa ja välittää sitä ylemmille tasoille ja ohjaa prosessia tason 1 ohjainten antamien komentojen perusteella.

Verkkotopologiat

Tietoliikenneverkot ovat todellisuudessa hankalasti hahmotettavia kokonaisuuksia, jotka ovat tyypillisesti laajalle hajautettuja ja erilaisia käyttötarkoituksesta ja -ympäristöstä riippuen. Verkkojen rakenteen hahmottamista helpottamaan on luotu topologiakarttoja verkoista. Topologiakartta on yksinkertaistettu kuvaus verkon rakenteesta ja sen eri osien liitynnöistä. Topologioita käytetään hyväksi uusia verkkoja suunnitellessa ja vanhoja laajennettaessa. Topologioiden ymmärtäminen auttaa helpottamaan verkon toimintaa ja rakennetta. Kuvassa 2 on esitetty havainnollistava topologiakartta, josta löytyy erilaisia topologioita.



Kuva 2. Havainnollistava kuva verkkojen eri topologioista. [3.]

Mesh-topologia

Mesh-topologia on paljon käytetty rakenne kriittisten laitteiden ja järjestelmien verkkoliitynnöissä. Mesh-topologiaa suositaan, kun verkolta vaaditaan suorituskykyä ja vikasietoisuutta. [3.] Mesh-topologian oleellinen piirre on sen redundanttinen rakenne, jolloin yhden tai useamman liitynnän vikaantuminen ei

vaikuta verkon suorituskykyyn ja toimintaan. Mesh-topologia on yleisesti käytetty myös langattomissa verkkoratkaisuissa.

Tähtitopologia

Tähtitopologian ominaispiirre on useamman kohteen liittäminen keskitettyyn tähtipisteeseen. Tähtipiste voi olla esimerkiksi Ethernet-kytkin. Tähtipisteestä haarautuviin liitäntöihin voidaan liittää erilaisia laitteita tai esimerkiksi kytkimiä, joilla saadaan luotua lisää tähtipisteitä. Tähtitopologia mahdollistaa tietoliikenteen eri laitteiden ja verkkojen välillä ilman, että muut laitteet ovat tietoisia viestinnästä. Tähtitopologian haittapuolena on, että tähtipisteen vikaantuessa koko siitä haaraantuva verkko menettää toimintakykynsä. [3.]

Rengastopologia

Rengastopologia on rakenteeltaan ympyränmuotoinen, eli sillä ei ole varsinaista päätepistettä. Verkon laitteet kytketään sarjaan ja sarjan viimeinen laite takaisin alkupään laitteeseen. Tämä tarkoittaa sitä, että jokaisella laitteella on vähintään kaksi liityntää verkkoon. Näin saavutetaan helposti toteutettava erittäin vikasietoinen verkko, joka kykenee jatkamaan toimintaansa, vaikka yksi renkaan linkeistä lakkaa toimimasta. Rengastopologian heikko piste on se laite, josta verkko saa alkunsa. Rengastopologia vaatii tarkoitukseen suunnitellut laitteet toimiakseen. [3.]

Väylätopologia

Erityisesti kenttäväylissä käytetty väylätopologia on rakenteeltaan lineaarinen topologia. Väylätopologiassa verkon laitteet kytketään ketjuttamalla sarjaan ja verkon päätepisteeksi kytketään päätevastus, signaalin heijastumisen estämiseksi. Väylätopologia on edullinen ja yksinkertainen rakenne, mutta kärsii useista ongelmista. Näitä ongelmia ovat mm. rakenteen heikko tietoturvallisuus, huono vikasietoisuus, huono suorituskyky ja rajallinen laitemäärä. [3.]

2.3 Automaatioverkkojen tiedonsiirto

Automaatioverkko on eritelty erilaisiin osakokonaisuuksiin tai segmentteihin. Tiedonsiirto automaatioverkon eri osien välillä tapahtuu yleensä valokuiduilla tai kuparikaapeleilla, sekä nykyään mahdollisesti myös langattomasti. Valokuituja käytetään erityisesti verkon ylemmillä tasoilla, joissa välimatkat ovat useasti pidempiä, siirrettävän tiedon määrät suurempia ja vaatimukset tiedonsiirron kapasiteetille korkeat. Nykyään myös alemmilla tasoilla ohjausjärjestelmät ovat digitalisaation myötä verkottuneet paljon. Tämä ja koko ajan kasvava tarve järjestelmien integraatiolle kasvattavat automaatioverkkojen kokoa, ja vaatimukset verkon tiedonsiirrolle kovenevat.

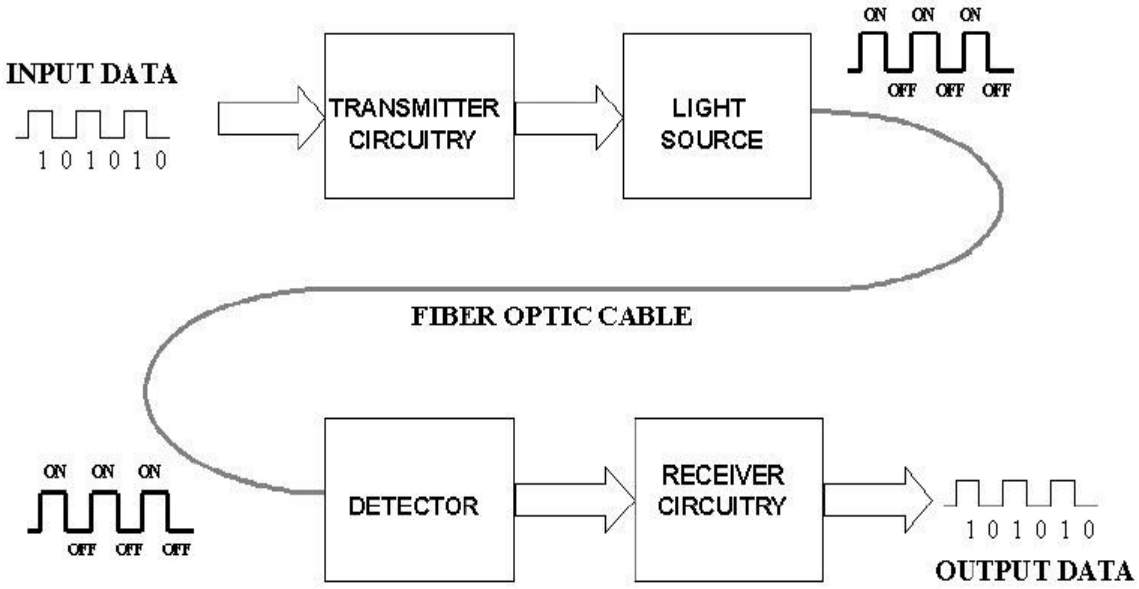
2.4 Ethernet

Ethernet on pakettipohjainen tiedonsiirtoprotokolla, jota käytetään laajasti verkkojen tiedonsiirrossa. Ethernet-protokollan määrittelee IEEE (Institute of Electrical and Electronics Engineers) -standardi 802.3. Ethernet on laajasti käytetty LAN- ja WAN-verkkojen tiedonsiirrossa. Ethernet toteuttaa OSI-mallin fyysisen- ja siirtoyhteyskerroksen, eli kerrokset 1 ja 2. Ethernet-tekniikka tukee valokuituyhteyksiä sekä parikaapelointia. Ethernet tukee laajasti eri tiedonsiirtonopeuksia alkaen 10 Mbit/s:stä, jopa 10 Gbit/s:iin asti.

2.5 Valokuidut

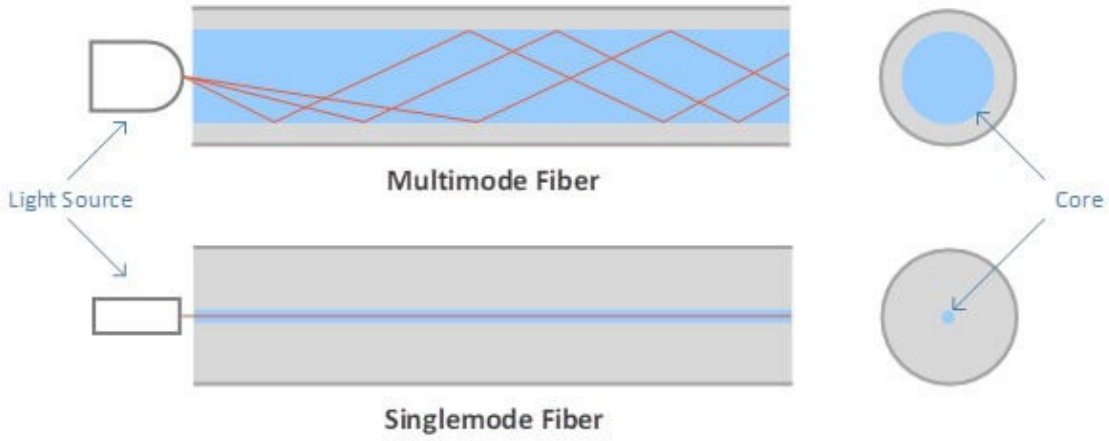
Valokuidut ovat muovista tai lasista valmistettuja kuituja, joita käytetään tiedonsiirrossa. Kuitu on valmistettu niin, että se johtaa valosignaaleja mahdollisimman pienellä signaalihäviöllä. Valokuiduilla saavutetaan korkeampia kaistanleveyksiä kuin perinteisellä kuparikaapeloinnilla. Valokuidun signaalihäviöt pidemmillä matkoilla ovat myös pienempiä kuin kuparikaapeleilla, mikä mahdollistaa pidemmät tiedonsiirtoetäisyydet. Valokuitujen signaalit eivät myöskään kärsi elektromagneettisen säteilyn aiheuttamista häiriöistä.

Valokuitujen valosignaali luodaan tyypillisesti sähkösignaalista lähettimen avulla. Lähetin vastaanottaa sähkösignaalin ja luo siitä valosignaalin laserin tai LED:n avulla. Tämän jälkeen valosignaali kulkee kuitua pitkin kuidun toiseen päähän, jossa se saavuttaa vastaanottimen. Vastaanotin muuntaa valosignaalin takaisin sähköiseksi signaaliksi ja lähettää signaalin sähköisenä eteenpäin.



Kuva 3. Yksinkertaistettu esitys valokuitutekniikan toimintaperiaatteesta. [4.]

Valokuidut jaetaan kahteen kategoriaan: yksimuotokuituihin (single-mode) ja monimuotokuituihin (multimode). Yksimuotokuidut ovat halkaisijaltaan pienempiä kuin monimuotokuidut, tyypillisesti 8–10 µm, kun taas monimuotokuitujen ydin on tyypillisesti kooltaan 50–100 µm. Monimuotokuitujen suurempi ydin tukee useampaa aaltomuotoa, mutta myös altistaa signaalin muotodispersiolle. Muotodispersio on signaaliaallon leviämistä ajan kuluessa johtuen valon muotojen eri nopeuksista kuidun ytimen sisällä. Tästä johtuen yksimuotokuitu soveltuu paremmin käyttötarkoituksiin, jossa vaaditaan korkeaa kaistanleveyttä, ja soveltuu paremmin pitkille tiedonsiirtoetäisyyksille pienemmän signaalihäviön ansiosta. Monimuotokuidun etu on pienempi hinta. Tämä johtuu monimuotokuidun paremmasta valon keräämiskyvystä, jonka vuoksi monimuotokuidun kanssa käytettävät komponentit ovat hinnaltaan edullisempia.



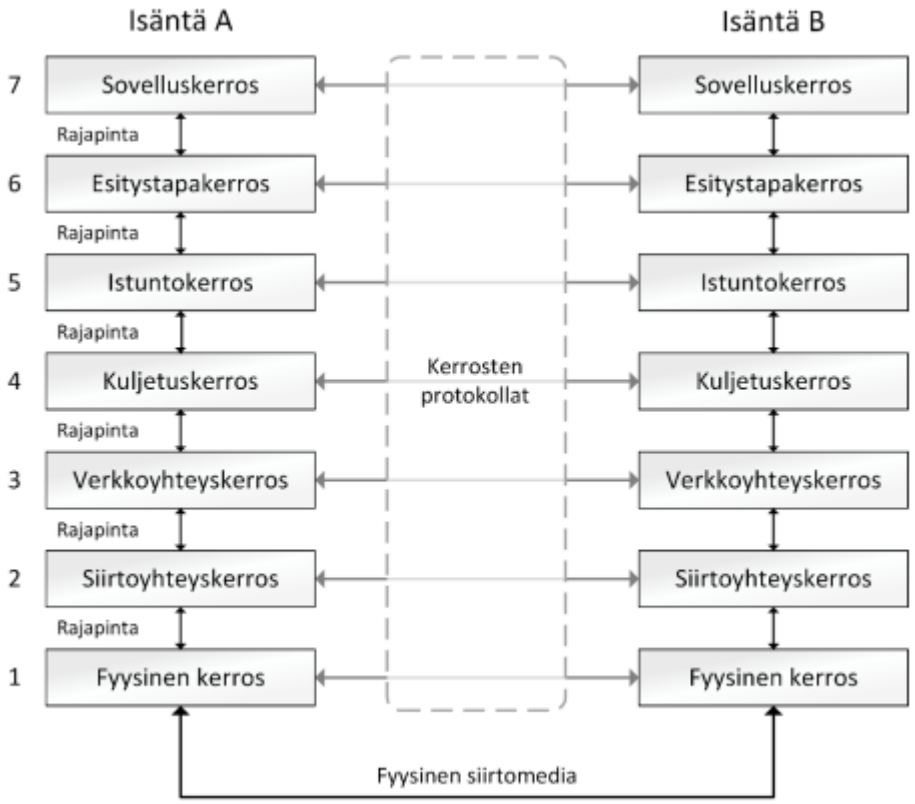
Kuva 4. Monimuoto- ja yksimuotokuitujen toiminta. [5.]

2.6 Tiedonsiirtostandardit

Tietoliikenneverkoissa käytetään tiedon liikuttelemiseen erilaisia tietoliikennestandardeja. Standardeja käytetään, jotta tietoliikenne tapahtuu halutuilla nopeuksilla, reaaliajassa ja turvallisesti. Verkkolaitteiden välisessä liikennöinnissä käytetään mm. TCP/IP-protokollaa, joka on pino (stack) verkkoliikennöinnissä käytettäviä tietoliikenneprotokollia. Teollisuusautomaatiossa käytetään myös tarkoitukseen kehitettyjä tiedonsiirtoratkaisuja. Näihin teollisuusautomaation tiedonsiirtostandardeihin kuuluvat esimerkiksi Modbus, Profibus ja Profinet.

2.6.1 OSI-malli

OSI-malli, eli Open Systems Interconnection refrence model on kansainvälisen standardijärjestön ISO:n (International Organization for Standardization) kehittämä seitsemän kerroksinen viitemallin avointen järjestelmien välisen kommunikaation määrittelemistä varten. OSI-malli toimii viitekehyksenä erilaisien standardien ja protokollien määrittelyssä. Malli yksinkertaistaa monimutkaiset verkkokokonaisuudet jakamalla kokonaisuudet kerroksiksi. [3.] OSI-mallin kerrokset on havainnollistettu kuvassa 5.



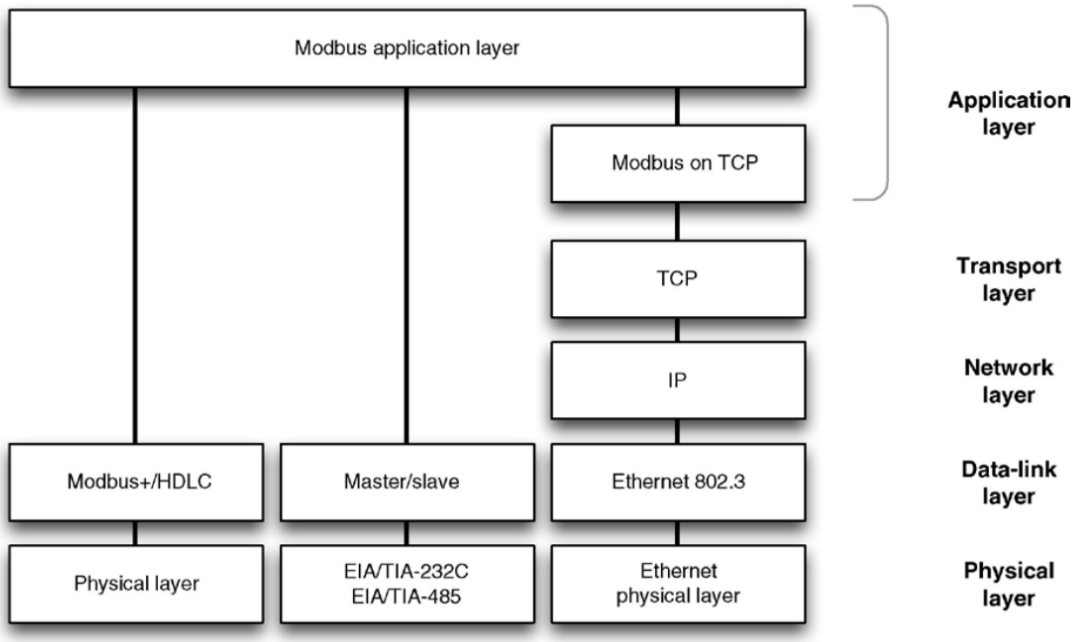
Kuva 5. OSI-viitemallin rakenne. [3.]

2.6.2 Modbus

Modbus on tietoliikenneprotokolla, jota on kehittänyt Modicon (nykyään osa Schneider Electriciä) 1970-luvulta lähtien. Modbus on jo vuosikymmeniä ollut yksi suosituimpia standardeja teollisuudessa. Modbus saavutti korkean suosionsa yksinkertaisuutensa ja helppokäyttöisyytensä ansiosta. Modbus oli alun perin sarjaliikenneprotokolla, mutta nykyään koostuu useammasta standardista, joihin kuuluvat mm. Modbus RTU, Modbus TCP/IP ja Modbus Plus. [6.]

Modbus-protokolla pohjautuu palvelin (server) – asiakas (client) -arkkitehtuuriin. Modbus on sovelluskerroksen standardi, eli se toimii OSI-mallin tasolla 7. Se mahdollistaa tehokkaan tietoliikenteen laitteiden välillä, yksinkertaisen pyyntö-vastaus (request-reply) -kommunikaationsa ansiosta. Modbusi-protokollaa käytettäessä kaikille kommunikoiville laitteille annetaan uniikki osoite, joiden avulla palvelin jakelee komentoja asiakkaille. Komento toimitetaan jokaiselle asiakkaalle, mutta siihen vastaa vain se asiakas, jolle käsky tai kysely on osoitettu.

Modbus -kommunikaatio vaatii verkon laitteilta hyvin vähän prosessointitehoa. Tämä tarkoittaa, että Modbus sopii hyvin esimerkiksi ohjelmoitavien logiikkaohjainten ja RTU-yksiköiden kommunikointiin. Ethernet-pohjaiset protokollat kuten Modbus TCP/IP eroavat perinteisestä mallista siten, että niissä kaikki laitteet voivat lähettää komentoja toisilleen.



Kuva 6. Havainnekuva Modbus-protokollan tiedonsiirtomallista. [7. s. 124]

Modbus on maailmanlaajuisesti yksi eniten käytettyjä tietoliikenneprotokollia teollisuudessa. Tämä johtuu osaksi siitä, että Modbus on avoin ja lisenssivapaa, sekä osaksi Modbus-protokollan yksinkertaisuudesta ja luotettavuudesta.

3 OPC

OLE for Process Control eli OPC on vuonna 1996 kehitetty avoin palvelin-asiakas (server-client) -arkkitehtuurin pohjautuva tiedonsiirtostandardi. Standardi luotiin helpottamaan teollisuusautomaation eri järjestelmien liittämistä toisiinsa ja täyttämään teollisuuden eri sovellusten vaatimukset. [8.] Ennen OPC-standardia laitetoimittajat joutuivat tuottamaan ja ylläpitämään lukuisia ajuriohjelmistoja tuotteilleen. Tämä oli kallista ja söi toimittajien resursseja. Täten alan

toimijat kerääntyivät yhteen vuonna 1995 ja perustivat OLE for Process Control -työryhmän. Tästä yhteistyöstä syntyi OPC:n ensimmäinen versio eli OPC 1.0, joka julkaistiin vuonna 1996. Tuolloin OPC oli vallankumouksellinen teknologia teollisuusautomaatiossa ja nousikin nopeasti teollisuusstandardiksi. OPC on ollut merkittävässä roolissa teollisuusautomaation kehityksessä sen julkaisusta lähtien. OPC tarjoaa edellytykset yritystason tietojärjestelmien, kuten ERP- (Enterprise Resource Planning) ja MES (Manufacturing Execution System) -järjestelmien tehokkaalle integroinnille. [9.]

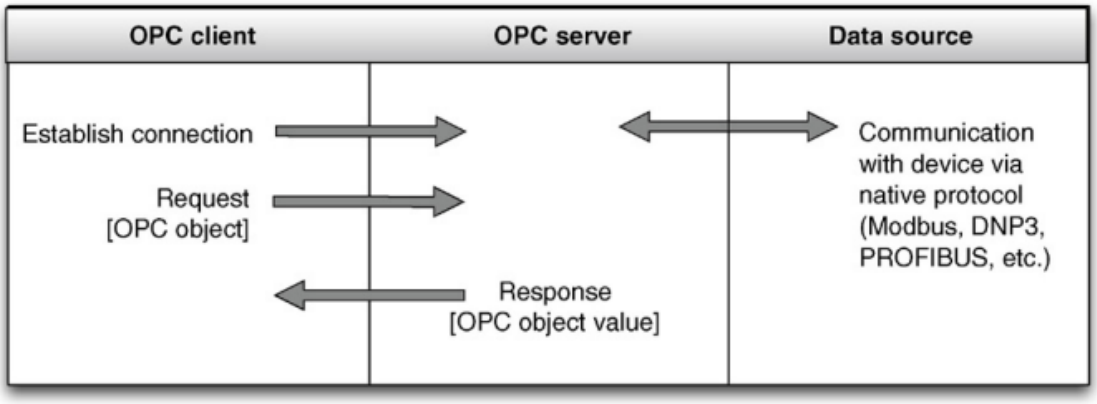
Vuonna 1996 perustettiin riippumaton ja voittoa tavoittelematon OPC Foundation kehittämään ja ylläpitämään OPC-standardia. OPC Foundationin jäsenet ovat joukko maailman johtavia automaatiotekniikan laitetoimittajia, instituutioita ja ammattilaisia.

3.1 OPC Classic

OPC Classic on joukko OPC-määrittelyitä, jotka perustuvat Microsoft Windows COM ja DCOM -teknologioihin. COM/DCOM -tekniikka sitoo OPC:n Microsoft Windows -alustalle eikä muita käyttöjärjestelmiä tueta. Tämä riippuvaisuus Windows-käyttöjärjestelmästä on ollut OPC:n suurin kompastuskivi sen julkistamisesta lähtien. OPC Classic -määrittelyihin kuuluvat OPC Data Access (OPC DA), OPC Alarms & Events (OPC AE) ja OPC Historical Data Access (OPC HDA). OPC Classic -nimitystä alettiin käyttämään erottamaan vanhat COM/DCOM-pohjaiset OPC-määrittelyt uudesta OPC UA -määrittelystä. [10.]

3.1.1 OPC Data Access

OPC DA, aikaisemmin OPC 1.0, määrittelee reaaliaikaisen datan siirron datan kerääjien, eli tyypillisesti ohjelmoitavien logiikkaohjainten (PLC) tai hajautettujen ohjausjärjestelmien (DCS) ja datan käyttäjien, esimerkiksi käyttöliittymien (HMI) tai SCADA-valvomojärjestelmien välillä. OPC DA keskittyy nimenomaan reaaliaikaiseen kommunikaatioon, eikä mahdollista pääsyä vanhaan prosessidataan. [7.]



Kuva 7. OPC-protokollan toimintaa. [7. s. 152]

3.1.2 OPC Alarms & Events

Vuonna 1999 julkaistu OPC Alarms & Events -määrittely mahdollistaa hälytys- ja tapahtumatietojen välittämisen järjestelmien välillä. [11.] OPC Alarms & Events ei luo hälytyksiä tai tapahtumia, vaan tallentaa ne ja välittää ne niitä tilaaville asiakkaille. Hälytykset ja tapahtumailmoitukset on määritelty prosessissa, esimerkiksi ohjelmoitavan logiikkaohjaimen sovelluksessa. Hälytys- ja tapahtumatietorekisteri on avoin kaikille asiakkaille, jotka ovat niistä kiinnostuneita.

3.1.3 OPC Historical Data Access

Vuonna 2001 julkaistiin OPC HDA mahdollistamaan historiallisen prosessidatan varastointi, käsittely ja analysointi. Siinä missä OPC DA oli keskittynyt reaaliaikaisen datan välitykseen, keskittyi OPC HDA mahdollistamaan pääsyn arkistoituun prosessidataan. [12.]

3.2 Microsoft Component Object Model

Kun Microsoftin käyttöjärjestelmät yleistyivät teollisuusautomaatiossa 1990-luvun alkupuolella, alkoivat laitetoimittajat hyödyntämään DDE-tekniikkaa järjestelmien välisessä tiedonsiirrossa. DDE eli Dynamic Data Exchange oli hyvin

yksinkertainen palvelin-asiakas-tyyppinen kommunikaatioprotokolla. Tästä protokollasta kehittyi Microsoft COM eli Component Object Model.

COM on 1993 julkaistu Microsoftin kehittämä olioperustainen ohjelmistokomponenttimalli. COM ei ole ohjelmointikieli vaan standardi, joka määrittelee objektimallin ja ohjelmointivaatimukset, joiden mukaan COM-objektit vaikuttavat toisiinsa. COM ei määrittele sovelluksen rakennetta, ohjelmointikieltä ja muita sovelluksen yksityiskohtia vaan jättää ne sovelluksen kehittäjän tehtäväksi. COM-objektit voivat sijaita yhden tai useamman prosessin sisällä. COM-objektit voivat olla rakenteeltaan hyvinkin erilaisia ja ohjelmoitu eri kielillä, jonka takia COM:ia kutsutaankin binääristandardiksi. Binääristandardilla tarkoitetaan määrittelyä, joka määritellään binääritasolla ja täten ei jätä varaa tulkinnalle. Binääriobjektien perusstandardin lisäksi COM määrittelee perusrajapinnat, jotka tarjoavat COM-pohjaisille tekniikoille yhteisiä toimintoja. [13.]

DCOM eli Distributed Component Object Model, aikaisemmin “Network OLE”, on Microsoftin myöhemmin kehittämä laajennus COM:ille. DCOM mahdollistaa ohjelmistokomponenttien hajautuksen useammalle samassa verkossa sijaitsevalle tietokoneelle käyttämällä etäproseduurikutsuja (remote procedure call). [14.]

DCOM Lockdown

8. kesäkuuta vuonna 2021 Microsoft julkisti tietoja merkittävästä haavoittuvuudesta. Tämä haavoittuvuus, tunnettu nimellä ”Microsoft DCOM Server Security Feature Bypass” (CVE-2021-26414), on laajasti hyväksikäytetty heikkous kyberhyökkäyksissä. Haavoittuvuutta hyväksikäyttämällä hyökkääjä pääsee ohittamaan DCOM-palvelimen todennuksen. Vaikka järjestelmätietojen ja -tiedostojen muuttaminen on mahdollista, niin hyökkääjä ei pysty vaikuttamaan järjestelmän muokkausoikeuksiin. [14.] Microsoftin mukaan haavoittuvuus vaikuttaa vain osittain eheyteen eikä vaikuta järjestelmän luotettavuuteen. Microsoft arvioi haavoittuvuuden haitallisuuden olevan 4.3/10 Common Vulnerability Scoring

System (CVSS) -asteikolla, jossa arvosana 0 merkitsee ”ei varaa” ja 10 merkitsee ”kriittistä” (kuva 8.). [15.]

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Kuva 8. Common Vulnerability Scoring System (CVSS) pisteytysasteikko. [16.]

Haavoittuvuuden julkistamisen yhteydessä Microsoft julkaisi tietoturvapäivityksen DCOM-protokollalle. Päivityksen tarkoituksena oli korjata haavoittuvuus. Tätä päivitystä kutsutaan nimellä ”DCOM Hardening” tai ”DCOM Lockdown”.

Päivitys nosti palvelimen ja asiakkaan välisen kommunikaation turvallisuuden tasoa estämällä yhteyksien muodostamisen DCOM-asiakkailta DCOM-palvelimille, jos asiakkaan tunnistautumistaso on alle tason ”Packet Integrity”. Päivitys paransi tietoturvallisuutta erityisesti DCOM-asiakkaan puolella. [17.]

Taulukko 1. Etäproseduurikutsujen tunnistautumistasot. [18.]

Tunnistautumisen taso	**Kuvaus**
None (RPC_C_AUTHN_LEVEL_CALL)	Tällä tasolla ei suoriteta tunnistautumista.
Call (RPC_C_AUTHN_LEVEL_CALL)	Tunnistautuminen suoritetaan jokaisen etäproseduurikutsun alussa palvelimen saatua kyselyn.
Packet (RPC_C_AUTHN_LEVEL_PKT)	Vaatii tunnistautumisen ja varmistaa, että kaikki asiakkaalta odotettu data on vastaanotettu.
Packet Integrity (RPC_C_AUTHN_LEVEL_PKT_INTEGRITY)	Vaatii tunnistautumisen ja varmistaa ettei asiakkaan ja palvelimen välillä kulkevaa dataa ole muokattu.
Packet Privacy (RPC_C_AUTHN_LEVEL_CALL)	Sisältää muiden tasojen ominaisuudet, sekä salaa siirretyn datan sisällön.

Päivitys aiheutti ongelmia erityisesti teollisuudessa, sillä se vaikutti vahvasti suoraan teollisuusautomaatiossa käytettyihin OPC Classic -rajapintoihin. Päivityksen aiheuttamat uudet tunnistautumisvaatimukset estivät joidenkin rajapintojen toiminnan kokonaan. Joissain tapauksissa tietoturvamuutokset vaativat kajoamista rajapintojen alkuperäisiin lähdekoodeihin, mutta koska monet OPC-rajapinnat ovat lähes yhtä vanhoja kuin OPC-standardi itse, oli tämä käytännössä mahdotonta. Tämänkaltaisten ongelmien vuoksi Microsoft päätti toteuttaa päivityksen kolmessa vaiheessa.

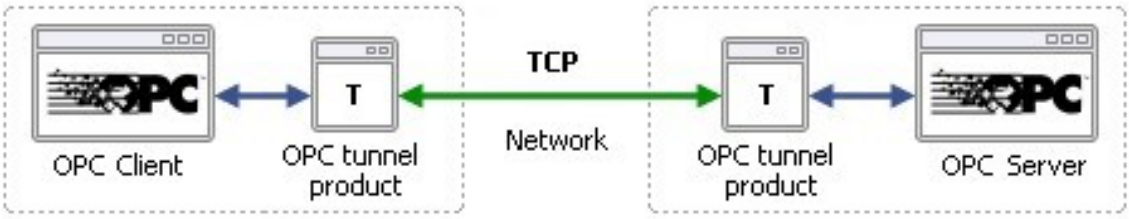
1. Ensimmäinen vaihe astui voimaan heti 8. kesäkuuta 2021, jolloin tietoturvapäivityksen muutokset olivat oletusarvoisesti poissa käytöstä, mutta sovelluksen käyttäjät saivat ottaa muutokset käyttöön, jos niin halusivat.

2. Toinen vaihe, joka astui voimaan vuotta myöhemmin 14. kesäkuuta 2022, asetti muutokset oletusarvoisesti käyttöön, mutta mahdollisuudella kytkeä ne pois.

3. 8. marraskuuta 2022 astui voimaan päivityspaketin kolmas vaihe. Tämä päivitys nosti kaikkien DCOM asiakkaalta DCOM palvelimelle saapuvien ei-anonyymien viestien vaaditun tunnistautumistason tasolle ”Packet Integrity”. (taulukko 1.)

14. maaliskuuta 2023 Microsoft pakotti tietoturvamuutokset päälle oletusarvoisesti, mutta tällä kertaa ilman mahdollisuutta kytkeä niitä pois. [15.]

Päivitys jätti teollisuuslaitoksille, joiden OPC Classic -rajapintoihin päivitys vaikutti yhden vaihtoehdon: Classic OPC:n hylkäämisen. Classic OPC:n hylkäämiseen oli kaksi lähestymistapaa: OPC-tunnelointi tai rajapintojen muuttaminen OPC UA -rajapinnoiksi. OPC-tunneloinnilla tarkoitetaan tekniikkaa, jolla OPC Classic -viesti muutetaan asiakkaan ja palvelimen välillä toisen protokollan viestiksi, tietoturvan ja yhteensopivuuden takaamiseksi. Kumpikin edellä mainituista vaihtoehdoista ovat työläitä ja kalliita, mutta ainoat tavat taata rajapintojen turvallinen toimivuus tulevaisuudessa. [19.]

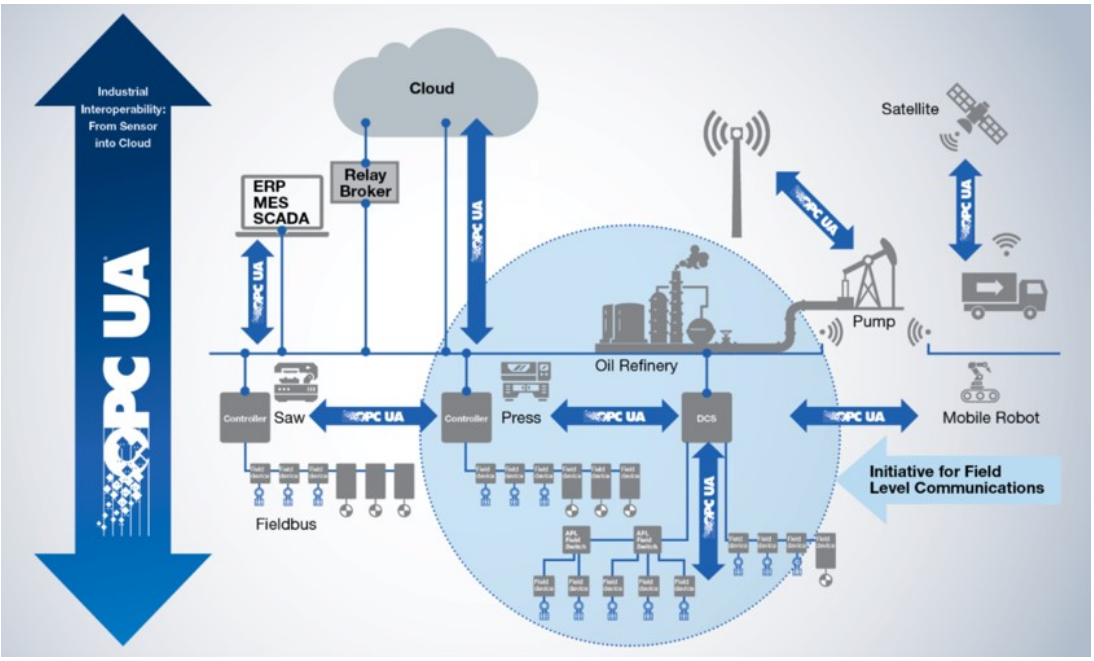


Kuva 9. OPC-tunneloinnin periaatekuva. [19.]

3.3 OPC UA - Unified Architecture

OPC levisi julkaisemisensa jälkeen voimakkaasti teollisuusautomaation maailmassa ja oli vallankumouksellinen tekniikka. Tästä huolimatta nopeasti OPC:n leviämisen jälkeen kävi ilmi, että OPC-standardissa on merkittäviä puutteita. Näitä puutteita ja ongelmia korjaamaan luotiin OPC UA, eli Unified Architecture. OPC UA:n ensimmäinen versio julkaistiin vuonna 2006 ja on täysin käyttöjärjestelmästä riippumaton, toisin kuin OPC Classic, joka on riippuvainen Microsoft Windows -käyttöjärjestelmästä. OPC UA saavutti tämän luopumalla ongelmallisesta DCOM teknologiasta. Sen lisäksi, että DCOM sitoi OPC:n Windows -käyttöjärjestelmään, oli DCOM:in turva-asetusten määrittely hankalaa ja aikaa vievää. DCOM turva-asetusten määrittely oli kompastuskivi muuten helposti määriteltävässä OPC-teknologiassa.

OPC UA on nimensä mukaisesti yhdistetty arkkitehtuuri. Se integroi ennestään erilliset OPC Data Accessin, OPC Alarms & Eventsin ja OPC Historical Data Accessin saman arkkitehtuurin alle. OPC UA toi myös tuen monimutkaisemmille tietorakenteille, paransi tiedonsiirron tietoturvaa ja mahdollisti metodikutsut, muiden alan uusien vaatimusten lisäksi. [20.]



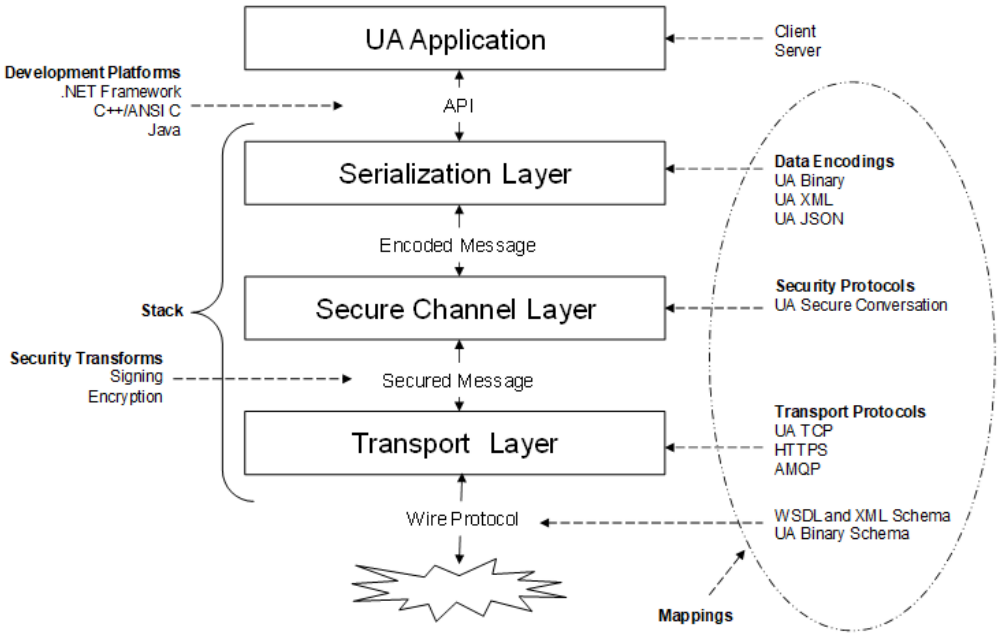
Kuva 10. OPC UA:n mahdollisia käyttökohteita havainnollistava kuva. [21.]

3.4 OPC UA:n Tietoturva

Teollisuuden digitalisoituessa kiihtyvällä vauhdilla tietoturvan merkitys korostuu entisestään. Tämä otettiin huomioon OPC Foundationin määritellessä uutta OPC UA -standardia 2000-luvulla. Vaikka OPC Classic ja OPC UA jakavat joitain toiminnallisuuksia, on niillä selviä eroavaisuuksia tietoturvan näkökannalta.

OPC Classic -standardit eivät itsessään sisällä tietoturvaa osana rajapinta määrittelyitä. Sen sijaan Microsoftin COM/DCOM-kommunikaatioprotokolla, jonka päälle OPC Classic -standardit pohjautuvat, sisältää joitain tietoturva ominaisuuksia. OPC Foundationilla on tiettyjä suosituksia COM/DCOM:in tietoturva-asetusten määrittelylle, mutta näitä suosituksia ei ole aina seurattu. Tämä johtuu siitä, että COM/DCOM:in turvallisuusasetusten määrittely on joissain tapauksissa suhteellisen raskas ja paljon ammattitaitoa vaativa työ. OPC Classic on tietoturvan suhteen lähes täysin riippuvainen COM/DCOM-protokollasta sekä Microsoft Windows -käyttöjärjestelmästä. Vaikka on olemassa kolmannen osapuolen COM/DCOM-versioita muille käyttöjärjestelmille, on hyvin harvinaista nähdä, että OPC Classicia käytetään muilla kuin Microsoft Windows -käyttöjärjestelmillä. [22.]

OPC UA -standardi sen sijaan pitää sisällään tietoturvatoiminnallisuuksia. Palvelin ja asiakas voivat sijaita saman koneen sisällä, tai eri puolilla maapalloa, jonka vuoksi OPC UA -standardia määritellessä tietoliikenteen suojaaminen oli korkealla prioriteettilistalla. OPC UA, toisin kuin OPC Classic, mahdollistaa eri kommunikaatioprotokollien ja käyttöjärjestelmien käytön. Tämän vuoksi OPC UA määrittelee tietoturvallisuustason tiedonsiirtotason yläpuolelle. Tämä pitää huolen siitä, että vaikka uusia tiedonsiirtotapoja lisätään pinon alimmalle tasolle, pysyy tietoturva ennallaan. [22.] Kuvassa 11 on havainnollistettu OPC UA -pino, sen tasot ja tiedonsiirto tasojen välillä.



Kuva 11. OPC UA -pinon (stack) yleiskuva, jossa näkyy turvallisuustaso. [23.]

Turvallisuustason yläpuolella sijaitsee serialisointitaso, joka koodaa lähtevät viestit ja välittää ne turvallisuustasolle tai vastaanottaa turvallisuustasolta saapuvat viestit ja dekoodaa ne. Turvallisuustaso suojaa lähtevät viestit, joko allekirjoituksella (Sign) tai salauksella ja allekirjoituksella (Sign and Encrypt) riippuen käyttäjämäärittelyistä. Haluttaessa suojauksen voi kytkeä myös pois päältä. Suojausta ei välttämättä tarvita joissain tapauksissa, esimerkiksi suljetuissa verkoissa. Turvallisuustaso välittää lähtevän, tyypillisesti salatun viestin tiedonsiirtotasolle, joka käsittelee viestit ja lisää niihin otsikot, jotka kertovat mm. viestin pituuden ja tyypin. [12.]

OPC UA:n sovellustaso ja tietoliikennetaso pitävät myös sisällään omat turvallisuustoiminnallisuutensa. Tämän lisäksi on panostettu osapuolien väliseen tunnistautumiseen, jossa käytetään hyväksi erilaisia salauksia ja tunnuksia.

OPC UA on alusta lähtien määritelty tietoturvallisuusmielessä täyttämään teollisuuden sille asettamat vaatimukset. Tämän takia tietoturvatoiminnallisuudet on integroitu standardiin. Tämä tekee OPC UA:sta huomattavasti turvallisemman

vaihtoehdon kuin edeltäjästään, joka on riippuvainen muista teknologioista tietoturvallisuutensa ja toiminnallisuutensa suhteen.

4 Automaatio- ja tietoliikenneverkkojen dokumentointi

Tervakosken tehtaalla suoritettiin keväällä 2023 merkittäviä automaatioverkon parannustöitä. Työt liittyivät pääasiassa koko ajan laajenevaan automaatiojärjestelmien tiedonsiirron tarpeeseen ja tämän tiedon turvaamiseen. Merkittävä työ oli myös OPC-rajapintojen uusintaprojekti liittyen DCOM-tietoturvakovennuksiin. Näitä töitä, sekä tulevaisuuden kunnossapitoa, laajennuksia ja projekteja tukemaan luotiin tehtaalla uusi tietoliikenteen runkoverkkojen dokumentaatiojärjestelmä.

4.1 Dokumentaatio

Lähtötilanteessa tehtaan tietoliikenneverkoista oli kertynyt vain vähän dokumentaatiota. Ennen projektia kuituverkkojen dokumentaatio koostui kartasta, josta kävi ilmi valokuitukaapelointi jakamoiden välillä. Tämän lisäksi osasta jakamoista oli laadittu kytkentälistat. Nämä kytkentälistat olivat formaatiltaan huonot käyttötarkoitukseen ja niiden sisältämä tieto vajavaista. Kytkentälistoja oli vain yksi kappale koottuna yhteen kansioon, ja kansiolla ei ollut vakituista sijaintia tehtaalla. Tehtaan suunnitteluosasto, sähkö- ja automaatiokunnossapito, sekä IT-osasto olivat samaa mieltä siitä, että tietoliikenneverkkojen dokumentaatio olisi tehtaan kannalta tärkeä uudistaa. Dokumentaation kehitystyö rajattiin tietoliikenteen runkoverkkoon työn laajuuden hillitsemiseksi. Runkoverkko sisältää yritys- ja automaatioverkon yhteyksiä. Runkoverkko koostuu pääasiassa jakamoista ja palvelinhuoneista. Runkoverkon jakamoiden ja muiden osien väliset yhteydet on toteutettu pääasiassa valokuitukaapeloinnilla.

4.2 Dokumentaation kehittäminen

Tietoliikenneverkkoja lähdettiin kehittämään suunnittelu-, kunnossapito- ja IT-osaston yhteistyönä. Tärkeää oli, että uusi dokumentaatio palvelisi kaikkia sen

käyttäjiä mahdollisimman hyvin. Dokumentaation tulisi olla helppokäyttöinen ja dokumentaatioon tulisi olla helppo ja nopea pääsy. Uuden dokumentaation olisi oleellista tukea tietoliikenneverkkojen laajentumista tulevaisuudessa. Dokumentaatio oli siis parasta tehdä sähköisenä täyttämään nykyajan vaatimukset muun teknisen dokumentaation tapaan. Kunnossapidon ja poikkeustilanteiden vuoksi oli kuitenkin oleellista myös ylläpitää fyysistä dokumentaatiota.

4.2.1 Dokumentaation sähköistäminen

Uutta dokumentaatiota lähdettiin tekemään siirtämällä ensin vanhat kytkentälistat sekä jakamo- ja laitetiedot käsin sähköiseksi. Ennen tätä käytiin läpi vanhaa, jo olemassa olevaa dokumentaatiota tietoliikenneverkoista. Tämän jälkeen dokumentaation sisältöä varmistettiin ja selvitettiin suorittamalla tarkastuskierroksia ja -käyntejä jakamoilla sekä muilla verkon osilla. Tieto koottiin taulukkoon niin, että jokainen taulukon rivi kuvasti yhtä kuitukaapelointilinkkiä tehtaalla. Riville listattiin kaikki mahdollinen tieto kuidusta, kuten kuitu- ja kaapelityypit, jakamot, paneelit, liitinnumerot sekä laitteet, joiden välillä yhteys on. Jokaiselle kuitukaapelille ja kuidulle luotiin omat tunnisteet. Joissain tapauksissa kuiduille lisättiin erinäisiä oleellisia lisätietoja esim. reitityksestä, kuidun päättämisestä ja kuidun, kaapelin tai laitteen kunnosta.

4.2.2 Tietokanta

Projektin suunnitteluvaiheessa lähdettiin miettimään uuden dokumentaation muotoa ja käyttöä. Työryhmä päätyi siihen lopputulokseen, että tietokantapohjainen ratkaisu toisi paljon hyötyjä projektin eri osapuolille. Tietokannan hyödyntäminen dokumentoinnin työkaluna mahdollistaisi monipuolisia toiminnallisuuksia kaikille projektin osapuolille.

Kun aikaisempi dokumentaatio oli siirretty sähköiseksi, lähdettiin yhteistyössä IT-osaston kanssa luomaan tietokantaa sähköisen dokumentaation pohjalta. Tietokantaa varten luotiin Excel-pohjainen ”masterdatan” käyttöliittymä. Käyttöliittymän avulla saadaan hallinnoitua tietokannan sisältöä lisäämällä,

poistamalla ja muokkaamalla runkoverkon tietoja. Tietokanta poimii käyttöliittymään tehdyt päivitykset ja päivittää ne kantaan. Käyttöliittymän pohjaksi valikoitui Excel, koska se oli kaikille osapuolille ennestään tuttu ja helppokäyttöinen sovellus.

Tietokannan kautta saadaan välitettyä automaattisia ilmoituksia ja tietoja tietoliikenneverkon vikatiloista ja kapasiteetista halutuille tahoille. Tietokanta mahdollistaa vikarekisterin ylläpidon, jolla saadaan seurattua tietoliikenneverkon vikaantumisia hyvin tarkasti tulevaisuudessa. Tietokannan kautta saadaan myös tietoa verkon laajentamistarpeista ja tämänhetkisestä koosta sekä sen kautta saadaan hyvä yleiskuva verkon tilasta. Tietokanta mahdollistaa myös automaattisesti päivittyvän tulostettavan dokumentaation, jota ei olisi työläs ylläpitää. Jatkossa eri tahot voivat laatia omiin käyttötarkoituksiinsa sopivia dokumentaatiopohjia, joihin saadaan koko ajan päivittyvää tietoa verkon tilasta, laitteista ja yhteyksistä.

Tietokantaratkaisu tukee suunnittelu- ja IT-osastojen verkkosuunnittelua sekä mahdollistaa monipuolisten verkon kunnossapito-, suunnittelu- ja analyysityökalujen kehittämisen tulevaisuudessa.

4.2.3 Fyysinen dokumentaatio

Fyysistä dokumentaatiota varten luotiin yhdessä kunnossapidon asentajien kanssa uudet pohjat runkoverkon kaapeloinnin ja kytkentöjen dokumentaatiolle. Dokumentaatiota suunnitellessa oli tärkeää ottaa huomioon sen käyttäjien mielipiteet. Tällä saavutettaisiin paras lopputulos ja helppokäyttöisin dokumentaatio. Kaapeloinnin ja kytkennän dokumentaatiosta tulisi käydä ilmi

- jakamon tunnus
- jakamon sijainti tehtaalla
- jakamon sähkönsyöttö

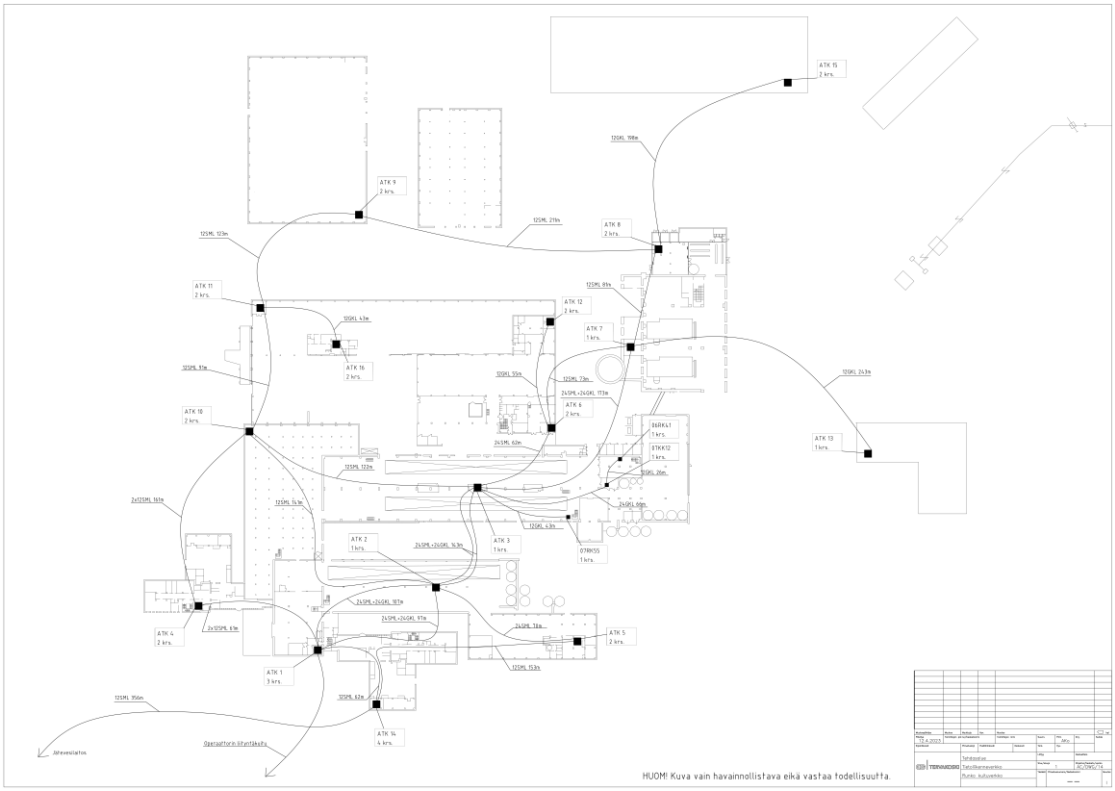
- kuitupaneelin tunnus
- kytkennät
- kytkentään liittyvät laitteet ja järjestelmät
- laitteiden tunnukset, sekä mahdolliset huomiot ja vikatilat
- kaapeloinnin tyyppi
- kuitukaapeloinnin reitti, jos mahdollista
- mahdolliset kaapelin vikatilat.

Dokumenttien tuli olla niin selkeitä, että tehtaan verkkoihin perehtymätönkin alan ammattilainen niitä tarvittaessa ymmärtäisi. Tämän takia dokumentaatiosta tuli käydä ilmi jakamoiden tunnusten lisäksi jakamon sijainti tehtaalla. Jakamon sähkönsyöttö lisättiin dokumentaatioon sähkönjakelun poikkeamien varalta.

4.2.4 Yhteyskartta

Jo ennen projektia oli olemassa karttapohjainen kuva jakamoiden välisistä kuituyhteyksistä tehtaalla. Tämä kuva on tehokas ja helppo tapa kuvata tehtaan kuituverkkoa ja on todettu toimivaksi. Täten tätä dokumentaatiota ei lähdetty uusimaan tämän työn yhteydessä. Yhteyskarttaan päivitettiin käynnissä olevien

automaatioverkon laajennusprojektien uusia yhteyksiä, päivitettiin reitityksiä, sekä pohjakuvaan lisättiin uusia rakennuksia ja laajennuksia.



Kuva 12. Havainnollistava esimerkkikuva yhteyskartasta. Kuva ei turvallisuussyistä vastaa todellisuutta.

5 Yhteenveto

Insinöörityön tavoitteena oli tutustua automaatioverkkojen ja OPC-teknologian teoriaan sekä kehittää Tervakosken tehtaan tietoliikenneverkkojen dokumentaatiota. Tiedonhankinta teoriaosuutta varten sujui pääasiassa ongelmitta hyvien lähteiden ansiosta. Työn yhteydessä pääsin hankkimaan tärkeää tietoa ja kokemusta teollisuuden tietoliikenneverkoista, joka oli itselle entuudestaan vieras osa-alue.

Työn yhteydessä pääsin myös kehittämään tehtaalle uutta dokumentaatiojärjestelmää. Uuden järjestelmän rakentaminen lähes tyhjästä oli mieluisa kokemus, jonka aikana pääsin hankkimaan kokemusta tehtaan eri osastoista ja toiminnoista. Kyseessä oli monialainen projekti, jossa pääsin tutustumaan tehtaan

sähkö-, automaatio- ja tietotekniikan toimintoihin. Tämä oli arvokasta kokemusta, sillä nämä eri osa-alueet tulevat tulevaisuudessa riippumaan toisistaan entistä enemmissä määrin.

Työn tuloksena syntynyt järjestelmä on kerännyt alusta alkaen paljon mielenkiintoa eri osapuolilta, mikä havainnollistaa sen tärkeyttä. Järjestelmä tulee olemaan keskeisessä osassa tukemassa tehtaan automaatiojärjestelmien suunnittelua ja kunnossapitoa aikana, jolloin prosessienohjaus digitalisoituu kiihtyvällä vauhdilla. Järjestelmän kehitystyötä jatketaan edelleen.

Lähteet

1. Tala, Henrik. 2018. Tervakosken paperitehdas: Tervakosken Paperitehtaan Historiaa 1818–2018. Tervakoski Oy.

2. Suomen Automaatioseura. 2021. Automaation Tietoturva – Kriittisen tuotannon turvaaminen. 1. painos.

3. Kaurto, Aleksi. 2018. Ethernet-pohjaisten automaatioverkkojen reaaliaikainen kunnonvalvonta. Diplomityö. Tampereen Teknillinen Yliopisto. Trepo-tietokanta.

4. Basic Elements of a Fiber Optic Communication System. Verkkoaineisto. ElProCus Technologies. < https://www.elprocus.com/basic-elements-of-fiber-optic-communication-system-and-its-working/>. Luettu 25.4.2023.

5. Fiber optic cable buying guide. Verkkoaineisto. Eaton Corporation. <https://tripplite.eaton.com/products/fiber-optic-cable-buying-guide>. Luettu 25.4.2023.

6. Introduction to Modbus TCP/IP. 2005. Verkkoaineisto. Acromag Inc. <https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf>. Luettu 27.4.2023.

7. D. Knapp, Eric & Langill, Joel Thomas. 2015. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems. Second Edition. Elsevier Inc.

8. What is OPC. Verkkoaineisto. The OPC Foundation. <https://opcfoundation.org/about/what-is-opc/>. Luettu 26.4.2023.

9. Keiski, Arto. 2016. OPC UA ja teollinen asioiden internet. Opinnäytetyö. Metropolia Ammattikorkeakoulu. Theseus-tietokanta.

10. Classic. Verkkoaineisto. The OPC Foundation. <https://opcfoundation.org/about/opc-technologies/opc-classic/>. Luettu 26.4.2023.

11. History. Verkkoaineisto. The OPC Foundation. <https://opcfoundation.org/about/opc-foundation/history/>. Luettu 26.4.2023.

12. Heikkilä, Mikko. 2016. OPC UA Automaation Tiedonsiirrossa. Opinnäytetyö. Tampereen Ammattikorkeakoulu. Theseus-tietokanta.

13. The Component Object Model. 2019. Verkkoaineisto. Microsoft Corporation. <https://learn.microsoft.com/en-us/windows/win32/com/the-component-object-model>. Luettu 27.4.2023.

14. KB5004442—Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414). 2023. Verkkoaineisto. Microsoft Corporation. <https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c>. Luettu 27.4.2023.

15. Microsoft DCOM Hardening Patch (CVE-2021-26414) – What You Need to Know. 2022. Verkkoaineisto. txOne Networks. <https://www.txone.com/blog/microsoft-dcom-hardening-patch-cve-2021-26414-what-you-need-to-know/>. Luettu 27.4.2023.

16. What is CVE and CVSS. 2020. Verkkoaineisto. BenQ <https://www.benq.com/en-us/business/resource/trends/what-is-cve-and-cvss.html>. Luettu 27.4.2023.

17. Windows DCOM Hardening And OPC Classic Applications. 2023. Verkkoaineisto. Prosys OPC. <https://www.prosysopc.com/blog/dcom-hardening-and-opc-classic-applications/>. Luettu 27.4.2023.

18. Authentication-Level Constants. 2020. Verkkoaineisto. Microsoft Corporation. <https://learn.microsoft.com/en-us/windows/win32/rpc/authentication-level-constants>. Luettu 27.4.2023.

19. OPC Tunneling - Know Your Options. 2003. Verkkoaineisto. Automation.com. <https://www.automation.com/en-us/articles/2003-1/opc-tunneling-know-your-options>. Luettu 27.4.2023.

20. Lange, Junge; Iwanitz, Frank & Burke, Thomas. 2010. OPC: From Data Access to Unified Architecture. 4. Painos. VDE Verlag GmbH.

21. OPC UA. Verkkoaineisto. MathWorks. <https://se.mathworks.com/discovery/opc-ua.html>. Luettu 28.4.2023.

22. OPC UA vs OPC Classic Security Discussion. Verkkoaineisto. Paul Hunkar. <http://www.dsinteroperability.com/OPCClassicVSUA.pdf>

23. OPC 10000-6: UA Part 6: Mappings – 4 Overview. Verkkoaineisto. The OPC Foundation. <https://reference.opcfoundation.org/Core/Part6/v105/docs/4>. Luettu 3.5.2023.