SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN ALA

FYYSISEN TIETOLIIKENNEVERKON SUUNNITTELU JA TURVALLISUUS TEOLLISUUSYMPÄRISTÖSSÄ

TEKIJÄ Santtu Tsupari

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Energiatekniikan tutkinto-ohjelma	
Työn tekijä Santtu Tsupari	
Työn nimi Fyysisen tietoliikenneverkon suunnittelu ja turvallisuus teollisuusympäristössä	
Päiväys 11.06.2025	12/0
Yhteistyötaho Luottamuksellinen	

Tämä työ on julkinen versio salatusta opinnäytetyöstä, jonka sisältö eroaa teemaltaan laajemmasta salatusta versiosta. Julkisessa versiossa ei käsitellä tekniseen toteutukseen liittyviä tarkempia asioita, vaan keskitytään yleisiin suunnitteluperiaatteisiin ja fyysisen turvallisuuden näkökulmaan teollisuuden tietoliikenneverkoissa.

Työssä tarkastellaan teollisuusympäristön fyysisen tietoliikenneverkon suunnittelun keskeisiä periaatteita, kuten laajennettavuutta, huollettavuutta, luotettavuutta ja turvallisuutta. Lisäksi analysoidaan modernin fyysisen turvallisuuden haasteita, kuten vanhenevan infrastruktuurin vaikutuksia ja dronejen aiheuttamia uhkia.

Työn tuloksena havaittiin, että mikrokanavatekniikka on kustannustehokas ja joustava vaihtoehto teollisuuskohteen tietoliikenneverkon laajennuksiin ja ylläpitoon. Samalla dronejen kehittynyt teknologia ja vanhentuneet suojausratkaisut lisäävät merkittävästi fyysisen turvallisuuden riskejä. Näiden uhkien hallinta edellyttää kokonaisvaltaista suunnittelua ja päivitettyjä suojauksia teollisuusympäristöissä. Fyysiseen turvallisuuteen tulee kiinnittää erityisesti enemmän huomiota vanhemmissa teollisuuskohteissa, joissa nykyiset suojausratkaisut ovat usein vanhentuneita. Näissä ympäristöissä on yleistä, että esiintyy kriittisiä fyysisen turvallisuuden riskejä, jotka voivat uhata sekä tuotannon jatkuvuutta että henkilöstön turvallisuutta. Näiden asioiden kartoittaminen ja päivittäminen on tärkeää turvallisen toiminnan varmistamiseksi.

Avainsanat
Fyysinen tietoliikenneverkko, ICT, turvallisuus, drone

SISÄLTÖ

1 JOHDANTO 4

2 FYYSISEN TIETOLIIKENNEVERKON NYKYTILAN KARTOITUS TEOLLISUUSYMPÄRISTÖSSÄ 5

2.1 Kuituverkkojen kehitys ja nykytilan kartoituksen merkitys teollisuudessa 5

2.2 Haasteet selvitystyössä 5

3 FYYSISEN TIETOLIIKENNEVERKON SUUNNITTELUN PERIAATTEET 7

4 MODERNIN FYYSISEN TURVALLISUUDEN HAASTEET: DRONET JA VANHENEVA INFRASTRUKTUURI 9

5 POHDINTA 11

LÄHTEET 12

1 JOHDANTO

Teollisuuden tietoliikenneverkon suunnittelussa on keskeistä huomioida sekä nykyiset että tulevaisuuden tarpeet. Erityisesti vanhoissa teollisuuslaitoksissa tulee ottaa huomioon olemassa olevan infrastruktuurin rajoitteet ja samalla arvioida maankäytön mahdollisuuksia uusien investointien toteuttamiseksi. Tämä edellyttää kokonaisvaltaista lähestymistapaa, jossa verkon modernisointi ja laajentaminen suunnitellaan palvelemaan sekä tämän päivän tuotantovaatimuksia että tulevaisuuden kasvua ja teknologista kehitystä.

Koska vanhat teollisuusympäristöt ovat usein haastavia asennusten suhteen ja vuosibudjetit asettavat investoinneille tiukat rajat, on erityisen tärkeää löytää joustavia ja kustannustehokkaita ratkaisuja. Joustavuuden huomioiminen korostuu suunnittelussa, jotta verkkoa voidaan helposti mukauttaa muuttuviin tarpeisiin, laajentaa vaiheittain ja vastata sekä nykyisiin että tulevaisuuden vaatimuksiin ilman merkittäviä lisäkustannuksia tai toiminnan keskeytyksiä.

Viime vuosina geopoliittiset jännitteet ja kyberuhkien lisääntyminen ovat korostaneet turvallisuuden merkitystä teollisuuden tietoliikenneverkoissa. Teollisuusympäristöissä tietoliikenneverkot toimivat kriittisenä infrastruktuurina, jonka häiriöt voivat aiheuttaa merkittäviä tuotantokatkoksia, taloudellisia menetyksiä sekä turvallisuusriskejä henkilöstölle tai ulkopuolisille. Lisäksi monissa laitoskokonaisuuksissa on myös sähkön- ja lämmöntuotantoon liittyvää toimintaa, jonka keskeytykset voivat johtaa laajamittaisiin häiriöihin sekä ympäristö- että turvallisuusriskeihin. Tästä syystä fyysisen verkon suunnittelussa ja ylläpidossa on kiinnitettävä erityistä huomiota myös verkon turvallisuuteen.

2 FYYSISEN TIETOLIIKENNEVERKON NYKYTILAN KARTOITUS TEOLLISUUSYMPÄRISTÖSSÄ

2.1 Kuituverkkojen kehitys ja nykytilan kartoituksen merkitys teollisuudessa

Kuituoptiset yhteydet otettiin Suomessa teollisuuskäyttöön vaiheittain teknologian kehittyessä, ja alkuvaiheen toteutuksissa hyödynnettiin usein monimuotokuituja sekä FC-, ST- tai SC-liittimiä. Näillä ratkaisuilla saavutettiin pidempiä siirtomatkoja ja parempaa häiriönsietoa verrattuna kuparikaapelointiin, mutta teknologian kehityksen myötä niiden kapasiteetti, siirtonopeus ja yhteensopivuus nykyaikaisten aktiivilaitteiden kanssa ovat jääneet jälkeen. Lisäksi varhaiset asennukset eivät useinkaan täytä nykyisiä teknisiä standardeja, esimerkiksi taivutussäteiden, tai kaapeloinnin mekaanisen suojauksen osalta, mikä voi aiheuttaa suorituskyky- tai luotettavuusongelmia vanhaa verkkoinfrastruktuuria käytettäessä.

Nykytilan selvittäminen on keskeinen osa tietoliikenneverkon uudistamista tai laajentamista. Ilman ymmärrystä olemassa olevasta infrastruktuurista on vaikea tehdä teknisesti, toiminnallisesti tai taloudellisesti kestäviä ratkaisuja. Erityisesti laajoissa teollisuusympäristöissä nykyverkon kartoitus ennen varsinaista suunnittelutyötä auttaa tunnistamaan, mitä osia voidaan mahdollisesti hyödyntää edelleen, mitkä kohdat vaativat korjausta ja missä uudisrakentaminen on väistämätöntä.

2.2 Haasteet selvitystyössä

Monissa vanhemmissa teollisuuslaitoksissa fyysinen tietoliikenneverkko perustuu mekaaniseen infrastruktuuriin, joka on rakennettu aikakaudella, jolloin verkkojen laajennettavuutta, standardointia tai turvallisuutta ei huomioitu nykypäivän vaatimusten mukaisesti. Vanhoissa jakamoissa ongelmia aiheuttavat muun muassa rajalliset tilat, puutteellinen ilmanvaihto ja kaapelointien dokumentoimaton asennus. Jakamoihin on saattanut vuosien varrella kertyä eri aikakausien kaapelointeja ja liitoksia ilman järjestelmällistä dokumentointia, mikä vaikeuttaa verkon ylläpitoa ja uusien osien integrointia. Usein jakamoiden turvallisuus- ja olosuhdetaso ei vastaa nykyisiä vaatimuksia, mikä lisää riskejä esimerkiksi pölyn, kosteuden tai lämpötilavaihteluiden muodossa.

Usein teollisuuslaitosten alueilla sijaitsee myös maanalaisia kaapeliputkia, jotka voivat olla ajan saatossa tukkeutuneita, sortuneita tai muuten vaurioituneita. Tällaiset rakenteelliset puutteet voivat vaikeuttaa uusien yhteyksien rakentamista, huoltotöitä sekä aiheuttaa ongelmia viankorjauksessa. Kaapelireittien selvittäminen voi osoittautua haastavaksi erityisesti silloin, kun kyseessä on pitkän elinkaaren aikana vaiheittain laajentunut tuotantoympäristö. Monissa vanhemmissa laitoksissa kaapelointi on rakennettu erillisinä kokonaisuuksina eri rakennusvaiheiden ja laajennuksien yhteydessä, jolloin reititykset voivat olla epäyhtenäisiä ja huonosti dokumentoituja. Tämä vaikeuttaa kokonaiskuvan muodostamista sekä uusien yhteyksien suunnittelua.

Erityisenä haasteena verkon rakentamisessa ovat massiiviset kaapelimäärät, joita on kertynyt vuosikymmenten aikana. Reitit voivat olla täynnä vanhaa, käytöstä poistettua tai muuten epäselvää kaapelointia, jonka selvittäminen vie aikaa ja vaatii usein fyysistä tarkastelua vaikeapääsyisissä tiloissa. Usein samoja kaapelireittejä on käytetty sekä sähkö- että tietoliikennekaapelointiin, mikä lisää riskejä erityisesti uudelleenkaapeloinnin tai korjaustöiden yhteydessä.

Lisäksi joissakin tapauksissa reittien tutkimista ja varsinaista rakennustyötä voi rajoittaa rakennusmateriaalien sisältämä asbesti tai muut haitta-aineet, joiden käsittely vaatii erityisjärjestelyjä ja -luvi-

tuksia. Asbestia voi esiintyä esimerkiksi seinärakenteissa, läpivienneissä tai vanhoissa eristysrakenteissa, jolloin selvitystyön turvallinen toteuttaminen edellyttää asiantuntevaa arviointia ja mahdollisesti erillisiä purkutöitä ennen varsinaisten verkkomuutosten toteuttamista. Vanhoissa tehdaskomplekseissa kannattaa asbestitutkimus teettää aina, kun on tiedossa, että kaapeloinnin toteuttaminen vaatii tilojen välisiä kaapeliasennuksia. Toimittajan työntekijän asbestialtistus voi johtaa rikostutkintaan. Joissain tapauksissa haasteita voivat aiheuttaa tilat, joissa käsitellään haitallisia-, tai räjähdysvaarallisia aineita. Suunnittelijan näkökulmasta vastuu asbestitutkimuksista on pääsääntöisesti tilaajalla, mutta asian selvittäminen ja sen esiin ottaminen on hyvää kommunikointia ja työturvallisuuden huomioon ottaminen on jokaisen työntekijän vastuulla.

Tehdasympäristössä selvitystyötä hankaloittaa usein käynnissä oleva tuotanto, joka asettaa merkittäviä rajoitteita työskentelylle sekä ajallisesti että fyysisesti. Monet verkon komponentit sijaitsevat tiloissa, joissa liikkuu raskaita koneita, kuljetuskalustoa tai joissa käsitellään vaarallisia aineita. Tällaisissa kohteissa selvitystyötä ei voida suorittaa vapaasti tai ilman erillistä yhteensovittamista tuotannon kanssa.

Suppeakin selvitys on arvokas päivitys- tai rakennushankkeen alkuvaiheessa, sillä ilman tietoa olemassa olevasta infrastruktuurista riskinä on virheelliset ratkaisut tai tarpeettomat kustannukset. Lisäksi suunnittelualojen välinen kommunikointi varmistaa, että reititykset, kapasiteettivaatimukset ja turvallisuusnäkökohdat huomioidaan kokonaisuutena. Tunnettujen ja kokeneiden urakoitsijoiden hyödyntäminen tuo arvokasta paikallistuntemusta ja käytännön kokemusta toimivista reiteistä ja mahdollisista ongelmakohdista, mikä edistää sujuvaa toteutusta ja vähentää riskejä.

3 FYYSISEN TIETOLIIKENNEVERKON SUUNNITTELUN PERIAATTEET

Tietoliikenneverkon suunnittelu teollisuusympäristössä edellyttää kokonaisvaltaista lähestymistapaa, jossa huomioidaan niin tekniset kuin toiminnallisetkin vaatimukset. Tärkeimpiä suunnitteluperiaatteita ovat laajennettavuus, huollettavuus, luotettavuus, redundanssi sekä fyysisen verkon turvallisuus ja suojausratkaisut.

Laajennettavuus tarkoittaa verkon kykyä mukautua tuleviin muutoksiin ja kasvuun. Verkon reitit ja kaapelivaraukset tulee mitoittaa siten, että uusien yhteyksien lisääminen onnistuu ilman merkittäviä muutostöitä. Esimerkiksi mikrokanavatekniikka ja ylimääräiset putkivaraukset mahdollistavat kaapeleiden jälkiasennuksen ilman suuria kaivuutöitä tai tuotannon häiriöitä. Mikrokanavatekniikka mahdollistaa edullisen lisäkapasiteetin asennuksen samalla, kun maanrakennusta tehdään. Kanavia voi olla järkevää asentaa maanrakennustöiden yhteydessä, vaikka tietoverkon kaapeloinnille ei olisi edes tarvetta.

Asiakasyrityksen tietoliikenneverkon fyysisen infrastruktuurin tulevia laajennuksia varten on päätetty selvittää mikrokanavatekniikan soveltuvuutta sisätiloihin. Tavoitteena on arvioida, voisiko mikrokanavajärjestelmä tarjota kustannustehokkaan, muuntojoustavan ja laajennettavan vaihtoehdon sisäverkon kaapeloinnin toteutukseen. Selvitystyöhön on ryhdytty opinnäytetyöprojektin aikana toteutetun ulkoalueen mikrokanavaverkon hyvien kokemusten perusteella: järjestelmä osoittautui teknisesti toimivaksi, helposti asennettavaksi ja laajennettavaksi ratkaisuksi. Selvityksen keskiössä ovat muun muassa asennusmenetelmät sisäympäristössä, tekniset vaatimukset, materiaalien paloturvallisuus sekä järjestelmän elinkaarikustannukset verrattuna perinteisiin kaapelointiratkaisuihin. Markkinoilla on saatavilla mikrokanavatuotteita, joita valmistajat erikseen markkinoivat sisäkäyttöön soveltuvina, mikä viittaa alan valmiuteen tukea sisäverkkoratkaisuja mikrokanavatekniikalla.

Tietoliikennetilojen väliin asennettava suurikapasiteettinen mikrokanavaverkko tarjoaa ratkaisun erityisesti haastavilla kaapelointiosuuksilla, joissa kaapelireitit ovat ahtaita, vaikeakulkuisia tai läpivientien avaaminen toistuvasti aiheuttaa merkittäviä työkustannuksia ja riskejä kaapeleille. Mikrokanava mahdollistaa useiden kuituyhteyksien asentamisen ilman jatkuvia kaapelinvetotöitä, sillä uusia yhteyksiä voidaan lisätä puhaltamalla kuituja valmiiksi asennettuun kanavaan. Tämä vähentää tarvetta fyysisille muutostöille reiteissä ja läpivienneissä sekä parantaa järjestelmän ylläpidettävyyttä ja turvallisuutta pitkällä aikavälillä.

Valokuitupaneeleita voidaan valita suuremmalla porttimäärällä kuin projekti vaatii, jolloin paneeliin voidaan lisätä myöhemmin uusia runkokaapeleita ilman uutta tilavarausta jakamosta. Kuitupaneeleissa tulee suosia LC-liittimillä varustettuja paneeleita suuremman kytkentätiheyden vuoksi. Laajennettavuus tulee ottaa mahdollisuuksien mukaan huomioon myös jakamovalinnoissa ja kaikessa muussakin tietoliikenneverkon suunnittelussa.

Huollettavuus on keskeinen osa kaikkien laitteistojen ja järjestelmien elinkaaren hallintaa. Helposti saavutettavat ja huollettavat aktiivi- ja passiivilaitteet mahdollistavat nopean vianmäärityksen, ennakoivan kunnossapidon ja lyhyemmät seisokkiajat, mikä tukee sekä tuotantotehokkuutta että turvallisuutta. Suunnitteluvaiheessa tehtävät ratkaisut kuten selkeä komponenttien sijoittelu, modulaarisuus ja dokumentoidut huoltomenettelyt vaikuttavat järjestelmän käytettävyyteen ja elinkaarikustannuksiin. Huollettavuus liittyy myös turvallisuuteen: järjestelmän nopea palauttaminen toimintakuntoon vikatilanteessa voi olla kriittistä esimerkiksi fyysisen suojauksen kannalta.

Luotettavuus on keskeistä kriittisissä teollisuusympäristöissä, joissa tietoliikenneyhteyksien katkeaminen voi aiheuttaa tuotannon seisahduksia tai turvallisuusriskejä. Verkossa tulee käyttää laadukkaita ja käyttötarkoitukseen sopivia komponentteja ja noudattaa asennusstandardeja, jotka takaavat pitkäikäisen ja häiriöttömän toiminnan. Kaikki asennukset tulee tarkistaa ja vaatia asennetusta tekniikasta tarpeelliset mittauspöytäkirjat. Ulkotilojen jakamosuunnittelussa materiaalivalinnat ja lämmitys- sekä jäähdytysratkaisut ovat tärkeitä luotettavuuden kannalta.

Redundanssilla tarkoitetaan tietoliikenneverkoissa järjestelmän kykyä säilyttää toimintakykynsä yksittäisten vikojen sattuessa. Tietoliikenneverkon kontekstissa redundanssi voi ilmetä useilla eri tasoilla – fyysisenä, loogisena tai palvelutasolla – mutta fyysistä infrastruktuuria tarkasteltaessa redundanssi viittaa erityisesti siihen, että verkossa on käytettävissä toimintaa varmistavia vaihtoehtoisia kaapelointeja, yhteysreittejä tai laitteistoja.

Mekaaniset ja sähköiset lukitusjärjestelmät jakamoiden ja kaapelireittien ja -tilojen osalta vähentävät asiattoman pääsyn riskiä verkon kriittisiin osiin. Rakenteiden tulee olla riittävän järeitä ja lukitusratkaisujen standardoituja. Kaikissa asennuksissa tulee suosia varsinaisia tietoliikennetiloja, mutta niissä tapauksissa, joissa jakamoita täytyy asentaa tehdasalueelle, tulee kiinnittää erityistä huomiota suojaukseen. Suojauksen tason tulee olla mahdollisimman lähelle tietoliikennetilaa vastaava. Lasiovellisia, tai lukottomia jakamoita ei tule suunnitella asennettavaksi mihinkään virallisten tietoliikennetilojen ulkopuolelle. Suunnittelussa tulee selvittää mahdollisten ATEX-alueiden vaikutus lisäsuojauksiin.

Valvontakamerat ja muut valvontaratkaisut lisäävät fyysistä turvallisuutta erityisesti verkon keskeisissä solmupisteissä. Kameravalvonta toimii sekä ennaltaehkäisevänä keinona että jälkikäteisenä apuvälineenä väärinkäytösten, vahinkojen tai vaurioiden selvittämisessä. Kohteita, joissa valvontaa usein hyödynnetään, ovat esimerkiksi tietoliikennetilat, kehävalvonta ja prosessin kriittiset toimintapisteet.

Kameravalvonnan suunnittelussa on huomioitava yksityisyyden suoja. Mikäli kameran valvontasektori ulottuu julkiselle alueelle, poliisilla on oikeus pyytää tallenteita tehdasalueen ulkopuolella tapahtuneen rikoksen tutkinnan tueksi. Lisäksi on tärkeää erottaa, käytetäänkö kameroita vartiointitarkoituksiin vai prosessinvalvontaan, sillä käyttötarkoitus vaikuttaa sekä tekniseen toteutukseen että lainsäädännöllisiin velvoitteisiin.

4 MODERNIN FYYSISEN TURVALLISUUDEN HAASTEET: DRONET JA VANHENEVA INFRASTRUKTUURI

Monissa vanhemmissa teollisuuslaitoksissa tietoliikenneverkon fyysinen suojaus on rakentunut aikakauden käytäntöjen mukaan, joissa turvallisuus on esimerkiksi perustunut pääosin alueen ulkokehän suojaukseen. Jakamot ovat saattaneet sijaita vapaasti tuotantotiloissa tai teknisissä tiloissa, ja niiden suojauksena on usein ollut vain lasiovellinen kaappirakenne ilman erillisiä kulunvalvonta- tai lukitusjärjestelmiä. Kokonaisuuden turvallisuus on tukeutunut ulkoaitaukseen, kameravalvontaan, vartiointikierroksiin sekä yleiseen aluevalvontaan, ei niinkään yksittäisten kohteiden suojaukseen.

Ajan saatossa monien teollisuuslaitosten kehäsuojaus on heikentynyt, mikä on lisännyt fyysisen turvallisuuden riskejä. Alun perin riittäväksi koettu ulkoinen aitaus saattaa nykytilanteessa olla fyysisesti kulunut, osittain vaurioitunut tai teknisesti vanhentunut niin, ettei se enää muodosta todellista estettä luvattomalle pääsylle. Teollisuuslaitoksen ulkopuolinen infrastruktuuri on voinut kehittyä sellaiseksi, että se mahdollistaa ulkoaitauksen ohittamisen helposti, esimerkiksi rakennuksen kattoa hyväksi käyttäen. Tehdasalueella voi liikkua erilaisia ulkopuolisia toimijoita, kuten kuljetus- ja logistiikkahenkilöstöä, siivouspalveluiden työntekijöitä tai huoltohenkilökuntaa. Vaikka heidän läsnäolonsa on osa normaalia toimintaa, voivat he samalla aiheuttaa riskejä sekä fyysisen turvallisuuden että tietoturvan näkökulmasta.

Lisäksi uudet uhkakuvat kuten dronejen käyttö tiedustelu- tai vaikuttamistoiminnassa eivät ole olleet turvallisuussuunnittelun lähtökohtina aiemmissa rakenteissa.

Monissa vanhoissa tuotantotiloissa alkuperäinen sähkövalaistus on ollut tehotonta, minkä vuoksi ikkunoita on hyödynnetty luonnonvalon lähteenä. Vaikka tämä on ollut toimiva ratkaisu valaistuksen kannalta, avoimien tai suurten ikkunoiden kautta syntyy myös uusia riskejä erityisesti nykyaikaisten dronejen aikakaudella.

Yksittäiselläkin kevyellä dronella voidaan nykyään kerätä visuaalista tietoa laitosalueen rakenteista, infrastruktuurista ja toimintatavoista. Tämä voi sisältää esimerkiksi kaapeloinnin reittejä, laitepositioita, laitemalleja tai kytkentätietoja, mikäli jakamot ja tekniset tilat ovat näkyvillä tai niihin on rajoittamaton näkö- tai lentoyhteys. Tällaiset uhat korostavat visuaalisen suojauksen ja paikallisen fyysisen suojan merkitystä kaikilla suunnittelualoilla. Dronella on helppo kerätä monenlaista tietoa laitosalueen haavoittuvuuksista aina fyysisestä suojauksesta ihmisten toimintatapoihin.

Droneen voidaan liittää monenlaista lisätekniikkaa, kuten kameroita, mittaamiseen ja seurantaan soveltuvia sensoreita, työkaluja tai langattoman viestinnän häirintävälineistöä, mikä mahdollistaa niiden käytön sekä passiiviseen havainnointiin että aktiiviseen vaikuttamiseen. Langattomien tekniikoiden yleistyminen lisää myös tietoliikenneverkon turvallisuushaasteita, sillä droneja voidaan käyttää sekä tiedonkeruuseen että langattomien yhteyksien häirintään tai tietoliikenteen monitorointiin. Niiden avulla on mahdollista helposti jättää laitteisto kohdealueelle esimerkiksi langattoman häirinnän tai tiedonkeruun jatkamiseksi ilman ihmisen läsnäoloa, mikä tekee uhasta vaikeasti havaittavan ja torjuttavan. Yksittäisen dronen kantama hyötykuorma voi olla niin suuri, että sillä voidaan kuljettaa myös tuhovoimaisia sotilasräjähteitä.

Ukrainan sodan myötä droneteknologian kehitys on kiihtynyt merkittävästi. Konfliktissa droneja on hyödynnetty ennennäkemättömän laajasti tiedustelussa, täsmäiskujen toteutuksessa ja logistisissa

tehtävissä, mikä on vauhdittanut teknologista murrosta myös siviilikäytön näkökulmasta. Kehityksessä on nähty uusina suuntauksina valokuitukaapelilla ohjattujen FPV-dronejen käyttö erityisesti elektronista torjuntaa vastaan, sekä autonomisten vesidronejen kehitys. Nopeasti kasvaneet kyvykkyydet, saatavuus ja soveltamisen monipuolistuminen tekevät droneista yhä merkittävämmän potentiaalisen uhkatekijän myös tietyissä teollisuusympäristöissä.

5 POHDINTA

Opinnäytetyön aikaisen projektin aikana opittiin runsaasti uutta osaamista, erityisesti eri suunnitteluohjelmista, viestinnästä ja yleisesti projektityöskentelystä. Projektin aikana opittiin tarkastelemaan asennustyötä suunnittelijan näkökulmasta ja tuomaan siihen mukaan käytännönläheisiä näkemyksiä, joita pelkkä teoreettinen tietopohja ei olisi mahdollistanut. Vastaavasti suunnittelutyön kautta saatiin uusia oivalluksia myös itse asennusprosessin kehittämiseen ja ymmärtämiseen. Projektin aikana heräsi yllättävä havainto siitä, kuinka vähän mikrokanavatekniikka on tunnettu suurtenkin teollisuuden toimijoiden keskuudessa.

Tällä hetkellä mikrokanavatekniikka on edelleen pääosin teleoperaattoritoimijoiden käyttämä verkon toteutustapa, ja sen käyttö on yleisintä laajojen tietoliikenneverkkojen rakentamisessa ja ylläpidossa. Tulevaisuudessa tullaan selvittämään tarkemmin mikrokanavatekniikan laajemman käytön mahdollisuuksia teollisuuden tietoliikenneinfrastruktuurin tukemisessa, vaihtoehtona tai täydentävänä ratkaisuna perinteiselle valokuitutekniikalle. Tämä avaa uusia näkökulmia teollisten verkkojen kehittämiseen, erityisesti tilanteissa, joissa tarvitaan muuntojoustavuutta, tiheämpää kaapelointia tai nopeaa käyttöönottoa. Laajempi käyttöönotto edellyttää kuitenkin lisää tutkimusta, esimerkkikohteita ja tiedon jakamista tekniikan eduista eri toimialoille.

Projektin yhteydessä kiinnitettiin huomiota myös fyysisen turvallisuuden merkitykseen osana tietoliikenneverkon kokonaisvaltaista suunnittelua. Havaittiin, että monissa vanhoissa teollisuuslaitoksissa fyysinen turvallisuus ja verkon yksittäisten komponenttien, kuten jakamoiden, suojaus perustuu yhä pitkälti perinteisiin keinoihin – esimerkiksi kehävalvontaan, mekaanisiin lukituksiin, vartiointiin ja kameravalvontaan. Vaikka nämä menetelmät tarjoavat perustason suojan, ne eivät aina ole riittäviä nykytilanteessa, jossa teknologian kehittyminen tuo mukanaan uusia uhkia ja hyökkäysvektoreita myös fyysisen infrastruktuurin tasolla.

Fyysisen turvallisuuden huomioiminen kriittisenä osana tietoliikenneverkon suunnittelua on siten entistä tärkeämpää. Uudet teknologiat mahdollistavat entistä hajautetumpia ja hienosyisempiä ratkaisuja, mutta samalla ne voivat altistaa verkon rakenteita ja komponentteja uusille riskeille – erityisesti, jos fyysisestä suojaustasosta tingitään. Suunnitteluvaiheessa tulisi kiinnittää huomiota paitsi verkon tekniseen toimintavarmuuteen, myös siihen, kuinka fyysiset asennuskohteet, jakamot ja muu tekniikka suojataan sekä tahallisilta että tahattomilta vaurioilta. Fyysisen turvallisuuden ja digitaalisen turvallisuuden yhteensovittaminen onkin keskeinen osa modernin teollisen tietoliikenneverkon kokonaisturvallisuutta.

LÄHTEET

Työssä on käytetty tekoälyä seuraavasti: ChatGPT 2025. OpenAI. GPT-3.5. Käytetty kielentarkistukseen, kesäkuu 2025. Lisätietoja kielimallista: https://chat.openai.com