Juuso Kekki

TEOLLISTEN IoT-LAITTEIDEN ELINKAAREN KYBERTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Kekki, Juuso
Teollisten IoT-laitteiden elinkaaren kyberturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2023, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Vuorinen, Jukka

IoT-laitteita on käytössä monissa eri ympäristöissä ja niiden käytön lisääntyminen teollisissa ympäristöissä on jatkuvassa kasvussa. IoT-laitteiden käyttöön teollisuudessa liittyy trendi nimeltä Industry 4.0 ja monia käsitteitä, kuten Industrial internet of things (IIoT) ja cyber-physical systems. IoT-laitteiden käytöstä teollisuudessa löytyy kattavasti kirjallisuutta ja tutkimuksia. Tässä kirjallisuuskatsauksessa keskitytään IIoT-laitteiden elinkaaren kyberturvallisuuteen ja elinkaaren aikana ilmeneviin haasteisiin. Tämän kirjallisuuskatsauksen alussa esitellään käsitteet IIoT, Industry 4.0 ja cyber-physical systems (CPS), jonka jälkeen käydään läpi IoT-laitteiden elinkaari ja lopuksi elinkaaren kyberturvallisuus ja sen vaiheiden haasteet. Tutkimuksessa selviää, että keskeisimmät haasteet liittyvät IoT-laitteiden määrään, yleisten laitestandardien puutteeseen ja IoT-laitteiden toiminnallisiin rajoitteisiin.

Asiasanat: Esineiden internet, teollinen esineiden internet, Industry 4.0, kyberfyysiset järjestelmät, kyberturvallisuus, elinkaari

ABSTRACT

Kekki, Juuso
The cybersecurity during industrial IoT devices lifecycle
Jyväskylä: University of Jyväskylä, 2023, 31 pp.
Information Systems Science, bachelor's thesis
Supervisor: Vuorinen, Jukka

IoT devices are beginning to be used in many different environments and the increase in its use is constantly increasing. The use of IoT equipment in an industry is associated with Industry 4.0 and many concepts such as Industrial Internet of Things (IIoT) and cyber-physical systems. There's a lot of literature and many studies on the use of IoT equipment in industrial environments. This literature review focuses on the cybersecurity in industrial IoT devices life cycle and the challenges that arise during it. This literature review begins with explaining the concepts of IIoT, Industry 4.0 and cyber-physical systems, followed by the life cycle of an IoT device and then reviewing literature about cybersecurity during the IoT life cycle and the challenges that arise during it. The study shows that the main challenges relate to the number of IoT devices, the lack of general device standards and the operational constraints of IoT equipment.

Keywords: Internet of Things, Industrial Internet of Things, Industry 4.0, cyber-physical systems, cybersecurity, lifecycle

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Teollisen esineiden internetin (Industrial Internet of Things, IIoT) viime aikoina lisääntynyt käyttö teollisuusympäristöissä on lisännyt kyberhyökkäysten määrää. Kyberhyökkäykset eivät uhkaa pelkästään laitteiden turvallisuutta vaan myös teollisia infrastruktuureita, henkilöstöä ja asiakkaita. Vuonna 2009 haittaohjelma manipuloi sentrifugien nopeutta ydinrikastuslaitoksessa, mikä sai ne riistäytymään käsistä. Tämä haittaohjelma, joka tunnetaan nykyään nimellä Stuxnet, pääsi eristetyn järjestelmän sisälle, muistitikun kautta ja levisi itsenäisesti tuotantoverkkoihin. (Zetter, 2014.) Stuxnet on yksi ensimmäinen merkittävä kyberhyökkäys ja esimerkki siitä, kuinka vaarallisia kyberhyökkäykset voivat pahimmillaan olla. Teolliset järjestelmät on tunnetusti suunniteltu toimimaan eristyksessä internetistä, mutta IoT-laitteiden integrointi luo tähän poikkeuksen ja tekee niistä alttiita kyberhyökkäyksille. Waslon ym. (2017) mukaan kyberriskeihin puuttumisen harkitseminen strategisen prosessin lopussa on yksinkertaisesti liian myöhäistä, minkä takia Waslon, Lewisin, Hajjin ja Cartonin (2017) mielestä kyberturvallisuuden tulisi tulla olennainen osa strategiaa, suunnittelua ja toimintaa. Tämän kirjallisuuskatsauksen tavoitteena on tutkia teollisten IoT-laitteiden elinkaarta ja sen aikaista kyberturvallisuutta. Tavoitteena on antaa hyvä yleiskuva teollisten IoT-laitteiden kyberturvallisuudesta ja auttaa sen ymmärtämisessä.

Tämä kirjallisuuskatsaus keskittyy käsittelemään teollisten IoT-laitteiden elinkaaren kyberturvallisuutta ja siihen liittyviä haasteita. Tutkielmalla pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Miten kyberturvallisuus otetaan huomioon IIoT-laitteiden elinkaaren aikana?
- Minkälaisia kyberturvallisuuden haasteita esiintyy elinkaaren aikana?

Tutkimus alustetaan käymällä läpi aiheeseen liittyviä keskeisimpiä käsitteitä, joihin kuuluvat kyberfyysiset järjestelmät, teollinen esineiden internet, Industry 4.0 ja kyberturvallisuus. Tämän jälkeen lukijalle muodostetaan yleiskäsitys IoT-laitteen elinkaaresta yhdistelemällä eri lähteiden tarjoamia malleja.

Kyberturvallisuus liitetään elinkaaren vaiheisiin omassa luvussaan, jossa käsitellään myös kunkin vaiheen turvallisuus haasteita. Tutkimuksen lopussa käydään läpi keskeisimmät tutkimustulokset ja vastaukset tutkimuskysymyksiin.

Tutkimuksessa on pyritty käyttämään mahdollisimman ajankohtaisia, relevantteja ja vertaisarvioituja lähteitä. Lähteitä on haettu ACM Digital Library, IEEE Xplore ja ScienceDirect tietokantoja, sekä Google Scholar hakupalvelua. Hakusanoina on käytetty termejä kuten cybersecurity, lifecycle, IoT, IIoT, Industry 4.0 ja security challenges. Tutkimus on aloitettu IoT-laitteen elinkaaren määrittelystä. Tämän jälkeen jokaiseen vaiheeseen on pyritty löytämään kirjallisuutta, joka käsittelee vaihetta tarkemmin teollisuuden ja kyberturvallisuuden näkökulmista. Tutkimukseen valittu kirjallisuus käsitteli pääasiassa kyberturvallisuutta ja sen haasteita teollisuuden näkökulmasta.

Tutkimuksessa pyritään ottamaan huomioon kyberturvallisuudessa tapahtuvat muutokset. Kyberturvallisuus saattaa olla asia, jonka organisaatio huomioi alussa mutta ajan kuluessa unohtaa. Tällä tutkimuksella pyritään herättämään ajattelutapa, jossa kyberturvallisuus nähdään elävänä ja jatkuvasti muuttuvana asiana, jota ei ole syytä jättää huomioimatta missään elinkaaren vaiheessa.

2 ESINEIDEN INTERNET TEOLLISUUDESSA

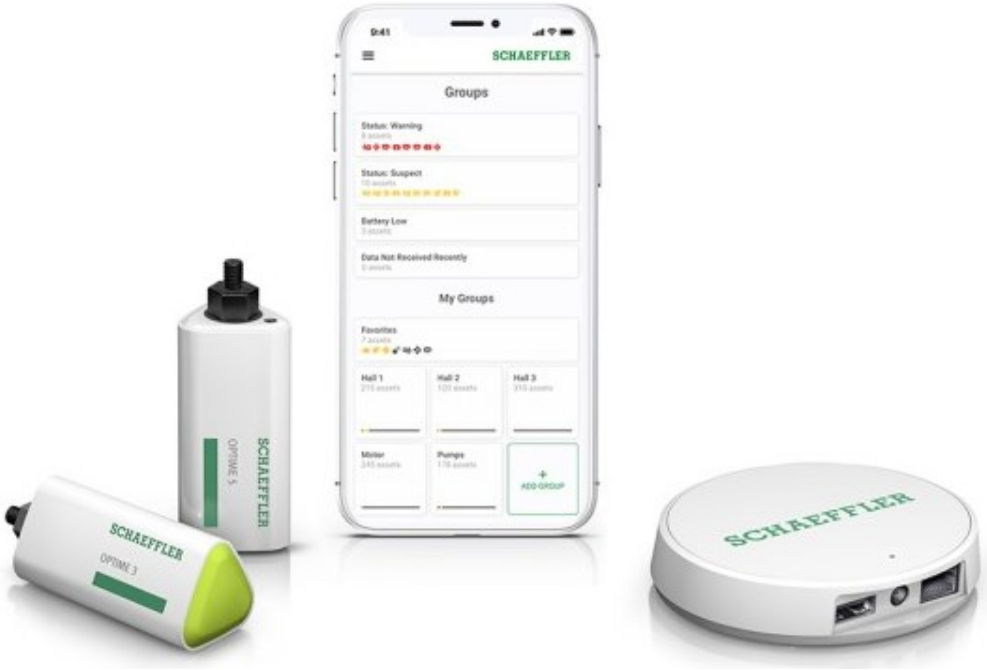
Tämä luku käsittelee yleisesti käsitettä Teollinen esineiden internet (IIoT). Luvussa avataan konsepteja, joihin IIoT liittyy. Keskeisiä käsitteitä ovat kyberfysikaaliset järjestelmät (CPS) ja Industry 4.0. Luvussa on havainnollistettu IIoT arkkitehtuuria ja esimerkkinä on käytetty Schaefflerin OPTIME-järjestelmää.

2.1 Kyberfyysiset järjestelmät

Kyberfyysisille järjestelmille (Cyber-Physical System, CPS) löytyy useita määritelmiä, eikä yhtä yleisesti hyväksyttyä määritelmää ole. Humayedin, Linin, Lin ja Luon (2017) mukaan CPS on järjestelmä, jota käytetään fyysisen maailman seuraamiseen ja hallitsemiseen. Xun, Yun, Griffithin ja Golmien (2018) mukaan kyberfyysiset järjestelmät koostuvat kahdesta osasta fyysisestä- ja kyberjärjestelmästä. Xu ym. (2018) mainitsevat että fyysiseen järjestelmään voi kuulua erilaisia komponentteja, kuten sensoreita, laitteita ja tuotantolaitoksia. Kyberjärjestelmään heidän mukaansa kuuluvat ohjaus-, verkostoitumis- ja laskentainfrastruktuurit. Fyysisiä järjestelmiä ovat esimerkiksi valmistus- ja automaatiojärjestelmät, jotka auttavat teollisuuslaitteita hoitamaan määrätyt tuotanto- ja automaatiotehtävät. Kyberjärjestelmät mahdollistavat teollisuusjärjestelmien toiminnan, yhteen liittämisen ja älykkyyden (Xu ym., 2018).

Kyberfyysisiä järjestelmiä käytetään monilla eri toimialoilla, kuten tuotanto-, kuljetus-, energia- ja terveydenhuoltoaloilla. Boyesin, Hallaqin, Cunninghamin ja Watsonin (2018) mukaan erottava tekijä kyberfyysisten järjestelmien ja perinteisten tieto- ja viestintäjärjestelmien välillä on niiden vuorovaikutus fyysisen maailman kanssa. Tiedon ja datan käsittelyn lisäksi kyberfyysiset järjestelmät keskittyvät fyysisten prosessien hallintaan, jossa käytetään apuna fyysistä komponenteista saatua tietoa (Boyes ym., 2018). Kyberfyysisten järjestelmien keskeisin etu on niiden kyky kommunikoida ja jakaa tietoja eri järjestelmien ja alustojen välillä. Niiden avulla voidaan myös tehostaa prosesseja ja auttaa päätöksenteossa.

Kyberfyysisillä järjestelmillä on myös ainutlaatuisia turvallisuushaasteita, joita tässä työssä käsitellään myöhemmin.
Esimerkki kyberfyysisestä järjestelmästä on Schaefflerin OPTIME huoltojärjestelmä. OPTIME-järjestelmä koostuu kuvassa (Kuvio 1) näkyvistä kolmesta komponentista, joita ovat värähtely- ja lämpötila-anturit, tietoliikenneväylä ja digitaalinen palvelu. Järjestelmän anturit kiinnitetään valvottaviin laitteisiin seuraamaan niiden lämpötilaa ja värähtelyä. Tietoliikenneväylä yhdistyy antureihin ja tallentaa niiden välittämän datan pilveen. Digitaalinen palvelu analysoi pilveen tallennettua dataa ja luo sen pohjalta diagnostiikka raportteja laitteiden kunnosta. Raportteja voi tarkastella mobiililaitteella tai tietokoneella ja niiden avulla voidaan ennakoida tarvittavia huoltoja. (Schaeffler Finland Oy, ei pvm.)



KUVIO 1 Schaeffler OPTIME huoltojärjestelmä (Schaeffler Finland Oy, ei pvm.)

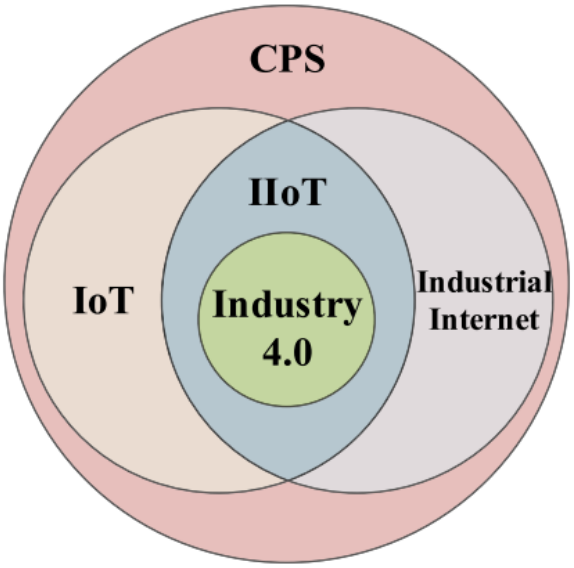
2.2 Teollinen esineiden internet

Teollinen esineiden internet (Industrial Internet of Things, IIoT) on käsitteenä osa laajempaa esineiden internet (Internet of Things, IoT) kokonaisuutta. IIoT viittaa erityisesti IoT-teknologian käyttöön teollisuus- ja valmistusympäristöissä. IIoT käsitteelle löytyy useita määritelmiä, joista Boyes ym. (2018) tarjoaa yksinkertaisen määritelmän, jonka mukaan IIoT:n määritelmä olisi tiettyjen IoT-tekniikoiden ja älyobjektien käyttö kyberfyysisissä järjestelmissä teollisessa ympäristössä teollisuuden tavoitteiden edistämiseksi. IIoT mahdollistaa teollisten laitteiden havaitsemisen ja yhteen liittämisen soveltamalla uusia IoT-teknologioita teollisuuden valmistus- ja automaatiojärjestelmissä (Xu ym., 2018).

Esineiden internet on vaikuttanut teollisuuteen ja tuonut uusia etuja kuten: Lyhyemmät tuotantosyklit, joiden avulla asiakkaiden tarpeet voidaan ottaa huomioon reaaliajassa. Ylläpito on mahdollista toteuttaa suurelta osin automaattisesti. Tilaukset voidaan täyttää automaattisesti oikeassa järjestyksessä ja lähetetään asiakkaille. (Pereira, Barreto & Amaral, 2017.) Yksi IIoT:n keskeisistä hyödyistä on sen kyky auttaa ennakoivaa ylläpitoa, johon kuuluu data-analytiikan käyttö mahdollisten ongelmien tunnistamiseksi ennen niiden ilmaantumista. Tästä toimii esimerkkinä tekstissä aiemmin esitelty Schaefflerin OPTIME-järjestelmä. Tällaiset järjestelmät voivat auttaa ennakoimaan vikaantumista, lyhentämään käyttökatkoja, parantamaan turvallisuutta ja pidentämään laitteiden käyttöikää (Schaeffler Finland Oy, ei pvm.). Muita IIoT:n tuomia hyötyjä ovat edistyneempi toimitusketjun seuranta ja omaisuudenhallinta, sekä tehokkuuden ja tuottavuuden lisääntyminen. IIoT voi kuitenkin tuoda mukanaan haasteita, kuten tietoturvaan, yksityisyyden suojaan, sekä vanhojen järjestelmien integraatioon liittyviä ongelmia.

2.3 Industry 4.0

Neljänneksi teolliseksi vallankumoukseksi määritelty Industry 4.0 on Saksan hallituksen vuonna 2011 tekemän aloite, jonka tavoitteena oli vaihtaa ja kerätä tietoa tuotteiden elinkaaren ajalta (Khan ym., 2020). Nykyisn Industry 4.0 tunnetaan älykkäiden koneiden yhteyksien lisääntymisenä teollisuudessa. Industry 4.0 pyrkii yhdistämään digitaalisen maailman ja fyysiset toiminnallisuudet edistääkseen älytehtaita ja mahdollistamaan edistynyttä tuotantoa (Waslo ym., 2017). Vallankumoukselle on tunnusomaista se, että siinä luotetaan CPS-järjestelmiin, jotka kykenevät kommunikoimaan keskenään ja tekemään itsenäisiä päätöksiä. Tavoitteena on lisätä teollisuuden tehokkuutta, tuottavuutta, turvallisuutta ja avoimuutta (Boyes ym., 2018). Kyberfyysiset järjestelmät, IIoT ja Industry 4.0 liittyvät käsitteinä toisiinsa ja niiden väliset suhteet on havainnollistettu Venn-diagrammilla (Kuvio 2).



KUVIO 2 CPS, IoT, Industrial Internet, IIoT and Industry 4.0 (Qiu ym., 2020, s. 2463)

Vaikka Industry 4.0 parantaa digitaalisia valmiuksia koko valmistus- ja toimitusketjun osalta ja mahdollistaa laitteiden toisiinsa kytkemisen, se tuo mukanaan myös uusia riskejä, joihin teollisuus ei ole valmistautunut (Waslo ym., 2017). IoT-laitteiden integrointi luo laajoja laite verkostoja, jotka voivat olla huonosti suojattuja. Kyberrikolliset voivat hyväksikäyttää laitteiden haavoittuvuuksia päästäkseen käsiksi arkaluontoisiin tietoihin tai häiritäkseen teollisten järjestelmien toimintaa aiheuttaen merkittävää vahinkoa valmistusprosesseille ja yrityksen muulle toiminnalle. Tämän takia kyberturvallisuus on hyvä huomioida jokaisessa järjestelmän elinkaaren vaiheessa.

2.4 Kyberturvallisuus

Käytettäessä IT-laitteita voidaan olettaa, että laitteen toiminta tulee jollain tavalla poikkeamaan suunnitellusta. Singerin ja Friedmanin (2014) mukaan poikkeamaa kutsutaan toimintahäiriöksi. Toimintahäiriöt eivät kuitenkaan aina ole turvallisuusongelmia. Kun toimintahäiriö johtuu vastapuolesta, eikä yksinkertaisesta virheestä tai onnettomuudesta on kyseessä turvallisuusongelma. Singerin ja Friedmanin (2014) mukaan turvallisuuteen liittyy vastustajan läsnäolo, joten sen toteuttamiseen tarvitaan ainakin kaksi osapuolta. Singer ja Friedman (2014) mainitsevat kirjassaan, että asiat saattavat mennä rikki ja virheitä voi tapahtua, mutta kyberongelmasta tulee kyberturvallisuuskysymys vain, jos vastapuoli pyrkii hyötymään siitä esimerkiksi hankkimalla yksityisiä tietoja, heikentämällä järjestelmää tai estämällä sen käytön. Kyberturvallisuuden tavoitteet pohjautuvat käsitteeseen uhasta ja perinteisesti niiden kolme tavoitetta on taata luottamuksellisuus, eheys ja käytettävyys. Nämä tavoitteet tunnetaan myös CIA-mallina

(confidentiality, integrity, availability, CIA) (Singer & Friedman, 2014). CIA-malli on havainnollistettu kuviossa (Kuvio 3).

KUVIO 3 CIA-malli

Singer ja Friedman (2014) kirjoittavat että luottamuksellisuudella tarkoitetaan tietojen luottamuksellisuutta. Schiller ym. (2022) määritelmä tästä turvallisuustavoitteesta on: viesti on luottamuksellinen, jos vain lähettäjä ja vastaanottaja tietävät sen olemassaolosta. Chhetrin, Rashidin, Faeziin ja Al Faruquen (2017) mukaan Industry 4.0:aan liittyy paljon tietovirtoja, joita hyökkääjät voivat voivat salakuunnella ja käyttää hyväksi. Luottamuksellisuuden menetys voi tulla yrityksille kalliiksi, koska yritykset voivat menettää asiakastietoja, teollis- ja tekijänoikeuksia ja liikesalaisuuksia (Chhetri ym., 2017). Singerin ja Friedmanin (2014) mukaan digitaalisen maailman informaatio on arvokasta ja siksi sen suojelu on tärkeää. Luottamuksellisuutta tuetaan teknisillä välineillä, kuten salauksella ja kulunvalvonnalla sekä oikeusturvalla (Singer & Friedman, 2014).

Singerin ja Friedmanin (2014) mukaan eheydellä tarkoitetaan sitä, että järjestelmää ja siinä olevia tietoja ei ole muutettu väärin tai muutettu ilman lupaa. Schiller ym. (2022) mainitsevat, että eheys voidaan osoittaa esimerkiksi sillä, että viestin sisältö on lähettäjälle ja vastaanottajalle sama. Eheyteen kuuluu järjestelmän kautta virtaavan tiedon johdonmukaisuus, täsmällisyys ja luotettavuus, sekä fyysisten komponenttien yhtenäisyys ja luotettavuus tuotteen koko elinkaaren ajan (Chhetri ym., 2017). Tämän lisäksi Singerin ja Friedmanin (2014) mukaan on luotettava siihen, että se käyttäytyy odotetusti.

Käytettävyydellä tarkoitetaan sitä, että järjestelmää voidaan käyttää odotetulla tavalla. Se että järjestelmää ei ole saatavilla ei Singerin ja Friedmanin (2014) mielestä yksinään ole turvallisuusongelma. Turvallisuusongelma syntyy, kun jokin taho yrittää jollain tavalla hyötyä käytettävyyden puutteesta esimerkiksi riistämällä käyttäjiltä järjestelmän, josta he ovat riippuvaisia tai uhkaamalla järjestelmän menettämisellä (Singer & Friedman, 2014). Kyberfyysiset hyökkäykset voivat johtaa siihen, että tuotantojärjestelmät ovat poissa käytöstä. Chhetrin ym.

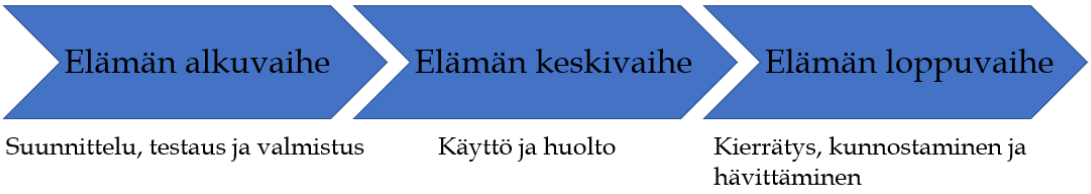
(2017) mukaan hyvin toteutetussa Industry 4.0:ssa voidaan käytettävyyteen kohdistuvia hyökkäyksiä lieventää hajautetun arkkitehtuurin avulla. Teollisuudessa kriittisten järjestelmien käytön estäminen voi johtaa prosessiketjun pysähtymiseen ja mahdollisiin taloudellisiin tappioihin.

Verrattuna perinteiseen tietotekniikan turvallisuuteen Chhetrin ym. (2017) mukaan tuotantojärjestelmien toiminnanohjausteknologiat ovat alttiimpia hyökkäyksille, koska ne ovat integroitu tiukemmin IT-infrastruktuuriin. Singer ja Friedman (2014) mainitsevat että on tärkeää tunnistaa turvallisuuden rajat, koska turvallisuuteen liittyy aina jonkinlainen vaihtokauppa. Turvallisuus maksaa rahaa, sekä siihen joutuu uhraamaan aikaa, mukavuutta, voimavaroja ja vapauksia (Singer & Friedman, 2014). Tätä Singerin ja Friedmanin (2014) mainitsemaa vaihtokauppaa tarkastellaan myöhemmin tässä tekstissä, kun käsitellään IIoT-laitteiden kyberturvallisuuden eri haasteita.

3 IoT-LAITTEIDEN ELINKAARI

Tässä luvussa käydään läpi IoT-laitteiden elinkaarta. Elinkaari jaetaan kolmeen vaiheeseen, joita käsitellään omissa kappaleissaan tarkemmin. Kappaleessa käytetty elinkaarta tarkasteleva esimerkki keskittyy teolliseen näkökulmaan ja IIoT:hen.

IoT-laitteiden elinkaari voidaan jakaa kolmeen vaiheeseen, kuten minkä tahansa teollisuuden tuotteen ja tuotteen kehityksen kohdalla: elinkaaren alku (Beginning of Life, BoL), elinkaaren keskivaihe (Middle of Life, MoL) ja elinkaaren loppu (End of Life, EoL) (Späthe, 2021). Nämä päävaiheet voidaan jakaa vielä Yousefnezgadin, Malhin ja Främlingin (2020) mukaan alaluokkiin, jotka näkyvät kuvassa (Kuvio 3). Elinkaaren alkuvaiheeseen sisältyy suunnittelu, testaus ja tuotanto. Keskivaihe sisältää käyttövaiheen ja huollon. Kierrätys, kuunostaminen ja laitteen hävittäminen kuuluvat loppuvaiheeseen (Yousefnezgad ym., 2020). IoT-laiteen elinkaaren alkuvaihe sisältää laitteen valmistuksen, sekä siirtymisen keskivaiheeseen, johon kuuluu laitteen myyminen ja asennus. Elinkaaren keskivaihe on laitteen käyttövaihe, joka sisältää käytön lisäksi ylläpitoon liittyviä toimenpiteitä. Elinkaaren loppuvaiheessa laitteen asennus puretaan ja laite poistetaan käytöstä. Späthen (2021) mukaan siirtymä asennusvaiheesta käyttövaiheeseen kuuluu elinkaaren keskivaiheeseen, mutta tässä tekstissä käytetään Yousefnezgad ym. (2020) tarjoamaa rakennetta, jossa asennus on sisällytetty elinkaaren alkuvaiheeseen.



KUVIO 4 Tuotteen elinkaaren vaiheet (Yousefnezgad ym., 2020, s. 8).

3.1 Elinkaaren alkuvaihe

Soós, Kozma, Janky ja Varga (2018) sanovat että suunnittelu vaiheessa on tärkeä kerätä uuden IoT-laitteen vaatimukset ja toteuttaa niistä suunnitelma. Suunnittelun aikana tehdään laitteen kannalta sitovia päätöksiä, jotka vaikuttavat erilaisiin ominaisuuksiin, kuten laitteisto- ja ohjelmistoalustaan, viestintätyyppiin, analysointiin, tallennukseen, hälytyksiin, verkon konfigurointiin, tietoturvaan, laitteistojen- ja ohjelmistojen asennukseen (Soós ym., 2018). Kun laite tai järjestelmä on suunniteltu ja käytettävät osat valittu huomioiden laitteen tarkoitus ja toiminnallisuudet aloitetaan sen valmistaminen. Alkuvaiheessa IoT-laitetta aletaan rakentamaan yksittäisitä komponenteista ja osakokoonpanoista (Späthe, 2021). Vaihe alkaa rakennusvaiheesta ja siitä on vastuussa laitevalmistaja. Rakennus vaiheeseen kuuluvat laitelaitteiston rakentaminen, sekä tehtaan alkuperäisten laiteohjelmistojen asentaminen. Lopputuotetta, laitetta tai järjestelmää ei ole vielä olemassa. Rahmanin, Ozcelebin ja Lukkienin (2018) mukaan alkuvaiheen tulisi noudattaa tuotekehityksen yleistä elinkaarta, joka kattaa määrittelyn, suunnittelun, toteutuksen sekä testauksen.

Späthe (20219 sanoo, että yksi valmistusprosessin kriittisimmistä vaiheista on laitetason lopputestaus. Tämän jälkeen, kun testit onnistuvat vakio ohjelmisto asennetaan tai aktivoidaan ja konfiguroidaan tehdasasetuksilla. Viestinnän ja tiedonvaihdon toimivuuden tarkistus päättää laitteiston testauksen. Tarkistamalla viestinnän toimivuus varmistetaan, että langaton viestintä toimii oikein ja kaikki tarvittavat laitetiedot ovat saatavilla. Lopuksi laitteelle asetetaan varmennusominaisuudet ja tunnistetiedot turvallisen viestintäkanavan luomiseksi, sekä salausavaimet viestintäkumppanien todentamista ja ohjelmistopäivityksien varmentamista varten. (Späthe, 2021.)

Kun laite tai järjestelmä on todettu toimivaksi, sen omistajuus vaihtuu, ja uusi omistaja ottaa sen käyttöön. Laite voi vaihtaa omistajaa useita kertoja ennen kuin se päätyy lopulliselle käyttäjälle. Lopullisen omistajan selvittyä laite siirretään fyysisesti paikkaan, jossa sitä aiotaan käyttää ja aloitetaan sen asennus. Laitteen käyttötarkoituksen mukainen fyysinen käyttöpiste voi olla kiinteä tai liikkuva. Laitteen asennuksessa laite valmistellaan verkon sisäistä käyttöä ja turvallista viestintää varten. (Späthe, 2021.) Rahman ym. (2018) mainitsevat käyttöönottovaiheeseen liittyviä toimenpiteitä kuten laitteen sijainnin- ja ryhmätietojen, toiminnallisten parametrien, salausmateriaalien konfiguroinnin, sekä laitteen alustamisen ja suojattuun verkkoon lisäämisen. Käyttöönottovaiheen jälkeen laite on käyttövalmis ja se siirtyy elinkaarensa keskivaiheeseen, jossa laitteen käyttö sille tarkoitetulla tavalla alkaa.

3.2 Elinkaaren keskivaihe

Elinkaaren keskivaiheessa laitetta käytetään sille tarkoitetulla tavalla. Käyttö vaiheessa voidaan käsitellä tai analysoida laitteen keräämää dataa, käyttää laitteen eri toimintoja, sekä muuttaa laitteen käyttämiä hallinta-arvoja (Späthe, 2021). Esimerkkinä Schaefflerin OPTIME-järjestelmää käytettäessä sovellus ja huoltoasentajat analysoivat anturien mittaamaa dataa, jonka avulla tuotantokoneiston kuntoa voidaan seurata. OPTIME-järjestelmä varoittaa huoltoasentajaa poikkeuksista ja asentaja voi määritellä mistä ja milloin varoituksia annetaan.

Käytön ohella laitteita monitoroidaan ja huolletaan. Laitteen toimintaa seurataan ja siitä kerätään laitekohtaista dataa. Späthen (2021) mukaan laitekohtaiseen dataan voi sisältyä akun tila, virrankulutus, laatuindikaattorit, laitteistoon ja ohjelmistoihin liittyvät virhekoodit, sekä lokitiedot. Späthe (2021) mainitsee että laitteen konfigurointia voidaan tarpeen vaatiessa myös muuttaa. Soós ym. (2018) mukaan uudelleen konfigurointeja voi tapahtua useita kertoja laitteen käyttöiän aikana. Konfiguraation aikana laite ei saa uusia ominaisuuksia, mutta sen käyttäytyminen tai ympäristöasetukset muuttuvat (Soós ym., 2018). Laitteistoon voidaan joutua tekemään muutoksia, kuten päivittämään yhteys- tai virranhallinta asetuksia, jos laiteympäristössä tapahtuu muutoksia. Soósin ym. (2018) mukaan useimpien IoT-laitteiden elinkaaren aikana niiden asennuksia on ennemmin tai myöhemmin muutettava. Laitteet voivat esimerkiksi tarvita ohjelmistopäivityksiä tai viankorjauksia (Soós ym., 2018). Tarve laitteen ohjelmistopäivitykselle voi syntyä, mikäli laitteessa ilmenee ongelmia, tai laitetta halutaan päivittää. Päivitykset eivät aina liity suoranaisesti itse laitteeseen. Laiteympäristön viestintä- ja sovelluspalvelut voivat myös vaatia päivityksiä. Laiteohjelmistojen, viestintä- ja sovelluspalvelujen päivittäminen yhdessä mahdollistaa uusien toimintojen toteutuksen. (Späthe, 2021.) Yleisesti päivitykset pyrkivät parantamaan laitteiden ominaisuuksia.

3.3 Elinkaaren loppuvaihe

IoT-laitteen elinkaari tulee päätökseen, kun sen tuki, varaosien saatavuus, ohjelmistojen yhteensopivuus loppuu, käyttö lopetetaan siksi, että se otetaan käyttöön toisessa ympäristössä tai se on määrä vaihtaa laitteen saavuttaessa käyttöikänsä. Soósin ym. (2018) mukaan suurimmat syyt laitteen käytöstäpoistoon ovat osittaiset tai täydelliset vauriot laitteessa, jotka johtuvat laitteen vioista tai ikääntymisestä. Rahmanin ym. (2018) mukaan mikäli laite aiotaan ottaa uudelleen käyttöön, se alustetaan takaisin tehdasasetuksiin, joka mahdollistaa uudelleen käyttöönoton ja yhdistämisen uuteen verkkoon.

Tilanteessa, jossa laitetta ei aiota käyttää uudelleen tulisi Späthen (2021) mukaan toimia seuraavasti: laitteesta tulisi poistaa sisäiset käyttötiedot ja oikeudet annettuihin resursseihin, laite tulisi vapauttaa tehtävästään, sekä poistaa

käyttöpisteestä. Elinkaaren viimeisenä vaiheena laite tuhotaan ja riippuen laitteesta joitakin sen osia voidaan käyttää uudelleen tai kierrättää (Späthe, 2021). Tämä vaihe on IoT-laiteen käyttöiän loppu ja päättää laitteen elinkaaren.

4 IIoT-LAITTEIDEN ELINKAAREN KYBERTURVALLISUUS

Tässä luvussa käydään läpi elinkaaren eri vaiheisiin liittyvää kyberturvallisuutta ja vaiheisiin liittyviä turvallisuushaasteita. Kyberturvallisuus on jaettu samalla tavalla alku-, keski- ja loppuvaiheeseen kuin edeltävässä luvussa. Haasteet liitetään myös aiemmin tekstissä esiteltyyn CIA-malliin.

IoT:n käyttö laajentaa hyökkäyspintoja ja monet tekijät vaikuttavat turvallisuusriskeihin. IoT-järjestelmillä ei välttämättä ole tarkkoja rajapintoja ja rajapinnat muuttuvat jatkuvasti. Lisäksi voi olla vaikeaa määrittää kaikki ne laitteet, jotka IoT-järjestelmä sisältää. Bertino (2019) mainitseekin että IoT-järjestelmät ovat monimutkaisia kokonaisuuksia, jotka koostuvat erilaisista järjestelmän osista, jotka voivat olla eri osapuolten hallitsemia tai omistamia. Bertinon (2019) mukaan ihmisten vuorovaikutus järjestelmien kanssa vaikuttaa myös turvallisuuteen. IIoT-järjestelmien pitkä käyttöikä, jatkuvan toiminnan tarve, sekä vanhentuneet toimintatavat aiheuttavat myös monia turvallisuusriskejä (Bertino, 2019).

IoT voi kohdata lähitulevaisuudessa monia uusia uhkia. Tämän takia Yousefnezgad ym. (2020) mukaan on tärkeää tietää, mistä turvallisuushaasteista tulisi olla huolissaan kussakin elinkaaren vaiheessa, koska myöhempien vaiheiden haasteita voidaan ehkäistä suunnittelemalla ja kehittämällä turvallinen järjestelmä ensimmäisestä vaiheesta lähtien. Tämän vuoksi seuraavissa luvuissa käsitellään elinkaaren kyberturvallisuutta ja siihen liittyviä haasteita.

4.1 Kyberturvallisuus elinkaaren alkuvaiheessa

4.1.1 Kyberturvallisuuden toteutus elinkaaren alkuvaiheessa

Kyberuhkiin valmistautuminen on tärkeää hyökkäysten ehkäisemisen ja estämisen kannalta. Valmistavia toimia ovat datan ja viestinnän salaaminen, palomuurien asennus ja oikeuksien hallinta, sekä laitteen haavoittuvuuksien testaus

(Bertino, 2019). Alkuvaiheessa pyritään suunnittelemaan ja valmistamaan luotettava, sekä eheä IoT-laite. Lisäksi suunnittelu ja valmistus vaiheessa pyritään varmistamaan luottamuksellisuus, jotta IoT-laitteiden suunnitelmat eivät päätyisi väärille henkilöille.

Fagan, Megas, Scarfone ja Smith (2020) tuovat esille laitevalmistajan näkökulman, jossa laitteen elinkaaren kyberturvallisuus koostuu markkinavaihetta edeltävistä ja markkinavaiheen jälkeisistä toimista. Markkinavaihetta edeltävät toimet kattavat valmistajan toimet ennen kuin laitetta markkinoidaan ja se myydään asiakkaille. Markkinavaiheen jälkeiseen vaiheeseen kuuluvat kaikki toimet, joita valmistaja toteuttaa IoT-laitteelle sen myynnin jälkeen. Yleisesti ottaen valmistajat pystyvät vaikuttamaan parhaiten laitteiden kyberturvallisuuteen ennen markkinavaihetta, koska sen jälkeen muutosten tekeminen on yleensä monimutkaisempaa ja kalliimpaa. Laitteiden valmistajien tulisi Fagan ym. (2020) mukaan toteuttaa muun toiminnan rinnalla seuraavat olennaiset kyberturvallisuus toimet: Ensimmäiseksi tulisi tunnistaa ja määrittää odotetut asiakkaat sekä käyttötapaukset, jotta voidaan määrittää mitkä kyberturvallisuusominaisuudet laitteeseen tulisi toteuttaa. Seuraavaksi tulisi selvittää asiakkaan kyberturvallisuustarpeet ja tavoitteet, sekä lopuksi tulee päättää, miten ne toteutetaan ja miten niitä tuetaan asianmukaisesti. (Fagan ym., 2020.)

Elinkaaren alun kyberturvallisuus kattaa suunnittelun lisäksi laitteen valmistamiseen ja käyttöönottoon liittyvät toimet. Valmistusvaiheessa laitteeseen asennetaan tehtaalla valmistajan tehdasasetukset. Kun laite on valmistettu, voidaan se sijoittaa käyttöpisteeseen ja asentaa laitesertifikaatit, joiden avulla laite voidaan yksilöidä muista laitteista ja tunnistaa myöhemmin. Yousefnezgadin ym. (2020) mukaan IoT-ympäristössä tulisi olla vahva tunnistautuminen, jotta se voidaan rakentaa turvalliseksi. Käyttöönoton aikana laitteet muodostavat luotettavan yhteyden käyttäjien ja laitteiden välille. Kaikki kyberhyökkäyksiä lieventävät toimenpiteet tulisi toteuttaa heti elinkaaren alussa, koska haavoittuvuus vaarantaa koko järjestelmän, ja siksi on tärkeää ottaa huomioon turvallisuusvaatimukset kuten tunnistautuminen, kulunvalvonta, luottamuksellisuus, järjestelmän eheys ja -käytettävyys. (Yousefnezgad ym., 2020.)

4.1.2 Kyberturvallisuuden haasteet elinkaaren alkuvaiheessa

Syitä elinkaaren alun haasteisiin on monia. Yu ja Guo (2019) mainitsevat yhtenä esimerkkinä sen, että perinteisesti teollisuuden järjestelmät on suunniteltu toimimaan eristyksessä tietoteknisestä infrastruktuurista ja kyberturvallisuutta ei ole otettu huomioon. Yhteenliitettyjen laitteiden lisääntyminen lisää myös mahdollisia hyökkäyspintoja ja siten järjestelmien haavoittuvuutta (Yu & Guo, 2019). Bertino (2019) mainitsee sen, että tietoturvaloukkaukset johtuvat usein konfiguraatiovirheestä, kuten väärin määritellyistä palomuureista tai käyttöluvista.

Alun haasteisiin kuuluu myös laitteen fyysinen turvallisuus, joka turvaa laitteen osat, joihin voi päästä fyysisesti käsiksi. Yousefnezgad ym. (2020) lainaavat tekstissään Bertinoa ja Islamia (2017), jotka mainitsevat IoT-ympäristöissä käytettävien laitteiden kuten USB-muistitikkujen käytön uhkana laitteiden turvallisuudelle. Serror, Hack, Henze, Schuba ja Wehrle (2020) tuovat esille IIoT-

laitteista syntyvän datan määrän ja tähän liittyvän haasteen tietojen luottamuksellisuuden osana. Haasteena on varmistaa datan luottamuksellisuus ja samalla mahdollistaa sen käytettävyys, jotta IIoT-laitteet voivat prosessoida ja analysoida sitä (Serror ym., 2020). Tietomurto IIoT-järjestelmissä voi johtaa katastrofaaliseen tilanteeseen ja siksi tietojen luottamuksellisuus on vakava turvallisuushaaste. Shafiquen, Khawajan, Sabirin, Qazin ja Mustaqimin (2020) mukaan dataa tulisi suojata salakuuntelulta ja dataan sekaantumiselta. Yu ja Guo (2019) sanovat, että datan suojaaminen ratkaistaan yleensä salaamalla järjestelmän käyttämä data, mutta sen toteutukselle on rajoitteita. Datan salausta rajoittaa IoT-laitteiden rajallinen virrankulutus ja laskentateho, sekä suuri datan määrä (Yu & Guo, 2019).

Yksi elinkaaren alun kyberturvallisuuden haasteista liittyy sertifikaattien asennukseen, jolloin jokaiselle laitteelle luodaan identiteetti, jota käytetään myöhemmin auditoinnissa ja laitteiden välisessä viestinnässä. Laitteiden yksilöiminen voi olla haasteellista. Syynä tähän on laitteiden määrän jatkuva kasvu (Cirne ym., 2022).

Viestinnän turvaamisessa haasteita voi syntyä, kun uusien laitteiden salausavaimille muodostetaan pareja jo olemassa olevien laitteiden avaimien kanssa. Salausavainten muodostaminen edellyttää IoT-laitteelta laskutoimitusten suoritusta mikä ei sovellu resurssirajoitteisille laitteille. Salausavaimet voidaan vaihtoehtoisesti myös esiasentaa, mutta tätä ei voida olettaa kaikilta laitevalmistajalta. (Yu & Guo, 2019.)

Tulevaisuudessa verkkoon liitettyjen laitteiden määrä tulee kasvamaan ja siksi Shafiquen ym. (2020) mukaan IoT-arkkitehtuurin on tuettava määrän kasvua. Haasteena IoT:n onnistuneessa käyttöönotossa on tasapainon löytäminen skaalautuvuuden, virrankulutuksen ja kustannusten välillä. Toisena haasteena onnistuneessa käyttöönotossa Shafique ym. (2020) mainitsevat universaalin alustan, protokollien ja ohjelmointikielen puutteen. Koska IoT-laitteet käyttävät erilaisia alustoja ja protokollia. Siksi käyttöönotto vaatii aikaa, jotta laitteet voivat toimia yhteistyössä (Shafique ym., 2020).

Elinkaaren alkuvaiheeseen turvallisuus haasteet koskevat kaikkia CIA-mallin osia, mutta varsinaisesti uhka kohdistuu tässä vaiheessa vain luottamuksellisuuteen ja eheyteen. Chhetri ym. (2017) sanovat että suunnitteluvaiheessa luotetaan vahvasti pilvipalveluihin, kun tuotteista kerätään ja jaetaan tietoja. Tämä on riski luottamuksellisuudelle, koska haavoittuvuudet pilvipalvelussa voi aiheuttaa tietovuodon ja laitteiden suunnitelmat voivat tulla julki, mikä edesauttaa seurata teollis- ja tekijänoikeuksien laiminlyömistä. IoT-laitetta valmistettaessa on myös syitä varmistaa toimittajien luotettavuus. Hyökkääjät voivat Chhetrin ym. (2017) mukaan käyttää kolmansien osapuolien toimittajia porttina yrityksiin. Tämän lisäksi IoT-laitteissa käytettävien osien ja komponenttien eheys kannattaa myös tarkistaa. Hyökkääjät voivat ilmetä joskus ilkeämielisinä myyjinä, jotka saattavat manipuloida tilattuja palveluita tai korvata materiaaleja väärennetyillä tuotteilla vaikuttaakseen tuotteiden eheyteen (Chhetri ym., 2017). Elinkaaren alkuvaiheessa pyritään luomaan mahdollisimman luotettava, eheä, sekä käyttökelpoinen IoT-laite. Vaikka alkuvaiheessa keskitytään käytettävyyteen eivät sitä koskevat haasteet vielä suoranaisesti vaikuta IoT-laitteen turvallisuuteen.

Käytettävyyttä koskevat ongelmat nousevat esille vasta elinkaaren keskivaiheessa, kun laitetta aletaan käyttää.

4.2 Kyberturvallisuus elinkaaren keskivaiheessa

4.2.1 Kyberturvallisuuden toteutus elinkaaren keskivaiheessa

Bertino (2019) kertoo tekstissään, että parhaitenkin valmistellut järjestelmät voivat murtua. Tämä pätee IoT-järjestelmiin, joissa haavoittuvuuksia voi löytyä useista komponenteista ja siksi laitteiden monitorointi on tärkeää. Elinkaaren keskivaiheessa laitetta monitoroidaan käytön ohella jatkuvasti, jotta haavoittuvuudet voidaan havaita ja korjata, sekä niihin voidaan tarvittaessa reagoida. Reagointi hyökkäyksiin on Bertinon (2019) mukaan ratkaisevassa asemassa. Soósin ym. (2018) mukaan etämonitorointi on nykyään pakollinen vaatimus, jotta laitteiden tilaa voidaan seurata ja tukea asianmukaisesti. Hyökkäykseen voidaan reagoida eristämällä hyökkäys, siirtämällä kriittiset toiminnallisuudet toisen järjestelmän vastuulle ja estämällä pääsy kriittisiin resursseihin (Bertino, 2019). Havaitut haavoittuvuudet voidaan korjata ohjelmistopäivityksillä tai muuttamalla laitteiden konfiguraatiota. Päivitysten hallinta on tärkeä osa kyberturvallisuutta, kun havaitaan haavoittuvuus tai järjestelmässä ilmenee ilkivaltaista toimintaa. Myös salausavaimia päivitetään elinkaaren keskivaiheessa salauksen varmistamiseksi esimerkiksi silloin, kun vanha laite poistuu järjestelmästä tai uusi laite liittyy järjestelmään. Keskivaiheessa varmistetaan myös laitteiden yhteisöllinen kyberturvallisuus. Yhteisöllisellä turvallisuudella tarkoitetaan tietoturvaa laitteiden ja palveluntarjoajan välillä. (Yousefnezgad ym., 2020.)

Vaikka laitevalmistajan kannalta laite on jo vaihtanut omistajaa ja laite on käytössä, jatkuu laitevalmistajien rooli asiakkaiden kyberturvallisuuden tukemisessa elinkaaren keskivaiheessa. Markkinavaiheen jälkeisessä vaiheessa laitevalmistajat voivat joutua reagoimaan haavoittuvuusraportteihin ja julkaisemaan kriittisiä turvallisuuspäivityksiä. Fagan ym. (2020) mukaan seuraavat laitevalmistajien toimet edistävät turvallisuutta. Laitevalmistajien tulisi määritellä se, miten asiakas ja laitevalmistaja viestivät keskenään, koska kyberturvallisuustietojen välittäminen voi edellyttää erilaisia viestintätapoja. Valmistajien tulisi myös päättää mitä tietoja valmistaja välittää asiakkaille ja miten tiedot välitetään. Asiakkaat voivat hyötyä siitä, että he tietävät mitä kyberturvallisuuteen liittyviä oletuksia valmistaja teki laitteen suunnittelussa ja kehityksessä, sekä kuinka pitkä käyttöikä laitteella on. Asiakkaalle on myös tärkeää kertoa laiteohjelmistoista, laitteistoista, palveluista, toiminnoista, tietotyypeistä ja ohjelmistopäivityksistä, jotka auttavat asiakasta ymmärtämään ja hallitsemaan kyberturvallisuutta. (Fagan ym., 2020.)

4.2.2 Kyberturvallisuuden haasteet elinkaaren keskivaiheessa

Sadeghi, Wachsmann ja Waidner (2015) tuovat esille teollisten IIoT-järjestelmien hyökkäyspinnat. Älykkäät tehtaat koostuvat useista kyberfyysisistä tuotantojärjestelmistä, jotka sisältävät useita komponentteja esimerkiksi prosessoreita ja muistia, sekä valvontalaitteita, jotka hallitsevat fyysisiä prosesseja sensorien ja koneiden avulla. Komponenttien toiminta perustuu ohjelmistoihin ja vuorovaikutukseen ihmisten tai muiden kyberfyysisten järjestelmien kanssa. Kaikkiin näihin elementteihin kohdistuu kyberhyökkäyksiä. Elektronisiin komponentteihin voi kohdistua fyysisiä laitteisto- tai takaisinmallinnus hyökkäyksiä. Ohjelmistot voivat altistua erilaisille haittaohjelmille ja viruksille. Laitteiden väliseen kommunikaatio voidaan ehkäistä palvelunestohyökkäyksillä ja käyttäjät voivat kohdata manipulointia, sekä tietojenkalastelua. (Sadeghi ym., 2015.) Yousefnezgad ym. (2020) mukaan haasteena onkin vaarojen havaitseminen, koska laitteessa voi ilmetä hallitsematon uhka, jota on usein mahdotonta tunnistaa etukäteen. Suurin osa IIoT-laitteista on kyberfyysisten järjestelmien osia ja siksi Yun ja Guon (2019) mukaan niiden eheys pitäisi pystyä tarkistamaan. Järjestelmän eheys varmistetaan vertaamalla sen lähettämää raporttia järjestelmän tilasta toiseen järjestelmään, joka on tunnetussa ja turvallisessa tilassa. Ohjelmistopohjainen varmentaminen luottaa siihen, että hyökkääjät ovat passiivisia ja varmennusalgoritmit ovat optimaalisia. Laitteistopohjaista varmentamista on tutkittu, mutta se on liian kallista ja monimutkaista käytettäväksi IIoT-järjestelmissä, jotka pyrkivät olemaan edullisia. (Yu & Guo, 2019.)

Yun ja Guon (2019) mukaan yksi esiin nousevista haasteista on IIoT-laitteiden tehokas ja turvallinen hallinta, kun hallittavia laitteita on paljon. Laitehallinnan on tuettava hallintotapoja ja seurantaa useissa vaiheissa, joihin kuuluvat komentojen lähettäminen, monitoroinnin tilan ja toimeksiantojen tulosten seuraaminen, laiteohjelmistojen päivitys, sekä ongelmien ratkominen interaktiivisesti. Laitehallinta sisältää myös salausavainparien, ominaisuuksien ja laitekohtaisen suhteiden hallinnan. Kaikki edellä mainitut asiat voivat muuttua IIoT-laitteen elinkaaren aikana ja ovat perustavanlaatuisia ominaisuuksia IIoT-järjestelmälle. (Yu & Guo, 2019.) Serrorin ym. (2020) mukaan IoT-järjestelmien laitteiden määrästä syntyy haasteita, kun laitteet on otettava käyttöön, konfiguroitava, ja niitä tulee pystyä hallitsemaan. Siksi IIoT-laitteet edellyttävät skaalautuvia ja automaattisia lähestymistapoja kyberturvallisuus toimien toteuttamiseen ja konfigurointiin (Serror ym., 2020).

Serrorin ym. (2020) listaavat haasteita yhteisöllisyyteen ja laitteiden päivittämiseen liittyen seuraavasti: 1) Komponenttien pitkä käyttöikä verrattuna kuluttajien laitteisiin. Haaste ei koske pelkästään uusia laitteita vaan pääasiassa jo käytössä olevia laitteita, joiden kyberturvallisuus on heikko. 2) Laitteiden päivittäminen voi olla vaivalloista, mutta niiden voidaan olettaa olevan käytössä vuosikymmeniä. IIoT yhteyksien lisääntyessä tietoturvariskit lisääntyvät varsinkin silloin, kun aiemmin eristyksissä olleet laitteet on integroitu IIoT verkkoon. 3) Teollisuuden kannalta kriittisten prosessien täytyy olla jatkuvasti toiminnassa eivätkä ne kestä käyttökatkoja. Tällaiset prosessit ovat riippuvaisia tietojen eheydestä, koska pienetkin poikkeamat voivat vaikuttaa tuotannon laatuun.

Turvatoimet saattavat olla ristiriidassa edellä mainittujen vaatimusten kanssa ja siksi turvatoimia täytyy mukauttaa prosesseihin sopiviksi. 4) IIoT-järjestelmien käytönaikaiset haasteet voivat johtua myös inhimillisistä erehdyksistä tai ilkivallasta. Haasteena on IIoT-järjestelmien käyttöoikeuksien määrä. Työntekijöillä, asiakkailla, toimittajilla ja yhteistyökumppaneilla voi kaikilla olla pääsy IIoT-järjestelmään, minkä takia käyttöoikeuksien hallinta vaatii omia menettelytapoja. (Serror ym., 2020.) Tähän liittyy myös haaste, joka koskee asiantuntemuksen ja tietoisuuden puutetta. Haaste liittyy Mentsievin, Guzuevan ja Magomaevin (2020) mukaan ihmisiin, jotka ovat osallisina tuotantoprosesseissa tai osana niiden turvallisuutta. Molemmissa tapauksissa tietoturvan asiantuntemuksessa voi olla puutteita. Mentsiev ym. (2020) kertovat, että tässä tapauksessa tuotantoprosesseihin osallistuvilla henkilöillä ei ole ymmärrystä vaadittavista turvatoimista ja ihmiset, jotka ovat vastuussa tietoturvasta eivät täysin ymmärrä tuotantoprosesseja. Mentsiev ym. (2020) mielestä henkilön tulisi olla pätevä useilla aloilla, jotta kokonaisuus turvallisuudesta tulisi ymmärretyksi.

Elinkaaren keskivaiheen haasteet liittyvät kaikkiin CIA-mallin osiin. Luotettavuus, eheys ja käytettävyys pyritään varmistamaan edellä mainittujen keinojen avulla. Luottamuksellisuuteen liittyviä asioita elinkaaren keskivaiheessa on tietosuoja ja tietojen säilytys, käyttöoikeuksien hallinta, päivitysten julkaiseminen ja laitteiden konfiguraatiot. Valvomalla ja monitoroimalla järjestelmää pyritään varmistamaan, että IoT-laitteiden keräämät ja välittämät arkaluonteiset tiedot pysyvät luottamuksellisina ja suojattuina. Laite- ja käyttöoikeuksien hallinnalla edistetään luottamuksellisuutta, jotta luvattomat käyttäjät eivät pääse käsiksi arkaluontoisiin tietoihin. Luottamuksellisuus esiintyy myös IoT-laitteiden huollossa ja päivityksissä. Päivitykset täytyy jakaa turvallisesti ja varmistaa, että kaikki laitteet päivitetään. Päivitysten yhteydessä tulee myös varmistaa, että laitteiden konfiguraatiot eivät paljastu. Sharman, Jainin, Guptan ja Chamolan (2021) mukaan monitoroinnissa suurin turvallisuushaaste on luottamuksen ylläpitäminen palveluntarjoajan ja käyttäjän välillä. Riippuen siitä kuinka paljon yritys luottaa järjestelmän turvallisuuteen voidaan voimavaroja kohdistaa muualle, kuten eheyden ja käytettävyyden varmistamiseen. IoT-laitteiden ja järjestelmien eheyteen liittyvät haasteet koskevat elinkaaren keskivaiheessa laitetta, dataa, konfiguraatioita, sekä ohjelmistoja ja niiden päivityksiä. IoT-laitteiden keräämien tietojen ja laitekonfiguraatioiden suojaaminen manipuloinnilta on tärkeää eheyden ylläpidossa. Varmistamalla ohjelmistojen eheys voidaan ehkäistä virheet toiminnallisuudessa. Ohjelmistojen eheyttä ylläpidetään päivityksillä ja siksi on myös tärkeää varmistaa, että päivitykset eivät ole viallisia. IoT-laitteiden eheys voi myös kärsiä viallisesta komponentista. Eheydellä voidaan vahvistaa IoT-laitteen käytettävyyttä ja toimintaa, koska eheät järjestelmät ja laitteet toimivat yleensä odotetulla tavalla.

Käyttökatkot vaikuttavat koko IoT-järjestelmän toimintaan. Käyttökatkoihin on monia syitä ja teollisuudessa on tärkeää, että niiden kesto pyritään minimoimaan. Käytettävyyteen vaikuttaa myös laitteiden skaalautuvuus. Industry 4.0 myötä lisääntyvien laitteiden ja datan määrä voi heikentää suorituskykyä ja käytettävyyttä merkittävästi. Sharma ym. (2021) mainitsevat, että IoT-ympäristöt

ovat dynaamisia ja niiden joustavuutta voidaan parantaa uudelleen konfiguroimalla sekä päivittämällä, mutta IoT-laitteiden rajalliset resurssit ovat kuitenkin haaste tällaiselle menetelmälle. Onkin tärkeää varmistaa, että ohjelmistopäivitykset ja laitteistomuutokset ovat yhteensopivia jo olemassa olevien laitteistojen kanssa, koska yhteensopivuus ongelmat voivat myös vaikuttaa käytettävyyteen.

CIA-mallin mukaisesti elinkaaren keskivaiheessa on tärkeää, että resursseja hallitaan järkevästi. Tasapainon löytäminen luottamuksellisuuden, eheyden ja käytettävyyden välillä voi olla haastavaa. Lisäksi turvallisuuden painotus voi muuttua elinkaaren keskivaiheen aikana. Kun uusi järjestelmä otetaan käyttöön voi sen käytössä esiintyä haasteita, mutta nämä haasteet voivat kadota ajan myötä, kun järjestelmää opitaan käyttämään, jolloin resurssit on mahdollista kohdistaa luottamuksellisuuden ja eheyden varmistamiseen. IoT-laite tai järjestelmä voi myös keskivaiheen alussa olla luotettava ja eheä, mutta ajan kuluessa siitä voi paljastua haavoittuvuuksia ja laitteen lähestyessä käyttöikänsä loppua käytettävyys voi heikentyä. Näiden syiden takia voidaan joutua tekemään päätös, että laite poistetaan käytöstä, jolloin se siirtyy elinkaaren loppuvaiheeseen.

4.3 Kyberturvallisuus elinkaaren loppuvaiheessa

4.3.1 kyberturvallisuuden toteutus elinkaaren loppuvaiheessa

Elinkaaren loppuvaiheessa IoT-laite poistetaan käytöstä tai se siirtyy uudelle omistajalle. Kun laite on tarkoitus uudelleenkäyttää, tulisi Yousefnezgadin ym. (2020) mukaan kaikki henkilökohtaiset tai salaiset tiedot poistaa ennen laitteen luovuttamista uudelle omistajalle. Käytöstäpoistossa tietojen poistaminen on tärkeää, jotta järjestelmästä ei vuoda luottamuksellisia tietoja. Tietojen vuotoa voidaan lieventää ymmärtämällä, missä tieto sijaitsee, mitä se on ja miten sitä voidaan suojella (Kissel, Regenscheid, Scholl & Stine, 2014). Faganin ym. (2020) mielestä asiakkaiden auttaminen käytöstäpoistossa on valmistajien vastuulla. Valmistajat voivat auttaa asiakkaitaan ohjeistamalla ja kertomalla eri vaihtoehdoista, kuten mahdollisessa tietojen nollauksessa tai laitteen toimintakelvottomaksi tekemisessä (Fagan ym., 2020).

4.3.2 Kyberturvallisuuden haasteet elinkaaren loppuvaiheessa

Tietojen puhdistaminen on avaintekijä luottamuksellisuuden varmistamisen osalta. Kissel ym. (2014) sanovat, että suuri lähde laittomalle tiedon keruulle on usein pois heitettyjen laitteiden läpikäynti ja tiedon keräys epäasianmukaisesti puhdistetuista tallennusvälineistä. Tietoa vuotaa organisaatioista ulos poisheitettyjen laitteiden mukana, laitevalmistajille laitteiden korjausten yhteydessä, sekä muihin järjestelmiin laitteisto tai ohjelmistovikojen seurauksena (Kissel ym., 2014). Faganin ym. (2020) mukaan laitevalmistajat voivat auttaa asiakkaitaan esittämällä kysymyksiä kuten: Haluaako asiakas siirtää laitteidensa omistuksen toiselle osapuolelle? Haluavatko asiakkaat tehdä laitteistaan käyttökelvottomia?

Riippuen siitä mitä asiakas haluaa laitevalmistajat voivat kertoa miten toimia, jotta heidän tietonsa eivät ole uuden omistajan saatavilla tai laite on varmasti toimintakyvytön. Asiakas voi haluta myydä rakennuksen, joka sisältää älykkäitä toimintoja ja varmistaa, että kaikki data on poistettu laitteista ennen kuin uusi talon omistaja pääsee niihin käsiksi. (Fagan ym., 2020.)

Elinkaaren loppuvaiheessa luottamuksellisuus, eheys ja käytettävyys nousevat esille poistettaessa tai siirrettäessä dataa, katkaistaessa yhteys muihin laitteisiin tai järjestelmiin, sekä hävitettäessä tallennusvälineitä ja laitteistoja. Poistamalla data IoT-laitteista ja hävittämällä tallennusvälineet asianmukaisesti varmistetaan tiedon luottamuksellisuus. Laitteiden eheyteen joudutaan kiinnittämään huomiota, jos IoT-laite on tarkoitus käyttää uudelleen, jotta vialliset laitteet eivät vahinkoa uudessa käyttökohteessa. Käytettävyys on syytä huomioida IoT-laitetta poistettaessa, jotta se ei häiritse muita siihen liitettyjä laitteita tai järjestelmiä. Käytön jatkuvuutta voidaan edistää siirtämällä käytöstäpoistettavan IoT-laitteen data toiseen laitteeseen tai muualle järjestelmässä. Tärkein huomioitava kohta on kuitenkin luottamuksellisuus. Mikäli laitetta tullaan käyttämään uudelleen palaa se elinkaaren alku- tai keskivaiheeseen, jolloin sen eheys tarkistetaan uudelleen ja koska laite poistetaan käytöstä ei tässä kohtaa itse laitteen käytettävyydellä ole merkitystä.

5 YHTEENVETO

Tässä tutkielmassa käsiteltiin IoT-laitteiden käyttöä teollisuudessa, sekä tarkasteltiin IoT-laitteiden elinkaarta ja sen aikaista kyberturvallisuutta kyberfyysisten järjestelmien, IIoT:n ja Industry 4.0 näkökulmasta. Tutkielmassa pyrittiin löytämään vastaus seuraaviin kysymyksiin:

- Miten kyberturvallisuus otetaan huomioon IIoT-laitteiden elinkaaren aikana?
- Minkälaisia kyberturvallisuuden haasteita esiintyy elinkaaren aikana?

Tutkimuksen tarkoitus on auttaa ymmärtämään puutteita ja huomioitavia kohtia teollisten IoT-laitteiden käytössä ja kyberturvallisuudessa sen koko elinkaaren ajalta. Teollisella esineiden internetillä on kyky mullistaa teollisuuden toimintatapoja ja luoda merkittäviä hyötyjä tuotannolle kuten tehokkuus, lyhyemmät tuotantosyklit, ennakoiva ylläpito, laitteiden pidennetty käyttöikä ja näistä aiheutuvat kustannussäästöt. Muita IIoT:n tuomia hyötyjä ovat esimerkiksi edistyneempi toimitusketjun seuranta ja omaisuudenhallinta, sekä tehokkuuden ja tuottavuuden lisääntyminen. Toisaalta IIoT käyttö tuo mukanaan uusia haasteita ja riskejä, kuten kyberturvallisuusuhkia, tietosuoja- tai yhteensopivuus ongelmia.

Tämä tutkielma auttaa lisäämään ymmärrystä ja tietoisuutta IIoT:n kyberturvallisuuden mukanaan tuomista haasteista. Tutkimuksessa selvisi, että kyberturvallisuus on syytä huomioida heti elinkaaren alusta lähtien, koska se vähentää korjaustoimien tarvetta myöhemmissä elinkaaren vaiheissa. Alkuvaiheessa turvallisuuteen vaikuttaminen on myös helpompaa. Hyvin suunnitellussa ja valmistetussa IoT-laitteessa tai järjestelmässä on parempi tietosuoja, kyberhyökkäyksiä on helpompi ehkäistä ja järjestelmät ovat eheämpiä. IIoT-laitteiden siirtyessä elinkaaren keskivaiheeseen niiden käyttö aloitetaan, jonka ohella huomioidaan myös kyberturvallisuus. Tähän elinkaaren vaiheeseen kuuluvat kyberturvallisuus uhkien havaitseminen ja ehkäiseminen, järjestelmän luotettavuuden varmistaminen ja toiminnan edistäminen, sekä muutoksiin sopeutuminen. Tämän vaiheen kyberturvallisuuden tavoite on pitää sekä IIoT-laitteet että niihin liittyvät järjestelmät toiminnassa, sekä varmistaa niiden luotettava ja turvallinen

käyttö. Elinkaaren loppuvaiheessa keskitytään siihen, että IIoT-laitteet eivät vuoda arkaluontoista dataa väärille henkilöille ja väärille tahoille.

Tutkimuksessa keskityttiin myös kyberturvallisuuden haasteisiin elinkaaren aikana. IIoT-laitteisiin liittyviä turvallisuus haasteita elinkaaren alussa ovat yleisten laitestandardien puute, IIoT-järjestelmien monimutkaisuus, sekä laitteiden rajallinen laskentateho, jotka rajoittavat turvatoimien toteutusta. Elinkaaren keskivaiheen kyberturvallisuushaasteet liittyvät monitorointiin ja laitteiden päivittämiseen. Haasteet johtuvat yleisesti IIoT-laitteiden suuresta määrästä, käyttökatkoista, sekä asiantuntemuksen ja tiedon puutteesta. Elinkaaren loppuvaiheen haasteena on löytää ja poistaa arkaluontoinen sisältö ja varmistaa että tietoihin ei pääse enää käsiksi.

Kyberturvallisuuden haasteita käsiteltiin myös CIA-mallin avulla. Näitä luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviä haasteita on koottu alla olevaan taulukkoon (Taulukko 1).

TAULUKKO 1 CIA haasteet elinkaaren aikana

Elinkaaren vaihe		CIA luokittelu	Haaste
Alkuvaihe	Suunnittelu	Luottamuksellisuus, eheys, käytettävyys	Tasapainon löytäminen luottamuksellisuuden ja käytettävyyden väliltä.
	Valmistus ja kokoonpano	Luottamuksellisuus ja eheys	Arkaluontoisten laite- ja tuotantotietojen suojaus, sekä laitevikojen eliminointi.
	Asennus, konfigurointi ja käyttöönotto	Luottamuksellisuus ja käytettävyys	Konfiguraatiotietojen, käyttäjätunnuksien ja salausavaiminen salassapito, sekä käyttöönotosta johtuvien käyttökatkojen minimointi.
Keskivaihe	Käyttö ja seuranta	Eheys ja käytettävyys	Poikkeamien havaitseminen ja luotettavan toiminnan varmistaminen.
	Ylläpito ja päivitykset	Eheys ja käytettävyys	Eheyttä parantavien päivitysten toteutus ja niistä johtuvien käyttökatkojen minimointi.

Loppuvaihe	Uudelleen käyttö ja käytöstäpoistaminen	Luottamuksellisuus ja käytettävyys	Tietojen asianmukainen poistaminen tai siirtäminen. Varmuus siitä, että laitteen poisto ei häiritse muita siihen liitettyjä laitteita tai järjestelmiä.

Tutkimuksen tarkoituksena oli antaa yleiskuva IIoT:n kyberturvallisuudesta ja sen haasteista. Tutkimuksen tulokset vastasivat esitettyihin tutkimuskysymyksiin ja niiden voidaan olettaa olevan luotettavia, koska useat lähteet käsittelivät samoja aiheita, eikä niiden väliltä löytynyt ristiriitoja. Käsitelty aihe on melko uusi ja IoT:n käyttö teollisuudessa on vasta alkuvaiheessa. On todennäköistä, että lähitulevaisuudessa tulee tapahtumaan muutoksia, joiden seurauksena syntyy uusia haasteita, sekä vanhoihin haasteisiin löydetään ratkaisuja. Aihetta olisi hyvä jatkaa tutkimalla laajemmin erilaisia ratkaisuvaihtoehtoja. Haasteiden ratkaisu vaihtoehdoista löytyykin jo tutkimuksia, jotka keskittyvät eri teknologisiin ratkaisuihin kuten tekoälyn tai lohkoketjujen käyttöön IoT-laitteissa. Mahdolliset uudet ratkaisut voivat auttaa löytämään ratkaisuja CIA-mallin haasteisiin, jolloin resurssit voidaan kohdistaa tehokkaammin CIA-mallin muihin alueisiin. Ratkaisujen löytäminen tutkimuksessa todettuihin haasteisiin on tärkeää, koska se edistäisi IIoT:n yleistymistä ja älykkäiden tuotantolaitosten kyberturvallisuutta.

LÄHTEET

Bertino, E. (2019). IoT Security A Comprehensive Life Cycle Framework. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 196–203. https://doi.org/10.1109/CIC48465.2019.00033

Boyes, H., Hallaq, B., Cunningham, J. & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Chhetri, S. R., Rashid, N., Faezi, S. & Al Faruque, M. A. (2017). Security trends and advances in manufacturing systems in the era of industry 4.0. 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 1039–1046. https://doi.org/10.1109/ICCAD.2017.8203896

Fagan, M., Megas, K. N., Scarfone, K. & Smith, M. (2020). Foundational cybersecurity activities for IoT device manufacturers (NIST IR 8259; s. NIST IR 8259). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259

Humayed, A., Lin, J., Li, F. & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Kissel, R., Regenscheid, A., Scholl, M. & Stine, K. (2014). Guidelines for Media Sanitization (NIST SP 800-88r1; s. NIST SP 800-88r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1

Mentsiev, A. U., Guzueva, E. R. & Magomaev, T. R. (2020). Security challenges of the Industry 4.0. Journal of Physics: Conference Series, 1515(3), 032074. https://doi.org/10.1088/1742-6596/1515/3/032074

Pereira, T., Barreto, L. & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia Manufacturing, 13, 1253–1260. https://doi.org/10.1016/j.promfg.2017.09.047

P.W. Singer & Allan Friedman. (2014). Cybersecurity and Cyberwar : What Everyone Needs to Know®. Oxford University Press. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=657629&site=ehost-live

Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. & Wu, D. O. (2020). Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. IEEE Communications Surveys & Tutorials, 22(4), 2462–2488. https://doi.org/10.1109/COMST.2020.3009103

Rahman, L. F., Ozcelebi, T. & Lukkien, J. (2018). Understanding IoT Systems: A Life Cycle Approach. Procedia Computer Science, 130, 1057–1062. https://doi.org/10.1016/j.procs.2018.04.148

Sadeghi, A.-R., Wachsmann, C. & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. Proceedings of the 52nd Annual Design Automation Conference, 1–6. https://doi.org/10.1145/2744769.2747942

Schaeffler Finland Oy. (ei pvm.). OPTIME. Noudettu 18. huhtikuuta 2023, osoitteesta https://www.schaeffler.fi/fi/products-and-solutions/industrial/product-portfolio/maintenance_products/optime/

Serror, M., Hack, S., Henze, M., Schuba, M. & Wehrle, K. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(5), 2985–2996. https://doi.org/10.1109/TII.2020.3023507

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S. & Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access, 8, 23022–23040. https://doi.org/10.1109/ACCESS.2020.2970118

Sharma, P., Jain, S., Gupta, S. & Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Networks, 123, 102685. https://doi.org/10.1016/j.adhoc.2021.102685

Soós, G., Kozma, D., Janky, F. N. & Varga, P. (2018). IoT Device Lifecycle – A Generic Model and a Use Case for Cellular Mobile Networks. 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 176–183. https://doi.org/10.1109/FiCloud.2018.00033

Späthe, S. (2021). Conception of a Generic IoT Device Life Cycle Model. 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 1–7. https://doi.org/10.1109/IoTaIS53735.2021.9628736

Waslo, R., Lewis, T., Hajj, R. & Carton, R. (2017). Industry 4.0 and cybersecurity. Deloitte Insights. Noudettu 28. huhtikuuta 2023, osoitteesta https://www2.deloitte.com/content/www/us/en/insights/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

Xu, H., Yu, W., Griffith, D. & Golmie, N. (2018). A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE Access, 6, 78238–78259. https://doi.org/10.1109/ACCESS.2018.2884906

Yousefnezhad, N., Malhi, A. & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. Journal of Network and Computer Applications, 171, 102779. https://doi.org/10.1016/j.jnca.2020.102779

Yu, X. & Guo, H. (2019). A Survey on IIoT Security. 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 1–5. https://doi.org/10.1109/VTS-APWCS.2019.8851679

Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. Noudettu 28. huhtikuuta 2023, osoitteesta https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/