Kyberturvallisuuden viitekehysten vastaavuus älykkäisiin tuotantolaitoksiin kohdistuviin uhkiin

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Joulukuu 2024
Arttu Einistö

TURUN YLIOPISTO
Tietotekniikan laitos

Arttu Einistö: Kyberturvallisuuden viitekehysten vastaavuus älykkäisiin tuotantolaitoksiin kohdistuviin uhkiin

TkK-tutkielma, 27 s.
Tietotekniikka
Joulukuu 2024

Teollisuuden tuotantolaitoksissa hyödynnetään yhä enenevissä määrin kehittynyttä informaatioteknologiaa, kuten teollista esineiden internetiä, pilvilaskentaa ja tekoälyä, minkä seurauksena myös niiden potentiaalinen hyökkäyspinta-ala on aiempaa laajempi. Perinteisesti teollisuuden tuotantoprosesseista vastaava operatiivinen teknologia on eristetty julkisista tietoverkoista, mutta informaatioteknologian integroiminen osaksi tuotantolaitoksia edellyttää monimutkaisempaa ja avoimempaa verkko- ja järjestelmäarkkitehtuuria. Toimintaympäristön fundamentaalisen muutoksen myötä yleispätevän ohjeistuksen ja standardoinnin merkitys kasvaa, minkä seurauksena kyberturvallisuuden viitekehysten rooli tässä neljänneksi teolliseksi vallankumoukseksi kutsutussa muutoksessa on suuri.
Tässä kirjallisuuskatsauksena toteutetussa tutkielmassa perehdyttiin siihen, miten tämä tuotantolaitosten rakenteellinen muutos vaikuttaa niiden kyberturvallisuuteen, ja miten keskeisimmät eurooppalais- ja yhdysvaltalaislähtöiset kyberturvallisuuden viitekehykset vastaavat keskeisimpiin uhkiin, joihin lukeutuvat toimitusketjuihin, työntekijöihin sekä laite- ja protokollatason haavoittuvuuksiin kohdistuvat kyberhyökkäykset. Tutkielman lopputuloksena havaittiin, että arvioinnin kohteena olleiden viitekehysten sisällön puutteet korostuivat erityisesti sekä perinteisten tuotantojärjestelmien ja modernin informaatioteknologian integroinnin että teollisen esineiden internetin laitteiden rajallisten resurssien huomioinnin kohdalla. Tulosten perusteella arvioitiin, että uusien ja nopeasti kehittyvien teknologioiden kyberturvallista käyttöönottoa voitaisiin mahdollisesti nopeuttaa tiivistämällä eri sektoreita edustavien organisaatioiden sekä julkisten ja yksityisten tutkimuslaitosten uhkatiedustelutiedon jakamiseen liittyvää yhteistyötä.

Asiasanat: esineiden internet, tuotantolaitos, kyberturvallisuuden viitekehys

Sisällys

1 Johdanto

Teollisuuden digitalisaatio ja niin kutsuttu neljäs teollinen vallankumous muokkaavat merkittävästi tuotantolaitosten toimintaympäristöjä. Yritykset pyrkivät lisäämään tuotantoprosessien automaatiota sekä tietopohjaista päätöksentekoa, jotka vaativat tuekseen katkeamatonta informaatiovirtaa tuotantoympäristön laitteista sekä kykyä analysoida suuria datamassoja. Nykypäivän älykkäissä tuotantolaitoksissa yhdistyvätkin niin perinteinen operatiivinen teknologia (OT) kuin informaatioteknologia (IT) esineiden internetin (IoT), tekoälyn (AI) ja pilvipalveluiden kautta.

Merkittävä toimintaympäristöön kohdistuva muutos toisaalta mahdollistaa entistä tehokkaamman tuotannon, mutta samalla laajentaa tuotantolaitoksiin kohdistuvien kyberuhkien kirjoa ja kasvattaa hyökkäyspinta-alaa. Myös siirtymäprosessi vanhasta infrastruktuurista moderniin arkkitehtuuriin sisältää merkittäviä kyberturvallisuuden haasteita. Uhkien torjunnassa epäonnistuminen voi johtaa tuotannon keskeytymiseen, taloudellisiin tappioihin ja kriittisimmillään jopa fyysisiin vahinkoihin ja vaaratilanteisiin. [1]

Kyberturvallisuutta pyritään perinteisesti mallintamaan ja soveltamaan erilaisiin toimintaympäristöihin viitekehysten ja standardien avulla. Niiden myötä organisaatioiden on mahdollista hallita ja torjua uhkia järjestelmällisemmin sekä vertailla eri puolustusmenetelmien tehokkuutta. Tuotantolaitosten nopea digitalisaatio yhdistettynä teollisuuden tietojärjestelmien erityispiirteisiin nostaa kuitenkin esiin kysymyksen siitä, miten hyvin modernit viitekehykset vastaavat näiden toimintaympäristöjen

haasteisiin. Tästä huolimatta modernien tuotantojärjestelmien ja kyberturvallisuuden viitekehysten välistä suhdetta ja vastaavuutta koskevia tieteellisiä julkaisuja on hyvin rajallinen määrä. [2]

Tässä tutkielmassa perehdytään älykkäisiin tuotantolaitoksiin kohdistuviin kyberuhkiin ja arvioidaan nykyisten kyberturvallisuuden viitekehysten soveltuvuutta näiden uhkien torjuntaan. Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

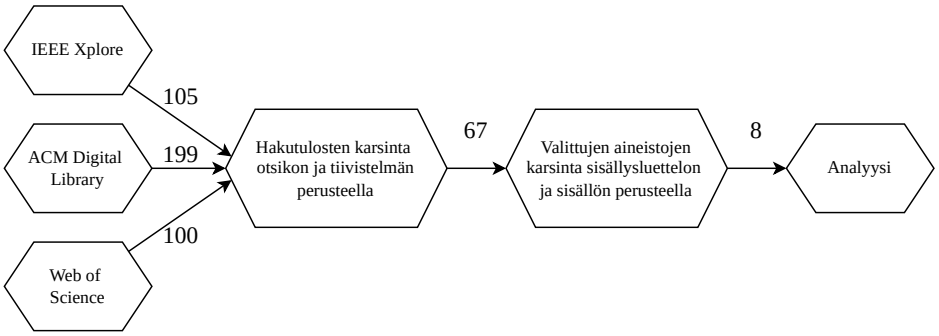
- TK1: Mitkä ovat keskeisimpiä älykkäisiin tuotantolaitoksiin kohdistuvia kyberuhkia?
- TK2: Miten hyvin nykyiset kyberturvallisuuden viitekehykset vastaavat älykkäisiin tuotantolaitoksiin kohdistuviin uhkiin?

Tutkielma toteutettiin analyyttisena kirjallisuuskatsauksena ja siinä käytetyt aineistot haettiin IEEE Xplore -, ACM Digital Library - ja Web of Science -hakutietokannoista. Tutkielman analyysiä käsitteleviä aineistoja ajatellen muotoiltiin kolme aineistojen haussa käytettyä hakulausetta:

- (“smart manufacturing” OR “smart factor*”) AND cyber* AND threat
- (“nist csf” OR enisa) AND (“internet of things” OR “smart manufacturing” OR “smart factor*”) AND framework

Alustavasti hakulauseiden tuottamia tuloksia karsittiin kuvan 1.1 mukaisesti otsikon ja tiivistelmän perusteella, minkä jälkeen jäljelle jääneiden aineistojen sisällön perusteella valittiin tutkielman aihepiiriä parhaiten vastaavat. Kaikkien tutkielman analyysiosioon valittujen aineistojen JUFO-luokitus on vähintään 1.

Tutkielmassa tarkastellaan älykkäiden tuotantolaitosten ominaispiirteitä, teknologioita sekä niihin kohdistuvia kyberuhkia perehtyen erityisesti teollisuus 4.0 -konseptin mukanaan tuomiin uhkatyyppeihin. Tämän jälkeen tarkastellaan tutkiel-



Kuva 1.1: Tiedonhaun toteutus

man keskiöön sijoittuvia kyberturvallisuuden viitekehyksiä, joiden vastaavuutta käsiteltyihin kyberuhkiin arvioidaan tutkielman analyysiosiossa. Analyysissä pyritään erityisesti vertailemaan viitekehyksiä keskenään hyödyntäen olemassaolevaa tutkimustietoa, tutkimaan yhdysvaltalaisen ja eurooppalaisen lähestymistavan eroavaisuuksia sekä yleisesti tunnistamaan viitekehysten keskeisimpiä vahvuuksia ja heikkouksia älykkäisiin tuotantolaitoksiin kohdistuvien uhkien näkökulmasta. Lopuksi analyysin tulosten perusteella pohditaan, mitä osa-alueita tai toimintamenetelmiä painottamalla älykkäiden tuotantolaitosten kyberturvallisuutta voitaisiin kehittää tulevaisuudessa.

2 Älykkäät tuotantolaitokset

Älykkäillä tuotantolaitoksilla viitataan tyypillisesti teollisuus 4.0 -konseptin mukaisiin kyberfysikaalisiin järjestelmiin (CPS), joissa yhdistyvät kehittyneet informaatioteknologian osa-alueet, kuten teollinen esineiden internet (IIoT) ja hajautetut laskentajärjestelmät, sekä operatiivinen teknologia (OT) [3]. Älykkäät tuotantojärjestelmät mahdollistavat reaaliaikaisen tuotantoprosessien kontrolloinnin ja automatisoidun mukauttamisen tuotantoympäristön tai ulkoisten tekijöiden, kuten kysynnän tai raaka-aineiden hintojen, muutoksiin [4].

Tässä luvussa esitellään älykkäiden tuotantolaitosten keskeisimmät teknologiset piirteet, joiden ymmärtäminen on olennaista tutkielman myöhemmissä luvuissa käsiteltävien kyberuhkien ja kyberturvallisuuden viitekehysten analysoinnin kannalta. Luvun lopussa analysoidaan myös tuotantojärjestelmien paradigman muutosta ja sen seurauksia älykkäiden tuotantomenetelmien käyttöönotolle.

2.1 Operatiivinen teknologia

Tuotantoympäristöissä tapahtuvan muutoksen ymmärtämiseksi on käsiteltävä tuotantolaitosten perinteisten automaatiojärjestelmien rakennetta. Näitä järjestelmiä kuvaillaan usein operatiivisen teknologian (OT) käsitteellä, joka itsessään käsittää ympäristönsä kanssa vuorovaikutuksessa olevat järjestelmät, jotka koostuvat laitteistosta ja ohjelmistoista. Informaatioteknologian roolin kasvaessa OT-järjestelmiä käytetään yhä runsaasti tarkasti rajattujen prosessien automatisaatioon. [5]

Moderneja OT-järjestelmiä kuvataan tyypillisesti ISA-95-referenssimallin kaltaisen hierarkkisen arkkitehtuurin kautta. ISA-95-malli jakaa OT-järjestelmän komponentit viisiportaisen arkkitehtuurin mukaisesti: tuotantoprosessit, ohjausteknologia ja valvontajärjestelmät sekä näistä harmaalla vyöhykkeellä (engl. *Industrial Demilitarized Zone*, iDMZ) eroteltuna liiketoimintalogiikkaan sekä muihin yritystoimintoihin liittyvät IT-järjestelmät. Tästä kategorisoinnista älykkäiden tuotantolaitosten IT- ja OT-järjestelmien konvergenssin kannalta korostuvat erityisesti tuotantoprosessit, niiden ohjausteknologia ja valvontajärjestelmät. [5]

ISA-95-mallin matalin taso pitää sisällään mekaaniset tuotantoprosessien komponentit, kuten yksittäiset sensorit, käyttölaitteet ja muun käyttökoneiston. Seuraava taso puolestaan pitää sisällään yksittäisten laitteiden automaatiosta vastaavan teknologian, kuten erilaiset ohjelmoitavat logiikat (PLC) ja muut mikropiiripohjaiset ohjauslaitteet. Ohjelmoitavien logiikoiden tehtävänä on noudattaa yksinkertaisia logiikkaketjuja vuorovaikutuksessa alimman tason komponenttien kanssa ja välittää komponenteista kerättyä dataa ylemmän tason valvontajärjestelmille. [5]

Kahden alimman tason edustaessa OT-järjestelmien hajautettua puolta, toimii valvontajärjestelmiä edustava kolmas taso esimerkkinä keskitetystä arkkitehtuurista. Tuotantoprosessien valvontaan ja informaation hallintaan keskittyvien järjestelmien (SCADA) tehtävänä on toimia hermokeskuksina ympäri tuotantojärjestelmää hajautetun laitteiston sekä koneen ja ihmisen välisen käyttöliittymän (HMI) välisenä rajapintana. SCADA-järjestelmät ovat OT-järjestelmien keskeisimpiä komponentteja, sillä niitä käytetään prosessien ohjaamiseen ja niistä kerätyn infromaation visualisoimiseen. Juuri keskeisestä roolistaan johtuen SCADA-järjestelmät ovat myös koko tuotantoprosessin ylläpidon ja turvallisuuden näkökulmasta tärkeitä. [5]

Laskentatehon kasvaminen on mahdollistanut älykkäiden laitteiden sijoittamisen yhä lähemmäs itse tuotantoprosesseja, joka muuttaa myös tuotantoprosesseista kerättävän informaation analysointia [5]. Toisaalta vastapainoisesti tuotantolaitok-

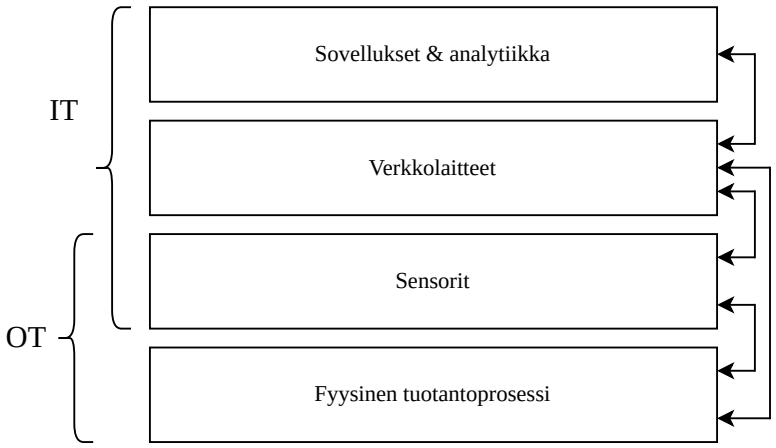
sia operoiviin pieniin ja keskisuuriin organisaatioihin kohdistetut kyselytutkimukset osoittavat, että siirtyminen älykkäisiin tuotantojärjestelmiin on haastavaa korkeiden kustannusten, kyberturvallisuuden riskien sekä pätevän työvoiman vähäisyyden vuoksi [6]. Kuvattu ilmiö korostaakin perinteisten OT-järjestelmien pitkää käyttöikää sekä korkeana pysynyttä käyttöastetta.

2.2 Teollisuus 4.0

Teollisuus 4.0 eli neljäs teollinen vallankumous kuvaa edistyneiden teknologioiden, kuten esineiden internetin, pilvilaskennan sekä tekoälyn, hyödyntämistä osana teollisuuden järjestelmiä. Tyypillisesti siirtymä älykkäisiin tuotantojärjestelmiin tapahtuu kolmannen teollisen vallankumouksen mukaisten ICT-automaatiojärjestelmien pohjalta. Lopputuloksena syntyviä tuotantolaitosten sisäisiä IT- ja OT-infrastruktuurin kokonaisuuksia kutsutaan kyberfysikaalisiksi järjestelmiksi [7]. [4]

Käytännössä teollisuus 4.0 -konseptin mukaiset tuotantolaitokset koostuvat kuvan 2.1 havainnollistamalla tavalla keskenään verkottuneista OT- ja IIoT-laitteista sekä data-analytiikan ja muut liiketoimintaa täydentävät toiminnot mahdollistavista IT-järjestelmistä. Arkkitehtuurinsa puolesta järjestelmät voidaan jakaa neljään eri pääkategoriaan: fyysiset tuotantolaitteet, tuotantoprosesseja mittaavat sensorit, kommunikaatiosta ja informaation jakamisesta vastaavat verkkolaitteet sekä päätöksenteosta ja kerätyn informaation jatkojalostuksesta vastaavat perinteiset IT-järjestelmät. [3]

IIoT-laitteiden pohjalle rakentuvat älykkäät järjestelmät ovat älykkäiden tuotantolaitosten toiminnallisuuden kannalta keskeisessä asemassa. Ne keräävät dataa perinteisestä tuotantolaitteistosta, hyödyntävät data-analytiikkaa osana reaaliaikaista päätöksentekoa ja pystyvät käsittelemään suuriakin datamassoja minimaalisin kustannuksin. Niiden pääasiallinen tehtävä on toimia informaation yhdyskäytävänä tuotantolaitteiston ja muiden IT-järjestelmien välillä. Modernit IIoT-laitteet muodosta-



Kuva 2.1: Kyberfysikaalisen järjestelmän arkkitehtuuri

vatkin dynaamisen verkkorakenteen, jossa kommunikaatio perustuu IP-protokollaan ja tapahtuu usein langattomasti. Verrattuna perinteisiin OT-laitteisiin ne myös kykenevät diagnosoimaan omaa toimintaansa ja mahdollisia vikatilanteita tehokkaasti ja sen seurauksena toimimaan hyvin itsenäisesti. [4]

Tuotantojärjestelmän osista, kuten ohjelmoitavista logiikoista tai sensoreista, IIoT-laitteiden välityksellä kerättyä informaatiota on mahdollista välittää niin automatisoidun päätöksenteon kuin muiden liiketoimintapohjaisten sovelluskohteiden käyttöön. Reunalaskentaa ja erilaisia tekoälypohjaisia ratkaisuja voidaan hyödyntää tuotantoprosessista kerättyjen lokitietojen tai tilastojen, kuten aikasarjojen, analysointiin ja hyödyntämiseen reaaliaikaisessa päätöksenteossa. Lisäksi IIoT-laitteiden mahdollistama IT-OT-konvergenssi mahdollistaa IT-pohjaisten yritysjärjestelmien liittämisen suoraan tuotantoprosessiin, jolloin liiketoiminnassa voidaan hyödyntää reaaliaikaista informaatiota. [4]

Informaatiopohjaisen automaation ohella kokonaisten tuotantojärjestelmien mallinnus ja simulointi ovat älykkäiden tuotantolaitosten keskeisimpiä etuja. Digitaalisen kaksonen (DT) -mallissa tietokonepohjainen malli ja todellisesta tuotantoympäristöstä kerätty informaatio voidaan synkronisoida keskenään ja näin syntyneellä

simulaatiomallilla voidaan testata erilaisia toimintamenetelmiä ja päätöksiä [8]. Varsinaisista tuotantojärjestelmistä erillisenä elementtinä DT toimii myös turvallisena ympäristönä kyberturvallisuuden ja muiden toimintavarmuuden kannalta kriittisten ominaisuuksien kehittämiseen tai analysointiin. [9]

Kokonaisuudessaan älykkäiden tuotantolaitosten uudenlainen arkkitehtuuri luo myös uusia toimintaympäristöön liittyviä haasteita, joista merkittävimmät liittyvät perinteisen OT-infrastruktuurin yhteensovittamiseen modernin IT-ympäristön kanssa. Moni OT-järjestelmän komponentti käyttää verkkokommunikaatiossaan suljettua teknologiaa tai erittäin sovelluskohtaisia protokollia. IIoT-laitteet puolestaan pyrkivät hyödyntämään standardisoituja menetelmiä keskinäisen yhteensopivuuden takaamiseksi [2]. Monet OT-järjestelmät on myös suunniteltu toimimaan suljetuissa ja tietoverkoiltaan hyvin eristetyssä ympäristössä, mutta älykkäiden tuotantolaitosten keskeisimpien komponenttien, kuten IIoT-laitteiden tai pilvilaskennan, tehokas hyödyntäminen vaatii tuotantoympäristön yhdistämistä avoimeen verkkoon, jonka seurauksena järjestelmän hyökkäyspinta-ala kasvaa huomattavasti. [1]

2.3 Paradigman muutos

Tässä luvussa käsiteltiin älykkäitä tuotantolaitoksia, niiden arkkitehtuurin ominaispiirteitä sekä niiden hyödyntämiä teknologioita. Luvussa perehdyttiin erityisesti operatiivisen teknologian järjestelmien sekä informaatioteknologian konvergenssiin ja sen tuomiin muutoksiin tuotantolaitosten toiminnassa verrattuna perinteisiin tuotantojärjestelmiin.

Operatiivinen teknologia luo älykkkäiden tuotantolaitosten järjestelmien perustan. OT-arkkitehtuuri perustuu pitkälti eri osa-alueiden keskinäiseen hierarkiaan, jossa ohjelmoitavat logiikat ohjaavat tuotantolinjastojen yksittäisiä komponentteja, ja SCADA-valvontajärjestelmät puolestaan ohjelmoitavia logiikoita vastaanottamiensa käskyjen perusteella. Laitetason laskentatehon kehitys on kuitenkin mahdol-

listanut älykkäiden laitteiden sijoittamisen yhä lähemmäs tuotantoprosesseja, minkä seurauksena kyberfysikaaliset järjestelmät kattavat keskeisen osan älykkäiden tuotantolaitosten toiminnoista. [5]

Teollisuus 4.0:n mukaisen IT- ja OT-järjestelmien konvergenssin myötä tuotantolaitosten toiminta on muuttunut perustavanlaatuisesti. Siirtymä automaatioteknologiasta älykkäisiin tuotantolaitoksiin edustaa merkittävää paradigman muutosta, jossa tuotantoprosessien joustavuus ja mukautuvuus nousevat perinteisen prosessioptimoinnin rinnalle. Digitaalisten kaksosten ja kehittyneen analytiikan avulla tuotantolaitokset kykenevät ennakoimaan tuotannontekijöiden muutoksia ja optimoimaan toimintaansa itsenäisesti reaaliajassa. [4], [9]

Toisaalta teknologinen murros asettaa organisaatioille huomattavia haasteita, kuten eri aikakausien teknologioiden integroinnin, kyberturvallisuudesta huolehtimisen sekä henkilöstön kouluttamisen [6]. Yleisesti ottaen vasta hiljattain yleistyneisiin teknologioihin siirtymistä saatetaan pitää riskialttiina, mikä voikin osittain selittää miksi etenkään pienet toimijat eivät ole kiirehtineet älykkäiden tuotantojärjestelmien käyttöönotossa. Järjestelmien verkottumisen ja avoimuuden lisääntymisen johdosta jokaisen työntekijän tulisi olla perillä toimintaympäristön kyberturvallisuudesta, mikä saattaa hankaloittaa sekä uuden työvoiman rekrytointia että kasvattaa nykyisten työntekijöiden koulutuskustannuksia.

3 Älykkäiden tuotantolaitosten kyberturvallisuus

Älykkäiden tuotantolaitosten toimintaperiaate pohjatuu laitteiden verkottuneisuuteen sekä IT-palveluiden hyödyntämiseen kaikilla tuotantoprosessin osa-alueilla. Kyberfysikaaliset järjestelmät muodostuvat suuresta määrästä erilaisia IIoT-laitteita, jotka kommunikoivat niin keskenään kuin sekä sisäisten että ulkoisten IT-palveluiden kanssa [1]. Tämä paradigman muutos kasvattaa huomattavasti tuotantolaitosten hyökkäysvektoria ja mahdollisesti luo haavoittuvuuksia, jotka huonoimmassa tilanteessa saattavat vaikuttaa suoraan tuotantoprosesseihin [1]. Älykkäiden tuotantolaitosten kohdalla kyberturvallisuus merkitseekin kompromissia käytettävyyden sekä saatavuuden ja turvallisuuden välillä [10].

Tässä luvussa käsitellään keskeisimpiä älykkäisiin tuotantolaitoksiin kohdistuvia uhkia keskittyen erityisesti IIoT-laitteisiin ja kyberfysikaalisiin järjestelmiin. Samalla käydään läpi sekä hyökkäysten juurisyitä älykkäiden tuotantolaitosten järjestelmäarkkitehtuurin pohjalta että erilaisten kyberuhkien teknisiä piirteitä. Lopuksi analysoidaan kyberturvallisuuden viitekehysten ja standardien suhdetta läpi käytyjen uhkien juurisyihin.

3.1 Keskeisimmät uhat

Merkittävimpiä IIoT-laitteiden kyberturvallisuuteen vaikuttavia piirteitä ovat laitteiden suuri lukumäärä, välitön reagointi vastaanotettuun informaatioon, verkottuneisuus, tarve pystyä kommunikoimaan perinteisen infrastruktuurin kanssa, järjestelmien dynaaminen rakenne, vikatilanteiden aiheuttama fyysinen uhka sekä tarve ylläpidettävien toimintojen jatkuvuudelle. Erilaisten laitteiden suuri lukumäärä sekä järjestelmien dynaaminen rakenne hankaloittavat yhtenäisten suojausratkaisujen kehittämistä ja tietoliikenteen suuri volyymi niin verkkojen valvontaa. [2]

Kuluttajakäyttöön suunnitellut IoT-laitteet ja tuotantoympäristöjen IIoT-laitteet ovat sekä rooliltaan että teknologisilta piirteiltään usein hyvin samankaltaisia. Molempien keskeisiin tehtäviin kuuluu informaation välittäminen verkottuneessa ympäristössä langattomien tai langallisten teknologioiden välityksellä [1]. Keskeisimmät IIoT-laitteiden kyberturvallisuuteen liittyvät ongelmat voidaan kategorisoida seuraavasti: hyökkäysten vaikutus, tietoliikenteen turvallisuus, käyttäjäntunnistus ja pääsynvalvonta sekä keskinäisen luottamuksen hallinnointi [10].

Älykkäiden tuotantolaitosten suuret ja vahvasti toisistaan riippuvaiset laiteverkot kasvattavat merkittävästi verkon yksittäisissä laitteissa tai järjestelmissä havaittujen haavoittuvuuksien vaikutusta koko verkon toimintavarmuuteen ja turvallisuuteen [2]. Kyseinen uhka on vahvasti liitännäinen IT-OT-konvergenssin myötä syntyneeseen ongelmatilanteeseen, jossa vanhojen kyberturvallisuuden standardien perusteella suunniteltuja perinteisiä järjestelmiä yhdistetään osaksi tietoverkkoja, jotka ovat suoraan yhteydessä internetiin. Toisaalta usein myös modernien IIoT-laitteiden suunnittelussa kyberturvallisuuden merkitystä väheksytään. Tämä altistaa suojaukseltaan puutteelliset laitteet haavoittuvuuksille, joita uhkatoimijat voivat kartoittaa julkisten verkkojen kautta. [10]

Laitetason suojauksen kattavuuden lisäksi laitteiden ja verkkojen eheyden merkitys on suuri. IIoT-laitekentän moninaisuuden sekä globaalin talouden monimutkais-

ten toimitusketjujen seurauksena laitteiden komponenttien tai ohjelmistojen hyödyntäminen vakoiluun tai toimintahäiriöiden aiheuttamiseen on varteenotettava uhka [10]. Yleisesti verkottuneessa toimintaympäristössä toimitusketjuhyökkäykset näyttäytyvät uhkatoimijoille tehokkaana menetelmänä, jossa yksittäisen toimittajayrityksen tai palveluntarjoajan järjestelmeen murtautuminen mahdollistaa toimitusketjun kautta pääsyn myös asiakasyritysten järjestelmiin [2]. Esimerkkinä toimitusketjujen haavoittuvuudesta voidaan pitää yhdysvaltalaisen SolarWinds-yrityksen järjestelmiin kohdistunutta tietomurtoa, jonka myötä hyökkääjä pääsi levittämään haitallista koodia ohjelmistoa käyttävien asiakasyritysten tietoverkkoihin, tuotantoteollisuuden laitokset mukaan lukien [11].

Vaikka älykkäät tuotantolaitokset toimivat hyvin itsenäisesti, operoi niitä loppupeleissä yhä työntekijä. Vaikka itse tuotantojärjestelmä olisi sekä laite- että järjestelmätasolla tarkasti suojattu, aiheuttavat siihen sisältä päin kohdistuvat hyökkäykset yhä merkittävän uhan. Uhkatoimijat voivat pyrkiä manipuloimaan järjestelmien käyttäjiä saadakseen näiden käyttäjätunnusten kautta pääsyn kohdejärjestelmiin [10]. Yhtälailla Bring Your Own Device -ilmiö (BYOD), jossa työntekijät saattavat käyttää samoja laitteita sekä vapaa-ajan aktiviteetteihin että työasioihin, mahdollistaa hyökkääjille pääsyn järjestelmiin niiden sisältä käsin [10]. Tämäntyyppisistä uhista merkittäviä tekee se, että hyökkäysten tunnistaminen on haastavaa hyökkääjien hyödyntäessä tietoihin oikeutettuja käyttäjätunnuksia sekä laitteita ja toimiessa järjestelmissä normaalin käyttäjän tavoin.

Merkittävä osa uhista kohdistuu älykkäissä tuotantolaitoksissa laitteiden ja järjestelmien väliseen kommunikaatioon. Kattava laite- ja järjestelmärajat ylittävä tietoliikenne sekä modernien laitteiden langattomuus mahdollistavat tehokkaan informaation hyödyntämisen ja joustavan järjestelmärakenteen, mutta samalla kasvattavat potentiaalista hyökkäyspinta-alaa. Teollisuudessa langattomaan kommunikaatioon usein käytettyä RFID-teknologiaa on mahdollista häiritä tai sen lähettämää

dataa muokata tai väärentää [10]. Myös langallisten yhteyksien protokollatason haavoittuvuudet esimerkiksi kryptografisten salausavainten vaihdossa altistavat tietoliikenteen väliintulohyökkäyksille (engl. *Man-in-the-Middle attack*, MITM). Uhan merkitystä korostavat laite- ja protokollatason haavoittuvuuksien korjaamisen haastavuus. [2]

Aiempaa avoimemmat tietoverkot, haavoittuvuudet tietoliikenteeseen käytettävissä protokollissa tai laitteissa sekä IIoT-laitteiden rajalliset laitteistoresurssit mahdollistavat myös sovellus- ja komponenttitason palvelunestohyökkäykset [1]. Uhkatoimijat voivat kohdistaa paljon laskentatehoa, muistia, tallennustilaa tai tietoliikennekapasiteettia kuluttavia toimintoja laitteisiin, jolloin niiden käyttö estyy ja ongelmat saattavat propagoitua myös muihin tuotantojärjestelmän osiin. Palvelunestohyökkäykset muodostavatkin erittäin kriittisen uhan älykkäille tuotantolaitoksille, sillä niiden tuotantojärjestelmät ovat kartoitettavissa julkisen verkon kautta ja pienetkin toimintavarmuuteen kohdistuvat ongelmat saattavat aiheuttaa mittavia taloudellisia vahinkoja tai jopa fyysisiä vaaratilanteita. [10]

3.2 Standardoinnin merkitys

Tässä luvussa käsiteltiin älykkäiden tuotantolaitosten kyberturvallisuutta erityisesti keskeisimpien uhkien näkökulmasta. Kyberturvallisuuden haasteet kumpuavat etenkin järjestelmien monimuotoisuudesta, verkottuneisuudesta sekä IIoT-laitteiden määrästä, jotka kokonaisuutena kasvattavat verkko-, laite- ja sovellustason hyökkäyspinta-alaa.

Merkittävimmän riskin muodostavat vanhojen OT-pohjaisten tuotantojärjestelmien ja modernin teknologian yhteensovittaminen, toimitusketjujen kautta leviävät hyökkäykset sekä työntekijöihin tai muihin järjestelmän käyttäjiin kohdistuva manipulointi. Lisäksi heikosti suojatut tai haavoittuvaiset tietoliikenneprotokollat ja langattomat yhteydet voivat altistaa tuotantojärjestelmiä häirinnälle, vakoilulle tai

muille väliintulohyökkäyksille. Erityisesti IIoT-laitteiden yleistyminen johtaa siihen, että tietoliikenteen ohella palvelunestohyökkäyksiä voidaan kohdistaa myös rajallisia laitteistoresursseja kohtaan. [10]

Teollisuus 4.0:n mukaisen järjestelmäarkkitehtuurin paradigman muutoksen seurauksena kasvanut hyökkäyspinta-ala vaatii kattavia laite- ja verkkotason suojauksia sekä jatkuvaa kyberturvallisuuden puolustusratkaisujen kehittämistä [1]. Kyberuhkien keskittyminen erityisesti eri aikakausien IT- ja OT-järjestelmien yhteensovittamiseen sekä monimuotoisten laiteverkkojen suojausratkaisujen kehittämiseen kertoo perinteisten kyberturvallisuuden menetelmien soveltamisen haasteista älykkäiden tuotantolaitosten kohdalla. Aiempaa avoimemmissa tuotantoympäristöissä eivät välttämättä päde IT- tai OT-järjestelmille kohdennetut viitekehykset, vaan suojausratkaisuissa tulee yhdistellä ohjeita molemmista.

4 Kyberturvallisuuden viitekehykset

Kyberturvallisuuden viitekehykset tarjoavat organisaatioille jäsennellyn lähestymistavan kyberturvallisuuden kehittämiseen ja soveltamiseen yksilöllisessä toimintaympäristössä. Tyypilliset modernit viitekehykset sisältävät keinoja luokitella monimutkaisten tietojärjestelmien osa-alueita niiden kriittisyyden perusteella, noudattaa zero trust -tietoturvamallia omassa toimintaympäristössä sekä muodostaa selkeän yritystason suunnitelman kyberuhkien torjumiseen ja niistä palautumiseen. Älykkäiden tuotantolaitosten kohdalla standardisoitujen toimintamallien tarve korostuu erityisesti IT- ja OT-järjestelmien konvergenssissa, jossa sekoittuvat perinteisten tuotannon automaatiojärjestelmien sekä IoT-laitteiden suojaaminen. [12]

Tässä luvussa käsitellään järjestelmällisesti keskeisimpien modernien kyberturvallisuuden viitekehysten sisältöä, jota seuraavassa luvussa vertaillaan tutkielman aiemmissa luvuissa käsiteltyihin älykkäisiin tuotantolaitoksiin kohdistuviin kyberuhkiin. Tarkastelun kohteena olevat viitekehykset ovat rakenteeltaan hyvin samankaltaisia, mutta pyrkivät vsataamaan eri maantieteellisten alueiden tarpeisiin. Viitekehysten rakenteessa keskitytään erityisesti kyberuhkien torjuntaa, tunnistamista sekä niiltä suojautumista käsitteleviin osioihin.

4.1 NIST CSF 2.0

Yhdysvaltain standardisointi- ja teknologiainstituutin (NIST) kehittämä kyberturvallisuuden viitekehyksen (CSF) versio 2.0 on alkuvuodesta 2024 julkaistu doku-

mentti, joka tarjoaa erityisesti Yhdysvalloissa toimiville organisaatioille korkean tason kuvauksen kyberturvallisuuden vaatimuksista modernissa toimintaympäristössä. Viitekehys koostuu sen ytimen muodostamasta kuusiportaisesta toimintavaiheiden luokittelusta, organisaatiokohtaisesta kyberturvallisuuden tarpeiden profiloinnista sekä kyberturvallisuuden hallinnointiin ja riskienhallintaan liittyvistä tasoista. Tämän tutkielman kontekstissa perehdytään ydintoimintojen sisältöön. [13]

NIST CSF 2.0:n ytimen muodostavat kuvan 4.1 mukaiset kuusi toisistaan keskeisesti riippuvaista toimintoa: hallinnointi (engl. *Govern*, GV), tunnistaminen (engl. *Identify*, ID), suojaaminen (engl. *Protect*, PR), havaitseminen (engl. *Detect*, DE), vastaaminen (engl. *Respond*, RS) ja palautuminen (engl. *Recover*, RC).

Kuva 4.1: NIST CSF 2.0 -viitekehyksen ydintoiminnot [13]

Toiminnot jakautuvat edelleen kategorioihin ja alakategorioihin. Kategoriat määrittelevät yksittäisten toimintojen osa-alueet ja alakategoriat puolestaan täsmentävät osa-alueiden aihepiiriä tarkkojen toimintamallien ja esimerkkien avulla. Toiminnoista hallinnointi, tunnistaminen ja palautuminen liittyvät vahvasti organisaatiotason kyberturvallisuusstrategian määrittelyyn toimintaympäristön tarpeiden kautta. Suojaaminen, havaitseminen ja vastaaminen puolestaan edustavat hyvin käytännönläheisiä toimintoja, joiden kohdalla ohjeistus keskittyy käsittelemään laite- ja järjestelmätason toimia. [13]

Hallinnointi sekä tunnistaminen käsittävät organisaatiotason riskienhallintastrategian eri osa-alueet: työntekijöiden roolit, linjaukset ja niiden toteutumisen valvonnan, toimintaympäristön elementtien tunnistamisen ja hallinnoinin sekä kyberturvallisuuden jatkuvan kehittämisen [13]. Erityisen painoarvon toimintojen muodostamassa kokonaisuudessa saavat toimitusketjujen riskien huomiointi ja torjunta, jolla käytännössä viitataan yritysrajat ylittävään yhteistyöhön sekä asianmukaiseen huolellisuuteen (engl. *due diligence*) yrityssuhteiden luomisessa ja ylläpitämisessä. Uhkien tunnistamisessa yhteistyö nostetaan erityiseen rooliin kyberuhkatiedon jakamisen sekä aktiivisen omien järjestelmien haavoittuvuuksien etsimisen kautta. [14]

Suojaaminen sekä havaitseminen kattavat järjestelmien resilienssiä kasvattavia täsmällisiä toimia, kuten pääsynhallinnan, tietojen turvallisen käsittelyn, tietoverkkojen valvonnan sekä poikkeamien havainnoinnin [13]. Toiminnoille yhteisenä osa-alueena esiin nostetaan laitteiden, ohjelmistojen sekä käyttäjien kokonaisvaltainen jatkuva valvonta, mitä edellä mainitut kategoriat tukevat. Teknisellä tasolla esimerkeiksi nostetaan protokollatason, kuten nimipalvelu- tai reititysprotokollien, valvonta sekä laitteiden ja käyttäjien yksilöinti. Informaation käsittelyn kokonaisuuden osalta painotetaan järjestelmällistä CIA-mallin (engl. *Confidentiality, Integrity, and Availability*) mukaista tietojenkäsittelyä koko datan elinkaaren ajan. [14]

Vastaaminen ja palautuminen täydentävät toimintojen ketjun: ne keskittyvät toimintamalleihin vahinkojen minimoimiseksi ja alkuperäisten toimintojen palauttamiseksi [13]. Vastaaminen kattaa neljä kategoriaa: poikkeamien hallinnan, analysoinnin, raportoinnin ja viestinnän. Niin vastaaminen kuin palautuminen ovat kokonaisuuksina vahvasti riippuvaisia hallinnoinnin toiminnon alaisesta organisaation kyberturvallisuusstrategiasta, joka ohjaa juurisyiden selvittämistä sekä keskeisimpien sisäisten ja ulkoisten sidosryhmien tiedottamista. Käytännön ennaltaehkäisevistä toimenpiteistä mainitaan muun muassa varmuuskopioiden eheyden varmistaminen ja palautettujen toimintojen yhtenäisyyden todentaminen. [14]

Kokonaisuutena NIST CSF 2.0:n ydintoiminnot korostavat strategista ja järjestelmällistä lähestymistapaa sekä elektronisten että fyysisten uhkien torjuntaan, niitä vastaan puolustautumiseen sekä onnistuneista hyökkäyksistä palautumiseen. Yksittäisistä toimintamalleista eniten korostuvat ennaltaehkäisevät menetelmät, kuten zero trust -arkkitehtuuri, CIA-mallin mukainen tietojenkäsittely sekä infrastruktuurin järjestelmien ja laitteiden ylläpitäminen ja aktiivinen valvonta. [13]

4.2 ENISA:n IoT-viitekehys

Euroopan unionin kyberturvallisuusviraston (ENISA) kehittämä "Good practices for Security of Internet of Things in the context of Smart Manufacturing" -raportti on loppuvuodesta 2018 julkaistu viitekehysmäinen EU-maissa toimiville organisaatioille. Sen päätavoitteena on koostaa useista eri viitekehyksistä ja standardeista älykkäiden tutoantolaitosten kyberturvallisuutta tukevia käytäntöjä ja toimintamalleja. Raportti koostuu älykkäiden tuotantolaitosten kohtaamista turvallisuushaasteista, kyberuhkien kartoituksesta, hyökkäysskenaarioiden analysoinnista sekä puolustusmenetelmistä ja suosituksista. Tämän tutkielman kontekstissa raporttia tarkastellaan puolustusmenetelmien sisällön osalta. [15]

ENISAN:n raportin puolustusmenetelmät jakautuvat kuvan 4.2 mukaisesti kolmeen eri osioon: linjauksiin (engl. *Policies*, PS), organisaatiotason toimintatapoihin (engl. *Organisational practices*, OP) sekä teknisiin menetelmiin (engl. *Technical practices*, TM). Kyseiset osiot sisältävät useita eri kategorioita, jotka rajaavat osion pienemmiksi kyberturvallisuuden piirteiksi. Kolmiportaisen rakenteen täydentävät kategorioiden osa-alueet, jotka käsittelevät käytännön toimia, joilla kyseisiä piirteitä voidaan kehittää. Osioista linjaukset edustavat kyberturvallisuuden suunnitelmallisuutta sekä sääntelypohjaista lähestymistapaa, ja organisaation toimintatavat puolestaan toimintaympäristön abstraktimpeja elementtejä, kuten työntekijöitä, liikekumppaneita sekä toimitiloja. Lähimmäksi käytäntöä osioista sijoittuvat tekniset

Kuva 4.2: Yleiskatsaus ENISA:n hyviin käytäntöihin [15]

menetelmät, jotka keskittyvät teknisen infrastruktuurin puolustamiseen laite- ja ohjelmistotasolla. [15]

Linjaukset kattavat älykkäiden tuotantolaitosten suunnitteluvaiheen perusperiaatteet, jotka toimivat perustana sekä organisaatiotason toimintatavoille että yksityiskohtaisemmille teknisille menetelmille. Osio perustuu turvallisuuden ja tietosuojan kehittämiseen tuotantoympäristön arkkitehtuurin, sen elementtien järjestelmällisen ylläpitämisen sekä riskien ja uhkien hallinnan kautta. Yksittäisistä kyberturvallisuuden kokonaisuutta tukevista toiminnoista esiin nostetaan uhkamallinnus sekä riskianalyysi yhteistyössä muiden organisaatioiden, kuten kansallisten CERT-toimijoiden (engl. *Community Emergency Response Team*), kanssa. Kokonaisuutena linjaukset tähtäävät koko organisaatiorakenteen kattavaan yhtenäiseen kyberturvallisuusstrategiaan, jonka perustalta organisaatiotason toimia ja teknisiä puolustusmenetelmiä voidaan toteuttaa. [15]

Organisaatiotason toimintatavat käsittävät toimintaympäristön sisäiset käytännön toimintamallit. Osiossa nostetaan esiin sekä olemassaolevan työvoiman kouluttaminen modernin kybertoimintaympäristön vaatimusten mukaisesti että tietosuojan ja turvallisuuden painottaminen yhteistyössä kolmansien osapuolten kanssa.

Henkilöstöresurssien lisäksi osiossa painotetaan kyberturvallisuuspainotteisen järjestelmäarkkitehtuurin, järjestelmien ja laitteiden järjestelmällisen hallinnoinnin sekä poikkeamien ja haavoittuvuuksien aktiivisen etsimisen merkitystä. Älykkäiden tuotantolaitosten kannalta keskeiseksi haasteeksi nostetaan IT- ja OT-järjestelmien konvergenssi sekä monimutkaiset toimitusketjut. Puolustusmenetelmien osalta suositellaan tietoturvavalvomoiden (engl. *Cybersecurity Operations Centre*, SOC) perustamista sekä aktiivista haavoittuvuuksien etsimistä sekä penetraatiotestauksen että haavoittuvuuspalkkio-ohjelmien kautta. [15]

Tekniset menetelmät täydentävät kahta edeltävää osiota yksityiskohtaisin laitteita ja ohjelmistoja käsittelevien käytännön suositusten kautta. Osio jakautuu luottamuksen- ja eheydenhallintaan, pilvipalveluiden turvallisuuteen, liiketoiminnan jatkuvuuden varmistamiseen ja häiriötilanteista palautumiseen, laitteiden välisen kommunikaation turvallisuuteen sekä tietosuojaan. Keskeisiksi painopisteiksi näiden osa-alueiden välille muodostuvat informaation suojaaminen kryptografisin menetelmin sekä kokonaisvaltainen tietoliikenteen valvonta laite-, järjestelmä- ja protokollatasolla. Näitä painopisteitä täydennetään nostamalla esiin yksittäisiä menetelmiä, kuten monivaiheinen tunnistautuminen, verkkojen segmentointi, toiminnallisuuden hajauttaminen pienempiin kokonaisuuksiin sekä lokitietojen reaaliaikainen analysointi poikkeamien havaitsemiseksi. [15]

Kokonaisuudessaan ENISA:n älykkäiden tuotantolaitosten kyberturvallisuutta käsittelevä raportti tarjoaa järjestelmällisen kolmiportaisen lähestymistavan kyberturvallisuuden kehittämiseen modernissa ja jatkuvasti muutoksessa olevassa toimintaympäristössä. Linjausten ja organisaatiotason toimintatapojen muodostamalle perustalle rakentuvat tekniset menetelmät kattavat laajan kirjon käytännön toimenpiteitä luottamuksen- ja eheydenhallinnasta protokollatason suojausmenetelmiin. Ohjeistus toimii osana Euroopan unionin kyberturvallisuusstrategiaa, jossa tehokas toimeenpano taataan turvallisuus- sekä raportointivelvoitteiden kautta [16]. [15]

5 Analyysi

Auttaakseen toimivien kyberturvallisuuden ratkaisujen kehittämisessä, on kyberturvallisuuden viitekehysten vastattava tarkasti käytännön toimintaympäristöön kohdistuvia uhkia [12]. Tässä luvussa arvioidaan, miten luvussa 4 käsitellyt viitekehykset vastaavat luvussa 3 esiin nostettuja kyberuhkia, ja erityisesti mitä potentiaalisia ongelmia viitekehysten ohjeistukset sisältävät älykkäiden tuotantolaitosten kyberturvallisuuden osalta. Lisäksi pohditaan mitkä tekijät ovat johtaneet havaittuun lopputulokseen, ja millä keinoilla tilannetta voitaisiin kehittää tulevaisuudessa.

5.1 Viitekehysten arviointi

Arviointivaiheessa kyberuhat jaoteltiin taulukon 5.1 mukaisesti älykkäiden tuotantolaitosten toimintaympäristön piirteiden perusteella. Piirteiden kategorisoinnissa pyrittiin huomioimaan luvussa 3 käsiteltyjen kyberuhkien taustasyitä sekä L. Axon et al. (2022) ja W. Zhou et al. (2019) artikkeleissaan käsittelemiä IoT- ja IIoT-ympäristöjä koskevia piirteitä, mutta samalla rajaamaan käsiteltävien kategorioiden määrää vastaamaan tutkielman pituuden asettamia rajoitteita. Yhdessä arviointiin käytetyt kategoriat luovat kattavan kuvan älykkäiden tuotantoympäristöjen kyberturvallisuuden kannalta olennaisista piirteistä, mutta yksittäin käsiteltyinä ne liittyvät vahvasti myös muiden digitaalisten järjestelmien turvallisuuteen. Viitekehysten kyberuhkien havaitsemista, torjuntaa ja ennaltaehkäisyä käsittelevien osa-alueiden vastaavuutta kategorioihin arvioitiin asteikolla hyvä, kohtalainen ja heikko. [2], [17]

Taulukko 5.1: Viitekehysten vastaavuus ominaispiirteisiin

	NIST CSF 2.0	**ENISA IoT I4.0**
Järjestelmien laajuus ja dynaamisuus	Hyvä	Hyvä
Toimintaympäristön kulttuurillinen muutos	Kohtalainen	Hyvä
Laiterajoitteet	Heikko	Kohtalainen
IT-OT-integraatio	Kohtalainen	Kohtalainen
Palveluvarmuus	Hyvä	Hyvä

Sekä NIST:n että ENISA:n viitekehyksissä tuotantojärjestelmien laajuuden, dynaamisuuden ja verkottuneisuuden luomia ongelmia pyritään ensisijaisesti torjumaan suunnitelmallisuudella, selkeällä vastuualueiden roolituksella, jatkuvalla järjestelmän eri komponenttien passiivisella valvonnalla ja dynaamisella kartoittamisella sekä pääsynhallinnalla. Molempien viitekehysten kohdalla painotetaan kyberturvallisuuspohjaisen koulutuksen tärkeyttä ja sen integroimista osaksi organisaatiotason henkilöstöresurssien hallintaa. Kuitenkin NIST:n ohjeistuksessa henkilöstöresurssien sopeuttaminen toimintaympäristön radikaaliin muutokseen jää teoreettiseksi, eikä käytännön toimintamalleja IIoT-pohjaisten järjestelmien hallintaan käsitellä.

ENISA:n viitekehys on analysoiduista viitekehyksistä huomattavasti teknologiakeskeisempi, jonka seurauksena se myös havainnoi laite- ja järjestelmätason suojausvaihtoehtoja huomattavasti NIST:n viitekehystä paremmin. Toisaalta molemmissa viitekehyksissä toistuvista tarpeellisuusperiaatteen (engl. *need-to-know principle*) mukaisesta tietojenkäsittelystä sekä laitetason todennuksesta ja pääsynhallinnasta on laajojen monimuotoisten laiteverkkojen kohdalla suhteellisen vähän toimintavalmiita ratkaisuja, mikä heikentää kyseisten menetelmien uskottavuutta [2].

Erityisesti NIST:n viitekehyksessä IT-OT-konvergenssin aiheuttamien rajoitteiden huomiointi on puutteellista. Esimerkiksi viitekehyksessä esiin nostettu tietoverkko- ja protokollatason valvonta on haasteellista IT- ja OT-järjestelmien eroavaisuuksien johdosta niiden käyttämien suljetun lähdekoodin tiedonsiirtoprotokollien

ja IT-standardeista eroavien tiedon tallennusmuotojen johdosta [2]. ENISA:n ohjeistus tuo sen sijaan esiin IT- ja OT-järjestelmien integraatiota tukevia ratkaisuja, kuten harmaan vyöhykkeen (engl. *Industrial Demilitarized Zone*, iDMZ), verkkojen mikrosegmentoinnin ja perinteisten järjestelmien eristämisen julkisesta verkosta välipalvelinten (engl. *proxy*) avulla.

Molemmat viitekehykset vastaavat älykkäiden tuotantolaitosten hyvän saatavuuden sekä palveluvarmuuden vaatimuksia painottamalla ongelmatilanteisiin varautumisen merkitystä. NIST:n viitekehyksessä varautumista käsitellään strategialähtöisesti, kun taas ENISA:n ohjeistuksessa nostetaan esiin muun muassa vian sattuessa turvallisten (engl. *fail-safe*) operaatiomallien ja varmuuskopioinnin merkitys. Korkean saatavuuden vaatimuksesta aiheutuvia järjestelmien ja laitteiden päivittämisen haasteita pyritään ohjeistuksissa minimoimaan muun muassa priorisoimalla ylläpidon tarvetta järjestelmän eri elementtien kriittisyyden perusteella.

Viitekehykset heijastavat sisällöllisesti lähtömaidensa yrityskulttuurisia aspekteja. NIST:n viitekehyksen ohjeistuksessa korostuvat niin innovatiivisuus kuin organisaatiokohtainen vapaus toteuttaa ohjeistuksia omien tarpeiden mukaisesti, kun ENISA:n viitekehys perustuu vahvasti laaja-alaisen sääntelyn ja kyberturvallisuuden standardoinnin hyödyntämiseen EU:n tietoturvaa ja -suojaa koskevien direktiivien ja asetusten kautta. Sama lähestymistapojen eroavaisuus on havaittavissa Euroopan ja Yhdysvaltojen välillä toimialasta riippumatta erityisesti uusien teknologioiden, kuten tekoälyn ja lohkoketjujen, kehityksessä ja käyttöönotossa.

5.2 Pohdinta

On selvää, että automaatio tulee lisääntymään runsaasti lähitulevaisuudessa niin tuotantoteollisuuden kuin muidenkin teollisuuden alojen kohdalla. Teknologian monimutkaistuessa ja muodostuessa osaksi jokaisen työntekijän työtehtäviä virallisesta roolista riippumatta on standardoiduilla menetelmillä entistä suurempi merkitys.

Onkin syytä tarkastella, miten kyberturvallisuuden ohjeistusta ja siihen suhtautumista tulisi kehittää tulevaisuudessa tasapainon löytämiseksi teoreettisen monipuolisuuden ja käytännön toimeenpanovalmiuden välillä.

Älykkäät tuotantolaitokset ja teollinen esineiden internet ovat uusia, vasta suhteellisen varhaisessa kehitysvaiheessa olevia konsepteja. Tästä syystä onkin ymmärrettävää, että erityisesti skaalautuvien ja toimintavarmojen kyberturvallisuuden toimintamallien ja teknologioiden vähäisyys on keskeisimpiä konseptiin liittyviä ongelmia. Tutkimustiedon ja kaupallisten toimijoiden markkinoimien ratkaisujen välinen ero on paikoittain hyvinkin suuri, mikä saattaa johtaa siihen, ettei tutkimustietoa pystytä hyödyntämään täysimääräisesti puolustusmenetelmien kehittämiseen.

Reaaliaikaisen käytännön toimintaympäristöjä koskevan informaation ja uhkatiedustelutiedon jakamisen merkitystä ei sovi väheksyä keinona kaventaa teorian ja käytännön realiteettien välistä eroa. Kyberturvallisuudessa puolustusratkaisut ovat pääsääntöisesti lähes aina uhkatoimijoiden hyökkäysmenetelmiä jäljessä, jolloin jakamalla entistä kattavampaa, organisaatiorajoista riippumatonta ja anonymisoitua tietoa voitaisiin mahdollisesti kehittää kokonaisvaltaista kykyä reagoida organisaatioihin kohdistuviin uhkiin. Lisäksi lyhentämällä teoreettisten konseptien ja toimeenpanovalmiiden tuotteiden välistä sykliä kyettäisiin tukemaan nopeasti kehittyvien teknologioiden käyttöönottoa.

Toisaalta erityisesti pienemmillä organisaatioilla on jo ennestään vaikeuksia pysytellä mukana kyberturvallisuuden kehityksessä. Tutkielmassa tarkasteltujen kyberuhkien taustasyinä korostuvat erityisesti vaikeudet soveltaa olemassaolevia puolustusmenetelmiä suuriin ja monimuotoisiin laiteverkkoihin. Niin ikään viitekehysten arvioinnissa keskeisimpien puutteiden havaittiin kohdistuvan IIoT-laitteiden rajallisten resurssien sekä IT-OT-integraation huomioimiseen. Kehittämällä modulaarisuuteen perustuvia ja rajapintojen välityksellä perinteiseen infrastruktuurin integroitavissa olevia puolustusmenetelmiä voitaisiin helpottaa vanhan infrastruktuurin in-

tegroimista uusien järjestelmien kanssa sekä parantamaan kustannustehokkuutta.

Perinteisesti teollisuusinfrastruktuuriin kohdistuvia hyökkäyksiä ovat pääsääntöisesti suorittaneet erinäiset vieraiden valtioiden tukemat APT-ryhmittymät (engl. *Advanced Peristent Threat*), mutta neljännen teollisen vallankumouksen myötä myös alkeellisempia hyökkäystekniikoita hyödyntävät uhkatoimijat pystyvät kohdentamaan hyökkäyksiä julkiseen verkkoon näkyviin järjestelmiin. Potentiaalisten hyökkääjien ja hyökkäystekniikoiden määrän kasvaessa erityisesti puolustuksen yhtenäisyyden merkitys korostuu entisestään, mikä on toisaalta myös helpotus erityisesti pienemmille ja vähemmän kriittistä infrastruktuuria operoiville organisaatioille. Kehittyneempiä hyökkäysmenetelmiä sovelletaan tyypillisesti korkeamman profiilin kohteisiin, kuten esimerkiksi kriittiseen infrastruktuuriin, jolloin jo perustason kyberturvallisuuden puolustusmenetelmiä hyödyntämällä voidaan saavuttaa uhka-arvioiden näkökulmasta tarpeellinen suojauksen taso.

6 Yhteenveto

Tutkielmassa pyrittiin tunnistamaan merkittävimpiä älykkäisiin tuotantolaitoksiin kohdistuvia kyberuhkia (TK1) ja arvioimaan, miten keskeisimmät yhdysvaltalaista ja eurooppalaista näkökulmaa edustavat kyberturvallisuuden viitekehykset vastaavat näihin uhkiin ja niiden taustalla vaikuttaviin syihin (TK2). Tutkimuksen perusteella keskeisimmiksi kyberturvallisuuden haasteiksi havaittiin OT-pohjaisten tuotantojärjestelmien integrointi moderniin IT-infrastruktuuriin sekä verkottuneiden ja monimuotoisten laiteverkkojen hallinnointi.

Merkittävimmiksi älykkäiden tuotantolaitosten IT- ja OT-pohjaisiin järjestelmäkokonaisuuksiin kohdistuviksi kyberuhiksi tunnistettiin toimitusketjuhyökkäykset, laite- ja protokollatason haavoittuvuudet sekä työntekijöihin kohdistetut manipulointihyökkäykset. Yksittäisenä merkittävänä uhkana käsiteltyjen kategorioiden joukosta korostuu perinteisten tuotantolaitteiden ja -järjestelmien puutteellinen suojaus, joka osaltaan myös vaikeuttaa yhtenäisten laite- ja verkkotason suojausmenetelmien käyttöä. Lisäksi IIoT-laitteiston rajalliset resurssit altistavat tietoverkkojen yksittäiset solmukohdat palvelunestohyökkäyksiin perustuvalle sabotaasille.

Tutkielmassa käsitellyt Yhdysvaltain standardisointi- ja teknologiainstituutin (NIST) sekä Euroopan union kyberturvallisuusviraston (ENISA) viitekehykset tarjoavat kattavia ja monipuolisia menetelmiä sekä kyberuhkien että fyysisten tuotantoympäristöihin kohdistuvien hyökkäysten torjuntaan, mutta eivät täysin vastaa älykkäiden tuotantolaitosten erityistarpeita. NIST:n viitekehys korostaa strategista

organisaatiotason riskinhallintaa, mutta sen käytännön ohjeistus erityisesti IT- ja OT-järjestelmien konvergenssin ja IIoT-laitteiden rajallisten resurssien huomioinnin osalta on puutteellista. ENISA:n viitekehys puolestaan esittelee tarkemmin teknisiä suojausmenetelmiä, kuten verkkojen segmentointia tai välipalvelinten käyttöä, mutta sen haasteena on yhtälailla yleispätevien ja toimintavalmiiden ratkaisujen tarjoaminen suurissa ja dynaamisissa toimintaympäristöissä.

Tutkielman lähdeaineisto sekä toteutettu analyysi osoittavat, että älykkäiden tuotantolaitosten nopea kehitys asettaa merkittäviä haasteita kyberturvallisuuden ylläpitämiselle. Nykyisten keinojen lisäksi haasteisiin voitaisiin pyrkiä vastaamaan aiempaa tiiviimmän yhteistyön sekä niin tieteellisten kuin kaupallisten puolustusratkaisujen perinteisiä järjestelmiä paremmin tukevan arkkitehtuurin kautta. Kokonaisuutena teollisuus 4.0 -menetelmien hyödyntämisen kasvattaman hyökkäyspinta-alan merkitystä erityisesti taloudellisesta näkökulmasta on vielä tässä vaiheessa tutkittu suhteellisen vähän, minkä johdosta se voisikin olla potentiaalinen jatkotutkimusnäkökulma tässä tutkielmassa käsitellylle aihepiirille.

Lähdeluettelo

[1] V. R. Kebande ja A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions", *ACM Comput. Surv.*, vol. 56, nro 5, tammikuu 2024, ISSN: 0360-0300. DOI: 10.1145/3635030.

[2] L. Axon, K. Fletcher, A. S. Scott et al., "Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda", *Digital Threats*, vol. 3, nro 4, joulukuu 2022. DOI: 10.1145/3503920.

[3] C. Qian, Y. Guo, A. Hussaini, A. Musa, A. Sai ja W. Yu, "A New Layer Structure of Cyber-Physical Systems under the Era of Digital Twin", *ACM Trans. Internet Technol.*, kesäkuu 2024, ISSN: 1533-5399. DOI: 10.1145/3674974.

[4] P. K. Illa ja N. Padhi, "Practical Guide to Smart Factory Transition Using IoT, Big Data and Edge Analytics", *IEEE Access*, vol. 6, s. 55 162–55 170, 2018. DOI: 10.1109/ACCESS.2018.2872799.

[5] C. Perducat, D. C. Mazur, W. Mukai, S. N. Sandler, M. J. Anthony ja J. A. Mills, "Evolution and Trends of Cloud on Industrial OT Networks", *IEEE Open Journal of Industry Applications*, vol. 4, s. 291–303, 2023. DOI: 10.1109/OJIA.2023.3309669.

[6] P. Bründl, M. Stoidner, H. G. Nguyen, A. Baechler ja J. Franke, "Digitalization and Adoption of Industry 4.0 in Engineer-to-order Small and Medium-sized Manufacturing Companies: An Empirical Analysis", teoksessa *2023 IEEE*

International Conference on Industrial Engineering and Engineering Management (IEEM), 2023, s. 0908–0912. DOI: 10.1109/IEEM58616.2023.10406684.

[7] M. Prist, A. Monteriù, A. Freddi et al., "Cyber-Physical Manufacturing Systems for Industry 4.0: Architectural Approach and Pilot Case", teoksessa *2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)*, 2019, s. 219–224. DOI: 10.1109/METROI4.2019.8792880.

[8] D. Allison, P. Smith ja K. Mclaughlin, "Digital Twin-Enhanced Incident Response for Cyber-Physical Systems", teoksessa *Proceedings of the 18th International Conference on Availability, Reliability and Security*, sarja ARES '23, Association for Computing Machinery, 2023. DOI: 10.1145/3600160.3600195.

[9] C.-T. Lin ja H.-J. Lu, "An Intelligent Product-Driven Manufacturing System Using Data Distribution Service", *IEEE Access*, vol. 12, s. 16 447–16 461, 2024. DOI: 10.1109/ACCESS.2024.3359228.

[10] G. Spathoulas ja S. Katsikas, "Towards a Secure Industrial Internet of Things", teoksessa *Security and Privacy Trends in the Industrial Internet of Things*, C. Alcaraz, toim. Springer International Publishing, 2019, s. 29–45, ISBN: 978-3-030-12330-7. DOI: 10.1007/978-3-030-12330-7_2.

[11] FireEye, "Evasive Attacker Leverages SolarWinds Supply Chain Compromises with Sunburst Backdoor", 2020. url: https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (viitattu 24. 10. 2024).

[12] V. Mullet, P. Sondi ja E. Ramat, "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0", *IEEE Access*, vol. 9, s. 23 235–23 263, 2021. DOI: 10.1109/ACCESS.2021.3056650.

[13] National Institute of Standards and Technology, ”The NIST Cybersecurity Framework (CSF) 2.0”, tekninen raportti NIST CSWP 29, helmikuu 2024. DOI: 10.6028/NIST.CSWP.29.

[14] National Institute of Standards and Technology, *Cybersecurity Framework 2.0 Reference Tool*, elokuu 2023. url: https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters (viitattu 05. 11. 2024).

[15] European Union Agency for Cybersecurity, ”Good Practices for Security of Internet of Things in the context of Smart Manufacturing”, tekninen raportti, marraskuu 2018, s. 36–43. DOI: 10.2824/851384.

[16] Euroopan parlamentti ja Euroopan unionin neuvosto, ”Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555”, nro 2022/2555, joulukuu 2022. url: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022L2555 (viitattu 05. 11. 2024).

[17] W. Zhou, Y. Jia, A. Peng, Y. Zhang ja P. Liu, ”The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”, *IEEE Internet of Things Journal*, vol. 6, nro 2, s. 1606–1616, 2019. DOI: 10.1109/JIOT.2018.2847733.