Datadiodin soveltaminen teollisuuden ohjausjärjestelmään

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Teknillinen tiedekunta
Toukokuu 2024
Riikka Kivi

TURUN YLIOPISTO
Tietotekniikan laitos

Riikka Kivi: Datadiodin soveltaminen teollisuuden ohjausjärjestelmään

TkK-tutkielma, 30 s.
Teknillinen tiedekunta
Toukokuu 2024

Tässä tutkielmassa pohditaan, miten datadiodia voidaan hyödyntää teollisuuden ohjausjärjestelmän tietoturvan parantamiseksi ja millainen datadiodikytkentä sopisi osaksi teollisuuden ohjausjärjestelmää. Tämä saavutetaan tarkastelemalla datadiodin toimintaperiaatetta sekä teollisuuden ohjausjärjestelmän rakennetta Purdue-mallin avulla. Johtopäätöksiin päästään analysoimalla teollisuuden ohjausjärjestelmän tietoturvaongelmia sekä datadiodikytkentää ja sen ominaisuuksia.
Teollisuuden ohjausjärjestelmät ovat moniosaisia järjestelmiä, jotka varmistavat kriittisen infrastruktuurin jatkuvan toiminnan. Häiriö niissä voi johtaa mittaviin vahinkoihin, esimerkiksi taloudellisiin tappioihin, ympäristövahinkoihin ja onnettomuuksiin. Silti niihin kohdistuu monia erilaisia hyökkäysvektoreita. Teollisuuden ohjausjärjestelmän valvomo-ohjelmistot voivat käyttää kommunikaatioprotokollia, jotka eivät tue autentikointia, mikä mahdollistaa haitallisen etäkoodin suorittamisen tai väärän tiedon syöttämiseen järjestelmään. Lisäksi niissä ei ole tarpeeksi laskentatehoa, jotta niihin voitaisiin asentaa tarpeellisia kryptografisia salausalgoritmeja. Järjestelmät voivat olla avoinna myös haittaohjelmille ja palvelunestohyökkäyksille. Datadiodi on fyysinen tietoturvalaite, joka rajaa tietoliikenteen yksisuuntaiseksi haluttuun suuntaan lähettävän ja vastaanottavan laitteen välille. Samalla se estää tietoliikenteen vastakkaiseen suuntaan. Tutkielman lopputuloksena havaitaan, että erilaisiin teollisuuden ohjausjärjestelmän tietoturvauhkiin voidaan vastata nykyisten ratkaisujen lisäksi kytkemällä kriittiseen tietoliikenteeseen lisätekniseksi tietoturvalaitteeksi palomuurilla varustettu datadiodi. Kustannustehokas kytkentä tarjoaa ratkaisuja autentikoinnin puutteeseen ja reagoi ohjelmistopohjaisiin uhkiin nykyisiä ratkaisuja tehokkaammin.

Asiasanat: datadiodi, teollisuuden ohjausjärjestelmä, Purdue-malli

Sisällys

Kuvat

Taulukot

1 Johdanto

Teollisuuden ohjausjärjestelmät (engl. Industrial Control Systems, ICS) ovat keskeinen osa kriittisen infrastruktuurin jatkuvaa toimintaa. Niillä valvotaan ja ohjataan tärkeitä prosesseja, kuten sähköntuotantoa, öljynjalostusta ja vedenjakelua [1]. Tällaisten teollisten ja kriittisten prosessien häiriintymisellä voi olla mittavia seurauksia, kuten taloudellisia tappioita, turvallisuusriskejä ja onnettomuuksia [2]. Teollisuuden ohjausjärjestelmät koostuvat monista osajärjestelmistä ja komponenteista, joten koko järjestelmä vaatii tarkasti suunniteltuja tietoturvatoimia toimiakseen kunnolla. Teollisuuden ohjausjärjestelmän viiterakennetta kuvaava Purdue-malli [3] auttaa hahmottamaan koko järjestelmää hierarkkisin tasoin. Vaikka mallin avulla pystytään suunnittelemaan tasoihin tietoturvatoimia, on tällä hetkellä teollisuuden ohjausjärjestelmissä silti monia tietoturvapuutteita.

Esimerkiksi Ukrainan voimaverkkoon kohdennettiin vuosina 2015 [4] ja 2016 [5] kyberhyökkäykset, joiden seurauksina oli tuhansiin ihmisiin vaikuttavia mittavia sähkökatkoksia. Molemmat iskut herättivät laajaa kansainvälistä huomiota teollisuuden ohjausjärjestelmien haavoittuvuuksista Ukrainassa ja kriittisen infrastruktuurin turvallisuudesta. Toinen kriittiseen infrastruktuuriin kohdistunut haittaohjelmaisku ”WannaCry” [6] levisi nopeasti vuonna 2017 ja käytännössä lamautti Iso-Britanniassa terveydenhuollon toiminnan useiksi päiviksi salaamalla tärkeitä potilastietoja ja vaatimalla salauksien purkamiseksi lunnaita.

Datadiodia on esitetty käytettäväksi turvalliseen tiedonsiirtoon erilaisille kriitti-

sille järjestelmille, jotta tulevaisuudessa voitaisiin välttyä vastaavilta hyökkäyksiltä. Datadiodi on kustannustehokas ja fyysinen tietoturvalaite, jonka avulla tietoliikenne voidaan rajata yksisuuntaiseksi ja samalla estää tietoliikenne päinvastaiseen suuntaan. Tässä tutkielmassa tarkastellaan, sopisiko datadiodi kriittisen tietoliikenteen yhdyskäytäväratkaisuksi teollisuuden ohjausjärjestelmään. Aihe on tärkeä, sillä teollisuuden ohjausjärjestelmien tiedonsiirron tietoturvallisuus liittyy suoraan kriittisen infrastruktuurin toiminnan jatkuvuuteen. Tarkastelun keskiössä on erityisesti yksi teollisuuden ohjausjärjestelmän osajärjestelmä, joka keskittyy valvontaan ja tiedonkeräämiseen [2]. Valvomo-ohjelmistolla (engl. Supervisory Control and Data Acquisition, SCADA) on usein paljon hyökkäyspinta-alaa puutteellisen tietoturvasuunnittelun takia.

Tutkielman tavoitteena on vastata kahteen tutkimuskysymykseen. Kysymykset ovat induktiivisia, eli tarkasteltaviin kohteisiin perehtymällä pyritään luomaan yleispäteviä teorioita tai paljastamaan yllättäviä tai odottamattomia yhteyksiä ilmiöiden välillä [7]. Tutkimuskysymyksiä merkitään lyhenteillä TK1 ja TK2.

TK1: Miten datadiodia voidaan hyödyntää teollisuuden ohjausjärjestelmän tietoturvan parantamiseksi?

TK2: Millainen datadiodikytkentä sopisi osaksi teollisuuden ohjausjärjestelmää?

Tämän tutkielman kannalta tutkimuskysymykset ovat työkaluja, joiden avulla voidaan yhdistellä olemassa olevaa kirjallisuutta ja muodostaa uusia johtopäätöksiä. Tutkielma on toteutettu integroivana kirjallisuuskatsauksena, eli tavoitteena on perehtyä kirjallisuuteen tietyltä aihealueelta, yhdistellä aineistojen teemoja ja muodostaa syvällisempi käsitys aiheesta uusien näkökulmien avulla [8].

Tiedonhaku kirjallisuuskatsausta varten on suoritettu IEEE Xplore -tietokannan avulla. Ensimmäisellä hakulausekkeella haettiin tietoa ainoastaan datadiodista yksisuuntaisena yhdyskäytävänä käyttämällä termejä ”data diode”, ”unidirectional ga-

teway" ja "unidirectional network". Julkaisuvuosiksi rajattiin vuodet 2014–2024. Lisäksi valittiin vain suomen- tai englanninkielisiä aineistoja. Tästä kirjallisuudesta rajattiin oleellisimmat aineistot lukemalla jokainen otsikko ja abstrakti. Rajatut aineistot luettiin kokonaisuudessaan. Tiedonhaun yhteydessä tuli esiin, että datadiodi on melko harvinainen käsite tieteellisissä julkaisuissa. Muokkaamalla hakulause muotoon *"data diode" AND ("ICS" OR "SCADA")* eli yhdistämällä hakulausekkeeseen teollisuuden ohjausjärjestelmät, hakutuloksia tuli vielä vähemmän. Tulokset olivat myös osittain samoja kuin datadiodin tiedonhaussa. Tämän perusteella teollisuuden ohjausjärjestelmiä koskevat aineistot haettiin omalla hakulausekkeellaan *("ICS" OR "SCADA") AND "security policy"*. Valittujen tutkimusten lähdeluetteloita hyödynnettiin aineiston keräämisessä. Tämän kirjallisuuskatsauksen päälähteet on jaoiteltu aihepiireittäin taulukkoon 4.1.

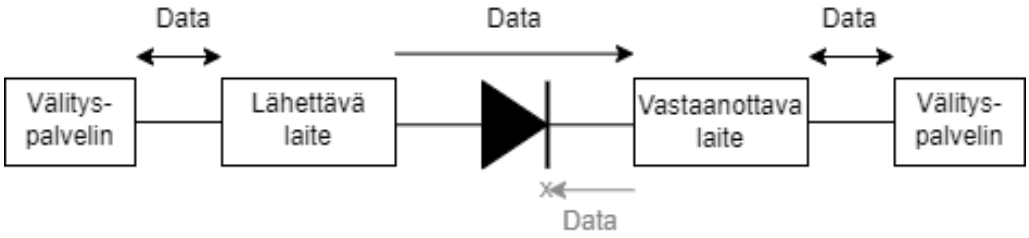
Tässä tutkielmassa on viisi lukua. Ensimmäinen luku on johdanto, jossa johdatellaan lukija aiheeseen ja tutkielman rakenteeseen. Toisessa luvussa perehdytään datadiodin ominaisuuksiin ja toimintaperiaatteeseen. Kolmannessa luvussa tarkastellaan teollisuuden ohjausjärjestelmän rakennetta ja tietoturvaongelmia. Pohdinta-luvussa pohditaan tutkimuskysymysten kautta datadiodin soveltamista teollisuuden ohjausjärjestelmään. Lopuksi yhteenvetoluvussa vastataan vielä kokoavasti tutkimuskysymyksiin ja esitellään jatkotutkimusideoita aiheesta.

2 Datadiodi

2.1 Toimintaperiaate

Datadiodi (engl. data diode) on fyysinen tietoturvalaite tai -järjestelmä, joka mahdollistaa tiedonsiirron kahden järjestelmän tai kahden eri turvaluokitellun verkon välillä yksisuuntaisesti [1]. Datadiodi toimii samalla periaatteella kuin elektroniikan komponentti diodi, joka päästää lävitseen sähkövirtaa vain yhteen suuntaan. Kun datadiodi kytketään kahden järjestelmän välille, se päästää lävitseen tietoa vain tulosta lähtöön. Usein datadiodista puhutaankin yksisuuntaisena yhdyskäytävänä (engl. unidirectional gateway). Tyypillinen datadiodi-implementaatio toteutetaan kytkemällä valokuitu kahden verkon välille, jolloin tieto kulkee valona vain tiettyyn suuntaan [2]. Tällöin tiedon on mahdotonta kulkea päinvastaiseen suuntaan.

Datadiodikytkennässä toinen laitteista on lähettävä ja toinen vastaanottava. Mikäli käytetään yhteysorientoitunutta tiedonsiirtoprotokollaa, molemmissa laitteissa on omat välityspalvelimensa (engl. proxy server). [1] Ne muokkaavat datadiodin läpikulkevaa tietoa omiin kommunikaatioprotokolliinsa ja takaisin. Nämä välityspalvelimet ovat tärkeä osa kytkentää, koska datadiodi yksisuuntaisena yhdyskäytävänä ei tue kaksisuuntaista kommunikaatiota. Välityspalvelimet tekevät ohjelmistotasoisia ratkaisuja, jotta kaksisuuntaiset protokollat kyetään muokkaamaan yksisuuntaisiksi ja vastakkaisesti. [9] Välityspalvelimet toimivat täten omina yhdyskäytävinään laitteille ja laitteiden välisille verkoille.



Kuva 2.1: Yksinkertainen datadiodikytkentä

2.2 Ohjelmistotasoiset ratkaisut

Yleensä datadiodista puhuttaessa tarkoitetaan sellaisia yksisuuntaisia yhdyskäytäväratkaisuja, joissa tietoa liikennöidään OSI-mallin alimmalla kerroksella eli fyysisellä tasolla [9]. Moni kaupallinen datadiodi käyttää Ethernet-tekniikkaa, ja niissä on jopa 10 Gbsp kaistanleveys [1].

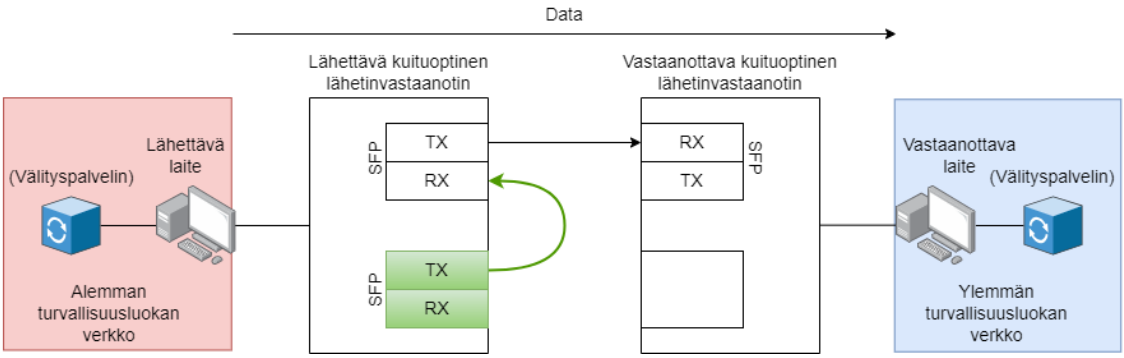
Datadiodi rajaa tiedon liikennöinnin yksisuuntaiseksi, mikä teettää ongelmia datadiodia kytkettäessä osaksi laajempaa tietoliikennettä. Kuljetuskerroksen eli OSI-mallin neljännen kerroksen TCP- ja UDP-protokollat edellyttävät mahdollisuutta kaksisuuntaiseen kommunikaatioon. Tiedonsiirrossa data pilkotaan pienempiin yksiköihin, joita kutsutaan paketeiksi. Jokainen paketti sisältää osan siirrettävästä datasta sekä metadataa, joka auttaa pakettien kuljettamisessa ja kokoamisessa perille saapuessaan. TCP (engl. Transmission Control Protocol) olisi luotettavampi ja eheämpi protokolla ICS-järjestelmille tiedonsiirtoon, kuin matkalla mahdollisesti paketteja hukkaava UDP (engl. User Datagram Protocol) [1]. Toisaalta kättelyä (engl. handshake) käyttävä TCP on hitaampi, kuin UDP, joka ei vaadi vahvistusta vastaanottajalta [1]. Vaikka molemmat protokollat vaativat mahdollisuutta kaksisuuntaiseen kommunikaatioon, soveltuu UDP silti datadiodin käyttöön. TCP on yhteysorientoitunut protokolla, eli se vaatii jatkuvasti yhteyttä ja yhteyden ylläpitoa kommunikaatiokumppaneihinsa [10]. UDP soveltuu yksisuuntaisille yhteyksille, sillä se on yhteydetön protokolla, eikä se edellytä yhteyden jatkuvaa muodostamista kommunikoiviin laitteisiin [11].

Useimmiten datadiodin yhteydessä on siten UDP-protokolla, koska sitä voi käyttää ilman ylimääräisiä ohjelmistotasoisia ratkaisuja. UDP ei silti sovellu kaikkeen ICS-järjestelmien tiedonsiirtoon, koska se voi olla epäluotettava. [1] Joskus nopea mutta puutteellinen tiedonsiirto on silti parempi ratkaisu. Esimerkiksi videokuvaa siirrettäessä on tärkeämpää, että ääni tulee kuvan mukana reaaliajassa, vaikka kuva olisi pikselöitynyttä.

2.3 Kytkentä

Yksinkertaisin datadiodi koostuu kolmesta osasta: lähettävä laite, vastaanottava laite ja laitteet yhdistävä kaapeli tai optinen kuitu. Tässä kirjallisuuskatsauksessa käytetyissä aineistoissa esitetään usein Stevensin vuonna 1999 toteuttama datadiodikytkentä [12]. Kytkentä toteutetaan kahden tietokoneen välille, joista toinen on lähettävä laite, ja toinen on vastaanottava. Tietokoneiden välillä on kaksi kytkiminä toimivaa kuituoptista lähetinvastaanotinta (engl. fibre optic transceiver) sarjaan kytkettynä, ja lähettävän laitteen puolella toisen kytkimen rinnalla on kolmas kuituoptinen lähetinvastaanotin. Kytkimien ja tietokoneiden välillä on tavallista kuparijohtoa. [12] Käytetään selvyyden vuoksi lähettävästä portista lyhennettä TX (engl. Transmit) ja vastaanottavasta RX (engl. Receive) [1]. Lähettävään laitteeseen kytketyn kytkimen TX-portista lähtee optinen kuitu vastaanottavan kytkimen RX-porttiin. Kolmannen kytkimen TX-portista lähtee optinen kuitu lähettävään laitteeseen kytketyn kytkimen RX-porttiin. Kolmannen kytkimen ideana on tuottaa paluu- eli ohjaussignaali lähettävään kytkimeen. [12] Stevensin kytkentä havainnollistaa, kuinka yhdeltä laitteelta voidaan yksinkertaisten ja ”hyllytavarana” löytyvien komponenttien avulla siirtää tietoa turvallisesti vain yhteen suuntaan.

Stevensin kytkentä voidaan rakentaa myös ilman kolmatta kytkintä. Ohjaussignaalia ei silloin ole käytössä. [12] Kuva 2.2 havainnollistaa molempia kytkentöjä: jättämällä kuvassa näkyvän vihreällä merkityn osan pois tarkastelusta, nähdään



Kuva 2.2: Stevensin kytkennän topologia

kytkentä ilman ohjaussignaalin lähettämistä.

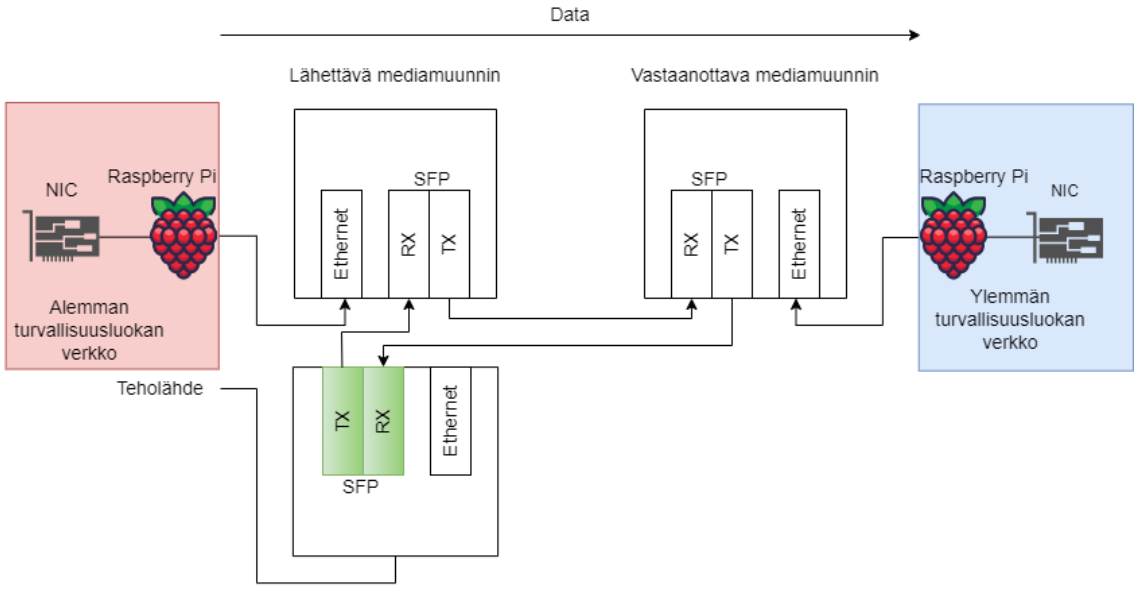
2.4 Kustannukset

Vaikka datadiodikytkentä itsessään ei koostu monesta komponentista, voivat datadiodin hankintakustannukset olla ongelmallisia. Vaikka datadiodeja on käytetty teollisuuden ohjausjärjestelmien tiedonsiirrossa jo vuodesta 2010, maksavat sertifioidut kaupalliset datadiodit silti $30 000 – $150 000 [13]. Kaupallisia datadiodeja löytyy myös alhaisemmilla hinnoilla, mutta niiltä saattaa puuttua hallituksen hyväksyntä tai sertifikaatti, joka saattaa olla tiettyä käyttökohdetta varten pakollinen. Toisaalta monella kaupallisella datadiodilla löytyy useita sertifikaatteja, joten ne ovat aika muokkaantuvia useisiin käyttökohteisiin myös lainsäädännöllisesti. [1]

Jotkin kyberturvallisuusammattilaiset mieltävät halvemmat ja/tai ei-kaupalliset datadiodit haavoittuviksi ja epäluotettaviksi [14]. Toisaalta moni alan ammattilainen on esittänyt omaa datadiodikytkentäänsä tieteellisissä artikkeleissaan turvaamaan kriittisiä järjestelmiä, kuten ICS- [1] ja PACS-järjestelmiä [15] haittaohjelmilta, aurinkosähköjärjestelmien hyökkäyspintaa [13] ja älykkäitä sähköverkkoja väärän tiedo syöttämiseltä [16].

Aliluvussa 2.3 esitetystä Stevensin kytkennästä huomataan, että datadiodikyt-

kennän rakentaminen ei vaadi harvinaisten tai monien komponenttien hankkimista, erityisesti jos laitteistoa löytyy jo omasta takaa. Lähettävänä- ja vastaanottavana laitteina voidaan käyttää tietokoneita, jotka tukevat tiedostojen siirtoa halutulla protokollalla. Tarvittaessa tietokoneisiin kytketään tarvittavat välityspalvelimet. Tietokoneet voidaan myös korvata esimerkiksi Raspberry Pi -piirilevyllä [9] ja verkkokorteilla (engl. Network Interface Card, NIC), mikä on selvästi tietokoneiden käyttöä edullisempaa. Tietokoneiden ja kytkimien välille tarvitaan kuparikaapelia, esim. CAT6- tai jotain muuta Ethernet-kaapelia. Kytkiminä toimivat lähetinvastaanottimet tarvitsevat kompaktit lähetinvastaanottimet (engl. Small Form-factor Pluggable, SFP), jotka vastaanottavat optisen kuidun kytkimiin. Kytkiminä voidaan käyttää myös mediamuuntimia, mutta nekin tarvitsevat SFP:t [9]. Kuva 2.3 mallintaa Stevensin datadiodikytkentää mediamuuntimien ja Raspberry Pi -piirilevyjen avulla.



Kuva 2.3: Vaihtoehtoinen kytkentä Raspberry Pi -piirilevyjen ja mediamuuntimien avulla

Käytännössä datadiodin rakentaminen on edullista, mikäli tarvittavaa laitteistoa on jo jonkun verran olemassa. Tarkastelemalla datadiodin rakentamiseen tar-

vittavien yksittäisten komponenttien kappalehintoja, huomataan datadiodin olevan melko edullinen tietoturvaratkaisu tiedonsiirtoprosessiin. Kaikki tarvittavat komponentit ovat saatavissa Verkkokauppa.com:ssa 2.5.2024. Verkkokaupan vaihtoehdoista valittiin edullisimmat, ja ne ovat listattuna taulukossa 2.1. Nopeampi ja tehokkaampi tiedonsiirto vaatisi joitain kalliimpia komponentteja, mutta listauksen ideana on osoittaa, että datadiodin rakentaminen on edullista.

Taulukko 2.1: Datadiodin rakentamiseen tarvittavien komponenttien hintatiedot

Komponentti	Edullisin	Hinta	Määrä
Raspberry Pi -piirilevy	Raspberry Pi Zero 2W	29,99 €	2
Verkkokortti	TP-LINK TL-WN781ND	11,99 €	2
SFP, FS.com 2.5.2024	SFP-1.25G-LX10	9,92 €	3
Mediamuunnin	TP-Link MC220L	25,99 €	2-3
Kuparikaapeli	CAT6, 1 m	4,99 €	2
Valokuitukaapeli	InLine LC-SC, 50/125, 1m	10,99 €	3

Tätä tutkielmaa varten ei ole rakennettu konkreettista datadiodia, mutta tässä tutkielmassa esitetään kirjallisuuskatsauksen aineistojen avulla topologioita, joiden mukaan datadiodin voi rakentaa. Taulukossa 2.1 esitettyjen komponenttien mukaista kytkentää ei ole toteutettu reaalimaailmassa. Toimivan datadiodin rakentamiseksi on suositeltavaa käyttää sellaisia komponentteja, jotka on suunniteltu ja testattu tällaista käyttöä varten.

3 Teollisuuden ohjausjärjestelmä

3.1 Turvallisuusluokat ja pääsynhallinta

Turvallisuusluokkia käytetään laajasti eri aloilla ja järjestelmissä suojaamaan tietoja ja varmistamaan niiden saatavuus, luottamuksellisuus ja eheys. Turvallisuusluokat ovat kansainvälinen tapa luokitella eri turvallisuustasojen tietoja. Suomen valtioneuvosto on määritellyt asetuksessaan 28.11.2019/1101 [17], että turvallisuusluokista käytetään merkintöjä ”TL I”, ”TL II”, ”TL III” ja ”TL IV”. Turvallisuusluokista on olemassa myös vastaavat kansainväliset ja NATO:n nimikkeet.

Taulukko 3.1: Turvallisuusluokkien selitykset, *suluissa NATO:n etuliite

Lyhenne	Merkintä asiakirjaan	Nimike kansainvälisesti*
TL I	ERITTÄIN SALAINEN	(COSMIC) Top Secret
TL II	SALAINEN	(NATO) Secret
TL III	LUOTTAMUKSELLINEN	(NATO) Confidential
TL IV	KÄYTTÖ RAJOITETTU	(NATO) Restricted

Teollisuuden ohjausjärjestelmissä turvallisuusluokat ovat keskeisessä roolissa tietojen ja operatiivisten prosessien suojaamisessa. Niiden avulla varmistetaan, että vain hyväksytyt käyttäjät pääsevät käsiksi kriittisiin järjestelmiin ja tietoihin. Esimerkiksi teollisuusprosessin valvomisessa voidaan kerätä tietoa, joka on salaista ja siihen on rajattu pääsy. Jokin toinen kerätty tieto voi olla julkisempaa ja rajatun käyttöoikeuden parissa. Kriittiset tiedot ja toiminnot halutaan usein eristää julkisemmasta tiedoista. Silti toimivassa järjestelmässä on siirrettävä tietoa eri turvallisuusluokasta toiseen. Teollisuuden ohjausjärjestelmien kaltaisissa kriittisissä järjes-

telmissä tiedon siirtäminen eri turvallisuusluokkien välillä luotettavasti on tärkeää, koska se vähentää ulkoisia uhkia järjestelmään.

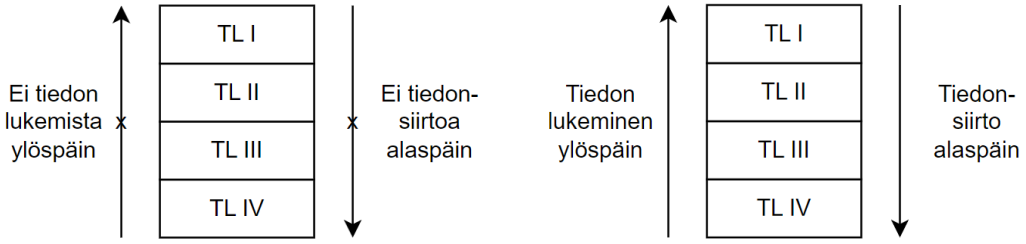
Ulkoministeriön julkaisema Katakri 2020 -kriteeristö [18] on auditointityökalu, jolla viranomainen voi arvioida organisaation tietoturvallisuusjärjestelyjä viranomaisten salassa pidettävien tietojen suojaamisessa. Kriteeristössä määritellään, että tietojenkäsittelyympäristöjen suojattuun yhteenliittämiseen voidaan käyttää yhtenä vaihtoehtona yksisuuntaista yhdyskäytävää, kun tietoa siirretään turvallisuusluokasta IV turvallisuusluokkaan III. Kriteeristön mukaan TL II -ympäristöt on eristettävä toisistaan. TL II -ympäristöjen välillä ja matalammista turvallisuusluokista turvallisuusluokkaan II sallitaan tiedonsiirtoa vain yksisuuntaisten yhdyskäytävien kautta. Datadiodi on siis Katakrin mukaan sopiva ratkaisu tiedonsiirtoon eri turvallisuusluokkien välillä, kun tietoa siirretään matalammista turvallisuusluokista ylempiin turvallisuusluokkiin.

Pääsynhallinta tarkoittaa käyttöoikeuksia hallitsemalla toteutettua kulunvalvontaa, ja pääsynhallinnalle on olemassa erilaisia malleja. Yleinen suunnitteluperiaate turvalliselle yhdyskäytävälle Katakrin [18] mukaan on toteuttaa tiedon luottamuksellisuuteen keskittyvän Bell-LaPadula-pääsynhallintamallin [19] kaksi sääntöä ”No read up” ja ”No write down”. Sääntöjen mukaan yhdyskäytäväratkaisun täytyy estää tiedon lukeminen ja käyttäminen käyttäjää itseään ylempien turvallisuusluokkien ympäristöistä sekä estää tiedonsiirto ylemmistä turvallisuusluokista matalampiin turvallisuusluokkiin.

Aiemmin datadiodeja on käytetty tiedonsiirron yhdyskäytävänä lähinnä noudattaen Bell-LaPadula-mallia, kun datadiodit ovat tehneet niin kutsuttujen ilmavälien (engl. air gap) työtä [9]. Datadiodille on olemassa toinenkin keskeinen pääsynhallintamalli, joka keskittyy tiedon eheyden säilyttämiseen. Jos tietoa halutaan siirtää ylemmistä turvallisuusluokista matalampiin turvallisuusluokkiin ja käyttäjä haluaa lukea tietoa ylemmistä turvallisuusluokista, on Biba-pääsynhallintamalli [20] sopiva.

Biba-malli on päinvastainen Bell-LaPadula-mallille, eli sen mukainen yhdyskäytävä toteuttaa säännöt ”Read up” ja ”Write down”.

Käytännössä Bell-LaPadula-mallin mukaista tiedonsiirtoa on esimerkiksi turvapäivitysten tuonti [18], sähköpostin välitys, sensori- ja hälytystietojen tuonti alemman turvallisuusluokan ympäristöstä ylempään. Biba-mallin toteuttavaa tiedonsiirtoa on esimerkiksi tilannekuvajärjestelmistä paikkatietojen tuonti ylemmän turvallisuusluokan ympäristöstä alempaan [21].



(a) Bell-LaPadula-malli (b) Biba-malli

Kuva 3.1: Pääsynhallintamallit

Pääsynhallinta ja tiedonsiirto turvallisuusluokkien välillä liittyvät merkityksellisesti toisiinsa, kun puhutaan datadiodin käyttökohteista. Mikäli datadiodi kytketään osaksi teollisuuden ohjausjärjestelmää, oikein valittu pääsynhallintamalli takaa tiedon siirron turvallisesti ja luotettavasti järjestelmän sisällä. Sen myötä vain tietyt hyväksytyt käyttäjät pääsevät näkemään ja käyttämään tiettyä turvallisuusluokiteltua tietoa, eikä tieto joudu vääriin käsiin.

3.2 Viiterakenne Purdue-mallin avulla

Teollisuuden ohjausjärjestelmä on kattonimi useista komponenteista ja laitteista koostuvalle tietojärjestelmälle, jolla hallitaan ja valvotaan teollisia prosesseja. Komponentteina voi olla muun muassa yhteen kytkettynä erilaisia antureita, ohjelmistoja ja tietokonepäätteitä. Erilaisia teollisuuden ohjausjärjestelmän osajärjestelmiä ovat

muun muassa valvontaan ja tiedonkeräämiseen keskittyvät Valvomo- eli SCADA-ohjelmistot, ohjelmoitavat logiikkaohjaimet (engl. Programmable Logic Controller, PLC) ja hajautetut ohjausjärjestelmät (engl. Distributed Control System, DCS). [22] Purdue-mallin 3.2 avulla pystytään tarkastelemaan osajärjestelmien ja komponenttien sijoittumista koko teollisuuden ohjausjärjestelmän rakenteeseen.

Teollisuuden ohjausjärjestelmille ei ole olemassa yleisesti hyväksyttyä standardia, jonka mukaan järjestelmässä luokiteltaisiin tietoa turvallisuusluokkien mukaan. Sen sijaan tietoa turvallisuusluokitellaan yleensä ottaen huomioon järjestelmän toiminnalliset ja tarvittavat tietoturvavaatimukset [18]. Teollisuuden ohjausjärjestelmän tietoturvatoimia voidaan silti suunnitella ANSI/ISA-95-standardin mukaisen Purdue-viitemallin [3] avulla.

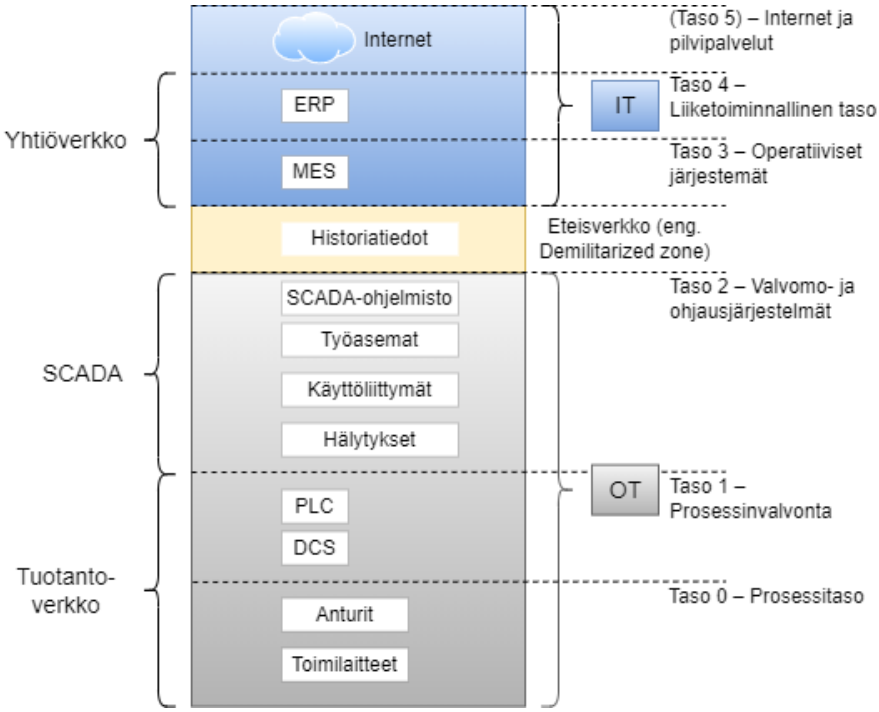
Kansainvälisessä ANSI/ISA-95-standardissa tuotannon kokonaisarkkitehtuurissa integroidaan ohjausjärjestelmät ja organisaatio Purdue-mallin viidelle tasolle [3]. Jako voidaan tehdä

1. prosessiin ja sen erilaisiin ohjaus- ja valvontajärjetelmiin sekä
2. yrityksen operatiivisiin- ja liiketoiminnallisiin järjestelmiin.

Ohjausjärjestelmät toimivat käytännössä tuotantoverkon (engl. Operational Technology Network, OT) kanssa eli sopivien OT-ympäristöjen kanssa [23]. Organisaatioympäristö koostuu erilaisista yhtiöverkon ja ulkoisten pilvipalveluiden muodostamista tietoteknisistä ratkaisuista (Information Technology, IT) eli IT-ympäristöistä [23]. OT-IT-jaottelua tukee myös kansainvälinen IEC 62443 -standardisarja, joka käsittelee teollisuuden ohjausjärjestelmien kyberturvallisuutta määrittämällä eri teknologioille vaatimuksia. Standardin mukaan OT- ja IT-verkot on eristettävä eri turva-alueisiin, jotka yhdistetään sopivalla yhdyskäytävällä [23].

Purdue-viitemalli puolestaan havainnollistaa viiden tason 0–4 avulla organisaation viiterakennetta sekä osajärjestelmien ja komponenttien välistä vuorovaikutusta [3]. Joskus malliin sisällytetään kuudes taso, joka kuvaa internetiä, pilvipalveluita

tai muita ulkoisia tietoverkkoja [24]. Konkreettiseen hierarkkisen järjestyksen avulla on selkeämpää suunnitella tietoturvatoimia.



Kuva 3.2: Organisaation tuotannon rakenne mukaillen ANSI/ISA-95-standardia ja Purdue-mallia

Alimmainen taso eli 0-taso kuvaa käytännön prosessia, jota mitataan antureilla ja ohjataan toimilaitteilla. Alimmalla tasolla tapahtuu siis fyysinen prosessi, esimerkiksi tuotantolaitoksessa jokin tuotantoprosessi. Ensimmäinen taso eli 1-taso on prosessinohjausta, ja tällä tasolla on komponentteja, joilla operoidaan ja manipuloidaan prosessitason prosessia. Joskus tätä tasoa nimitetään myös älykkäiden laitteiden tasoksi komponenttiensa luonteen vuoksi. Toisella tasolla eli 2-tasolla on valvomotoimenpiteet, joita yleensä operoi SCADA-järjestelmä. [3] SCADA kerää tietoa kahdelta alemmalta tasolta ja tarjoaa tiedot käyttöliittymien kautta hyväksytyille käyttäjille [25]. Useimmiten historiatiedot tai tietokannat, joissa on prosessin tai yrityksen kannalta merkittävää tietoa, sijaitsevat eteisverkossa (eng. Demilitarized zone, DMZ) [3]. Kolmas taso kattaa laajan valikoiman järjestelmiä ja teknologioita, jotka ovat olennaisia tuotantoprosessin hallinnalle ja optimoinnille. Esimerkiksi

valmistuksen valvonta -järjestelmä (engl. Manufacturing Execution System, MES) seuraa tuotantolaitteiden tilaa ja suorittaa tuotannon aikataulutusta. Neljäs taso eli liiketoiminnallinen taso keskittyy toiminnanohjausjärjestelmien (engl. Enterprise Resource Planning, ERP) avulla hallinnoimaan liiketoiminnan osia ja tuotantoprosesseja. [3] Neljänneltä tasolta ollaan yhteydessä internetiin ja muihin ulkoisiin verkkojärjestelmiin [24].

ANSI/ISA-95-standardin ohjausjärjestelmät ja organisaatio -erottelun muodostamassa jaossa pystytään selkeämmin hahmottamaan teollisuuden ohjausjärjestelmän tietoliikennettä käsiteltyjen pääsynhallintamallien ja turvallisuusluokkien avulla. Jos halutaan siirtää tietoa alemmasta ympäristöstä eli alemman turvallisuusluokan piiristä ylempään ympäristöön, noudatetaan Bell-LaPadula-mallia. Jos tietoa halutaan siirtää alaspäin, on se Biba-mallin mukaista.

Pääsynhallintamallien ja turvallisuusluokkien avulla on selkeää hahmottaa, miten tiedonsiirron suuntaa pystytään kuvaamaan ja millaisia sääntöjä on tiedonkäyttöoikeuksille. Yllä jäsennellyssä jaottelussa tietoliikenteen on kuljettava sopivien tietoturvatoimien- tai laitteiden, kuten palomuurien, läpi. Tässä tutkielmassa tarkastellaan, sopisiko datadiodi yhdeksi tällaiseksi tietoturvalaitteeksi teollisuuden ohjausjärjestelmään.

3.3 Tietoturvaongelmat ja uhkakuvat

Teollisuuden ohjausjärjestelmät rakennetaan tyypillisesti osaksi tuotantoverkkoa (OT network, Operational Technology Network), jossa järjestelmän prosessi ja prosessinohjaus tapahtuvat. Tuotantoverkko voi sisältää muun muassa ihmisen ja koneen välisiä käyttöliittymiä (engl. HMI, Human-Machine Interface) tai teollisuuden ohjausjärjestelmän osajärjestelmiä, kuten valvomo-ohjelmistoja ja hajautettuja ohjelmistojärjestelmiä. [23] Tuotantoverkot on usein eristetty internetistä ja niihin on rajoitettu määrä hyväksyttyjä käyttäjiä. Chan'n ja Zhoun [2] mukaan tuotantoverk-

kojen valvomo-ohjelmistoihin ei ole usein implementoitu yhtään turvamekanismeja, jotka suojaisivat valvomo-ohjelmistoja erilaislta kyberhyökkäyksiltä. Joskin silloin kun ensimmäiset valvomo-ohjelmistot 1960-luvulla on rakennettu, on ajateltu, että eristäytyminen muusta maailmasta riittää turvatoimeksi [2]. Nykypäivänä tuotantoverkkoja on alettu kytkeä koko ajan enemmän osaksi internetiä, pilvipalveluita ja esineiden internetiä (IoT, Internet of Things) [24]. Teollisuuden ohjausjärjestelmien prosessinohjaukseen keskittyneet tuotantoverkot ovat nyt teknologisessa murroksessa, kun integroituminen osaksi tietoteknisiä (Information Technology, IT) ympäristöjä altistaa OT-verkot yhä enemmän uusille tietoturvariskeille. [23]

Teollisuuden ohjausjärjestelmissä hyökkäyspintaa on siis erityisesti valvomo-ohjelmistoissa. Chan'n ja Zhoun [2] mukaan niissä ei usein ole tarpeellisia kryptografisia salausalgoritmeja, joita käytetään salausprotokollien rakentamiseen tietoturvajärjestelmille. Lisäksi valvomo-ohjelmistojen käyttämät kommunikaatioprotokollat ovat vanhentuneita tai haavoittuvia. Valitettavasti vanhemman sukupolven valvomo-ohjelmistoissa ei ole tarpeeksi laskentatehoa, että niihin voitaisiin asentaa tarvittavia salausalgoritmeja. Usein valvomo-ohjelmistojen käyttämät kommunikaatioprotokollat, kuten Modbus, Profibus, IEC60870 ja Sinaut 8FW, eivät vaadi autentikointia eli vahvaa todennusta viestien lähettämiseen. [2] Tämän lisäksi viestit saattavat lähteä salaamatta tai selväkielisenä [22]. Artikkelissaan [25] A. Abou el Kalam luettelee kattavasti yleisiä valvomo-ohjelmistojen haavoittuvuuksia ja uhkakuvia. Näitä ovat yllä mainittujen lisäksi muun muassa tietoturvatietoisuuden puute, järjestelmien puutteelliset turvallisuusratkaisut sekä tuotantoverkon ja käyttöjärjestelmäalustojen puutteelliset konfiguraatiot. Lisäksi ohjelmistot eivät ole koskaan haavoittumattomia, ja laitteiston fyysinen turvallisuus on huomioitava.

Tuotantoverkon haavoittuvuudet altistavat teollisuuden ohjausjärjestelmät monille tietoturvauhille. Ne ovat alttiita palelunestohyökkäyksille ja haittaohjelmille, kuten Stuxnet [1]. Ohjelmistojen ja laitteistojen haavoittuvuuksien myötä Valvomo-

ohjelmistoissa voidaan myös suorittaa haitallista etäkoodia [25] tai syöttää väärää tietoa [2]. Autentikoinnin puute kommunikaatioprotokollissa mahdollistaa luvattoman pääsyn järjestelmään, mikä tekee mahdolliseksi syöttää väärää tietoa prosessiin. Se voi johtaa virheellisiin toimintoihin tai vaarallisiin tilanteisiin fyysisissä prosesseissa. [2] Teollisuuden ohjausjärjestelmän häiriintymisestä voi seurata isoja taloudellisia tappioita muun muassa tuotantolaitosten seisokkien, energianjakelun häiriöiden ja vedenjakelun katkoksien myötä. Näistä saattaa seurata epäsuoria vaikutuksia, kuten häiriöitä liiketoiminnassa ja laitteiden vahingoittumista. Lisäksi teollisuuden ohjausjärjestelmien häiriintymisistä voi seurata erilaisia onnettomuuksia, ympäristövahinkoja ja jopa kuolemia [22].

Monet teollisuuden ohjausjärjestelmän tietoturvaongelmista ovat sellaisia, että niihin varautuminen on monimutkaista. Esimerkiksi haavoittuvista tai vanhentuneista kommunikaatioprotokollista turvallisempiin vaihtaminen on kallista, koska tuotantoverkon koko järjestelmä täytyisi rakentaa liki alusta. Autentikointitietojen sovittamista osaksi valvomo-ohjelmiston kommunikaatioprotokollaa on koetettu, mutta sovittamisessa päädyttiin yhteensopivuusongelmiin [2]. Eräs ratkaisu autentikoinnin saavuttamiseksi olisi kytkeä jokin lisätekninen tietoturvalaite halutun kommunikaatioprotokollan yhteyteen. Tällainen lisätekninen ratkaisu voisi olla esimerkiksi palomuurilla varustettu datadiodikytkentä.

4 Pohdinta

Tässä luvussa pohditaan TK1:n avulla miten datadiodilla voidaan vaikuttaa teollisuuden ohjausjärjestelmän tietoturvallisuuteen. Lopussa yhdistetään käsitellyt asiat TK2:een vastaamiseksi ehdottamalla datadiodikytkentää sovellettavaksi Purdue-malliin. Lisäksi alustetaan jatkotutkimusideoita katsahtamalla nollaluottamusmalliin. Pohdinnan tukena on kirjoitusprosessin ajan ollut taulukko 4.1, joka mallintaa aineistojen jakautumista aihepiireittäin.

4.1 Datadiodi tietoturvalaitteena

Tietoturvalaitteena datadiodin tärkein ominaisuus on yksisuuntaisuus, koska datadiodi on yksisuuntainen yhdyskäytävä. Yksisuuntaisuuden myötä datadiodi soveltuu hyvin yhdyskäytäväksi kriittisen tiedon siirtämiseen, koska tieto kulkee vain haluttuun suuntaan. Samalla eristetään tietoliikenne vastakkaiseen suuntaan. ANSI/ISA-95-standardin mukaista ohjausjärjestelmien ja organisaation jaottelua toisistaan voidaan tarkastella myös OT- ja IT-ympäristöjen välisenä jakona. Teollisuuden ohjausjärjestelmän OT-ympäristöjen parissa toimivaa valvomo-ohjelmistoa on alettu viime vuosina integroimaan internetiin ja monipuolisiin IT-ympäristöihin [24]. Kokonaisrakenteen ylläpitämiseksi on silti tärkeää pitää selvä jako OT- ja IT-ympäristöjen välillä asettamalla ympäristöjen väliin sopiva yhdyskäytäväratkaisu, esimerkiksi usein palomuuri. Koska datadiodi on yksisuuntainen yhdyskäytävä, se voisi olla sopiva ratkaisu OT-IT-sillaksi.

Taulukko 4.1: Aineistojen jakautuminen aihepiireittäin

Tutkimus	Vuosi	Tutkimus-kohde	Tarkoitus kirjallisuuskatsauksen näkökulmasta
Jeon ja Na [1]	2016	Datadiodi	ICS:n turvallisuuden parantaminen datadiodilla; Kaupalliset datadiodit; Datadiodikytkennät tiedonsiirron virheidenhallintaan
Chan ja Zhou [2]	2023	SCADA, Datadiodi	SCADA:n tietoturvaongelmat ja uhkakuvat; Tietoturvalaite-ehdotukset
Knapp ja Langill [3]	2014	Purdue-malli	ANSI/ISA-95 ja Purdue-malli
Almaazmi et al. [9]	2022	Datadiodi	Kokoava kirjallisuuskatsaus olemassa oleviin datadioditutkimuksiin
Stevens [12]	1999	Datadiodi	Datadiodikytkentä
Larkin et al. [13]	2020	Datadiodi	Datadiodin kustannukset aurinkosähköjärjestelmässä
El Hajal et al. [15]	2019	Datadiodi	Datadiodikytkentä PACS-järjestelmässä; Tietoturvauhkia kriittiselle tietoliikenteelle
Mukherjee et al. [16]	2021	Datadiodi	Väärän tiedon syöttäminen; Datadiodikytkentä tiedonsiirron virheidenhallintaan
Bhamare et al. [22]	2020	ICS	ICS:n rakenne ja tietoturvauhat
Ha et al. [23]	2023	Datadiodi, ICS	OT-IT-silta datadiodilla
Sverko et al. [24]	2022	Purdue-malli	ANSI/ISA-95:n ja Purdue-mallin integroituminen ulkoisiin pilvipohjaisiin järjestelmiin
Abou el Kalam [25]	2021	ICS, SCADA	SCADA:n tietoturvahaavoittuvuudet
Obregon [26]	2015	ICS, Purdue-malli	Ohjeistus Purdue-mallin käyttöön ICS:lle
Li et al. [27]	2015	FEC	Virheenkorjauskoodi; Optiset kuidut
Tsai et al. [28]	2024	ZTA	Nollaluottamusmallin implementointi organisaatioon
Syed et al. [29]	2022	ZTA	Kokoava kirjallisuuskatsaus olemassa oleviin nollaluottamusmallitutkimuksiin

Yksisuuntaisen tiedonsiirron myötä datadiodi voisi myös siirtää tietoa nopeammin kuin perinteinen palomuuri, koska palomuuri saattaa hidastaa tiedonsiirtoa tarkastaessaan ja suodattaessaan sitä [9]. Datadiodia käytetään yksisuuntaisuutensa ansiosta päivitysten tuontiin alemman turvallisuusluokan ympäristöstä ylempään [18]. Sen puolesta datadiodi auttaa teollisuuden ohjausjärjestelmää päivittymään ja esimerkiksi palautumaan väärän tiedon syöttämisestä [2]. Lisäksi datadiodeilla ei ole mitää IP- tai MAC-osoitteita, jolloin ne eivät ole jäljitettävissä [16].

Toinen datadiodin tärkeä ominaisuus on sen fyysinen rakenne. Datadiodi on fyy-

sinen laite, joka erottaa kaksi eri turvallisuusluokan laitetta tai verkkoa toisistaan eristämällä tietoliikenteen vain yhteen suuntaan. Eräs käyttökohde datadiodikytkennälle on korvata ilmaväli (engl. air gap) [9]. Aiemmin erityisesti kriittisessä infrastruktuurissa on käytetty ilmaväliä eli kahden eri turvallisuusluokan verkon täydellistä fyysistä erottamista. Tämä on estänyt tietoverkkojen välisen tiedonsiirron. [9] Datadiodinkin tarjoama verkkojen välinen ehdoton erotus tulon ja lähdön välillä varmistaa, että laitteet/verkot eivät koskaan yhdisty, kommunikoi tai vaihda tietoa keskenään.

Laitteen fyysinen rakenne takaa sen, että tiedonsiirtoprosessissa tietoa ei voi muuttaa tai manipuloida järjestelmän ulkopuolelta eli tieto on eheää. Esimerkiksi palomuuri voi toimiessaan ohjelmistopohjaisesti olla alttiina ohjelmistohaavoittuvuuksille ja hyökkäyksille. Toisaalta palomuurilla on muitakin käyttökohteita, kuin vain tiedonsiirto. Tiedon suodattaminen, palveluiden estäminen ja tietoliikenteen valvominen ovat tehtäviä, joita datadiodi ei yksin voi hoitaa [9]. Toisaalta datadiodilla tiedonkäsittelyä on luottamuksellisempaa valvoa, sillä tiedonsiirtoprosessiin pääsee osallistumaan vain hyväksytyt käyttäjät [9]. Lisäksi turvallinen tiedonsiirto vaatii myös ohjelmistotasoisia ratkaisuja. Datadiodi ei yksin estä tiedon muokkaamista tai väärän tiedon syöttämistä, jos hyökkääjä pääsee käsiksi järjestelmään ennen tiedon siirtämistä datadiodin läpi.

Kaiken kaikkiaan datadiodilla on monia hyviä ominaisuuksia, jotta se sopisi tietoturvalaitteeksi kriittiselle tietoliikenteelle. Yksisuuntaisuus ja fyysinen rakenne estää ohjelmistopohjaisiin ratkaisuihin suunnatut haittaohjelmaiskut, ja kaiken lisäksi datadiodikytkentä on edullinen rakentaa.

4.2 Datadiodi teollisuuden ohjausjärjestelmässä

Tarkastelemalla teollisuuden ohjausjärjestelmän tietoturvaongelmia ja uhkakuvia, pystytään pohtimaan, millaisia tietoturvatoimia teollisuuden ohjausjärjestelmä tar-

vitsee. Usein teollisuuden ohjausjärjestelmien valvomo-ohjelmistot on rakennettu puutteellisin tietoturvatoimin. Valvomo-ohjelmistot tarvitsevat siis ulkoisia tietoturvalaitteita, koska niillä ei ole tarpeeksi laskentatehoa autentikointitietojen tai tarpeellisten salausalgoritmien asentamiseksi.

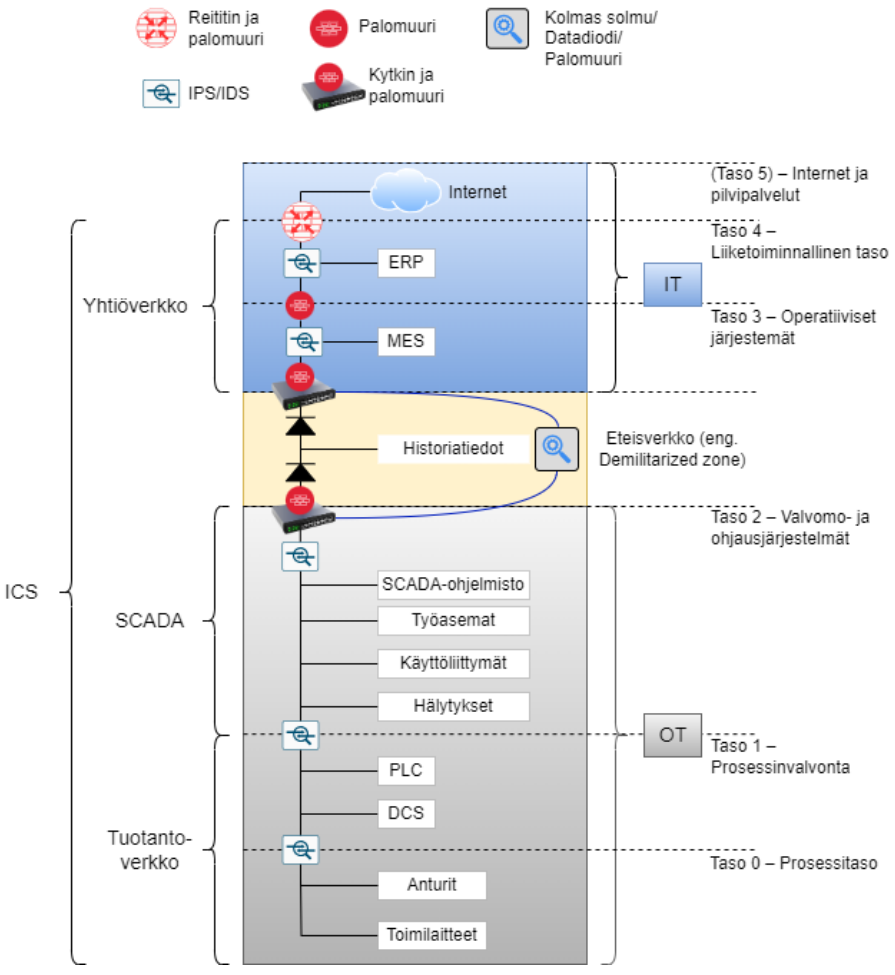
Tähän asti Purdue-mallin mukaisessa teollisuuden ohjausjärjestelmässä on pääsääntöisesti käytetty fyysisiä tai ohjelmistopohjaisia palomuureja tällaisina lisäteknisinä tietoturvalaitteina. Esimerkiksi yksinkertaisessa organisaatiorakenteessa [24] riittää kaksi palomuuria, joista ensimmäinen sijoitetaan yhtiöverkon ja valvomo-ohjelmiston välille. Historiatiedot haetaan toisen palomuurin takaa. Toisessa turvallisemmassa Purdue-mallissa [26] palomuurit asetetaan jokaisen tason väliin, ja jokaisen palomuurin yhteyteen asennetaan tunkeilijan havaitsemisjärjestelmä (engl. Intrusion Detection System, IDS) ja/tai tunkeilijan estojärjestelmä (engl. Intrusion Prevention System, IPS). Lisäksi asioidessa teollisuuden ohjausjärjestelmästä ulkopuolisiin tietoverkkoihin tai internetiin, asennetaan myös reitittimen yhteyteen palomuuri. Reaalimaailman järjestelmässä täytyy ensisijaisesti silti huomioida järjestelmän tietoturvatarpeet, ennen kuin päätetään, mitä kaikkia tietoturvalaitteita järjestelmään implementoidaan.

Tietoturvalaitteena datadiodi sopisi palomuurin rinnalle. Kriittisin yhdyskäytäväratkaisu tarvitaan OT- ja IT-ympäristöjen väliin. Ympäristöt voitaisiin yhdistää datadiodisillalla, joka sijoitettaisiin esimerkiksi OT-ympäristöstä IT-ympäristöön. Kytkentäsuunta valittaisiin sen mukaan, onko tietoliikenne Bell-LaPadula- vai Biba-mallin mukaista. Myös historiatietopalvelin voitaisiin kytkeä siltaan, jolloin kytkentä koostuisi kahdesta datadiodista.

Autentikointitietojen vaatimiseksi datadiodin yhteyteen voidaan asentaa palomuuri. Palomuuri ja autentikointi toimivat usein yhdessä parantaakseen tietoturvaa. Esimerkiksi ennen kuin käyttäjä pääsee verkon resursseihin, palomuuri voi tarkistaa, onko käyttäjä autentikoitu ja valtuutettu pääsemään näihin resursseihin. Toisaalta

datadioditkin tarjoavat jonkin verran roolipohjaista pääsynhallintaa, jossa autentikointia tukee pitkät salasanat [9]. Datadiodilla voidaan siis estää luvaton pääsyn järjestelmään ja varmistaa, että vain hyväksytyt käyttäjät voivat käyttää tietoja.

OT-IT-jaossa halutaan silti kyetä tietoliikenteeseen molempiin suuntiin. Yksinkertainen ratkaisu olisi sijoittaa samanlainen datadiodisilta päinvastaiseen suuntaan OT- ja IT-ympäristöjen välille. Toisaalta ratkaisuksi sopisi myös vaikkapa palomuuri. Tällaisen kytkennän avulla tietoa pystyttäisiin siirtämään Purdue-mallin tasoista molempiin suuntiin.



Kuva 4.1: Purdue-malli ja ehdotettu datadiodikytkentä

Kuvassa 4.1 on tutkielman alussa esitetty organisaation tuotannon rakenne mukaillen ANSI/ISA-95-standardia ja Purdue-mallia, mutta siihen on myös sijoitettu

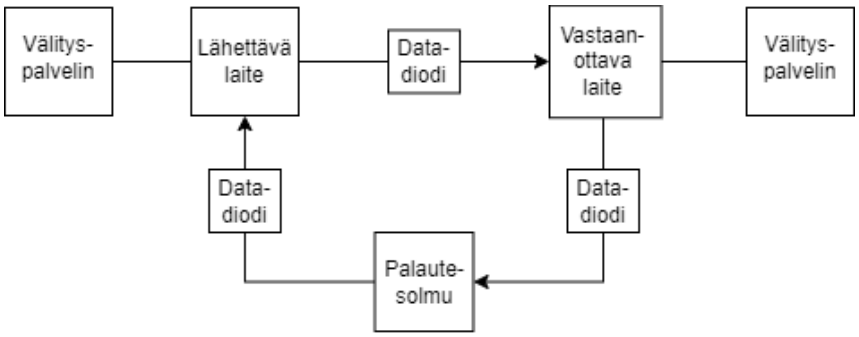
yllä kuvattu datadiodikytkentä. Kuvaan on myös lisätty tarpeellisia ja ehdotettuja tietoturvatoimia onnistuneen tiedonsiirron takaamiseksi. Tarkasteltaessa kuvaan 4.1 sijoitettuja tietoturvalaitteita, huomataan, että kuvassa on datadiodeja, palomuureja, kytkimiä palomuureilla ja reititin palomuurilla. Datadiodikytkentään on otettu inspiraatiota erityisesti Obregonin [26], Ha et al. [23] ja Sverko et al. [24] julkaisuista. Kuvaan sijoitettu kolmas solmu havainnollistaa erilaisia ratkaisuja, jotta tietoliikenne kulkee OT-IT-sillan molempiin suuntiin.

Datadiodia käytettäessä on silti huomioita yksisuuntaisuuden tuomat haasteet. Tiedonsiirrossa olisi käytettävä yhteysorientoitumatonta protokollaa, kuten UDP:tä, jos ei haluta lisätä kytkentään välityspalvelimia. UDP:n haasteena on se, että se saattaa hukata paketteja tiedonsiirtoprosessissa. Toisaalta myös niin kutsutut äänekkäät kanavat (engl. noisy channel) voivat vaikuttaa tiedonsiirron virhemäärään, riippumatta valitusta kommunikaatioprotokollasta. Miten lähettävä laite tai verkko voisi tietää, että kaikki paketit eivät saapuneet vastaanottajalle? Seuraavaksi esitetään ratkaisuja esitetyn datadiodikytkennän rinnalle.

Kolmen solmun arkkitehtuuri

Yksi ratkaisu voisi olla lisätä kytkentään kolmas laite, jonka välityksellä lähettäjälle pystyttäisiin ilmoittamaan tarvittavista siirroista. Nimitetään kytkentään osallistuvia laitteita selvyyden vuoksi solmuiksi. Kolmen solmun arkkitehtuurissa on lähettäjä-, vastaanottaja- ja palautesolmu sekä kolme datadiodia [16]. Jokainen solmu kytketään toisiinsa datadiodilla, jotta tieto kulkee oikeaan suuntaan. Lähettävä solmu lähettää dataa vastaanottavalle solmulle datadiodin läpi. Vastaanottava solmu lähettää dataa palautesolmulle datadiodin läpi. [16] Palautesolmu tarkistaa tiedon eheyden vertaamalla vastaanotetun datan tiivistetietoja, ja välittää tarvittaessa tiedon eheyden tarkistustietoja lähettävälle solmulle. [1] Kolmen solmun arkkitehtuuri yhdessä UDP-protokollan kanssa varmistaisi turvallisen tiedonsiirron, sillä palaute-

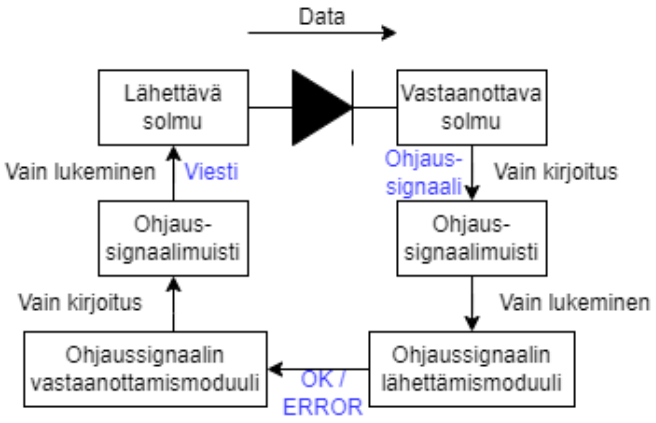
solmu ilmoittaisi, jos osa paketeista katoaisi matkalla. Silloin lähettävä solmu osaisi lähettää paketit uudelleen vastaanottavalle solmulle niin monta kertaa, kunnes kaikki paketit pääsisivät perille. Huonona puolena kytkennässä olisi, että tarvittaisiin kolme datadiodia ja kolme laitetta solmuiksi.



Kuva 4.2: Kolmen solmun arkkitehtuuri

Ohjaussignaalimuistin käyttäminen

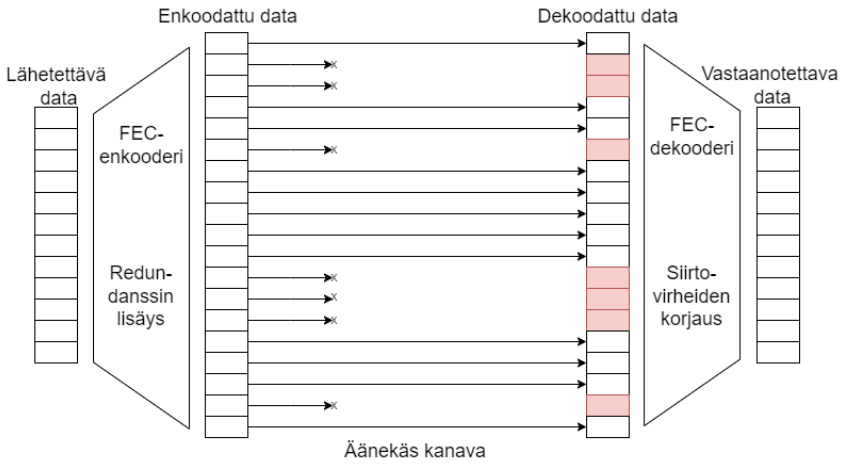
UDP:n aiheittaman pakettien katoamiseen voidaan varautua myös implementoimatta kytkentään kolmatta solmua. Jeon ja Na esittelevät artikkelissaan [1] kytkennän, joka koostuu vain kahdesta solmusta. Solmut viestivät toisilleen ohjaussignaalimuistin (engl. Control Signal Memory) välityksellä, mikäli paketteja puuttuu. Tämä kytkentä käyttää siis kolmen solmun arkkitehtuurin tavoin ohjaussignaalia, mutta on edullisempi, sillä tähän kytkentään tarvitaan ainoastaan yksi datadiodi. Tässä kytkennässä lähettävä solmu lähettää dataa vastaanottavalle solmulle datadiodin läpi. Pieni osa datasta on ohjaussignaalia, joka kirjoitetaan vastaanottavan solmun ohjaussignaalimuistiin. Vastaanottavan solmun ohjaussignaalin lähettämismoduuli lukee ohjaussignaalin sieltä, ja tulkitsee signaalin viestin. Sama lähettämismoduuli lähettää ohjaussignaalin viestin, joko ”OK” tai ”ERROR” lähettävän solmun ohjaussignaalin vastaanottamismoduulille. Tämä moduuli kirjoittaa viestin lähettävän solmun ohjaussignaalimuistiin. Lähettävä solmu lukee viestin sieltä, ja viestin perusteella lähettää paketit tarvittaessa uudestaan vastaanottavalle solmulle.



Kuva 4.3: Kahden solmun arkkitehtuuri käyttämällä ohjaussignaalimuistia

Virheenkorjauskoodin käyttäminen

Kolmas tapa varmistaa onnistunut ja luotettava tiedonsiirto on käyttää virheenkorjauskoodia (engl. Forward Error Correction, FEC). Virheenkorjauskoodia käytettäessä virhetilanteet havaitaan automaattisesti, koska lähetettävään dataan lisätään redundanssia [1]. Vastaanottava solmu kykenee korjaamaan datan dekooderin avulla ilman tarvetta pyytää lähettävää solmua uudelleenlähettämään dataa [1].



Kuva 4.4: Virheenkorjauskoodin toimintaperiaate

Virheenkorjauskoodi osana datadiodikytkentää on edullisempi ratkaisu kuin kolmen solmun arkkitehtuuri, mutta se voi olla myös ohjaussignaalimuistia hyödyntävää kytkentää tehokkaampi. Virheenkorjauskoodi on tarkoitettu erityisesti tiedon-

siirtoon epäluotettavien tai niin kutsuttujen ”äänekkäiden” kanavien (engl. noisy channel) yli [1]. Virheenkorjauskoodin käyttäminen on erityisen tärkeää, kun siirtymisnopeuksia kasvatetaan [27]. Virheenkorjauskoodin kehitystyön alussa se toimi 2,5 Gbps nopeudessa, mutta nykyään tutkijat ovat saavuttaneet jo 400 Gbps nopeuden ja pyrkivät sitäkin suurempaan. Ideaalinen virheenkorjauskoodi toimii yksinkertaisella algoritmilla, sillä on korkea virheenkorjauskerroin ja se skaalautuu oikeassa suhteessa kasvavan tiedonsiirtonopeuden kanssa. [27]

Kaiken kaikkiaan on siis useita tekniikoita, joilla voidaan varautua UDP:n aiheuttamiin haasteisiin. On myös mahdollista käyttää toista protokollaa, kuten TCP:tä, jolloin lähettävään ja vastaanottavaan laitteeseen täytyy vain asentaa välityspalvelimet muokkaamaan yksisuuntaista tietoliikennettä kaksisuuntaiseksi.

4.3 Nollaluottamusmalli Purdue-mallin apuna

Tietoturva-arkkitehtuurin maailmassa Purdue-malli on ollut pitkään vakiintunut viitekehys, joka on tarjonnut hierarkkisen lähestymistavan tietoturvaan. Malli jakaa teollisuuden ohjausjärjestelmän eri tasoihin, jolloin siihen on selkeämpää suunnitella tietoturvaratkaisuja. Nyt kun teollisuuden ohjausjärjestelmät integroituvat koko ajan enemmän internetiin ja ulkoisiin tietoteknisiin ympäristöihin, Purdue-malli ei ehkä ole enää soveltuvin ratkaisu uusien ympäristöjen vaatimuksille.

Nollaluottamusmalli (engl. Zero Trust Architecture, ZTA) on noussut esiin jopa muoti-ilmiön kaltaisena vastauksena nykypäivän tietoturvahaasteisiin. Nollaluottamusmallin mukaan turvallisuutta ei voida enää luottaa vain eri Purdue-mallin tasoihin [28]. Sen sijaan jokainen tiedon pääsyvaatimus on tarkasteltava erikseen ja varmistettava, että sillä on oikeutettu ja turvallinen pääsy yrityksen järjestelmiin ja tietoihin. Purdue-mallille ei ole oikein löytynyt suoraa nykyaikaista seuraajaa, joten nollaluottamusmalli tarjoaa kiinnostavan vaihtoehdon. Se toimii jatkuvan valvonnan avulla ja varmistaa, että kaikki kulunvalvonta ja pääsynhallinta on asianmukaisesti

tunnistettu, valtuutettu ja valvottu. [29] Tämä lähestymistapa mahdollistaa toiminnallisen reagoinnin muuttuviin uhkiin ja ympäristöihin, mikä voi olla tehokkaampaa kuin Purdue-mallin nykyinen muuttumattomiin tasoihin nojaava tapa.

Nollaluottamusmalli voi olla parempi vaihtoehto kuin Purdue-malli, koska se tarjoaa joustavuutta ja tarkkuutta tietoturvan hallinnassa. Silti on tärkeää tunnistaa, että nollaluottamusmalli edellyttää myös mittavia muutoksia organisaation sisällä ja sitoutumista. Lisäksi se on tällä hetkellä eräänlainen muoti-ilmiö tietoturvaratkaisuna, eli siihen voi kohdistua liiallisia tai epärealistisia odotuksia. Tästä huolimatta nollaluottamusmalli tarjoaa mielenkiintoisen näkökulman tietoturvaan ja voi olla arvokas työkalu teollisuuden ohjausjärjestelmille, jotka pyrkivät parantamaan tietoturvansa tasoa ja vastaamaan nykypäivän vahvasti tietoteknisten ympäristöjen vaatimuksiin.

5 Yhteenveto

Teollisuuden ohjausjärjestelmän tietoturvallisuudella on merkityksellinen rooli kriittisen infrastruktuurin jatkuvan toiminnan kannalta. Näillä moniosaisilla järjestelmillä on silti monia tietoturvaongelmia, joihin vastaaminen voi olla monimutkaista. Datadiodi tarjoaa mielenkiintoisen ja kustannustehokkaan vaihtoehdon olemassa olevien tietoturvaratkaisujen rinnalle erityisesti OT- ja IT-ympäristöjen yhdyskäytäväksi. Tämän tutkielman tarkoituksena oli perehtyä, miten datadiodia voidaan hyödyntää teollisuuden ohjausjärjestelmän tietoturvan parantamiseksi (TK1) ja millainen datadiodikytkentä sopisi osaksi teollisuuden ohjausjärjestelmää (TK2). Näihin tutkimuskysymyksiin pystytään vastaamaan seuraavasti pohjaten vastaukset taulukon 4.1 mukaisiin kirjallisuuskatsauksen aineistoihin:

TK1: Tutkimuskysymykseen vastaamiseksi tutkielmassa analysoitiin teollisuuden ohjausjärjestelmän tietoturvaongelmia. Erityisesti niitä on valvomo-ohjelmistoilla, joilla ei ole tarpeeksi laskentatehoa kryptografisten salausalgoritmien asentamiseksi, eli erilaisilla haittaohjelmaiskuilla on paljon avointa hyökkäyspinta-alaa. Lisäksi niiden usein käyttämät haavoittuvat kommunikaatioprotokollat eivät tue autentikointia, jolloin järjestelmät ovat avoinna väärän tiedon syöttämiselle ja haitallisen etäkoodin suorittamiselle. Myös OT-ympäristöjen integroituminen IT-ympäristöihin tuo mukanaan uusia tietoturvahaasteita.

Datadiodin ominaisuuksilla on keskeinen rooli teollisuuden ohjausjärjestelmän tietoturvallisuuden parantamisessa. Erityisesti yksisuuntaisuus ja fyysinen ra-

kenne ovat keskiössä. Ne estävät tietojen palaamisen vastaanottajan verkon turvallisuustasolta lähettäjän verkon turvallisuustasolle, mikä suojaa järjestelmää tietovuodoilta, haittaohjelmahyökkäyksiltä ja väärän tiedon syöttämiseltä. Lisäksi datadiodi on kustannustehokas, koska sen rakentamiseen tarvittavat komponentit ovat edullisia ja helposti saatavilla. Kaupallisten datadiodien etuna on puolestaan niiden mittava kaistanleveys, jopa 10 Gbps.

Toisaalta tiedonsiirron tietoturvallisuus vaatii myös ohjelmistotasoisia ratkaisuja. Datadiodi ei yksin estä tiedon muokkaamista tai väärän tiedon syöttämistä, jos hyökkääjä pääsee käsiksi järjestelmään ennen tiedon siirtämistä datadiodin läpi. Silloin ohjelmistot ovat välttämättömiä tietojen tarkastuksen ja mahdollisten virheiden korjaamisen varmistamiseksi. Tietojen eheys vaatii lisäsuojauksia, kuten kryptografiaa ja ohjelmistotarkastuksia. Sen tähden datadiodin rinnalle voitaisiin kytkeä esimerkiksi autentikointia tukeva palomuuri pääsynhallinnan ja kulunvalvonnan saavuttamiseksi. Lisäksi teollisuuden ohjausjärjestelmän kokonaisrakenteen tietoturvallisuutta voidaan parantaa merkittävästi kytkemällä jokaiselle Purdue-mallin tasolle tunkeilijan havaitsemisjärjestelmä ja/tai -estojärjestelmä.

TK2: Teollisuuden ohjausjärjestelmän kokonaisrakenteeseen sijoitettavaa datadiodikytkentää pohdittiin TK1:n johtopäätösten avulla. Kytkennässä sijoitettaisiin OT- ja IT-ympäristöjen väliin datadiodiyhdyskäytävä, joka koostuisi palomuurilla varustetuista kytkimistä. Kahden datadiodin väliin sijoitettaisiin historiatietopalvelin. Jos datadiodin yhteydessä käytettäisiin UDP-protokollaa, kytkentää voitaisiin täydentää eheyden parantamiseksi kolmannella solmulla tai ohjaussignaalimuistin- tai virheenkorjauskoodin käyttämisellä. Datadiodit varmistaisivat turvallisen tietoliikenteen historiatietoihin, ja kytkimien palomuurit ratkaisisivat autentikointipulman. Tietoliikenne vastakkaiseen suuntaan ratkaistaisiin joko uudella datadiodikytkennällä tai palomuurilla. Toisaal-

ta Purdue-mallin muuttumattomien tasojen mallinnusta voitaisiin täydentää nollaluottamusmallilla, jolloin teollisuuden ohjausjärjestelmä pystyisi varautua toiminnallisemmin tietoturvauhkiin. Kuva 4.1 havainnollistaa ehdotettua datadiodikytkentää sovitettuna teollisuuden ohjausjärjestelmän kokonaisrakenteeseen.

Kaiken kaikkiaan datadiodilla voidaan parantaa teollisuuden ohjausjärjestelmän tietoturvallisuutta, jos se implementoidaan lisäteknisenä tietoturvalaitteena osaksi teollisuuden ohjausjärjestelmää palomuurin rinnalle. Kytkennän avulla pystytään jakamaan organisaation OT- ja IT-ympäristöt turvallisesti omiksi ympäristöikseen ja varmistetaan turvallisuusluokitellulle tiedolle tehokas yhdyskäytävä. Lisäksi datadiodi on kilpailukykyinen ja edullinen tietoturvalaite turvaamaan muutakin kriittistä tietoliikennettä.

Kirjoitusprosessin aikana heräsi myös tulevaisuuden jatkokysymyksiä aiheesta. Esimerkiksi datadiodien integroituminen ja soveltuvuus uusiin teknologioihin ja protokolliin, kuten ulkoisiin tietoverkkoihin ja teolliseen esineiden internetiin, ovat mielenkiintoisia tutkimusaiheita. Lisäksi olisi hyödyllistä tarkastella datadiodien käyttöönottoa ja käyttökokemuksia käytännön sovelluksissa empiirisesti, mikä auttaisi ymmärtämään paremmin datadiodien käytännön hyötyjä ja haasteita. Kirjoitusprosessin aikana keskeistä oli myös huolellinen lähdemateriaalin valinta ja kirjallisuuskatsauksen tekeminen. Kirjallisuuskatsauksen avulla oli mahdollista hahmottaa aiheen keskeisiä käsitteitä ja teemoja, mikä auttoi olemassa olevien aineistojen arvioinnin ohella tutkimuskysymyksiin vastaamisessa.

Lähdeluettelo

[1] B.-S. Jeon ja J.-C. Na, "A study of cyber security policy in industrial control system using data diodes", teoksessa *2016 18th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South): IEEE, 2016, s. 314–317. DOI: 10.1109/ICACT.2016.7423374.

[2] A. C.-F. Chan ja J. Zhou, "Non-Intrusive Protection for Legacy SCADA Systems", *IEEE Communications Magazine*, vol. 61, nro 6, s. 36–42, 2023. DOI: 10.1109/MCOM.003.2200564.

[3] E. D. Knapp ja J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd. Syngress Publishing, 2014.

[4] K. Zetter. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid". (2016), url: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (viitattu 10. 03. 2024).

[5] P. Polityuk, O. Vukmanovic ja S. Jewkes. "Ukraine's power outage was a cyber attack - Ukrenergo". (2017), url: https://www.reuters.com/article/idUSKBN1521BB/ (viitattu 10. 03. 2024).

[6] R. Collier. "NHS ransomware attack spreads worldwide". (2017), url: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/ (viitattu 10. 03. 2024).

[7] S. E. Woo, E. H. O'Boyle ja P. E. Spector, "Best practices in developing, conducting, and evaluating inductive research", *Human Resource Management Review*, vol. 27, nro 2, s. 255–264, 2017. DOI: https://doi.org/10.1016/j.hrmr.2016.08.004.

[8] M. Coughlan ja P. Cronin, *Doing a Literature Review in Nursing, Health and Social Care*, 2nd edition. SAGE Publications Ltd, 2017.

[9] I. A. Almaazmi, M. S. Al Shehhi, O. A. Alkhoori, S. J. Al Shehhi ja Y. Hamid, "Data Diode for Cyber-security: A Review", teoksessa *2022 International Conference on Artificial Intelligence of Things (ICAIoT)*, Istanbul, Turkey: IEEE, 2022, s. 1–6. DOI: 10.1109/ICAIoT57170.2022.10121887.

[10] RFC 793. "Transmission Control Protocol". (1981), url: https://www.ietf.org/rfc/rfc0793.txt (viitattu 29. 03. 2024).

[11] RFC 768. "User Datagram Protocol". (1980), url: https://datatracker.ietf.org/doc/html/rfc768 (viitattu 29. 03. 2024).

[12] M. Stevens. "An implementation of an optical data diode. Salisbury: DSTO Electronics and surveillance research laboratory". (1999), url: https://apps.dtic.mil/sti/pdfs/ADA365579.pdf (viitattu 02. 05. 2024).

[13] R. D. Larkin, T. J. Wagner ja B. E. Mullins, "Securing Photovoltaic System Deployments with Data Diodes", teoksessa *2020 47th IEEE Photovoltaic Specialists Conference (PVSC)*, Calgary, AB, Canada: IEEE, 2020, s. 2525–2531. DOI: 10.1109/PVSC45281.2020.9300863.

[14] K. Kertysova, E. Frinking ja G. Gricius. "Understanding the strategic and technical significance of technology for security. The case of data diodes for cybersecurity. The Hague Secrity Delta (HSD)". (2019), url: https://securitydelta.nl/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf (viitattu 02. 05. 2024).

[15] G. El Hajal, R. Abi Zeid Daou, Y. Ducq ja J. Börcsök, "Designing and validating a cost effective safe network: application to a PACS system", teoksessa *2019 Fifth International Conference on Advances in Biomedical Engineering (ICABME)*, Tripoli, Lebanon: IEEE, 2019, s. 1–4. DOI: 10.1109/ICABME47164.2019.8940252.

[16] D. Mukherjee, B. Kumar Sethi, S. Chakraborty, R. Banerjee, P. Kumar Guchhait ja J. Bhunia, "Real-time Mitigation of Effects of False Data in Smart Grid: A Data Diode Approach", teoksessa *2021 IEEE 9th Region 10 Humanitarian Technology Conference (R10-HTC)*, Bangalore, India: IEEE, 2021, s. 1–6. DOI: 10.1109/R10-HTC53172.2021.9641729.

[17] "Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 28.11.2019/1101". (2019), url: https://www.finlex.fi/fi/laki/ajantasa/2019/20191101#P12 (viitattu 23. 03. 2024).

[18] Ulkoministeriö. "Katakri – tietoturvallisuuden auditointityökalu viranomaisille". (2020), url: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille (viitattu 23. 03. 2024).

[19] D. E. Bell ja L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations", *The MITRE Corporation*, vol. I, 1973. url: https://web.archive.org/web/20060618092351/http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf (viitattu 23. 03. 2024).

[20] K. J. Biba, "Integrity Considerations for Secure Computer Systems", *The MITRE Corporation*, vol. MTR-3153, 1975. url: https://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf (viitattu 23. 03. 2024).

[21] Kyberturvallisuuskeskus. "Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista". (2021), url: https://www.kyberturvallisuuskeskus.

fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf (viitattu 23. 03. 2024).

[22] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan ja N. Meskin, "Cybersecurity for industrial control systems: A survey", *Computers and Security*, vol. 89, s. 101 677, 2020. DOI: 10.1016/j.cose.2019.101677.

[23] S. S. Ha, H. Beuster, T. R. Doebbert ja G. Scholl, "An FPGA-based Unidirectional Gateway Proposal for OT-IT Network Separation to Secure Industrial Automation Systems", teoksessa *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, Lemgo, Germany: IEEE, 2023, s. 1–6. DOI: 10.1109/INDIN51400.2023.10218126.

[24] M. Sverko, T. G. Grbac ja M. Mikuc, "SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0", *IEEE Access*, vol. 10, s. 109 395–109 430, 2022. DOI: 10.1109/ACCESS.2022.3211288.

[25] A. Abou el Kalam, "Securing SCADA and critical industrial systems: From needs to security mechanisms", *International Journal of Critical Infrastructure Protection*, vol. 32, s. 100 394, 2021. DOI: https://doi.org/10.1016/j.ijcip.2020.100394.

[26] L. Obregon. "Secure Architecture for Industrial Control Systems. GIAC (GSEC) Gold Certification". (2015), url: https://www.giac.org/paper/gsec/37212/secure-architecture-industrial-control-systems/146660 (viitattu 02. 05. 2024).

[27] B. Li, K. J. Larsen, D. Zibar ja I. Tafur Monroy, "Reconfigurable Forward Error Correction Decoder for Beyond 100 Gbps High Speed Optical Links", *IEEE Communications Letters*, vol. 19, nro 2, s. 119–122, 2015. DOI: 10.1109/LCOMM.2014.2379655.

[28] M. Tsai, S. Lee ja S. W. Shieh, ”Strategy for Implementing of Zero Trust Architecture”, *IEEE Transactions on Reliability*, vol. 73, nro 1, s. 93–100, 2024. DOI: 10.1109/TR.2023.3345665.

[29] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig ja R. Doss, ”Zero Trust Architecture (ZTA): A Comprehensive Survey”, *IEEE Access*, vol. 10, s. 57 143–57 179, 2022. DOI: 10.1109/ACCESS.2022.3174679.