Artturi Hoffrén

IEC 62443 -SERTIFIKAATTIEN TARVE SUOMALAISSA YRITYKSISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Hoffrén, Artturi
IEC 62443 -sertifikaattien tarve suomalaisissa yrityksissä
Jyväskylä: Jyväskylän yliopisto, 2024, 64 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Tämän tutkimuksen tavoitteena oli selvittää IEC 62443 -sertifikaattien tarvetta suomalaisissa yrityksissä. Tutkimus on erittäin ajankohtainen, sillä tietoturvan merkitys on kohonnut hyökkäysten yleistyessä. Etenkin automaatioympäristöjen suojaaminen on tärkeää, sillä Suomen kriittisen infran toiminta perustuu näihin ympäristöihin. Automaatioympäristöjen riskit ovat myös suuret sen vuoksi, että ihmishenget saattavat olla vaarassa, jos automaatioympäristön kyberturva vaarantuu. Tutkimuksessa käsiteltävä IEC 62443 -standardiperhe on kehitetty vastaamaan automaatioympäristöjen kasvaviin tietoturvatarpeisiin. Tutkimuksen päätutkimuskysymyksenä oli: ”Onko Suomalaisissa yrityksissä havaittu tarvetta IEC 62433 sertifikaateille?”.

Tutkimuksen teoriaosuudessa kerrotaan ensimmäiseksi automaatioympäristöjen merkityksestä, sen perusperiaatteista, ja sen eroista IT-ympäristöihin. Toisessa teorialuvussa kerrotaan IEC 62443 standardin sisällöstä. Luvussa avataan ylätasolla standardin eri osioiden sisältöä, kerrotaan mihin standardin osioihin voi sertifioitua, ja kerrotaan miten standardiin voi sertifioitua. Itse tutkimuksen ensimmäisessä osioissa selvitettiin julkisista lähteistä yrityksiä, joilla on sertifikaatit IEC 62443 standardiin liittyen. Luvussa todettiin, että sertifikaatteja on pääasiassa suurilla yrityksillä. Luvussa myös havaittiin, ettei sertifikaatteja ole monella yrityksellä.

Tutkimuksen toisessa osassa haastateltiin kahdeksaa suomalaista yritystä. Haastatteluissa selvitettiin, kuinka tuttu standardi on yritykselle, onko yrityksessä hyödynnetty standardia, millaista kysyntää näille on kohdistunut standardiin liittyen, ja mitkä ovat tulevaisuuden suunnitelmat standardiin liittyen. Standardi oli tuttu kaikille haastatelluille yrityksille. Kaikissa yrityksissä oli esiintynyt etenkin ulkoista kysyntää standardille. Suuri osa yrityksistä hyödynsi tiettyjä standardin osia toiminnassaan. Usealla yrityksellä oli myös lähitulevaisuudessa tarkoituksena sertifioitua etenkin standardin 4-1 osioon. Osioon 4-1 sertifioitumista tuki, tai seurasi usein sertifioituminen 4-2 osuuteen. Haastattelujen kautta saatiin vastaus tutkimuskysymykseen: Suomalaisissa yrityksissä on havaittu tarvetta IEC 62443 mukaisille sertifikaateille. Standardin merkityksen uskotaan tutkimuksen pohjalta kasvavan lähitulevaisuudessa.

Asiasanat: IEC 62443, Automaatioympäristö, OT-ympäristö, Tietoturva, Kyberturva

ABSTRACT

Hoffrén, Artturi
The need for IEC 62443 certificates in Finnish companies
Jyväskylä: University of Jyväskylä, 2024, 64 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

This study aimed to find out the need for IEC 62443 certificates in Finnish companies. The research is very timely, as the importance of information security has increased as attacks become more common. Protecting automation environments in particular is important because Finland's critical infrastructure is based on these environments. The risks related to automation environments are also high because human lives may be at risk. IEC 62443 standard discussed in the study has been developed to meet the growing information security needs of automation environments. The main research question of the study was: "Is there a need for IEC 62433 certificates in Finnish companies?".

In the theory part of the study, the meaning of automation environments, their basic principles, and their differences from IT environments are explained. The second theoretical chapter describes the content of the IEC 62443 standard. The contents of different sections of the standard are opened at a high level, it is explained which sections of the standard can be certified to, and how can one be certified against the standard. In the first sections of the research itself, companies with IEC 62443 certificates were identified from public sources. It was stated that certificates are mainly held by large companies. It was also found that many companies do not have certificates.

In the second part of the study, eight Finnish companies were interviewed. In the interviews, it was found out how familiar the company is with the standard, whether the company has used the standard, what kind of demand has been directed at them in relation to the standard, and what are the plans in relation to the standard. The standard was familiar to all interviewed companies. There had been especially external demand for the standard in all companies. A large number of companies used certain parts of the standard in their operations. In the near future, several companies also had the intention of becoming certified, especially for section 4-1 of the standard. Certification to section 4-1 was supported or often followed by certification to section 4-2. The answer to the research question obtained was: Finnish companies have found a need for IEC 62443-based certificates. The importance of the standard is believed to increase in the near future.

Keywords: IEC 62443, Automation environment, OT-environment, Information security, Cybersecurity

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Nyky-yhteiskunnassa tietoturvan merkitys on kohonnut entisestään, ja kyberhyökkäykset ovat yhä vakavampi uhka yrityksille. Voimme melkein päivittäin lukea erilaisista hyökkäyksistä ja haavoittuvuuksista, joita julkisten ja yksityisten tahojen tietojärjestelmissä on havaittu. Hyökkäävä puoli on aktiivinen, mutta pystyykö puolustautuva puoli vastaamaan riittävän tehokkaasti.

Uutisartikkeleista voi huomata, että fokus on selkeästi IT-ympäristöjen kyberturvassa, mutta automaatioympäristöjen (OT, Operational Technology) kyberturva jää vähemmälle huomiolle. Tämä johtunee osaksi siitä, että IT-ympäristön hyökkäyspinta-ala on suurempi, ja IT-ympäristö on tutumpi niin uutisten lukijoille kuin toimittajillekin. Hyökkäys OT-ympäristöön voi kuitenkin olla merkittävämpi, koska taloudellisten vaikutusten lisäksi myös ihmishenget saattavat olla vaarassa (Setola ym., 2019).

OT-ympäristöjen kyberturvan merkitys korostuu etenkin epävarmoina aikoina, joina valtiolliset toimijat käyttävät mahdollisesti kyberympäristöä hybridisotaan, kuten Ukrainassa 2015 (Case, 2016). Tällöin Ukrainan läntisen alueen sähköverkkoon murtauduttiin, ja noin 230 tuhatta kuluttajaa jäi ilman sähköjä. Iskun takana oli todennäköisesti venäläinen ryhmä nimeltään ”Sandworm”. Iskuilla OT-ympäristöön vois siis olla erittäin laajoja vaikutuksia.

Aihealue on erityisen ajankohtainen vallitsevan maailmantilanteen vuoksi. Tässä tutkimuksessa käsiteltävä IEC 62443 -standardiperhe kehitettiin alun perin vastaamaan automaatioympäristöjen kasvaviin tietoturvatarpeisiin (International Society of Automation, 2020). Tällöin havaittiin, että OT-ympäristöjen tietoturvaan tarvittiin järjestelmällistä kehitystä ja standardisoituja käytäntöjä. Vaikka standardin parissa on tehty töitä jo yli kaksikymmentä vuotta, OT-ympäristöjen tietoturva on silti monesti heikompi kuin IT-ympäristöjen tietoturva (Mansfield-Devine, 2019).

IEC 62443 -standardiperhettä pidetään yhtenä tämän päivän merkittävimmistä OT-ympäristön tietoturvaan keskittyneistä julkaisuista, joka on kehittynyt paljon ajan myötä (Piggin, 2013). Tämä tutkimus tarkastelee IEC 62443 -standardien käyttöönoton tarvetta ja hyötyjä suomalaisten yritysten näkökulmasta tavoitteenaan tuoda esiin sertifikaattien merkitys liiketoimintaympäristössä, jossa

kyberuhkat ovat jatkuvasti kasvava huolenaihe. Tutkimuksessa avataan myös standardiperheen eri osioiden sisältöjä.

Tutkimuksen teoria perustuu kirjallisuuskatsaukseen, jossa hyödynnetään tutkimusartikkeleita, raportteja ja muita akateemisia lähteitä, jotka tarjoavat tietoa tietoturvan haasteista ja standardien vaikutuksesta liiketoimintaan. Keskeisiä lähteitä ovat esimerkiksi IEC:n viralliset julkaisut, kansainväliset tutkimukset sekä suomalaisten yritysten käytännön kokemukset standardien soveltamisesta ja tarpeista. Tutkimuksen teorialuvuissa esitellään aluksi OT-kyberturvan käsitettä, tämän jälkeen IEC 62443 -standardin sisältöä.

Varsinaisessa tutkimuksessa haastatellaan suomalaisia yrityksiä näiden tarpeista standardiin liittyen. Tutkimuksessa pyritään ymmärtämään, kuinka hyvin standardi tunnetaan yrityksissä, ja millaisia tarpeita tätä kohden nähdään tulevaisuudessa. Tämän monipuolisen lähdemateriaalin avulla pyritään luomaan kattava kuvan IEC 62443 -sertifikaattien tarpeesta suomalaisissa yrityksissä. Tutkimuksessa havaittiinkin, että IEC 62443 -standardiin liittyvien tarpeiden määrä on kasvamassa. Tämän vuoksi IEC 62443 -standardin merkitys on myös kasvamassa. Monilla yrityksillä on myös suunnitelmissa sertifioitua tiettyihin standardin osiin.

On huomioitava, että OT-ympäristöjen kyberturvasta on saatavilla melko vähän tieteellistä materiaalia eivätkä yritysten käyttämät menetelmät perustu aina tieteellisesti tutkittuun dataan. OT-ympäristöjen kyberturvaa on rakennettu usein IT-ympäristön näkökulmasta. OT-ympäristöjen kyberturvaa rakennetaan usein myös perustuen viitekehyksiin, kuten ISO 27000 -standardiin. Standardit eivät kuitenkaan perustu vain tieteellisiin tutkimuksiin. Tämän vuoksi tämä tutkimus on käytännönläheinen. Tutkimus vastaa osaksi myös siihen, miten erityisesti OT-ympäristöjen kyberturvan kasvava tarve nähdään organisaatioissa.

2 MITÄ ON OT-KYBERTURVA?

Tässä luvussa vastataan avustaviin kysymyksiin 1. ”Mitä tarkoittaa OT-kyberturva?” ja 2. ”Miten OT-kyberturva eroaa IT-kyberturvasta?”. Ensimmäiseen avustavaan kysymykseen vastataan alaluvussa 2.1 ja 2.3, ja toiseen alaluvussa 2.2. Jotta näitä teemoja voidaan käsitellä, tulee avata OT ja ICS käsitteitä lukijalle.

Automaatioympäristöjen teknologia tunnetaan nimellä OT (Operational Technology). OT-ympäristöissä valvotaan ja ohjataan kriittistä infrastruktuuria kuten sähköverkkoja, vedenjakelua, lämmöntuotantoa ja valmistavaa teollisuutta (Mansfield-Devine, 2019; Murray ym., 2017). OT-ympäristössä suurin osa toimijoista on laitteita, jotka kommunikoivat keskenään. Nämä laitteet vaikuttavat usein fyysiseen maailmaan. Näitä laitteita käytetään fyysisen maailman ilmiöiden havainnoimiseen tai siihen vaikuttamiseen. Laitteita näihin tarkoituksiin voivat olla esimerkiksi erilaiset sensorit, pumput tai moottorit (Stouffer ym., 2022).

Teollisuuden ohjausjärjestelmä eli Industrial Control System (ICS) tarkoittaa teollisuuden ohjausjärjestelmää. Joissakin lähteissä niistä käytetään myös IACS (Industrial Automation and Control System) nimeä. Ohjausjärjestelmiä on monenlaisia ja moneen eri tarkoitukseen. Teollisuuden ohjausjärjestelmillä ohjataan OT-verkon laitteita (Krotofil & Gollmann, 2013). Ohjausjärjestelmät on suunniteltu teollisuuden tarpeiden mukaisesti. Teollisuuden ohjausjärjestelmä ei ole yksittäinen sovellus, vaan kyseessä on laajempi, automaatioympäristön ohjaamista varten suunniteltu kokonaisuus (AlMedires & AlMaiah, 2021).

2.1 OT-ympäristöjen merkitys ja johtaminen

2.1.1 OT-ympäristöjen merkitys

Jotta voidaan ymmärtää OT-ympäristöjen merkitys, tulee ymmärtää mitä kaikkea teollisuuden ohjausjärjestelmillä ohjataan. OT-ympäristöjä nähdään kaikissa

kriittiseen infraan liittyvissä ympäristöissä, ja näitä käytetään muun muassa seuraavilla toimialoilla (Stouffer ym., 2022):

- Kemian ala
- Logistiikkalaitokset
- Valmistava teollisuus
- Padot
- Puolustus
- Hätäpalvelutoiminta
- Energian tuotanto
- Energian välitys
- Elintarvikevalmistus
- Terveydenhoito
- Ydinvoima ja tähän liittyvä materiaalinhallinta
- Kuljetusjärjestelmien hallinta
- Vesihuolto
- Jätehuolto

Kuten nähdään, listan jokainen toimija on merkittävä yhteiskunnan toiminnan kannalta. Jos tietoturva näillä osa-alueilla ei ole kunnossa, tietoturvatapahtumilla voi olla hyvin merkittäviä vaikutuksia.

Johdannossa esiteltiin esimerkki tilanteesta, jossa Ukrainan läntisen alueen sähköverkkoon murtauduttiin, ja noin 230 tuhatta kuluttajaa jäi ilman sähköjä. Vastaavia esimerkkejä on lukuisia. Monet näistä ovat jääneet onneksi vain yrityksen tasolle. Esimerkiksi vuonna 2017 Triton-haittaohjelman havaittiin pyrkivän hyökkäämään Saudi Arabialaisen öljy- ja kaasutehtaan kimppuun. Arvioitiin, että hyökkäyksen yhtenä tavoitteena oli aiheuttaa kuolonuhreja. Tämä haittaohjelma pyrki vaikuttamaan prosessinohjaukseen liittyvään kriittisen turvajärjestelmään (Firoozjaei ym., 2022). Turvajärjestelmät ovat kriittisiä järjestelmiä poikkeustilanteissa. Jos ulkopuolinen taho pääsee vaikuttamaan turvajärjestelmään, voivat vaikutukset olla katastrofaaliset.

Toisena esimerkkinä voinee mainita vuonna 2016 vesilaitokselle tehty hyökkäys. Tässä haittaohjelma pääsi käsiksi ohjausjärjestelmään ja vaikutti veden virtauksen säätimiin sekä kemikaalien sekoittumiseen (Makrakis ym., 2021). Hyökkäys havaittiin ajoissa, mutta riskinä olisi voinut olla esimerkiksi veden myrkyttäminen vaikuttamalla kemikaalien sekoittumisprosessiin.

Kolmas esimerkki on Colonial Pipelineen kohdistunut hyökkäys vuonna 2021, jossa Yhdysvaltain suurin polttoaineputkisto joutui kyberhyökkäyksen kohteeksi. Hyökkäys aiheutti polttoaineen toimitushäiriöitä eteläisillä ja itäisillä osilla Yhdysvalloissa. Ryhmä nimeltään DarkSide hyödynsi järjestelmän haavoittuvuuksia saaden ohjausjärjestelmän haltuunsa. Lopulta Colonial Pipeline maksoi hakkereille lunnaat (Beerman ym., 2023).

Kuten esimerkeistä nähdään iskuilla OT-ympäristöön voi olla erittäin laajoja vaikutuksia. OT-ympäristöön kohdistuvat uhat eivät kohdistu vain rahalliseen menetykseen, vaan uhan alla voi olla ihmisten terveys ja henki. Tämä

korostaa OT-ympäristöjen merkitystä ja etenkin sitä, miksi OT-ympäristöjen tietoturvaan tulisi kiinnittää erityisesti huomiota.

2.1.2 OT-tietoturvan johtaminen

Tietoturvaa, kuten mitä tahansa muutakin osa-aluetta, tulee hallita ja johtaa, jotta siinä voidaan onnistua. Lehto & Limnell (2021) toteavat, että tietoturvasta on tullut yksi tärkeimmistä prioriteeteista niin hallituksille kuin muillekin organisaatioille. Heidän mukaansa sen johtamiseen tarvitaan selkeää strategista johtamismallia.

Myös Johnston ja Hale (2009) toteavat, että tietoturvan hallinta on välttämätön osa koko organisaation strategista hallintaa. Heidän mukaansa tietoturvan hallinnan kautta tietoturvaan liittyvät päätökset tukevat koko organisaation liiketoiminnallisia tavoitteita. Tällöin tietoturva ei olisikaan kustannus, kuten useasti tietoturvaan viitatessa ajatellaan (Ioannidis ym., 2013). Tietoturva voidaan tällöin nähdä investointina organisaation tulevaisuuteen. Tietoturva olisi siis vastaava investointi kuin uuden tuotantolaitteen hankkiminen.

Johnstonin ja Halen (2009) mukaan organisaatioiden tulee olla proaktiivisia tietoturvaan liittyvissä kysymyksissä. Tähän kykeneminen vaatii johdon ja muun organisaation valveutuneisuutta tietoturvaan. Jos organisaatio kulkee jälkijunassa esimerkiksi tietyn haavoittuvuuden suojauksen kanssa, on ymmärrettävää, että tällöin jää auki enemmän hyökkäyspinta-alaa.

Tietoturvan johtamismallin määrittäminen ei kuitenkaan ole aina yksinkertaista. Tietoturvan johtamiseen, ja siihen liittyvien vastuiden jakamiseen, on olemassa lukuisia erilaisia malleja (Savaş & Karataş, 2022). Vaikka malleja on erilaisia, Peltierin (2014, s. 16) mukaan vastuu tietopääoman turvaamisesta on lopulta ylimmällä johdolla. Kun tietoturva on osa organisaation strategista hallintaa, tietoturva integroituu helpommin organisaation tavoitteisiin (Johnston & Hale, 2009). Tällöin tietoturvaan liittyvät aloitteet saavat paremmin tukea johdon suunnalta.

Johdon tuki ja sitoutuminen ovatkin tietoturvan onnistumisen kannalta kriittisiä elementtejä (Knapp ym., 2006). Tästä huolimatta Straubin ja Welken (1998) mukaan tietoturvaa on väheksytty usein johdon ja työntekijöiden toimesta. Heidän mukaansa tämä on johtanut tietoturvan heikentyneeseen tasoon, jonka vuoksi myös vahingot ovat tuhoisampia. Tietoturvaan liittyvän valveutuneisuuden voidaan kuitenkin uskoa lisääntyneen, johtuen lukuisista hyökkäyksistä, joista uutisoidaan lähes päivittäin. Kuitenkin, tietoturvakulttuuri on usein vajavainen (Triplett, 2022). Sen rakentamisen tulisi olla yksi tärkeimmistä tehtävistä tietoturvaa kehittäessä (Uchendu ym., 2021).

Sen, että johto ei sitoudut tietoturvaan, on havaittu lisäävän organisaatioiden haavoittuvuutta (Rhee ym., 2012). Samassa tutkimuksessa havaittiin, että johdon tietoisuuden ollessa riittämättömällä tasolla, johto saattoi olla liian optimistista uhkia kohtaan. Tällöin johto aliarvioi helposti haavoittuvuuksien vaikutusta, ja yliarvioi organisaation kykyä vastata uhkiin. Jos johto ei ole sitoutunut tietoturvan parantamiseen, ei ymmärrä tietoturvan merkitystä, eikä käsitä

heikkoon tietoturvaan liittyviä riskejä, on organisaatio todennäköisesti haavoittuvaisempi. Tämä korostaa entisestään johdon merkitystä tietoturvan hallinnassa.

Johto ei aina ymmärrä tietoturvaan liittyviä riskejä. Johdon ymmärrys ja koulutus aiheesta ei ole välttämättä riittävän korkealla tasolla (Knapp ym., 2006). Jos esimerkiksi keskustellaan teknisistä riskeistä, on mahdollista, ettei johdolla ole mitään käsitystä aiheesta. Nykyään on kuitenkin yleistynyt CISO:n (Chief Information Security Officer) rooli. CISO:n voidaan olettaa tietävän laajemmin tietoturvaan liittyvistä asioista (Fleckenstein & Fellows, 2018, s. 167–169). Tällaista roolia ei kuitenkaan ole läheskään kaikissa organisaatioissa, jonka vuoksi ongelma on vieläkin läsnä. On myös mahdollista, että CISO:lla ei ole tarpeeksi hyvää käsitystä OT-ympäristöjen perusperiaatteista, jotta tämä pystyisi ottamaan kantaa OT-kyberturvaan.

Boundin (1988) mukaan turvallisuuteen liittyvistä asioista tulisi keskustella johdon kanssa tietyn kaavan mukaan. Hänen mukaansa asia tulee esittää johdolle niin, että heidän on helppo sitoutua turvallisuuden parantamiseen. Bound mainitsee johtoa kiinnostavia asioita olevan esimerkiksi vahingon seuraukset, kustannukset ja lainsäädännön.

Vaikka Bound viittaa perinteiseen turvallisuuteen, voidaan tästä vetää yhteys tietoturvaan laajemmassa käsitteessä. Samat haasteet esiintyvät, kun tietoturvasta keskustellaan johtavassa asemassa olevan henkilön kanssa. Tällä henkilöllä ei mahdollisesti ole tarpeeksi ymmärrystä tai aikaa keskustella syvällisesti tietoturvasta. Tämän vuoksi johdolle tulee esittää asiat heitä kiinnostavasta näkökulmasta. Näiden periaatteiden voidaan nähdä toimivan etenkin tuotannon johdon kanssa.

Cleveland & Cleveland (2018) tukevat Boundin esittämiä periaatteita. Heidän mukaansa eri tilanteissa tulee tietoturvaa johtaa, ja siitä tulee keskustella eri mallilla. Esimerkiksi tiedon suojauksen johtamisessa tarvitaan erilaisia ominaisuuksia kuin toipumisvaiheessa. Ydinsanomana tässä on, että tärkeintä on tuoda johdolle tieto sillä tavalla, että he pystyvät sen perusteella tekemään kriittisiä päätöksiä.

Basie Von Solms ja Rossouw Von Solms (2004) mainitsevat yhden tietoturvan johtamisen synneistä olevan se, ettei ymmärretä tietoturvan olevan johdon vastuualueella. Synnillä he tarkoittavat virhettä, jonka seurauksena kattavan tietoturvasuunnitelman käyttöönotossa voi tulla haasteita. Heidän mukaansa tietoturva on liiketoiminnallinen, ei tekninen haaste.

Tietoturvan heikon tason voisi helposti sysätä johdon harteille. Tietoturvaan liittyvät päätökset eivät kuitenkaan ole yksinkertaisia johdollekaan. Yksi haaste, jonka johto kohtaa tietoturvan hallinnan kanssa, on tietoturvan taloudellinen puoli. Tietoturvan taso paranee investoimalla. (Straub Jr, 1990) Johdon tulee määrittää, kuinka paljon tietoturvaan tulisi investoida. Investoinnin tulisi olla suhteessa havaittuun riskiin ja haavoittuvuuteen (Gordon & Loeb, 2002). Gordon ja Loeb esittävät laskelmiin perustuvan mallin, johon tietoturvasijoitusten määrän tulisi suhteutua.

Parhaissa tapauksissa tietoturvainvestointeja voidaan pitää strategisina investointeja, jotka tuovat kilpailullista etua (Kosutic & Pigni, 2022). Andersonin ja Choobinehin (2008) mukaan johdon tulee kuitenkin verrata tietoturvainvestointeja muihin investointeihin. Johto siis miettii, saisiko investoinneille parempaa vastinetta muista kohteista. Artikkelin mukaan päätöksentekijän riskinsietokyky vaikuttaa myös investoinnin määrään. Kun edellä esitettyjä teorioita vertaillaan, voidaan ymmärtää, ettei investoinnin koon määrittäminen ole helppoa. Organisaatioiden resurssit ovat kuitenkin yleensä rajalliset. Tämän vuoksi tietoturvainvestoinnit vaativat priorisointia.

On myös huomioitava, että erilaiset päätöksentekijät ovat valmiita tekemään erikokoisia investointeja tietoturvaan. Huang, Hu ja Behara (2008) havaitsivat tutkimuksessaan, että riskejä välttävät päätöksentekijät investoivat todennäköisemmin tietoturvaan. Päätöksentekijän riskinsietokyky on vain yksi tekijä tietoturvaan liittyvissä päätöksissä. Tämän esimerkin nostaminen kuitenkin osoittaa sen, etteivät nämä päätökset ole yksinkertaisia tai nollasummapeliä.

Oppliger (2007) uskoo, että suuri osa tietoturvaan ja sen riskeihin liittyvistä päätöksistä tapahtuu alitajuntaisesti. Jos tämä pitää paikkaansa, tietoturvapäätökset syntyvät suureksi osaksi päättäjien aiemmin opittujen taitojen ja tietojen perusteella. Tällöin ei välttämättä edes ymmärretä, että tehdään tietoturvaan liittyvää päätöstä. Tämä teoria korostaa tarvetta kehittää johdon osaamista tietoturvaan liittyvissä aihepiireissä.

OT-tietoturvan johtamisesta voidaan vetää yhteen se, ettei johdolla ole useinkaan syvällistä käsitystä tietoturvasta, tai sen hallinnasta. Johdon tulee myös harkita monia eri näkökulmia tehdessään päätöksiä. Tämä lisää haastetta OT-ympäristöjen turvaamisessa, sillä johdon on annettava tukensa kehitysprojekteille.

2.2 IT/OT erot

IT (Information Technology) ja OT tulee erottaa eri käsitteikseen, jotta tiedetään mistä puhutaan. Näillä on merkittäviä eroja toisiinsa nähden. IT:n ja OT:n erot on avattu kuviossa 1 ja kukin kohta käsitellään erikseen kuvion alapuolella.

	IT	OT
Tarkoitus	Hallita informaatiota Ohjata liiketoimintaprosesseja	Hallita omaisuutta ja tapahtumia Ohjata prosesseja
Fokus	Luottamuksellisuus, eheys, saatavuus	Saatavuus, turvallisuus ja luotettavuus
Arkkitehtuuri	Transaktioiden ohjaama, vuorovaikutukseen perustuva, mukautuva	Tapahtumien ohjaama, reaaliaikainen, Sääntöjä noudattava
Rajapinnat	Lukuisia	Rajatusti
Käyttäjiä	Lukuisia	Rajatusti
Avainhenkilöt	CIO, sisäinen IT	Tehdashenkilökunta, automaatioinsinöörit
Laitteet	Työasemat, IT-palvelimet	Automaatiolaitteet, tehdastyöasemat ja –palvelimet
Järjestelmät	ERP, CRM, sähköposti,	SCADA, ohjausjärjstelmät
Riskit	Tiedon ja luottamuksen menetys	Ihmishengen menetys, laitoksen pysähtyminen jonka myötä taloudelliset menetykset

KUVIO 1. IT:n ja OT:n erot

Kuten kuviosta 1 nähdään IT:llä ja OT:lla on paljon eroja. Ensimmäisenä kohtana on IT:n ja OT:n tarkoitus. Yksi IT:n tarkoituksista on informaation hallinta ja ohjaus (Dewett & Jones, 2001). Tällä tarkoitetaan esimerkiksi kommunikaatiota. Tarkoitus on myös tallentaa ja jakaa informaatiota (Kim & Lee, 2006). IT:n puolella tarkoitus on myös ohjata ja johtaa liiketoimintaprosesseja (Ali ym., 2014). IT:n puolella tarkoitus on siis kehittää yrityksen tehokkuutta monella eri tapaa.

OT:n puolella tarkoitus on hallita omaisuutta ja tapahtumia (Stouffer ym., 2022). Omaisuutta ovat esimerkiksi tuotantolaitteet ja tapahtumia taas ovat tuotantoprosessit. OT:n tarkoitus on siis ohjata tuotantoprosesseja. Myös OT:n puolella tarkoituksena on toki kehittää tehokkuutta, mutta fokuksena on vain tuotantoprosessit.

IT:n fokuksena kyberturvan kannalta on tiedon luottamuksellisuus, eheys ja saatavuus (Samonas & Coss, 2014). Muitakin malleja IT:n fokuksen määrittämiseen on olemassa. Tämä malli on kuitenkin riittävä tämän työn kannalta. Perinteisesti ajatellaan, että IT-ympäristössä tärkeintä on luottamuksellisuus ja vähiten tärkeintä saatavuus. OT-ympäristössä tilanne on päinvastainen. Täällä tärkeimmäksi nähdään saatavuus (Jelacic ym., 2020). Tärkeintä on, että tuotanto pysyy käynnissä, kun taas vähemmän vaarallista on tiedon vuotaminen. Tähän liittyy luotettavuus, koska ilman luotettavaa toimintaympäristöä ei saatavuudesta voida varmistua. OT-ympäristöissä myös turvallisuus on merkittävässä roolissa. Riskien realisoituessa useat henget voivat olla vaarassa (Sonkor & García de Soto, 2021).

IT-ympäristössä arkkitehtuuri voi olla dynaamista (Wagter ym., 2005). Ympäristössä tapahtuu paljon muutoksia, kun ihmiset ja työlaitteet vaihtuvat. IT-ympäristön toiminta perustuu siihen, että ihmiset kommunikoivat keskenään. Ihmiset itse käynnistävät toiminnan esimerkiksi lähettämällä sähköpostia kollegalleen pyytääkseen jotain. OT-ympäristöissä asiat käynnistyvät puolestaan silloin, kun laitteet kommunikoivat keskenään (Stouffer ym., 2022). Tärkeintä on, että tapahtumat noudattavat tiettyjä sääntöjä, ja että toiminta on lähes reaaliaikaista. Jos esimerkiksi prosessissa sensori ilmoittaa äkillisestä lämmönnoususta, on tähän reagoitava välittömästi turvajärjestelmän toimesta.

IT:ssä sekä rajapintoja että käyttäjiä on enemmän. Kuten aiemmin mainittiin, IT:n tarkoituksena on kommunikoida, eli yhdistää ihmisiä toisiinsa. Tämä tarkoittaa ihmisiä niin sisäverkossa kuin sen ulkopuolellakin. Ulkopuolisia rajapintoja on oletettavasti siis paljon. Käyttäjiä on myös huomattavasti enemmän kuin OT:n puolella. OT:ssa tärkeimmät toimijat ovat laitteita (Stouffer ym., 2022). OT:ssa myöskään rajapintoja ei ole perinteisesti paljon, kuten luvussa 2.3 esiteltävässä Purdue-mallista huomataan (Williams, 1994). Laitteiden, joista on yhteys myös OT-verkon ulkopuolelle, määrä on kasvanut jatkuvasti (Boyes ym., 2018). Suunta on oletettavasti sama myös tulevaisuudessa. IoT-laitteiden myötä myös OT-laitteiden yhdistettävyys lisääntyy (Sari ym., 2020).

IT:n puolella avainhenkilöitä ovat CIO (Chief Information Officer), tietohallintopäällikkö ja sisäinen IT. Sisäinen IT kokonaisuudessaan on merkittävä tekijä digitaalisen kyvykkyyden kehityksessä (Hsu ym., 2018). Digitaalinen kyvykkyys on merkittävä tekijä yrityksen menestyksen kannalta. Usein pienemmälle huomiolle jää OT-puolen tietotekniikkaympäristö, jonka hallintaan ei ole välttämättä määritetty erillisiä tekijöitä (Stouffer ym., 2022). Nämä voivat jäädä IT-henkilöstön vastuulle, joilla ei kuitenkaan aina ole riittävästi ymmärrystä IT:n ja OT:n eroista. OT-vastaavaa ei ole aina erikseen nimetty. OT:n puolella tärkeimpiä avainhenkilöitä ovat tehdashenkilökunta, mukaan lukien tehtaanjohto, ja muut henkilöt, jotka hallinnoivat ja huoltavat automaatioympäristöä.

Kummassakin ympäristössä laitekanta on erilainen. IT:n puolella tärkeimpiä laitteita ovat työasemat ja palvelimet. Palvelimia käytetään esimerkiksi taloushallinnon sovellusten pyörittämiseen tai verkkosivujen ylläpitämiseen. Työasemia on mahdollisesti hyvin suuri määrä, kun taas OT-ympäristössä työasemia ja palvelimia on rajoitetummin (Neitzel & Huba, 2014). Työasemia ja palvelimia käytetään tuotannon pyörittämiseen. OT-ympäristön kannalta myös tärkeimpiä laitteita ovat automaatiolaitteet, jotka vastaavat käytännön prosessien hallinnoimisesta (Stouffer ym., 2022). Näitä ovat esimerkiksi PLC:t (Programmable Logic Controller), RTU:t (Remote Terminal Unit) ja IED:t (Intelligent Electronic Device).

IT- ja OT-ympäristön järjestelmät eroavat toisistaan. IT-ympäristössä tuttuja järjestelmiä ovat esimerkiksi ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) ja sähköposti. Vaikka OT-ympäristössä voidaan myös hyödyntää esimerkiksi ERP-järjestelmiä, OT-ympäristön tärkeimmät järjestelmät ovat ohjausjärjestelmiä. Yksi ohjausjärjestelmätyyppi on SCADA

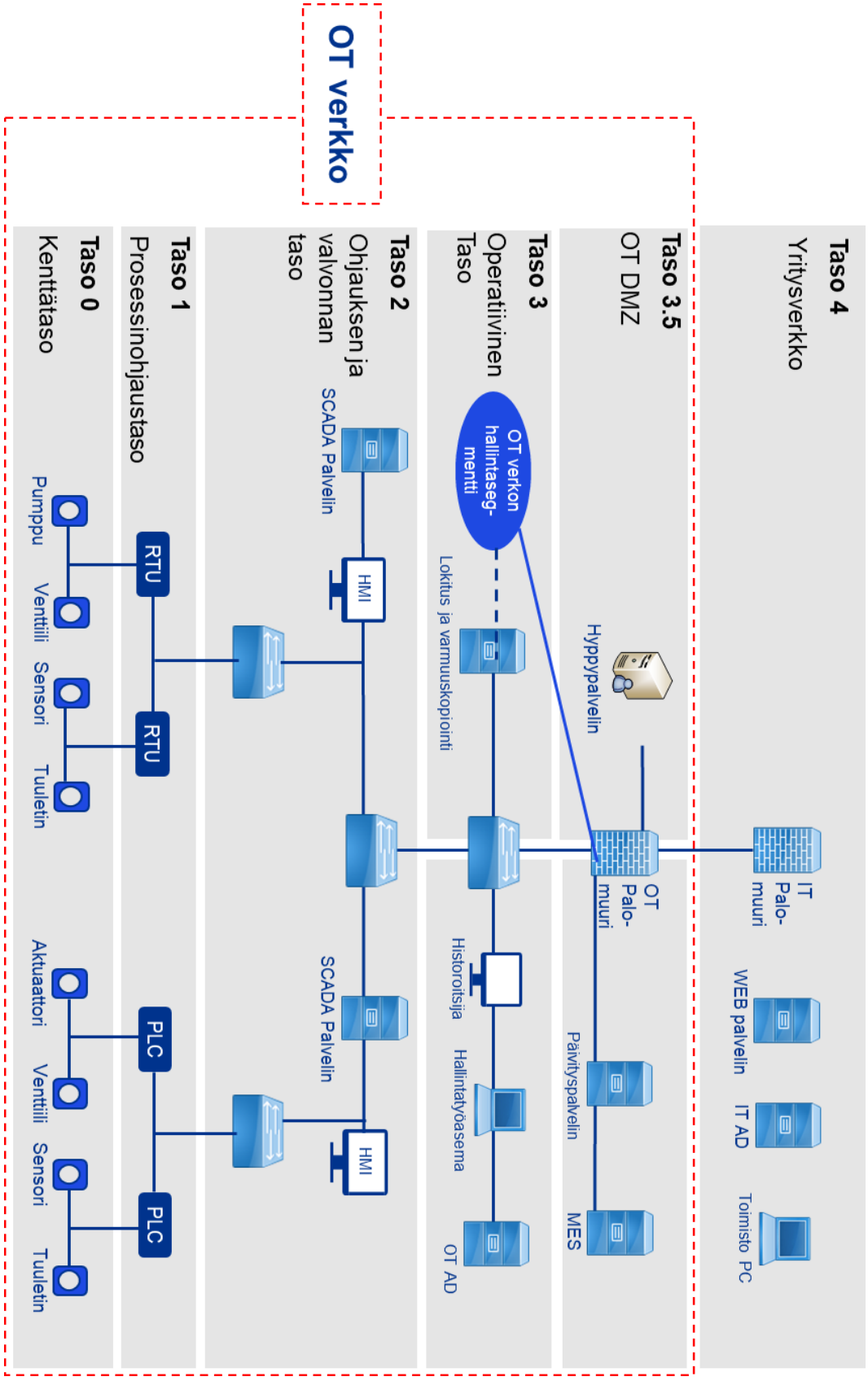
(Supervisory Control and Data Acquisition) (Daneels & Salter, 1999). Näitä järjestelmiä käytetään esimerkiksi sähköverkkojen ylläpidossa.

Viimeisenä erona IT ja OT-ympäristöjen välillä ovat riskit, jotka voivat realisoitua esimerkiksi tietomurron seurauksena. IT-ympäristössä uhkana voi olla esimerkiksi tietovuodot, jonka myötä menetetään asiakkaiden luottamus (Jouini ym., 2014). Riskit ovat kuitenkin pääasiassa rahallisia. OT-ympäristössä riskit voivat realisoituessaan uhata yksilön henkeä (Stouffer ym., 2022). Jos esimerkiksi turvajärjestelmä päästään poistamaan käytöstä, saattaa myrkyllistä kaasua päästä hengitysilmaan, uhaten työntekijöiden ja muun lähialueen terveyttä. Tuotantoon vaikuttaessa myös taloudelliset seuraukset voivat olla merkittäviä. Jos tuotantolinja pystytään pysäyttämään, saattaa materiaalia mennä nopeasti pilalle, ja tuotannon käynnistämiseen saattaa mennä merkittävästi aikaa.

Kuten aiemmista esimerkeistä nähdään IT:n ja OT:n välillä on suuria eroja niin teknologioiden kuin hallinnollisten asioiden kannalta. Tämän vuoksi tulee ymmärtää se, että nämä ovat kaksi erillistä käsitettä ja ympäristöä, joita tulee hallinnoida eri tavalla.

2.3 Purdue-malli

Purdue-malli on Theodore J. Williamsin (1994) kehittämä referenssimalli, joka on suunniteltu teollisuusjärjestelmien ja kriittisen infrastruktuurin kyberturvan hallintaan. Purdue-mallissa järjestelmäarkkitehtuuri jaetaan eri tasoille, ja jokaisella tasolla on oma roolinsa ja vastuunsa kyberturvassa. Malli on nimeltään myös Purdue Enterprise Reference Architecture (PERA). Purdue-mallin tarkoitus on auttaa organisaatioita suunnittelemaan, toteuttamaan ja ylläpitämään turvallisia teollisuusjärjestelmiä. Malli on vanha ja siinä on puutteensa, mutta sitä käytetään edelleen kuvaamaan erityisesti sitä, miten OT-verkot rakentuvat. Purdue-malli onkin hyvänä tukena etenkin silloin, kun keskustellaan OT-arkkitehtuurista. Purdue-mallia on sovellettu moneen otteeseen. Yksi tunnetuin on ISA-95 (Unver, 2013). Purdue-mallin yksi sovellettu versio on esitetty kuviossa 2.



KUVIO 2. Purdue-malli (tehty mukaillen (Industrial Internet Consortium, 2019; Stouffer ym., 2022; Unver, 2013; Williams, 1994)

Kuten kuviosta 2 nähdään, OT-verkko rajautuu tasoille 0-3.5. Taso 3.5 on OT-verkon ja IT-verkon välissä. Sen voitaisiin siis nähdä kuuluvan myös OT-verkon ulkopuolelle. Esimerkissämme tämä on kuitenkin sisällytetty OT-verkkoon kuuluvaksi, koska taso 3.5 on erittäin tärkeä OT-verkon turvallisen toiminnan kannalta.

Purdue-mallin tasolla 0 tarkastellaan fyysistä prosessitasoa tai kenttätasoa, joka on teollisuusohjausjärjestelmän perusta. Tässä tasossa käsitellään laitoksen tai järjestelmän prosesseja ja fyysisiä laitteita. Purdue-malli on hierarkkinen malli, joka jakaa ICS-ympäristön kerroksiin. Siinä taso 0 edustaa fyysisiä prosesseja. Tasolla 0 ovat siis käytännön tuotantoprosessit ja niihin liittyvät laitteet. Laitteet tällä tasolla ovat aktuaattoreita ja sensoreita. Aktuaattorit muuttavat prosessia ja sensorit havainnoivat sitä. Esimerkiksi sensori voisi tarkkailla huoneen lämpötilaa ja käynnistää tuulettimen, jos lämpötila kohoaa liian korkealle.

Tasolla 1 ohjataan käytännön prosessia. Tällä tasolla keskitytään ohjauslaitteisiin kuten PLC (Programmable Logic Controller) tai RTU (Remote Terminal Unit) jotka ohjaavat ja valvovat prosessilaitteita. Tason 1 laitteet lähettävät ja vastaanottavat syötteitä tasolta 0 ja lähettävät näitä eteenpäin tasolle 2. PLC voisi esimerkiksi vastaanottaa tasolta 2 käskyn tarkistaa lämpötila tason 0 sensorista. Tällöin PLC pyytää dataa sensorilta, joka lähettää sen PLC:lle, ja lähettää sen tiedoksi tasolle 2. Tämä on hyvin yksinkertaistettu esimerkki, koska tason 1 laitteita voidaan ohjelmoida toimimaan melko itsenäisesti ja niiden vastuut ympäristössä voivat olla laajempia.

Taso 2 liittyy teollisuusprosessin ohjausjärjestelmiin. Se on kuitenkin vielä lähellä itse prosessia ja tuotantolaitteita. Tällä tasolla on esimerkiksi OT-palvelimia ja HMI:ta (Human Machine Interface). OT-palvelimia voidaan käyttää esimerkiksi kommunikaatioon tai ohjausjärjestelmän pyörittämiseen. HMI:t ovat monesti tärkeä osa prosessia, koska operaattorit käyttävät niitä järjestelmän valvomiseen ja ohjaamiseen. OT-palvelimella voisi olla esimerkiksi sähköverkon ohjausjärjestelmä, jota valvomohenkilökunta käyttää HMI:tä hyödyntäen. On huomioitavaa, että HMI ei ole tarpeellinen kaikissa ohjausjärjestelmissä. Kaikkiin prosesseihin ei ole tarpeen vaikuttaa ohjauspaneeleja hyödyntämällä.

Tasolla 3 siirrytään laajemman ohjauksen tasolle. Tasolla keskitytään järjestelmien ohjaukseen ja ohjaamiseen, ja tämä taso edustaa laajempaa näkökulmaa kuin alemmat tasot. Tasolla 3 käsitellään yläpuolisia ohjausjärjestelmiä, jotka hallitsevat useamman laitoksen tai teollisuusprosessin osia ja integroivat usean yksikön järjestelmiä. Sitä käytetään ohjausjärjestelmän hallinnoimiseen. Tällä tasolla voi olla esimerkiksi lokipalvelimet, varmuuskopioiden tallennuspaikat, historoitsija (jota käytetään prosessidatan tallentamiseen), hallintatyöasemat (jota käytetään esimerkiksi PLC-tason koodin muokkaamiseen) ja OT Active Directory. Tason 3 laitteet ovat hyvin kriittisiä järjestelmän ohjauksen kannalta, mutta periaatteessa tason 0-2 laitteet voisivat toimia itsenäisesti, jos yhteydet jostain syystä tulisi katkaista.

Tasolla 3.5 tarkoitetaan DMZ-aluetta (Demilitarized Zone). Tämä taso toimii välipisteenä aina, kun OT-verkkoon halutaan yhdistää sen ulkopuolelta. Kaikkien yhteyksien tulisi kulkea OT-palomuurin kautta. Etäyhteyksien tulisi

terminoitua hyppypalvelimelle, jonka myötä etäyhteyksiä pystytään valvomaan ja kontrolloimaan. Tasolla 3.5 on myös päivityspalvelin ja MES (Manufacturing Execution System). Nämä palvelimet ovat yhteydessä alemmille tasoille, mutta näillä tulee olla myös yhteys OT-verkon ulkopuolelle. Tämän vuoksi ne tulee sijoittaa DMZ:lle. On huomioitavaa, että myös yritysverkosta tullaan OT-verkkoon DMZ:n kautta. OT-verkon näkökulmasta yritysverkko on turvaton.

Taso 4 ei ole enää OT-verkkoa. Tämä on yrityksen sisäistä yritysverkkoa, jossa suurin osa käyttäjistä työskentelee. Tässä verkossa on muun muassa palvelimia eri tarkoituksiin sekä tulostimia, toimisto-pc:tä ja IT Active Directory. Tärkein huomioitava asia on, että yritysverkko on eriytetty OT-verkosta. Usein puhutaan myös tasosta 5, joka on julkinen verkko. Tämä on jätetty pois kuviosta, koska sille ei nähty tarvetta käsillä olevan tutkimuksen kannalta.

Purdue-malli jakaa laitteet ja toiminnot loogisesti erilaisiin kokonaisuuksiin. Laitteiden ja arkkitehtuurin kokonaisuus voidaan ymmärtää kuvion pohjalta. Valitettavasti todellisuus ei aina ole näin selkeä. Laitteet voivat sijaita samaan aikaan eri tasoilla, ja toimittaa useaa eri tehtävää. Malli ei ole riittävän hyvä kuvaamaan nykyisiä arkkitehtuureja, malli on kuitenkin erittäin hyödyllinen, kun halutaan ymmärtää OT-verkon yleisperiaatteita.

3 MIKÄ ON IEC 62443?

Tässä luvussa vastataan avustaviin kysymyksiin ”3. Miksi organisaatiot sertifioituvat?”, 4. ” Mikä on IEC 62443 -standardiperhe ja mitä tämä sisältää?” ja 5. ”Miten IEC 62443 -sertifikaattiin liittyen voi sertifioitua?”. Kolmanteen apututkimuskysymykseen vastataan alaluvussa 3.1, toiseen alaluvussa 3.2. ja kolmanteen luvussa 3.3.

IEC 62443 syntyi 2000-luvun alussa, kun teollisuuden automaatiojärjestelmiin liittyvät tietoturvariskit alkoivat herättää huolta (ISA, 2024). ISA (International Society of Automation) ja IEC (International Electrotechnical Commission) alkoivat yhteistyössä kehittää IEC 62443 -standardiperhettä. Ensimmäiset osat (ISA/IEC 62443-1-1 ja ISA/IEC 62443-2-1) julkaistiin 2010-luvun alussa. Nykyään IEC 62443 -standardit tarjoavat viitekehyksen, jonka avulla organisaatiot voivat suojata teollisuuden ohjausjärjestelmiä ja vastata digitaalisen aikakauden tietoturvahaasteisiin. Standardiperhe on nykyään kansainvälisesti hyväksytty ja laajasti käytetty viitekehys.

3.1 Miksi sertifioitua?

Tässä luvussa käsitellään yleisesti kysymystä siitä, miksi organisaatioiden tulisi hankkia tietoturvasertifikaatti. Tietoturvasertifikaatteja voidaan hankkia esimerkiksi seuraavista syistä:

- Asiakkaiden luottamuksen parannus
- Kumppanisuhteiden parannus
- Kilpailuetu
- Lakisääteiset vaatimukset
- Sisäisen tietoturvan parannus

Ensinnäkin asiakkaiden ja kumppaneiden luottamus toimijaa kohtaan paranee, kun toimijalla on virallinen sertifikaatti (Humphreys, 2006; Saint-Germain & others, 2005). Tietoturvasertifikaatin hankkiminen voi lisätä asiakkaiden luottamusta organisaatioon. Tällöin asiakas on todennäköisemmin valmis käyttämään toimittajan palveluita tai tilaamaan heidän tuotteitaan, koska se on turvallisempaa. Myös kumppanisuhteet paranevat. Joissain tapauksissa organisaation on hankittava tietoturvasertifikaatti voidakseen muodostaa kumppanuuksia muiden organisaatioiden kanssa. Yhteistyökumppanit voivat vaatia tietoturvasertifikaattia varmistaakseen, että tietoja käsitellään asianmukaisesti. Tätä kautta sertifikaatit tuovat myös kilpailuetua, koska yhteistyökumppanit toimivat mieluummin tahojen kanssa, jotka vastaavat heidän vaatimuksiinsa tietoturvaan liittyen, ja joiden ympäristöjen uskotaan olevan turvallisia.

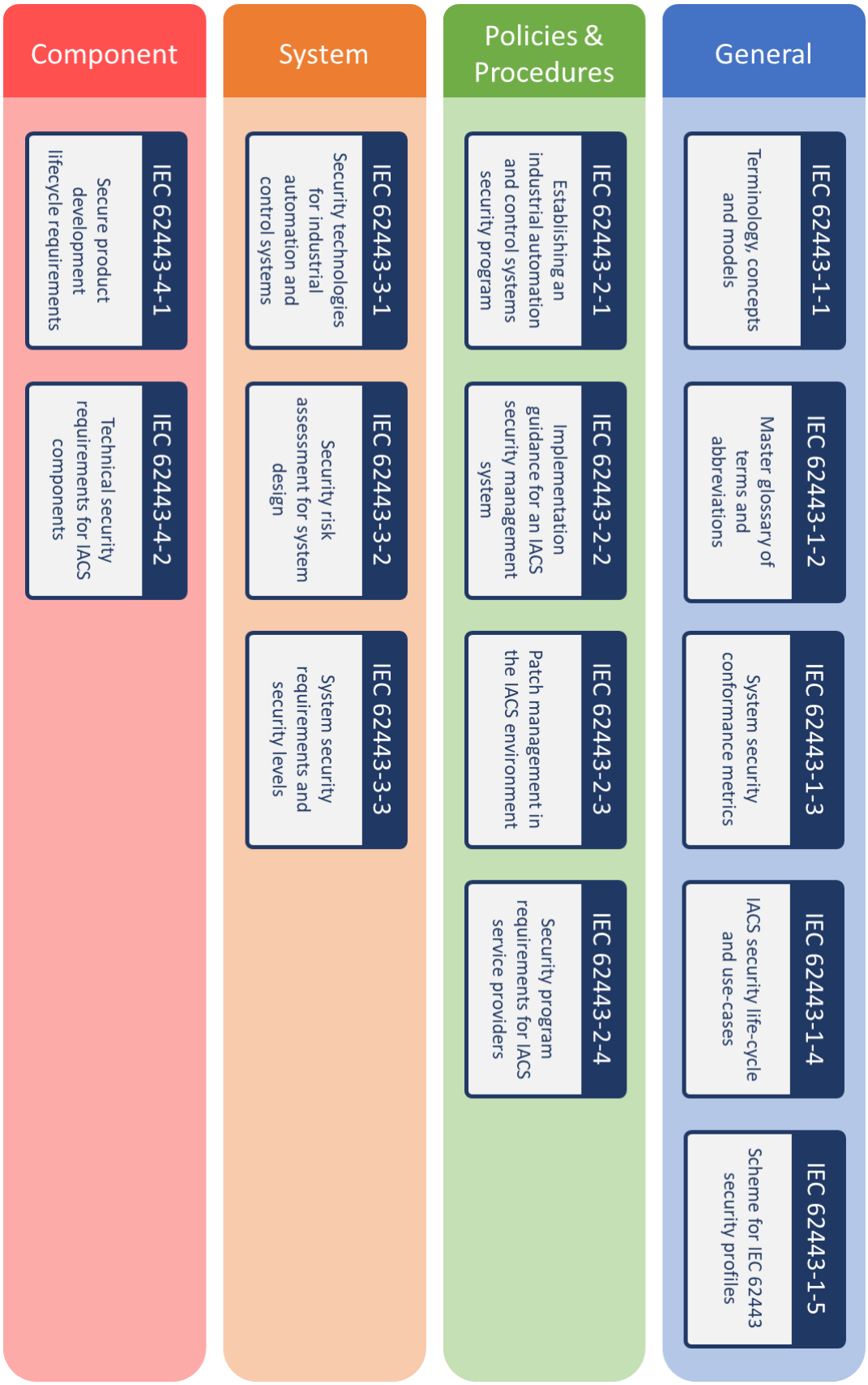
Tietoturvasertifikaatteja hankitaan osaksi myös lakisääteisten vaatimusten takia. Osa valtioista/muista tahoista vaatii tiettyjä sertifikaatteja organisaatioilta. Esimerkiksi NIS2-direktiivin myötä organisaatioille tulee laajoja vaatimuksia tietoturvan hallintaan (Singh, 2023). Tämä on johtanut siihen, että useat organisaatiot ovat harkinneet ISO 27001 -sertifikaatin hankkimista tietoturvan hallintajärjestelmälleen.

Viimeinen esiteltävä syy tietoturvasertifikaatin hankkimiseen on sisäisen tietoturvan parantaminen. Organisaatiot voivat hankkia tietoturvasertifikaatin varmistuakseen ympäristönsä turvallisuudesta, ja saadaksensa varmuutta hallintajärjestelmän toimivuudesta (Humphreys, 2006; Saint-Germain & others, 2005). Sertifikaatti takaa järjestelmän laadukkuuden. Tietoturvasertifikaatin hankkiminen on pieni kustannus verrattuna koko organisaation lamauttavaan kyberturvaiskuun. Etenkin jos kyseessä on OT-ympäristö.

Yhteenvetona voidaan todeta, että syyt sertifikaatin hankkimiseen voivat vaihdella organisaatioiden välillä. Tietoturvasertifikaatti auttaa joka tapauksessa organisaatioita suojaamaan tietojaan, vahvistamaan luottamusta asiakkaiden keskuudessa sekä noudattamaan sääntelyä ja parantamaan kilpailukykyään markkinoilla.

3.2 IEC 62443

IEC 62443 -standardi jakautuu neljään eri osaan, jotka käsittelevät eri aihealueita. Aihealueet ovat nimeltään Yleinen, Politiikat ja menetelmät, Järjestelmä ja Komponentti. Kullakin osa-alueella on omat alaosionsa, jotka käsittelevät aihealueita eri näkökulmista. Koko standardiperhe esitellään kuviossa 3. Kuvio on englanninkielinen, kuten standardiperhekin alkuperäismuodossaan.



KUVIO 3. IEC 62443 -standardin osat. Tehty mukaillen (ISA, 2024)

Seuraavissa alaluvuissa esitellään tarkemmin IEC 62443 -standardin osat. Työn kannalta tärkeintä on esitellä yleistiedot kustakin alaosiosta, kertoa kenelle ja mihin tarkoitukseen kyseinen standardin osa on tarkoitettu ja voiko kyseiseen standardin osaan sertifioitua. On huomioitavaa, että osaa standardin alaosioista ei ole vielä julkaistu. Nämä osat ovat vielä työn alla. Osat, joita ei ole vielä luotu mainitaan kunkin alaluvun kohdalla. Lähteenä seuraavissa luvuissa toimii itse standardiperhe.

3.2.1 IEC 62443-1

IEC 62443-1 käsittelee yleisiä asioita, jotka toistuvat standardiperheessä. Tämä osa siis luo pohjaa muille osa-alueille, joissa varsinaiset standardin vaatimukset on esitelty. Osassa esitellään muun muassa käsitteitä, mittarointia ja malleja muiden osien tueksi. (ISA/IEC, 2009, 2023b)

IEC 62443-1-1: Terminologia, käsitteet ja mallit

Julkaistu:	2009
Kenelle tarkoitettu:	Kaikille standardia hyödyntäville
Voiko sertifioitua:	Ei
Sivumäärä:	81

Tämä standardin osa esittelee terminologian, käsitteet ja mallit teollisuusautomaatio- ja ohjausjärjestelmien tietoturvalle luoden perustan IEC 62443 -sarjan muille standardeille. Osa alkaa termien ja lyhenteiden määrittelyllä ja se kattaakin kolmasosan itse dokumentista. Näitä määritellään erittäin monipuolisesti huomioiden tärkeimmät OT-ympäristöihin liittyvistä lyhenteistä ja teemoista.

Seuraavaksi dokumentissa käsitellään yleisiä periaatteita OT-ympäristöjen turvaamisessa. Tässä näkökulma on etenkin nykytilanteessa OT-ympäristöissä. Vaikka dokumentti on vanha, osio kuvaa suurelta osin nykytilannetta. Seuraavassa luvussa avataan peruskäsitteitä muille standardeille IEC 62443 -sarjassa. Käsitteitä ovat esimerkiksi ”tietoturvavaatimukset”, ”Uhkien ja riskien arviointi” ja ”Politiikat”. Näitä käsitteitä avataan standardissa melko syvällisesti.

Viimeisenä lukuna tässä osassa on Mallit. Tässä luvussa kuvaillaan sarja malleja, joita voidaan käyttää tietoturvaohjelman suunnittelussa. Malleja on eri tarpeisiin mukaan lukien referenssiarkkitehtuurimallit ja suojattavien kohteiden mallit. Standardin esittämä referenssiarkkitehtuuri vastaa hyvin pitkälle Purdue-

mallissa esiteltyä referenssiarkkitehtuuria. Standardissa myös esitellään esimerkkejä siitä, miten referenssiarkkitehtuuria voi soveltaa.

Tämä standardin osa on kattava kokonaisuus, joka antaa hyvän taustan muille standardin osille. Osiota 1-1 voisikin pitää johdantona muille osioille. Jos omaksuu tämän alaosion, on huomattavasti helpompaa ymmärtää myös muiden standardin osien sisältö.

IEC 62443-1-2: Termien ja lyhenteiden yleissanasto

Julkaistu:	Ei vielä
Kenelle tarkoitettu:	Kaikille standardia hyödyntäville

Tämä standardin osio tulee olemaan yksinkertaisesti yhteenveto termeistä ja lyhenteistä, joita standardiperheessä käytetään. Tämä tulee siis olemaan sanakirja, jota voi hyödyntää lukiessaan standardia. Toistaiseksi sanastot on julkaistu kunkin standardin alaosion yhteydessä.

IEC 62443-1-3: Järjestelmän tietoturvan vaatimustenmukaisuuden mittarit

Julkaistu:	Ei vielä
Kenelle tarkoitettu:	Kaikille standardia hyödyntäville, etenkin johto

Osio 1-3 tulee esittämään mittareita, joilla voidaan seurata sitä, kuinka hyvin tämän standardin vaatimuksiin vastataan. Mittareiden fokuksesta tai kohdeyleisöstä ei ole vielä tietoa. Yleisesti mittarit kiinnostavat etenkin johtoa.

IEC 62443-1-4: IACS:n tietoturvan elinkaari ja käyttötapauksia

Julkaistu:	Ei vielä
Kenelle tarkoitettu:	Kaikille standardia hyödyntäville

Tämä standardin osa tulee esittämään yksityiskohtaisen kuvauksen ohjausjärjestelmien suojauksen elinkaaresta. Tässä osiossa tullaan myös esittämään esimerkkejä ja käyttötapauksia elinkaareen liittyen. Perusperiaatteet elinkaareen liittyen esitettiin standardin luvussa 1-1.

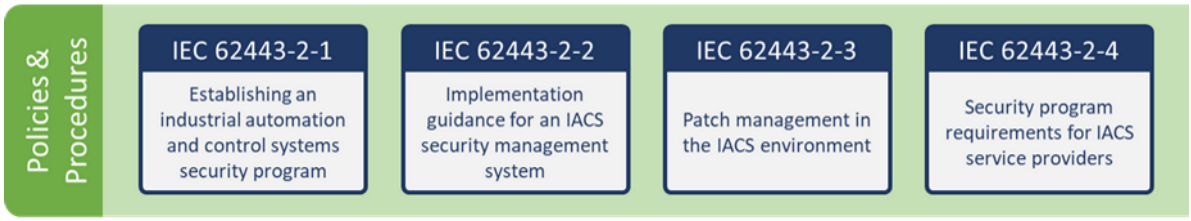
IEC 62443-1-5: Ohjelma IEC 62443 -suojausprofiileille

Julkaistu:	2023
Kenelle tarkoitettu:	Kaikille standardia hyödyntäville
Voiko sertifioitua:	Ei
Sivumäärä:	16

Tässä osassa määritellään ohjelma standardin suojausprofiilien määrittelyä varten. Osassa kerrotaan, miten suojausprofiilit valitaan, kirjoitetaan ja luodaan. Nämä suojausprofiilit itsessään on tarkoitus julkaista myöhemmin osana

standardia, ja osa-alueita näistä onkin jo julkaistu. Osiossa otetaan kantaa siihen, miten suojausprofiili valitaan huomioiden kohdeorganisaation konteksti. Toistaiseksi 1-5 osio ei ole laajasti käytössä muun muassa sen uutuuden vuoksi.

3.2.2 IEC 62443-2



Tässä osassa esitellään politiikat ja proseduurit IEC 62443 hallintaan liittyen. Osan pääasiallinen tavoite on esitellä, kuinka organisaatio pystyy rakentamaan tietoturvan hallintajärjestelmän standardiin perustuen. Osassa myös esitellään vaatimuksia hallintajärjestelmälle. IEC 62443-2 keskittyy täten hallinnolliseen tietoturvaan, ei niinkään teknisiin vaatimuksiin. (ISA/IEC, 2010, 2015, 2023a)

IEC 62443-2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten

Julkaistu:	2010
Kenelle tarkoitettu:	Tietoturvajohtajat
Voiko sertifioitua:	Ei
Sivumäärä:	145

Tämä alaosio esittelee, kuinka rakennetaan tietoturvan hallintajärjestelmä IEC 62443 -standardiin perustuen. Tietoturvan hallintajärjestelmä tarjoaa organisaatiolle vakiintuneet prosessit ja menetelmät ympäristönsä suojaamiseksi. Yksi tunnettu tietoturvan hallintajärjestelmä on ISO 27001. Hallintajärjestelmät, kuten ISO 27001, ovat keskittyneet yleisesti tietoturvan prosesseihin ylätasolla. Niissä huomioidaan harvemmin erityisesti OT-ympäristöjen kyberturvaa. Tämä standardin alaosio pyrkiikin vastaamaan tähän puutteeseen.

Alaosio alkaa johdannosta, jossa kerrotaan standardin sisällöstä. Huomioitavaa on, että standardissa suositellaan tutustumaan ISO 27001 -standardiin, koska IEC 62443-2-1 rakentuu osaksi tämä pohjalle. ISO 27001 -standardin mukainen hallintajärjestelmä onkin markkinoilla yleisesti tunnettu järjestelmä. Organisaatiot, joilla on OT-ympäristö ja haluavat kehittää tietoturvaansa, saavatkin synergiaetuja, jos tuovat IEC 62443 osaksi tietoturvan hallintajärjestelmäänsä.

Seuraavaksi alaosiossa esitellään termit ja lyhenteet, jotka ovat tämän osan kannalta merkittäviä. Näiden esittelyn jälkeen siirrytään suoraan asiaan, jossa esitellään tietoturvallisuuden hallintajärjestelmän luokat, joita ovat ”Riskianalyysi”, ”Riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla” ja ”Tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen”. Kunkin luokan

alla on elementtejä, jotka muodostavat käytännön hallintajärjestelmän. Esimerkiksi Riskianalyysin alla näitä ovat ”Liiketoimintaperustelu” ja ”Riskien tunnistaminen, luokittelu ja arviointi”. Kunkin elementin alla avataan elementin sisältöä tarkemmin ja kerrotaan perustelut, miksi elementti on tärkeä. Yhtenä tärkeänä osana elementtien alla on käytännön vaatimukset siitä, mitä organisaatiolla tulisi olla, jotta ne vastaavat standardin vaatimuksiin.

Tämän standardin pääosa onkin elementtien ja vaatimusten määrittelyssä. Seuraavaksi osaan kuuluu Liite A, jossa on neuvoja tietoturvallisuuden hallintajärjestelmän elementtien kehittämistä varten. Liitteen A avulla organisaatio tietää, miten elementtien vaatimuksiin pystytään vastaamaan. Liite A on melko yksityiskohtainen, vaikkakin siinä on maininta, etteivät kaikki siinä mainitut asiat sovellu kaikkiin toimintaympäristöihin. Liitteessä esitetään perustason käytäntöjä, jotka ovat suosituksia organisaatioille tietoturvallisuuden perustason saavuttamiseksi. Lisäksi esitellään lisäkäytäntöjä, joiden avulla organisaatiot voivat saada lisäparannuksia tietoturvaan.

Liitteessä B esitellään tietoturvallisuuden hallintajärjestelmän kehittämisprosessi. Dokumentissa esitetään ylätason prosessi hallintajärjestelmän perustamisesta, ja kerrotaan, mitä kukin prosessin osa-alue sisältää. Osan prosessikaavioita pystytään tarvittaessa hyödyntämään oman tietoturvan hallintajärjestelmän luomisessa. Viimeisenä tässä alaosiossa on Liite C, jossa vaatimukset on rinnastettu ISO 27001 -vaatimuksiin. ISO 27001 -versio on kuitenkin 2005, kun uusin versio tästä on 2022. Listaus ei siis ole enää kovin käytännöllinen.

IEC 62443-2-2: IACS:n tietoturvan hallintajärjestelmän täytäntöönpano-ohjeet

Julkaistu:	Ei vielä
Kenelle tarkoitettu:	Tietoturvajohtajat

Tämä standardin osa tulee sisältämään täytäntöönpano-ohjeita tietoturvan hallintajärjestelmän käyttöönottamiseksi. Osa tulee siis liittymään läheisesti osaan 2-1. Osa sisältää mahdollisesti ohjeita hallintajärjestelmän ylläpitämiseksi.

IEC 62443-2-3: Päivitysten-hallinta IACS-ympäristössä

Julkaistu:	2015
Kenelle tarkoitettu:	Laitosten omistajat, toimittajat, ylläpitäjät
Voiko sertifioitua:	Ei
Sivumäärä:	66

Tässä alaosiossa kuvataan vaatimukset tahoille, jotka ylläpitävät OT-laite-/järjestelmäympäristöä. Dokumentti esittelee suosituksen ympäristön päivityksen hallintaa varten. Dokumentissa kuvataan, kuinka tietoturvapäivityksiä ja korjaustiedostoja jaetaan turvallisesti OT-ympäristöön. Dokumentissa kuvattuja menetelmiä voidaan käyttää myös muiden kuin tietoturvapäivitysten hallintaan.

IEC 62443-2-3 alkaa tuttuun tapaan esisanoista ja käsitteen määrittelyistä. Dokumentissa mainitaan, että standardi esittää suositellun tavan

tietoturvapäivitysten viemiseen ja asentamiseen OT-ympäristöön. Esitelty prosessi sopii yhtä lailla niin käyttöjärjestelmien, sovellusten tai laitteiden päivitykseen.

Seuraavaksi standardissa kuvataan yleisiä haasteita tietoturvapäivitysten viemisessä ympäristöön. Yleinen syy haasteisiin on se, että tuotantoa ei voi aina pysäyttää päivitysten ajaksi. Lisäksi siinä kuvataan seurauksia siitä, jos tietoturvapäivityksiin liittyvä prosessi ei ole tehokas. Näillä osa-alueilla haetaan pohjaa sille, miksi standardin esittämä prosessi on tärkeä.

Seuraavassa luvussa esitetään suosituksia laitoksen omistajille. Suosituksien joukossa on esimerkiksi kattavan inventaariolistauksen pitäminen, joka sisältää versiotiedot. Itse standardissa käsitellään tätä vain ylätasolla, mutta liitteessä B asioita käydään läpi yksityiskohtaisemmin. Liitteessä B annetaan ohjeita omistajille tietoturvapäivitysprosessin luomiseksi ja ylläpitämiseksi. Liitteessä esitellään prosessi siitä, miten päivityksiä monitoroidaan, testataan ja ajetaan ympäristöön. Kukin prosessin vaihe avataan yksityiskohtaisesti, ja nämä linkitetään osaksi IEC 62443-2-1 alaosioon.

Standardissa esitetään myös suosituksia tuotteiden toimittajille. Nämä käsitellään jälleen vain ylätasolla itse standardissa, mutta liitteessä C kerrotaan näistä tarkemmin. Osan tärkeimpinä asioina on, että toimittajat kehittävät ja jakavat päivityksiä säännöllisesti, kommunikoivat niistä, ja skannaavat haavoittuvuuksia omissa tuotteissaan.

Viimeinen osa itse standardissa on hyvin käytännönläheinen. Standardissa esitellään kuinka tietoturvapäivitykset tulisi siirtää ympäristöön turvallisesti. Tässä kuvataan esimerkiksi näiden tiedostomuodot ja nimeämiskäytännöt. Näitä avataan hyvin syvällisesti liitteessä A.

IEC 62443-2-4: Tietoturvajärjestelmän vaatimuksia IACS palveluntuottajille

Julkaistu:	2023
Kenelle tarkoitettu:	Palveluntuottajat, omistajat
Voiko sertifioitua:	Kyllä
Sivumäärä:	92

IEC 62443-2-4 on ensimmäinen osa standardia, jota vasten organisaatiot voivat sertifioitua. Tässä alaosiossa on kuvattu kattava määrä vaatimuksia IACS palveluntuottajille. Toimittajat ja palveluntuottajat voivat käyttää näitä vaatimuksia automaatioympäristön toimitus- ja ylläpitovaiheissa. Tämä standardin osa ei ota kantaa tietoturvan hallintajärjestelmään, vaikka nimi läheisesti siihen viittaakin.

Standardissa esitetään aluksi kunkin eri toimijoiden roolit automaatioympäristöjen hallintaan liittyen. Omistajilla, integraattoreilla ja toimittajilla on omat roolinsa ja omat vastuualueensa. Standardissa esitellään myös miten eri toimijat voivat hyödyntää kyseistä dokumenttia. Seuraamalla standardia, palveluntuottajat voivat todentaa toimittamansa palvelun luotettavuutta. Omistajat taas voivat vaatia toimittajilta tiettyjä kyvykkyyksiä standardiin liittyen.

Seuraavaksi standardissa esitellään maturiteettimalli, jossa on neljä eri kypsyystasoa: Initial, Managed, Defined, Improving. Näitä maturiteettitasoja

voidaan käyttää arvioimaan toimittajan kypsyyttä. Maturiteettitasoja ei kuitenkaan esitetä varsinaisen vaatimuslistauksen yhteydessä.

Varsinaisen standardin viimeisessä osa-alueessa kerrotaan, miten vaatimukset rakentuvat. Jokaiselle vaatimukselle on määritetty ID, vaatimuksen taso, mitä vaatimus koskee, otsikko, vaatiiko kohdan täyttäminen dokumenttia omistajan suuntaan, kuvauksen vaatimuksesta ja perustelun vaatimukselle. Vaatimuksia on käytännössä kahta eri tasoa, BR (Base Requirement) ja RE (Requirement Enhancement indicator). BR on vaatimus, joka koskee kaikki palveluntuottajia. RE-vaatimukset ovat syvällisempiä, jotka otetaan käyttöön, kun halutaan saavuttaa tietyn tason kypsyys eri osa-alueilla.

Itse vaatimuslistaus on liitteessä A, joka on standardin viimeinen ja suurin osa. Vaatimuksia on yli 60 sivun verran. Kullakin vaatimuksella on tietty funktionaalinen osa-alue. Näitä ovat (lista englanniksi vastaten standardin sisältöä):

- Solution staffing
- Assurance
- Architecture
- Wireless
- SIS
- Configuration management
- Remote access
- Event management
- Account management
- Malware protection
- Patch management
- Backup/Restore

Kuten nähdään, vaatimuksia on kattavasti eri osa-alueille. Täyttämällä standardin vaatimukset palveluntuottaja pystynee vakuuttamaan laitostenomistajat huomioineensa riittävät tietoturvastandardit palveluissaan.

3.2.3 IEC 62443-3

Standardin 62443 osassa 3 tarkastelun kohteena on järjestelmät. Tämän alaosion pääasiallisena tarkoituksena on esittää vaatimuksia ja periaatteita järjestelmien turvallisuuden takaamiseksi. Osan 3 fokus on siis teknisempi kuin aiemmassa osa-alueessa. (ISA/IEC, 2013, 2019a, 2020)

IEC 62443-3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille

Julkaistu:	2013
Kenelle tarkoitettu:	Omistajat, (palveluntuottajat)
Voiko sertifioitua:	Ei
Sivumäärä:	91

Standardissa IEC 62443-3-1 esittelee erilaisia teknologioita, työkaluja ja vastatoimenpiteitä, joita voidaan hyödyntää OT-ympäristöjen turvaamisessa. Osassa kuvataan yksityiskohtaisesti, minkälaisia metodeja voidaan käyttää ympäristöjen turvaamisessa. On huomioitava, että dokumentti on yli kymmenen vuotta vanha, joten osa sen esittämistä teknologioista tai menetelmistä ei ole välttämättä enää nykyään vallitsevia. Dokumentissa on kuitenkin hyviä periaatteita ympäristöjen turvaamiseksi. Dokumentissa mainitaankin, että se kuvasta sen hetkistä arviointia työkaluista ja menetelmistä.

Käsitteiden määrittelyn jälkeen dokumentissa perustellaan automaatioympäristöjen suojaamisen tarvetta. Tarvetta perustellaan muun muassa luvattomien pääsy-yritysten lisääntymisellä. Pääteknologiat, joita tässä standardissa käsitellään, on esitelty Taulukossa 1. Kunkin pääteknologian alle kuuluu useampi menetelmä, työkalu tai vastatoimi, jotka esitellään myös samassa taulukossa.

Taulukko 1. IEC 62443-3-1 Teknologiat

Pääteknologia	Menetelmät, työkalut ja vastatoimet
Todennus- ja valtuutusteknologiat	• Roolipohjaiset valtuutustyökalut • Salasanaan perustuva todennus • Haaste-vaste-todennus • Fyysinen todennus • Todennus toimikortilla • Biometrinen todennus • Sijaintiin perustuva todennus • Salasanojen jakelun ja hallinnan teknologiat • Laitteesta laitteeseen -todennus
Suodatuksen/estämisen/pääsyhallinnan teknologiat	• Verkon palomuuri • Käyttöjärjestelmään asennetut palomuurit • Virtuaaliverkot
Salausteknologiat ja tietojen kelpuutus	• Symmetriseen avaimeen perustuva salaus • Julkiseen avaimeen perustuva salaus • VPN-verkot
Hallinta-, auditointi-, mittaus-, valvonta- ja havaitsemistyökalut	• Lokitietojen auditointivälineet • Virusten ja haittakoodien havaitsemisjärjestelmät • Tunkeutumisen havaitsemisjärjestelmät (IDS) • Haavoittuvuusskannerit • Tutkinta- ja analysointityökalut • Isäntäkoneen konfiguraation hallinnan työkalut • Ohjelmistojen automaattiset hallintatyökalut
Teollisuusautomaatio- ja ohjausjärjestelmien tietokoneohjelmistot	• Palvelimien ja työasemien käyttöjärjestelmät • Tosiaikaiset ja sulautetut käyttöjärjestelmät • Web-teknologiat
Fyysinen tietoturvan valvonta	• Fyysinen suojaus • Henkilöstöön liittyvä tietoturva

Pääteknologioiden kohdalla aluksi esitetään yleistä tietoa tähän liittyen, kuten miksi todennus ja valtuutus on tärkeää. Näissä fokuksena on selkeästi OT-ympäristöt. Menetelmien, työkalujen ja vastatoimien kohdalla annetaan yleiskatsausta ratkaisusta, kerrotaan mitä haavoittuvuuksia sillä voidaan käsitellä, kerrotaan ratkaisun käyttöönotosta, arvioidaan sen ongelmia ja heikkouksia, arvioidaan sen käyttöä teollisessa ympäristössä, tutkitaan sen tulevaisuuden näkymiä ja viimeisenä annetaan suosituksia ja ohjeita ratkaisuun liittyen.

Kuten nähdään, tämä alaosio huomioi melko kattavasti erilaisia teknologioita. Suurimpana puutteena standardissa on sen ikä. Kymmenessä vuodessa ympäristöt ja työkalut ovat muuttuneet melko paljon. Tämän vuoksi listausta ei voi pitää kattavana.

IEC 62443-3-2: Järjestelmäsuunnittelun tietoturvariskien arviointi

Julkaistu:	2020
Kenelle tarkoitettu:	Omistajat
Voiko sertifioitua:	Ei
Sivumäärä:	31

Kyseisessä standardin alaosiossa käsitellään sitä, miten organisaatiot voivat suorittaa riskiarviointeja teollisuuden ohjausjärjestelmiin. Standardissa jaetaan tarkasteltava ohjausjärjestelmä osa-alueisiin (vyöhykkeet ja kanavat), joita tutkitaan. Kullekin määritetään tietoturvan tavoitetaso. Dokumentin perusteella etenkin omistajat voivat arvioida tietoturvariskejä automaatioverkossa.

Standardi esittää prosessin, jolla riskejä lähdetään arvioimaan. Ensimmäiseksi valitaan järjestelmä, joka on tarkastuksen alla, ja pyritään löytämään tähän liittyvät liitäntäpisteet. Tämän jälkeen järjestelmälle tehdään alustava riskiarviointi ja järjestelmä jaetaan tarkasteltaviin osa-alueisiin. OT-ympäristö jaetaan tämän jälkeen palasiin muun muassa niin, että liiketoiminnalliset osat ovat erillään ohjausjärjestelmistä. Alustavan riskiarvioinnin tuloksia verrataan hyväksyttävään riskiin, jonka jälkeen siirrytään riskiarvioinnin käsittelyyn.

Tärkein osa standardia on itse riskiarviointi, johon dokumentti antaa kattavat ohjeet. Ytimessä on riskiarvioinnin teko tarpeeksi kattavasti, ja tulosten dokumentointi. Riskiarviointeja tulisi myös tehdä säännöllisesti. Dokumentin viimeisenä kohta on Omaisuuden omistajan hyväksyntä. Tässä kohdassa omaisuuden omistaja määrittää, onko suunniteltu vastakeino riittävä, ja onko tämän jälkeen riski siedettävällä tasolla.

IEC 62443-3-3: Järjestelmän turvallisuusvaatimukset ja turvallisuustasot

Julkaistu:	2019
Kenelle tarkoitettu:	Omistajat, palveluntuottajat, toimittajat
Voiko sertifioitua:	Kyllä
Sivumäärä:	84

IEC 62443-3-3 on standardiperheen toinen osa, johon organisaatiot voivat sertifioitua. Tämä osa on yksi teknisimmistä osioista, koska se sisältää yksityiskohtaiset vaatimukset ohjausjärjestelmille. Vaatimukset perustuvat turvallisuustasoihin, jotka esiteltiin jo lyhyesti osassa 1-1. Tätä standardin osaa voi hyödyntää moneen tarkoitukseen. Omistajat voivat vaatia toimittajilta tiettyjen vaatimusten täyttämistä, kun taas palveluntuottajat ja toimittajat voivat sertifioida järjestelmänsä vastaamaan tiettyihin vaatimuksiin.

Standardissa kerrotaan tekniset vaatimukset (SR = System Requirement) ohjausjärjestelmälle. Nämä vaatimukset on jaettu kategorioihin (FR = Foundational Requirement). Jokaisella organisaatiolla, joka hyödyntää dokumenttia, tulisi olla päätettynä tietoturvan taso, jota tavoitellaan (SL = Security Level). Eri tasoille on eritasoisia vaatimuksia. Vaatimuksissa käytetään samaa nimeämistapaa kuin IEC 62443-2-4 -standardissa eli perustason vaatimukset on nimetty BR ja korkeamman tason vaatimukset RE. Tietoturvan tasoja ovat:

Taulukko 2. Tietoturvan tasot

SL 1	Estä tietojen luvaton paljastaminen salakuuntelun tai satunnaisen altistumisen avulla.
SL 2	Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle yksinkertaisilla keinoilla, joilla on vähän resursseja, hieman taitoja ja alhainen motivaatio.
SL 3	Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle kehittyneillä keinoilla, joilla on kohtuulliset resurssit, ICS -erityistaitoja ja kohtalainen motivaatio.
SL 4	Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle kehittyneillä keinoilla, joilla on laajat resurssit, ICS -erityistaitoja ja korkea motivaatio.

Kuten taulukosta 2 nähdään taso SL 1 on helpoin saavuttaa, kun taas taso SL 4 vaativin taso. Kullekin FR-tason vaatimukselle on määritetty yleiset kuvaukset siitä, mitä tulisi olla tehtynä, jotta järjestelmä on tietyllä SL-tasolla. Dokumentin kannalta tärkein on kuitenkin listaus SR-tason vaatimuksista, joiden kautta tietty SL-taso saavutetaan. FR-tason vaatimukset ovat:

- FR 1 – Identification and authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Kuten mainittu, näihin kaikkiin liittyy SR-tason vaatimuksia. Esimerkiksi “FR 1 – Identification and authentication control” liittyviä SR-tason vaatimuksia otsikkotasolla ovat muun muassa:

- SR 1.1 Human user identification and authentication
- SR 1.2 – Software process and device identification and authentication

Kunkin SR-tason vaatimuksen alla voi vielä olla RE-vaatimuksia. Esimerkiksi ”SR 1.2 Software process and device identification and authentication” vaatimuksen alle kuuluu:

- SR 1.2 RE 1 – Unique identification and authentication

Näiden vaatimusten kautta syntyy kattava lista vaatimuksista järjestelmille. Käytännössä 3-3 osan sisältö rakentuu näistä palasista. Dokumenttiin sisältyy myös liitteitä. Liitteessä A käsitellään SL-tasoja kertoen tarkemmin siitä, miten SL-tasoja käytetään, ja miten itselle sopiva taso valitaan. Liitteessä B on erittäin hyödyllinen taulukko siitä, mitkä SR tason vaatimukset liittyvät mihinkin SL tasoon. Eli taulukko kuvaa sen, mitä vaatimuksia tulee täyttää, jos organisaatio haluaa päästä tietylle SL-tasolle.

3.2.4 IEC 62443-4

Standardin 62443 osassa 4 fokuksen alla on komponentit. Tämän alaosion tarkoituksena on määrittää vaatimukset komponenttien tuotekehitykselle ja tekniset vaatimukset itse komponenteille. Luvussa on yhtäläisyyksiä osan 3 kanssa, mutta erona on se, että tarkastelun alla ovat juurikin komponentit kun aiemmassa osassa tarkasteltiin järjestelmiä. (ISA/IEC, 2018, 2019b)

IEC 62443-4-1: Turvallisen tuotekehityksen elinkaaren vaatimukset

Julkaistu:	2018
Kenelle tarkoitettu:	Toimittajat
Voiko sertifioitua:	Kyllä
Sivumäärä:	62

IEC 62443-4-1 on standardiperheen kolmas osa, johon organisaatiot voivat sertifioitua. Osa poikkeaa hieman muista osista, koska tässä tarkastellaan tarkemmin toimittajan tuotekehitysprosessia. Standardi määrittelee vaatimukset OT-ympäristöihin toimitettavien tuotteiden tuotekehitysprosessille. Standardi myös ohjaa kattavasti tuotekehityksessä. Vaatimuksia voidaan soveltaa uusien laitteiden toimituksissa, ylläpitovaiheessa tai käytöstä poistossa.

Standardin alussa esitellään yleisiä periaatteita turvalliseen tuotekehitykseen. Standardia seuraamalla pystytään vastaamaan myös helpommin IEC

62443-4-2 vaatimuksiin, jotka koskevat itse komponentin/tuotteen vaatimuksia. 4-1 osassa viitataan ”secure by design”-periaatteeseen, jossa tietoturva rakennetaan tuotteeseen alusta saakka. Ydinperiaate standardissa on kerroksittainen suojaus, johon turvallisella tuotekehityksellä pyritään. Turvallisen tuotekehityksen ajurina on uhkamallinnus, jota tehdään samanaikaisesti tuotekehitysprosessin kanssa.

Standardin vaatimukset on jaettu kahdeksan eri praktiikan alle:

1. Security management
2. Specification of security requirements
3. Secure by design
4. Secure implementation
5. Security verification and validation testing
6. Management of security-related issues
7. Security update management
8. Security guidelines

Kunkin praktiikan alla esitetään aluksi, mikä on niiden tarkoitus. Esimerkiksi ”Security management” -praktiikan tarkoitus on varmistaa, että tietoturvaan liittyvät aktiviteetit on suunniteltu, dokumentoitu ja suoritettu oikealla tavalla läpi tuotekehityksen elinkaaren.

Praktiikoiden alla on tarkempia vaatimuksia siitä, mitä osa-alueet sisältävät. Esimerkiksi ensimmäisen praktiikan alla on kuvattu mitä kehitysprosessiin tulee sisältyä. Sen alla on myös määritelty se, että vastuut on selkeästi jaettu. Jokaiseen vaatimukseen sisältyy perustelut, miksi näin on oltava sekä ohjeistuksia siitä, miten vaatimuksen voi täyttää.

Standardin liitteessä A esitellään erilaisia metriikoita, joilla tuotekehitysprosessia voi mitata. Liitteessä A on muutamia esimerkkejä, joita organisaatiot voivat halutessaan soveltaa tuotekehityksessä. Liitteessä B kerätään yhteen kaikki dokumentin vaatimukset. Tässä luvussa esitellään taulukko, jossa on vaatimukset otsikkotasolla.

IEC 62443-4-2: Tekniset turvallisuusvaatimukset IACS komponenteille

Julkaistu:	2019
Kenelle tarkoitettu:	Toimittajat
Voiko sertifioitua:	Kyllä
Sivumäärä:	103

IEC 62443-4-2 on standardiperheen viimeinen osa, ja samalla viimeinen osa, johon organisaatiot voivat sertifioitua. Tämä osa määrittelee yksityiskohtaiset tekniset vaatimukset komponenteille, joita käytetään IACS-ohjausjärjestelmien yhteydessä. Standardin sisältö on hyvin lähellä osaa 3-3, mutta fokus on komponenteissa.

Standardissa mainitaan jo aluksi, että vaatimukset on johdettu osan 3-3 vaatimuksista. Osassa 4-2 nämä ovat nimeltään CR (Component Requirements). Dokumentti esittää vaatimuksia neljälle erityyppiselle komponentille: applikaatiot, sulautetut järjestelmät, isäntälaitteet ja verkkolaitteet. Suurin osa vaatimuksista on samoja kaikille laitteille, mutta myös joitain komponenttispesifejä vaatimuksia esitetään.

Tässä standardin osassa vaatimukset on jaoteltu samojen FR-tason vaatimusten mukaisesti, jotka esitettiin osan 3-3 yhteydessä. Standardissa käytetään myös SL-tasoja vastaavasti. Vaatimuksissa itsessään ja näihin liittyvissä tarkemmissa RE-vaatimuksissa on eroja, mutta muuten standardit 3-3 ja 4-2 ovat hyvin toistensa kaltaisia. Tämä vuoksi ei ole tarpeen esitellä standardin 4-2 rakennetta tarkemmin enää tässä yhteydessä.

Liitteessä A annetaan esimerkkejä kustakin komponenttityypistä. Näiden tarkoitus on helpottaa standardin soveltamista. Liitteeseen B on taulukoitu vaatimukset ja näiden SL-tasot. Myös komponenttikohtaiset erot on huomioitu tässä taulukossa.

3.3 Miten IEC 62443 -standardiin voi sertifioitua?

IEC 62443 -standardin osiin 2-4, 3-3, 4-1 ja 4-2 voi sertifioitua. Seuraava kysymys kuuluu, miten näihin standardeihin voi sertifioitua. Käytännössä erilaisia sertifiointiohjelmia hallinnoivia tahoja on kaksi: ISASecure ja IECEE (Hohenegger ym., 2021).

ISASecure on ISA:n alainen, voittoa tavoittelematon organisaatio (International Society of Automation, 2020). Organisaatio on nimennyt sertifikaatit standardista poikkeavasti. Sertifikaatit ovat nimeltään Security Development Lifecycle Assurance (SDLA), System Security Assurance (SSA), Component Security Assurance (CSA) ja IIoT Component Security Assurance (ICSA). ISASecure ei itse tee auditointeja, vaan näitä hoitaa CB:t (Certification Body) (ISASecure, 2024). Kyseiset CB:t ovat ISASecuren hyväksymiä ja ulkopuolisen organisaation auditoimia.

Toinen vaihtoehto hakea sertifikaattia on IECEE:n ohjelman kautta. IECEE on IEC:n standardeihin perustuva sertifikaattiohjelma (IECEE, 2024a). IECEE:n standardit on nimetty suoraan IEC 62443 -standardin osien mukaisesti toisin kuin ISASecuren standardit. Myöskään IECEE ei tee itse auditointeja (IECEE, 2024b). IECEE:n kautta sertifioinnit tulevat vastaavasti kuin ISASecuren kautta, eli hyödyntämällä ulkopuolisia CB:ja.

4 TUTKIMUSASETELMA JA SUORITUS

Luvussa esitellään tutkimuksen käytännön toteutus, aineisto sekä tutkimuskysymykset. Tämä luku vastaa siihen, miten tutkimus on suoritettu.

4.1 Kirjallisuuskartoitus

Tutkimuksen perusteet ja teoriaosuus tehtiin kirjallisuuskartoituksella. Ensimmäiseksi käytiin läpi alan tärkeimmät julkaisut, kuten Computer & Security, Information Management & Computer Security ja European Journal of Information Systems. Näiden julkaisuihin tutustumisen jälkeen tutustuttiin laajemmin alan materiaaliin käyttämällä hakukoneita: JYKDOK, Web Of Science, Science Direct, Scopus and Google Scholar. Hakusanoina käytettiin muun muassa:

- IEC 62443
- IEC 62443 certificate
- Operational technology security
- OT security
- ICS security
- IT vs. OT
- Purdue model

Myös näiden yhdistelmiä käytettiin hakusanoina. Lähteitä etsittiin englannin kielellä, koska aiheesta on rajallisesti akateemista materiaalia suomeksi. Tarkoitus oli löytää mahdollisimman paljon hyödyllisiä lähteitä näillä hakusanoilla. Myös löydetyn materiaalin lähdeluetteloita käytettiin uusien lähteiden löytämiseen. Yhtenä tärkeänä lähteenä teoriaosuudessa toimii itse IEC 62443 -standardi, mutta tavoitteena oli etsiä standardia tukevaa materiaalia.

Ensimmäisellä haravoinnilla alan tärkeimmistä julkaisuista löydettiin melko suuri määrä aiheeseen liittyviä artikkeleita. Aihetta on myös sivuttu monessa eri artikkelissa, joten teoriapohjaa aiheesta on saatavilla laajasti. Taulukossa 1 esitetään löydetyt lähteet Google Scholarista.

Taulukko 3. Lähteiden määrät

Hakusana	Lähteiden määrä
IEC 62443	4 000
IEC 62443 certificate	2 110
Operational technology security	4 320 000
OT security	685 000
ICS security	1 770 000
IT vs. OT	5 180 000
Purdue model	1 230 000
IEC 62443	4 000

Jos vain lähteiden määriä katsotaan, voisi olettaa, että hyviä lähteitä ja materiaalia on saatavilla erittäin paljon. Näin ei kuitenkaan ole. Suuri osa lähteistä ei käsittele suoraan tutkimusaihetta. Esimerkiksi Purdue-malliin liittyen löytyy paljon materiaalia, mutta päätutkimuskysymyksen käsitellessä IEC 62443 -sertifiointeja Suomessa, jää tähän liittyvien lähteiden määrä rajalliseksi. Tämän vuoksi tutkimuksessa tukeudutaan suuresti IEC 62443 -standardiin. Tutkimukseen saatava suurin hyöty tutkimuskysymyksen kannalta on käytännön haastatteluissa.

4.2 Tutkimuskysymykset ja -strategia

Tutkimuskysymyksenä on:

- **Onko Suomalaisissa yrityksissä havaittu tarvetta IEC 62433 sertifikaateille?**

Tähän vastataan avustavien tutkimuskysymysten kautta:

1. **Mitä tarkoittaa OT-kyberturva?**
2. **Miten OT-kyberturva eroaa IT-kyberturvasta?**
3. **Miksi organisaatiot sertifioituvat?**
4. **Mikä on IEC 62443 -standardiperhe ja mitä tämä sisältää?**
5. **Miten IEC 62443 -sertifikaattiin liittyen voi sertifioitua?**
6. **Kenellä Suomessa on IEC 62443 -sertifikaatteja?**
7. **Onko yrityksissä tietoisuutta sertifikaatista?**
8. **Onko yrityksissä havaittu tarvetta sertifikaatille?**

Vastaukset ensimmäisestä avustavasta kysymyksestä viidenteen pyrittiin löytämään teoriaosuuden avulla, eli luvuissa 2–3. Loppuihin avustaviin kysymyksiin vastataan tulosten kautta. Kuudenteen avustavaan kysymykseen vastataan kartoittamalla suomalaisten yritysten sertifikaateista löytyviä tietoja. Seitsemänteen ja kahdeksanteen avustavaan tutkimuskysymykseen vastataan haastattelujen avulla.

Tutkimusmenetelmänä käytetään puolistrukturoitua teemahaastattelua. Haastattelut ovat kvalitatiivisia. Puolistrukturoituun teemahaastatteluun päädyttiin, koska tämän tyyppiset haastattelut antavat joustavuutta, mutta samalla ohjaavat haastatteluja tiettyyn suuntaan (Hirsjärvi & Hurme, 2022). Tavoitteena on saada syvällistä dataa siitä, nähdäänkö organisaatioissa tarvetta sertifikaateille. Haastattelujen kautta on mahdollista päästä käsiksi hiljaiseen tietoon, toisin kuin kvantitatiivisten menetelmien avulla (Ahlström-Laakso, 2015).

Kvalitatiiviselle tutkimukselle tyypillistä on tuoda esiin tutkimukseen osallistuvien henkilöiden näkökulmia ja ajatuksia (Puusa ym., 2020). Myös tämän vuoksi tutkimus suoritetaan haastattelemalla. Hirsjärvi ja Hurme (2022) kuvaavatkin että haastattelu, joustavana tutkimusmenetelmänä sopii moniin erilaisiin tutkimuksiin.

Kvalitatiivisessa tutkimuksessa on vahvuutena sen joustavuus (Puusa ym., 2020). Tutkimuskysymyksiä voidaan tässä menetelmässä tarkentaa tarvittaessa aineistonkeruun jälkeen. Tutkimuksessa nähtiin tärkeäksi tämä mahdollisuus, koska tutkimuksessa ei esitetä hypoteeseja lopputuloksista. Ennen tutkimusta ei ollut oletuksia siitä, mitä tulokset tulevat olemaan.

Haastatteluissa on riskinä se, että tulokset voivat vääristyä haastateltavan näkökulmista johtuen (Qu & Dumay, 2011). Haastattelijoilla on usein tietoa aiheesta, joka ohjaa keskustelua tiettyyn suuntaan. Tässä tutkimuksessa haastattelijan hyvää tietämystä aiheesta ei kuitenkaan nähty riskiksi tutkimuskysymysten luonteesta johtuen. Koska tarkoituksena on kartoittaa standardiin liittyviä tarpeita, ei tietämys standardista tai markkinasta vaikuta tuloksiin. Vastausten täytyy tulla haastateltavilta itseltään.

4.3 Aineiston keruu ja analyysi

Ensimmäisenä osana aineistonkeruuta on suomalaisten yritysten kartoitus. Tässä pyrittiin kartoittamaan millä suomalaisilla yrityksillä on IEC 62443 -sertifikaatteja, ja minkä tyyppisiä nämä yritykset ovat. Tämä aineistonkeruu tehtiin pääasiassa selaamalla internetistä yritysten sivuja, pyrkien löytämään tietoja sertifikaateista. Hakukoneita, kuten Googlea käytettiin tässä työkaluna.

Seuraavassa vaiheessa haastatellaan suomalaisia yrityksiä tietoturvatarpeista. Haastattelut toteutettiin etähaastatteluina videopalaverina. Laadullisessa tutkimuksessa ei pyritä yleistyksiin, vaan tarkoituksena on ilmiöiden ja tapahtumien kuvaaminen ja toiminnan ymmärtäminen (Tuomi & Sarajärvi, 2018). Tämän vuoksi jo melko pienellä haastattelumäärällä voidaan vastata tutkimuskysymyksiin. Tavoitteena oli haastatella noin viittä keskisuurta/suurta yritystä. Pienet yritykset jätettiin ulkopuolelle, koska haastattelijan kokemuksen perusteella harvalla näistä on riittävästi resursseja tehdä merkittäviä panostuksia tietoturvaan. Haastateltavaksi pyrittiin saamaan se henkilö, joka vastaa yrityksen tietoturvasta tai vastaava henkilö. Haastatteluissa käytetään haastattelukysymyksinä seuraavia kysymyksiä:

- Kuinka tuttu IEC 62443 on yritykselle?
- Onko hallintaympäristöä, tuotetta tai palveluita rakennettu standardin mukaisesti?
- Onko yrityksellä esiintynyt kysyntää IEC 62443 -standardille/sertifikaateille?
- Jos on, mille standardin osille?
- Onko kysyntä tullut sisäisistä vai ulkoisista lähteistä?
- Onko yrityksellä tarkoitus sertifioitua lähitulevaisuudessa tai onko se sertifioitunut johonkin standardin osaan?

Haastattelut tallennettiin, jos haastateltava antoi luvan. Jollei nauhoitusta sallittu, kirjattiin asiat ylös haastattelun yhteydessä. Haastattelujen jälkeen tallenteet litteroitiin. Litteroitujen haastattelujen pohjalta tehtiin johtopäätökset. Haastattelujen tallenteet olivat vain kirjoittajan omaksi avuksi, ne poistettiin prosessin jälkeen. Haastateltuja henkilöitä tai yrityksiä ei mainita nimeltä. Yrityksistä ei myöskään jaeta tietoja niin, että sen pystyisi päättelemään tutkimuksen perusteella.

Tutkimuksessa haastateltiin lopulta kahdeksaa eri yritystä. Haastatteluista saatujen vastausten perusteella pyrittiin luomaan käsitys siitä, onko suomalaisilla yrityksillä tarvetta IEC 62443 -sertifikaateille. Oletus oli, että yleisesti markkinoilla on havaittu lisääntyvää tarvetta IEC 62443 -sertifikaateille. Tutkimustulokset nähdään joka tapauksessa mielenkiintoisiksi, koska tutkimus antaa lisää tietoa nykytilanteesta useassa eri yrityksessä.

5 TULOKSET

Luvussa 5 esitellään tutkimuksen tulokset. Ensimmäisessä alaluvussa esitellään tulokset, jotka liittyvät kuudenteen avustavaan tutkimuskysymykseen, eli ” Kenellä Suomessa on IEC 62443 -sertifikaatteja?”. Seuraavassa alaluvussa esitellään tulokset, joiden avulla vastataan loppuihin avustaviin tutkimuskysymyksiin, eli ”Onko yrityksissä tietoisuutta sertifikaatista?” ja ”Onko yrityksissä havaittu tarvetta sertifikaatille?”. Tässä osassa esitellään myös yritykset, joita tutkimuksessa haastateltiin, ja kerrotaan näiden yritysten haastatteluissa esille tulleet vastaukset haastattelukysymyksiin kysymyskohtaisesti.

5.1 Yritykset, joilla on IEC 62443 -sertifikaatti

Yrityksiä, joilla on IEC 62443 –sertifikaatti, kartoitettiin internetin välityksellä. Tavoitteena oli löytää mahdollisimman paljon erilaisia yrityksiä, jotka ovat ilmoittaneet sertifioituneensa tiettyyn osaan IEC 62443 -standardiperheestä. Listalle valittiin yrityksiä, joiden toimintaa johdetaan Suomesta, tai joilla on vahvasti omaa toimintaa Suomessa. Listalle ei kuitenkaan otettu yrityksiä, joiden Suomen toiminnot keskittyvät vain myyntiin ja huoltoon. Lista ei ole kaiken kattava. Sen tarkoituksena ei ole antaa yleispätevää listausta kaikista sertifioituneista yrityksistä. Listan tavoitteena on antaa kuvaa siitä, millaiset yritykset hakevat sertifikaatteja.

Taulukossa 4 esitellään yritykset, joiden havaittiin hankkineen sertifikaatti IEC 62443 -standardia vasten.

Taulukko 4. Yritykset, joilla on IEC 62443 -sertifikaatteja

Yritys	Koko		62443-2-4	62443-3-3	62443-4-1	62443-4-2	Lähde
	Liikevaihto	Työntekijät					
Valmet	5,5 B€	n. 19 000			**X**		(Valmet, 2024)
ABB	$32,2 B	n. 105 000			**X**	**X**	(ABB, 2023)
Hitachi	$70,51 B	n. 300 000	**X**	**X**	**X**	**X**	(Hitachi, 2024)
Wärtsilä	5,8 B€	n. 18 000			**X**	**X**	(Wärtsilä, 2020)
Kone	10,5 B€	n. 56 000			**X**	**X**	(Kone, 2023)
Kalmar	2 B€	n. 5000			**X**		(Kalmar, 2023)
Etteplan	359 M€	n. 4000			**(X)** Haettu, ei varmuutta onko saatu		(Etteplan, 2023)
Insta	153 M€	n. 1100			**X**		(Insta, 2024)
WithSecure	79 M€	n. 500			**X**	**X**	(WithSecure, 2019)

Kuten taulukosta 4 nähdään, suurin osa yrityksistä, joilla on IEC 62443 – sertifikaatteja, ovat erittäin isoja. Jokaisen yrityksen liikevaihto ylitti 50 miljoonaa euroa, ja työntekijämäärä oli yli 250. Tämä tarkoittaa sitä, ettei yksikään yritys ole keskisuuri, vaan kyseessä on suuryrityksiä. Tuloksista näemme, että markkinoilla sertifikaatteja on lähtökohtaisesti vain suurilla yrityksillä.

Sen lisäksi, että tutkimuksen perusteella nähdään, millaisilla yrityksillä on sertifikaatteja, nähdään, että sertifikaatteja on markkinoilla toistaiseksi melko vähän. Tutkimuksessa ei onnistuttu löytämään julkisista lähteistä enempää yrityksiä, joilla sertifikaatti olisi.

Mielenkiintoinen havainto on myös se, että 62443-2-4 ja 62443-3-3 sertifikaatteja oli hyvin vähän. Vain yhdellä havaituista toimijoista oli sertifikaatit näihin standardin osiin liittyen. 62443-3-3 osuus koskee useampaa toimijaa, mutta myöskään siihen ei ole sertifioiduttu suuresti.

Yleisimpänä standardin osana oli selkeästi 62443-4-1. Kaikilla tutkimuksen alla olevilla yrityksillä olikin sertifikaatti tähän osuuteen. Organisaatiot ovat nähneet tärkeimmäksi tai ensisijaiseksi sertifioida tuotesuunnitteluprosessinsa.

5.2 Tutkimukseen osallistuneet yritykset

Tutkimukseen osallistuneita yrityksiä käsitellään tässä työssä anonyymisti. Yritysten perustietoja on kuitenkin jaettu riittävästi, jotta näiden toimialaan, toimenkuvaan ja kokoon liittyviä faktoja voidaan hyödyntää tutkimuksessa. Kustakin yrityksestä haastattelussa oli henkilö, jolla oli laajaa näkemystä tietoturvasta niin yrityksen sisäisesti kuin ulkoisestikin. Haastatteluun osallistuneet yritykset esitellään taulukossa 5.

Taulukko 5. Tutkimukseen osallistuneet yritykset

Yritys	Kokoluokka	Toimiala	Toimenkuva
Yritys 1	Suuri	Koneet ja laitteet	Suunnittelu ja valmistus
Yritys 2	Keskisuuri	Koneet ja laitteet	Suunnittelu ja valmistus
Yritys 3	Suuri	Elektroniikka	Suunnittelu ja valmistus
Yritys 4	Suuri	Koneet ja laitteet	Suunnittelu ja valmistus
Yritys 5	Suuri	Ohjelmistot	Suunnittelu
Yritys 6	Suuri	Koneet ja laitteet	Suunnittelu
Yritys 7	Suuri	Koneet ja laitteet	Suunnittelu ja valmistus
Yritys 8	Keskisuuri	Elektroniikka	Suunnittelu ja valmistus

Taulukon 5 yrityksistä kaikilla on vahvasti toimintaa Suomessa, ja niitä voidaankin pitää suomalaisina. Yritykset pyrittiin valitsemaan sillä perusteella, että niillä olisi mahdollisimman todennäköisesti tekemistä IEC 62443 -sertifikaattiin liittyen. Valinta tehtiin perustuen siihen, minkälaisilla yrityksillä markkinoilla oli sertifikaatteja.

5.3 Haastattelujen tulokset

Haastattelujen tulokset esitellään haastattelukysymyksittäin. Kunkin yrityksen vastaukset kysymyksiin esitetään taulukoissa. Tulosten tulkinta ja pohdinta tehdään luvussa 6.

Kuinka tuttu IEC 62443 on yritykselle?

Taulukko 6. IEC 62443 tunnettuus

Yritys	Vastaus
Yritys 1	Erittäin tuttu
Yritys 2	Tuttu ylätasolla
Yritys 3	Erittäin tuttu
Yritys 4	Erittäin tuttu
Yritys 5	Melko tuttu
Yritys 6	Melko tuttu
Yritys 7	Erittäin tuttu
Yritys 8	Erittäin tuttu

Taulukosta 6 nähdään, että standardi on tuttu kaikille tutkimukseen osallistuneista yrityksistä. Viidelle yrityksistä standardi on erittäin tuttu, kahdelle melko tuttu ja yhdelle tuttu vain ylätasolla. Standardi vaikuttaa kuitenkin kaikkien yritysten toimintaan jollain tavalla, koska jokaisessa haastatellussa yrityksessä se oli tullut vastaan.

Onko hallintaympäristöä, tuotetta tai palveluita rakennettu standardin mukaisesti?

Taulukko 7. Ympäristön, prosessin tai tuotteiden standardin mukaisuus

Yritys	Hallintaympäristö	Prosessi	Tuote
Yritys 1		**X**	**X**
Yritys 2			
Yritys 3	**X**	**X**	**X**
Yritys 4		**X**	
Yritys 5			
Yritys 6		**X**	
Yritys 7		**X**	**X**
Yritys 8		**X**	**X**

Toisessa kysymyksessä selvitettiin sitä, onko yritysten hallintaympäristöä, prosesseja tai tuotteita rakennettu standardin mukaisesti. Taulukosta 7 voi nähdä, että vain yksi yrityksistä on rakentanut hallintaympäristöään standardin vaatimusten mukaisesti. Kuusi yrityksistä on rakentanut prosessejaan standardin vaatimusten mukaisesti. Yritykset, jotka eivät ole tätä tehneet ovat yritykset 2 ja 5. Erityispiirteinä näissä yrityksissä on, että toinen näistä on keskisuuri yritys ja toinen tekee ohjelmistosuunnittelua.

Tuotteitaan standardin mukaisesti ovat rakentaneet neljä yritystä kahdeksasta. Kaksi näistä ovat elektroniikan suunnittelijoita ja valmistajia. Loput kaksi ovat koneiden ja laitteiden suunnittelijoita ja valmistajia.

Onko yrityksellä esiintynyt kysyntää IEC 62443 -standardille/sertifikaateille? Jos on, mille standardin osille? Onko kysyntä tullut sisäisistä (S) vai ulkoisista (U) lähteistä?

Taulukko 8. Kysyntä IEC 62443 -standardille/sertifikaateille

Yritys	2-4	3-3	4-1	4-2
Yritys 1		**S&U**	**S&U**	**S&U**
Yritys 2		**U**		**U**
Yritys 3	**S**	**U**	**S&U**	**U**
Yritys 4			**U**	**U**
Yritys 5			**U**	
Yritys 6			**S&U**	
Yritys 7		**U**	**S&U**	**U**
Yritys 8			**U**	**U**

Taulukot 8, 9 ja 10 muodostavat avaintuloksen tämän tutkimuksen tutkimuskysymyksen kannalta. Taulukkoon 8 on listattu, mille yrityksille on esiintynyt kysyntää IEC 62443 -standardiin liittyviin sertifikaatteihin liittyen. Taulukkoon on lueteltu, onko tarve lähtöisin sisäisistä (S) vai ulkoisista (U) lähteistä. Kuten taulukosta nähdään, 2-4 osioon liittyviä sertifikaattitarpeita on ollut vain yhdellä yrityksellä, ja kysyntä on sisäistä. 3-3 osiin liittyviä tarpeita on esiintynyt puolella yrityksistä. Näistä kaikilla yrityksistä kysyntä on ollut ulkoista, mutta Yrityksellä 1 kysyntä on ollut osaksi myös sisäistä.

Osioon 4-1 liittyvää kysyntää on ollut kaikkein eniten. Seitsemällä kahdeksasta yrityksestä on esiintynyt kysyntää tälle osiolle. Kaikilla näistä yrityksistä kysyntä on ollut ulkoista, mutta neljällä kysyntä on ollut myös osaksi sisäistä. Vain yrityksellä 2 ei ole ollut kysyntää tälle standardin osalle.

Standardin osaan 4-2 liittyen kysyntää on ollut kuudella yrityksellä. Kaikilla näistä kysyntä on ollut ulkoista, mutta yhdellä myös sisäistä. Yritykset, joilla ei ole ollut kysyntää tähän standardin osaan liittyen, ovat keskittyneet suunnitteluun, eikä tämä standardin osa näin kosketa näitä toimijoita.

Taulukkoihin 9 ja 10 on kirjattu kysynnän lähteet tarkemmin, kappalemäärittäin.

Taulukko 9. Sisäiset kysynnän lähteet

Kysynnän lähde, sisäinen	kpl
Yleinen tietoturvan kehitys ja varautuminen tulevaan	**4**

Taulukko 10. Ulkoiset kysynnän lähteet

Kysynnän lähde, ulkoinen	kpl
Asiakasvaatimukset	**8**
CRA (Cyber Resilience Act)	**2**
Koneasetus	**2**
NIS2	**2**

Taulukoissa 9 ja 10 on esitelty kysynnän lähteet. Taulukossa 9 on sisäiset lähteet, taulukossa 10 ulkoiset lähteet. Kuten Taulukosta 9 nähdään, kaikilla yrityksillä sisäiset kysynnän lähteet olivat lähtöisin tarpeesta kehittää tietoturvaa ja varautua tulevaan. Yhdellä yrityksistä tarve on herännyt tietoturva-auditoinnin myötä, yhdellä on tehty strateginen päätös olla edelläkävijä tällä saralla ja lopuissa on todettu, että standardin mukainen tietoturvan kehitys on sijoitus tulevaan. Näissä on nähty todennäköiseksi että, standardin mukaisesta prosessista tulee olemaan konkreettista hyötyä tulevaisuudessa.

Ulkoisia lähteitä kysynnälle on huomattavasti enemmän kuin sisäisiä. Taulukon 10 mukaan kaikissa yrityksistä ulkoisina lähteinä standardille toimi asiakasvaatimukset. Kaikki yritykset olivat nähneet asiakkaiden vaatimuksissa viittauksia 62443 -standardiin. Vain harvoin yrityksiltä oli vaadittu varsinaista sertifikaattia. Kaikilta oli kuitenkin vaadittu, että nämä täyttäisivät osia standardin sisällöstä. Haastatteluissa kävi kuitenkin ilmi, että IEC 62443 liittyvät vaatimukset markkinoilla eivät ole vielä normi, vaatimuksia esiintyy satunnaisesti. Haastatteluissa kävi ilmi, että suuret asiakkaat esittävät useammin vaatimuksia IEC 62443 -standardiin liittyen kuin pienet asiakkaat.

Muita ulkoisia kysynnän lähteitä olivat CRA (Cyber Resilience Act), Koneasetus ja NIS2. Nämä kaikki ovat pakottavia vaatimuksia yrityksiä/laitevalmistajia kohtaan, ja ne tulevat sisältämään tietoturvaan liittyviä vaatimuksia (EUR-Lex, 2022, 2023; European Commission, 2022). Haastatelluissa yrityksissä oli koettu, että IEC 62443 -standardin mukaisella toiminnalla pystytään vastaamaan myös näiden pakottavien vaatimusten tarpeisiin. Yritykset olivat siis lähteneet ennakoivasti kehittämään toimintaansa IEC 62443 -standardin mukaiseksi, jotta tulevaisuudessa vastataan CRA:n, Koneasetuksen ja NIS2:den vaatimuksiin.

Onko yrityksellä tarkoitus sertifioitua lähitulevaisuudessa, tai onko se sertifioitunut johonkin standardin osaan?

Taulukko 11. Sertifioinnit ja sertifioitumissuunnitelmat

Yritys	2-4	3-3	4-1	4-2
Yritys 1			**X**	**X**
Yritys 2				
Yritys 3	**X**	**X**	**X**	**X**
Yritys 4			**X**	
Yritys 5				
Yritys 6				
Yritys 7		**X**	**X**	**X**
Yritys 8			**X**	

Taulukossa 11 on esitetty haastateltujen yritysten sertifioinnit ja/tai sertifioitumissuunnitelmat. Yrityksellä 3 on ainoana sertifikaatti tai suunnitelmissa sertifioitua osioon 2-4. 3-3 osioon sertifioituminen on ajankohtainen kahdelle yritykselle. Osioon 4-1 liittyen oli eniten sertifikaatteja tai suunnitelmia sertifioitua. Näitä oli viidellä yrityksellä. Kolmella yrityksellä oli sertifikaatti, tai suunnitelmissa sertifioitua osioon 4-2. Yrityksellä 7 oli myös suunnitelmia osion 3-3 suhteen, mutta yrityksessä ei ollut vielä varmuutta tuleeko se lopulta hakemaan sertifikaattia vain 4-2 osuuteen.

Kolmella yrityksistä ei ollut sertifikaatteja tai suunnitelmia sertifioitua mihinkään osioista. Yritys 2 on tutkimuksen ainoa keskisuuri yritys. Yritykset 5 ja 6 ovat ainoat yritykset, jotka ovat keskittyneet suunnitteluun, eivätkä valmista tuotteita.

Yrityksien 4 ja 8 sertifiointisuunnitelmat koskivat vain osiota 4-1. Näissäkin yrityksissä oli kuitenkin puhuttu mahdollisuudesta sertifioitua jossain vaiheessa etenkin osioon 4-2, mutta tämä ei ollut lähitulevaisuuden suunnitelmissa.

6 JOHTOPÄÄTÖKSET & POHDINTA

Luvussa 6 vastataan jäljellä oleviin tutkimuskysymyksiin ja pohditaan tulosten merkitystä. Ensimmäisessä alaluvussa vastataan kuudenteen avustavaan tutkimuskysymykseen, eli ”Kenellä Suomessa on IEC 62443 -sertifikaatteja?”. Seuraavassa alaluvussa vastataan loppuihin avustaviin tutkimuskysymyksiin, eli ”Onko yrityksissä tietoisuutta sertifikaatista?” ja ”Onko yrityksissä havaittu tarvetta sertifikaatille?”. Tässä luvussa myös pohditaan tulosten merkitystä ja arvioidaan niiden oikeellisuutta.

6.1 Kenellä Suomessa on IEC 62443 -sertifikaatteja?

Kuten tuloksista nähdään, sertifikaatteja on lähtökohtaisesti vain suurilla yrityksillä. Pienet yritykset eivät ole nähneet tarpeelliseksi tai niillä ei ole resursseja sertifioida prosessejaan tai tuotteitaan IEC 62443 -standardin mukaisesti. Standardiperheen ollessa melko uusi, on mahdollista, että standardiperhe tulee tulevaisuudessa koskettamaan myös pieniä yrityksiä. Tämä voi tapahtua esimerkiksi sitä kautta, että isommat yritykset vaativat sertifikaattia pieniltä yrityksiltä tulevaisuudessa.

Tulosten perusteella sertifikaatteja havaittiin melko pienellä määrällä yrityksiä. Yrityksille on tavanomaista julkaista tieto saaduista sertifikaateista monista eri syistä, kuten luvussa 3.1 mainittiin. Tästä voidaan päätellä, että sertifikaatteja on todellakin vielä melko vähän eri yrityksillä.

Organisaatiot ovat nähneet tärkeimmäksi sertifioida tuotesuunnitteluprosessinsa 62443-4-1 mukaisesti. Kaikilla tutkimuksen alla olleilla yrityksillä oli tämä sertifikaatti. Tähän syynä voi olla esimerkiksi se, että prosessien sertifiointi on usein helpompaa kuin tuotteiden, koska tuotteiden sertifioinnissa tuotteen muutokset vaikuttavat helpommin negatiivisesti sertifikaatin validiuteen.

Organisaatiot eivät ole nähneet tarvetta tai eivät ole pystyneet sertifioida 62443-2-4 tietoturvajärjestelmää. On myös mahdollista, ettei 62443-2-4 osuus ole

relevantti monelle toimijalle. Vain yhdellä toimijalla oli sertifikaatti tähän osuuteen liittyen. 62443-2-4 sertifikaatti on spesifimpi ja se koskee pienempää osaa toimijoista markkinoilla.

62443-3-3 liittyvä sertifikaatti on myös melko harvinainen. Tähän yhtenä syynä voi olla se, että 62443-4-2 vaatimukset ovat hyvin lähellä 3-3 osuuden vaatimuksia. Organisaatioissa on useammin sertifioiduttu juurikin 62443-4-2 osuuteen. Tämä voi johtua tarpeista markkinoilla tai esimerkiksi 4-2 osuuden läheisyydestä osuuteen 4-1. Tässä tapauksessa 4-2 osuus voidaan mieltää sopivan paremmin tarpeisiin, kun sertifikaatti osuudelle 4-1 on jo aiemmin haettu. Tätä tukee havainto, että kaikilla yrityksillä, joilla oli 4-2 sertifikaatti, oli myös sertifikaatti 4-1 osuuteen.

6.2 Tutkimuksen tulosten tulkinta ja pohdinta

Tutkimusten tulosten tulkinta ja pohdinta esitetään haastattelukysymyksittäin. Luvussa 6.3 vedetään yhteen johtopäätökset, ja vastataan varsinaiseen tutkimuskysymykseen.

Kuinka tuttu IEC 62443 on yritykselle?

Ensimmäiseksi haastatteluissa tutkittiin kuinka hyvin standardi tunnetaan yrityksissä. Tuloksista voimme päätellä, että standardilla on nykyisellään vaikutus kaikkiin yrityksiin, ja näiden toimialoihin. Standardin sisältö oli hyvin hallussa kaikilla yrityksillä, yhtä lukuun ottamatta. Tämä yritys on keskisuuri, ja sen toimialaa on koneiden ja laitteiden suunnittelu ja valmistus. Kuten aiemmin totesimme, sertifikaatteja on lähtökohtaisesti vain suurilla yrityksillä. On siis jopa oletettavaa, että todennäköisemmin keskisuuressa yrityksessä on heikompi ymmärrys standardin sisällöstä. Toisaalta Yritys 8 on myös keskisuuri yritys, mutta standardi oli tälle yritykselle erittäin tuttu. Tämän pohjalta emme siis voi tehdä johtopäätöksiä siitä, että standardi olisi lähtökohtaisesti vähemmän tuttu keskisuurille yrityksille.

Jos ensimmäisen haastattelukysymyksen tuloksia verrataan yritysten toimialoihin, näemme että elektroniikan toimialalla työskenteleville yrityksille standardi oli erittäin tuttu. Ohjelmistojen parissa työskentelevälle yritykselle 5 standardi oli vain melko tuttu. Koneiden ja laitteiden parissa työskentelevissä yrityksissä oli vaihtelua eikä selkeää trendiä ole nähtävissä. Suuremmalle osalle yrityksistä standardi oli kuitenkin erittäin tuttu.

Selkein trendi on nähtävissä, kun yrityksen toimenkuvaa peilataan ensimmäisen kysymyksen vastauksiin. Yrityksille 5 ja 6, jotka tekevät vain suunnittelua, standardin sisältö ei ollut yhtä tuttu kuin suunnittelua ja valmistusta tekeville yrityksille. Näillekin yrityksille standardi oli tuttu, mutta näillä ei ollut kattavaa näkemystä sen kaikista eri osista. Tämä voi johtua esimerkiksi siitä, että standardi ei koske näitä yrityksiä yhtä kattavasti kuin suunnittelua ja valmistusta tekeviä yrityksiä.

Onko hallintaympäristöä, tuotetta tai palveluita rakennettu standardin mukaisesti?

Toisessa haastattelukysymyksistä näemme, että on harvinaista rakentaa hallintaympäristöä standardin vaatimusten mukaisesti. Hallintaympäristön rakentamisella standardin mukaisesti viitataan etenkin 62443-2 osan vaatimuksiin. Tulosten valossa emme voi päätellä suoraan, että tietyllä toimialalla tai toimenkuvalla työskentelevä yritys rakentaisi todennäköisemmin hallintaympäristöään standardin mukaisesti. Haastatteluissa kävi ilmi, että Yrityksen 3 tavoitteena on olla edelläkävijä tietoturvassa etenkin standardiperheeseen liittyen. Tämän vuoksi Yritystä 3 voidaan pitää poikkeustapauksena.

Suurin osa haastatelluista yrityksistä oli rakentanut prosessejaan standardin mukaisesti. Haastatellut yritykset viittasivat 62443-4-1 mukaisiin vaatimuksiin prosesseille. Suuri osa yrityksistä on siis huomioinut tuotekehitysprosesseissaan standardin vaatimukset. Tästä voimme päätellä, että tämä osa standardia on melko läsnä markkinoilla. Poikkeuksina olivat yritykset 2 ja 5. Yritys 2 on keskisuuri yritys, jolle standardi ei ole kovin tuttu. On siis oletettavaakin, ettei prosesseja ole rakennettu standardin mukaisesti. Yritys 5 oli ainoa ohjelmistosuunnitteluun keskittynyt yritys. Tuloksista voimme päätellä, että ainakaan kyseisellä alalla toimivaa ohjelmistonsuunnitteluyritystä standardi ei kosketa suuresti, koska prosesseja ei ole nähty tarpeelliseksi rakentaa tämän mukaisesti.

Tuotteitaan standardin mukaisesti oli rakentanut puolet yrityksistä. Yritykset, jotka eivät olleet rakentaneet tuotteitaan standardin mukaisesti, olivat Yritys 2,4,5 ja 6. Yritys 2 kohdalla edellisen kappaleen perustelu pätee myös tuotteen kohdalla. Toisaalta haastatteluissa kävi ilmi, että tuotteiden osat vastaavat standardin tiettyihin vaatimuksiin, mutta tuotteita ei ole varsinaisesti rakennettu standardin mukaisesti. Yritykset 5 ja 6 ovat keskittyneet suunnitteluun. Tällöin näillä ei ole tuotetta, jota voisi valmistaa standardin mukaisesti. Ainoana oikeana poikkeuksena on Yritys 4, joka ei ole rakentanut tuotteitaan standardin vaatimusten mukaisesti. Tälläkin yrityksellä oli kuitenkin tulevaisuuden suunnitelmissa tuotteiden rakentaminen standardin mukaisesti, joten tätäkään ei voi pitää poikkeuksena. Yritys 5 ei ole haastattelujen perusteella vielä yhtä pitkällä tuotteiden rakentamisessa standardin mukaisesti kuin muut yritykset.

Lopputuloksena toiseen haastattelukysymykseen liittyen voidaan todeta, että prosessien rakentaminen on melko yleistä. Myös tuotteiden rakentaminen on yleistä. Hallintaympäristön rakentaminen standardin mukaisesti taas on harvinaista.

Onko yrityksellä esiintynyt kysyntää IEC 62443 -standardille/sertifikaateille? Jos on, mille standardin osille? Onko kysyntä tullut sisäisistä (S) vai ulkoisista (U) lähteistä?

Kuten aiemmassa luvussa todettiin, suurin osa kysynnästä yrityksille on johtunut ulkoisista lähteistä. Tutkimuksessa havaittiin kuitenkin, että myös sisäistä kysyntää standardille on. Erityishuomiona tuloksissa on 2-4 standardin osuus, jolle oli vain sisäistä kysyntää. Ainoastaan yksi yrityksistä oli nähnyt tarvetta

tälle osiolle. Yrityksen tavoitteena oli kehittää tietoturvaansa tämän osion mukaisesti oman sisäisen kysyntänsä vuoksi. Tästä voidaan päätellä, että tälle standardin osiolle ei ole suuremmin tarvetta markkinoilla. On myös mahdollista, että 2-4 osion sisältö ei koske muita haastateltuja yrityksiä.

Sisäisen kysynnän kohdalla lähteenä oli aina tarve kehittää tietoturvaa ennakoivasti. Nämä yritykset kokivat, että panostus IEC 62443 mukaiseen toimintaan tuottaisi tulosta tulevaisuudessa. Näissä yrityksissä oli nähty strategisena etuna se, että vaatimuksiin vastataan jo tässä kohdassa, vaikkei kysyntää olisi hirveästi.

Huomionarvoisena asiana kysyntään liittyen on, että melkein kaikilla yrityksillä kysyntä koski 4-1 osiota, eli tuotekehitysprosessia. Tutkimuksen perusteella tarpeet koskevat yleisimmin juuri tätä osiota. Melkein yhtä yleisenä on kuitenkin 4-2 osuus, jota kohden kysyntää oli kuudella yrityksellä. Vain suunnitteluun keskittyneillä yrityksillä ei ollut kysyntää tätä osiota kohden. Tuloksista näemme selkeästi, että standardin 4-1 ja 4-2 osiot ovat selkeästi yleisimmät. Näihin liittyen esiintyy eniten kysyntää.

Osioiden 3-3 ja 4-2 sisällöt ovat pitkälti samanlaisia, mutta 4-2 osiota kohden on huomattavasti enemmän kysyntää kuin 3-3- osiota kohden. Tämä saattaa johtua esimerkiksi siitä, että 4-2 vaatimukset pystytään kohdistamaan paremmin tietynlaiselle tuotteelle. Näin 4-2 vastaa paremmin tarpeisiin.

Tässä haastattelukysymyksessä havaitut tulokset tukevat aiemman kysymyksen tuloksia. Eniten kysyntää on prosessia (osio 4-1), toiseksi eniten tuotteita (osiot 3-3 ja 4-2) ja vähiten hallintaympäristöä kohtaan (osio 2-4). Yrityksen olivat vastanneet kysyntään, sillä suurin osa yrityksistä oli rakentanut tuotteitaan ja prosessejaan sen mukaan, miten näihin liittyen oli kysyntää. Poikkeuksiakin oli, sillä Yritys 2, 4 ja 5 eivät olleet rakentaneet tuotteitaan tai prosessejaan kysynnän mukaisesti. Yrityksissä 2 ja 4 kuitenkin ymmärrettiin puute ja suunnitelmissa oli aloittaa kehitystyöt lähitulevaisuudessa. Yrityksessä 5 vastaavia suunnitelmia ei vielä ollut.

Oli odotettavaa, että ulkoisen kysynnän osuus on suurempaa kuin sisäisen kysynnän osuus. Ulkoisen kysynnän lähteinä olivat etenkin asiakasvaatimukset. Yritykset saavat rahansa lähtökohtaisesti asiakkailta, jolloin asiakasvaatimusten mukaista kehitystä on helpompi ajaa eteenpäin. IEC 62443 -standardiin liittyviä vaatimuksia on markkinoilla ja vaatimusten määrä tulee oletettavasti kasvamaan. Myös CRA:n, Koneasetuksen ja NIS2:den vaatimusten myötä on uskottavaa, että yhä useammin yrityksiltä tullaan vaatimaan IEC 62443 mukaisia vaatimuksia. Kuitenkaan sertifikaatteja ei vaadittu usein. Tästä johtuen, voidaan olettaa tilanteen markkinoilla etenevän tulevaisuudessa niin, että sertifikaatteja tullaan vaatimaan useammin. Tämä ei kuitenkaan tapahdu välttämättä nopeasti.

Onko yrityksellä tarkoitus sertifioitua lähitulevaisuudessa, tai onko se sertifioitunut johonkin standardin osaan?

Haastattelukysymyksen kohdalla selvitettiin olemassa olevia sertifikaatteja ja suunnitelmia sertifioitua. Poikkeuksina tähän liittyen olivat etenkin keskisuuri yritys, ja pelkkään suunnitteluun keskittyneet yritykset. Näissä kyseisissä

yrityksissä ei nähdä riittävää tarvetta sertifikaateille, jotta niissä olisi edes suunniteltu virallista sertifioitumista. Voidaan päätellä, että virallista sertifiointia hakevat todennäköisemmin suuret ja tuotteita valmistavat yritykset.

Muuten tulokset olivat pitkälti oletettuja aiempien haastattelukysymysten ja vastausten perusteella. Yritykset olivat sertifioitumassa niihin osioihin, joita kohden oli tehty kehitystyötä ja joita kohden oli vaatimuksia. Varsinaisia muita poikkeuksia ei ollut. Tuloksista voidaan päätellä, että kysyntää myös virallisille sertifioinneille on markkinoilla. Tuloksista myös nähdään, kuten luvussa 5.1 todettiin, että 4-1 osioon sertifioituminen on yleisintä. Osioon 4-1 sertifioitumista tukee tai seuraa usein sertifioituminen 4-2 osuuteen.

6.3 Johtopäätös

Tutkimuksen tutkimuskysymyksenä oli **"Onko Suomalaisissa yrityksissä havaittu tarvetta IEC 62433 sertifikaateille?"**. Tähän vastaus pohjustettiin edellisen alaluvun vastausten perusteella. **Suomalaisissa yrityksissä on havaittu tarvetta IEC 62443 mukaisille sertifikaateille.** Etenkin suurissa yrityksissä, jotka valmistavat tuotteita on tarpeita standardiin liittyen. Nämä yritykset ovat tehneet kehitystyötä tähän liittyen, ja ovat sertifioitumassa standardin alle. Sertifiointitarpeita nähtiin erityisesti 4-1 osioon. Samanaikaisesti, tai yrityksen saatua sertifikaatin osioon 4-1, yritykset ovat sertifioitumassa osioon 4-2, ja osaksi osioon 3-3. Useimmiten yrityksillä on kuitenkin sertifikaatit joko pelkästä osioista 4-1, tai osioista 4-1 ja 4-2.

Toistaiseksi markkinoilla on melko vähän sertifikaatteja. Tutkimuksen perusteella kuitenkin monella yrityksellä on tulevaisuuden tarpeita ja suunnitelmia standardin suhteen. Tämä johtuu osaksi toimituksiin liittyvistä asiakasvaatimuksista ja osaksi kansainvälisten vaatimusten kehittyessä (NIS2, CRA, Koneasetus). Voidaankin todeta, että tulevaisuudessa IEC 62443 -standardiin liittyvien sertifikaattien määrä tulee lisääntymään. Tämä tapahtuu mahdollisesti nopeastikin. Luultavammin parin seuraavan vuoden kuluessa saamme kuulla usean eri yrityksen sertifioineen tuotesuunnitteluprosessinsa ja tuotteensa. Standardin vaatimukset tulevat koskemaan myös pienempiä yrityksiä tulevaisuudessa. Isommat yritykset määrittävät usein vastaavat vaatimukset toimittajille kuin itselleen, jolloin myös pienempien yritysten tulee kehittää toimintaansa standardiin liittyen.

6.4 Tutkimuksen merkitys, arviointi ja jatkotutkimusaiheet

Tämän tutkimuksen suurin anti ei ole ainoastaan sen akateemisessa sisällössä, vaan etenkin sen käytännönläheisyydessä. Tutkimus antaa kuvaa siitä, mitä markkinoilla tapahtuu tätä tutkimusta tehtäessä. Tämän tutkimuksen avulla pystytään arvioimaan miten toimintaympäristö IEC 62443 -standardiin liittyen tulee muuttumaan lähivuosina. Tutkimus antaakin hyvää taustatietoa aiheesta

kiinnostuneille tutkijoille, yrityksille, ja muille tahoille. Tutkimuksen suurin merkitys on sen uutuusarvo, sillä vastaavaa tutkimusta ei ole aiemmin tehty suomessa.

Tätä tutkimusta voidaan pitää luotettavuudeltaan melko hyvänä. Haastatteluissa tuli selkeästi ilmi tarpeet standardiin liittyen. Tutkimustulokset eivät anna paljon sijaa virheille, sillä haastattelut suoritettiin suoraan avainhenkilöiden kanssa. Riskinä tutkimuksessa kuitenkin on, että se voi antaa virheellistä kuvaa markkinoiden tarpeesta. Tutkimukseen valittiin yrityksiä, joita standardi todennäköisesti koskee. Vaikka kaikilla tutkimukseen osallistuneilla yrityksillä oli käsitys standardista, tämä ei tarkoita, että kaikissa yrityksissä olisi vastaavaa käsitystä. Haastatteluja sopiessa onkin mahdollista, että yritykset, joille standardi ei ole tuttu, eivät suostuneet haastatteluun tämän takia. Haastatteluihin suostui kuitenkin suurin osa yrityksistä, joita lähestyttiin. On siis mahdollista, että muissakin yrityksissä on käsitys standardin sisällöstä. Tutkimuksen laatua voisikin vielä parantaa laajemmalla otannalla. Tuloksia tukisi hyvin haastattelun sijaan tehty kysely, joka olisi helpompaa kohdistaa isommalle määrälle erilaisia yrityksiä.

Jatkotutkimuskohteena voisi toimia IEC 62443 -standardin vaikutus eri toimialoilla. Tähän liittyen voisi tutkia sitä, millaisia yrityksiä standardi koskee ja millaisia ei. Toisena jatkotutkimuskohteena voisi olla standardin vastaavuus CRA:n, Koneasetuksen ja NIS2 vaatimuksiin. Tulevissa tutkimuksissa voitaisiin selvittää, mitä vaatimuksia IEC 62443 -standardista tulee täyttää, jotta vastataan CRA:n, Koneasetuksen ja NIS2 vaatimuksiin.

7 YHTEENVETO

Tässä luvussa vedetään lyhyesti yhteen vastaukset avustaviin tutkimuskysymyksiin, ja tätä kautta varsinaiseen tutkimuskysymykseen. Yhteenveto tehdään kysymyskohtaisesti.

Mitä tarkoittaa OT-kyberturva?

Automaatioympäristöjen teknologia tunnetaan nimellä OT (Operational Technology). OT-ympäristöissä valvotaan ja ohjataan kriittistä infrastruktuuria. OT-ympäristössä suurin osa toimijoista on laitteita, jotka kommunikoivat keskenään. Nämä laitteet vaikuttavat usein fyysiseen maailmaan. OT-ympäristöissä valvotaan ja ohjataan kriittistä infrastruktuuria, kuten sähköverkkoja, vedenjakelua, lämmöntuotantoa ja valmistavaa teollisuutta. Iskuilla OT-ympäristöön voi olla erittäin laajoja vaikutuksia. OT-ympäristöön kohdistuvat uhat eivät kohdistu vain rahalliseen menetykseen, vaan uhan alla voi olla ihmisten terveys ja henki. OT-ympäristöjen kyberturvaan tulisikin kiinnittää erityisesti huomiota.

Miten OT-kyberturva eroaa IT-kyberturvasta?

IT:n ja OT:n välillä on suuria eroja niin teknologioiden kuin hallinnollisten asioiden kannalta. Tärkeää on ymmärtää se, että nämä ovat kaksi erillistä käsitettä ja ympäristöä, joita tulee hallinnoida eri tavalla. Eroja on näiden tarkoituksessa, fokusalueissa, arkkitehtuureissa, rajapinnoissa, käyttäjissä, avainhenkilöissä, laitteissa, järjestelmissä ja riskeissä.

Miksi organisaatiot sertifioituvat?

Organisaatioilla voi olla lukuisia eri syitä sertifioitua. Tutkimuksessa havaittuja syitä oli: asiakkaiden luottamuksen parannus, kumppanisuhteiden parannus, kilpailuetu, lakisääteiset vaatimukset tai sisäisen tietoturvan parannus. Osassa tapauksista organisaatiot ovat pakotettu hankkimaan sertifikaatin, osassa sertifikaatti hankitaan omasta tahdosta. Syyt sertifikaatin hankkimiseen vaihtelevat

organisaatioiden välillä. Tietoturvasertifikaatti auttaa organisaatioita suojaamaan tietojaan, vahvistamaan luottamusta asiakkaiden keskuudessa sekä noudattamaan sääntelyä ja parantamaan kilpailukykyään markkinoilla.

Mikä on IEC 62443 -standardiperhe ja mitä tämä sisältää?

IEC 62443 -standardi jakautuu neljään eri osaan, jotka käsittelevät eri aihealueita. Aihealueet ovat nimeltään Yleinen, Politiikat ja menetelmät, Järjestelmä ja Komponentti. Kullakin osa-alueella on omat alaosionsa, jotka käsittelevät aihealueita eri näkökulmista. Standardi käsittelee kokonaisvaltaisesti teollisuusautomaatioja ohjausjärjestelmien tietoturvaa. Standardi on rakennettu niin, että standardin eri alaosiot ovat itsenäisiä kokonaisuuksia. Tietystä aiheesta kiinnostuneen lukijan ei tarvitse ostaa koko standardia, pystyäkseen hyödyntämään yhtä alaosiota. Osa standardin osioista esittää vaatimuksia ympäristöjen, prosessien ja tuotteiden kypsyydelle, kun taas osa keskittyy antamaan ylätason ohjeistuksia aihepiiriin liittyen.

Miten IEC 62443 -sertifikaattiin liittyen voi sertifioitua?

IEC 62443 -standardin osiin 2-4, 3-3, 4-1 ja 4-2 voi sertifioitua. Erilaisia sertifiointiohjelmia hallinnoivia tahoja on kaksi: ISASecure ja IECEE. Nämä organisaatiot eivät itse tee auditointeja, vaan toimivat sertifikaattiohjelmia hallinnoivina tahoina. Sertifikaattiohjelmat poikkeavat toisistaan hieman, mutta kummassakin pääasiallisena taustamateriaalina toimii IEC 62443 standardi.

Kenellä Suomessa on IEC 62443 -sertifikaatteja?

Markkinoilla sertifikaatteja on lähtökohtaisesti vain suurilla yrityksillä. Pienet yritykset eivät ole nähneet tarpeelliseksi tai niillä ei ole resursseja sertifioida prosessejaan tai tuotteitaan IEC 62443 -standardin mukaisesti.

Sertifikaatteja on markkinoilla toistaiseksi melko vähän. 62443-2-4 ja 62443-3-3 sertifikaatteja oli hyvin vähän. Organisaatiot eivät ole nähneet tarvetta tai eivät ole pystyneet sertifioida 62443-2-4 tietoturvajärjestelmää. On myös mahdollista, ettei 62443-2-4 osuus ole relevantti monelle toimijalle.

62443-3-3 liittyvä sertifikaatti on myös melko harvinainen. Tähän yhtenä syynä voi olla se, että 4-2 osion vaatimukset ovat lähellä 3-3 osuuden vaatimuksia. Organisaatioissa on useammin sertifioiduttu juurikin 62443-4-2 osuuteen. Yleisimpänä standardin osana oli selkeästi 62443-4-1. Organisaatiot ovat nähneet tärkeimmäksi sertifioida tuotesuunnitteluprosessinsa 62443-4-1 mukaisesti.

Onko yrityksissä tietoisuutta sertifikaatista?

Standardi on tuttu kaikille tutkimukseen osallistuneista yrityksistä. Standardilla on vaikutus kaikkiin tutkimukseen yrityksiin, ja näiden toimialoihin. Standardin sisältö oli hyvin hallussa kaikilla yrityksillä, yhtä lukuun ottamatta (keskisuuri yritys). Elektroniikan toimialalla työskenteleville yrityksille standardi oli erittäin

tuttu. Ohjelmistojen parissa työskentelevälle yritykselle standardi oli vain melko tuttu. Koneiden ja laitteiden parissa työskentelevissä yrityksissä oli vaihtelua eikä selkeää trendiä ole nähtävissä. Yrityksille, jotka tekevät vain suunnittelua, standardin sisältö ei ollut yhtä tuttu kuin suunnittelua ja valmistusta tekeville yrityksille. Näillekin yrityksille standardi oli tuttu, mutta näillä ei ollut kattavaa näkemystä sen kaikista eri osista.

Suuri osa yrityksistä on huomioinut tuotekehitysprosesseissaan standardin vaatimukset. Haastatellut yritykset viittasivat 62443-4-1 mukaisiin vaatimuksiin prosesseille. Tuotteitaan standardin mukaisesti oli rakentanut puolet yrityksistä. Prosessien rakentaminen standardin mukaisesti on yleistä, tuotteiden rakentaminen melko yleistä. Hallintaympäristön rakentaminen standardin mukaisesti taas on harvinaista.

Onko yrityksissä havaittu tarvetta sertifikaatille?

Osioon 4-1 liittyvää kysyntää on ollut kaikkein eniten. Vain yhdellä yrityksellä ei ollut kysyntää tähän liittyen. Melkein yhtä yleisenä on kuitenkin 4-2 osuus, jota kohden kysyntää oli usealla yrityksellä. Tuloksista nähdään että 4-1 osioon sertifioituminen on yleisintä. Osioon 4-1 sertifioitumista tukee tai seuraa usein sertifioituminen 4-2 osuuteen.

Osuudelle 2-4 standardista oli vain vähän kysyntää. Ainoastaan yksi yrityksistä oli nähnyt tarvetta tälle osiolle. Yrityksen tavoitteena oli kehittää tietoturvaansa tämän osion mukaisesti oman sisäisen kysyntänsä vuoksi. Tälle standardin osiolle ei ole suuremmin tarvetta markkinoilla

Tarpeita standardille oli tullut sekä sisäisistä että ulkoisista lähteistä. Sisäiset kysynnän lähteet olivat lähtöisin tarpeesta kehittää tietoturvaa ja varautua tulevaan. Ulkoisia lähteitä kysynnälle on huomattavasti enemmän kuin sisäisiä. kaikissa yrityksistä ulkoisina lähteinä standardille toimi asiakasvaatimukset. Kaikki yritykset olivat nähneet asiakkaiden vaatimuksissa viittauksia 62443 -standardiin. Vain harvoin yrityksiltä oli kuitenkaan vaadittu varsinaista sertifikaattia. Suuret asiakkaat esittävät useammin vaatimuksia IEC 62443 -standardiin liittyen kuin pienet asiakkaat.

Muita ulkoisia kysynnän lähteitä olivat CRA (Cyber Resilience Act), Koneasetus ja NIS2. Nämä kaikki ovat pakottavia vaatimuksia yrityksiä/laitevalmistajia kohtaan, ja ne tulevat sisältämään tietoturvaan liittyviä vaatimuksia

Tuloksien perusteella voidaan olettaa tilanteen markkinoilla etenevän tulevaisuudessa niin, että sertifikaatteja tullaan vaatimaan useammin. Tämä ei kuitenkaan tapahdu välttämättä nopeasti.

Onko Suomalaisissa yrityksissä havaittu tarvetta IEC 62433 sertifikaateille?

Tutkimuksen päätutkimuskysymykseen vastauksena saatiin: **Suomalaisissa yrityksissä on havaittu tarvetta IEC 62443 mukaisille sertifikaateille.** Etenkin suurissa yrityksissä, jotka valmistavat tuotteita on tarpeita standardiin liittyen. Nämä yritykset ovat tehneet kehitystyötä tähän liittyen, ja ovat sertifioitumassa standardin alle. Sertifiointitarpeita nähtiin erityisesti 4-1 osioon liittyen.

Samanaikaisesti, tai yrityksen saatua sertifikaatin osioon 4-1, yritykset ovat sertifioitumassa osioon 4-2. Useimmiten yrityksillä on sertifikaatit joko pelkästä osioista 4-1, tai osioista 4-1 ja 4-2.

Tutkimuksen perusteella monella yrityksellä on tulevaisuuden tarpeita ja suunnitelmia standardin suhteen. Tulevaisuudessa IEC 62443 -standardiin liittyvien sertifikaattien määrä tulee lisääntymään. Standardin vaatimukset tulevat tulevaisuudessa koskemaan myös pienempiä yrityksiä.

LÄHTEET

ABB. (1.8.2023). *ISA/IEC 62443 cyber security standard confirms protection integral to development for ABB Electrification Smart Power*. News. https://new.abb.com/news/detail/105775/isaiec-62443-cyber-security-standard-confirms-protection-integral-to-development-for-abb-electrification-smart-power

Ahlström-Laakso, S. (2015). *Kysely vai haastattelu?*

Ali, S., Faheem, M. & Fakher, A. (2014). Role of information technology (IT) in business management: An overview. *International Journal of Management, IT and Engineering*, *4*(9), 48–56.

AlMedires, M. & AlMaiah, M. (2021). Cybersecurity in Industrial Control System (ICS). *2021 International Conference on Information Technology (ICIT)*, 640–647. https://doi.org/10.1109/ICIT52682.2021.9491741

Anderson, E. E. & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security*, *27*(1), 22–29. https://doi.org/10.1016/j.cose.2008.03.002

Beerman, J., Berent, D., Falter, Z. & Bhunia, S. (2023). A review of colonial pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15.

Bound, W. A. J. (1988). Discussing security with top management. *Computers & Security*, *7*(2), 129–130. https://doi.org/10.1016/0167-4048(88)90323-9

Boyes, H., Hallaq, B., Cunningham, J. & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, 1–12.

Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, *388*(1–29), 3.

Cleveland, S. & Cleveland, M. (2018). Toward cybersecurity leadership framework. *Proceedings of the Thirteenth Midwest Association for Information Systems Conference*.

Daneels, A. & Salter, W. (1999). *What is SCADA?*

Derrick Huang, C., Hu, Q. & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, *114*(2), 793–804. https://doi.org/10.1016/j.ijpe.2008.04.002

Dewett, T. & Jones, G. R. (2001). The role of information technology in the organization: a review, model, and assessment. *Journal of management*, *27*(3), 313–346.

Etteplan. (2023). *Etteplan has applied for the certification of IEC 62443-4-1 Secure Product Development Lifecycle process with CertX*. Etteplan. https://www.etteplan.com/about-us/news/2023/08/15/etteplan-has-applied-for-the-certification-of-iec-62443-4-1-secure-product-development-lifecycle-process-with-certx/

EUR-Lex. (14.12.2022). *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (ETA:n kannalta merkityksellinen teksti)*. http://data.europa.eu/eli/dir/2022/2555/oj/fin

EUR-Lex. (14.6.2023). *Asetus - 2023/1230 - FI - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2023/1230/oj?locale=fi

European Commission. (15.9.2022). *Cyber Resilience Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Firoozjaei, M. D., Mahmoudyar, N., Baseri, Y. & Ghorbani, A. A. (2022). An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection*, *36*, 100487.

Fleckenstein, M. & Fellows, L. (2018). Data Security. Teoksessa M. Fleckenstein & L. Fellows (toim.), *Modern Data Strategy* (s. 165–177). Springer International Publishing. https://doi.org/10.1007/978-3-319-68993-7_15

Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Hirsjärvi, kirjoittaja, Sirkka & Hurme, kirjoittaja, Helena. (2022). *Tutkimushaastattelu : teemahaastattelun teoria ja käytäntö* ([2. painos]). Gaudeamus. https://www.ellibslibrary.com/jyu/9789523458123

Hitachi. (2024). *Certificates | Hitachi Energy*. https://www.hitachienergy.com/products-and-solutions/cybersecurity/certificates

Hohenegger, A., Krummeck, G., Baños, J., Ortega, A., Hager, M., Sterba, J., Kertis, T., Novobilsky, P., Prochazka, J., Caracuel, B., & others. (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.

Hsu, C.-C., Tsaih, R.-H. & Yen, D. C. (2018). The evolving role of IT departments in digital transformation. *Sustainability*, *10*(10), 3706.

Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems*, *6*(1), 15–18.

IECEE. (2024a). *About us*. https://www.iecee.org/who-we-are/about-us

IECEE. (2024b). *CB scheme*. https://www.iecee.org/who-we-are/cb-scheme

Industrial Internet Consortium. (2019). *The Industrial Internet of Things Volume G1: Reference Architecture*. https://api.semanticscholar.org/CorpusID:208051025

Insta. (2024). valmet-and-intopalo-digital-cybersecurity-experts-created-a-certified-secure-product-development-process/. https://www.insta.fi/en/news-and-events/valmet-and-intopalo-digital-cybersecurity-experts-created-a-certified-secure-product-development-process/

International Society of Automation. (2020). *An Overview of ISA/IEC 62443 Standards*. https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

Ioannidis, C., Pym, D. & Williams, J. (2013). Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach. Teoksessa B. Schneier (toim.), *Economics of Information Security and Privacy III* (s. 171–191). Springer. https://doi.org/10.1007/978-1-4614-1981-5_8

ISA, I. society of automation. (23.1.2024). *ISA/IEC 62443 Series of Standards*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

ISA/IEC. (2009). *IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*. *1.0*.

ISA/IEC. (2010). *IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*.

ISA/IEC. (2013). *IEC TR 62443-3-1:2013 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*.

ISA/IEC. (2015). *IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment*.

ISA/IEC. (2018). *IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*.

ISA/IEC. (2019a). *IEC 62443-3-3:2019 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*.

ISA/IEC. (2019b). *IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*.

ISA/IEC. (2020). *IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*.

ISA/IEC. (2023a). *IEC 62443-2-4:2023 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*. *2.0*, 194.

ISA/IEC. (2023b). *IEC TS 62443-1-5:2023 Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles*.

ISASecure. (2024). *Secure and Certify Your Products to ISA/IEC 62443*. https://isasecure.org/certification/get-certified

Jelacic, B., Lendak, I., Stoja, S., Stanojevic, M. & Rosic, D. (2020). Security risk assessment-based cloud migration methodology for smart grid OT services. *Acta Polytechnica Hungarica*, *17*(5), 113–134.

Johnston, A. C. & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Jouini, M., Rabai, L. B. A. & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496.

Kalmar. (2023). *Kalmar becomes first ports and terminals industry solution provider to receive cyber security certification for its automation system for all terminal equipment*. Cargotec. https://www.cargotec.com/en/nasdaq/trade-press-release-kalmar/2023/kalmar-becomes-first-ports-and-terminals-industry-solution-provider-to-receive-cyber-security-certification-for-its-automation-system-for-all-terminal-equipment/

Kim, S. & Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public administration review*, *66*(3), 370–385.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R. & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24–36. https://doi.org/10.1108/09685220610648355

Kone. (2023). *KONE to gain cybersecurity certifications for its DX class elevators and digital services*. https://www.kone.com/en/news-and-insights/releases/kone-to-gain-cybersecurity-certifications-for-its-dx-class-elevators-and-digital-services-2023-05-03.aspx

Kosutic, D. & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28–36.

Krotofil, M. & Gollmann, D. (2013). Industrial control systems security: What is happening? *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 670–675.

Lehto, M. & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139–148.

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C. & Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *Ieee Access*, *9*, 165295–165325.

Mansfield-Devine, S. (2019). The state of operational technology security. *Network security*, *2019*(10), 9–13.

Murray, G., Johnstone, M. N. & Valli, C. (2017). *The convergence of IT and OT in critical infrastructure*.

Neitzel, L. & Huba, B. (2014). Top ten differences between ICS and IT cybersecurity. *InTech*, *61*(3), 12–18.

Oppliger, R. (2007). IT security: In search of the holy grail. *Communications of the ACM*, *50*(2), 96–98.

Peltier, T. R. (2014). *Information Security Fundamentals*. Auerbach Publications; eBook Collection (EBSCOhost). https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=639918&site=ehost-live

Piggin, R. S. H. (2013). Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, 1–6. https://doi.org/10.1049/cp.2013.0001

Puusa, kirjoittaja, Anu, toimittaja, Juuti, kirjoittaja, Pauli, toimittaja & Aaltio, kirjoittaja, Iiris. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus. https://www.ellibslibrary.com/jyu/9789523456167

Qu, S. Q. & Dumay, J. (2011). The qualitative research interview. *Qualitative research in accounting & management*, *8*(3), 238–264.

Rhee, H.-S., Ryu, Y. U. & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Saint-Germain, R. & others. (2005). Information security management best practice based on ISO/IEC 17799. *INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE-*, *39*(4), 60.

Samonas, S. & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Sari, A., Lekidis, A. & Butun, I. (2020). Industrial networks and IIoT: Now and future trends. *Industrial IoT: Challenges, Design Principles, Applications, and Security*, 3–55.

Savaş, S. & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34.

Setola, R., Faramondi, L., Salzano, E., Cozzani, V., & others. (2019). An overview of cyber attack to industrial control system. *Chemical Engineering Transactions*, *77*, 907–912.

Singh, C. (2023). The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in By the Network and Information Security 2 (NIS2) Directive 2022/2555. *International Company and Commercial Law Review*, *5*, 251–261.

Sonkor, M. S. & García de Soto, B. (2021). Operational technology on construction sites: A review from the cybersecurity perspective. *Journal of Construction Engineering and Management*, *147*(12), 04021172.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V. & Lightman, S. (2022). Guide to operational technology (ot) security. *NIST Special Publication*, 800–882.

Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly*, 441–469.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information systems research*, *1*(3), 255–276.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586.

Tuomi, kirjoittaja, Jouni & Sarajärvi, kirjoittaja, Anneli. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos). Kustannusosakeyhtiö Tammi. https://www.ellibslibrary.com/jyu/9789520400118

Uchendu, B., Nurse, J. R., Bada, M. & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

Unver, H. O. (2013). An ISA-95-based manufacturing intelligence system in support of lean initiatives. *The International Journal of Advanced Manufacturing Technology*, *65*, 853–866.

Valmet. (2024). *Cybersecurity - Valmet DNA*. https://www.valmet.com/automation/control-systems/dna/cybersecurity/

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Wagter, R., Van Den Berg, M., Luijpers, J. & Van Steenbergen, M. (2005). *Dynamic enterprise architecture: how to make it work*. Wiley.

Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in industry*, *24*(2–3), 141–158.

WithSecure. (2019). *WithSecure security engineering awarded IEC 62443 certifications*. https://www.withsecure.com/en/whats-new/pressroom/withsecure-security-engineering-awarded-iec-62443-certifications

Wärtsilä. (2020). *Wärtsilä receives first in the industry IEC 62443 Cybersecurity Certification for its GEMS hybrid energy storage technology*. Wartsila.Com. https://www.wartsila.com/media/news/27-02-2020-wartsila-receives-first-in-the-industry-iec-62443-cybersecurity-certification-for-its-gems-hybrid-energy-storage-technology-3383473