Jarno Alkiomaa

IEC 62443-4-2 STANDARDIN HYÖDYT JA HAASTEET YRITYKSELLE - SYSTEMAATTINEN KIRJALLISUUS-KATSAUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Alkiomaa, Jarno
IEC 62443-4-2 standardin hyödyt ja haasteet yritykselle – systemaattinen kirjallisuuskatsaus
Jyväskylä: Jyväskylän yliopisto, 2023, 25 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Clements, Kati

Teollisuus digitalisoituu siinä missä muukin maailma, mutta digitalisaation myötä myös riskit lisääntyvät. Yhä suurempi osa laitteista on jollain tavalla yhteydessä toisiinsa ja internettiin. Teollisessa kontekstissa tämä tarkoittaa esimerkiksi sensoreita, robotteja, hallintajärjestelmiä ja automaatiota. Nopean kehityksen takia turvallisuuteen liittyvät toimet eivät aina kehity yhtä nopeasti. On kuitenkin standardeja, jotka auttavat tekemään laitteista turvallisia. Viime vuosina onkin huomioon pääsyt IEC 62443 standardi, josta puhutaan de facto standardina teollisuuden automaatiolaitteissa. Standardi antaa kokonaisvaltaisen viitekehyksen automaatiolaitteiden turvaamiseen. Vuonna 2019 standardiin lisättiin virallisesti alakohta 4–2, joka tuo turvaa automaatio ja IoT-laitteisiin jo valmistajan puolesta komponenttitasolla. Tutkimuksessa tarkastellaankin mitä hyötyjä ja haasteita kyseinen standardi IEC 62443-4-2 tuo yrityksille. Tutkimus löysi hyötyjä suuremmasta läpinäkyvyydestä ja luotettavuudesta, hyökkäyksien riskien pienentymisestä, hyökkäyksiltä suojautumisessa ja operatiivisen teknologian turvaamisesta. Kuitenkin haasteita tuottaa standardin kompleksisuus, rahallinen panostus, tasapainon löytäminen eri tasojen kanssa, ja puuttuva ohjeistus päivityksiin ja digitaaliseen forensiikkaan. Tutkimus tuotettiin systemaattisena kirjallisuuskatsauksena perustuen suuremmilta osin lähteisiin, jotka kerättiin kolmesta eri tietokannasta. Aihe on vielä verrattain uusi ja aiempaa tutkimusta on tehty vähän liittyen IEC 62443-4-2 standardiin. Aihe vaatisi vielä syvällisempää tutkimusta ja yhteistyötä standardia käyttävien yrityksien kanssa.

Asiasanat: IEC 62443, IEC 62443-4-2, I4.0, Teollisuus 4.0, kyberturvallisuus

ABSTRACT

Alkiomaa, Jarno
IEC 62443-4-2 standard benefits and challenges for the company – systematic literature review
Jyväskylä: University of Jyväskylä, 2023, 25 pp.
Information Systems, Bachelor's Theses
Supervisor(s): Clements, Kati

Industry is becoming more digital as well as the rest of the world, but this digitalization also brings risks. An increasing number of devices are somehow connected to each other and to the internet. In an industrial context, this means sensors, robots, management systems and automation, for example. Due to rapid development, safety-related activities do not always develop as quickly. However, there are standards that help make devices safe. In recent years, the IEC 62443 standard has been spoken of as the de facto standard for industrial automation devices. The standard provides a comprehensive framework for securing automation devices. In 2019, subsection 4-2 was officially added to the standard, which brings security to automation and IoT devices on the manufacturer's behalf at component level. This study examines the benefits and challenges that IEC 62443-4-2 presents to companies. The study found benefits from greater transparency and reliability, reduced risk of attacks, protection from attacks, and protection for operative technology. However, challenges are presented by the complexity of the standard, monetary investment, finding a balance with different levels, and missing guidance on upgrades and digital forensics. The study was produced as a systematic literature review, largely based on sources collected from three different databases. The topic is still relatively new and previous research has been limited in relation to the IEC 62443-4-2 standard. The topic would require even more in-depth research and collaboration with companies using the standard.

Keywords: IEC 62443, IEC 62443-4-2, I4.0, Industry 4.0, Cybersecurity

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDATO

Teollisuuden automatisointi on suuressa nousussa teknologian kehityksen takia. Esineiden internet, tekoäly, pilvipalvelut ja monet muut teknologiat mahdollistavat monia toimia teollisuudessa ja muissakin yrityksissä. Teollisuudessa tästä älykkäästä tuotannosta puhutaan nimellä teollisuus 4.0 (eng. Industry 4.0, lyh. I4.0) tai teollisesta internetistä, joka on hyvin automatisoitu, älykäs, yhteenkytketty ja yhteentoimiva tuotanto ekosysteemi (Ma, Hudic, Shaaban & Polsz, 2017). Longueire-Romero, Flores & Garitano (2022) osoittivat tutkimuksessaan, että teollisuus 4.0 myötä tuotantolaitoksien kompleksisuus kasvaa, ja monet teknologiat mahdollistavat myös hyökkääjille monia erilaisia hyökkäysmahdollisuuksia. Onkin tärkeää muistaa, että kompleksisuus on kriittinen suunnittelukohde, koska se on läheisesti yhteydessä haavoittuvuuksien määrään (Longueira-Romero ym., 2022). Yhteenkytketty teknologia johtaa tehokkaampaan tuotantoon ja parempaan käyttäjäkokemukseen, mutta samalla tietoturvariskit nousevat, jotka kohdistuvat kriittisiin laitteisiin ja laitoksiin (Hohenegger ym., 2021).

Tietoturvariskien minimoimiseen on kehitetty monia standardeja kuten ISO/IEC 27001 tai ISO 9001, mutta nämä eivät käsittele teollisuuden automaatio ja ohjausjärjestelmien (eng. Industrial Automation and Control Systems, lyh. IACS) kyberturvallisuutta silla tasolla millä IEC 62443-4-2 käsittelee (Martins & Vidal Garcia Oliveira, 2022). Uudet IACS-laitteet mahdollistavat uudenlaisia yhteyksiä, automaatioratkaisuja ja liiketoimintamalleja erilaisten IoT-laitteiden kanssa, joita ei ennen ole ollut (Mugarza, Flores & Montero, 2020). Tästä syystä uudet standardit ja niiden tutkiminen on tärkeässä roolissa tulevaisuuden kriittisten laitteiden turvallisuuden takaamisessa. IEC 62443 standardin tarkoitus onkin tarjota täydellinen viitekehys IACS-laitteille eri organisaatiotasoilla aina tuotekehityksestä komponenttitasolla yrityksen toimintatapoihin saakka (Schmittner, Shaaban & Macher, 2022). Standardi tekee tämän jakamalla laitteet ja eri toiminnan osa-alueet omiin alueisiinsa ja jokainen alue turvataan omalla turvallisuustasolla (Shaaban ym., 2018). Alueista ja turvallisuustasoista on tarkemmin tietoa tutkimuksen luvussa 2.2 Standardin käyttö. Standardin on kehittänyt yhteistyössä ISA (eng. International Society of Automation) ja IEC (eng. Internationl Electrotechnical Comission) vastaamaan puuttuviin kyberturvallisuuteen

liittyviin haasteisiin teollisuudessa (Santos, Oliveira, Saores, Satis & Santos, 2021). Teollisuuden laitteet eroavat normaaleista IT-alan järjestelmistä käyttämällä operatiivista teknologiaa eli OT-laitteita (eng. Operative Technology). Näitä laitteita ovat esimerkiksi erilaiset sensorit, robotit, mittaristot ja muut toiminnalliset laitteet (Erwin, Kloibhofer, Díaz & Castillejo, 2021). Standardin tarkoitus onkin taata tietoturvallisuuden lisäksi fyysinen turvallisuus. OT laitteen jouduttua hyökkäyksen kohteeksi voi seuraukset olla todella merkittäviä myös ihmisten turvallisuudelle (Hollerer, Sauter & Kastner, 2022).

Standardi on hyvin laaja ja sitä myös päivitetään edelleen, jonka takia on tärkeä tutkia sen vaikutuksia ja mahdollisuuksia yrityksissä. Tässä tutkimuksessa on tarkoitus antaa yleiskuvaa standardista ja perehtyä Standardin alaosaan 4–2, joka painottuu komponenttien turvallisuuteen. Seuraavassa alaluvussa on tarkemmin tutkimukselle asetetut tutkimuskysymykset ja kuinka tutkimus toteutettiin.

Johdannon jälkeen luvussa kaksi tutkimus etenee standardin toiminnan kuvaamiseen ja standardin rakenteeseen. Näissä luvuissa rakennetaan parempaa yleiskuvaa mikä IEC 62443 standardi on ja mitä se mahdollistaa. Luvussa kolme perehdytään paremmin standardin kohtaan 4–2 joka koskee IACS ja IoT-laitteiden komponenttien turvallisuutta. Kolmannessa luvussa tarkastellaan myös IEC 62443-4-2 standardin tuomia mahdollisia hyötyjä ja haasteita yrityksille. Näiden jälkeen on yhteenveto tutkimuksen tuloksista ja esitetään jatkotutkimusaiheita liittyen standardiin.

1.1 Tutkimuskysymys

Tutkimuksen tarkoitus on kartoittaa IEC 62443-4-2 standardin mahdollisia hyötyjä ja haasteita yritykselle. Täten nämä kaksi aihetta olivat tutkimuksen tutkimuskysymyksinä, tutkimuskysymykset on:

- Mitkä ovat IEC 62443-4-2 standardin hyödyt?
- Millaisia haasteita IEC 62443-4-2 standardissa voi ilmetä?

Tutkimuksessa saatiin vastattua molempiin kysymyksiin, mutta aihe vaatisi vielä syvempää tutkimusta ja yhteistyötä standardia käyttävien yrityksien kanssa. Standardi on uusi ja siitä ei ole vielä laajaa tutkimusaineistoa, joka hieman vaikutti tuloksiin. Tutkimus kuitenkin selvitti, että standardista on todellista hyötyä yrityksille, jotka haluavat vahvaa suojaa kriittisille laitteistoille. Standardi tuo luottamusta ja läpinäkyvyyttä sidosryhmille, suojaa hyökkäyksiltä ja pienentää niiden riskiä ja turvaa operatiivisen teknologian. Suurimpina haasteina ilmeni standardin laajuus, kompleksisuus, ja rahallinen panostus. Tutkimuksessa ilmeni myös, että standardista puuttuu ohjeistukset laitteiden turvalliseen päivittämiseen ja digitaalisen forensiikan tekemiseen. Tarkemmat tulokset löytyvät tutkimuksen alaluvuista 3.1 ja 3.2.

1.2 Tutkimusmenetelmä

Tutkimus toteutettiin systemaattisena kirjallisuuskatsauksena käyttäen Okoli & Schabram (2010) ohjetta viitekehyksenä tutkimuksen tekemiseen. Tutkimus toteutettiin tällä metodilla, koska aihe on vielä suhteellisen uusi ja tarve tutkimuksen kartoittamiselle on tarpeen. Systemaattinen kirjallisuuskatsaus antaa hyvän yleiskuva millaista standardia käsittelevää tutkimusta on julkaistu ja tämän tutkimuksen jälkeen on helpompi lähteä rakentamaan jatkotutkimuksia aiheeseen liittyen.

Lähteitä tutkimukseen haettiin erilaisista tietokannoista kuten ACM Digital Library, Proquest ja IEEE Xplorer. Haut toteutettiin aikavälillä 21.-22.01.2023. ACM Digital Library tietokannassa hakusanana oli ”IEC 62443-4-2”, valintana ”Research article”, tulosten aikaväli 2007–2023, järjestys ”Relevance” ja tuloksia tuli 312 507 kappaletta. Suurin osa tuloksista oli epäolennaisia tutkimuksen kannalta ja näistä valittiin 14 tutkimusta seuraavaan vaiheeseen.

Advanced Technologies & Aerospace collection – proquest tietokannasta haettiin tuloksia hakusanalla “IEC 62443-4-2”, valintoina oli ”Anywhere”, ”Peer reviewed”, ”case study”, “dissertation/theses”, “literature review”, “standard” ja kieli joko Suomi tai Englanti. Näillä valinnoilla hakutuloksia tuli 47 kappaletta, joista 18 valittiin seuraavaan vaiheeseen.

Computer science database – proquest tietokannasta haettiin tuloksia hakusanalla ”IEC 62443-4-2”, valintoina oli ”Anywhere”, ”Peer reviewed”, ”Article”, “case study, “literature review”, “standard” ja kieli Englanti. Näillä valinnoilla hakutuloksia tuli 18 kappaletta, joista 2 valittiin seuraavaan vaiheeseen. monet tuloksista olivat samoja kuin edellisessä haussa.

Viimeisenä tietokantana käytettiin IEEE Xplorer tietokantaa, jossa hakusanana oli ”IEC 62443-4-2”, valintoina oli ”full text & metadata”. Näillä valinnoilla hakutuloksia tuli 147 kappaletta. Näistä jatkotutkimukseen valittiin kolme eniten viitattua (”most cited”) ja kuusi ”relevance” perusteella.

Näiden hakujen jälkeen lähteitä oli yhteensä 43 kappaletta, joita tutkittiin tarkemmin ja lopullisiksi lähteiksi tutkimukseen sopivia oli alle puolet. Tämä johtui siitä, että monet tutkimukset käsittelivät IEC 62334 standardia jonkin muun alakohdan kuin 4–2 perusteella, tai käsittelivät standardia yleisesti käsittelemättä tarkemmin alakohtaa 4–2. Tämä on seurausta siitä, että IEC 62443-4-2 standardi on vielä hyvin uusi ja siihen kohdistuvaa tarkempaa tutkimusta on niukasti. Näiden lisäksi muutama lähde löytyi ISA:n omilta nettisivuilta, joissa he kertovat tarkemmin standardin toiminnasta, lähteet ovat ISA (2020a), ISA (2020b) ja ISA (2021).

2 IEC 62443 STANDARDI

IEC 62443 on standardi, jonka tarkoitus on auttaa teollisuuden IACS-järjestelmien kyberturvallisuuden uhkien ja riskien hallintaa (Leander, Čaušević & Hansson, 2019). Standardi on kehitetty ISA99 komitean ja IEC teknisen komitea 65:n yhteistyönä vastaamaan IACS laitteiden turvallisuudesta, kun huomattiin ettei sen hetkiset standardit vastanneet IACS-laiteiden turvallisuuden turvaamisen haasteisiin (Leander ym., 2019). Koska digitalisaatio ja automaatio ovat teollisuudessa yleistä ja alati kasvavaa, on myös teollisuuden eri osa-alueiden välillä liikkuva tieto lisääntynyt (Leander ym., 2019; Martins & Vidal Garcia Oliveira, 2022). Teollisuuden digitalisaatiota kutsutaan myös teollisuuden esineiden internetiksi (eng. Industrial Internet of Things, lyh. IIoT) tai teollisuus 4.0 (eng. Industry 4.0, lyh. I4.0) (Dhirani, Armstrong & Newe, 2021). Dihrani ym. (2021) mukaan IIoT tarkoittaa teollisuuden ja tuotannon teknisten laitteiden liittämistä hajautettuihin teknologioihin. Näitä teknologioita ovat esimerkiksi esineiden internet, pilvilaskenta ja tekoäly. Näiden teknologioiden kautta pyritään saamaan parempaa dataa, automaatiota ja seurantaa, jotka taas auttavat vähentämään kustannuksia, saavuttamaan ketteryyttä ja tehokkuutta (Dhirani ym., 2021). Kaikki tämä tuo mukanaan myös uusia turvallisuusriskejä, jotka pitää huomioida teollisuuden ja tuotannon digitaalista muutosta tehtäessä. Tämä on erityisen tärkeää juuri teollisuuden laitoksissa, koska erilaiset laitteistot voivat olla käytössä jopa vuosikymmeniä (Mugaraza, Flores & Montero, 2020). ISA (2020a) huomioi kuinka erilaisia seuraukset voivat olla hyökkäyksissä perinteisiä IT-laitteita kohtaa, kuin IACS-laitteita kohtaan. Perinteisissä IT-laitteisiin kohdistuneissa hyökkäyksissä seuraukset ovat yleensä rahallisia tai yksityisyyteen liittyviä, kun taas IACS-laitteisiin kohdistuva hyökkäys voi vaarantaa ihmisten turvallisuutta, ympäristöä tai tuotteiden laatua (ISA, 2020a). Lender ym. (2019) puhuu aiheesta myös, ottaen huomioon kuinka IACS laitteita käytetään erilaisissa fyysisissä prosesseissa esimerkiksi ydinlaitoksissa, sähkölaitoksissa tai kemianteollisuudessa. Näitä kyseisiä laitoksia miettien pitäisi ymmärtää kuinka tärkeää IACS-laitteiden turvallisuuden takaaminen on (Leander ym., 2019). Esimerkiksi mitä tapahtuisi, jos hyökkäys kohdistuisi ydinlaitokseen ja laitoksen lämpösensorit tai jäähdytyskoneistot lakkaisivat toimimasta tai näyttäisivät vääriä lukemia.

2.1 IEC 62443 Standardin rakenne

IEC 62443 standardi koostuu neljästä osa-alueesta ja nämä osa-alueet pitävät sisällään tarkemmin tiettyyn alueeseen kohdistettuja ohjeistuksia. Taulukosta 1 löytyvät eri osa-alueet ja näiden ala-alueet tarkemmin määriteltynä. Pelkistetysti standardin eri kohdat pitävät sisällään Leander ym. (2019) mukaan seuraavia asioita.

- Standardin ensimmäinen osa pitää sisällään yleisiä käytänteitä asiakirjojen käsitteiden, terminologian, käyttötapausten ja vastaavien määrittelyyn.
- Standardin toinen osa pitää sisällään käytäntöjä ja menettelytapoja muun muassa turvalliseen päivitysten hallintaan ja tietoturvaohjelmien vaatimuksiin.
- Standardin kolmas osa pitää sisällään järjestelmätason vaatimukset, järjestelmäriskien arvioinnin ja muut järjestelmiin liittyvät säännökset.
- Standardin neljäs ja viimeinen osa pitää sisällään komponenttitason vaatimukset, mukaan lukien komponenttien kehitysvaiheen vaatimukset.

TAULUKKO 1 IEC 62443 standardin eri osa-alueet (Fujdiak, Mlynek, Blazek, Barabas & Mrnustik, 2018, s. 289)

Ryhmä	Osa	Sisältö
Yleiset	IEC 62443-**1-1**	Terminologia, konseptit, mallit
	IEC 62443-**1-2**	Termien ja lyhenteiden yleissanasto
	IEC 62443-**1-3**	Järjestelmän tietoturvan vaatimustenmukaisuuden mittarit
	IEC 62443-**1-4**	IACS:n tietoturvaelinkaari ja käyttötapaus
Toimintatavat & Käytänteet	IEC 62443-**2-1**	IACS:n turvallisuusjohtamisjärjestelmää koskevat vaatimukset
	IEC 62443-**2-2**	IACS:n turvallisuusjohtamisjärjestelmän täytäntöönpano-ohjeet
	IEC 62443-**2-3**	Päivityksien-hallinta IACS-ympäristössä
	IEC 62443-**2-4**	IACS-toimittajien asennus- ja huoltovaatimukset
Järjestelmä	IEC 62443-**3-1**	IACS:n turvallisuusteknologiat
	IEC 62443-**3-2**	Turvallisuustasot vyöhykkeille ja kanaville
	IEC 62443-**3-3**	Järjestelmän turvallisuusvaatimukset ja turvallisuustasot
Komponentti	IEC 62443-**4-1**	Tuotekehitysvaatimukset
	IEC 62443-**4-2**	IACS-komponenttien tekniset turvallisuusvaatimukset

2.2 IEC 62443 Standardin käyttö

Standardin ensisijainen tarkoitus on tarjota viitekehys nykyisten ja tulevaisuuden kyberuhkien ja haavoittuvuuksien varalle jotka uhkaavat teollisuuden laitteita (Shaaban, Chalup, El-Araby & Schmittner, 2022). Standardi käsittelee näiden laitteiden koko elinkaaren toimittajan komponenteista aina yrityksen

laitteiden käyttöoikeuksien solmimiseen asti (Leander ym., 2019). Tästä voimme todeta, että standardi on hyvin laaja ja moniulotteinen, joka vaatii hyvää standardiin perehtymistä ja sen käytön suunnittelemista. Tätä laajuutta auttaa standardin eri osien lokeroiminen ja yritys voi ottaa käyttöön vain tietyn osan standardista (Hohenegger ym., 2021). Schmittner (2022) mukaan osien sisällä pystyy päättämään, kuinka turvallisen tietystä osa-alueesta haluaa. Tämän standardi toteuttaa erilaisilla vyöhykkeillä (eng. Zone) ja vyöhykkeisiin liittyvillä turvallisuus tasoilla (eng. Security Level) (Schmittner ym., 2022). ISA (2020a) määrittelee vyöhykkeen seuraavanlaisesti:

> Vyöhyke määritellään loogisen tai fyysisen omaisuuden ryhmittelynä, joka perustuu riskiin tai muihin kriteereihin, kuten omaisuuden kriittisyyteen, operatiiviseen toimintoon, fyysiseen tai loogiseen sijaintiin, vaadittuun pääsyyn tai vastuulliseen organisaatioon. (ISA, 2020a, s. 7)

Vyöhykkeiden lisäksi standardissa on määritelty kanava (eng. Conduit), joka toimii suojana seuraavalle vyöhykkeelle suojaten viestinnän eheyttä ja luottamuksellisuuta (Erwin ym., 2021). ISA (2020a) määrittelee kanavan seuraavanlaisesti: ”Kanavalla tarkoitetaan sellaisten viestintäkanavien loogista ryhmittelyä, joilla on yhteiset turvallisuusvaatimukset kahden tai useamman vyöhykkeen kanssa.” (ISA, 2020a, s. 7). Kun vyöhykkeet ja niiden käyttämä tiedonsiirtokanava on asetettu samalle tai paremmalle turvallisuus tasolle, voidaan varmistua yhtenäisestä turvallisuudesta ja suojauksesta kyberuhkia vastaan (Erwin ym., 2021).

Turvallisuustason ISA (2020a) määrittelee ” luottamuksen mittariksi, jonka mukaan tarkasteltava järjestelmä, vyöhyke tai kanava on vapaa haavoittuvuuksista ja toiminnoista tarkoitetulla tavalla.” (ISA, 2020a, s. 7). Turvallisuustasoja standardissa on neljä kappaletta ja ne ovat numeroitu 1–4, jossa yksi tarkoittaa vähiten turvallista tasoa ja neljä on suurin mahdollinen turvallisuustaso (Leander ym., 2019). Taulukossa 2 on eri turvallisuustasot määriteltynä ja millainen mahdollisen hyökkääjän tietotaidon tason pitäisi olla. Huomioitavaa on, että joissakin tapauksissa voi käyttää implisiittistä turvallisuustaso nollaa, joka tarkoittaa ettei erityistä suojausta tarvita (Leander ym., 2019).

TAULUKKO 2 IEC 62443 standardin turvallisuustasot (ISA, 2020a, s. 8)

Turvallisuus-taso	Määritelmä	Keinot	Resurssit	Taidot	Motivaatio
1	Suoja yksinkertaisia tai satunnaisia rikkeitä vastaan				

2	Suoja tahallisia rikkeitä vastaan, joissa käytetään yksinkertaisia keinoja, vähäisä resursseja, geneerisiä taitoja ja matalaa motivaatiota	Yksinkertaiset	Matalat	Geneeriset	Matala
3	Suoja tahallisia rikkeitä vastaan käyttämällä kehittyneitä keinoja, kohtuullisia resursseja, IACS-spesifisiä taitoja ja kohtalaista motivaatiota	Kehittyneet	Kohtuulliset	IACS-spesifinen	Kohtalainen
4	Suojaus tahallista rikkomusta vastaan käyttämällä kehittyneitä keinoja, laajoja resursseja, IACS-spesifisiä taitoja ja korkeaa motivaatiota	Kehittyneet	Laajat	IACS-spesifinen	Korkea

Jokaiselle vyöhykkeelle on määritelty seitsemän perusvaatimusta (eng. Foundational requirements) ja jokaiselle perusvaatimukselle annetaan tietty turvallisuustaso (Fujdiak ym., 2018). Tällä tavoin varmistutaan, että vyöhykkeen kaikki tärkeimmät osa-alueet käydään läpi ja niille saadaan asetettua haluttu turvallisuustaso (Fujdiak ym., 2018). ISA (2020a) mukaan perusvaatimukset (lyh. PV) ovat seuraavanlaiset:

- PV 1 – Tunnistamisen ja todentamisen valvonta
- PV 2 – Käytön valvonta
- PV 3 – Järjestelmän toimivuus
- PV 4 – Datan luottamuksellisuus
- PV 5 – Tietovirran rajoittaminen
- PV 6 – Oikea-aikainen reagointi tapahtumiin
- PV 7 – Resurssien saatavuus

Esimerkkinä tietyn vyöhykkeen datan luottamuksellisuuden suojaaminen korkeimmalla tasolla tapahtuisi asettamalla kyseisen vyöhykkeen PV 4

turvallisuustaso tasolle neljä. Tällä tavoin suunnitellaan ja käydään läpi vyöhykkeen kaikki perusvaatimukset ja asetetaan halutut turvallisuustasot.

Turvallisuustasoja on vielä kolmea erilaista tyyppiä, joita käytetään turvallisuustasojen suunnittelussa. ISA (2020b) mukaan standardissa käytettävät turvallisuustasot ovat: kyvykkyys turvallisuustaso (eng. Capability Security Levels), haluttu turvallisuustaso (eng. Target Security Levels), ja saavutettu turvallisuustaso (eng. Achieved Security Levels). Ensimmäisellä tarkasteltavalla turvallisuustasolla eli turvallisuustason kyvykkyydellä tarkoitetaan mihin turvallisuustasoon vyöhykkeen järjestelmät ja komponentit ovat kykeneväisiä. Toisena suunnitellaan mikä turvallisuustaso kyseiselle automaatioratkaisulle haluttaisiin saavuttaa. Halutut turvallisuustasot määritellään riskinarviointiprosessissa standardin osassa 3–2. Tätä turvallisuustasoa käytetään esimerkiksi turvallisuustuotteiden valinnassa ja kompensoivien turvatoimien suunnittelussa. Viimeisenä on saavutettu turvallisuustaso eli mikä turvallisuustaso kyseiselle automaatioratkaisulle saatiin, kun se on toteutettu ja otettu käyttöön (ISA, 2020b).

Turvallisuustasojen lisäksi standardista löytyy mittaristo organisaation turvatoimille, jota kutsutaan kypsyysasteeksi (eng. Maturity Level). Kun turvallisuustasoilla mitataan teknistä suojautumista uhilta niin kypsyysastella mitataan ihmisiä, toimintatapoja ja menettelytapojen turvallisuutta (ISA, 2020b). ISA (2020b) mukaan ”kypsyysaste määritellään asteeksi, jolla menettelyllinen kyky (prosessi) suoritetaan, virallistetaan, harjoitellaan ja optimoidaan.” (ISA, 2020b, s. 11). Kypsyystasoa käytetään standardin osissa 2-1, 2-2, 2-4 ja 4-1 mittaamaan kuinka turvallisuusvaatimukset täyttyvät ja kuinka niitä ylläpidetään (ISA, 2020b). Taulukossa 3 on kypsyystasot selitettynä.

TAULUKKO 3 Kypsyystason (lyh. KT) määritelmä (ISA, 2020b, s. 11)

KT 4	Parannetaan	Prosessit paranevat ajan myötä suoritus- ja tehokkuusmittareiden avulla
KT 3	Määritelty/harjaantunut	Prosessit dokumentoidaan, toteutetaan ja toistetaan
KT 2	Hallittu	Prosessit dokumentoidaan ja kuvataan, miten toiminnan toimitusta ja tuloksellisuutta hallitaan
KT 1	Alustava	Prosessit suoritetaan ad-hoc- tai paperittomalla tavalla

3 IEC 62443-4-2 Standardi

Standardin osa 4–2 painottuu komponentteihin eli mistä järjestelmät rakentuvat ja täten on siis suunnattu järjestelmien valmistajille. Leander ym. (2019) mukaan standardin osa koostuu komponenttivaatimuksista, jotka on jaoteltu neljään kategoriaan:

- Ohjelmiston sovellusvaatimukset
- Sulautettujen laitteiden vaatimukset
- Isäntälaitevaatimukset
- Verkkolaitevaatimukset

Leander ym. (2019) mainitsee tutkimuksessaan, että on myös yleistä jakaa samat vaatimukset kaikkien komponenttien kesken, ja täten nämä ilmaistaan vain yleisinä komponentti vaatimuksina (Leander ym., 2019). Taulukossa neljä kerrotaan tarkemmin mitä kullakin komponenttikategorialla tarkoitetaan.

TAULUKKO 4 Komponenttikategoriat (Leander ym., 2019)

Kategoria	Selitys
Ohjelmistosovellus	Yksi tai useampi ohjelma/palvelu, joka on vuorovaikutuksessa prosessin tai ohjausjärjestelmän kanssa ja suoritetaan sulautetulla- tai isäntälaitteella.
Sulautettu laite	Tiettyyn tarkoitukseen suunnattu laite, jossa on tietty laitteisto ja ohjelmisto, joka on kehitetty täyttämään tämä tarkoitus. Tyypillisesti laite osallistuu suoraan tai välillisesti fyysisen prosessin seurantaan tai ohjaukseen ja sillä on reaaliaikaiset vaatimukset täytettävänä.
Isäntälaite	Yleiskäyttöinen laite, jolla on ominaisuuksia useiden palveluiden suorittamiseen, yleensä "avoimella" käyttöjärjestelmällä, esim. Windows tai Linux.
Verkkolaite	Laite, joka helpottaa (tai rajoittaa) tiedonkulkua laitteiden välillä, mutta ei ole suoraan vuorovaikutuksessa prosessin kanssa.

Komponentit ovat järjestelmien rakennuspalikoita ja täten tärkeitä myös suojata. Ilman näitä komponentteja on vaikea rakentaa toimivaa järjestelmää, olipa se teollisuuden tuotantolaitos, sairaala, lentokone, metro, kauppakeskus, tai auto.

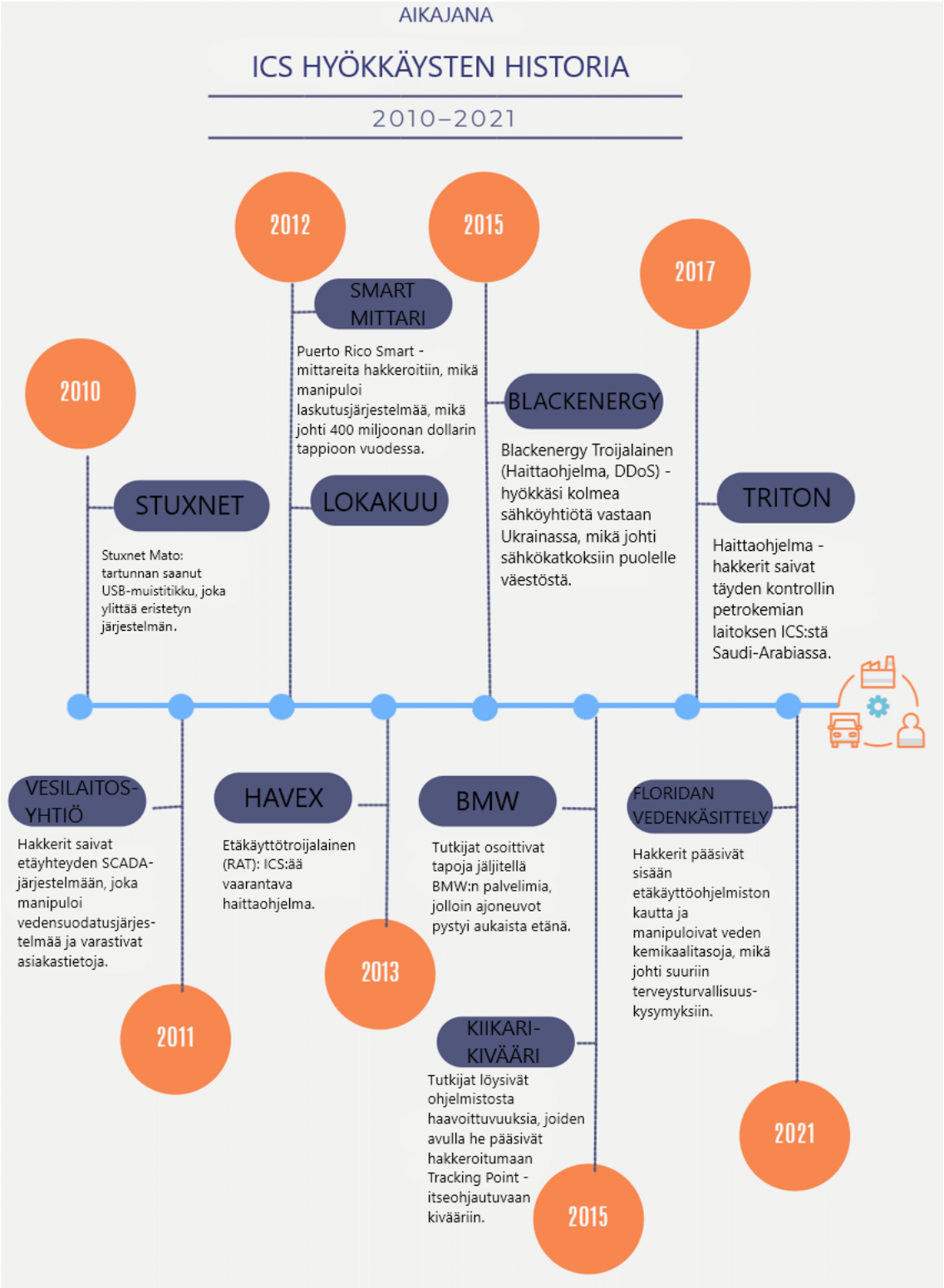
Otetaan esimerkkinä sairaala, sairaalassa on paljon erilaisia laitteistoja, tietokoneita, ja automaatiolla toimivia koneita. Kaikissa näissä laitteissa on jonkinlainen ohjelmistosovellus, joka saa laitteen toimimaan niin kuin kuuluukin. Monet näistä laitteista ovat sulautettuja järjestelmiä, jotka vaikuttavat fyysiseen maailmaan, kuten hengityskone tai elintoimintoja seuraava laite. Nämä laitteet voivat lähettää dataa eteenpäin erilaisten verkkolaitteiden kautta. Verkkolaitteita voi olla asennettuna ympäri sairaalaa erilaisilla asetuksilla. Osa laitteista kuljettaa järjestelmädataa, osa on vierailijoille tarkoitettu internet, ja osa henkilökunnalle tarkoitettu erillinen yhteys. Nämä verkkolaitteet voivat lähettää datan isäntälaitteelle, joka voi olla jokin monitorointitietokone, jossa joku valvoo

tapahtumia ja vastaa tapahtumiin asiaankuuluvalla tavalla. Isäntälaitteelta voidaan myös lähettää käskyjä ja dataa sulautetuille laitteille.

Tämä oli vain yksi pelkistetty esimerkki, kuinka komponentit voivat toimia. Samalla tavalla komponentteja käytetään muissakin paikoissa, ja tämä standardi auttaa turvaamaan näitä komponentteja hyökkäyksiltä. Varsinkin kriittisen infrastruktuurin kohdalla tämä on tärkeää.

Vuosien aikana on tapahtunut monia hyökkäyksiä kriittisiin kohteisiin kuten vesilaitoksiin, sähkölaitoksiin ja öljyjalostamoihin (Dhirani ym., 2021). Kuvassa 1 on aikajana vuosienvarrella tapahtuneista ja tiedetyistä merkittävistä teollisuuden ohjausjärjestelmiin kohdistuneista (eng. Industrial Control System, lyh. ICS) hyökkäyksistä. Kuva kuvastaa vain pientä osaa hyökkäyksistä, joita on tapahtunut, mutta kertoo kuinka haavoittuvaisia erilaiset järjestelmät ovat ja kuinka suurta tuhoa hyökkäys voi tehdä.

KUVA 1 ICS hyökkäyksien aikajana (Dhirani ym., 2021, s. 6)



Standardi auttaa pienentämällä hyökkäyksen riskiä ja varmistamalla komponenttien turvallisuuden (Leander ym., 2019). Kuitenkaan standardi ei tule ilman haasteita ja seuraavassa taulukossa 5 on löydettyjä tuloksia standardin tuomista

hyödyistä ja haasteista. Luvuissa 3.1 ja 3.2 on tarkemmin vielä löydetyistä hyödyistä ja haasteista.

TAULUKKO 5 IEC 62443-4-2 standardin hyödyt ja haasteet

HYÖDYT	HAASTEET
Läpinäkyvyys ja luottamus (Rintala, Loukkalahti, Musunuri, Haapaniemi & Hampel, 2023)	Sopivan turvallisuustason löytäminen (Dolezilek, Gammel & Fernandes 2020)
Turvaa operationaalista teknologiaa (Hollerer ym., 2022)	Päivityksien yhtenäinen ylläpito kaikissa laitteissa (Dolezilek ym., 2020; Leander ym., 2019)
Auttaa pienentämään hyökkäyksen riskiä (Martins & Vidal Garcia Oliveira, 2022)	Standardin käyttöönotto olemassa olevaan laitokseen on kallista (Dolezilek ym., 2020)
Auttaa suojautumaan hyökkäyksiltä (ISA, 2021)	Vaikea löytää tasapinoa turvallisuustasojen ja perusvaatimuksien kanssa (Fujdiak ym., 2018)
	Päivityksien ja niiden automaatioon liittyvien ohjeiden vajavaisuus (Leander ym., 2019)
	Ohjeistus digitaaliseen forensiikkaan puuttuu (Kebande, 2022)

3.1 IEC 62443-4-2 Standardin hyödyt

Standardista on paljon hyötyä yritykselle, jos yritys haluaa luoda todellakin tietoturvallisen ympäristön toiminnalleen. Standardi on suunnattu laitteistojen tuottajalle ja tätä kautta syntyy luotto tuottajaan, jos standardi on käytössä (Rintala ym., 2023). Ei myöskään pidä aliarvioida miltä yritys näyttää mahdollisten sijoittajien tai yhteistyökumppaneiden silmissä, kun kyseinen standardi on käytössä. Tämä luo läpinäkyvyyttä turvallisuuden tasosta ja mahdollisista tietoturva-aukoista (Rintala ym., 2023). Tämä kaikki ovat vain lisähyötyä yleisen turvallisuuden lisäksi.

Standardin tarkoituksena on luoda mahdollisimman turvallinen ympäristö laitteille ja täten yritykselle. Komponentit ovat todella tärkeässä roolissa ja erilaisten turvallisuustasojen kautta pystytään määrittelemään omaan tarkoitukseen sopivat turvallisuustasot. Teollisuus 4.0 lisää koko ajan yhdistettyjen laitteiden määrää ja täten erilaisten riskien määrä kasvaa (Martins & Vidal Garcia Oliveira, 2022). Onkin hyvä lähteä heti komponenttitasolta suojaamaan laitteita. Standardin avulla saadaan luottamus siihen, että laitteistot ovat oikeasti

turvallisia. Standardi auttaa tekemään ja parantamaan turvallista järjestelmä arkkitehtuuria, järjestelmän koventamista, pääsyn-, ja käyttäjähallintaa, lokienhallintaa, turvallisuuspäivityksiä, haittaohjelmasuojausta, varmuuskopiointia, turvallista etäkäyttöä, datan suojausta ja eheyttä, ja yksityisyydensuojaa (Rintala ym., 2023). Standardi on siis hyvin laaja ja auttaa suojaamaan laitteistoja hyvin.

Huomioitavaa on, että suurin osa teollisuuteen ja yrityksiin kohdistuvista hyökkäyksistä tiedetään jo entuudestaan, eli millä tavoin ja millä työkaluilla hyökkääjä mahdollisesti hyökkäyksen tekee. Tiedettyjä ja yleisiä hyökkäyksiä ovat esimerkiksi palvelunestohyökkäykset, erilaiset haittaohjelmat, porttiskannaus, tai sisäverkkoon pääsy (Dhirani ym., 2021). Tiedetyt hyökkäykset ja niiltä suojautuminen on tärkeä ottaa huomioon, ja standardia noudattamalla saa paremman valmiuden suojautua tiedetyiltä-, ja ei-tiedetyiltä hyökkäyksiltä (ISA, 2021). Onnistunut hyökkäys voi maksaa yritykselle tuhansia tai jopa miljoonia. Pahimmassa tapauksessa teollisuuden laitoksissa ihmisten fyysinen turvallisuus voi olla vaarassa (Hollerer ym., 2022). Standardi siis suojaa operatiivista teknologiaan ja täten, myös ihmisiä.

3.2 IEC 62443-4-2 Standardin haasteet

Standardi tuo mukanaan myös omia haasteitaan, ja nämä haasteet ovat hyvä huomioida, kun rupeaa suunnittelemaan standardin käyttöönottoa. Yleinen haaste on sopivan turvallisuustason löytäminen eri laitteille. Dolezilk ym. (2020) oli tutkimuksessaan huomannut, että teollisuuden alalla on tullut ehdotuksia suositella turvallisuustaso kolmea erilaisille alemman tason laitteille. Palomuurin ulkopuolella oleville IoT-laiteille tämä voi olla suotavaa, mutta muille operatiivisille laitteille kuten automaatiolaitteille, sensoreille ja releille tämä voi olla ongelmallista. Tämän turvallisuustason implementointi voisi tehdä enemmän harmia kuin hyötyä. Huomioitavaa on, että turvallisuustason implementointi asettaa laitteen päivityksen ajaksi pois käytöstä. Normaalissa isossa teollisuuden laitoksessa voi olla 12 000 operatiivista laitetta ja niiden kaikkien päivitys turvallisuustaso kolmeen kuluttaisi yli 1000 päivää ja maksaisi 60 miljoonaa (Dolezilek ym., 2020). Onkin siis tärkeää miettiä kriittisesti mitä laitteita haluaa milläkin turvallisuustasolla suojata. Standardissa IEC 62443 on muitakin tapoja suojautua ja suojata näitä laitteita, eikä osion 4–2 mukaan implementointi ole mahdollisesti paras ratkaisu.

Toinen ongelma tulee turvallisuustasojen ja perusvaatimuksien määrässä. perusvaatimuksia on seitsemän kappaletta ja turvallisuustasoja neljä. Erilaisia mahdollisia kombinaatioita tulee tällöin $4^7 = 16384$, mikä on todella paljon ja hyvää tasapainoa on vaikea saavuttaa laitteiden välillä (Fujdiak ym., 2018). Fujdiak (2018) ehdottaakin tutkimuksessaan sopivaksi turvallisuustasojen määräksi kolmea, perustuen NIST 800-82 standardiin. NIST 800-82 standardi määrittelee vaarat ja turvallisuustason joko alhaiseksi, kohonneeksi, tai korkeaksi. Kolmella eri tasolla kombinaatioiden määrä laskisi $3^7 = 2187$ mahdollisuuteen, mikä on

huomattavasti vähemmän (Fujdiak ym., 2018). Tällä tavalla olisi mahdollisuus selkeyttää standardia ja sen eri vaiheita.

Kriittinen aihe joka puuttuu standardista on päivityksiin liittyvät ohjeet ja niiden automaation turvaaminen (Leander ym., 2019). Päivitykset ovat hyvin kriittinen aihe ja varsinkin erilaisiin IIoT-laitteisiin elintärkeää. Hakkerit ja muut hyökkääjät ovat hyvin nopeita iskemään, kun uusia tietoturva-aukkoja ilmestyy. Täten nopeiden päivityksien saaminen ja niiden implementoinnin suunnittelu on ensiarvoisen tärkeää. Dolezilek ym. (2020) puhuu tutkimuksessaan, kuinka ongelma syntyy myös laitteiden päivityksien yhtenäisestä ylläpidosta. Jos yksi laite päivitetään uuteen versioon voi laitteen salausavaimet muuttua ja yhteys muihin laitteisiin katkeaa. Täten päivittäminen pitäisi tapahtua kaikkiin laitteisiin samanaikaisesti, jotta laitteidenvälinen keskusteluyhteys ei katkea. Laitteiden määrä voi olla isossa laitoksessa todella suuri ja päivitys voi tuottaa haasteita (Dolezilek ym., 2020).

Viimeisenä aiheena on digitaalisen forensiikan implementointi standardeihin. Digitaalinen forensiikkaa on edelleenkin hyvin nouseva ala, mutta silti sillä ei ole kunnolla omia standardeja tai toimintamalleja. Myöskin kaikista IoT-laitteisiin keskittyvistä standardeista puuttuu toimintamallit forensiikan hyödyntämiseen (Kebande, 2022). Forensiikka on kriittinen aihealue vikojen synnyn ja hyökkäysten alkuperän löytämiseksi, ja mahdollisesti tiedon palauttamiseksi. Standardi ottaa huomioon vain uhat, haavoittuvuudet, riskit ja näiden lieventämisen yleisellä tasolla, mutta standardi ei ota huomioon digitaalista forensiikkaa (Kebande, 2022).

Tärkeintä on muistaa kuitenkin, että turvallisuus on koko ajan toimiva prosessi eikä vain kertatuote (Schneier, 2000). Hyökkäykset muuttuvat ja laitteistot paranevat. Tämän takia on tärkeää muistaa turvallisuus kaikissa arkipäivän prosessissa ja pitää laitteistot päivitettynä.

4 Yhteenveto

Tämän tutkielman tarkoituksena oli selvittää IEC 62443-4-2 standardin hyötyjä ja haasteita. Samalla oli myös tarkoitus kartoittaa yleiskuvaa standardista ja missä tutkimus on tällä hetkellä menossa. Standardia käytetään yhä enemmän teollisuus-, automaatio- ja IoT-laitteissa. Tällä hetkellä maailma ja teollisuus digitalisoituu suurella vauhdilla, mutta laitteiden tietoturvallisuus ei aina kehity yhtä nopeasti. Näiden perusteella tutkimuksessa tutkimuskysymyksinä on:

- Mitkä ovat IEC 62443-4-2 standardin hyödyt?
- Millaisia haasteita IEC 62443-4-2 standardissa voi ilmetä?

Tutkimus tehtiin systemaattisena kirjallisuuskatsauksena, ja lähteitä etsittiin erilaisista tietokannoista kuten ACM Digital Library, Computer Science Database ja IEEE Xplorer. Hakuprosessista ja metodeista on laajemmin tietoa luvussa 1.2 Tutkimusmenetelmä. Tutkimus osoitti, että standardin osiota 4-2 on tutkittu verrattain vähän. Standardi ei itsessään ole uusi, mutta tutkimusaihe standardin osiosta 4–2 on vain muutaman vuoden vanha. Tämä tuotti haasteita löytää sopivaa tietoa ja luotettavia lähteitä. Uuden tutkimusaiheen parissa ei ole monia tutkimuksia vielä tehty, eli viittauksia on määrällisesti vähän erilaisiin tutkimuksiin. Myös pääsy itse viralliseen standardiin on maksumuurin takana.

Yleiskuvaa standardista sai kuitenkin rakennettua ja sen osiosta 4–2 pystyi tekemään pintapuolista arviointia liittyen sen mahdollisuuksiin ja haasteisiin. Tämän standardin kohdalla kuten muissakin standardeissa nousee pinnalle painotus tarkkaan käyttökohteen arviointiin. Tämä tarkoittaa sitä, että pitää ymmärtää missä ja miten standardin implementoi.

Tämän kirjallisuuskatsauksen mukaan standardin osio 4–2 mahdollistaa vahvan suojauksen ja tekee tietoturvasta läpinäkyvämpää ja luotettavampaa sidosryhmille. Standardi auttaa myös pienentämään hyökkäyksien riskejä, suojaamaan hyökkäyksiltä ja turvaamaan operatiivisen teknologian. Operatiivisen teknologian suojaus on tärkeä suunnitella riittävälle turvallisuustasolle mutta ei kuitenkaan liian vahvaksi. Kriittinen suunnittelu on avainasemassa. Osio onkin oivallinen teollisuuden laitteistoille, jos haluaa varmistua laitteiden turvallisuudesta alusta alkaen.

Haasteita standardissa ja osiossa 4–2 aiheuttaa sen laajuus ja rahallinen panostus. Standardoiminen tietylle turvallisuustasolle on aina oma prosessinsa. IEC 62443 standardi on itsessään jo yli 1000 sivua, mutta osio 4–2 on vain osa siitä. Tämä vaatii panostusta standardin ymmärtämiseen ja siihen, kuinka tavoitteisiin päästään. Tästä tulee samalla kuluja ja varsinkin jo valmiin laitoksen laitteiden muuntaminen standardiin sopivaksi voi maksaa miljoonia yritykselle (Dolezilek ym., 2020). Samalla kun vanhoja laitteita vaihdetaan tai päivitetään, voi laitos joutua olemaan poissa käytöstä, mikä tuottaa lisää kuluja. On tärkeää myös suunnitella mitkä laitteet ovat kannattavia toteuttaa osion mukaan ja mille turvallisuustasolle laitteet asetetaan. Mitä korkeampi turvallisuustaso on, sitä enemmän

se vaatii panostusta. Turvallisuustasojen kanssa on myös vaikea löytää sopivaa tasapainoa, koska turvallisuustasoja on neljä ja perusvaatimuksia seitsemän, mikä tuottaa yhteensä $4^7 = 16384$ erilaista kombinaatiota (Fujdiak ym., 2018).

Viimeisenä haasteena tutkielmassa ilmeni se, että standardista puuttuu ohjeistus päivityksiin ja niiden turvalliseen automatisointiin (Leander ym., 2019). IoT-laitteisiin on kuitenkin ensisijaisen tärkeää saada nopeasti päivitettyä viimeisimmät suojaukset. Viimeinen löydetty puutos oli digitaalisen forensiikan puuttuminen (Kebande, 2022). Digitaalinen forensiikka on ensisijaisen tärkeää hyökkäykseen johtaneiden syiden selvittämisessä ja datan palauttamisessa. Vaarana voi olla liian vahvasti suojatut laitteet ja näin ollen forensiikan tekeminen laitteelle voi vaikeutua.

Tutkielmassa saatiin selville haasteita ja hyötyä liittyen IEC 62443-4-2 standardiin, mutta aiheeseen on tarve saada vielä lisätutkimusta. Koska aihe on vielä uusi ja standardia päivitetään ja rakennetaan edelleen, olisi tärkeää saada tietoa yrityksiltä, jotka ovat ottaneet standardin käyttöön. Yrityksillä on kuitenkin käytännöntietoa siitä, mitä hyötyjä ja haasteita standardi tuottaa ja miten sitä voisi parantaa. Tutkimus vaatisi lisää yhteistyötä ja haastatteluita yrityksien kanssa, jotta standardista saataisiin parempaa ja luotettavampaa tietoa. Tutkimuskysymyksiä tai -aiheita voisivat olla esimerkiksi:

- IEC 62443-4-2 standardin tuoma arvo yritykselle
- Kuinka IEC 62443-4-2 standardin käyttöönotto onnistui tai epäonnistui
- IEC 62443-4-2 standardin käyttöönoton elinkaari
- IEC 62443 standardin tulevaisuuden näkymät ja kehityskohteet

Tutkielma ja lähteinä käytetyt tutkimukset antavat kuvan, että standardi yleisesti ja sen osiota 4–2 tullaan käyttämään yrityksissä aiempaa enemmän. Osa tutkimuksista puhuu standardista jo tällä hetkellä de facto standardina, eli standardi tulisi olemaan yleisesti se, mitä pitäisi kaikkialla teollisuuden automaatiossa käyttää. Tämä on hyvä, sillä standardi antaa todella laajaa turvaa, mutta osa standardin osioista ovat uusia kuten osio 4–2. Standardia myös edelleen päivitetään ja siihen lisätään osioita. Onkin ensisijaisen tärkeää tehdä tutkimusta aiheesta ja saada näin parempaa kuvaa standardista. Standardi vaikuttaa kuitenkin teollisuuteen ja erilaisiin laitoksiin, jotka ovat tärkeitä yhteiskunnalle. Osa laitoksista, kuten energialaitokset ovat osa yhteiskunnan kriittistä infrastruktuuria, ja täten ne tarvitsevat vahvaa suojautumista.

LÄHTEET

Dhirani, L. L., Armstrong, E. & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*, *21*(11), 3901. https://doi.org/10.3390/s21113901

Dolezilek, D., Gammel, D. & Fernandes, W. (2020). Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems. *15th International Conference on Developments in Power System Protection (DPSP 2020)*, 1–6. https://doi.org/10.1049/cp.2020.0016

Erwin, K., Kloibhofer, R., Díaz, V. H. & Castillejo, P. (2021). Security Assessment of Agriculture IoT (AIoT) Applications. *Applied Sciences*, *11*(13), 5841. https://doi.org/10.3390/app11135841

Fujdiak, R., Mlynek, P., Blazek, P., Barabas, M. & Mrnustik, P. (2018). Seeking the Relation Between Performance and Security in Modern Systems: Metrics and Measures. *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, 1–5. https://doi.org/10.1109/TSP.2018.8441496

Hohenegger, A., Krummeck, G., Baños, J., Ortega, A., Hager, M., Sterba, J., Kertis, T., Novobilsky, P., Prochazka, J., Caracuel, B., Sanz, A. L., Ramos, F., Blasum, H., Brotz, M., Gries, C., Vögler, T., Neškudla, J., Rollo, J., Burgstaller, L., … & Schulz, T. (2021). Security certification experience for industrial cyberphysical systems using Common Criteria and IEC 62443 certifications in certMILS. *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, 25–30. https://doi.org/10.1109/ICPS49255.2021.9468241

Hollerer, S., Sauter, T., & Kastner, W. (2022). Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3538969.3543814

ISA - International Society of Automation. (2020a). Quick Start Guide: An Overview of ISA/IEC 62443 Standards, Security of Industrial Automation and Control Systems. *ISA - Global Cybersecurity Alliance.* Haettu osoitteesta https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

ISA - International Society of Automation. (2020b). Security Lifecycles in the ISA/IEC 62443 Series, Security of Industrial Automation and Control Systems. *ISA - Global Cybersecurity Alliance*. Haettu osoitteesta https://gca.isa.org/hubfs/21-

29%20-%20ISAGCA/ISAGCA%20Security%20Lifecycles%20whitepaper%20FINAL.pdf

ISA - International Society of Automation. (2021). IIoT Component Certification Based on the 62443 Standard. ASCI-Automation Standards Compliance Institute, *ISA - Global Cybersecurity Alliance.* Haettu osoitteesta https://f.hubspotusercontent10.net/hubfs/5382318/ISCI%20and%20ISAGCA%20Joint%20IIoT%20Study%20-%20Full%20Study-5.pdf

Kebande, V. R. (2022). Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. *Forensic Science International: Reports*, *5*, 100257. https://doi.org/10.1016/j.fsir.2022.100257

Leander, B., Čaušević, A., & Hansson, H. (2019). Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3339252.3341481

Longueira-Romero, Á., Iglesias, R., Flores, J. L. & Garitano, I. (2022). A Novel Model for Vulnerability Analysis through Enhanced Directed Graphs and Quantitative Metrics. *Sensors*, *22*(6), 2126. https://doi.org/10.3390/s22062126

Ma, Z., Hudic, A., Shaaban, A. & Plosz, S. (2017). Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems. *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 153–159. https://doi.org/10.1109/EuroSPW.2017.65

Martins, T. & Vidal Garcia Oliveira, S. (2022). Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported. *Sensors*, *22*(20), 8024. https://doi.org/10.3390/s22208024

Mugaraza, I. Flores, J. L. & Montero, J. L. (2020). Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era. *Sensors*, *20*(24), 7160. https://doi.org/10.3390/s20247160

Okoli, C. & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

Rintala, J., Loukkalahti, M., Musunuri, S., Haapaniemi, J. & Hampel, C. (2023). Is the cybersecurity standard IEC 62443 applicable to distribution substations? *27th International Conference on Electricity Distribution (CIRED 2023)*, 1554–1558. https://doi.org/10.1049/icp.2023.0931

Santos, H., Oliveira, A., Soares, L., Satis, A. & Santos, A. (2021). Information Security Assessment and Certification within Supply Chains. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–6. https://doi.org/10.1145/3465481.3470078

Schmittner, C., Shaaban, A. M. & Macher, G. (2022). ThreatGet: Ensuring the Implementation of Defense-in-Depth Strategy for IIoT Based on IEC 62443. *2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS)*, 1–6. https://doi.org/10.1109/ICPS51978.2022.9816864

Shaaban, A. M., Chlup, S., El-Araby, N. & Schmittner, C. (2022). Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. *Applied Sciences*, *12*(11), 5653. https://doi.org/10.3390/app12115653

Shaaban, A. M., Schmittner, C., Gruber, T., Mohamed, A. B., Quirchmayr, G. & Schikuta, E. (2018). CloudWoT - A Reference Model for Knowledge-based IoT Solutions. *Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services*, 272–281. https://doi.org/10.1145/3282373.3282400

Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons Inc.