Tampereen ammattikorkeakoulu

OT-verkkojen vaatimukset automaatiosuunnittelussa

Joakim Sundberg

OPINNÄYTETYÖ
Helmikuu 2025

Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Automaatiotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Automaatiotekniikka

SUNDBERG, JOAKIM:
OT-verkkojen vaatimukset automaatiosuunnittelussa

Opinnäytetyö 38 sivua, joista liitteitä 0 sivua
Helmikuu 2025

Opinnäytetyönä laadittiin tutkimustyö OT-verkoista ja niiden standardien mukaisista rakenteellisista vaatimuksista. Työn avulla kehitetään automaatiosuunnittelijoille perustason ymmärrys OT-verkon laitteistosta, yleisimmistä malleista ja rakenteellisista vaatimuksista. Tämän lisäksi tuotettiin aineistoa, jonka avulla voidaan edistää automaatiosuunnittelijoiden yhdenmukaista toimintaa yrityksessä. Työssä hyödynnettiin NIS2-direktiiviä, IEC 62443-standardia ja Purdue-mallia. Opinnäytetyön teetti Insta Automation Oy, joka toimii teollisuudessa kokonaisvaltaisena automaation järjestelmätoimittajana.

Opinnäytetyössä on käsitelty yleisimmät ja tärkeimmät OT-verkon laitteet ja niiden toimintaperiaatteet. Lisäksi jokainen laite on liitetty laajempaan OT-verkon kokonaisuuteen niiden roolien ja merkitysten selventämiseksi. Laitteiden lisäksi opinnäytetyössä tarkastellaan OT-verkon prioriteetteja, yleisimpiä tietoverkkomalleja sekä etäyhteyksien perusteita. Lopuksi yhdistetään käsitellyt laitteet ja käsitteet yhdeksi kokonaisuudeksi, joka täyttää fyysisen rakenteen osalta IEC 62443-standardin SL 2 -tason. Tämän lisäksi nostetaan esille standardin kohdat, jotka tulevat lainsäädäntöön tulevaisuudessa osana NIS2-direktiiviä.

Julkisessa raportissa ei ole esitetty opinnäytetyön perusteella tehtyä yksiselitteistä ohjeistusta OT-verkkojen suunnitteluun. Luottamuksellinen materiaali on työn tilaajan pyynnöstä julistettu salaiseksi sekä poistettu julkisesta raportista.

Lopputuloksena opinnäytetyössä on esimerkkitapaus OT-verkon suunnittelusta huomioiden SL 2 -tason fyysisen rakenteen vaatimukset. Opinnäytetyötä voisi jatkokehittää ottamalla käsittelyyn IEC 62443-standardin ohjelmistopohjaiset vaatimukset tai SL 3 -tason vaatimukset.

Asiasanat: automaatio, standardi, kyberturvallisuus, IEC 62443, OT-verkko

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Electrical Engineering
Automation Engineering

SUNDBERG, JOAKIM:
Requirements for OT Networks in Automation Design

Bachelor's thesis 38 pages, appendices 0 pages
February 2025

The aim of this thesis was to create a research study on OT networks and the structural requirements defined by their standards. The goal was to provide automation designers with a fundamental understanding of the most common devices, models, and structural requirements used in OT networks. In addition, materials were produced to aid in consistent practices among the company's automation designers. The NIS2 directive, IEC 62443 standard and the Purdue model were utilized in the thesis. The thesis was commissioned by Insta Automation Oy which operates in the industrial field as a comprehensive automation system supplier.

The thesis covered the most common and important devices in OT networks and their operating principles. In addition, an effort was made to highlight each device's role and meaning in an OT network. Apart from the devices, the thesis also addressed the priorities of OT networks, the most common data network models, and the basics of remote connections. Finally, the aforementioned devices and concepts were combined into a single system that meets the SL 2 requirements of the IEC 62443 standard in terms of physical structure. In addition, the points of the standard that will be incorporated into legislation under the NIS2 directive were highlighted.

The public report does not contain the unambiguous instructions for the design of OT networks that were created based on the thesis. The confidential material has been hidden at the request of the commissioner and thus removed from the public report.

The end result of the thesis is an example case of the design of an OT network, taking into account the physical structure requirements set by the standard. The thesis could be further developed by addressing the software-based requirements, or the SL 3 requirements set by the standard.

Key words: automation, standard, cybersecurity, IEC 62443, OT network

SISÄLLYS

LYHENTEET JA TERMIT

ANSI	American National Standards Institute. Yhdysvaltalainen standardointiorganisaatio.
DCS	Distributed Control System. (suom. hajautettu automaatiojärjestelmä). Suurien automaatioprosessien ohjaukseen.
DHCP	Dynamic Host Configuration Protocol. Protokolla dynaamisten IP-osoitteiden jakamiseen.
DMZ	Demilitarized Zone (suom. demilitarisoitu vyöhyke). Erillinen verkko, joka erottaa julkisen ja yksityisen verkon.
ERP	Enterprise Resource Planning. (suom. toiminnanohjausjärjestelmä). Yrityksen liiketoimintaprosessien hallintaan käytettävä järjestelmä.
HMI	Human-Machine Interface. (suom. ihmisen ja laitteen välinen käyttöliittymä). Teollisuuden koneiden ja prosessien ohjaukseen käytettävä käyttöliittymä.
IEEE	Institute of Electrical and Electronics Engineers. Sähkö- ja elektroniikkatekniikan alan kansainvälinen standardointiorganisaatio.
IoT	Internet of Things. (suom. esineiden Internet). Viittaa järjestelmiin, jossa laitteet kommunikoivat Internetin välityksellä.
ISA	International Society of Automation. Kansainvälinen automaatiojärjestelmien standardointiorganisaatio.

ISO	International Organization for Standardization. Kansainvälinen standardointiorganisaatio.
ISP	Internet Service Provider. (suom. Internet-palveluntarjoaja). Internet-yhteyden tarjoava yritys.
IT	Information Technology. (suom. tietotekniikka). Tiedonsiirtoon ja käsittelyyn liittyvä teknologia. Käytetään tässä yhteydessä kuvastamaan yrityksen toimistoverkkoa.
MAC	Media Access Control. Laitteen yksilöllinen osoite.
MES	Manufacturing Execution System. (suom. tuotannonohjausjärjestelmä). Prosessien ohjaukseen ja hallinnointiin käytettävä järjestelmä.
NIS	Network and Information Security. (suom. verkon ja tiedon turvallisuus). EU:n kyberturvallisuusdirektiivi.
NIST	National Institute of Standards and Technology. Yhdysvaltalainen standardointiorganisaatio.
OT	Operational Technology. (suom. operatiivinen teknologia). Verkkojärjestelmä teollisuuden ja infrastruktuurin ohjaukseen ja valvontaan.
PAW	Privileged Access Workstation. (suom. erityisoikeutettu työasema). Työasema, jolla on pääsy korkean suojauksen järjestelmiin.
PLC	Programmable Logic Controller. (suom. ohjelmoitava logiikka). Käytetään pienien tai keskisuurien prosessien ohjaukseen.

SCADA	Supervisory Control and Data Acquisition. (suom. tiedonkeruu- ja ohjausjärjestelmä). Ohjelmisto, jolla ohjataan ja valvotaan teollisuusprosessia.
SFS	SFS Suomen Standardit ry. Suomalainen standardointiorganisaatio.
SL	Security Level. (suom. suojaustaso). Taso, joka määrittelee automaatiojärjestelmän tietoturvallisuuden tason IEC 62443-standardissa.
SL-A	Security Level – Achieved. (suom. saavutettu suojaustaso). Saavutettu ja todennettu suojaustaso IEC 62443-standardissa.
SL-C	Security Level – Capability. (suom. mahdollinen suojaustaso). Järjestelmän mahdollinen suojaustaso IEC 62443-standardissa.
SL-T	Security Level – Target. (suom. tavoiteltu suojaustaso). Suojaustaso, johon pyritään järjestelmässä IEC 62443-standardin mukaisesti.
VLAN	Virtual Local Area Network. (suom. virtuaalinen paikallisverkko). Virtuaalisesti toteutettu erillinen, paikallinen verkko.
VPN	Virtual Private Network. (suom. virtuaalinen yksityisverkko). Luo yhteyden yksityiseen verkkoon julkisen verkon välityksellä.
WSUS	Windows Server Update Services. (suom. Windowsin päivityspalvelin). Työkalu, jolla voidaan hallinnoida Windows-päivityksiä järjestelmässä.

1 JOHDANTO

Tässä opinnäytetyössä pyritään kehittämään työn tilaajan, Insta Automation Oy:n tehokkaampaa ja yhdenmukaisempaa toimintaa OT-verkkojen suunnittelun osalta. Työn tarkoituksena on selventää opinnäytetyön tekijälle sekä lukijalle, mitä OT-verkot ovat, millaisia laitteita ne pitävät sisällään ja mitkä ovat niiden keskeisimmät mallit ja vaatimukset.

Insta Automation Oy kuuluu Insta-konserniin, joka on jo lähes 65-vuotta vanha suomalainen perheyritys. Insta-konserniin kuuluu muun muassa sähkö- ja automaation, ohjelmistokehityksen, puolustusteknologian ja kyberturvallisuuden asiantuntijoita. Insta Automation Oy on automaation, sähköistyksen ja digitalisaation kokonaistoimittaja. Yritys ei ole riippuvainen tietystä järjestelmästä, vaan on riippumaton järjestelmä- ja laitetoimittajista. Insta Automation Oy:n palveluihin kuuluu sähkö- ja automaatiosuunnittelu, keskusvalmistus, sähköasennus, käyttöönotto, kunnossapito sekä kokonaistoimitukset.

Teollisuudessa automaatio on laajentunut ja yhä enemmän tuotteita tehdään erilaisin automatisoiduin ratkaisuin. Tämän automatisoinnin myötä myös OT-verkot ovat yleistyneet ja laajentuneet. Automatisoinnin taustalla on usein halu tuottaa tuotteita mahdollisimman tehokkaasti, joka on osaltaan johtanut siihen, että OT-verkosta halutaan erilaisia tietoja ja raportteja yrityksen omaan IT-verkkoon. Kyseinen kehityssuunta aiheuttaa mielenkiintoisia haasteita OT-verkkojen turvallisuuden kannalta, sillä perinteisesti tiedon luottamuksellisuus ei ole ollut korkealla prioriteettilistassa.

Etenkin kriittisen infrastruktuurin, kuten vesilaitosten ja sähköasemien OT-verkkojen turvallisuus on nykypäivänä keskustelua herättävä aihe. Mikäli vesilaitos joutuisi hyökkäyksen kohteeksi, voisi pahimmassa tapauksessa kyseisen laitoksen jakelualue jäädä täysin ilman vettä tai saada juomakelvotonta vettä. Näiden uhkakuvien myötä OT-verkoissa tullaan todennäköisesti näkemään luottamuksellisuuden roolin kasvua, eli verkon sisäisten yhteyksien ja oikeuksien rajoittamista. Luottamuksellisuuden lisäksi erilaiset tunkeutumisen havaitsemisjärjestelmät tulevat todennäköisesti yleistymään.

Tietoverkkojen, mukaan lukien OT-verkkojen, kyberturvallisuuden tärkeys on myös huomattu EU:n tasolla. EU on julkaissut päivitetyn NIS2-direktiivin vuonna 2022, jonka oli määrä astua voimaan kansallisesti vuonna 2023. Kyseinen direktiivi on jatkoa vuonna 2018 voimaantulleeseen NIS-direktiivin. Uusi NIS2-direktiivi toi mukanaan tiukentuneen säätelyn, jonka lisäksi soveltamisalaa laajennettiin. Tämä vaikuttaa siis myös useamman toimialan OT-verkkojen vaatimuksiin.

Opinnäytetyöstä on tarkoituksena muodostua selkeä dokumentaatio OT-verkkojen eri osista ja oleellisista käsitteistä. Työtä on käytetty Insta Automation Oy:n sisäiseen, erillisen suunnitteluohjeen luomiseen. Suunnitteluohje kehittää yrityksen yhdenmukaisempaa ja tehokkaampaa toimintaa uusimpien vaatimusten mukaisesti.

Työssä ensin selvitetään lukijalle, mikä on OT-verkko ja mitkä ovat sen prioriteetit. Tämän jälkeen lukija johdatetaan tarkemmin direktiivien ja standardien tarkoitukseen, jonka jälkeen käsitellään OT-verkoissa yleisimmin käytetyt verkkorakenteiden mallit. Sen jälkeen työssä käsitellään OT-verkoissa yleisimmin käytetyt verkkolaitteistot, jonka jälkeen käydään läpi erilaisia etäyhteyksiä, jotka vaikuttavat OT-verkkoihin. Lopuksi käydään läpi havainnollistavana esimerkkinä kuvitteelliselle asiakkaalle suunnitellun SL 2 -tason OT-verkon fyysinen rakenne ja huomioitavat asiat.

2 OT-verkko

OT-verkoilla tarkoitetaan järjestelmiä, joiden tarkoituksena on ohjata ja valvoa teollisuudessa käytettäviä laitteistoja ja ohjelmistoja. OT-verkot eroavat IT-verkoista siten, että IT-verkoissa ei ohjata tai valvota suoraan fyysisiä prosesseja. Molemmissa verkoissa kuitenkin käytetään usein samankaltaisia verkkolaitteita tai ohjelmistoja, kuten kytkimiä ja palomuureja. Taulukkoon 1 on koottu IT- ja OT-verkkojen prioriteetit (What Is IT/OT Convergence? n.d.)

TAULUKKO 1. IT- ja OT-verkkojen prioriteetit.

IT-verkon prioriteetit	**OT-verkon prioriteetit**
1. Luottamuksellisuus	1. Saatavuus
2. Tiedon eheys	2. Tiedon eheys
3. Saatavuus	3. Luottamuksellisuus

Tärkein OT-verkon ominaisuus on lähes reaaliaikainen tiedonsiirto, eli saatavuus. Reaaliaikaisella tiedonsiirrolla voidaan varmistaa prosessin tehokkuus ja turvallisuus, kun prosessin ohjausjärjestelmä pystyy reagoimaan muutoksiin lähes reaaliajassa. Vaikka OT-verkot voivat olla langattomia, pitää varmistaa, että langattomuudesta johtuva tiedonsiirron viive ei ole kriittinen prosessin toiminnalle. Usein langattomia verkkoja käytetään vain valvomoissa, joissa tiedonsiirron viive voidaan sietää. PLC:t ja muut mahdolliset verkossa olevat laitteet toteutetaan usein fyysisillä kaapeleilla viiveen minimoimiseksi.

Tiedon eheys on molemmissa verkoissa kohtalaisen tarpeellinen. Eheys tarkoittaa tiedon muuttumattomana pysymistä, eli tieto ei saa muuttua sen haun, siirron, ja tallennuksen aikana. Luottamuksellisuus taas ei ole OT-verkossa korkealla prioriteetilla. OT-verkoissa oletetaan, että verkkoon kytketyt laitteet ovat tarkoituksenmukaisia ja turvallisia, jolloin niiden oikeuksia ei tarvitse niin tiukasti valvoa. Luottamuksellisuus siis kattaa ne oikeudet, joita tarvitaan tietoihin tai järjestelmiin pääsemiseen.

Laitteiden käyttöikä OT-verkoissa on usein jopa kymmeniä vuosia. Pitkän elinkaaren lisäksi tuotantokatkoja voi olla vaikeaa järjestää. (Ahonen, Seppälä & Tyynelä 2021, 129–130.) Nämä seikat voivat johtaa siihen, että laitteiden ohjelmistoja ei päivitetä, joka saattaa johtaa tietoturvahaavoittuvuuksiin.

Perinteisesti OT-verkot ovat olleet eristettyjä internetistä ja yrityksen muista IT-verkoista, joka osaltaan on vahvistanut OT-verkkojen tietoturvaa, vaikka tietoturvahaavoittuvuuksia olisikin. Ainoa tapa hyökätä tällaiseen verkkoon on päästä fyysisesti laitteiden äärelle. Nykyään kuitenkin halutaan liittää OT-verkkoja vähintään yrityksen omaan IT-verkkoon, joka avaa reitin hyökätä verkkoon Internetin välityksellä. Näin ollen nykyaikana tekemättömät päivitykset laitteissa voivat olla suuri tietoturvariski. (Toivonen 2020.)

3 DIREKTIIVIT JA STANDARDIT

3.1 Direktiivit

Direktiivi on EU:n säädös, joka on osoitettu kaikille EU:n jäsenvaltioille. Sen tarkoitus on yhdenmukaistaa eri jäsenvaltioiden lainsäädäntöä sen osoittamalla osa-alueella. Direktiivit on siis otettava osaksi kansallista lainsäädäntöä ja yleensä tämä on tehtävä kahden vuoden sisällä. (EUR-Lex n.d.)

Direktiivit voivat asettaa vähimmäisvaatimukset tai puitteet, jotka pitää ottaa huomioon lainsäädäntöä tehdessä. Tällöin jäsenvaltio voi asettaa korkeammat vaatimukset, kuin direktiivissä. Muussa tapauksessa direktiivin vaatimukset pätevät sellaisenaan, eikä niitä saa korottaa. Mikäli jäsenvaltio ei ota direktiiviä osaksi lainsäädäntöään, EU:n komissio voi aloittaa rikkomismenettelyn ja nostaa kanteen EU:n tuomioistuimessa. (EUR-Lex n.d.)

3.2 Standardit

Sanastokeskuksen (n.d.) mukaan standardi on ”toistuvien ongelmien ratkaisuja esittävä asiakirja, joka perustuu asianosaisten yhteisymmärrykseen ja on tähän tehtävään tunnustetun elimen hyväksymä” (TSK 9, 1986). Standardin tarkoitus on siis esittää vaatimustenmukainen ratkaisu tiettyyn ongelmaan. Standardit julkaistaan kirjallisesti ja niissä voidaan määritellä esimerkiksi tuotteiden ominaisuuksia sekä vaatimuksia, tai järjestelmien toimintaa. Hyvä esimerkki standardista on paperikoot. A4-koon paperi on aina samankokoinen valmistajasta riippumatta.

Standardit voivat olla kansallisia, eurooppalaisia tai kansainvälisiä. Standardi alkaa esipuheella ja johdannolla, joiden tarkoitus on johdattaa lukija standardin sisältöön sekä taustoihin. Tämän jälkeen kerrotaan mihin standardia voidaan soveltaa ja mitä muita standardeja tulisi myös noudattaa kyseisen standardin lisäksi. Seuraavaksi termit-osiossa käsitellään standardissa käytettäviä termejä ja niiden määritelmiä. Perusasioiden jälkeen päästään tarkkoihin vaatimuksiin, eli

standardin ytimeen. Standardin lopussa on opastavaa sisältö, eli esimerkiksi erilaisia taulukoita. (Mitä standardi tarkoittaa? n.d.)

Jokaisella standardilla on tunnus. Tunnuksen eri osista voidaan tulkita kyseisen standardin voimassaoloalue, sen yksilöivä numero ja vahvistamisvuosi. Kuviossa 1 on esitelty erään standardin tunnus.

KUVIO 1. Standardin tunnuksen osat (Mitä standardi tarkoittaa? n.d.).

Tunnuksen alusta voidaan nähdä, että kyseinen standardi on vahvistettu, eli voimassa Suomessa. Tämän lisäksi standardi on vahvistettu EU:n alueella ja myös kansainvälisesti. Tunnuksessa ei ole aina kansallista, eurooppalaista ja kansainvälistä tunnusta, vaan voi olla myös esimerkiksi pelkkä SFS. Seuraavaksi on standardin numero, jolla kyseinen standardi voidaan yksilöidä. Viimeisenä on sen vahvistamisvuosi, eli milloin kyseinen standardi on vahvistettu. Myös standardin nimi on jaettu osiin kuvion 1 mukaisesti. Nämä ovat johdanto-osa, pääosa ja sivuosa. (Mitä standardi tarkoittaa? n.d.)

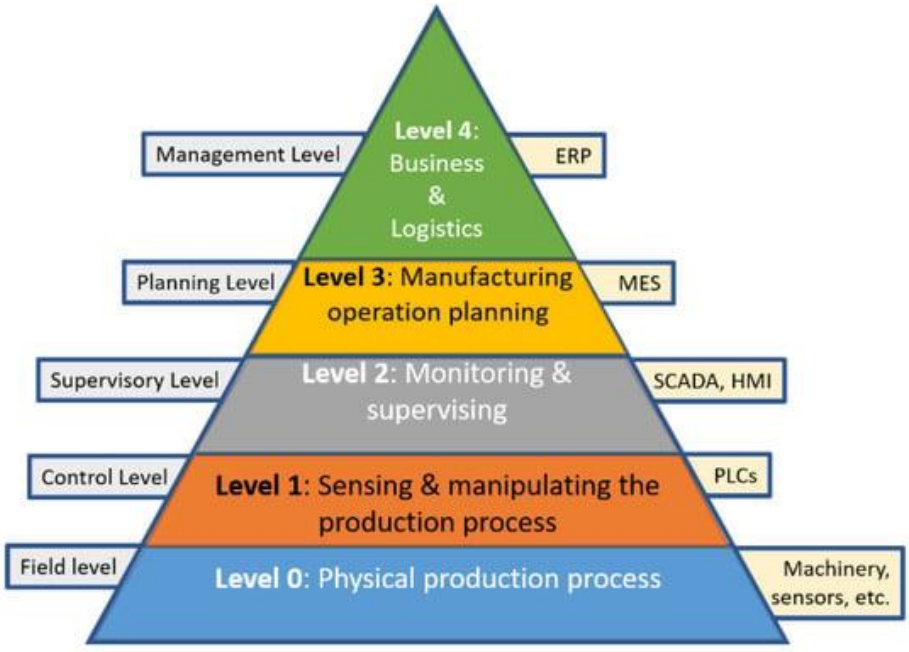
4 VERKKORAKENTEEN MALLIT

4.1 ANSI/ISA-95-hierarkiamalli

ISA-95-hierarkiamalli, viralliselta nimeltään ANSI/ISA-95 Enterprise-Control System Integration ja kansainvälisesti IEC/ISO 62264 on OT-verkkojen malli, joka käsittää viisi tasoa (ISA-95 framework and layers n.d.). ISA-95 on kansainvälinen standardi, jonka tavoitteena on luoda viitekehys ERP:in, MES:in ja prosessin ohjausjärjestelmien välille. Viitekehyksen avulla saadaan selkeä ja johdonmukainen erottelu eri järjestelmätasojen välillä, joka helpottaa muun muassa järjestelmän toteuttamista ja siihen tehtävien muutosten ja lisäysten tekemistä. (Eisner 2023.)

Vuonna 1995 International Society of Automation ja American National Standards Institute kehittivät ISA-95-mallin seuraajaksi ISA-88-mallille. ISA-88-malli ei ottanut huomioon nykypäivän teknologioita, kuten IoT:ta. Tämän vuoksi kehitettiin ISA-95-malli, jonka tarkoitus on sietää muutoksia ja uudistuksia eri tasojen teknologioissa. (Eisner 2023.)

Mallin viisi tasoa ovat numeroitu välille 0–4 kuvion 2 mukaisesti.



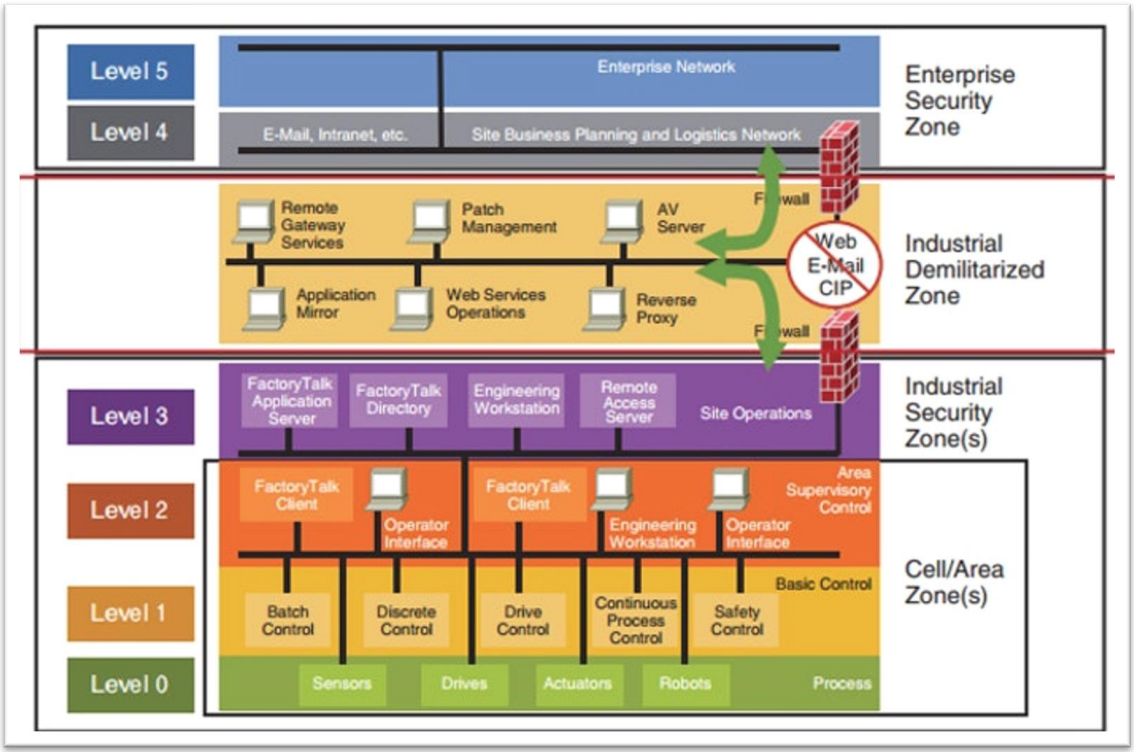
KUVIO 2. ISA-95-hierarkiamallin tasot (Martinez, Ponce, Macias & Molina 2021. CC BY 4.0).

Alin taso nolla (0), eli kenttätaso käsittää fyysiset prosessin laitteet, jotka ovat liitettyinä kenttäväylällä prosessia ohjaaviin laitteisiin. Tämä ei kuitenkaan käsitä analogisesti ja digitaalisesti ohjattuja laitteita, koska nämä eivät ole suoraan kenttäväylällä ohjattuja. Taso yksi (1) on ohjaustaso, johon kuuluu PLC:t, DCS-järjestelmät sekä muut mahdolliset prosessia ohjaavat laitteet. Tasoon kaksi (2), eli valvontatasoon sisältyy erilaiset laitteet ja ohjelmistot, joilla valvotaan ja seurataan prosessin toimintaan. Tasolla kolme (3), eli suunnittelutasolla on MES-järjestelmä, joka toimii siltana hallintotasoon, eli tason neljä (4) ERP-järjestelmään (What is a manufacturing… n.d.). Yrityksen oma IT-verkko yhdistyy OT-verkkoon yleensä tasoilla kolme (3) ja neljä (4).

MES-järjestelmän tehtävä on muun muassa seurata prosessin tilaa, siihen vaadittavien materiaalien määrää ja saatavuutta sekä seurata tuotteiden laatua (What is a manufacturing… n.d.). Kun valvontatasolla seurataan pelkästään prosessin toimintaa, suunnittelutasolla seurataan prosessin toimintaa ja materiaalien saatavuutta korkeammalla tai yleisemmällä tasolla. MES-järjestelmä voi liittyä IT-verkkoon sen tuottamien raporttien osalta, mutta itse materiaalien hallinta ja tuotannon seuraus on osa OT-verkkoa sen vaatiman reaaliaikaisen tiedon takia.

4.2 Purdue-malli

Purdue-malli on Center for Information Systems Security Studies and Research -keskuksen 1990-luvulla kehittämä viitekehys OT-verkoille. Malli on hyvin samankaltainen, kuin ISA-95-malli. Tärkeimpänä erona Purdue-malliin on sisällytetty tietoverkkojen rakennetta, joita ISA-95-mallissa ei ole. Mallin tarkoitus on erottaa IT- ja OT-verkko toisistaan. Eräs esimerkki mallin hierarkiasta on esitetty kuviossa 3.



KUVIO 3. Purdue-malli (Pease 2021).

Kuviosta nähdään, että malli on hyvin samankaltainen, kuin ISA-95-malli. Nimeämisten lisäksi eroina on DMZ-taso sekä neljännen tason jakaminen tasoihin neljä ja viisi.

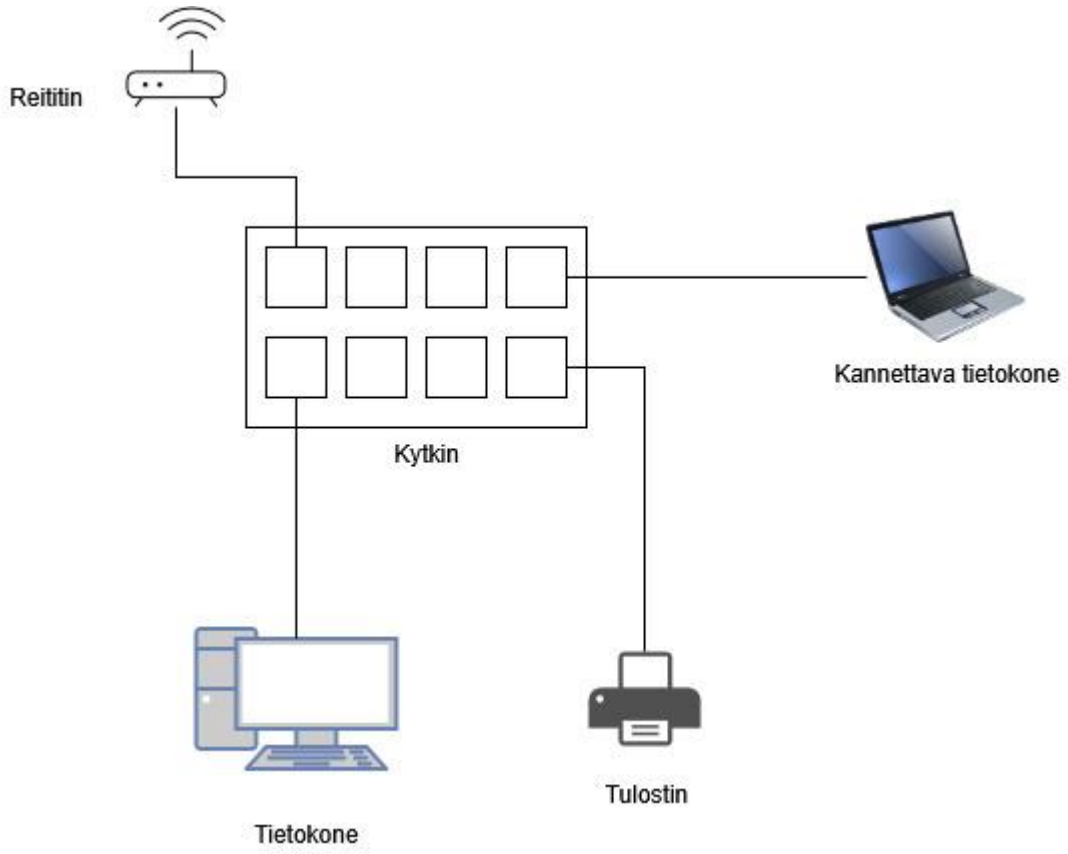
Tasojen kolme ja neljä välillä on DMZ, eli demilitarized zone. DMZ on erillinen fyysinen tai virtuaalinen verkko, joka erottaa yksityisen verkon julkisesta verkosta (DMZ Networks. n.d.). Tätä tasoa saatetaan myös joskus kutsua tasoksi 3,5. DMZ-tasolla voi olla esimerkiksi etäyhteyksiä hallinnoiva palvelin tai historiapalvelimen varmuuskopio. Tasolla on siis laitteita ja palveluita, joita ulkopuoliset käyttäjät voivat käyttää. Palomuurien avulla ulkopuoliset yhteydet pidetään yrityksen IT- ja OT-verkoista erotettuna. Tämä samalla erottaa yrityksen IT- ja OT-verkon toisistaan, sillä DMZ-taso on kyseisten verkkojen välillä.

Parhaassa tilanteessa DMZ-tasossa on kaksi palomuuria. Yksi palomuuri erottaa tason ulkoisilta yhteyksiltä ja toinen palomuuri erottaa tason sisäisiltä yhteyksiltä. Tämän ansiosta, vaikka hyökkääjä onnistuisi pääsemään DMZ-tason ulkoisen palomuurin läpi, ei hyökkääjä vielä pääse yrityksen sisäiseen verkkoon. (DMZ Networks. n.d.)

5 VERKKOJEN LAITTEISTO

5.1 Verkkokytkin

Verkkokytkin on laite, joka vastaanottaa ja lähettää tietoa fyysisiä kaapeleita pitkin. Yleensä kytkimessä on RJ45-liittimet, joita käytetään Ethernet-kaapeleissa sekä joissain Ethernet-pohjaisissa kenttäväyläratkaisuissa, kuten Profinetissä. Tämän lisäksi kytkin voi tukea koaksiaali- tai kuitukaapeleita liittimineen. Kytkimeen voidaan myös kytkeä langaton reititin kuvion 4 mukaisesti, jolloin laitteet voivat kommunikoida paikallisesti sekä langattomasti. Kuvion kytkimessä on 8 porttia, eli liitäntäpaikkaa. Kytkimissä voi kuitenkin olla tätä vähemmän tai enemmän portteja.



KUVIO 4. Kytkimen periaatekuva.

Kytkimen toiminta perustuu MAC-osoitteisiin. MAC-osoite on yksilöivä osoite tai numerosarja, jonka avulla laite voidaan tunnistaa ja yksilöidä verkossa. Se on

useimmiten valmistajan määrittelemä, mutta joissain laitteissa se voidaan vaihtaa. Osoite on usein merkitty laitteeseen tarralla tai tekstillä.

MAC-osoite koostuu 12:ta heksadesimaalinumerosta, jotka ovat ryhmitelty pareittain. Parit ovat erotettu joko viivoilla (-) tai kaksoispisteillä (:) standardin IEEE 802.3 mukaisesti. Osoitteet ovat jaettu kahteen osaan kuvion 5 mukaisesti.

KUVIO 5. MAC-osoitteen rakenne.

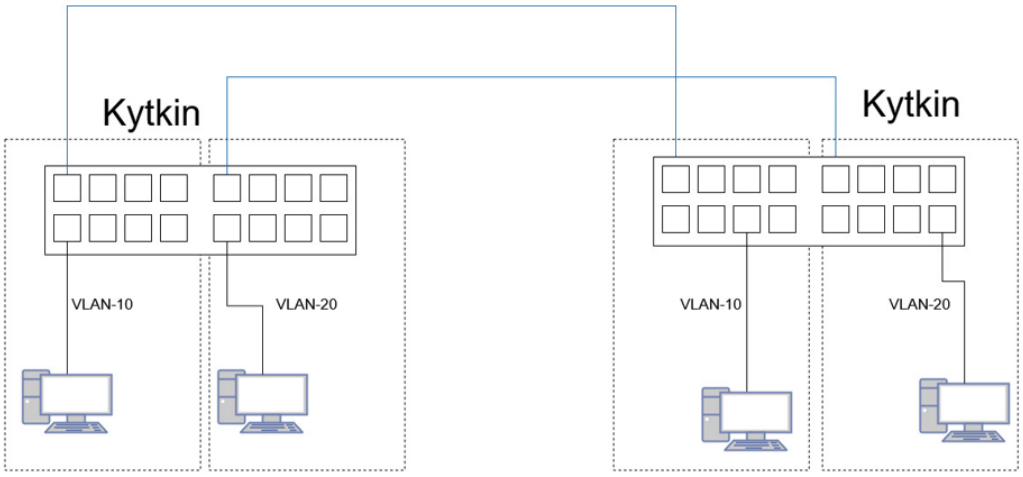
Osoitteen kolme ensimmäistä paria ovat valmistajakohtaisia, jotka IEEE on määritellyt. Kolme viimeistä ovat laitekohtaisia, uniikkeja tunnisteita. (Kumar 2023.)

Kun kytkin vastaanottaa Ethernet-paketin, se tallentaa lähettäjän MAC-osoitteen ja portin, johon lähettäjä on kytketty. Tallennus tapahtuu kytkimen sisäisessä muistissa olevaan MAC-osoite taulukkoon. Jos paketin määränpään MAC-osoite on jo olemassa laitteen taulukossa, kytkin lähettää paketin eteenpäin suoraan oikealle laitteelle oikean portin kautta. Mikäli MAC-osoitetta ei ole tallennettu kytkimen taulukkoon, lähetetään paketti jokaiselle portille. Tällöin laite, jolla on oikea MAC-osoite, hyväksyy Ethernet-paketin ja vastaa kytkimelle. Vastauksen avulla kytkin voi tallentaa vastaanottavan laitteen MAC-osoitteen ja portin seuraavia lähetyksiä varten. (What Is an Ethernet Switch? n.d.)

5.2 VLAN

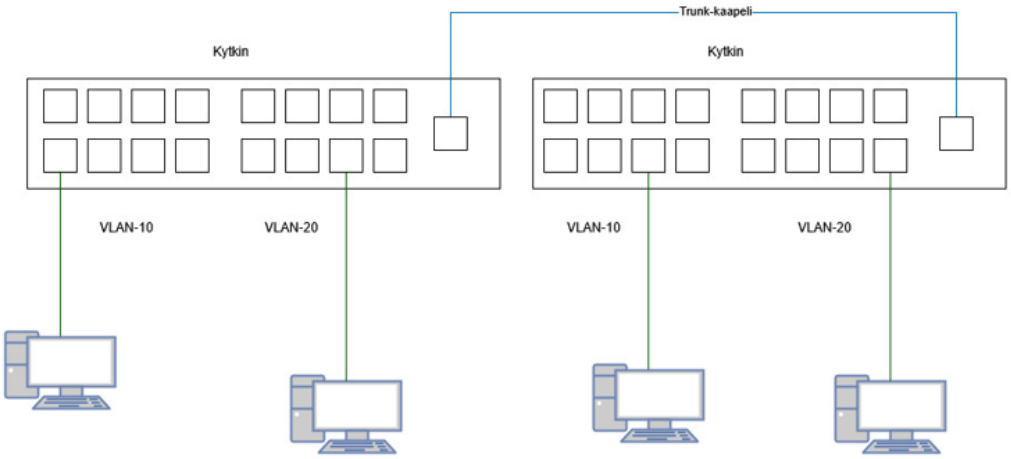
VLAN, eli virtuaalinen paikallisverkko on looginen verkko, jonka avulla fyysinen paikallisverkko voidaan jakaa osiin (What is VLAN… n.d.). VLAN:ia voidaan hyödyntää esimerkiksi verkon segmentointiin. VLAN ei siis itsessään ole fyysinen laite, vaan sen käytön myötä tarvitaan vähemmän fyysisiä laitteita eri verkkojen perustamiseen, ja verkkojen rakenne pysyy yksinkertaisempana.

VLAN voidaan jakaa kahteen eri tyyppiin. Tyypit ovat on port-based ja tagged. Port-based VLAN:issa kytkimen eri portit määritellään ennalta kuuluvan tiettyyn VLAN:iin. Tätä käytetään, kun laite yhdistetään kytkimeen, tai kytkin toiseen kytkimeen kuvion 6 mukaisesti. VLAN-10 portit ovat yhdistetty toisiinsa, jolloin kyseisiin portteihin kytketyt tietokoneet ovat samassa verkossa. VLAN-20 portteihin kytketyt tietokoneet ovat taas omassa verkossaan, eivätkä voi suoraan kommunikoida muiden tietokoneiden kanssa.



KUVIO 6. Port-based VLAN periaatekuva.

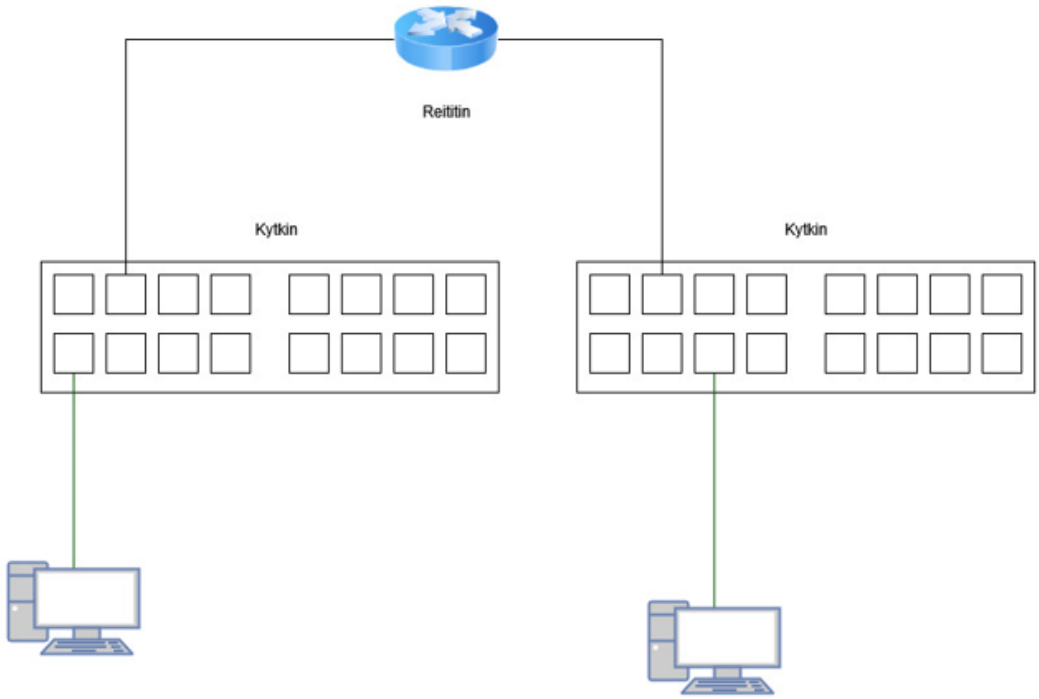
Toinen olemassa oleva VLAN:in tyyppi on tagged. Tämän erikseen määritellyn ”trunk”-portin kautta kulkeviin tiedonsiirtopaketteihin on lisätty erillinen tunniste, joka määrittelee mihin VLAN:iin kyseinen tiedonsiirto kuuluu. Tämän portin avulla useita kytkimiä voidaan helposti yhdistää yhdellä Ethernet-kaapelilla, jota kutsutaan ”trunk”-kaapeliksi. Tämän avulla sama VLAN voi olla fyysisesti useissa eri kytkimissä, eli saman VLAN:in laitteet voivat kommunikoida keskenään, vaikka ne olisivat kytketty eri kytkimiin kuvion 7 mukaisesti.



KUVIO 7. Tagged VLAN periaatekuva

5.3 Reititin

Reititin on laite, joka mahdollistaa kahden tai useamman verkon yhdistämisen keskenään. Kuviossa 8 on esitelty periaatekuva kahdesta verkosta, jotka ovat yhdistetty reitittimellä. Näin on saatu yhdistettyä kaksi eri verkkoa ja niiden tietokoneet voivat kommunikoida keskenään. Usein kotitalouksissa reititin myös mahdollistaa kommunikoinnin internetiin.



KUVIO 8. Reitittimen periaatekuva.

Reitittimet ovat joko langallisia, langattomia tai näiden yhdistelmä (What is a router? n.d.). Langallinen reititin voi olla fyysisesti samankaltainen kuin kytkin, mutta nykyiset reitittimet yleensä sisältävät DHCP-palvelimen. Tämän palvelimen tarkoitus on jakaa paikallisia IP-osoitteita. Reititin siis vastaanottaa ja jakaa tietoliikenteen MAC-osoitteen sijasta IP-osoitteella (What is a router? n.d.). Langaton reititin toimii vastaavasti, mutta siihen ei tarvitse kytkeä fyysisiä johtoja laitteilta, vaan voidaan käyttää langatonta yhteyttä.

Ennen DHCP-palvelimia kaikki verkon laitteiden IP-osoitteet piti määritellä manuaalisesti. Näitä osoitteita kutsutaan staattisiksi IP-osoitteiksi. Tämä saattoi olla suuressa verkossa erittäin aikaa vievää, jonka lisäksi inhimillisten virheiden mahdollisuus oli olemassa. Virheiden oireet ovat tyypillisesti epäselviä, jonka johdosta niiden selvitys on hankalaa. (Klusaitė 2023.) Esimerkiksi jos kahdella laitteella on sama IP-osoite, voi toinen laitteista poistua verkosta tai toimia epävakaasti.

Nykyaikana määritetään edelleen staattisia IP-osoitteita varsinkin OT-verkkojen sisällä. OT-verkkojen laitemäärä on usein vakio, jolloin vapaiden IP-osoitteiden

seuraaminen on huomattavasti helpompaa, kuin IT-verkossa. OT-verkkoja toteutettaessa on toivottavaa pitää kirjaa käytetyistä IP-osoitteista, jotta mahdolliset lisäykset ja muutokset ovat helpommin toteutettavissa.

Internetiin yhdistämistä varten tarvitaan yleensä modeemi. Reititin usein yhdistetään modeemiin, jolloin verkkoon voi yhdistää enemmän laitteita, kuin ilman reititintä. Modeemin tehtävä on siis muuntaa Internet-palveluntarjoajan eli ISP:n signaali analogisesta digitaaliseen muotoon, jotta laitteet voivat prosessoida kyseisen datan. Nykyään varsinkin kotitalouksissa on käytössä modeemi-reititin-yhdistelmä, joiden avulla vain yksi laite riittää yhdistämään talouden laitteet keskenään sekä Internetiin. (Modem vs Router… n.d.)

Tämän lisäksi asiakkaille tarjotaan yhä useammin mahdollisuutta yhdistää suoraan valokuituun, jolloin modeemia ei enää tarvita. Modeemin sijasta tässä tapauksessa tarvitaan optinen verkkopääte (Optical Network Terminal, ONT), joka muuntaa valokuidun optisen tiedon sähköiseksi tiedoksi ja toisinpäin. (What is fiber internet? n.d.)

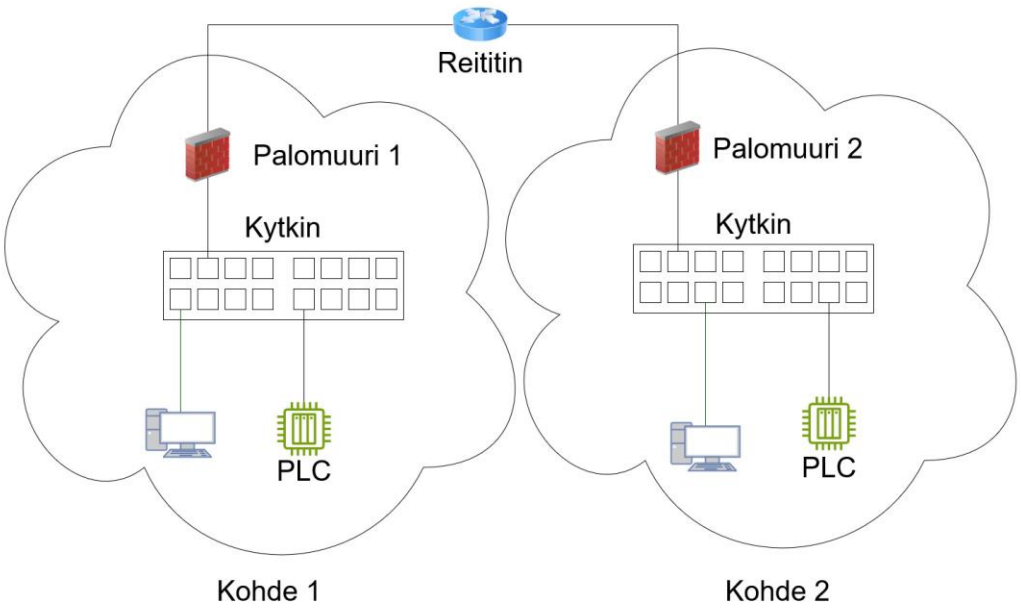
5.4 Palomuuri

Palomuuri on laite tai ohjelmisto, jonka tarkoituksena on valvoa ja hallita sen kautta kulkevia yhteyksiä. Palomuuri on yleensä sijoitettu sisäisen ja ulkoisen verkon väliin. Yhteyksien valvomiseen käytetään käyttäjän luomia sääntöjä. Sääntöjä voi määrittää esimerkiksi

- porttien
- protokollien
- IP-osoitteiden
- sovelluksien perusteella. (Okeke 2023.)

OT-verkoissa palomuureja käytetään usein verkon segmentointiin, eli sen jakamiseen osiin. Näin voidaan estää tarpeettomia ja luvattomia yhteyksiä segmentin ulkopuolelta. Samalla kuitenkin segmentin sisällä laitteet voivat kommunikoida keskenään vapaasti, jolloin palomuuri ei aiheuta ongelmia laitteiden kommuni-

koinnissa. Usein OT-verkkojen laitteet ovatkin eristettyjä Internetistä ja toimistoverkosta palomuurien avulla (What is OT security? n.d.). Esimerkki segmentoinnista on esitetty kuviossa 9.



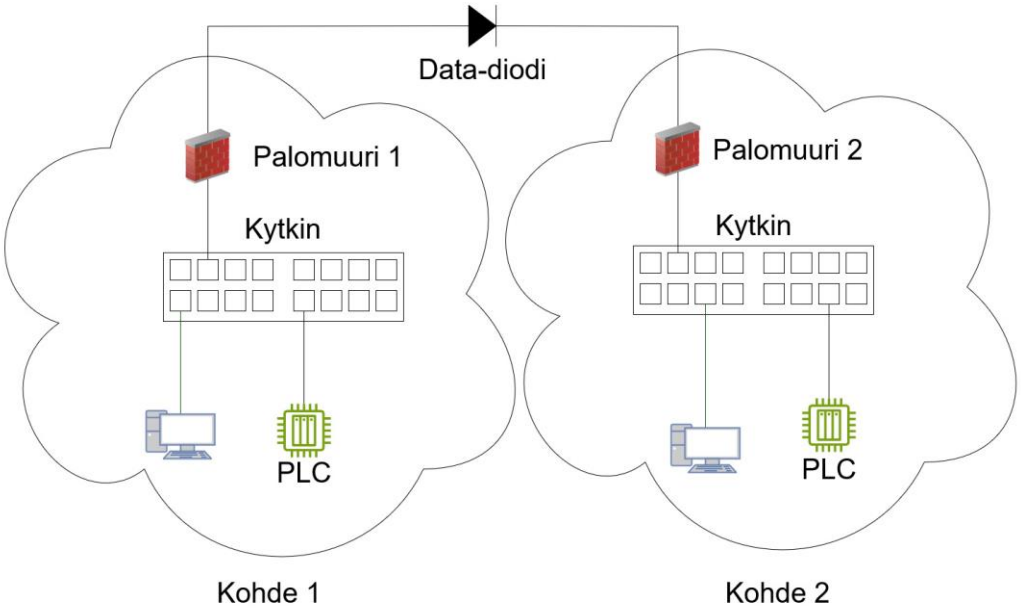
KUVIO 9. OT-verkkojen segmentointi palomuurin avulla.

Kuviossa on palomuureilla eroteltu kaksi tehdasta Kohde 1 ja Kohde 2 IT-verkosta. Nämä voisivat myös olla kaksi eri osaa suurempaa prosessia. Tämä mahdollistaa prosessilaitteiden saumattoman kommunikoinnin keskenään, ja estää samalla luvattomat yhteydet ohjaustasolta.

Yhteyksien luottamuksellisuus on OT-verkkojen matalin prioriteetti. Kuitenkin, jos ulkopuolinen hyökkääjä pääsee verkkoon, voi hyökkääjä saada pääsyn liikesalaisuuksiin tai muokata jopa prosessin arvoja. Nämä voivat johtaa suuriin rahallisiin menetyksiin, jos esimerkiksi patentin alainen valmistustapa pääsee julkisuuteen. Myös prosessin arvoja tai PLC:n ohjelmaa muokkaamalla voidaan jopa rikkoa kenttälaitteita, jolloin koko tehdas voi joutua keskeyttämään toimintansa hetkellisesti. Näiden seikkojen takia on tärkeää estää luvattomien tahojen pääsy yrityksen järjestelmiin.

5.5 Data-diodi

Data-diodi on fyysinen laite, jonka tarkoitus on rajoittaa tietoliikenteen kulkua yhteen suuntaan (Stouffer ym. 2023, 161). Laite toimii nimensä mukaisesti diodin tavoin, eli sallii tietoliikenteen kulun vain yhteen suuntaan. Data-diodin käyttökohteita ovat kriittisten järjestelmien rajapinnat, jotka eivät vaadi kahdensuuntaista kommunikaatiota. Esimerkiksi OT-verkosta voitaisiin viedä raportti IT-verkkoon data-diodin kautta. Näin voidaan fyysisesti varmistaa, ettei IT-verkosta voi lähettää mitään tietoa OT-verkkoon. Kuviossa 10 on havainnollistettu, miten data-diodin kautta voidaan lähettää tietoa toiseen kohteeseen turvallisesti.



KUVIO 10. Data-diodin käyttöesimerkki.

Kuviossa käytetään aiemman kohdan esimerkkiä Kohteista 1 ja 2. Tässä esimerkissä Kohde 1 voi lähettää tietoa kohteeseen 2. Kohde 2 taas ei voi lähettää tietoa takaisin kohteeseen 1.

Data-diodi voi siis fyysisen rakenteen takia lähettää tietoa yhteen suuntaan. Tämän takia diodia voidaan käyttää vain, jos tietoliikenne on yhdensuuntaista, kuten

erilaiset raportit. Diodin fyysinen toiminta perustuu lähettimeen ja vastaanottimeen. Lähetin muuntaa signaalin sähköisestä optiseksi ja vastaanotin muuntaa optisen signaalin takaisin sähköiseksi (Paillet 2020). Näin signaali ei voi fyysisesti kulkea toiseen suuntaan, sillä vastaanotin ei kykene lähettämään optista signaalia.

Data-diodia käytetään usein OT-verkon ja IT-verkon välissä niin, että OT-verkko voi lähettää tietoa IT-verkkoon. Tämä mahdollistaa esimerkiksi raporttien keräämisen ja tarkastelun sekä erilaisten ERP-järjestelmään tarvittavien tietojen keräämisen. Samalla varmistetaan, ettei mikään hyökkäys IT-verkon suunnalta voi päästä OT-verkkoon.

6 ETÄYHTEYDET

VPN, eli virtuaalinen erillisverkko on salattu yhteys laitteiden välillä Internetissä. VPN muodostaa salatun yhteyden, jota kutsutaan tunneliksi. Kun tietoa lähetetään, se menee ensin VPN-ohjelmalle, jonka jälkeen se kulkee Internet-palveluntarjoajan kautta VPN-palvelimelle ja tämän jälkeen vasta Internetiin. (What Is a VPN… n.d.).

VPN myös piilottaa lähettävän laitteen IP-osoitteen. Ulkopuolelta katsottaessa lähetys tulee VPN-palvelimen IP-osoitteesta. Vaikka lähetys joutuisi ulkopuolisen toimijan haltuun, ei lähetyksen tietoja voi nähdä. Tämä johtuu salauksesta, jonka purkamiseen vaaditaan tietty avain. Avain muodostuu, kun käyttäjä luo yhteyden VPN:ään. Tässä vaiheessa käyttäjä todennetaan sertifikaatilla, joka on käyttäjän laitteella. Tämän jälkeen ohjelma ja palvelin sopivat käytettävät protokollat, joiden perusteella luodaan salausavaimet ja tunneli. (How does a VPN Work? n.d.).

Mikäli halutaan esimerkiksi yhteys yrityksen eri toimipisteiden välillä, voidaan hyödyntää site-to-site VPN:ää, eli kahden toimipisteen välistä VPN:ää. Näin saadaan yrityksen toimipaikkojen verkot käyttäytymään, kuin ne olisivat yhdessä paikallisessa verkossa. Tämän ansiosta kaikki työntekijät voivat käyttää muun muassa yrityksen verkkolevyjä, vaikka niiden palvelimet sijaitsevat eri paikkakunnalla. Tämän käyttöön ei tarvita VPN-ohjelmaa, vaan toimipisteiden välillä on luotu pysyvä VPN-tunneli.

Henkilöstön etäyhteyksissä taas ei yhdistetä verkkoja keskenään, vaan käytetään VPN-ohjelmaa. Tätä voidaan hyödyntää muun muassa etänä työskentelyssä ja asiakkaan automaatiojärjestelmiin pääsyssä. Näin voidaan tehdä päivityksiä tai tarkastella automaatiojärjestelmän toimintaa turvallisesti ilman, että pitää olla fyysisesti asiakkaan tiloissa.

7 VAATIMUKSIEN SOVELTAMINEN – ESIMERKKITAPAUS

7.1 Sovellettavat standardit ja direktiivit

OT-verkkojen suunnittelussa voidaan käyttää useita eri standardeja. Ahosen, Seppälän ja Tyynelän (2021) mukaan parhaita tietoturvastandardeja ovat IEC 62443-sarja, ISO/IEC 27000 -sarja sekä NIST viitekehys, standardit, julkaisut ja raportit (Ahonen, Seppälä & Tyynelä 2021, 84). Standardien lisäksi on hyvä huomioida tuleva NIS2-direktiivi, joka voimaantullessaan määrittelee lainsäädännön kautta tiettyjä toimenpiteitä ja velvollisuuksia verkkojen suunnittelussa ja käytössä.

IEC 62443-sarja keskittyy teollisuuden automaatiojärjestelmiin, joten sitä sovelletaan tässä opinnäytetyössä. ISO/IEC 27000 -sarja on yleiskäyttöinen tietoturvastandardi. Yhdysvaltain Kauppaministeriön virasto NIST julkaisee erilaisia kokonaisuuksia kuten CSF-viitekehyksen, FIPS-standardit, SP-julkaisut ja IR-raportit. NIST CSF saattaa antaa lukijalle helpommin konkreettisin käsityksen kyberriskienhallinnan käytännöistä sekä viittaa aina muihin standardeihin, kuten esimerkiksi IEC 62443-standardiin (Ahonen, Seppälä & Tyynelä 2021, 89-91).

7.1.1 NIS2-direktiivi

NIS2-direktiivi, eli Euroopan unionin verkko- ja tietoturvadirektiivi on säädös, joka koskee useimpien toimialojen tietoturvavelvollisuuksia ja häiriöraportointia. Toimialoihin kuuluu muun muassa energia, terveys ja juomavesi (Kyberturvallisuuskeskus 2024a). Tämän lisäksi on muutamia poikkeuksia – esimerkiksi jos toimija on yhteiskunnan järjestyksen kannalta keskeinen. (Kyberturvallisuuskeskus 2024b.) Direktiivi on julkaistu 14.12.2022, ja se on tämän opinnäytetyön kirjoitushetkellä edelleen Suomen eduskunnan käsittelyssä (Eduskunta 2024).

Direktiivi velvoittaa soveltamisalaan kuuluvien toimialojen harjoittavan riskienhallintaa ja sen arviointia. Toimijoiden on otettava huomioon vähintään direktiivin 21.

artiklan luettelon kohdat. Riskienhallinta on myös suhteutettava toimijan toimialaan ja sen laajuuteen. (Kyberturvallisuuskeskus 2024b.)

Toimijoilla on direktiivin myötä ilmoitusvelvollisuus viranomaisille merkittävistä poikkeamista. Merkittävä poikkeama on sellainen, joka on esimerkiksi aiheuttanut taloudellisia tappioita tai vaikuttaa muihin luonnollisiin henkilöihin aiheuttamalla huomattavaa vahinkoa. Mikäli ensi-ilmoitusta, jatkoilmoitusta ja loppuraporttia ei tehdä viranomaisille, voidaan toimijalle määrittää seuraamusmaksu. (Kyberturvallisuuskeskus 2024b.)

7.1.2 IEC 62443-standardi

IEC 62443-standardi on kansainvälisesti hyväksytty standardi, joka käsittelee OT-verkkojen ja ohjausjärjestelmien tietoturvaa. Standardi koostuu neljästä pääryhmästä, jotka ovat jaettu edelleen osiin. Pääryhmien sisältö on listattuna seuraavaksi.

Osassa yksi (1), terminologia, käsitteet ja mallit, käsitellään

- soveltamisalaa toiminnallisuuden ja järjestelmien perusteella
- käsitteitä, lyhenteitä ja termejä
- uhkamalleja ja riskien arviointia.

Osassa kaksi (2), politiikat ja prosessit, käsitellään

- vaatimuksia omistajille sekä palveluntarjoajille
- rooleja ja vastuita
- vikakorjausten hallintaa
- kypsyystasojen (ML) määritelmät.

Osassa kolme (3), järjestelmät, käsitellään

- tietoturvateknologioita
- riskiarviointia ja järjestelmäsuunnittelua
- järjestelmien tietoturvatasoja ja vaatimuksia.

Osassa neljä (4), tuotteiden ja komponenttien vaatimukset, käsitellään

- tuotteiden ja komponenttien kyberturvallisuusvaatimuksia
- ohjeita ja vaatimuksia laitevalmistajille.

Standardin soveltaminen perustuu osaltaan eri SL-tasoihin, jotka kuvaavat numeerisesti, kuinka hyvin järjestelmä on suojattu uhkia vastaan. SL-tasoja on neljä, jotka ovat:

- SL 1 – suojaus tahattomia tai satunnaisia uhkia vastaan.
- SL 2 – suojaus yksinkertaisia, pienien resurssien hyökkäyksiä vastaan.
- SL 3 – suojaus kehittyneitä, keskivertaisten resurssien hyökkäyksiä vastaan.
- SL 4 – suojaus kehittyneitä, suurten resurssien hyökkäyksiä vastaan. (IEC 62443-4-2 2019, 26.)

Tämän lisäksi SL-tasot ovat jaoteltu kolmeen ryhmään, jotka ovat:

- SL-T – tavoiteltu turvallisuustaso riskienarvioinnin perusteella.
- SL-A – saavutettu turvallisuustaso, joka määritellään järjestelmän valmistumisen jälkeen.
- SL-C – komponenttien tai järjestelmien suunniteltu turvallisuustaso, kun ne ovat oikein asennettu ja määritelty. (IEC 62443-3-3 2019, 68.)

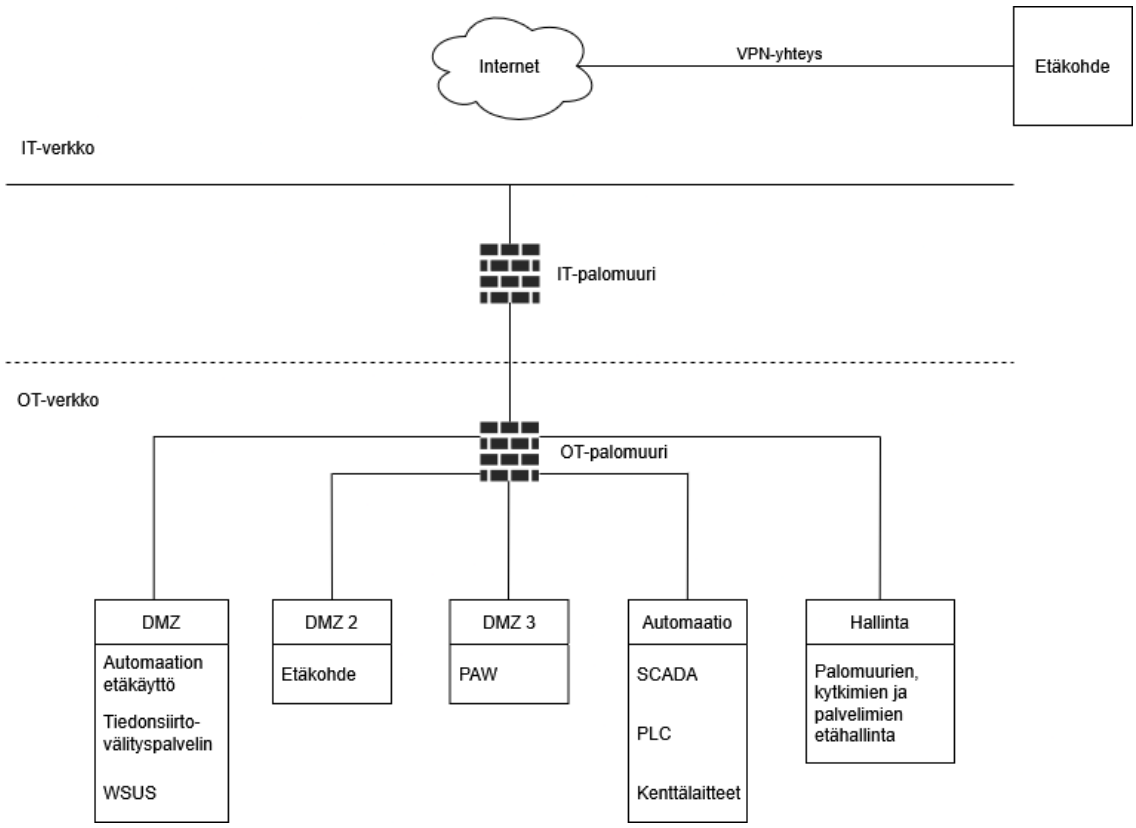
7.2 OT-verkon suunnitelma

Esimerkkitapauksessa kuvitteelliselle asiakkaalle rakennetaan OT-verkko, johon esimerkiksi automaatiosuunnittelija voi yhdistää etäyhteydellä. Tämän lisäksi tiedonsiirto pilvipalveluihin on oltava mahdollista. Asiakkaalla on myös etäkohde, eli erillisessä kohteessa on erillinen OT-verkko, ja kyseisten verkkojen on pystyttävä kommunikoimaan keskenään tarvittaessa. OT-verkko tullaan yhdistämään IT-verkkoon, jonka kautta kyseiset kommunikoinnit tehdään. Suunnittelun pohjana käytetään Purdue-mallia, NIS2-direktiivin teknisiä vaatimuksia ja IEC 62443-3-3-standardia. Oikean asiakkaan tapauksessa asiakkaan tulisi myös tehdä oma tietoturvariskienhallinnan arviointi, jonka vaatimuksien perusteella verkko tulisi suunnitella. Tässä opinnäytetyön tapauksessa OT-verkko tullaan fyysisen rakenteen osalta suunnittelemaan IEC 62443-3-3-standardin SL 2 -tason mukaisesti.

OT-verkon yhdistäminen IT-verkkoon tuo omat riskit ja haasteensa. Näiden riskien minimoimiseksi OT-verkko vyöhykkeistetään eli segmentoidaan kokonaisuudessaan IT-verkosta, jonka lisäksi OT-verkko itsessään segmentoidaan (IEC 62443-3-3 2019, 56). Myös NIS2-direktiivi määrittelee, että verkko tulisi segmentoida (Direktiivi 2022/2555/EU, 127). Esimerkiksi palomuurien ja kytkimien hallintaverkko erotetaan valvomoverkosta. Standardi myös määrittelee, että verkkojen tulisi toimia erillisinä, eristettyinä saarekkeina tarpeen tullessa (IEC 62443-3-3 2019, 56-57). Tällaisia tarpeita on esimerkiksi yhteyden katkeaminen tai tietoturvaselkkaus IT-verkossa.

Standardissa on määritelty, että tarpeettomat toiminnallisuudet, portit, protokollat ja palvelut tulisi poistaa käytöstä (IEC 62443-3-3 2019, 65). Tämä standardin kohta tukee pienimmän oikeuden periaatetta. Tarpeettomat yhteydet pitäisi estää myös NIS2-direktiivin mukaan osana pääsynhallintaa (Direktiivi 2022/2555/EU, 127). Mikäli vain tarpeelliset yhteydet sallitaan palomuurin kautta, on hyökkääjän huomattavasti vaikeampi soluttautua järjestelmään.

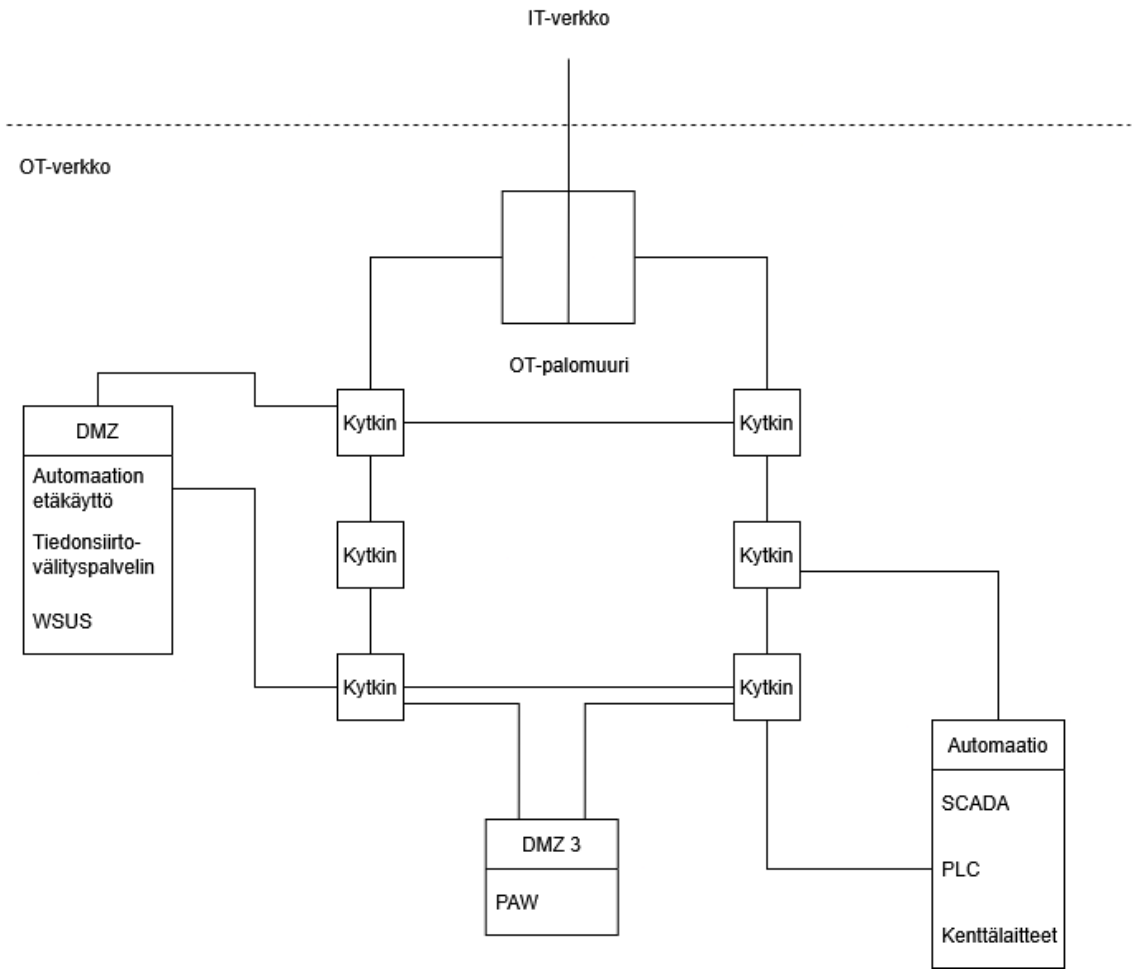
Segmentointi IT-verkosta toteutettiin kahdella palomuurilla verkkojen välillä, yksi IT-verkon puolella ja toinen OT-verkon puolella. Tämän lisäksi OT-verkkoon perustettiin segmentit VLANia hyödyntäen. Kaikki tietoliikenne on reititetty OT-palomuurin kautta, jolloin luvattomien yhteyksien riski pienenee. Kuviossa 11 on esitelty verkon topologia, josta nähdään segmentoidut osat.



KUVIO 11. OT-verkon suunniteltu topologia.

OT-verkossa on kolme DMZ-verkkoa, joiden kautta tehdään kaikki kommunikaatio verkon ulkopuolelle. Ensimmäisessä DMZ-verkossa on automaation etäkäyttö, jonka kautta voidaan ottaa yhteys automaatiolaitteistoon. Tämän lisäksi siellä on tiedonsiirto-välityspalvelin, jonka kautta voidaan lähettää erilaiset automaation tuottamat raportit ja pöytäkirjat yrityksen pilvipalveluun. Lopuksi on vielä WSUS, eli keskitetty Windows-pohjaisten järjestelmien päivitys- ja hallintapalvelu. DMZ 2 -verkon kautta tämän kohteen automaatiojärjestelmä voi kommunikoida etäkohteen kanssa. DMZ 3 -verkko sisältää PAW-tietokoneen, eli tietokoneen, jonka käyttö on rajoitettu vain järjestelmien hallintaan. Automaatioverkko sisältää SCADA-järjestelmän ja PLC:t. Lopuksi on vielä hallintaverkko, jonka avulla voidaan hallita verkon laitteita, kuten palomuureja, kytkimiä ja palvelimia.

Aiemman kuvion 11 yleinen topologia on helposti luettava, mutta sisältää vain osan tiedosta. Yksityiskohtaisempi verkon rakenne on esitetty kuviossa 12.



KUVIO 12. OT-verkon yksityiskohtaisempi rakenne.

Kuviosta nähdään huomattavasti monimutkaisemman näköinen rakenne. Tärkeimpinä huomioina kuviossa on kytkimien rengasrakenne, jonka ansiosta yhden kaapelin rikkoutuminen ei vaikuta verkon toimintaan. Tämän lisäksi palomuuri on kahdennettu eli redundanttinen. Mikäli palomuuri vikaantuisi, redundanttinen palomuuri varmistaisi, että tietoliikenne ei koe katkoksia. Lopuksi vielä jokainen laite on kytketty kahteen eri kytkimeen. Tämän ansiosta yhden kaapelin rikkoutuminen ei vaikuta laitteen toimintaan. Nämä aiemmin mainitut redundanttiset rakenteet varmistavat, että OT-verkon ensimmäinen prioriteetti, eli korkea saatavuus täyttyy.

Mikäli turvallisuustasoa haluttaisiin nostaa edelleen, voidaan käyttää esimerkiksi data-diodeja. Data-diodeilla voidaan saavuttaa jopa SL 4 -taso. IEC 62443-3-3 standardi määrittelee SL 4 -tason täyttämiseksi, että kriittiset ohjausjärjestelmät pitää segmentoida loogisesti sekä fyysisesti ei-kriittisistä ohjausjärjestelmistä (IEC 62443-3-3 2019, 56-57). Tämä voidaan toteuttaa asentamalla data-diodi

OT-verkon ja IT-verkon väliin. Tämä kuitenkin tuo mukanaan tiettyjä haasteita. Näistä yksi merkittävimmistä on se, että automaatiojärjestelmää ei voida hallita etänä, koska se vaatii kahdensuuntaista tietoliikennettä. Samasta syystä suora VPN-yhteys etäkohteeseen ei ole mahdollista. Näitä rajoituksia voidaan kuitenkin kiertää esimerkiksi etäyhteyspalvelimella DMZ 2 -verkossa. Etäkohteen ja palvelimen välillä on jatkuva VPN-yhteys. Palvelimen ja muun verkon välissä on taas data-diodi, jolloin tieto ei voi fyysisesti kulkea etäkohteesta pääkohteen OT-verkkoon.

8 POHDINTA

Opinnäytetyön tarkoituksena oli selventää opinnäytetyön tekijälle sekä lukijalle OT-verkkojen keskeisimmät laitteistot, mallit ja termit. Tämän lisäksi kuvitteelliselle asiakkaalle suunniteltiin standardien ja hyvien suunnittelutapojen mukainen OT-verkko. Työtä voi käyttää tukena OT-verkon suunnitteluun, mutta työ ei kuitenkaan ole yksiselitteinen ohje verkon suunnitteluun.

Työssä syvennytään enimmäkseen OT-verkon teoriaan ja tärkeimpiin käsitteisiin. Aiheeseen liittyviin standardeihin on viitattu soveltuvin osin, mutta tämän syvempää analyysiä niistä ei ole tämän opinnäytetyön laajuuteen sisällytetty. Kuten esimerkkitapauksesta selviää, aivan kaikkea OT-verkoista ei ole standardoitu. Standardit ja mallit antavat karkeat raamit verkon toteutukseen, jonka lisäksi sovelletaan niin kutsuttuja hyviä toteutustapoja. Näitä toteutustapoja on selvitetty konsultoimalla alan asiantuntijaa, ja tavat ovat perusteltu esimerkiksi OT-verkon prioriteeteilla. Tämä esimerkkitapaus ei siis ole yksi ja ainoa totuus, vaan tarpeen mukaan on tehtävä muutoksia.

Lähteinä työssä on käytetty monipuolisesti sekä kirjallisuutta, että Internetistä löytyviä verkkosivuja. Varsinkin verkkosivujen tapauksessa kyseistä tietoa on etsitty useammalta sivustolta valheellisen tiedon välttämiseksi. Useat lähteet ovat peräisin laitteistojen valmistajilta, joten lähteet voidaan perustella luotettaviksi. Suurin osa lähteistä on englanninkielisiä johtuen alan ja aiheen kansainvälisyydestä.

Työn perusteella on luotu erillinen dokumentaatio Insta Automation Oy:lle, jota ei julkaista tämän opinnäytetyön yhteydessä. Dokumentaatio pitää sisällään yksityiskohtaiset ja selkeät opastukset yleisimpiin ratkaisuihin ja haasteisiin OT-verkkojen suunnittelussa. Tämän pohjalta yrityksen työntekijät voivat toimia tehostetummin ja yhtenäisemmin.

Opinnäytetyön rajaus tehtiin aluksi karkeasti, jonka jälkeen rajausta tarkennettiin sopivaksi opinnäytetyön laajuuteen nähden. Rajaus palvelee mielestäni hyvin automaatiosuunnittelijan tarpeita, kuitenkin jättäen hieman kehitysvaraa. Aikataulu

oli mielestäni sopiva, jolloin tekijällä oli hyvin aikaa perehtyä aiheeseen ja rajata aihetta kohdeyleisöä varten.

Jatkokehittämistä aiheen ympärillä on vielä runsaasti. Tässä opinnäytetyössä on käsitelty laajuuden takia vain fyysiset laitteistot sekä niihin liittyvät mallit ja vaatimukset. Jatkokehityskohteena voisi olla esimerkiksi erilaisten ohjelmistopohjaisten vaatimuksien täyttäminen, kuten nopeasti yleistyvä Multifactor Authentication, eli monivaiheinen tunnistautuminen.

Opinnäytetyö onnistui mielestäni kuitenkin hyvin. Työ etenee loogisesti ja teoriaosuutta on hyödynnetty esimerkkitapauksessa. Työn teoriaosuus palvelee lukijaa aiheen ymmärtämisessä ja opinnäytetyön pohjalta voidaan muodostaa kokonaiskuva OT-verkoista sekä niiden rakenteellisista vaatimuksista.

Suurimpina haasteina työn tekemisessä oli aiheen rajaus. Koska aihe ja siihen liittyvät standardit ovat erittäin laajoja, täytyi aiheen rajaukseen käyttää huomattava määrä aikaa.

LÄHTEET

Ahonen, P., Seppälä, J. & Tyynelä, M. 2021. Automaation tietoturva. Kriittisen tuotannon turvaaminen. Helsinki: Suomen Automaatioseura ry.

Direktiivi 2022/2555/EU. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

DMZ Networks. n.d. Fortinet. Verkkosivu. Viitattu 14.1.2025. https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Eduskunta. 2024. Asian käsittelytiedot HE57/2024 vp. Verkkosivu. Viitattu 13.2.2025. https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_57+2024.aspx

Eisner, C. 2023. What is ISA-95. Verkkosivu. Viitattu 5.11.2024. https://www.getmaintainx.com/learning-center/what-is-isa-95

EUR-Lex. n.d. Direktiivi. Verkkosivu. Viitattu 18.12.2024. https://eur-lex.europa.eu/FI/legal-content/glossary/directive.html

How Does a VPN Work? n.d. Paloalto Networks. Verkkosivu. Viitattu 9.12.2024. https://www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work

ISA-95 framework and layers. n.d. Siemens. Verkkosivu. Viitattu 12.11.2024. https://www.sw.siemens.com/en-US/technology/isa-95-framework-layers/

Klusaitė, L. 2023. Mikä DHCP on ja mihin sitä käytetään? Verkkosivu. Viitattu 15.1.2025. https://nordvpn.com/fi/blog/dhcp-mika-on/

Kumar, R. 2023. What is MAC Address? Verkkosivu. Viitattu 19.11.2024. https://tecadmin.net/media-access-control-address/

Kyberturvallisuuskeskus. 2024a. TRAFICOM_NIS2_taulukko. PDF-tiedosto. Viitattu 13.2.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_07012025.pdf

Kyberturvallisuuskeskus. 2024b. Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2). Verkkosivu. Viitattu 13.2.2025. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tarkeaa-tietoa-euroopan-unionin-kyberturvallisuusdirektiivista#67853-0

Martinez, E., Ponce, P., Macias, I. & Molina, A. 2021. Automation Pyramid as Constructor for a Complete Digital Twin, Case Study: A Didactic Manufacturing System. Verkkosivu. Viitattu 12.11.2024. CC BY 4.0. https://www.mdpi.com/1424-8220/21/14/4656

Mikä on standardi? SFS. n.d. Verkkosivu. Viitattu 18.12.2024. https://sfs.fi/standardeista/mika-on-standardi/

Modem vs Router: What's the Difference? n.d. Xfinity. Verkkosivu. Viitattu 26.11.2024. https://www.xfinity.com/hub/internet/modem-vs-router

Okeke, F. 2023. Firewall Policy: Design, Configuration, and Examples. Verkkosivu. Viitattu 19.11.2024. https://www.enterprisenetworkingplanet.com/security/firewall-policy/

Paillet, D. 2020. Securing OT networks with unidirectional gateways/diodes. Verkkosivu. Viitattu 22.2.2025. https://iebmedia.com/technology/industrial-5g/securing-ot-networks-with-unidirectional-gateways-diodes/

Pease, M. 2021. Supporting Digital Transformation with Legacy Components. Verkkosivu. Viitattu 6.4.2025. https://www.nist.gov/blogs/manufacturing-innovation-blog/supporting-digital-transformation-legacy-components

Sanastokeskus. n.d. TEPA-termipankki. Verkkosivu. Viitattu 18.12.2024. https://termipankki.fi/tepa/fi/haku/standardi

SFS-EN IEC 62443-4-2. 2019. Security for industrial automation and control systems – Part 4-2: Techniocal security requirements for IACS components. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 27.1.2025. Vaatii käyttöoikeuden. https://online.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/6/761379.html.stx

SFS-EN IEC 62443-3-3. 2019. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 27.1.2025. Vaatii käyttöoikeuden. https://online.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/6/764470.html.stx#

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. & Thompson M. NIST SP 800-82r3. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology 20.9.2023. Viitattu 22.2.2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Toivonen, M. 2020. Kyberturvallisuus tuotantoverkoissa ja järjestelmissä. Verkkosivu. Viitattu 5.11.2024. https://yrityksille.elisa.fi/ideat/kyberturvallisuus-tuotantoverkoissa-ja-jarjestelmissa/

What is a manufacturing execution system (MES)? n.d. IBM. Verkkosivu. Viitattu 12.11.2024. https://www.ibm.com/topics/mes-system

What is a router? n.d. Cloudflare. Verkkosivu. Viitattu 26.11.2024. https://www.cloudflare.com/learning/network-layer/what-is-a-router/

What Is a VPN? | VPN Explained. n.d. Paloalto Networks. Verkkosivu. Viitattu 9.12.2024. https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

What is an Ethernet Switch? n.d. Cisco. Verkkosivu. Viitattu 19.11.2024. https://www.cisco.com/c/en/us/products/switches/what-is-an-ethernet-switch.html

What is fiber internet? n.d. Centurylink. Verkkosivu. Viitattu 15.1.2025. https://www.centurylink.com/home/help/internet/fiber/what-is-fiber-internet.html

What Is IT/OT Convergence? n.d. Paloalto Networks. Verkkosivu. Viitattu 6.4.2025. https://www.paloaltonetworks.com/cyberpedia/what-is-it-ot-convergence

What is OT security? n.d. Cisco. Verkkosivu. Viitattu 26.11.2024. https://www.cisco.com/site/us/en/learn/topics/security/what-is-ot-security.html

What is VLAN and how it works. n.d. Etherwan. Verkkosivu. Viitattu 2.2.2025. https://www.etherwan.com/support/featured-articles/brief-introduction-vlans