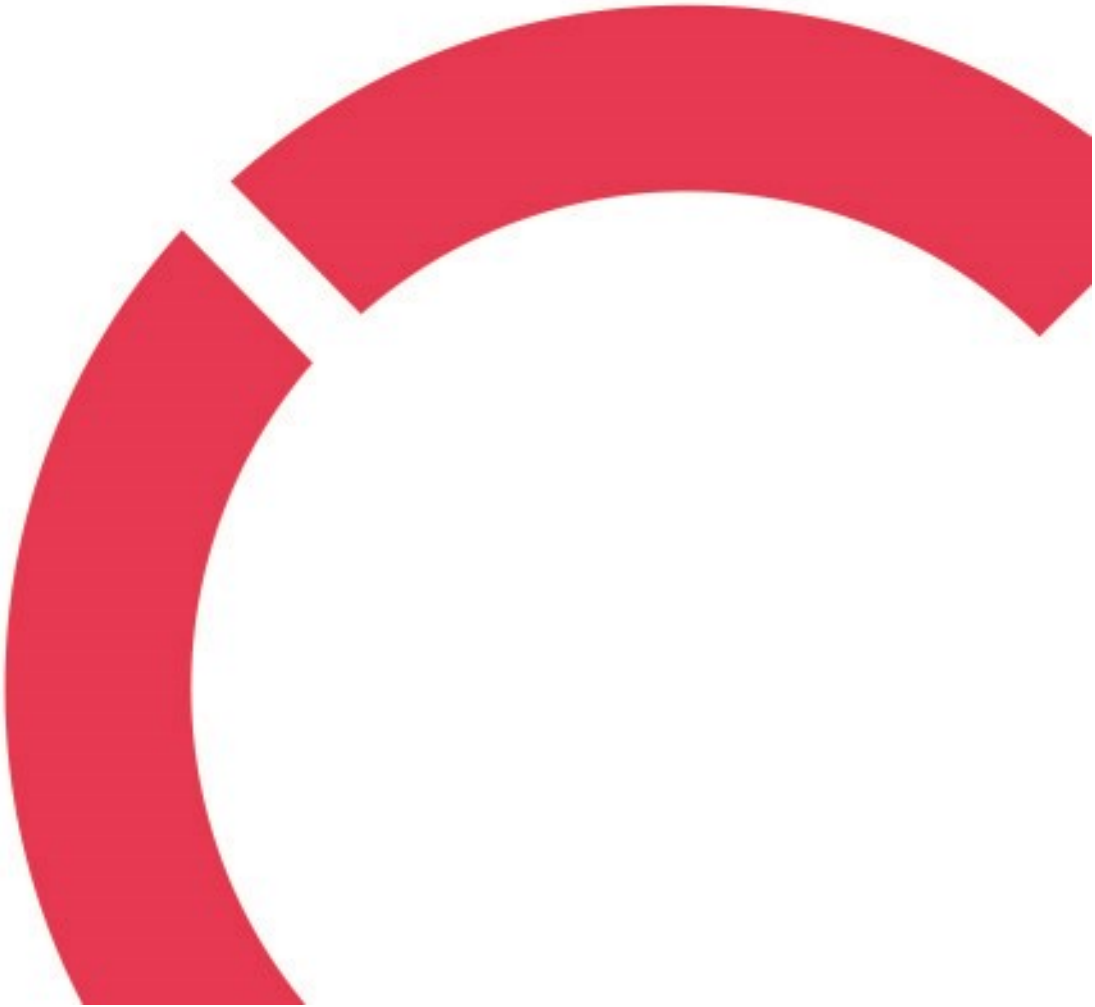
Marjo Hanhikoski

ISA/IEC 62443-4-1 STANDARDI

Turvallisen tuotekehityksen elinkaari

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Huhtikuu 2024



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Huhtikuu 2024	**Tekijä/tekijät** Marjo Hanhikoski
Koulutus Insinööri (AMK), tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi ISA/IEC 62443-4-1 STANDARDI. Turvallisen tuotekehityksen elinkaari		
Työn ohjaaja Henry Paananen		**Sivumäärä** 53 + 1
Työelämäohjaaja Joni Jämsä		

Kyber- ja tietoturvallisuus ovat osa jokapäiväistä elämää ja niiden rooli yhteiskunnalle kriittisten järjestelmien ja toimintojen turvallisuudessa on merkittävä. Täten kyber- ja tietoturvallisuus onkin syytä huomioida tuotekehitysprosessin varhaisessa vaiheessa. Turvallisen tuotekehityksen elinkaari on viitekehys, jossa tietoturvallisuus rakennetaan osaksi tuotteen ominaisuuksia. Kehitysprosessi sisältää turvallisuusvaatimukset, turvallisen suunnittelun ja toteutuksen, verifioinnin ja validoinnin, vika- ja korjaushallinnan sekä tuotteen elinkaaren lopun. Lisäksi viitekehyksessä huomioidaan sitä tukevat toiminnot.

ISA/IEC 62443 -standardikokoelma käsittää teollisuusautomaatio- ja ohjausjärjestelmien koko elinkaaren aikaisen tietoturvan ja sen tavoitteena onkin lisätä niiden turvallisuutta, luotettavuutta ja eheyttä elinkaaren aikana. Näiden järjestelmien kehittyminen eristyneistä verkoista standardeihin perustuviksi verkoiksi on lisännyt niiden uhkien määrää ja niihin kohdistuvien kyberhyökkäysten todennäköisyyttä.

Standardikokoelman osa 4-1 määrittelee turvallisen tuotekehityksen elinkaariprosessin vaatimukset teollisuusautomaatio- ja ohjausjärjestelmissä käytettäville tuotteille. Tuotetoimittaja voi soveltaa standardin vaatimuksia olemassa oleviin tai uusiin elinkaariprosesseihin olemassa olevassa tai uudessa tuotteessa. Standardin tarkoituksena onkin tarjota turvallisen suunnittelun ja syväsuojauksen viitekehys, jota tuotetoimittaja voi soveltaa tuotteeseensa. Standardi jakaantuu kahdeksaan turvallisuuskäytäntöön ja niiden sisältämiin vaatimuksiin.

Opinnäytetyöprosessin aikana tutustuttiin turvallisen kehittämisen elinkaareen, ISA/IEC 62443 -standardikokoelmaan ja erityisesti standardiin 4-1. Prosessin aikana tultiin siihen tulokseen, että standardin 4-1 käyttöönotto voidaan tiivistää vaiheisiin: suunnittele, toteuta, verifioi ja validoi sekä ylläpidä ja kehitä. Vaatimusten integrointi vaatii resursseja ja aikaa perehtyä standardiin ja sen soveltamiseen käytännössä. Lisäksi vaaditaan ymmärrystä, mihin standardin käyttöönotolla pyritään ja mitä sen käyttöönotolta toivotaan. Opinnäytetyössä pyrittiin antamaan kokonaiskuva turvallisen kehityksen elinkaaresta, 4-1 standardista ja antamaan näkökohtia standardin käyttöönotosta. Työn motiivina oli tarjota organisaatioille kattava kuvaus aiheesta ja toimia ensiaskeleena standardin käyttöönotolle.

Asiasanat
ISA/IEC 62443, ISA/IEC 62443-4-1, kyberturvallisuus, syväsuojaus, tietoturva, turvallinen suunnittelu, turvallisen kehityksen elinkaari, turvallisen tuotekehityksen elinkaari

ABSTRACT

Centria University of Applied Sciences	**Date** April 2024	**Author** Marjo Hanhikoski
Degree programme Bachelor of Engineering, Information and Communications technology		
Name of thesis ISA/IEC 62443-4-1 STANDARD. Secure product development lifecycle		
Centria supervisor Henry Paananen		**Pages** 53 + 1
Instructor representing commissioning institution or company Joni Jämsä		

Cyber and information security are part of everyday life and their role in the security of critical systems and functions to society is significant. Thus, cyber and information security should be considered at an early stage of product development. The secure product development lifecycle is a framework in which information security is built into the product's features. The development process includes secure requirements, secure design and implementation, verification and validation, defect and repair management, and the product's end of life. In addition, the framework must consider the functions that support the secure development lifecycle process.

The ISA/IEC 62443 series of standards covers the information security of industrial automation and control systems throughout the entire lifecycle and the goal is to increase their security, reliability, and integrity during the lifecycle. The evolution of these systems from isolated networks to standards-based networks has increased the number of threats they face and the probability of cyber attacks against them.

Part 4-1 of the series of standards defines the requirements of the secure product development lifecycle process for products used in industrial automation and control systems. The product supplier can apply the requirements of the standard to existing or new lifecycle processes in an existing or new product. The purpose of the standard is to provide a secure design and defense-in-depth framework, which product supplier can apply to their product. The standard is divided into eight security practices and the requirements they contain.

During the thesis process, the secure development lifecycle, the ISA/IEC 62443 series of standards and especially the standard 4-1 were introduced. It was concluded that the implementation of the standard 4-1 can be summarized into phases: planning, implementing, verifying and validating, and maintaining and developing. The integration of requirements requires resources and time to familiarize with the standard and its application in practice. In addition, an understanding is required of what the implementation of the standard aims at and what is expected from its implementation. The thesis aimed to give an overall picture of secure development lifecycle, the 4-1 standard and to give aspects of the implementation of the standard. The objective of the thesis was therefore to provide organizations with a comprehensive description of the subject and act as the first step for the implementation of the standard.

Key words
Cyber security, defense-in-depth, information security, ISA/IEC 62443, ISA/IEC 62443-4-1, secure design, secure development lifecycle, secure product development lifecycle

KÄSITTEIDEN MÄÄRITTELY

CMMI-DEV

(Capability Maturity Model Integration for Development) CMMI-DEV on tuotekehityksen kypsyysmalli, jota tuotekehittäjäorganisaatiot voivat käyttää suunnittelu- ja kehitysprosessin parantamiseen.

CVSS

(Common Vulnerability Scoring System) CVSS on pisteytysjärjestelmä, jonka avulla voidaan arvioida ja luokitella haavoittuvuuksien vakavuutta.

Digitaalinen allekirjoitus

(Digital signature) Digitaalista allekirjoitusta käytetään vahvistamaan viestin, ohjelmiston tai dokumentin aitous ja eheys. Se on matemaattinen tekniikka.

Haavoittuvuus

(Vulnerability) Haavoittuvuus on jokin heikkous esim. järjestelmässä, jota voidaan hyödyntää vahingontekoon.

Hyökkäysvektori

(Attack vector) Hyökkäysvektori on väline, jota käyttämällä on mahdollista hyökätä tietojärjestelmään tai -verkkoon. Hyökkäysvektorin toiminta perustuu haavoittuvuuksien hyödyntämiseen. Hyökkäysvektorina voi toimia esim. haittaohjelma, ponnahdusikkuna, verkkosivut tai sähköpostin liitetiedosto.

IACS

(Industrial Automation and Control System) Teollisuusautomaatio- ja ohjausjärjestelmä

IEC

(International Electrotechnical Commission) Sähköalan maailmanlaajuinen standardointijärjestö

IEC TC65/WG 10

(IEC Technical Committee 65 / Working Group 10) Technical Committee 65 on IEC:n alainen komitea, joka valmistelee kansainvälisiä standardeja teollisuuden prosessien mittaukseen, ohjaukseen ja automaatioon käytettäville järjestelmille ja elementeille. Komitean tehtävänä on myös koordinoida standardointitoimia, jotka vaikuttavat komponenttien ja toimintojen integrointiin edellä mainittuihin järjestelmiin

sisältäen turvallisuusnäkökulmat. Working Group 10 vastaa teollisuusprosessien mittauksen ja ohjauksen turvallisuudesta (verkko- ja järjestelmäturvallisuus).

ISA

(International Society of Automation) Teollisuusautomaation insinöörien, teknikkojen ja johdon voittoa tavoittelematon kansainvälinen ammattiyhdistys

ISA99-komitea

(ISA99 Committee) ISA99-komitea on ISA:n alainen asiantuntijoista koostuva komitea, joka vastaa standardien kehittämisestä koko teollisuusalalle ja kriittisille infrastruktuureille.

ISO

(International Organization for Standardization) Kansainvälinen voittoa tavoittelematon standardoimisjärjestö

Koventaminen

(Hardening) Toimenpiteitä, joilla pyritään vähentämään haavoittuvuuksia minimoimalla hyökkäyspinta-alaa

Kryptografinen tiiviste

(Cryptographic hash) Kryptografinen tiiviste on kryptografinen arvo, jota käytetään digitaalisissa allekirjoituksissa ja tiedon eheyden varmistamisessa.

Luottamusraja

(Trust boundary) Luottamusrajatermiä käytetään tietotekniikassa ja -turvassa kuvaamaan rajaa, jossa joko tieto tai toiminta muuttaa luottamustasoaan. Termillä viitataan rajoihin, joiden sisällä järjestelmä luottaa kaikkiin sen alijärjestelmiin.

NIST

(National Institute of Standards and Technology) NIST on Yhdysvaltojen kauppaministeriön alainen virasto, joka edistää maan innovaatioita ja teollista kilpailukykyä edistämällä mittaustieteitä, standardeja ja teknologiaa.

OWASP

(Open Worldwide Application Security Project) OWASP on voittoa tavoittelematon ohjelmistojen turvallisuustta parantava säätiö, joka tarjoaa ohjeistuksia turvallisten sovellusten kehittämiseen, ylläpitoon ja hankintaan.

RACI-matriisi

RACI-matriisi on projektinhallinnan tehtävälista, jossa määritellään, mitä tehdään, kuka tekee ja mihin mennessä.

Regressio

Muutos tai päivitys aiheuttaa, että aikaisemmin toiminut ominaisuus lakkaa toimimasta tai aiheuttaa virheitä

Riski

Todennäköisyys, että haitallinen tapahtuma toteutuu ja siitä aiheutuvat seuraukset

SDL

(Secure Development Lifecycle) Turvallisen kehityksen elinkaari

STRIDE-viitekehys / STRIDE-malli

(Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) STRIDE-viitekehys on uhkamallinnuksen työkalu, jolla voidaan tunnistaa uhkia ja haavoittuvuuksia. STRIDE käyttää seuraavia kategorioita uhkien ja haavoittuvuuksien kategoriointiin: huijaaminen, peukalointi, kieltäminen, tietovuoto, palvelunesto ja oikeuksien väärentäminen.

Uhka

Haitallinen tapahtuma tai kehityskulku, jonka on mahdollista toteutua

Yksityinen avain

(Private key) Yksityinen avain on kryptografinen muuttuja, jota käytetään tietojen salaamiseen ja salauksen purkamiseen.

KUVIOT

TAULUKOT

1 JOHDANTO

Kyber- ja tietoturvallisuus ovat olennaisia osia jokapäiväistä elämää. "Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin." Se on tavoitetila, jossa yhden tai useamman digitaalisen tietojärjestelmän muodostamaa toimintaympäristön toimintaa turvataan ja jossa kyseiseen toimintaympäristöön voidaan luottaa. (Sanastokeskus TSK ry 2018, 21–22.) Tietoturva tarkoittaa erilaisia toimia, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. (Sanastokeskus TSK ry 2018, 15). Tietoturva kattaa kaikki tietomuodot aina digitaalisista tiedoista fyysisiin tietoihin ja niiden suojaamisen. Kyberturvallisuus kattaa laitteiden, verkkojen, järjestelmien, palveluiden ja tietojen suojaamisen kyberhyökkäyksiltä. (Cybersecurity & infrastructure security agency 2021; Galarita & Swanston 2024.)

Kyber- ja tietoturvallisuuden rooli yhteiskunnalle kriittisten järjestelmien ja toimintojen turvallisuudessa on merkittävä. Näin ollen kyber- ja tietoturvallisuus olisikin syytä huomioida jo varhaisessa vaiheessa, kun lähdetään kehittämään tuotteita, järjestelmiä ja palveluita. (Liikenne- ja viestintävirasto Traficom 2018, 6.) Turvallisen kehityksen elinkaari -ajattelumalli ohjaa ottamaan huomioon kyber- ja tietoturvallisuuden koko tuotteen, järjestelmän tai palvelun elinkaaren ajan aina määrittelystä poistoon asti. Ajattelumallin ehdoton hyöty on toimintavarmuuden parantuminen sekä tietomurtojen ja -vuotojen ennaltaehkäisy (Liikenne- ja viestintävirasto Traficom 2018, 6).

Teollisuusautomaatio- ja ohjausjärjestelmät ovat järjestelmiä, joita käytetään ohjaamaan ja valvomaan teollisuusprosesseja ja kriittisiä infrastruktuureja (IEC/TR 62443-3-1:fi 2013, 20). Teollisuusautomaatio- ja ohjausjärjestelmät ovat enemmän kuin niihin liittyvät teknologiat ja järjestelmät. Teollisuusautomaatio- ja ohjausjärjestelmien määritelmän mukaan ne määritellään kokoelmaksi henkilöstöä, laitteita, ohjelmistoja ja teollisuusprosessien toimintatapoja, jotka voivat vaikuttaa tai joilla voi olla vaikutus niiden turvalliseen ja luotettavaan toimintaan. (IEC/TS 62443-1-1:fi, 32; International Society of Automation 2023, 3–4.)

Teollisuusautomaatio- ja ohjausjärjestelmät ovat vuosien saatossa kehittyneet eristyneistä verkoista standardeihin perustuviksi verkoiksi. Lisääntynyt avoimuus ja erilaisten yhteistyötahojen sekä ulkoistamisen lisääntyminen ovat kasvattaneet uhkien määrää ja lisänneet kyberhyökkäysten todennäköisyyttä. Myös teknologian kehittyminen verkottuneempaan ja helpomman yhdistettävyyden suuntaan on lisän-

nyt alttiutta mahdollisille verkkotunkeutumisille. Ei pidä myöskään unohtaa ihmisten kasvavaa tietokonelukutaitoa, joka on lisännyt ihmisten kykyä hakkerointiin ja haavoittuvuuksien hyödyntämiseen. (IEC/TR 62443-3-1:fi 2013, 18, 40; IEC/TS 62443-1-1:fi 2012, 54.) Teollisuusautomaatio- ja ohjausjärjestelmien vaarantuminen voi vahingoittaa organisaation toimintaa ja aiheuttaa taloudellisia menetyksiä, mutta sillä voi olla myös vakavia seurauksia ihmisten ja ympäristön turvallisuudelle sekä kansalliselle turvallisuudelle. Myös lakisääteisten vaatimusten rikkominen on yksi vakavimmista seurauksista. (IEC/TS 62443-1-1:fi 2012, 52, 56; International Society of Automation 2024; Purpose and Scope of the ISA99 Committee 2023.)

Jotta asia ei jää epäselväksi, todettakoon, että teknologiakehitys ja lisääntynyt avoimuus sekä yhteistyö ovat myös positiivisia asioita, koska ne voivat olla hyväksi organisaation liiketoiminnalle. Menestyvä liiketoiminta vaatii kuitenkin myös kyber- ja tietoturvallisuuden huomioimista koko organisaation toiminnassa aina organisaation johtamiskäytännöistä tuotekehitykseen. Organisaation panostukset kyber- ja tietoturvaan ovat panostusta kannattavaan liiketoimintaan, koska asiakkaiden luottamus organisaatioon on yksi menestyksen avaimista. Näin ollen teollisuusautomaatio- ja ohjausjärjestelmien kyber- ja tietoturva on otettava huomioon tuotteen tai järjestelmän koko elinkaaren ajan. Kyber- ja tietoturvallisuuden ylläpitäminen ja kehittäminen ovat jatkuvia prosesseja, joilla ei ole loppumispäivämäärää. Haavoittuvuudet, uhat ja riskit muuttuvat ajan saatossa, joten kyber- ja tietoturvallisuuden takaamiseksi tarvitaan jatkuvaa kehittämistyötä. (IEC/TS 62443-1-1:fi 2012, 76.)

Tässä työssä käsitellään turvallisen tuotekehityksen elinkaarta ja siihen liittyvää teollisuusautomaatio- ja ohjausjärjestelmiin liittyvien tuotteiden kansainvälistä standardia ISA/IEC 62443-4-1. Työssä käydään ensin läpi yleisesti turvallisen tuotekehityksen elinkaarta ja ISA/IEC 62443 -standardikokoelman rakennetta. Tämän jälkeen työssä käydään läpi yksityiskohtaisemmin standardikokoelman osa 4-1 eli turvallisen tuotekehityksen elinkaaren standardi. Lopuksi tuodaan esille käytännön näkökulmia standardin käyttöönotosta. Tiedonhaun perusteella ilmeni, että turvallisen tuotekehityksen standardista ei ole toteutettu yleiskattavaa opinnäytetyötä, maisterityötä tmv., jossa standardi käytäisiin perusteellisesti läpi ja tarjottaisiin käytännön näkökulmia koko standardin käyttöönotosta. Näin ollen työn tarkoituksena on antaa kokonaiskuva turvallisen tuotekehityksen elinkaaresta, ISA/IEC 62443-4-1 standardista ja antaa käytännönvinkkejä sen käyttöönotosta. Tämän työn motiivina on tarjota standardista kiinnostuneille organisaatioille kokonaiskuva turvallisen tuotekehityksen elinkaaresta ja ISA/IEC 624433-4-1 standardista ja täten toimia alkusysäyksenä standardin käyttöönotolle. Standardin käyttöönotolla organisaatiot voivat parantaa tuotteidensa tietoturvaa, parantaa siten tuotteensa ja tuotekehitysprosessinsa laatua sekä tehostaa toimintaansa, mitkä puolestansa lisäävät niiden kilpailuetua ja tuovat taloudellista hyötyä.

2 TURVALLISEN KEHITYKSEN ELINKAARI

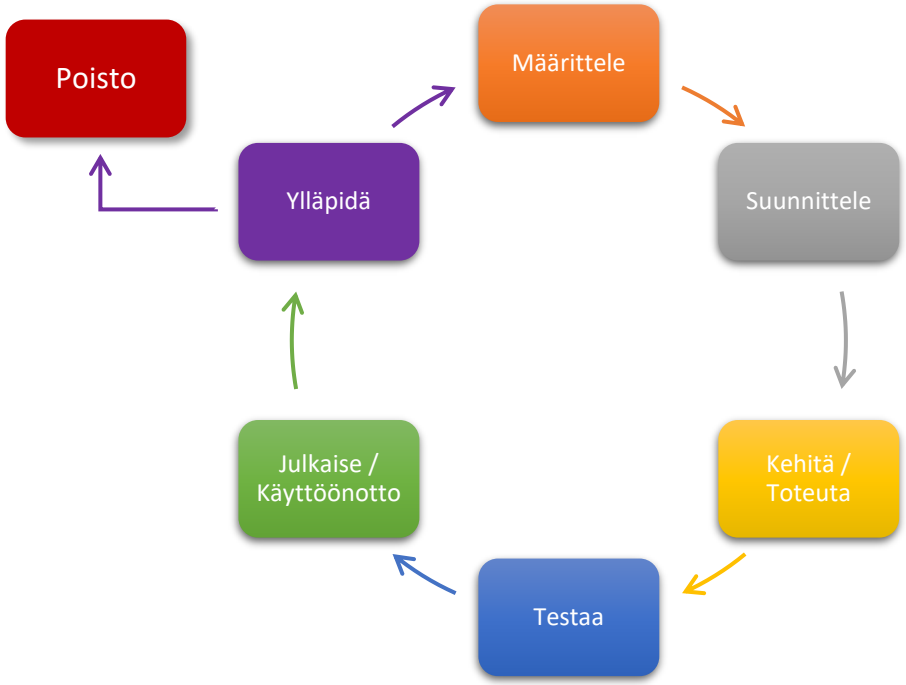
Turvallisen kehityksen elinkaari (Secure Development Lifecycle (SDL)) on viitekehys, jossa tietoturvallisuus rakennetaan osaksi tuotetta aina sen määrittelystä käytöstä poistoon. Lisäksi viitekehyksessä huomioidaan mm. myös organisaation yleinen tietoturvapolitiikka, ihmiset ja tilat kuin myös tuotteen ylläpitotoiminnot. Turvallisen kehityksen elinkaari -viitekehys asettaa tietoturvan keskeiseksi osaksi tuotekehitysprosessia ja mahdollistaa toistettavissa olevan prosessimallin, joka lisää varmuutta tuottaa turvallisia tuotteita. (Gupta ym. 2007; Cyber Security - Secure Development Lifecycle 2021; Liikenne- ja viestintävirasto Traficom 2018; Lipner 2004.) Kun turvallisuus otetaan huomioon kehitysprosessin alusta lähtien, voidaan kehittää tuote, jossa turvallisuus on kiinteä osa tuotteen ominaisuuksia (Liikenne- ja viestintävirasto Traficom 2018, 16; Lipner 2004).

Turvallisen kehityksen elinkaari -viitekehyksen tarkoituksena on vähentää tietoturvahaavoittuvuuksien todennäköisyyttä (The Security Development Lifecycle (SDL) Explained 2016). Tiedonhaun tuloksena kyseisellä termillä tuli vastaan pääsääntöisesti termi Secure Software Development Lifecycle (SSDL) eli turvallisen ohjelmistokehityksen elinkaari. Pääasiallisesti turvallisen kehityksen elinkaari -viitekehys keskittyikin nimenomaan ohjelmistokehitykseen, mutta myöhemmin huomattiin, varsinkin ISA/IEC 62443-4-1 standardin myötä, että malli on sovellettavissa myös laitteiston kehitykseen (The Security Development Lifecycle (SDL) Explained 2016). Turvallisen tuotekehityksen elinkaari -viitekehys soveltuu siis ohjelmistojen, laiteohjelmistojen ja laitteiden turvallisen tuotekehityksen viitekehykseksi ja sitä voidaankin soveltaa kaikenlaisessa tuotekehityksessä tietoturvahaavoittuvuuksien löytämiseksi ja lisäämään tuotteiden resilienssiä nopeasti kehittyvässä turvallisuusuhkien maailmassa (Dorsey 2020).

Turvallisen kehityksen elinkaaren edelläkävijänä pidetään Microsoftia (The Security Development Lifecycle (SDL) Explained 2016). 2000-luvun alussa tietokoneet ja Internetin käyttö yleistyivät, jonka myötä myös haittaohjelmat lisääntyivät. Vuonna 2002 Microsoft käynnisti hankkeen, jonka tarkoituksena oli varmistaa heidän tuotteidensa ja palveluidensa turvallisuus, saavutettavuus ja luotettavuus. Tämän tuloksena syntyi Microsoftin Security Development Lifecycle -viitekehys, joka liitettiin olennaiseksi ja pakolliseksi osaksi Microsoftin ohjelmistokehitystä vuonna 2004. (Microsoft 2024a.) Microsoftin käyttöönottama viitekehys perustuu SD^3 + C -periaatteisiin, joita se noudattaa. Nämä periaatteet ovat turvallinen suunnittelu (Secure by Design), turvallisuus oletusarvoisesti (Secure by Default), käyttöönoton turvallisuus (Secure in Deployment) ja viestintä (Communications). (Lipner 2004.)

Microsoftin periaatteiden mukaan turvallisessa suunnittelussa turvallisuus huomioidaan tuotteen suunnittelu- ja toteutusvaiheessa, jolloin tuote itsessään on kykenevä suojaamaan itseään ja vastustamaan hyökkäyksiä. Tuotteen oletusarvoinen turvallisuus taas viittaa, että tuote edistää oletusarvoisesti omaa turvallisuuttaan. Käytännössä tämä tarkoittaa, että esim. ei-välttämättömät ominaisuudet ovat oletusarvoisesti kytketty pois päältä ja tuotteen toiminta vaatii mahdollisimman suppeat käyttöoikeudet. Näillä kahdella periaatteella on suurin vaikutus tuotteen turvallisuuteen. Turvallisen suunnittelun lähtökohtana on estää haavoittuvuuksia ja oletusarvoisen turvallisuuden on tarkoitus minimoida tuotteen hyökkäyspinta-alaa. Lisäksi käyttäjille on tarjottava riittävästi tietoa tuotteen turvalliseen käyttöön ja päivitysten käyttöönottoon sekä informoida heitä ilmenneistä haavoittuvuuksista ja tarvittavista suojaustoimenpiteistä. (Lipner 2004.)

Turvallisen kehityksen elinkaaren mallia määriteltäessä selvitys- ja vertailutyön tulokseksi saatiin erilaisia kuviomalleja, joilla kehityskulkua voidaan kuvata, esim. Gupta ym., Lipner ja Microsoft esittivät omissa julkaisuissa turvallisen kehityksen elinkaaren mallin (Gupta ym. 2007, 22; Lipner 2004; Microsoft 2023). Kuvioiden sisältö vaihteli eri organisaatioilla toisistaan, mutta yhteenvetona voidaan todeta, että pääpiirteissään sisältö oli sama ja se kytkeytyi vahvasti ohjelmistokehityksen elinkaarimalliin. Selvitys- ja vertailutyön tuloksena turvallisen kehityksen elinkaarimallin pohjaksi valikoituivat lähteet Gupta ym., Lipner, Microsoft, Traficom ja ISA/IEC 62443-4-1 standardi. Tutkittuani näitä lähteitä yhteenvedoksi saatiin kuvion 1 kaltainen turvallisen kehityksen elinkaari -malli. Lisäksi mallin ulkopuolelle jäävät kehitysmallia tukevat toiminnot eli esim. tietoturvapolitiikka, henkilöstö ja tilat (Gupta ym. 2007, 34–36; Liikenne- ja viestintävirasto Traficom 2018, 12–13). Seuraavaksi käydään lyhyesti läpi, mitä tuotteen turvallisuuteen tähtääviä toimia jokainen turvallisen kehityksen elinkaari -mallin vaihe sisältää.



KUVIO 1. Turvallisen kehityksen elinkaari (mukaillen Gupta ym. 2007, 22; Lipner 2004; Microsoft 2023)

Määrittelyvaiheessa määritellään tulevan tuotteen vaatimukset. Turvallisessa tuotekehityksessä tämä tarkoittaa, että määrittelyvaiheessa määritellään myös tulevan tuotteen turvallisuusvaatimukset mukaan lukien tietosuojavaatimukset. Turvallisuusvaatimukset määrittelevät suojaustoimenpiteet, joilla voidaan suojata tuotteen tietoja ja palveluita haitallisilta toimijoilta ja muilta vastoinkäymisiltä. Vaatimukset voivat olla toiminnallisia, kuten kirjautuminen käyttäjätunnuksella ja salasanalla, tai ei-toiminnallisia, kuten verkon kautta saapuvien syötteiden tarkistus. Toimivien turvallisuusvaatimusten laatiminen vaatii, että tiedetään, miten tuotetta ja minkälaisessa ympäristössä sitä käytetään sekä minkälaista dataa se käsittelee. Toisin sanoen on ymmärrettävä tuotteen käyttötarkoitus. Lisäksi turvallisuusvaatimusmäärittelyssä on huomioitava tunnetut uhat, oman alan säädökset ja vaatimukset sekä mahdolliset aikaisemmat kokemukset sattuneista tapauksista. (Liikenne- ja viestintävirasto Traficom 2018, 7, 14–15; Microsoft 2023.)

Lisäksi määrittelyssä huomioidaan, mikäli tuotteessa käytetään kolmannen osapuolen komponentteja, että näille kyseisille komponenteille toteutetaan tarvittavat turvallisuusarvioinnit ja otetaan huomioon mahdolliset lisenssit (Dorsey 2020; Liikenne- ja viestintävirasto Traficom 2018, 27–28). Näin voidaan välttää, että komponenttien mahdollisesti tuomat haavoittuvuudet on huomioitu ja käsitelty eikä tuotteelle jouduta toteuttamaan suurempia korjaustoimenpiteitä takautuvasti, mitkä voivat olla aikaa vieviä, hankalia ja kalliita toteuttaa. (Dorsey 2020.) Turvalliseen kehittämiseen kuuluukin, että erilaisten komponenttien käyttöön hyväksymisestä on tehty selkeät ja sovitut käytännöt tai prosessit. (Liikenne- ja

viestintävirasto Traficom 2018, 27–28.) Kun tuotetta koskeva määrittelytyö on tehty, turvallisuusvaatimukset dokumentoidaan ja niitä seurataan sekä päivitetään tuotteen elinkaaren aikana (Liikenne- ja viestintävirasto Traficom 2018, 7, 14–15; Microsoft 2023).

Suunnitteluvaiheessa suunnitellaan tuotteen rakenne eli arkkitehtuuri turvallisen suunnittelun periaatteiden mukaisesti. Vuonna 2021 OWASP on listannut turvattoman suunnittelun neljänneksi yleisimmäksi syyksi sovellusturvallisuuden riskeistä (OWASP Foundation 2021). Turvallisen suunnittelun periaatteita ovat

- hyökkäyspinta-alan minimoiminen,
- turvalliset oletusasetukset,
- syötteenkäsittely,
- erilliset tehtävät,
- mahdollisimman suppeat valtuudet,
- syväsuojaus,
- salassapitoon perustuvan turvallisuuden välttäminen,
- sokean luottamuksen välttäminen kolmannen osapuolen palveluihin tai tuotteisiin,
- turvallisuus vikatilanteissa,
- turvallisuusongelmien korjaaminen oikein ja
- tuotteen rakenteen pitäminen yksinkertaisena eli liian monimutkaisten ratkaisujen välttäminen.

(Liikenne- ja viestintävirasto Traficom 2018, 19–26; OWASP Foundation 2006.)

Osana suunnitteluvaihetta toteutetaan myös uhkamallinnus, jossa arvioidaan tulevan tuotteen turvallisuutta huomioiden kaikki tuotteen sisältämät komponentit (Liikenne- ja viestintävirasto Traficom 2018, 16; Microsoft 2023). Uhkamallinnuksessa pyritään tunnistamaan mahdolliset tuotteeseen kohdistuvat nykyiset ja tulevaisuuden uhat sekä arvioimaan niistä aiheutuvia riskejä ja pohtimaan, mitä toimenpiteitä voidaan tehdä, jotta näitä uhkia voidaan estää tai lieventää (Drake 2024; Microsoft 2023). Uhkamallinnus on suunniteltua toimintaa, jonka päämääränä on tunnistaa ja arvioida tuotteeseen kohdistuvia uhkia ja sen haavoittuvuuksia. Uhkamallinnus on syytä toteuttaa mahdollisimman varhaisessa vaiheessa tuotteen elinkaarta. (Drake 2024.) Mallinnusta on kuitenkin jalostettava ja päivitettävä tuotteen elinkaaren ajan. Käytännössä jokaiselle tuotteeseen lisättävälle uudelle ominaisuudelle tai komponentille on syytä

toteuttaa uhkamallinnus, tai uhkamallinnus on tehtävä tilanteessa, jossa tuotteen rakenteeseen tehdään merkittäviä muutoksia. (Drake 2024; Microsoft 2023.)

Kehittämis- ja toteutusvaiheessa aloitetaan tuotteen varsinainen toteuttaminen. Tuotteen turvallinen kehittäminen toteutetaan määrittely- ja suunnitteluvaiheessa tehtyjen vaatimusten sekä suunnitelmien mukaisesti (Microsoft 2023). Uhkamallinnuksen tietojen hyödyntäminen on myös olennainen osa toteutusvaihetta, koska se tarjoaa tietoa tuotteeseen kohdistuvista uhista, joita pyritään estämään tai lieventämään (Lipner 2004). Esimerkiksi ohjelmistotuotannossa suunnitelmat huomioidaan turvallisessa ohjelmoinnissa. Ensinnäkin valitaan turvalliset työvälineet turvallisen tuotteen aikaansaamiseksi ja kirjoitettua koodia tarkastellaan koodikatselmuksissa sekä suorittamalla staattisia analyyseja. (Liikenne- ja viestintävirasto Traficom 2018, 27; Microsoft 2023.) Samat toimintatavat pätevät myös laitteiston kehitykseen. Toteutusvaiheen aikana on huolehdittava, että toteutettu tuote vastaa suunnitelmaa ja että toiminnot toimivat suunnitellusti. (Dorsey 2020.)

Tärkeä kehittämisvaiheessa huomioitava asia on salaustoiminnot. Lähes kaikki järjestelmät ja tuotteet tarvitsevat salaustoimintoja, joiden avulla luottamuksellisia tietoja voidaan tallentaa tai lähettää turvallisesti. Suositeltavaa onkin välttää omatekoisten ratkaisujen tekemistä ja hyödyntää hyvin tunnettuja ja korkealaatuisia ratkaisuja sekä noudattaa standardeja ja parhaita käytäntöjä. Turvallisuuden kannalta on myös syytä perehtyä valittavan ratkaisun toimintaan, jotta ratkaisua voidaan käyttää oikein. (Liikenne- ja viestintävirasto Traficom 2018, 27.)

Kehitysvaiheen jälkeen siirrytään testausvaiheeseen, jossa tuotetta testataan ennen sen julkaisua ja käyttöönottoa. Testaus limittyy kehitysvaiheen kanssa, koska alustavaa testausta suoritetaan myös jo kehitys- ja toteutusvaiheen aikana. Turvallisen tuotekehityksen testausvaiheessa katsotaan, että tuote vastaa aikaisemmin asetettuja turvallisuusvaatimuksia, suunnitellut turvallisuustoiminnot toimivat odotetusti, onko olemassa jotain turvallisuusnäkökohtia, joita ei ole huomioitu, ja onko toteutuksen aikana ilmennyt uusia haavoittuvuuksia. Testaus sisältää niin manuaalisia kuin automatisoituja testauksia. (Gupta ym. 2007, 24; Liikenne- ja viestintävirasto Traficom 2018, 30–31; Microsoft 2023.) Tuotteelle suoritetaan tarvittavat testaukset, jotka dokumentoidaan. Tärkeimpiä testauksia ovat turvallisuusvaatimusten testaus, uhkien lievennysten testaus, haavoittuvuuksien testaus ja läpäisytestaus. (Dorsey 2020; IEC 62443-4-1:2018, 35–36.)

Turvallisen tuotekehityksen näkökulmasta hyväksymistestauksen suorittaa riippumaton testaustiimi tai kolmas osapuoli, joka ei ole ollut kehittämässä tuotetta. Ohjelmistotuotannossa tämä tarkoittaa henkilöitä, jotka eivät ole olleet mukana ohjelmiston koodauksessa. Mikäli tuotteesta löydetään vakavia puutteita, palautetaan tuote kehitystiimin korjattavaksi, jonka jälkeen voidaan joutua tekemään uudet hyväksymistestaukset. (Liikenne- ja viestintävirasto Traficom 2018, 30; Microsoft 2023.) Hyväksymistestauksessa vastataan kysymykseen, onko tuote valmis toimitettavaksi asiakkaille (Lipner 2004).

Kun tuote on läpäissyt hyväksymistestaukset hyväksytysti, se voidaan julkaista. Tuote myydään asiakkaalle ja se otetaan käyttöön. Käyttöönottovaiheessa tuotetoimittajan onkin varmistettava, että sen kehittämä tuote otetaan käyttöön turvallisesti ja sitä käytetään tarkoituksenmukaisella tavalla. Näin ollen käyttäjää täytyy opastaa tuotteen turvallisesta käyttöönotosta, käytöstä, ylläpidosta ja käytöstä poistosta. Ohjelmistotuotannossa järjestelmät asennetaan nykyisin joko verkon välityksellä tai harvemmin paikan päällä. Näin ollen täytyy varmistaa myös portaalipalvelimen turvallisuus ja käyttää salattuja verkkosivuja. Tuotetoimittajan on myös varmistuttava, että asiakas ei vahingossa asenna järjestelmää väärennetystä latausportaalista. Pilvisovellusten yleistyessä varsinaista asennusta ei tarvita lainkaan, koska sovellusta käytetään verkkoselaimella. (Liikenne- ja viestintävirasto Traficom 2018, 35–37.)

Tuotteen käyttöönoton jälkeen on todennäköistä, että siinä havaitaan ajan kuluessa jokin haavoittuvuus. Näin ollen turvallisen kehityksen elinkaaren näkökulmasta onkin huolehdittava tuotteen ylläpidosta. Kun tuotteessa havaitaan haavoittuvuus, on siihen reagoitava mahdollisimman nopeasti ja huolellisesti. Tuotetoimittajan onkin informoitava käyttäjiä ilmenneistä haavoittuvuuksista, korjaavista toimenpiteistä tai vastatoimista, ja huolehdittava, että haavoittuvuudet korjataan. Tuotteen ylläpidossa on syytä myös huomioida, että tuotteen version päivittäminen voi mitätöidä aikaisemmalle versiolle saadun hyväksynnän. Näin ollen näihin tilanteisiin on hyvä varautua ennakolta ja keskustella asiasta hyväksyjän kanssa. (Liikenne- ja viestintävirasto Traficom 2018, 36.)

Tuotteen saavuttaessa elinkaarensa loppupään on huolehdittava tuotteen turvallisesta poistosta. Näin ollen onkin mietittävä, mitä tuotteelle tapahtuu käytöstä poistamisen jälkeen. Jos tuote sisältää esim. levyjä, joille on tallennettu arkaluontoisia tietoja, on ne tuhottava asianmukaisesti. Turvallisen elinkaaren hallinta vaatii, että asiakkaita on opastettu asianmukaisesti myös käytöstä poistamiseen. (IEC 62443-4-1:2018, 46; Liikenne- ja viestintävirasto Traficom 2018, 35.)

Turvallisen kehityksen elinkaari -menetelmää hyödynnettäessä on huomioitava myös turvallista kehitystä tukevia toimia. Näitä toimia ovat kehittäjäorganisaation yleinen tietoturvapolitiikka, henkilöstöön

ja tiloihin liittyvät toimet (Gupta ym. 2007, 34; IEC/TR 62443-3-1:fi 2013, 158; Liikenne- ja viestintävirasto Traficom 2018, 12–13). Ensinnäkin organisaation yleisen tietoturvapolitiikan pitää tukea turvallista tuotekehitysprosessia. Tietoturvapolitiikka heijastaa organisaation johdon näkemyksiä tietoturvasta ja näin ollen sillä on vaikutusta myös organisaation tuotekehitysprosessiin. Tietoturvapolitiikka luo pohjan organisaation tietoturvalliselle toiminnalle. Tietoturvapolitiikka muuntaa johdon odotukset tietoturvatavoitteiksi, jotka ohjaavat tietoturvan toteutumista tuotekehityksen elinkaaren aikana. Näin ollen tietoturvapolitiikan tarkoituksena on tiivistää johdon odotukset koskien tuotteiden tietoturvaa, kuten tuotteen kehittäminen ja ylläpito sekä tuotteen turvallisuutta tukevat toiminnot. (Gupta ym. 2007, 34–35.)

Turvallisen tuotteen kehittäminen vaatii turvallisen kehitysympäristön. Työtilojen ja työvälineiden on oltava turvallisia, jotta voidaan vähentää mahdollisia hyökkäyksiä fyysisiin tiloihin ja verkon välityksellä tapahtuvia hyökkäyksiä, ja näin ollen pienentää riskiä tuotteen vaarantumisesta. Työtiloja on suojattava valtuuttamattomalta pääsyltä niin ulkoisten kuin sisäisten toimijoiden toimesta. Työtiloja voidaan suojata esim. kulunvalvonnalla ja työtilojen suunnitelulla. Käytettyjen työvälineiden on oltava turvallisia ja vastata kehitettävän tuotteen turvallisuusvaatimuksia, esim. huolehditaan työvälineiden säännöllisestä päivittämisestä. Lisäksi on huomioitava, että organisaation muut prosessit tukevat turvallista tuotekehitystä. (IEC/TR 62443-3-1:fi 2013, 158; Liikenne- ja viestintävirasto Traficom 2018, 12–13.)

Henkilöstön kohdalla tukevia toimia ovat selkeä työnkuva, perehdytys ja kouluttaminen. Työntekijän työnkuva määritellään selkeästi, jotta voidaan varmistua työntekijän riittävästä osaamisesta kyseiseen työtehtävään. Perehdytyksen on oltava riittävää vaadittuihin työtehtäviin. Henkilöstön olisi myös yleisesti oltava tietoisia tietoturvahygienian yleisistä periaatteista, kuten turvallisesta sähköpostin käytöstä, turvallisesta verkkoselaamisesta ja järjestelmän pitämisestä ajantasaisena. Lisäksi kehitystyössä olevalle henkilöstölle on tarjottava lisäkoulutusta turvallisesta suunnittelusta, uhkamallinnuksesta ja ohjelmointia tekeville turvallisen ohjelmoinnin periaatteista. Organisaation on myös varauduttava työntekijöiden vaihtuvuuteen siten, että uusille työntekijöille tarjotaan riittävä perehdytys ja koulutus tuleviin työtehtäviin liittyen. (Gupta ym. 2007, 35; IEC/TR 62443-3-1:fi 2013, 166; Liikenne- ja viestintävirasto Traficom 2018, 12; Lipner 2004; Microsoft 2023.)

Nykypäivän organisaatiot ovat tietoisempia kyberturvallisuudesta, tietoturvaan ja tietosuojaan liittyvistä asioista. Näin ollen vaatimukset tuotteiden ja palveluiden turvallisuudelle sekä laadulle ovat kasvaneet. Tietoturva nähdään yhtenä laatutekijänä ja se luo kilpailuetua. Turvallisen kehityksen elinkaari -viitekehys tuo taloudellisia hyötyjä mm. parantamalla tuotteiden turvallisuutta ja pienentämällä korjauksista

aiheutuvia kustannuksia sekä edesauttamalla liiketoiminnan jatkuvuutta. Yleisestikin menetelmä parantaa työn laatua ja siten myötävaikuttaa positiivisesti organisaation toimintaan. (Liikenne- ja viestintävirasto Traficom 2018, 7, 10.) Jälkikäteen toteutetut turvallisuustoimenpiteet eivät ole pitkäkestoisia, kattavia ja kustannustehokkaita ratkaisuja (Gupta ym. 2007, 22).

Monimutkaisten järjestelmien ja alati muuttuvan uhkamaiseman vuoksi on mahdotonta kehittää tuotetta, joka olisi täysin turvallinen (Dorsey 2020). Näin ollen organisaatioiden onkin panostettava turvalliseen tuotekehitykseen sekä kehitettävä ja parannettava näitä prosesseja, jotta tuotteen turvallisuus voidaan taata myös tulevaisuudessa. Monimutkaiset verkko- ja palvelurakenteet vaativat, että turvallisuus huomioidaan ja että turvallisuus on sisällytetty osaksi jokaista tuotteen komponenttia (Gupta ym. 2007, 22). Näin ollen turvallisuus onkin otettava olennaiseksi osaksi tuotteen ominaisuuksia, eikä sitä pidä pitää enää vain tuotteen toissijaisena ominaisuutena.

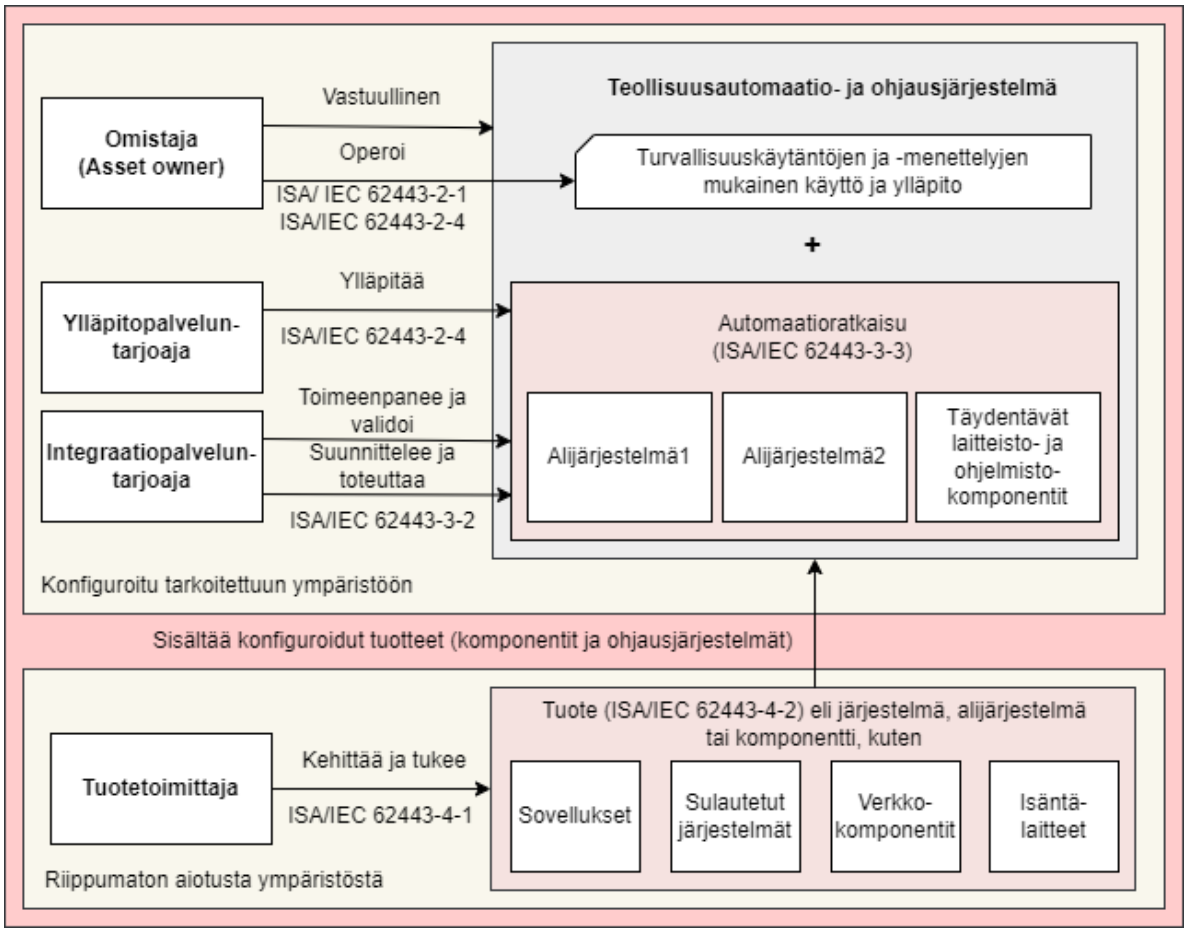
3 ISA/IEC 62443 -STANDARDIKOKOELMA

Standardikokoelmassa käsitellään teollisuusautomaatio- ja ohjausjärjestelmien (IACS) koko elinkaaren aikaista tietoturvaa. Standardikokoelman päivittämisestä ja ylläpidosta vastaa International Society of Automation (ISA) alainen ISA99-komitea yhdessä International Electrotechnical Commissionin (IEC) alaisen TC65/WG 10 -komitean kanssa. ISA99-komitea on kuitenkin standardikokoelman pääasiallinen kehittäjä. Organisaatioiden välille on solmittu yhteistyösopimus, joten riippumatta siitä, kumpi organisaatio toimii standardin julkaisijana, ovat molemmat standardit tekniseltä sisällöltään identtisiä (International Society of Automation 2023, 2, 4.) Standardikokoelma kehitettiin alun perin teollisuusprosesseja varten, mutta nykyisin kokoelmaa sovelletaan myös esim. kuljetusalalla, lääketieteellisissä laitteissa ja rakennusautomaatiossa. (International Society of Automation 2023, 2–3.) Kuten johdannossa jo todettiin, teollisuusautomaatio- ja ohjausjärjestelmien ja niiden käyttöympäristöjen kehittyminen vuosien kuluessa sekä monet muutkin seikat ovat johtaneet siihen, että kyber- ja tietoturvallisuudesta on tullut olennainen ominaisuus kyseisille järjestelmille.

Standardikokoelman tavoitteena onkin lisätä teollisuusautomaatio- ja ohjausjärjestelmien turvallisuutta, luotettavuutta ja eheyttä koko elinkaaren aikana. Standardikokoelmassa käydään läpi yleisiä ehtoja ja vaatimuksia, joita tuotteen omistaja, tuotetoimittaja tai palveluntuottaja voivat hyödyntää ohjausjärjestelmien ja niiden alaisten laitteiden turvallisuuden parantamiseksi. (International Society of Automation 2023, 2–3.) Standardikokoelma antaa kattavan viitekehyksen teollisuusautomaatio- ja ohjausjärjestelmien jo olemassa olevien ja tulevien tietoturva-aukkojen korjaamiseen ja minimoimiseen (International Society of Automation 2024). Tietotekniikan tietoturvallisuuden yleiset tavoitteet luottamuksellisuus, eheys ja saavutettavuus eivät ole kuitenkaan yksistään riittäviä, kun halutaan ymmärtää teollisuusautomaatio- ja ohjausjärjestelmien tietoturvaa. ISA/IEC 62443-1-1 spesifikaatiossa määritellään perusvaatimukset teollisuusautomaatio- ja ohjausjärjestelmien tietoturvalle. Näitä perusvaatimuksia ovat pääsyn valvonta, käytön valvonta, tiedon eheys, tiedon luottamuksellisuus, rajoitettu tiedon virtaus, nopea reagointi tapahtumaan ja resurssien saatavuus. (IEC/TS 62443-1-1:fi, 56, 58.)

Ennen standardikokoelmaan perehtymistä on myös syytä määritellä eri toimijoiden erilaiset roolit. Standardikokoelmassa puhutaan neljästä pääroolista, jotka ovat omistaja (asset owner), kunnossapitopalveluntarjoaja (maintenance service provider), integraatiopalveluntarjoaja (integration service provider) ja tuotetoimittaja (product supplier). Omistaja on organisaatio, joka on vastuussa teollisuusautomaatio- ja ohjausjärjestelmästä sekä on järjestelmän käyttäjä (ks. kuvio 2). Kunnossapitopalveluntarjoaja voi olla

henkilö tai organisaatio, joka tarjoaa automaatioratkaisun kunnossapitopalveluita (ks. kuvio 2). Integraatiopalveluntarjoaja on organisaatio, joka tarjoaa automaatioratkaisujen integrointipalveluita, kuten käyttöönotot, asennukset, konfiguroinnit ja testaukset (ks. kuvio 2). Tuotetoimittaja on organisaatio, joka valmistaa ja ylläpitää laitteisto- ja/tai ohjelmistotuotteita kuten sovellukset, verkkolaitteet, ohjausjärjestelmät ja sulautetut järjestelmät (ks. kuvio 2). Kuviossa 2 on esitetty yhteenveto eri roolien, tuotteiden, automaatioratkaisujen, automaatio- ja ohjausjärjestelmien sekä standardikokoelman eri standardiosien suhteesta toisiinsa. (IEC 62443-4-1:2018, 9–10; International Society of Automation 2023, 10.) Rooleissa on hyvä huomioida, että yhdellä organisaatiolla voi olla useita rooleja tai vastuut voivat olla jaettu useille organisaatioille. Esimerkiksi omistaja voi olla itse vastuussa myös kunnossapitopalveluista tai tuotetoimittaja voi tarjota integrointipalveluita. Omistaja on kuitenkin aina päävastuullinen. (ISA Global Cybersecurity Alliance 2020, 7–8.)

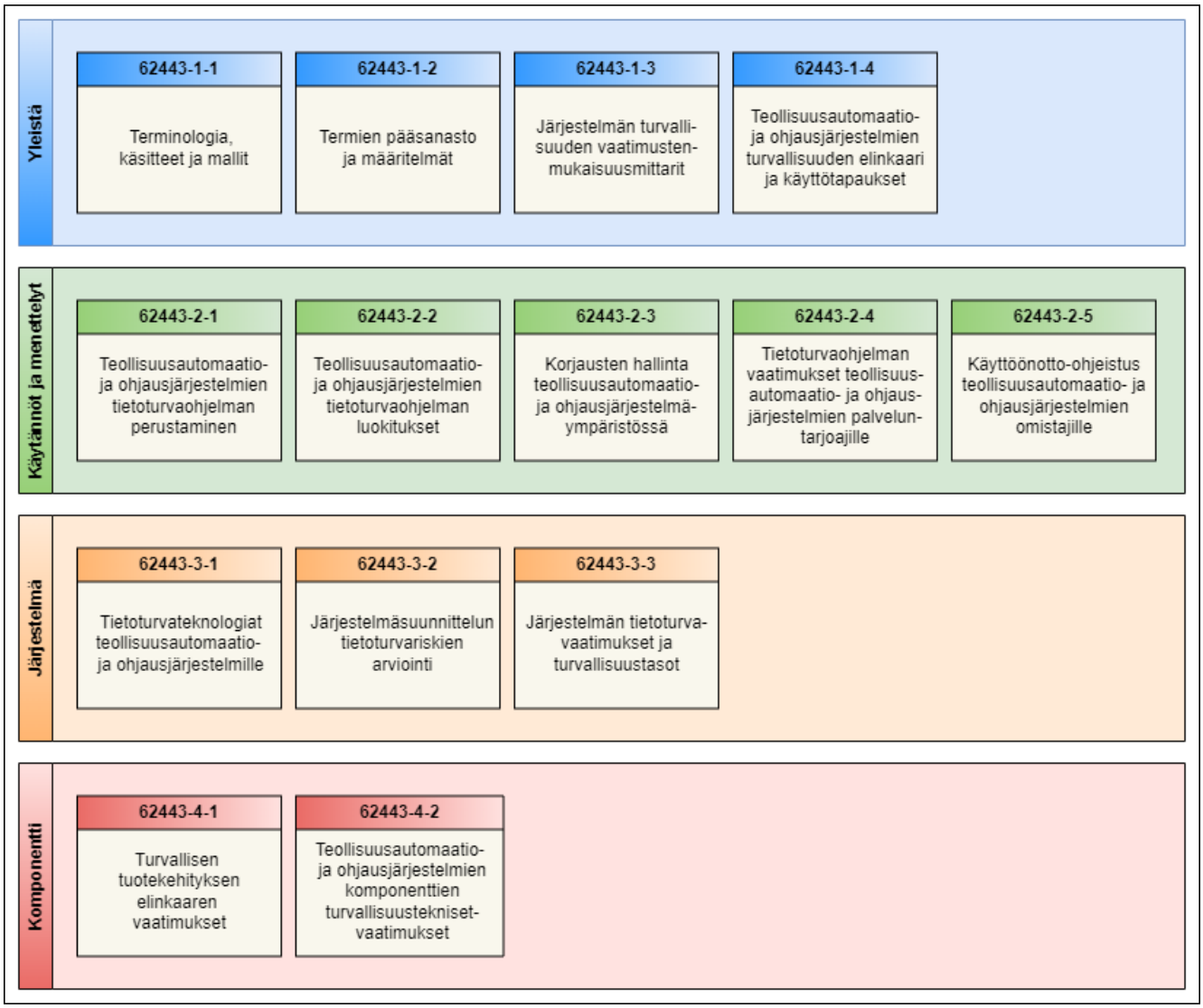


KUVIO 2. Yhteenveto roolien, tuotteiden, automaatiorakenteiden, automaatio- ja ohjausjärjestelmien ja standardien suhteesta toisiinsa (mukaillen IEC 62443-4-1:2018, 10; International Society of Automation 2023, 10)

Standardikokoelman peruskäsitteitä ovat turvallisuusohjelma, riskienhallinta, perusvaatimukset, tietoturvatasot, kypsyystasot ja suunnittelun periaatteet. Turvallisuusohjelmassa omistaja määrittelee turvallisuusvaatimukset teollisuusautomaatio- ja ohjausjärjestelmille. Turvallisuusohjelma kattaa järjestelmän koko elinkaaren. Riskienhallinta sisältää riskien arviointia, turvallisuusvaatimusten määrittelyä ja uhkamallinnusta. Perusvaatimukset asettavat teollisuusautomaatio- ja ohjausjärjestelmille perustietoturvavaatimukset, jotka ovat luetulta aikaisemmassa kappaleessa. (International Society of Automation 2023, 6–8.)

Tietoturvatasot ovat malli, jonka avulla voidaan määrittää, että tarkasteltava järjestelmä (system under consideration eli SUC), tietoturvavyöhyke tai tietoväylä toimii odotetusti ja eikä se sisällä haavoittuvuuksia. Standardikokoelman tietoturvatasot jaetaan kolmeen tasoon: tavoitetaso (Target Security Level (SL-T)), saavutettu taso (Achieved Security Level (SL-A)) ja kykytaso (Capability Security Level (SL-C)). Tavoitetaso on nimensä mukaisesti tietoturvan taso, johon pyritään. Saavutettu taso on nimensä mukaisesti tietoturvan taso, joka on saavutettu. Kykytaso on tietoturvan taso, johon arvioitavan kohteen tietoturvatoimenpiteet, laitteet ja järjestelmät luontaisesti kykenevät, kun ne on integroitu ja konfiguroitu asianmukaisesti. (IEC/TS 62443-1-1:fi, 24, 46, 98; International Society of Automation 2023, 8–9.) Tietoturvatasot ovat teknillisten vaatimusten mittari, kun taas kypsyystasoja käytetään prosessien mittarina (International Society of Automation 2023, 9). Kypsyystasot käsitellään tarkemmin myöhemmin tässä työssä.

ISA/IEC 62443 -standardikokoelma (ks. kuvio 3) jakaantuu neljään pääryhmään: yleistä (general), käytännöt ja menettelyt (policies & procedures), järjestelmä (system) ja komponentti (component) (International Society of Automation 2023, 4). Jokainen pääryhmä sisältää dokumentteja (standardeja, teknisiä raportteja ja spesifikaatioita), jotka liittyvät kyseiseen pääryhmään (International Society of Automation 2023, 3). Jokainen pääryhmä jakaantuu kuvion 3 mukaisiin dokumentteihin. Näiden pääryhmien sisältö on suunnattu eri roolissa toimiville organisaatioille ja/tai henkilöille.



KUVIO 3. ISA/IEC 62443 -standardikokoelman rakenne (mukaillen International Society of Automation 2023, 5)

Yleistä-pääryhmän dokumentit ovat ns. yleisdokumentteja, jotka ovat yhteisiä koko standardikokoelmalle (International Society of Automation 2023, 4). Yleistä-pääryhmä jakaantuu neljään osaan (ks. kuvio 3), jotka ovat lueteltu alla.

- Osa 1-1: Terminologia, käsitteet ja mallit (Terminology, concepts and models)
- Osa 1-2: Termien pääsanasto ja määritelmät (Master glossary of terms and definitions)
- Osa 1-3: Järjestelmän turvallisuuden vaatimustenmukaisuusmittarit (System security conformance metrics)
- Osa 1-4: Teollisuusautomaatio- ja ohjausjärjestelmien turvallisuuden elinkaari ja käyttötapaukset (IACS security lifecycle and use cases)

Yleistä-pääryhmän osa 1-1 on tekninen spesifikaatio, joka luo perustan koko standardikokoelman muille standardeille, koska siinä määritellään terminologia, käsitteet ja mallit teollisuusautomaatio- ja ohjausjärjestelmien tietoturvalle (International Society of Automation 2023, 6; Sesko 2024). Tämä osa on suunnattu kaikille, jotka haluavat tutustua standardikokoelman peruskäsitteisiin. Osa 1-2 on tekninen raportti, joka listaa standardikokoelmassa käytetyt termit ja lyhenteet. Osassa 1-3 kuvataan menetelmiä, miten voidaan kehittää prosessien kvantitatiivisia mittareita ja teknisiä vaatimuksia standardeista. Osa 1-4 antaa tarkempia kuvauksia teollisuusautomaatio- ja ohjausjärjestelmien turvallisesta elinkaaresta ja käyttötapauksia erilaisista sovelluksista. (International Society of Automation 2023, 4–6.)

Käytännöt ja menettelyt -pääryhmä sisältää dokumentteja, jotka keskittyvät teollisuusautomaatio- ja ohjausjärjestelmien turvallisuuteen liittyviin käytäntöihin ja menettelyihin (International Society of Automation 2023, 5). Toinen pääryhmä on jaettu viiteen osaan (ks. kuvio 3), jotka ovat lueteltu alla.

- Osa 2-1: Teollisuusautomaatio- ja ohjausjärjestelmien tietoturvaohjelman perustaminen (Establishing an IACS security program)
- Osa 2-2: Teollisuusautomaatio- ja ohjausjärjestelmien tietoturvaohjelman luokitukset (IACS security program ratings)
- Osa 2-3: Korjausten hallinta teollisuusautomaatio- ja ohjausjärjestelmäympäristössä (Patch management in the IACS environment)
- Osa 2-4: Tietoturvaohjelman vaatimukset teollisuusautomaatio- ja ohjausjärjestelmien palveluntarjoajille (Security program requirements for IACS service providers)
- Osa 2-5: Käyttöönotto-ohjeistus teollisuusautomaatio- ja ohjausjärjestelmien omistajille (Implementation guidance for IACS asset owners)

Osa 2-1 on kansainvälinen standardi, jossa kuvataan, mitä vaaditaan tehokkaan teollisuusautomaatio- ja ohjausjärjestelmien tietoturvallisuuden hallintajärjestelmän perustamiseen (International Society of Automation 2023, 5–6; Sesko 2024). Tämän osion sisältö on suunnattu erityisesti omistajille, jotka ovat vastuussa teollisuusautomaatio- ja ohjausjärjestelmien suunnittelusta ja toteutuksesta. Osa 2-2 tarjoaa menetelmän arvioida toiminnassa olevan teollisuusautomaatio- ja ohjausjärjestelmän turvallisuutta suhteessa standardikokoelman vaatimuksiin. Osa 2-3 on tekninen raportti, jossa annetaan opastusta, miten teollisuusautomaatio- ja ohjausjärjestelmien korjauksia voidaan hallita. Osion sisältö on suunnattu erityisesti henkilöille, jotka ovat vastuussa järjestelmän suunnittelusta, toteutuksesta ja korjaustenhallintaohjelmasta. Osa 2-4 on kansainvälinen standardi, joka määrittelee vaatimukset teollisuusautomaatio- ja

ohjausjärjestelmien palveluntarjoajille, kuten integrointi- ja ylläpitopalvelua tarjoaville palveluntarjoajille. Osa 2-5 on tekninen raportti, jossa annetaan opastusta, mitä vaaditaan tehokkaaseen teollisuusautomaatio- ja ohjausjärjestelmän tietoturvallisuuden hallintajärjestelmän toimintaan. Sisältö on suunnattu omistajille, jotka ovat vastuussa tietoturvan hallintajärjestelmän toiminnasta. (International Society of Automation 2023, 5–6).

Järjestelmä-pääryhmän sisältämät dokumentit kohdistuvat järjestelmävaatimuksiin (International Society of Automation 2023, 5). Kolmas pääryhmä on jaettu kolmeen osaan (ks. kuvio 3), jotka ovat lueteltu alla.

- Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille (Security technologies for IACS)
- Osa 3-2: Järjestelmäsuunnittelun tietoturvariskien arviointi (Security risk assessment for system design)
- Osa 3-3: Järjestelmän tietoturvavaatimukset ja turvallisuustasot (System security requirements and security levels)

Osassa 3-1 kuvataan erilaisten tietoturvateknologioiden soveltamista teollisuusautomaatio- ja ohjausjärjestelmäympäristöön. Teknisen raportin sisältö sopii kaikille, jotka haluavat oppia lisää tiettyjen teknologioiden soveltuvuudesta ohjausjärjestelmäympäristöön. (International Society of Automation 2023, 5–6.) Osa 3-2 on kansainvälinen standardi, joka käsittää teollisuusautomaatio- ja ohjausjärjestelmien riskiarvioinnin ja järjestelmäsuunnittelun. Standardin tuotoksena tarkasteltava järjestelmä jaetaan tietoturvavyöhykkeisiin ja tietoväyliin, joista jokaiselle tehdään riskiarviointi ja turvallisuustason määritys. Standardi käsittää myös dokumentoinnin kyberturvallisuusspesifikaatioon. Tämä standardi on suunnattu ensisijaisesti omistajille ja järjestelmän integroijille. (International Society of Automation 2023, 6; Sesko 2024.) Osa 3-3 on kansainvälinen standardi, jossa kuvataan vaatimukset teollisuusautomaatio- ja ohjausjärjestelmille perustuen turvallisuustasoihin, jotka on kuvattu standardikokoelman osassa 1-1 (International Society of Automation 2023, 6; Sesko 2024). Standardin pääasiallinen kohderyhmä on ohjausjärjestelmien toimittajat, järjestelmän integroijat ja omistajat (International Society of Automation 2023, 6).

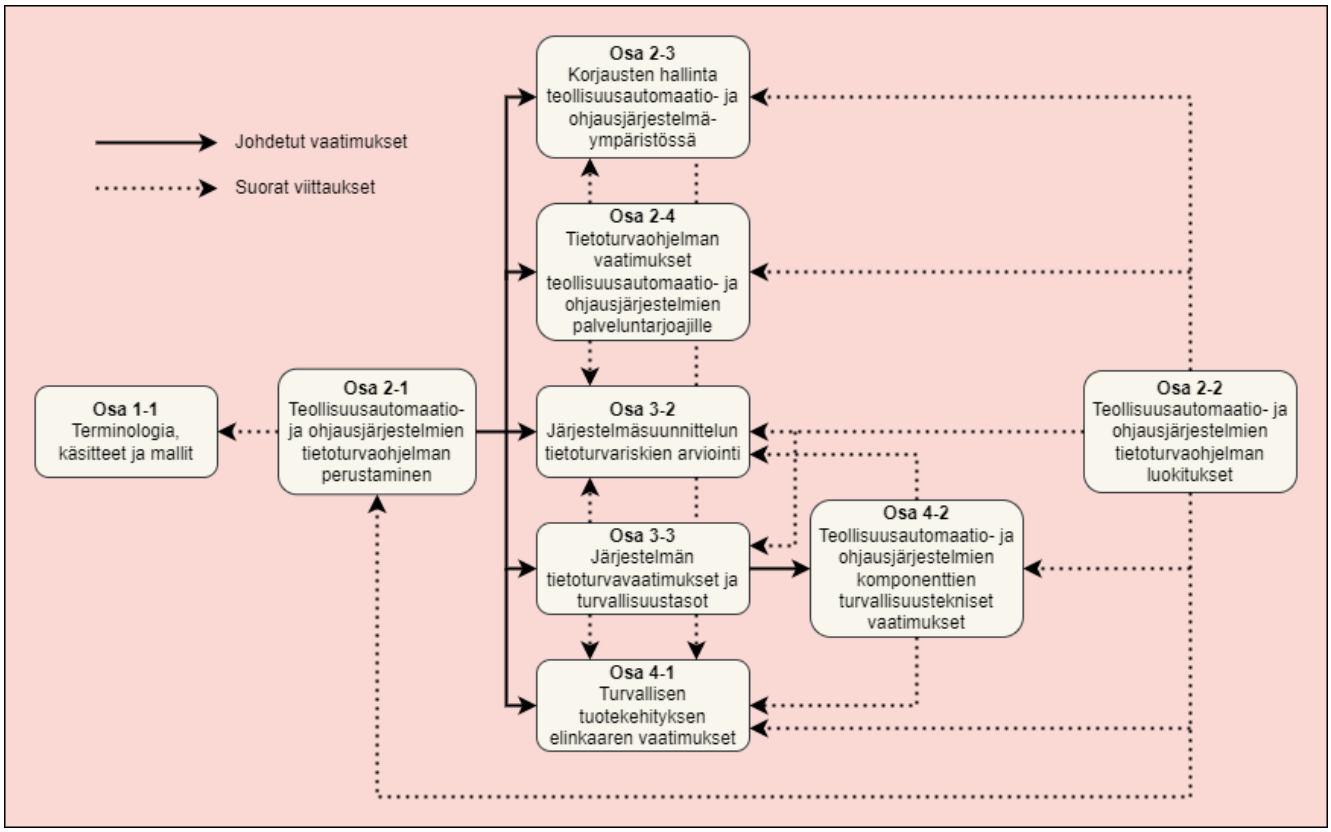
Komponentti-pääryhmä on standardikokoelman neljäs ja viimeinen pääryhmä. Neljäs pääryhmä sisältää dokumentit, jotka antavat tarkempaa ja yksityiskohtaisempaa tietoa teollisuusautomaatio- ja ohjausjärjestelmien komponenttien kehitykseen liittyvistä vaatimuksista (International Society of Automation 2023, 6). Komponentti-pääryhmä on jaettu kahteen osaan (ks. kuvio 3), jotka ovat lueteltu alla:

- Osa 4-1: Turvallisen tuotekehityksen elinkaaren vaatimukset (Product security development lifecycle requirements)
- Osa 4-2: Teollisuusautomaatio- ja ohjausjärjestelmien komponenttien turvallisuustekniset vaatimukset (Technical security requirements for IACS components)

Osat 4-1 ja 4-2 ovat kansainvälisiä standardeja. Tässä opinnäytetyössä käsitellään tarkemmin ja laajaalaisemmin standardikokoelman osa 4-1. Lyhyesti kuvattuna osa 4-1 määrittelee vaatimukset turvallisen tuotekehityksen elinkaarelle. Standardin pääasiallinen kohderyhmä käsittää ohjausjärjestelmien ja komponenttien toimittajat. Osassa 4-2 kuvataan vaatimukset teollisuusautomaatio- ja ohjausjärjestelmien komponenteille turvallisuustasoon perustuen. Komponenteiksi katsotaan sulautetut laitteet, isäntälaitteet, verkkolaitteet ja ohjelmistosovellukset. Standardin pääasiallinen kohderyhmä käsittää ohjausjärjestelmien komponenttien toimittajat. (International Society of Automation 2023, 6.)

Kuviossa 4 esitellään standardikokoelman standardien välisiä yhteyksiä. Pistemäisillä nuolilla on kuvattu suorat viittaukset standardien välillä ja mustilla nuolilla on merkitty johdetut vaatimukset. Nuolenpään suunta osoittaa, mihin suuntaan johtaminen suuntautuu. Kuten edellä on kuvattu ja kuviosta 4 voidaan nähdä kaikissa standardeissa viitataan osaan 1-1, jossa esitellään käsitteet ja mallit. Osa 2-1 määrittelee vaatimukset turvallisuusohjelmalle. Standardikokoelman muut standardit johtavat omat vaatimuksensa osan 2-1 vaatimuksista ja täten laajentavat sen vaatimuksia yksityiskohtaisemmin. Osa 2-2 viittaa muihin standardeihin, jotta sen perusteella voidaan luoda arviointimenetelmä toiminnassa olevalle teollisuusautomaatio- ja ohjausjärjestelmälle. Tämä on standardikokoelman hierarkkinen esitystapa. (ISA Global Cybersecurity Alliance 2020, 6.)

Standardikokoelma voidaan esittää myös elinkaarimallina. Standardikokoelma sisältää kaksi erillistä ja itsenäistä elinkaarta. Standardikokoelmassa kuvataan turvallisen tuotteen elinkaari (product security lifecycle) ja turvallisen automaatioratkaisun elinkaari (automation solution security lifecycle). (ISA Global Cybersecurity Alliance 2020, 7.) Kuviosta 5 on hyvin nähtävissä, mitkä standardit koskevat turvallisen tuotteen elinkaarta ja mitkä turvallisen automaatioratkaisun elinkaarta. Kuviosta 5 nähdään myös, että osat 1-1 ja 3-3 kattavat molemmat elinkaaret.



KUVIO 4. ISA/IEC 62443 -standardikokoelman standardien väliset yhteydet (mukaillen ISA Global Cybersecurity Alliance 2020, 6)

Turvallisen tuotteen elinkaari	Turvallisen automaatioratkaisun elinkaari
Osa 1-1: Terminologia, käsitteet ja mallit	
	Osa 2-1: Teollisuusautomaatio- ja ohjausjärjestelmien tietoturvaohjelman perustaminen
	Osa 2-2: Teollisuusautomaatio- ja ohjausjärjestelmien tietoturvaohjelman luokitukset
	Osa 2-3: Korjausten hallinta teollisuusautomaatio- ja ohjausjärjestelmäympäristössä
	Osa 2-4: Tietoturvaohjelman vaatimukset teollisuusautomaatio- ja ohjausjärjestelmien palveluntarjoajille
	Osa 3-2: Järjestelmäsuunnittelun tietoturvariskien arviointi
Osa 3-3: Järjestelmän tietoturvavaatimukset ja turvallisuustasot	
Osa 4-1: Turvallisen tuotekehityksen elinkaaren vaatimukset	
Osa 4-2: Teollisuusautomaatio- ja ohjausjärjestelmien komponenttien turvallisuustekniset vaatimukset	

KUVIO 5. ISA/IEC 62443 -standardikokoelman elinkaaret (mukaillen ISA Global Cybersecurity Alliance 2020, 7)

4 ISA/IEC 62443-4-1 STANDARDI

ISA/IEC 62443-4-1 standardi määrittelee turvallisen tuotekehityksen elinkaari -prosessin vaatimukset teollisuusautomaatio- ja ohjausjärjestelmissä käytettäville tuotteille. Turvallisen tuotekehityksen prosessi sisältää turvallisuusvaatimukset, turvallisen suunnittelun ja toteutuksen, verifioinnin ja validoinnin, vika- ja korjaushallinnan sekä tuotteen elinkaaren lopun. Standardin vaatimuksia voidaan soveltaa jo olemassa oleviin tai uusiin laitteiston, ohjelmistojen tai laiteohjelmistojen kehitys-, ylläpito- ja käytöstä poisto -prosesseihin olemassa olevassa tai uudessa tuotteessa. Standardin vaatimukset ovat kohdennettu tuotteen kehittäjälle ja ylläpitäjälle, eivätkä ne koske tuotteen integroijaa tai käyttäjää. (IEC 62443-4-1:2018, 11.)

Tuote voi olla joko yksittäinen komponentti tai ryhmä komponentteja, jotka toimivat yhdessä muodostaen järjestelmän tai alijärjestelmän. Tuotteet integroidaan sitten automaatioratkaisuksi integraatiopalveluntarjoajan toimesta osan 2-4 prosessin mukaisesti. Automaatioratkaisusta tulee osa teollisuusautomaatio- ja ohjausjärjestelmää, kun se asennetaan tarkoitettuun ympäristöönsä. Ks. myös kuvio 2 yhteenveto teollisuusautomaatio- ja ohjausjärjestelmästä. Standardissa 4-1 kuvataan tuotekehitysprosessille määriteltyjä vaatimuksia, kuten käytäntöjä ja menettelyjä, eikä niinkään turvallisuusteknisiä vaatimuksia. Teollisuusautomaatio- ja ohjausjärjestelmien turvallisuustekniset vaatimukset on määritelty osassa 3-3 ja komponenttien turvallisuustekniset vaatimukset on määritelty osassa 4-2. (IEC 62443-4-1:2018, 9–10; International Society of Automation 2023, 8; ISA Global Cybersecurity Alliance 2020, 11.)

Teollisuusautomaatio- ja ohjausjärjestelmien turvallisen tuotekehityksen elinkaari jakaantuu kahdeksaan turvallisuuskäytäntöön, jotka jokainen itsessään sisältävät omat osaprosessinsa kyseisen turvallisuuskäytännön toimeenpanemiseksi (ISA Global Cybersecurity Alliance 2020, 11). Nämä osaprosessit eli vaatimukset alkavat pääsääntöisesti sanoilla ”A process shall be employed…”. Tämä tarkoittaa, että vaadittujen osaprosessien on oltava osa tuotetoimittajan dokumentoitua tuotekehityksen elinkaari -prosessia. (IEC 62443-4-1:2018, 17.) Alla oleva taulukko 1 tiivistää nämä käytännöt yhteen taulukkoon. Käytännöt ja niiden osaprosessit esitellään tarkemmin omina alalukuinaan.

TAULUKKO 1. Teollisuusautomaatio- ja ohjausjärjestelmien komponenttien tuotekehityksen elinkaaren turvallisuuskäytännöt (mukaillen ISA Global Cybersecurity Alliance 2020, 11)

Käytäntö	Nimike	Vaatimusten määrä
1	Turvallisuuden hallinta (Security management, SM)	13
2	Turvallisuusvaatimusten määrittely (Spesification of security requirements, SR)	5
3	Turvallinen suunnittelu (Secure by design, SD)	4
4	Turvallinen toteutus (Secure implementation, SI)	2
5	Turvallisuuden verfiointi- ja validointitestaus (Security verification and validation testing, SVV)	5
6	Turvallisuusongelmien hallinta (Management of security-related issues, DM)	6
7	Tietoturvapäivitysten hallinta (Security update management, SUM)	5
8	Turvallisuusohjeet (Security guidelines, SG)	7

Standardin tavoitteena on tarjota turvallisen suunnittelun ja syväsuojauksen viitekehys, jota voidaan soveltaa teollisuusautomaatio- ja ohjausjärjestelmissä käytettävien tuotteiden suunnitteluun, toteutukseen, ylläpitoon ja käytöstä poistoon. Tämä lisää luottamusta, että tuotteen turvallisuus on mitoitettu oikeassa suhteessa sen riskitasoon nähden koko elinkaaren ajan. Standardin soveltaminen varmistaa myös, että tuotteen turvallisuusominaisuudet on toteutettu oikein ja sen tietoturvahaavoittuvuudet on joko poistettu tai niitä on lievennetty. Näin ollen standardin noudattaminen tukee tuotteen turvallisuustasoa SL-C (kykytaso). Standardin toisena tavoitteena on yhtenäistää kehitysprosesseja vastaamaan teollisuusautomaatio- ja ohjausjärjestelmien käyttäjien kohonneita turvallisuustarpeita. (IEC 62443-4-1:2018, 17–18.)

ISA/IEC 62443-4-1 standardi sisältää ns. kypsyystason mallin (maturity model), jolla voidaan arvioida tuotetoimittajan turvallisuustoimenpiteiden tasoa koskien henkilöstöä, käytäntöjä ja menettelyjä. Kypsyystasossa (maturity level) määritellään, millä tasolla prosessin toiminnot ovat eli onko prosessi toiminnassa, onko sitä harjoitettu, onko prosessia kehitetty ja onko prosessi dokumentoitu. (ISA Global Cybersecurity Alliance 2020, 11.) Standardin käyttämä kypsyysmalli perustuu CMMI-DEV-malliin (Capability Maturity Model Integration for Development). Omistajat ja järjestelmän integroijat voivat-

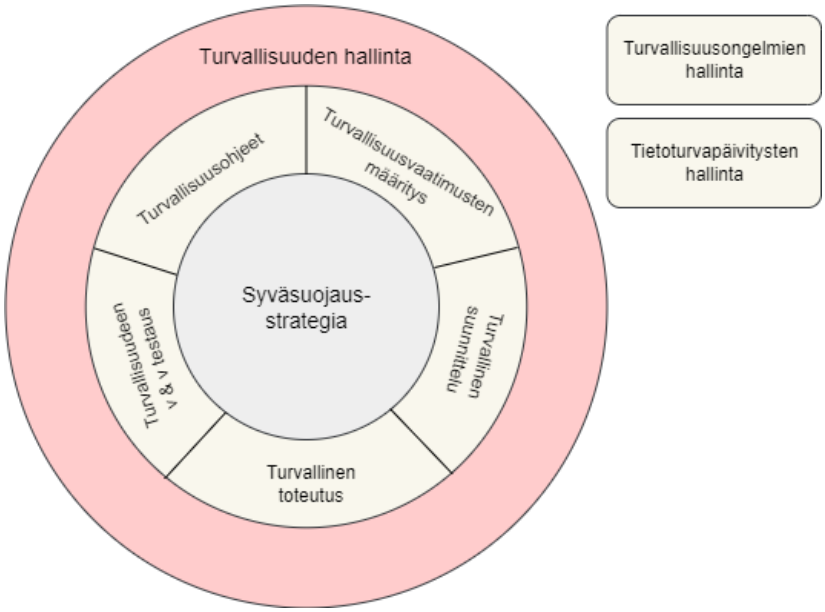
kin käyttää tätä mallia arvioidakseen, kuinka täsmällisesti tuotetoimittaja on toteuttanut standardin asettamia vaatimuksia tuotekehityksessään. (IEC 62443-4-1:2018, 19.) Kypsyystasoja kuvaa ja selventää parhaiten alla oleva taulukko 2, jossa käydään läpi kaikki mallin tasot.

TAULUKKO 2. Kypsyystasot (mukaillen IEC 62443-4-1:2018, 20; ISA Global Cybersecurity Alliance 2020, 11)

Kypsyystaso	Kuvaus	Selite
ML1	Alustava (Initial)	Tuotetoimittaja suorittaa tuotekehitysprosessit ad hoc -tyyppisesti ja/tai dokumentoimattomasti (tai ei täysin dokumentoidusti). Näin ollen projekteja ei voida välttämättä suorittaa johdonmukaisesti eivätkä prosessit ole välttämättä toistettavissa.
ML2	Hallittu (Managed)	Tuotetoimittaja kykenee hallitsemaan tuotekehitysprosessia dokumentoiduilla menettelytavoilla. Tuotetoimittaja pystyy osoittamaan, että prosessia suorittavalla henkilökunnalla on tarvittava pätevyys ja he ovat koulutettuja toimimaan käytäntöjen mukaisesti. Tuotetoimittajalla ei ole vielä tällä tasolla kuitenkaan kokemusta kaikkien menettelyjen täytäntöönpanosta.
ML3	Määritelty (Harjaantunut) (Defined (Practiced))	Tuotetoimittaja voi osoittaa, että sen prosessit ovat toistettavissa ja ne ovat dokumentoituja. Prosesseja on harjoitettu ja tuotetoimittajalla on näyttää todisteita siitä, että näin on toimittu.
ML4	Edistyvä (Improving)	Tuotetoimittajalla on käytössään sopivia prosessimittareita, joilla varmistetaan prosessien tehokkuus ja suorituskyky. Prosesseja parannetaan jatkuvasti näitä mittareita hyödyntäen.

Turvallisen tuotekehityksen elinkaaren avainajatuksena toimii syväsuojaus (ks. kuvio 6). Näin ollen ISA/IEC 62443-4-1 standardin seuraamisen tuloksena luodaan tuotteelle syväsuojauksen strategia. Turvallisuuden hallinta- käytäntö luo pohjan turvallisen tuotekehityksen koko prosessille. Turvallisuuden hallintaa sovelletaan kaikkiin muihin käytäntöihin ja sen tarkoituksena onkin varmistaa, että käytäntöjä noudatetaan ja niitä hallitaan. Kuvion 6 toiseksi uloimmassa renkaassa olevia käytäntöjä noudatetaan

koko tuotekehityksen elinkaaren ajan ja hyvin usein iteratiivisesti. Jokainen käytäntö edistää itsessään syväsuojausstrategiaa. Turvallisuusongelmien ja tietoturvapäivitysten hallinta sisältyvät kuviossa 6 turvallisuuden hallinnan alaisuuteen tarjoten verifioituja korjauksia turvalliseen toteutukseen. (IEC 62443-4-1:2018, 18.) Kuviossa 6 kyseiset käytännöt on kuitenkin esitetty omissa laatikoissaan selvyyden vuoksi.



KUVIO 6. Turvallisen tuotekehityksen ja syväsuojausstrategian yhteys (mukaillen IEC 62443-4-1:2018, 18)

4.1 Turvallisuuden hallinta

Turvallisuuden hallinnan käytännön tarkoituksena on varmistaa, että turvallisuuteen liittyvät toiminnot suunnitellaan, toteutetaan ja dokumentoidaan asianmukaisesti koko tuotteen elinkaaren ajan. Turvallisuustoimintojen suunnitteluun ja tukemiseen täytyy varata riittävästi resursseja ja aikaa. Lisäksi prosesseja täytyy tarkastella siten, että ne eivät sisällä turhaa tehottomuutta. Mikäli näihin asioihin ei kiinnitetä huomiota, voivat turvallisuustoiminnot osoittautua tehottomiksi. Suunnittelussa on huomioitava myös, että tuotteen turvallisuustarpeiden on oltava linjassa tuotetoimittajan sisäisten prosessien kanssa, kuten tietotekniikkapolitiikka ja -käytännöt sekä toimitusketjujen hallinta. Tuotetoimittajan sisäisten prosessien huomioiminen lisää turvallisen tuotekehityksen elinkaaren tehokkuutta. (IEC 62443-4-1:2018, 20). Turvallisuuden hallinta -käytännön vaatimukset jakaantuvat kolmeentoista osaprosessiin, jotka ovat lueteltu alla:

1. Kehitysprosessi (Development process),
2. Vastuiden tunnistaminen (Identification of responsibilities),
3. Soveltuvuuden tunnistaminen (Identification of applicability),
4. Turvallisuusasiantuntemus (Security expertise),
5. Prosessin laajuus (Process scoping),
6. Tiedostojen eheys (File integrity),
7. Kehitysympäristön turvallisuus (Development environment security),
8. Yksityisten avainten hallinta (Controls for private keys),
9. Turvallisuusvaatimukset ulkoisesti toimitetuille komponenteille (Security requirements for externally provided components),
10. Kolmannen osapuolen räätälöidyt komponentit (Custom developed components from 3rd party suppliers),
11. Turvallisuusaongelmien arviointi ja käsittely (Assessing and addressing security-related issues),
12. Prosessin verifiointi (Process verification) ja
13. Jatkuva parantaminen (Continuous improvement).

(ISA Global Cybersecurity Alliance 2020, 11–12.)

Turvallisuuden hallinnan ensimmäinen osaprosessi kehitysprosessi käsittää yleisen tuotekehitys-, ylläpito- ja tukiprosessin. Standardissa määritellään, että edellä mainitut prosessit tulevat olla dokumentoituja ja pantu täytäntöön johdonmukaisesti. Prosessien on oltava myös yleisesti hyväksyttyjen tuotekehityksen standardien mukaisia. (Automation Standards Compliance Institute 2022, 5 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 21.) Kehitysosaprosessi varmistaa ja olettaa, että tuotetoimittajalla on käytössään kypsä, hyvin suunniteltu ja määritelty tuotekehitysprosessi, jota voidaan edelleen laajentaa vastaamaan standardin määrittelemiä vaatimuksia. Näin ollen tuotetoimittajan täytyy ensin varmistaa, että sen tuotekehitysprosessi on määritelty ennen kuin standardin vaatimuksia voidaan soveltaa. (IEC 62443-4-1:2018, 21.)

Vastuiden tunnistamisen osaprosessin tarkoituksena on, että tuotetoimittaja tunnistaa organisaation roolit ja henkilöstön vastuualueet. Jokaiselle standardin määrittelemälle prosessille on oltava vastuuhenkilö. Vastuunjaon tarkoituksena on varmistaa, että standardin vaatimat prosessit pannaan täytäntöön ja että ne saatetaan loppuun. Käytännössä tämä tarkoittaa, että tuotetoimittajan tuotekehitys-, tuotteen ylläpito- ja tuotetukiprosesseille pitää olla määriteltynä vastuuhenkilöt ja organisaation roolit pitää olla tunnis-

tettu. Standardin mukaan organisaatio ja henkilöstö voivat olla joko kehittäjäorganisaation sisäisiä yksiköitä ja henkilöstöä tai kehittäjäorganisaation ulkopuolisia organisaatioita ja henkilöitä. Tämän vaatimuksen täyttämiseksi voidaan käyttää apuna esim. RACI-matriisia. (Automation Standards Compliance Institute 2022, 5 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 21.)

Soveltuvuuden tunnistamisessa on tunnistettava tuotteet tai tuotteen osat, joihin standardia sovelletaan. Tarkoituksena on siis varmistaa, että standardin sisältämiä prosesseja sovelletaan tarkoituksenmukaisiin tuotteisiin tarpeen mukaan ja tarvittavalla tarkkuudella. Käytännössä tuotevalmistajalla on oltava kriteerit, joiden avulla voidaan tunnistaa tuotteet, joita kehitetään, ylläpidetään ja tuetaan standardin vaatimusten mukaisesti. Näitä kriteereitä voivat olla esim. tuotteen markkinaympäristö, tuotteen sisäiset turvallisuusvaatimukset tai turvallisuusriskit. Tämän osaprosessin vaatimuksia voidaan soveltaa myös kolmannen osapuolen tuottamiin tai räätälöimiin komponentteihin. (Automation Standards Compliance Institute 2022, 5 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 21–22.)

Turvallisuusasiantuntemuksen osaprosessissa varmistetaan, että vastuiden tunnistamisen osaprosessissa määritellyillä vastuuhenkilöillä on tarvittava turvallisuusasiantuntemus kyseiseen erityistehtävään. Turvallisuusasiantuntemuksen osaprosessissa varmistetaan myös, että tuotetoimittajalla on keinot arvioida vastuiden ja roolien vaatiman turvallisuusasiantuntemuksen tasoa ja että tuotetoimittaja kykenee tarjoamaan tarvittavaa koulutusta. Standardin mukaan asiantuntemus on voitu hankkia esim. kouluttautumalla tai kokemuksella. Asiantuntemus sisältää myös teknisen osaamisen koskien syväsuojauksen strategioita ja tekniikoita sekä käytäntöjen tuntemusta, joita tuotteen kehittäminen ja ylläpito vaativat. Tuotetoimittaja todentaa, että henkilöstöllä, joka on mukana turvallisuuteen liittyvissä prosesseissa, on asiaankuuluvat pätevyydet prosessien suorittamiseksi mukaan lukien henkilöt, jotka eivät suoranaisesti ole mukana turvallisen tuotekehityksen elinkaaren prosessissa, kuten turvallisuusvaatimusten analyysiin osallistuvat henkilöt. Henkilöstöllä pitäisi olla asiantuntemusta turvallisuuden lisäksi turvallisuuteen liittyvistä standardeista (esim. koodausstandardit), tekniikoista (esim. parhaat käytännöt) ja työkaluista (esim. staattiset analyysityökalut). (Automation Standards Compliance Institute 2022, 5 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 22.)

Prosessin laajuus -osaprosessin tarkoituksena on tunnistaa standardin osiot, jotka ovat sovellettavissa valittuun tuotekehitysprosessiin. Tunnistusprosessi pitää sisällään dokumentoidun turvallisuusanalyysin perustelut, miksi jokin standardin osio ei ole sovellettavissa kyseiseen tuotekehitysprosessiin. Esimerkiksi, mikäli tuote ei sisällä ohjelmistoa, ei ohjelmistoja koskevia vaatimuksia tarvitse soveltaa tuotteeseen. Tämän tarkastelun ja arvioinnin suorittaa henkilö, jolla on tarvittava turvallisuusasiantuntemus

aikaisemmin suoritetun turvallisuusasiantuntemuksen arvioinnin perusteella. (Automation Standards Compliance Institute 2022, 6 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 22–23.)

Tiedostojen eheys -osaprosessin tarkoituksena on varmistaa, että tuotetoimittajalla on käytössään menetelmät todentaa tuotteessa käytettyjen tiedostojen eheys. Näitä tiedostoja ovat erilaiset skriptit, suoritettavat tiedostot ja muut tärkeät tiedostot. Osaprosessin tarkoituksena on varmistaa, että tuotteen käyttäjät voivat olla varmoja, että tuotetoimittajan toimittamat tiedostot ovat muuttumattomia. Tämän vaatimuksen täyttämiseen voidaan käyttää yleisiä menetelmiä, jotka sisältävät mm. kryptografiset tiivisteet ja digitaaliset allekirjoitukset. (Automation Standards Compliance Institute 2022, 6 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 23.)

Kehitysympäristön turvallisuus -osaprosessin tarkoituksena on varmistaa, että tarvittavat turvallisuustoimet on huomioitu tuotteen tai tuotteen päivitysten elinkaaren eri vaiheissa (suunnittelu, kehitys, testaus jne.) tuotteen tai päivityksen turvaamiseksi. Näin varmistetaan, että tuotetta tai pävitystä ei ole muutettu tai julkaistu kehitysprosessin aikana ilman hyväksyntää. Tuotetoimittajan on menettelyillään suojattava myös tuotteen suunnitteludokumenttien eheyttä, toteutusta (esim. lähdekoodi ja käyttöohjeet), kokoonpanoasetuksia ja yksityisiä avaimia. Näiden vaatimusten täyttämiseksi voidaan soveltaa esim. ISO/IEC 27001 (tietoturvallisuuden standardisarja) ja 27002 (tietoturvallisuuden hallintakeinot) standardien määrittelemiä menettelyjä. Erityistä huomiota on kiinnitettävä autentikointiin, esim. salasanat, pääsynhallintaluettelot ja koodiallekirjoitustodistukset. Yksityisten avainten hallinta -osaprosessissa vaaditaankin, että tuotetoimittajan on varmistettava, että sillä on käytössään keinot suojata yksityisiä avaimia, joita käytetään koodiallekirjoituksissa, niiden luvattomalta käytöltä tai muutoksilta. (Automation Standards Compliance Institute 2022, 6 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 23.)

Turvallisuusvaatimukset ulkoisesti toimitetuille komponenteille -osaprosessi tarkoittaa, että tuotetoimittajalla täytyy olla dokumentoitu prosessi, jonka avulla voidaan tunnistaa turvallisuusriskit ja hallita turvallisuusriskejä ulkoisen toimittajan toimittamissa komponenteissa, joita käytetään tuotteessa. Vaatimuksen mukaan täytyy huolehtia ensinnäkin siitä, että tuotteen kaikki ulkoiset komponentit on tunnistettu. Toiseksi täytyy tunnistaa komponentteihin liittyvät turvallisuusriskit ja kuinka riskejä voidaan hallita tai lieventää tuotteen eliniän ajan. Näin toimien varmistetaan, että toimitusketjun turvallisuus on huomioitu kokonaisuudessaan. (Automation Standards Compliance Institute 2022, 7 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 24.)

Kolmannen osapuolen räätälöityjen komponenttien -osaprosessissa vaaditaan, että kun komponentti on kehitetty nimenomaista tarkoitusta varten ja tietylle toimittajalle sekä kun sillä voi olla vaikutusta turvallisuuteen, täytyy komponentin tuotekehityksen elinkaari -prosessin vastata tämän standardin asettamia vaatimuksia. Tämä vaatimus koskee tuotetoimittajalle alihankintana tehtyjä komponentteja, joilla voi olla vaikututusta tuotteen turvallisuuteen. Uhkamallinnusta voidaan käyttää, kun määritellään, onko komponentilla vaikutuksia lopullisen tuotteen turvallisuuteen. (Automation Standards Compliance Institute 2022, 7 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 24–25.)

Turvallisuusongelmien arviointi ja käsittely -osaprosessilla halutaan varmistaa, että tuotetoimittjalla on dokumentoitu prosessi siitä, että tuotteessa tai tuotteen korjausversiossa havaitut turvallisuusongelmat dokumentoidaan, jäljitetään ja käsitellään. Osaprosessin tarkoituksena on, että mitään ei julkaista ennen kuin turvallisuusongelmat ovat käsitelty niin, että ne ovat alle hyväksyttävän jäännösriskitason. Näihin turvallisuusongelmiin lasketaan kaikki havaitut ongelmat tuotteen kehityksen ja ylläpidon aikana. (Automation Standards Compliance Institute 2022, 7 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 25.)

Turvallisuuden hallinta -käytännön kaksi viimeistä osaprosessia ovat prosessin verifiointi ja jatkuva parantaminen. Prosessin verifiointi -osaprosessin tarkoituksena on varmistaa, että ennen tuotteen julkaisua kaikki standardin vaatimat ja tuotteeseen sovellettavat (ks. prosessin laajuus -osaprosessi) turvallisuuteen liittyvät prosessit on suoritettu dokumentoidusti. Prosessin verifioinnissa on huomioitava, että vaatimus koskee kaikentyyppisiä julkaisuja aina alkujulkaisusta korjausjulkaisuihin riippuen prosessin laajuuden perusteella tehdystä arviosta koskien standardin prosessien soveltuvuudesta tuotteelle. Tämä tarkoittaa, että mikäli julkaisu on prosessin laajuuden ulkopuolella, ei verifiointia tarvita. (Automation Standards Compliance Institute 2022, 7 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 25.)

Lopuksi jatkuvan parantamisen osaprosessin tarkoituksena on, että tuotetoimittaja parantaa jatkuvasti turvallisen tuotekehityksen elinkaaren prosessiaan. Prosessin parantaminen lisää tuotteen laatua ja prosessin kehitystyö on välttämätöntä, koska uusia turvallisuusuhkia, joita hyökkääjät voivat hyödyntää, ilmenee jatkuvasti. Tähän prosessiin sisällytetään myös lopulliseen julkaisuun jääneiden turvallisuusvikojen ja käytössä huomattujen turvallisuusvikojen analysointi. (Automation Standards Compliance Institute 2022, 8 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 25–26.)

4.2 Turvallisuusvaatimusten määrittely

Turvallisuusvaatimusten määrittely -käytännön tarkoituksena on määritellä ja dokumentoida tuotteen vaaditut tietoturvaominaisuudet tuotteen odotetussa turvallisuuskontekstissa. Tietoturvaominaisuudet voivat sisältää mm. autentikoinnin (todennus), auktorisoinnin (valtuutus) ja enkryptauksen (salaus). Tuotteen turvallisuuskonteksti voi pitää sisällään fyysisen turvatason, ulkoisten rajapintojen suojauksen palomuureilla jne. (IEC 62443-4-1:2018, 26; ISA Global Cybersecurity Alliance 2020, 12.) Käytännön vaatimukset ovat jaettu viiteen osaprosessiin, jotka ovat lueteltu alla:

1. Tuotteen turvallisuuskonteksti (Product security context),
2. Uhkamallinnus (Threat model),
3. Tuotteen turvallisuusvaatimukset (Product security requirements),
4. Tuotteen turvallisuusvaatimusten sisältö (Product security requirements content) ja
5. Turvallisuusvaatimusten tarkastelu (Security requirements review).

(ISA Global Cybersecurity Alliance 2020, 12.)

Tuotteen turvallisuuskontekstin osaprosessilla varmistetaan, että tuotteen tuleva turvallisuuskonteksti on dokumentoitu johdonmukaisesti jokaiselle kehityksen ja testauksen prosessille (Automation Standards Compliance Institute 2022, 9 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 27). Turvallisuuskontekstilla tarkoitetaan odotuksia ja oletuksia, jotka kohdistuvat tuotteen tulevaan turvallisuusympäristöön, jossa tuotetta käytetään. Tässä huomioidaan uhat, riskit ja mahdolliset muut korvaavat turvallisuustoimet. (ISA Global Cybersecurity Alliance 2020, 12.) Turvallisuuskontekstin dokumentoinnilla pyritään varmistamaan, että tuotteen suunniteltu turvallisuustaso saavutetaan. Päämääränä on, että tuotekehittäjillä ja tuotteen käyttäjillä olisi samanlainen käsitys tuotteen tulevista käyttötavoista ja -ympäristöstä. Näin tuotekehittäjät voivat tehdä oikeanlaisia suunnittelupäätöksiä ja käyttäjät kykenevät käyttämään tuotetta tarkoituksenmukaisesti. Tuotteen ulkoisten turvallisuusominaisuuksien kirjaaminen mahdollistaa syväsuojauksen suunnittelun, jolla voidaan täydentää turvallisuuskontekstin tarjoamia ja vaatimia turvallisuusominaisuuksia (IEC 62443-4-1:2018, 27.).

Uhkamallinnus on standardin keskeisin käsite. Tuotteille toteutetaan uhkamallinnus, joka vastaa tuotteen senhetkistä toteutusta. Uhkamallinnuksessa on huomioitava, että mallinnusta päivitetään säännöllisesti ja erityisesti, kun toteutukseen tehdään muutoksia. Uhkamallinnusta on kuitenkin tarkasteltava vuosittain, vaikka tuotteeseen ei olisikaan tehty muutoksia. Uhkamallinnuksessa huomioidaan ja siihen sisäl-

lytetään myös ulkoiset riippuvuudet, joilla on vaikutusta tuotteen turvallisuuteen, kuten ulkoiset komponentit, järjestelmät tai kolmannen osapuolen lähdekoodi. Uhkamallinnuksella pyritään tunnistamaan mm. tietovirrat, luottamusrajat (trust boundaries), hyökkäysvektorit, turvallisuusongelmat ja potentiaaliset uhat. Tunnistetut uhat pisteytetään joko käyttämällä hyväksyttyjä pisteytysmenetelmiä (esim. CVSS) tai hyvin dokumentoituja ja järkeistettyjä menetelmiä. Uhkia pyritään minimoimaan tai vastaavasti annetaan riittävät perustelut sille, miksi uhkaa ei minimoida. Ennen tuotteen lopullista julkaisua on käsiteltävä uhkamallinnuksessa ilmenneet turvallisuuskysymykset. Osaprosessin päämääränä on, että tuotteelle toteutetaan uhkamallinnus, jota ylläpidetään koko tuotteen elinkaaren ajan. (Automation Standards Compliance Institute 2022, 9–10 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 27–28; International Society of Automation 2023, 8.)

Turvallisuusvaatimusten määrittely -käytännön kolme viimeistä osaprosessia liittyvät tuotteen turvallisuusvaatimuksiin. Tuotteen turvallisuusvaatimusten osaprosessin tarkoituksena on, että tuotetoimittaja on dokumentoinut kehitettävän tuotteen tai ominaisuuden turvallisuusvaatimukset. Dokumentointiin sisällytetään myös turvallisuusominaisuuksien vaatimukset koskien asennusta, käyttöä, ylläpitoa ja käytöstä poistoa. Osaprosessin päämääränä on varmistaa, että tuotetoimittaja on määritellyt tuotteen kaikki turvallisuusvaatimukset huomioiden tuotteen koko elinkaaren. Tähän sisältyy myös tuotteelle ominaiset turvallisuusvaatimukset mukaan lukien tekniset (esim. salasanojen monimutkaisuus) ja liiketoiminnalliset (esim. arkaluontoinen data, käyttäjähallinta) turvallisuusvaatimukset. (Automation Standards Compliance Institute 2022, 10 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 28–29.) Turvallisuusvaatimusten on oltava linjassa uhkamallinnuksen kanssa (Mikhaleva 2022, 53). Onkin tärkeä muistaa, että mikäli uhkamallinnusta päivitetään, täytyy myös turvallisuusvaatimuksia tarkastella uudelleen ja päivittää tarvittaessa.

Tuotteen turvallisuusvaatimusten sisältö -osaprosessin tarkoituksena on varmistaa, että tuotteen turvallisuusvaatimukset sisältävät seuraavat tiedot: komponentin tai järjestelmän laajuus ja rajat niin fyysisellä kuin loogisella tasolla sekä tuotteen vaadittava turvallisuustaso. Turvallisuustaso täytyy sisällyttää vaatimuksiin, mikäli tuotteelle on määritetty turvallisuustaso, jonka sen pitää saavuttaa. Näin ollen tuote sisältää tiettyjä turvallisuusominaisuuksia riippuen saavutettavasta turvallisuustasosta. Turvallisuustasot ja vaaditut turvallisuusominaisuudet ovat määritelty standardeissa ISA/IEC 62443-4-2 (komponentit) ja 62443-3-3 (järjestelmät). (Automation Standards Compliance Institute 2022, 11 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 29.)

Lopuksi turvallisuusvaatimusten tarkastelun osaprosessin tarkoituksena on varmistaa, että turvallisuusvaatimukset tarkastellaan, päivitetään ja hyväksytään. Tämän tarkoituksena on varmistaa, että turvallisuusvaatimukset ovat selkeitä, päteviä, yhteneväisiä tehdyn uhkamallinnuksen kanssa ja että niiden kelvollisuus on verifioitu eli vaatimukset ovat testattavissa tai muuten todennettavissa. Osaprosessin päämääränä on, että turvallisuusvaatimukset sisältävät vain päteviä, testattavia tai todennettavia vaatimuksia. (Automation Standards Compliance Institute 2022, 11 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 29.)

4.3 Turvallinen suunnittelu

Turvallinen suunnittelu on muotoiluperiaate, jossa turvallisuustoimet huomioidaan jo turvallisen tuotekehityksen elinkaaren varhaisessa vaiheessa eli tarkoituksena on luoda mahdollisimman vankat turvallisuusmenettelyt, -arkkitehtuurit ja -käytännöt ja noudattaa niitä koko elinkaaren ajan. Periaatteen tuloksena turvallisuustoimet toimivat sisäänrakennetusti järjestelmässä tai komponentissa ilman korvaavia toimenpiteitä. (International Society of Automation 2023, 9.) Turvallinen suunnittelu -käytännön tarkoituksena onkin varmistaa, että jo tuotteen määrittely- ja suunnitteluvaiheessa otetaan huomioon tarkoituksenmukaiset turvallisuusnäkökohdat. Käytännön pohjana toimii defense in depth -strategia eli syväsuojaussuunnittelu. Tämänkaltainen suunnittelu mahdollistaa useampikerroksisen turvallisuusratkaisun rakentamisen turvallisuusuhkia vastaan. Turvallisen suunnittelun käytäntöä sovelletaan kaikkiin suunnitteluvaiheisiin konseptisuunnittelusta yksityiskohtaiseen suunnitteluun ja myös suunnittelun eri tasoihin yleisestä arkkitehtuurista yksittäisen komponentin suunnitteluun. (IEC 62443-4-1:2018, 30; ISA Global Cybersecurity Alliance 2020, 12.) Turvallinen suunnittelu -käytännön vaatimukset ovat jaettu neljään osaprosessiin, jotka ovat lueteltu alla:

1. Turvallisen suunnittelun periaatteet (Secure design principles),
2. Syväsuojaussuunnittelu (Defense in depth design),
3. Turvallisen suunnittelun tarkastelu (Security design review) ja
4. Turvallisen suunnittelun parhaat käytännöt (Secure design best practices).

(ISA Global Cybersecurity Alliance 2020, 12.)

Turvallisen suunnittelun periaatteet -osaprosessissa tuotetoimittajan on varmistettava, että heillä on käytössään dokumentoitu turvallisen kehittämisen prosessi, jossa tunnistetaan ja kuvataan kaikki tuotteen

rajapinnat mukaan lukien niin fyysiset, kuten fyysiset tai langattomat yhteydet (esim. Ethernet) ja laitteet, kuin loogiset rajapinnat, kuten tietovirrat tuotteen komponenttien välillä (esim. sovellusten välinen viestintä). (Automation Standards Compliance Institute 2022, 12 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 30.) Osaprosessin tarkoituksena on varmistaa, että tuotetoimittaja tarkastelee kattavasti tuotteen sisäisiä ja ulkoisia rajapintoja, jotta voidaan taata kattava resurssien suojaus. Käytännössä tämä tarkoittaa, että tuotteen rajapinnat tunnistetaan ja rajapinnoissa tapahtuva vuorovaikutus kuvataan. Lisäksi määritellään, mitä turvallisuusmekanismeja rajapintojen suojaamiseksi on suunniteltu ja mitkä resurssit voivat vaarantua rajapintojen vaillinaisesta suojauksesta. (IEC 62443-4-1:2018, 30–31.)

Syväsuojauksen suunnittelun osaprosessissa varmistetaan, että tuotetoimittajalla on käytössään prosessi, jolla varmistetaan, että tuotteelle on toteutettu riskiperustainen monitasoinen puolustus perustuen uhkamallinnukseen. Syväsuojauksessa turvallisuusrakenteet rakennetaan siten, että ne kerrostuvat toistensa päälle, minkä tarkoituksena on estää tai viivästyttää mahdollista hyökkäystä. Tähän sisältyy myös hyökkäysten havaitsemisen keinot. Jokaisen suojauskerroksen täytyy tarjota lisäpuolustusmekanismeja ja jokaiseen kerrokseen sovelletaan turvallisen suunnittelun periaatteita. Jokaisen kerroksen tarkoituksena on myös pienentää myöhempien kerrosten hyökkäyspinta-alaa. Tällaisen rakenteen hyötynä on, että ylempi kerros suojaa alempia kerroksia, jolloin yhden kerroksen vaarantuminen ei vaaranna koko systeemiä. Syväsuojauksessa on kuitenkin erityisesti huomioitava haavoittuvuudet, jotka voivat vaarantaa useamman kerroksen suojaustoimet. (Automation Standards Compliance Institute 2022, 12 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 31–32; International Society of Automation 2023, 9.)

Turvallisen suunnittelun tarkastelun osaprosessin tarkoituksena on, että tuotetoimittajalla on prosessi turvallisen suunnittelun tarkasteluun. Tarkastelun tarkoituksena on tunnistaa, jäljittää ja kuvata turvallisuuteen liittyvät ongelmat jokaisen merkittävän versiomuutoksen yhteydessä. Käytännössä tarkastelussa huomioidaan, onko tuotteen syväsuojauksen suunnittelussa jätetty riittämättömälle huomiolle joitain tuotteen turvallisuusvaatimuksia, ja onko olemassa hyökkäysvektoreita, jotka kykenevät ohittamaan tuotteen syväpuolustuksen tai muuten läpäisemään sen. Osaprosessin tarkoituksena on varmistaa, että suunnittelu vastaa tuotteen vaatimuksiin ja uhkiin. Lisäksi tarkoituksena on varmistaa, että suunnittelussa noudatetaan parhaita käytäntöjä. Havaitut puutteet tunnistetaan, kuvataan, dokumentoidaan ja käsitellään. (Automation Standards Compliance Institute 2022, 13 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 32.)

Lopuksi tuotetoimittajalla on oltava prosessi, jolla varmistetaan, että turvallisen suunnittelun parhaat käytännöt (ks. luku 2 turvallisen kehityksen elinkaari) on dokumentoitu ja ne on otettu käyttöön suunnitteluprosessissa (turvallisen suunnittelun parhaat käytännöt -osaprosessi). Tarkoituksena on tarjota tuotteen kehittäjille ohjeistus, jonka avulla voidaan välttää yleisimmät virheet, jotka voisivat johtaa myöhemmin ilmeneviin turvallisuusongelmiin. Parhaiden käytäntöjen on perustuttava yleisesti hyväksyttyihin parhaisiin tietoturvakäytäntöihin, mutta tuotetoimittaja määrittelee itse käytännöt, jotka soveltuvat parhaiten sen omiin suunnittelukäytäntöihin. Määriteltyjä parhaita käytäntöjä voidaan soveltaa niin laitteiston kuin ohjelmiston suunnitteluun. Lisäksi näitä käytäntöjä tarkastellaan ja päivitetään säännöllisesti. Tuotetoimittaja ylläpitää käytäntöjä saatujen kokemusten ja alan muutosten mukaisesti. (Automation Standards Compliance Institute 2022, 13 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 32–33.)

4.4 Turvallinen toteutus

Turvallisen toteutuksen käytännön tarkoituksena on varmistaa, että tuotteen toiminta ja turvallisuustoimenpiteet ovat toteutettu turvallisesti. Turvallinen toteutus -käytännön vaatimukset koskevat kaikkia tuotteen laitteisto- ja ohjelmistokomponentteja pois lukien ulkoiset komponentit, joiden vaatimukset ovat määritelty turvallisuuden hallinta -käytännössä. (IEC 62443-4-1:2018, 33; ISA Global Cybersecurity Alliance 2020, 12.) Käytännön vaatimukset jakaantuvat kahteen osaprosessiin:

1. Turvallisuuden toteutuksen tarkastelu (Security implementation review) ja
2. Turvallisen koodauksen standardit (Secure coding standards).

(ISA Global Cybersecurity Alliance 2020, 12.)

Turvallisuuden toteutuksen tarkastelun osaprosessin tarkoituksena on varmistaa, että tuotetoimittajalla on käytössään prosessi toteutuksen tarkasteluun. Tarkastelussa tunnistetaan, jäljitetään ja kuvataan toteutuksessa ilmenneet turvallisuusongelmat. Päämääränä on varmistaa, että toteutuksessa on huomioitu turvallinen suunnittelu ja siihen liittyvät turvallisuusvaatimukset, ja että toteutuksessa on noudatettu parhaita käytäntöjä. Käytännössä tuotetoimittajan on toteutettava mahdollisimman kattavat turvallisuustarkastelut toteutukselle ja sen rakenteelle. Kattava tarkastelu sisältää useantyyppisiä tarkasteluita, joista jokainen vastaa eri päämääriin. Esimerkiksi manuaalisella tarkastelulla voidaan verifioida, että toteutus täyttää vaatimukset ja että toteutus suojaa odotetuilta uhilta. (Automation Standards Compliance Institute 2022, 14 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 33–34.)

Turvallisen koodauksen standardit -osaprosessissa vaaditaan, että toteutusprosessissa noudatetaan dokumentoituja turvallisen koodauksen standardeja. Näitä standardeja on myös tarkasteltava ja päivitettävä säännöllisesti. Minimissään turvallisen koodauksen standardit sisältävät seuraavat kohdat: vältetään turvattomia rakenteita, malleja ja ohjelmistotoimintoja, vältetään kiellettyjä toimintoja ja rakenteita tai malleja, käytetään automaattisia työkaluja ja asetuksia, noudatetaan turvallisia koodauksen käytäntöjä, validoidaan luottamusrajat ylittävät syötteet ja käsitellään virheet. Osaprosessin tarkoituksena on tarjota kehittäjille ohjeistus, jonka avulla voidaan välttää yleisimmät virheet, jotka voisivat johtaa myöhemmin ilmeneviin turvallisuusongelmiin. Koodausstandardien täytyy perustua yleisesti hyväksyttyihin parhaisiin käytäntöihin, mutta tuotetoimittaja määrittelee itse koodausstandardit, jotka soveltuvat parhaiten sen omiin koodaus- ja suunnittelukäytäntöihin. Tuotetoimittajan koodausstandardeja ylläpidetään saatujen kokemusten ja alan muutosten mukaisesti. (Automation Standards Compliance Institute 2022, 15 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 33–34.)

4.5 Turvallisuuden verifiointi- ja validointitestaus

Turvallisuuden verifiointi- ja validointitestauksen käytännössä varmistetaan, että tuotteen turvallisuusvaatimukset täyttyvät, tuotteen turvallisuutta ylläpidetään käytettäessä sitä turvallisuuskontekstissaan ja että tuote on konfiguroitu syväsuojauksen mukaisesti. Testauksia voidaan suorittaa turvallisen tuotekehityksen elinkaaren eri vaiheissa riippuen testauksen tyypistä ja kehitysprosessin mallista. Testauksia voivat toteuttaa useat eri henkilöt. Esimerkiksi fuzz-testaus voidaan toteuttaa jo ohjelmiston kehitysvaiheessa kehitystiimin toimesta ja sama testaus voidaan toistaa kehityssyklin myöhemmässä vaiheessa testaustiimin toimesta. (IEC 62443-4-1:2018, 34–35; ISA Global Cybersecurity Alliance 2020, 12.) Testaukset suunnitellaan, dokumentoidaan, suoritetaan ja testien tulokset raportoidaan (Mikhaleva 2022, 55). Käytännön vaatimukset jakaantuvat viiteen osaprosessiin, jotka ovat lueteltu alla:

1. Turvallisuusvaatimusten testaus (Security requirements testing),
2. Uhkien lieventämisen testaus (Threat mitigation testing),
3. Haavoittuvuuksien testaus (Vulnerability testing),
4. Läpäisytestaus (Penetration testing) ja
5. Testaajien riippumattomuus (Independence of testers).

(ISA Global Cybersecurity Alliance 2020, 12.)

Turvallisuusvaatimusten testauksessa verifioidaan, että tuotteen turvallisuustoiminnot vastaavat turvallisuusvaatimuksia. Lisäksi verifioidaan, että tuote pystyy käsittelemään oikein virhetilanteet ja virheelliset syötteet. Testauksen pitäisi sisältää mm. turvallisuusvaatimusten funktionaalisen testauksen, suorituskyvyn ja skaalautuvuuden testauksen sekä odottamattomien ja virheellisten syötteiden testauksen. Testauksella todennetaan, että tuote täyttää dokumentoidut turvallisuusvaatimukset. (Automation Standards Compliance Institute 2022, 16 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 35.)

Uhkien lieventämisen testauksessa testataan uhkamallinnuksessa tunnistettujen uhkien lieventämisen tehokkuus. Testaustoimilla varmistetaan, että tietyn uhan lieventämiseen tarkoitetuille toimille on suoritettu riittävät testaukset ja että toimet ovat toimineet suunnitellun mukaisesti. Lisäksi täytyy testata, miten uhkia voidaan hyödyntää haitallisesti ja miten uhkien lievennystoimia voidaan ehkäistä (tässä voidaan käyttää esim. STRIDE-mallia). Testauksen tarkoituksena on varmistaa, että tuotteen syväsuojaus ja uhkien lieventämistoimenpiteet ovat tehokkaita. (Automation Standards Compliance Institute 2022, 16 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 35.)

Turvallisuuden verifiointi- ja validointitestaus -käytännön haavoittuvuuksien testaus ja läpäisytestaus liittyvät tuotteen haavoittuvuuksiin. Haavoittuvuuksien testauksen osaprosessissa suoritetaan testejä, joiden avulla voidaan tunnistaa ja kuvata tuotteen mahdollisia haavoittuvuuksia turvallisuuden kannalta. Tunnettujen haavoittuvuuksien testauksen on perustuttava viimeisimpiin, alalla tunnustettuihin ja julkisiin haavoittuvuuksiin. Standardissa on lueteltu useita määritelmiä ja testausmenetelmiä, joita haavoittuvuustestauksen on sisällettävä, mm. hyökkäyspinta-alan analyysi, fuzz-testaus, virheellisten tai odottamattomien syötteiden testaus ja black box -testaus. Läpäisytestauksen osaprosessin tarkoituksena on, että tuotetoimittajalla on käytössään testausmenetelmät, joiden avulla se kykenee löytämään tuotteen tai tuotedokumenttien mahdollisesti sisältämiä turvallisuusongelmia. Läpäisytestauksessa keskitytään nimenomaan tietoturva-aukkojen (haavoittuvuuksien) löytämiseen ja niiden hyväksikäyttöön. Läpäisytestauksella halutaan varmistaa, että tietoturva-aukkojen löytämiseen on panostettu riittävästi. (Automation Standards Compliance Institute 2022, 17–18 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 36–37.)

Testaajien riippumattomuus osaprosessin tarkoituksena on varmistaa, että tuotteen testaajat ovat tarvittaessa riippumattomia. Käytännössä tämä tarkoittaa, että testaaja on riippumaton tuotteen kehittäjästä. Vaatimus testaajan riippumattomuudesta riippuu suoritettavasta testauksesta. Itsenäisen testaajan käyttö voi edesauttaa vikojen ja ongelmien, jotka muuten olisivat jääneet huomaamatta, löytämisessä. Itsenäisen testaajan näkökulma tuotteeseen on erilainen kuin kehitystiimiin jäsenellä tai testaajalla, joka on

taustaltaan ohjelmoija. Lisäksi itsenäinen testaaja voi tuoda havaintonsa esille rehellisesti ja puolueettomasti. (Automation Standards Compliance Institute 2022, 18–19 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 37.)

4.6 Turvallisuusongelmien hallinta

Turvallisuusongelmien hallinnan käytännön tarkoituksena on hallita tuotteen, jonka konfigurointi on tehty syväsuojauksen mukaisesti turvallisuuskontekstissaan, turvallisuusongelmia. Käytännön vaatimukset ovat jaettu kuuteen osaprosessiin, jotka ovat lueteltu alla:

1. Turvallisuusongelmiin liittyvien ilmoitusten vastaanottaminen (Receiving notifications of security-related issues),
2. Turvallisuusongelmien tarkastelu (Reviewing security-related issues),
3. Turvallisuusongelmien arviointi (Assessing security-related issues),
4. Turvallisuusongelmien käsittely (Addressing security-related issues),
5. Turvallisuusongelmien esiintuominen (Disclosing security-related issues) ja
6. Määräajoin tehtävä turvallisuusvikojen hallintakäytäntöjen tarkastelu (Periodic review of security defect management practice).
   (ISA Global Cybersecurity Alliance 2020, 12.)

Tuotetoimittajalla on oltava dokumentoitu prosessi turvallisuusongelmiin liittyvien sisäisten ja ulkoisten ilmoitusten vastaanottamiseen ja ilmoitettujen turvallisuusongelmien jäljittämiseen (turvallisuusongelmiin liittyvien ilmoitusten vastaanottamisen osaprosessi). Tuotetoimittajalla on oltava helposti saatavissa olevat ohjeistukset turvallisuusongelmien raportointiin niin sisäisille kuin ulkoisille ilmoittajille. Ohjeet voidaan esimerkiksi sisällyttää tuotedokumentaatioon ja tuotetukiverkkosivustolle. Tuotetoimittajan on varmistettava, että ilmoitetut turvallisuusongelmat tutkitaan viipymättä, jotta voidaan määrittää niiden soveltuvuus tuotteeseen, todennettavuus ja uhat, jotka laukaisevat ongelman (turvallisuusongelmien tarkastelun osaprosessi). Osasprosessin tarkoituksena on varmistaa, että tuotetoimittaja tarkistaa ja tutkii kaikki sille ilmoitetut turvallisuusongelmat. Näin varmistetaan, onko ilmoitettu ongelma todellinen ja soveltuuko se tuotteeseen vai onko ilmoitus perusteeton. (Automation Standards Compliance Institute 2022, 20 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 38–39.)

Tuotteen vahvistetut turvallisuusongelmat analysoidaan (turvallisuusongelmien arvioinnin osaprosessi). Analysointiin kuuluu ongelmien vaikutusten arviointi suhteessa turvallisuuskontekstiin, jossa ongelma havaittiin, tuotteen turvallisuuskontekstiin ja syväsuojaussuunnitelmaan. Analyysissa arvioidaan ongelman vakavuus, tunnistetaan muut tuotteen versiot, joissa ongelma voi esiintyä, tunnistetaan ongelman pohjimmainen syy ja tunnistetaan ongelmaan liittyvät muut turvallisuusongelmat. Osaprosessin tarkoituksena on varmistaa, että tuotetoimittaja arvioi turvallisuusongelman vaikutukset ja vakavuuden, määrittelee, missä tuotteissa tai tuoteversioissa ongelma esiintyy ja tunnistaa ongelman perimmäisen syyn tai syyt. Näin toimien voidaan määritellä keinot ongelman ratkaisemiseksi, ja mitä turvallisen tuotekehityksen elinkaariprosesseja voidaan ratkaisussa hyödyntää, kuten uhkamallinnuksen päivitys. (Automation Standards Compliance Institute 2022, 20 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 39.)

Turvallisuusongelmat käsitellään ja turvallisuusongelmien vaikutusten arvioinnin perusteella määritellään, onko ongelmista raportoitava (turvallisuusongelmien käsittelyn osaprosessi). Tuotetoimittaja määrittelee jäännösriskin hyväksyttävän tason, kun määritellään tapoja käsitellä turvallisuusongelmia. Turvallisuusongelmien käsittelyyn on monia eri vaihtoehtoja, joista voidaan valita yksi tai useampi:

- ongelma korjataan syväsuojaussuunnitelulla tai muuttamalla rakennetta, lisäämällä turvallisuusvaatimuksia ja/tai -ominaisuuksia, käyttämällä korvaavia menetelmiä ja/tai poistamalla käytöstä tai poistamalla ominaisuuksia,
- tehdään korjaussuunnitelma ongelman korjaamiseksi,
- siirretään ongelmanratkaisu myöhempään ratkaisuun, täsmennetään ongelman syyt ja niihin liittyvät riskit ja/tai
- ongelmaa ei korjata, mikäli jäännösriski on alle hyväksyttävissä olevan tason. (Automation Standards Compliance Institute 2022 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 40.)

Kaikissa tapauksissa kuitenkin informoidaan muita prosesseja ongelmasta tai siihen liittyvistä ongelmista mukaan lukien muut tuotteet tai tuoteversiot sekä informoidaan kolmansia osapuolia, mikäli heidän lähdekoodinsa on osana löydettyä ongelmaa. Ongelmien ratkaisun jälkeen arvioidaan, miten vastaavat ongelmat voitaisiin välttää. Prosessiin kuuluu säännöllinen avointen turvallisuusongelmien tarkastelu, jonka tarkoituksena on varmistaa, että ongelmat käsitellään asianmukaisesti. Säännöllinen tarkas-

telu suoritetaan vähintään jokaisen julkaisun tai iterointisyklin aikana. Osaprosessilla halutaan varmistaa, ettei yksikään turvallisuusongelma jää käsittelemättä. Tuotetoimittajan onkin tarkasteltava jokainen turvallisuusongelma ja sen mahdollinen jäännösriski, joiden pohjalta voidaan tehdä perustellut päätökset ongelman korjaamisesta. Jäännösriskin arvioinnissa voidaan hyödyntää esim. CVSS-pisteytystä. Päätettäessä keinoja turvallisuusongelman ratkaisemiseksi on huomioitava myös ratkaisun mahdolliset vaikutukset tuotteeseen esim. mahdolliset ei-hyväksyttävät sivuvaikutukset, ratkaisun hyöty, ratkaisun monimutkaisuus ja vaikutukset tuotteen muuhun rakenteeseen. (Automation Standards Compliance Institute 2022, 20 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 40–41.)

Tuotetoimittajalla pitää olla prosessi informoida tuotteen käyttäjiä raportoitavista turvallisuusongelmista viipymättä (turvallisuusongelmien esiintuomisen osaprosessi). Ilmoituksessa kuvataan ongelma, pisteytetään haavoittuvuus joko CVSS:n tai muun vastaavan pisteytyksen mukaan, ilmoitetaan tuoteversiot, joita ongelma koskee, ja kuvataan ongelman ratkaisu. Markkinavoimat ohjaavat, kuinka nopeasti ongelmista on raportoitava ja myös, kuinka nopeasti korjausten on oltava saatavissa. Osaprosessin tarkoituksena on varmistaa, että käyttäjiä informoidaan turvallisuusongelmista, joiden vakavuus on arvioitu sen verran korkeaksi, että niistä on informoitava tuotteen käyttäjiä, ja niiden ratkaisuista. Tuotetoimittajalla onkin oltava prosessi informoinnin tarpeen arvioimiseksi. (Automation Standards Compliance Institute 2022, 20 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 41.)

Tuotetoimittajan on vuosittain tarkasteltava turvallisuusongelmien hallintaprosessia. Prosessin tarkastelussa tarkastellaan vähintään, miten prosessin avulla on vuoden aikana onnistuttu hoitamaan turvallisuusongelmia. Tarkastelussa tarkastellaan, käytiinkö prosessi loppuun asti, oliko prosessi tehokas ja johtiko prosessi turvallisuusongelman ratkaisuun. Osaprosessin päämääränä on, että turvallisuusongelmien hallintaprosessia kehitetään ja parannetaan jatkuvasti. (Automation Standards Compliance Institute 2022, 21 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 42.)

4.7 Tietoturvapäivitysten hallinta

Tietoturvapäivitysten hallinnan käytännöllä tahdotaan varmistaa, että tuotteeseen liittyvät tietoturvapäivitykset (laitteisto-, laiteohjelmisto- ja ohjelmistopäivitys) ovat testattu regressioiden varalta ja että ne ovat tuotteen käyttäjien saatavissa ajallaan. Käytännön vaatimukset ovat jaettu viiteen osaprosessiin, jotka ovat lueteltu alla:

1. Tietoturvapäivitysten hyväksyntä (Security update qualification),
2. Tietoturvapäivitysten dokumentaatio (Security update documentation),
3. Riippuvaisen komponentin tai käyttöjärjestelmän päivitysten dokumentointi (Dependent component or operating system update documentation),
4. Tietoturvapäivitysten jakelu (Secure update delivery) ja
5. Tietoturvakorjausten oikea-aikainen jakelu (Timely delivery of secure patches).

(ISA Global Cybersecurity Alliance 2020, 13.)

Tuotetoimittajalla on oltava prosessi, jolla verifioida, että sen tietoturvapäivitykset kohdistuvat päivityksen kohteena olleisiin tietoturvahaavoittuvuuksiin ja että päivitykset eivät sisällä regressioita (tietoturvapäivitysten hyväksynnän osaprosessi). Nämä vaatimukset pätevät tuotekehittäjän ja kolmansien osapuolien tietoturvapäivityksiin. Lisäksi varmistetaan, että päivitykset eivät ole ristiriidassa toiminnallisten, turvallisuuden tai laillisten rajoitusten kanssa. Osaprosessin tarkoituksena on varmistaa, että tietoturvapäivitykset ovat päteviä, yleensä testausten kautta, ja todentaa, että päivitykset eivät vaaranna tuotteen toimintaa tai syväsuojausta esim. ei-toivottujen sivuvaikutusten kautta. Kaikkien tuotteiden ja tuoteversioiden tietoturvapäivitykset tulevat olla käyttäjien saatavissa siten, että organisaatiossa voidaan varmistaa käyttäjille päivitysten aitous (tietoturvapäivitysten jakelun osaprosessi). Tietoturvapäivitykset on myös dokumentoitava ja dokumentin on oltava saatavissa tuotteen käyttäjille (tietoturvapäivitysten dokumentaation osaprosessi). Dokumentin on sisällettävä vähintään seuraavat tiedot:

- tuoteversio, jota tietoturvapäivitys koskee,
- ohjeet, miten päivitykset otetaan käyttöön manuaalisesti tai automaattisen prosessin kautta,
- kuvaus päivityksen vaikutuksista tuotteeseen,
- ohjeet, kuinka varmistetaan, että päivitys on otettu käyttöön, ja
- mitä riskejä päivityksen tekemättä jättämiseen tai sovellettujen päivitysten tekemiseen liittyy.

  (Automation Standards Compliance Institute 2022, 22 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 42–43.)

Tuotetoimittajan tehtävänä on varmistaa myös, että tuotteen käyttäjän saatavilla on dokumentti tuotteen ulkopuolisten komponenttien tai käyttöjärjestelmän, joista tuote on riippuvainen, tietoturvapäivityksistä

(riippuvaisen komponentin tai käyttöjärjestelmän päivitysten dokumentoinnin osaprosessi). Dokumentista on käytävä ilmi, että onko komponentin tai käyttöjärjestelmän tietoturvapäivitykset yhteensopivia tuotteen kanssa. Dokumentissa on käytävä myös ilmi tilanteet, joissa tuotetoimittaja ei ole hyväksynyt tietoturvapäivityksiä, ja mitä lievennyskeinoja voidaan käyttää tilanteessa, jossa kyseistä komponentin tai käyttöjärjestelmän tietoturvapäivitystä ei voida ottaa käyttöön. (Automation Standards Compliance Institute 2022, 22 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 43.)

Tuotetoimittajalla on oltava määriteltynä prosessi, jossa määritetään tietoturvapäivityksen aikaikkuna päivityksen hyväksymiselle ja käyttäjille jakamiselle (tietoturvakorjausten oikea-aikaisen jakelun osaprosessi). Prosessilla varmistetaan, että käytäntöä noudatetaan. Dokumentoidussa käytännössä huomioidaan vähintään haavoittuvuuden mahdolliset vaikutukset, onko haavoittuvuus julkisesti tiedossa ja onko sen hyväksikäytöstä julkaistu tietoa, tuotemäärä, jota haavoittuvuus koskee, ja onko haavoittuvuuden lieventämiseen keinoja päivityksen sijaan. Tavoiteaikataulu perustuu yleensä yllä lueteltuihin tekijöihin. Tavoiteaikataulu voi olla esim., että tietoturvapäivitys pitää olla saatavissa 30 päivän sisällä tietoturvahaavoittuvuuden löytymisestä. (Automation Standards Compliance Institute 2022, 22 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 44.)

4.8 Turvallisuusohjeet

Turvallisuusohjeet-käytännön tarkoituksena on tarjota käyttäjälle dokumentti, jossa kuvataan, miten tuote integroidaan ja konfiguroidaan sekä miten ylläpidetään tuotteen turvallisuuskontekstin mukaista syväsuojausta. Vaatimusten täyttämiseksi tuotetoimittajalla pitää olla määriteltynä prosessi dokumentin luomiseen, ylläpitämiseen ja jakamiseen. (IEC 62443-4-1:2018, 44; ISA Global Cybersecurity Alliance 2020, 13.) Käytännön vaatimukset jakaantuvat seitsemään osaprosessiin, jotka ovat lueteltu alla:

1. Tuotteen syväsuojaus (Product defense in depth),
2. Syväsuojauksen toimet, joita ympäristöltä odotetaan (Defense in depth measures expected in the environment),
3. Turvallisuuden koventamisen ohjeet (Security hardening guidelines),
4. Turvallisen hävityksen ohjeet (Secure disposal guidelines),
5. Turvallisen toiminnan ohjeet (Secure operation guidelines),
6. Tilihallinnan ohjeet (Account management guidelines) ja
7. Dokumentaation tarkastelu (Documentation review).

(ISA Global Cybersecurity Alliance 2020, 13.)

Tuotetoimittajan on luotava käyttäjille dokumentti, jossa kuvataan tuotteen syväsuojausstrategia tuotteen asennuksen, käytön ja ylläpidon tukemiseksi (tuotteen syväsuojauksen osaprosessi). Dokumentissa käsitellään tuotteen turvallisuusominaisuuksia ja niiden merkitystä syväsuojauksessa, uhat, jotka on huomioitu syväsuojauksessa, ja käyttäjän keinot lieventää tuotteen tunnettuja turvallisuusriskejä mukaan lukien vanhentunut lähdekoodi (legacy code). Osaprosessin tarkoituksena on varmistaa, että tuotetoimittajalla on olemassa dokumentaatio tuotteen syväsuojauksesta, joka tukee tuotteen koventamista (hardening) asiakkaan päässä. Päämääränä on, että dokumentti tarjoaa useita näkökohtia tuotteen syväsuojaukseen liittyen, jotta tuotetta voidaan koventaa asennuksen aikana ja että tuote säilyy kovennettuna koko sen käyttöiän ajan. Näitä näkökohtia ovat jäljelle jääneet uhat ja tuotteen turvallisuusominaisuudet tuotteen suojaamiseksi näitä uhkia vastaan sekä mahdolliset korvaavat toimenpiteet, joita voidaan käyttää tuotteen suojaamiseksi edelleen. Turvallisuusohjeet sisältävät käyttäjälle olennaiset tiedot turvallisuuteen liittyvistä riskeistä eli käytännössä turvallisuusriskeistä, jotka liittyvät tuotteen konfigurointiin, asennukseen ja ylläpitoon. Lisäksi käyttäjille kuvataan, mitä syväsuojauksen toimia odotetaan tuotteen ulkoiselta käyttöympäristöltä (syväsuojauksen toimet, joita ympäristöltä odotetaan -osaprosessi). (Automation Standards Compliance Institute 2022, 23 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 44–45.)

Tuotetoimittajan on annettava ohjeistuksia tuotteen koventamiseksi tuotteen asennuksen ja ylläpidon aikana (turvallisuuden koventamisen ohjeet -osaprosessi). Ohjeistusten on sisällettävä ohjeita, perusteluja ja suosituksia mm. tuotteen integroinnista turvallisuuskontekstissa, tuotteen syväsuojauksesta, turvallisuuden ylläpidon toimista ja tuotteen ylläpidon parhaista käytännöistä sekä hallinnasta. (Automation Standards Compliance Institute 2022, 23–24 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 45.) Osaprosessin tarkoituksena on varmistaa, että tuotetoimittaja luo käyttäjädokumentin, jossa annetaan ohjeistuksia tuotteen koventamiseksi asennuksen aikana ja kuinka pitää tuote kovennettuna koko tuotteen käyttöiän ajan. Turvallisuuskäytännöt ja asiakasvaatimukset ovat erilaisia, joten on tärkeää tarjota dokumentaatio, jolla voidaan tukea tuotteen turvallista integrointia, konfigurointia ja ylläpitoa. (IEC 62443-4-1:2018, 46.)

Tuotetoimittajan on luotava käyttäjälle (mukaan lukien järjestelmänvalvoja) dokumentti, jossa kuvataan käyttäjän vastuut ja tarvittavat toiminnot, jotta tuotetta voidaan käyttää turvallisesti (turvallisen toiminnan ohjeet -osaprosessi). Dokumentissa kuvataan myös käyttäjän oletettu toiminta ja suhde tuotteen turvalliseen käyttöön. Päämääränä on luoda dokumentti, jossa annetaan ohjeistuksia tuotteen turvallisesta

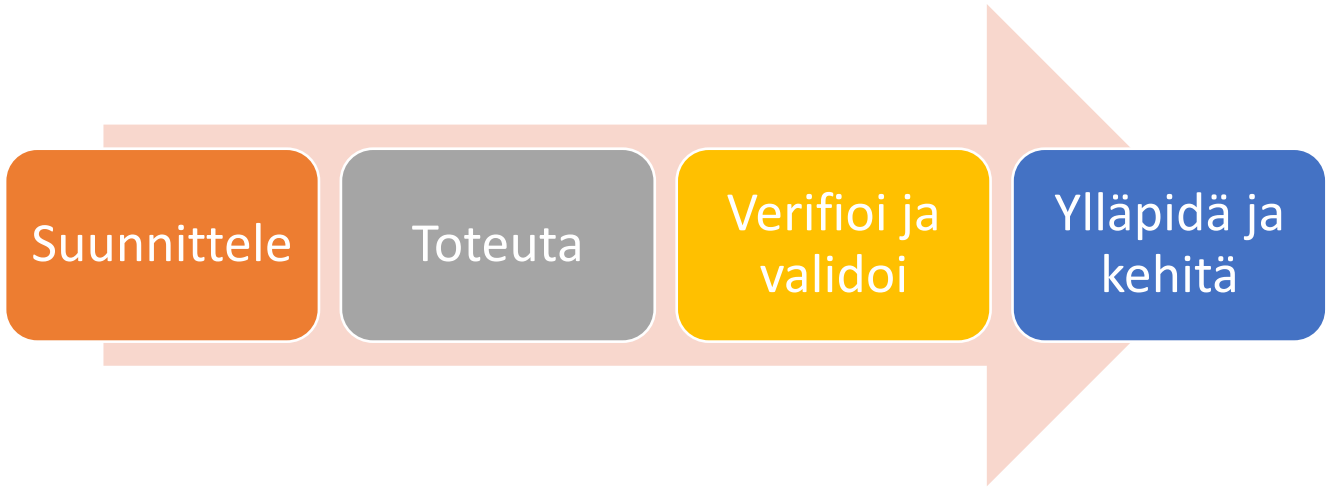
käytöstä esim. ohjeistuksia salasanojen ja varmenteiden hallintaan. Käyttäjälle on myös dokumentoidusti määriteltävä käyttäjätilien vaatimukset ja suositukset tuotteen käyttöön (tilihallinnan ohjeet -osaprosessi). Dokumentissa on käsiteltävä tuotteen käyttäjätilien pääsynhallinta ja käyttöoikeudet. Tähän lasketaan mukaan mm. käyttöjärjestelmien tilit, ohjausjärjestelmien tilit ja tietokantatilit. Dokumentissa on myös käsiteltävä tuotteen käyttämät oletustilit ja ohjeet siitä, kuinka oletustilin käyttäjätunnuksia ja salasanoja voidaan muuttaa. Päämääränä on, että tuotetoimittaja luo dokumentin, jossa määritellään käyttäjätilit ja oletustilit sekä niiden asetukset tuotteen käyttämiseksi. (Automation Standards Compliance Institute 2022, 24 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 46–47.)

Käyttäjälle on annettava myös ohjeistuksia tuotteen turvalliseen käytöstä poistamiseen (turvallisen hävityksen ohjeet -osaprosessi). Ohjeistukseen sisällytetään ohjeita ja suosituksia tuotteen poistamisesta ympäristöstään, ympäristöön tallennettujen viitteiden ja konfigurointidatan poistamisesta, tuotteeseen tallennetun datan turvallisesta poistamisesta sekä tuotteen turvallisesta hävityksestä, mikäli tuotteen kaikkia tietoja ei ole pystytty poistamaan. Osaprosessin tarkoituksena on, että tuotetoimittaja on luonut dokumentoidut ohjeistukset tuotteen käytöstä poistamiseen turvallisesti. Ohjeistuksen on tarjottava ohjeet tuotteen puhdistamiseksi arkaluontoisista, luottamuksellisista ja omistusoikeudellisista tiedoista ja ohjelmistoista. (Automation Standards Compliance Institute 2022, 24 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 46.)

Tuotetoimittajalla on oltava prosessi, jonka tarkoituksena on tunnistaa, jäljittää ja kuvata kaikki virheet ja puutteet kaikissa käyttäjäoppaissa mukaan lukien turvallisuusohjeistukset (dokumentaation tarkastelun osaprosessi). Tämän täytyy kattaa tuotteen turvallisuusominaisuudet, sisältää tuotteen integroinnin käyttöympäristöönsä ja vakuuttaa, että kaikki dokumentoidut käytännöt ovat turvallisia. Tarkoituksena on varmistaa, että tuotteen turvallisuuteen liittyvät dokumentit ovat täsmällisiä ja valmiita eikä turvattomia toimia ole dokumentoitu käyttäjädokumentteihin. Käytännössä on tarkasteltava, että dokumentissa on käsitelty kattavasti tuotteen turvallisuusominaisuudet ja kuvattu riittävällä laajuudella tuotteen syväsuojaus integroitaessa tuote turvallisuuskontekstiinsa. Lisäksi on varmistettava, että kaikki löydetyt poikkeavuudet käsitellään. (Automation Standards Compliance Institute 2022, 25 [ANSI/ISA 62443-4-1 2018]; IEC 62443-4-1:2018, 47.)

5 ISA/IEC 62443-4-1 STANDARDIN KÄYTTÖÖNOTTO

Opinnäytetyöprosessin aikana olen tutustunut turvallisen tuotekehityksen elinkaaren -käsitteeseen, teollisuusautomaatio- ja ohjausjärjestelmien elinkaaren tietoturvaa standardoivaan standardikokoelmaan ja erityisesti niissä käytettyjen tuotteiden turvallisen tuotekehityksen standardiin ISA/IEC 62443-4-1. Kyseinen standardi luettelee 47 eri vaatimusta, joten näin ollen herääkin kysymys, miten vaatimukset voidaan jalkauttaa käytäntöön. Tutkittuani turvallisen tuotekehityksen elinkaari -mallia ja sen standardia olen tullut siihen tulokseen, että standardin käyttöönotto voidaan tiivistää kuvion 7 mukaisiin askelmerkkeihin. Tätä näkemystä tukee myös ISO/IEC TR 33014:2020 standardi prosessien arvioinnista ja parantamisesta (SFS-ISO/IEC TR 33014:2020, 10).



KUVIO 7. Askelmerkit standardin ISA/IEC 62443-4-1 käyttöönottoon (mukaillen SFS-ISO/IEC TR 33014:2020, 10)

Tässä luvussa esittelen omat näkemykseni standardin käyttöönotosta kuvion 7 askelmerkkien mukaisesti. Nämä näkemykset ovat muodostuneet allekirjoittaneelle standardiin perehtymisestä ja sen tulkinnasta. Standardin vaatimusten integrointi organisaation tuotekehitysprosessiin voi olla haasteellista, mikä vaatiikin henkilöresursseja ja aikaa perehtyä standardiin sekä sen soveltamiseen käytännössä (Kanniah & Mahrin 2016, 3026). Lisäksi vaaditaan ymmärrystä, mihin standardin käyttöönotolla pyritään ja mitä sen käyttöönotolta toivotaan, eli mikä on organisaation haluama lopputulos. (Tuptuk & Hailes 2018, 101.) Liitteessä 1 olevaan tarkistuslistaan olen kirjannut omia näkemyksiäni, mitä käytännön toimia jokainen askel standardin käyttöönotossa voisi käytännössä organisaatiolta vaatia.

5.1 Suunnittele

Standardin käyttöönoton lähtökohtana on, että organisaatio on selkeästi määritellyt tuotteen tai tuotteen osat, johon turvallisen tuotekehityksen standardin vaatimuksia halutaan soveltaa. Standardin soveltaminen on mahdotonta, mikäli organisaatiolla ei ole selkeää käsitystä standardin sovelluksen kohteesta, koska standardi on kehitetty nimenomaan tuotekehitysprosessia ajatellen. Lisäksi on huomioitava, onko standardi ylipäätänsä sovellettavissa omaan tuotteeseen. Tämä on myös yksi standardin vaatimuksista (soveltuvuuden tunnistamisen osaprosessi). Soveltuvuutta on arvioitava, jotta vältytään turhalta työltä ja kustannuksilta.

Kun tuote on määritelty, on aika tarkastella tuotteen kehitysprosessia. Standardissa vaaditaan ja oletetaan, että organisaatiolla on valmiiksi määriteltynä tuotekehitysprosessi (kehitysprosessiosaprosessi). Ilman määriteltyä tuotekehitysprosessia, organisaatio ei pysty johdonmukaisesti kehittämään tuotteitaan tietyn prosessimallin mukaisesti ja toistamaan prosessejaan. Tällöin organisaation prosessit ovat ad hoc -tyyppisiä ja/tai dokumentoimattomia. Tuotekehitysprosessissa on oltava huomioituna tuotekehityksen elinkaarimalli, joka standardin mukaan on sisällettävä vähintään vaatimusmäärittelyn, suunnittelun, toteutuksen, testauksen ja ylläpidon. Lisäksi elinkaaressa huomioidaan myös aina tuotteen käytöstä poistaminen, joka on olennainen osa tuotteen turvallista elinkaarta. Tämä mainitaan myös standardissa ja tiedonhaun perusteella se sisällytetään yleisesti tuotekehityksen elinkaari -malliin. Organisaation on hyvä muistaa, että standardin käyttöönoton on tarkoitus laajentaa tuotteen elinkaarimallia turvallisuusnäkökohdilla eikä luoda täysin uutta tuotekehityksen prosessimallia, joten standardi tarvitsee rinnalleen myös varsinaisen tuotekehityksen elinkaarimallin. Kanniahin ja Mahrinin tutkimuksessa tämä todettiin yhdeksi tavaksi helpottaa turvallisen tuotekehityksen toteutumista organisaatiossa (Kanniah & Mahrin 2016, 3027).

Ennen standardin käyttöönottoa kannattaa myös tarkastella, että organisaation sisäiset prosessit ja käytännöt, kuten tietotekniikka- ja tietoturvapolitiikka, tukevat turvallisen tuotekehityksen elinkaarta. Kanniahin ja Mahrinin toteuttamassa tutkimuksessa tietoturvapolitiikat, standardit ja ohjeistukset olivat yksi syistä, joilla voi olla vaikutusta turvallisen ohjelmistokehityksen käytäntöjen käyttöönottoon. Tutkimuksen mukaan turvallisen ohjelmistokehityksen käyttöönoton onnistuminen on varmempaa, mikäli organisaatiolla on käytössään asianmukainen tietoturvapolitiikka ja asianmukaiset standardit sekä ohjeistukset. (Kanniah & Mahrin 2016, 3027.) Kuten luvussa 2 todettiin tietoturvapolitiikka ohjaa tietoturvan toteutumista tuotekehityksen elinkaaren aikana. Näin kehitystiimi ymmärtää, mitä siltä odotetaan (Kanniah & Mahrin 2016, 3027).

Huolehtimalla organisaation sisäisestä toiminnasta tuetaan lisäksi turvallista tuotekehitysprosessia ja tuotteen turvallisuutta. Tuotekehitysprosessin suojaamisella voidaan estää tuotteen haitallinen peukalointi tuotekehitysprosessin aikana. Tähän linkittyy mielestäni olennaisesti standardin vaatimus kehitysympäristön turvallisuudesta, jossa viitataan ISO 27001 ja 27002 standardeihin koskien organisaation tietoturvan hallintajärjestelmää. Näkökulmaan linkittyy myös vahvasti tuotekehitysympäristön tietoturvallisuudesta huolehtiminen fyysisesti. Tuotekehityksessä käytettyjen tilojen ja välineiden tietoturvallisuus on taattava. Tilojen fyysistä tietoturvaa voidaan lisätä mm. tilasuunnittelulla ja kulunvalvontajärjestelmillä. Kehitystyökaluja on tarkasteltava kriittisesti ja niissä on suosittava mahdollisimman turvallisia vaihtoehtoja. Lisäksi tutkimuksen mukaan on huolehdittava riittävästä koulutuksesta työkalujen käyttöön, jotta voidaan taata niistä saatava hyöty, ja etteivät kehitystyökaluihin panostetut rahalliset resurssit mene hukkaan (Kanniah & Mahrin 2016, 3025). Huolehtimalla kehitysympäristön turvallisuudesta täytetään myös standardin vaatimukset tiedostojen eheydestä ja yksityisten avainten hallinnasta.

Ennen varsinaista standardin käyttöönoton toteutusta olisi hyvä myös tarkastella oman organisaation rooleja ja vastuita. Tarkastelussa tulee miettiä, mikä on oman organisaation rooli tuotekehitysprosessissa eli toimitaanko esim. alihankkijana toiselle tuotetoimittajalle vai onko organisaatio itse pääasiallinen tuotetoimittaja. Lisäksi organisaation on mietittävä, onko se tuotetoimittajana yksin vastuussa tuotekehitysprosessista vai käytetäänkö kehitysprosessissa myös ulkopuolisia toimijoita. Mikäli kehitysprosessissa on mukana ulkopuolisia toimijoita, mitkä ovat heidän roolinsa ja vastuunsa. Tähän liittyy myös, että organisaatio tunnistaa, mikäli sen tuotteessa käytetään kolmannen osapuolen komponentteja tai räätälöityjä komponentteja, jolloin näihin komponentteihin on sovellettava standardin vaatimuksia siinä määriteltyjen kriteerien mukaisesti (turvallisuusvaatimukset ulkoisesti toimitetuille komponenteille ja kolmannen osapuolen räätälöidyt komponentit -osaprosessit).

Roolien ja vastuiden tunnistamisen lisäksi organisaation on arvioitava, onko sen henkilöstöllä riittävää asiantuntemusta standardissa esitettyjen vaatimusten toteuttamiseksi (turvallisuusasiantuntemusosaprosessi). Organisaation on varmistettava, että henkilöstöllä on tarvittavat pätevyydet tehtäviensä suorittamiseksi, ja organisaation on oltava valmis tarvittaessa tarjoamaan lisäkoulutusta. Henkilöstön asianmukaiseen perehdyttämiseen ja koulutukseen on panostettava niin yleisellä tasolla kuin tehtäväkohtaisella tasolla. Kanniahin ja Mahrininin tutkimuksen mukaan turvallisen ohjelmistokehityksen toteuttamiseksi täytyy kehittäjien ymmärtää erilaisia tietoturvauhkia ja heiltä vaaditaan tietoa sekä taitoa toteuttaa turvallisen tuotekehityksen käytäntöjä (Kanniah & Mahrin 2016, 3025). Kehittäjien asiantuntemuksen puute voi johtaa ohjelmistojen tahattomien haavoittuvuuksien luomiseen (Bartsch 2011).

Näin ollen ja standardiin perehdyttyäni olen sitä mieltä, että organisaatiossa on oltava ymmärrystä yleisesti turvallisen tuotekehityksen elinkaaren perusteista ja standardin vaatimuksista ennen varsinaista standardin käyttöönottoa. Käytännössä tämä tarkoittaa, että standardin sisältöön ja turvallisen tuotekehityksen elinkaari -malliin olisi hyvä tutustua ja perehtyä ennakolta. Tutkimuksen mukaan organisaation tietoisuutta turvallisesta tuotekehityksestä on lisättävä, jotta voidaan varmistaa turvallisen tuotekehityksen tuki (Kanniah & Mahrin 2016, 3025). Tiedonhaun perusteella voin todeta, että mm. Youtube tarjoaa useita videoita, joista voi ammentaa yleiskäsitystä turvallisen tuotekehityksen elinkaaresta ja ISA/IEC 62443 -standardikokoelmasta. Lisäksi mm. ISA tarjoaa yleistietoa standardikokoelmasta ja sen tytäryhtiön ylläpitämistä standardikokoelman sertifiointiohjelmista, kuten SDLA-sertifiointiohjelmasta, joka perustuu ISA/IEC 62443-4-1 standardiin.

Suunnitteluvaiheessa kannattaa myös tutustua yleispäteviin ja oman erikoisalan standardeihin, parhaisiin käytäntöihin ja suosituksiin. Itse ISA/IEC 62443-4-1 standardi sisältää useita viittauksia muihin standardeihin. Yleispäteviä standardeja ovat esim. ISO/IEC 27034, ISO 27001 ja 27002, ISO/IEC 30111 ja ISO/IEC 29147. Lisäksi hyviä käytäntöjä ja vinkkejä mm. ohjelmointiin saa OWASP-säätiön julkaisemista ohjeistuksista, käytännöistä ja muista julkaisuista. Esimerkiksi OWASP SAMM -viitekehys auttaa parantamaan turvallisen ohjelmistokehityksen elinkaarta ja OWASP top 10 listaa yleisimpiä verkkoohjelmistojen turvallisuusriskejä. Asianmukaista tietoa voi myös ammentaa NIST:n julkaisuista. NIST tuottaa ja kehittää kyberturvallisuuden standardeja, ohjeistuksia ja parhaita käytäntöjä Yhdysvalloissa. Microsoft tarjoaa myös verkkosivustollaan tietoa omasta turvallisen tuotekehityksen elinkaaresta, työkaluja ja erilaisia koulutusmateriaaleja esim. uhkamallinnuksesta. Myös ISA/IEC 62443 -standardikokoelman muihin osiin tutustumisesta saa lisätietoa, jota voidaan hyödyntää. Erityisesti standardikokoelman yleisosa voi tarjota organisaatiolle hyvää pohjatietoa määritelmistä, termeistä ym., mikä voi lisätä ymmärrystä osan 4-1 käyttöönottoon.

Lopuksi organisaatiossa on arvioitava, onko organisaation tavoitteena sertifioida oma tuotekehitysprosessinsa. Jos organisaatiolla ei ole aikomusta sertifioida tuotekehitysprosessiaan juuri sillä hetkellä, mutta se haluaa syystä tai toisesta noudattaa standardin vaatimuksia, voi standardin hankkia organisaation käyttöön ostamalla virallisen standardin esim. SFS Suomen Standardit ry:ltä. Standardin hinta on reilu 300 euroa. ISASecure tarjoaa myös verkkosivustollaan (www.isasecure.org) tekniset tiedot koskien omaa SDLA-sertifiointiohjelmaansa, jossa käydään läpi standardin vaatimukset ja käytännön esimerkkejä, kuinka vaatimukset voidaan täyttää SDLA-sertifiointiohjelman mukaisesti. Mikäli organisaatio haluaa sertifioida tuotekehitysprosessinsa, löytyy sertifioimiseen useita eri vaihtoehtoja. Tiedonhaun perusteella monet sertifiointielimet ovat rakentaneet oman sertifiointiohjelmansa standardin pohjalta,

mutta kaksi yleisintä sertifiointielinten tarjoamaa sertifiointiohjelmaa ovat IECEE:n teollisuuden kyberturvallisuuden ohjelma ja ISASecure SDLA -sertifiointiohjelma (Mikhaleva 2022, 23).

5.2 Toteuta

Kun organisaatiossa on tehty alustavat toimenpiteet, suunnitelma ja päätös standardin käyttöönottamisesta, on aika lähteä toteuttamaan standardin integroimista osaksi määriteltyä tuotekehitysprosessia. Nyt organisaation onkin aika paneutua turvalliseen tuotekehitysprosessiin liittyviin yksityiskohtiin. Standardin toteuttamisen lähtökohtana on tuotteen vaatimusmäärittely, toimintojen, rakenteen, käyttötarkoituksen ja -ympäristön määrittely. Turvallisessa tuotekehityksessä tämä tarkoittaa turvallisuusominaisuuksien, turvallisen rakenteen ja turvallisuuskontekstin huomioimista osana tuotteen määrittely- ja suunnitteluprosessia (tuotteen turvallisuuskontekstin ja turvallisuusvaatimusten osaprosessit). Organisaation onkin mietittävä, mitä turvallisuusvaatimuksia tuotteelta itseltä vaaditaan, esim. käsitteleekö tuote arkaluontoista dataa tai kommunikoiko tuote jonkin muun komponentin kanssa, joka mahdollistaa pääsyn edellä mainittuihin tietoihin, ja/tai mitä turvallisuusominaisuuksia vaaditaan suhteessa tuotteen turvallisuuskontekstiin, esim. minkälaisia turvallisuusominaisuuksia tuotteen tuleva käyttöympäristö tarjoaa. Lisäksi määrittelyssä huomioidaan oman alan lainsäädäntö, eli asettaako lainsäädäntö jotain vaatimuksia tuotteelle. Kun tarvittavat määrittelyt on tehty, toteutetaan tarvittavat mallinnukset tuotteesta ja sen käytöstä mm. tietovirtakaavio.

Myös Kanniahin ja Mahrinin tutkimuksen mukaan turvallisen tuotekehityksen toteuttaminen vaatii selkeiden, kattavien, johdonmukaisten ja yksiselitteisten turvallisuusvaatimusten määrittämistä. Tutkimuksen mukaan tämä helpottaa eri sidosryhmien (käyttäjät ja kehittäjät) kykyä ymmärtää, mitä turvallisuusvaatimuksia tarvitaan toivotunlaisen tuotteen toteuttamiseksi. Näin ollen vaatimuksiin sisältyy myös sidosryhmien tunnistaminen. Tätä työtä helpottaa myös edellä mainittu tietoturvapolitiikka ja eri standardien hyödyntäminen. Riittämättömästä vaatimusmäärittelystä voi seurata, että turvallisen tuotekehityksen käytäntöjä ei noudateta tuotekehitysprosessissa. (Kanniah & Mahrin 2016, 3027.)

Uhkamallinnus on yksi ISA/IEC 62443-4-1 standardin pääkäsitteistä ja standardin vaatimuksista (uhkamallinnuksen osaprosessi). Uhkamallinnuksen tarkoituksena on tunnistaa turvallisuusongelmat mahdollisimman varhaisessa vaiheessa tuotekehitysprosessia. Uhkamallinnuksen toteutus voidaan jakaa neljään pääasialliseen vaiheeseen: tuotteen määrittely ja suunnittelu, uhkien tunnistaminen, turvallisuustoimen-

piteiden määrittely ja toteutus, toimien verifiointi ja validointi (Conklin 2024; Microsoft 2024b; Microsoft 2024c). Uhkamallinnus on olennainen osa tuotekehitystä ja sitä voidaan täydentää ja tarkentaa tuotekehitysprosessin edetessä sekä täten lieventää tuotteen turvallisuusriskejä entisestään. Uhkamallinnusta voidaan käyttää turvallisen suunnittelun pohjana, mutta toisaalta sitä voidaan käyttää myös arvioitaessa senhetkisen tuotteen turvallisuusongelmia. Näin ollen uhkamallinnusta voidaan hyödyntää tuotekehitysprosessin elinkaaren eri vaiheissa.

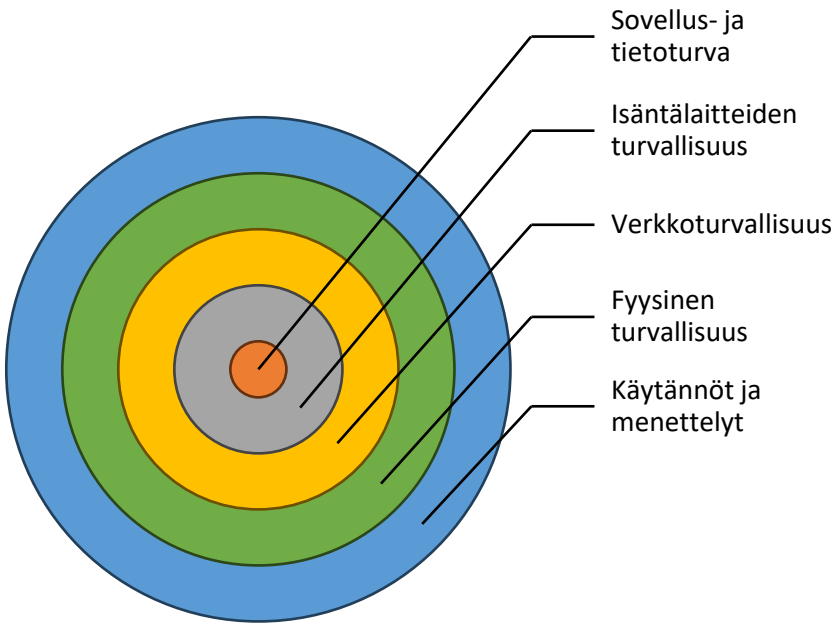
Uhkamallinnus kannattaa toteuttaa jo mahdollisimman varhaisessa vaiheessa tuotekehitysprosessia eli käytännössä jo tuotteen määrittelyvaiheessa, jolloin vaadittavat turvallisuustoimenpiteet voidaan ottaa osaksi tuotetta jo kehitysprosessin alkuvaiheessa. Käytännössä organisaation on valittava sovellettava uhkamallinnuksen viitekehys ja/tai työkalut, esim. STRIDE-viitekehys, toteuttaa mallinnus, arvioida uhkien vaikutukset, vakavuus ja riski esim. CVSS-pisteytysjärjestelmällä, laittaa uhat prioriteettijärjestykseen, suunnitella tarvittavat vastatoimet (poisto- tai lievennystoimet) ja määritellä hyväksyttävä jäännösriskin taso. Uhkamallinuksen toteuttamiseen voidaan käyttää erilaisia työkaluja, kuten Microsoftin Threat Modeling Tool -työkalua. (Automation Standards Compliance Institute 2022, 9–10 [ANSI/ISA 62443-4-1 2018]; Conklin 2024; Marty 2019; Microsoft 2024b; Microsoft 2024c.) Uhkamallinnuksen perusteella voidaan tehdä tietoon perustuvia turvallisuuspäätöksiä ja priorisoida turvallisuustoimia (Otieno ym. 2023, 61).

Standardin integroimisessa on kuitenkin otettava huomioon standardin vaatimusten soveltuvuus omaan tuotteeseen. Standardissa vaaditaankin, että vaatimuksien soveltuvuutta täytyy arvioida suhteessa tuotteeseen (prosessin laajuus -osaprosessi). Esimerkiksi jos oma tuote ei sisällä räätälöityjä komponentteja, ei ole mitään perusteita soveltaa räätälöityjen komponenttien vaatimusta. Näkisinkin, että tämä osaprosessi olisi syytä toteuttaa jo standardin käyttöönoton varhaisessa vaiheessa, jolloin voidaan arvioida sovellettavia vaatimuksia ja sujuvoittaa standardin käyttöönottoa, kun aikaa ei kulu ns. turhien vaatimusten täytäntöönpanoon. Käytännössä tämä vaatii organisaatioilta perehtymistä standardin sisältöön ja standardin vaatimusten peilaamista suhteessa omaan tuotteeseen jo ennen varsinaista standardin vaatimusten integrointia tuotekehitysprosessiin.

Turvallinen suunnittelu varmistaa, että tuote vastaa sille määriteltyjä turvallisuusvaatimuksia ja että turvallisuus on osa tuotteen ominaisuuksia (turvallisen suunnittelun periaatteet -osaprosessi). Organisaation onkin varmistettava, että sen tuotekehitysprosessissa noudatetaan turvallisen suunnittelun parhaita käytäntöjä. Turvallisen suunnittelun käytäntöjä ovat mm. mahdollisimman suppeat käyttöoikeudet, roolien erottaminen, syväpuolustus, nollaluottamus ja hyökkäyspinta-alan minimoiminen (International Society

of Automation 2023, 9; Kelly & Sastre 2023; OWASP Foundation 2024). Käytäntöjä on useita ja tiedonhaun perusteella jokainen organisaatio listaa itselleen tärkeimmiksi arvioimansa käytänteet. Käytännössä organisaation on siis määriteltävä, mitkä turvallisen suunnittelun periaatteet soveltuvat heidän omaan tuotekehitysprosessiinsa (turvallisen suunnittelun parhaat käytännöt -osaprosessi). Käytäntöjen hyödyntäminen hyödyttää kehittäjiä, jotka eivät ole varsinaisia turvallisuusasiantuntijoita (Kanniah & Mahrin 2016, 3027).

Turvallisen suunnittelun käytänteisiin sisällytetään kuitenkin aina syvyyssuuntaisen puolustuksen ajatusmalli, koska standardi perustuu vahvasti nimenomaan syväpuolustusajatteluun (ISA Global Cybersecurity Alliance 2020, 12). Standardin vaatima uhkamallinnus toimii pohjana tuotteen syvyyssuuntaisen puolustuksen suunnittelulle (syväsuojaussuunnitteluosaprosessi). Syväsuojauksessa lähdetään oletuksesta, että jokainen puolustuksen kerros on alttiina hyökkäykselle ja jokainen kerros on mahdollista murtaa. Näin ollen jokaisen puolustuskerroksen on toimittava itsenäisesti ja pienennettävä alempien kerrosten hyökkäyspinta-alaa. Yleisesti ottaen syväsuojauksen kerrosten voidaan ajatella muodostuvan kuvion 8 mukaisesti.



KUVIO 8. Teollisuusautomaatio- ja ohjausjärjestelmän syväsuojauksen kerrokset (mukaillen Marty 2020; Patel 2018)

Kuvion 8 mukainen ajatusmalli linkittyy koko teollisuusautomaatio- ja ohjausjärjestelmän syvyyssuuntaisen puolustuksen suunnitteluun kuin myös tuotetoimittajan yksittäisen komponentin kehitystyöhön.

Perustelut tälle ovat, että tuotetoimittajan on huomioitava tuotteen tuleva turvallisuuskonteksti suunnitellessaan tuotteen sisäisiä turvallisuusominaisuuksia. Näin ollen tuotekehitystyössä onkin huomioitava tulevan käyttöympäristön tarjoamat turvallisuusominaisuudet kuin myös sen tuotteelta vaatimat turvallisuusominaisuudet. Tämän ajatuksen myötä tuotetoimittaja määrittelee tarvittavat turvallisuusominaisuudet ja toteuttaa ne osaksi tuotetta. Tuloksena saadaan aikaiseksi mahdollisimman turvallinen tuote, joka tukee koko teollisuusautomaatio- ja ohjausjärjestelmien syväpuolustusta. Tuotteen kehitystyössä on kuitenkin muistettava, että turvallisuustoimenpiteet eivät saa estää teollisuusautomaatio- ja ohjausjärjestelmien olennaisia toimintoja, esim. pääsynhallinta ei saa estää olennaisten toimintojen toimintaa (International Society of Automation 2023, 9–10). Toisaalta näkisin, että kuvion 8 mallia voidaan myös hyvin hyödyntää organisaation tuotekehitysympäristön tietoturvan suunnittelussa, koska se sisältää kehitysympäristön turvallisuudessa huomioitavia asioita aina organisaation yleisistä käytännöistä ja menettelyistä työvälineiden turvallisuuteen (sovellus- ja tietoturva).

Turvallisen kehittämisen lähtökohtana on, että kehitetään mahdollisimman turvallinen tuote, jonka kehitysprosessin aikana on huomioitu tuotteen turvallisuusnäkökohdat koko elinkaaren ajan. Täytyy kuitenkin muistaa, että on täysi mahdottomuus kehittää tuotetta, joka ei sisältäisi haavoittuvuuksia jossain käyttöikänsä vaiheessa. Kehityksen mennessä eteenpäin ilmenee myös uusia haavoittuvuuksia, jotka ovat uhka tietoturvalle. Näin ollen organisaation täytyy panostaa siihen, että sillä on tarvittavat keinot ja käytännöt tunnistaa tuotteeseen jääneet ja käytössä ilmenneet turvallisuusongelmat (turvallisuusongelmien hallinnan käytäntö). Lisäksi organisaation on huolehdittava, että sillä on selkeä toimintasuunnitelma, miten havaitut ongelmat käsitellään ja kuinka mahdolliset korjaustoimenpiteet jalkautetaan tuotteen käyttäjille kohtuullisessa ajassa (turvallisuusongelmien ja tietoturvapäivitysten hallinnan käytännöt). Tietoturvan toteuttaminen ei ole kertaluontoinen toimenpide, vaan sen vaaliminen vaatii jatkuvaa ylläpitoa ja päivittämistä (Otieno ym. 2023, 62).

Tuotteen käyttäjän kannalta organisaation on panostettava riittävään informointiin ja opastukseen (turvallisuusohjeet -käytäntö). Organisaation onkin informoitava käyttäjiä ilmenneistä ongelmista, mikäli ne vaarantavat tuotteen tietoturvallisuuden (turvallisuusongelmien esiintuomisen osaprosessi). Lisäksi organisaation on tarjottava kattava informointi päivityksistä ja korjauksista sekä niiden vaikutuksista tuotteeseen ja/tai tuotteen käyttöön (tietoturvapäivitysten dokumentaation osaprosessi). Informoinnissa ei tule myöskään unohtaa kattavaa tuotteen käyttöopastusta käyttäjäoppaiden ja tukisivustojen muodossa. Tarvittaessa käyttäjille voidaan tarjota jopa koulutusta tuotteen turvallisesta käytöstä. Kattavan ja riittävän informoinnin tarjoaminen vaatii organisaatiolta johdonmukaista prosessia, jolla varmistetaan, että tieto on saatavilla, se on ajantasaista eikä se sisällä virheitä.

5.3 Verifioi ja validoi

Standardin käyttöönoton verifiointi ja validointi ei ole niinkään erillinen osa, vaan osa koko käyttöönottoprosessia. Standardi sisältää useita kohtia, joissa vaaditaan, että tehtyjä toimia tarkastellaan, jotta ne vastaavat standardin asettamia vaatimuksia ja että tehdyt toimet ovat toimivia ja asianmukaisia (prosessin verifioinnin, turvallisuusvaatimusten tarkastelun, turvallisen suunnittelun tarkastelun, turvallisuuden toteutuksen tarkastelun jne. osaprosessit). Organisaation onkin standardin käyttöönottoprosessin edetessä pysähdyttävä välillä tarkastelemaan, tehdäänkö asioita oikein ja tehdäänkö oikeita asioita. Tässä tarkastelussa auttaa, mikäli organisaatio huolehtii kattavasti turvallisen tuotekehitysprosessin dokumentoinnista. ISA/IEC 62443-4-1 standardi vaatiikin, että kaikki soveltuvien vaatimusten prosessit dokumentoidaan. Dokumentoinnissa on käytävä ilmi lisäksi perustelut, miksi jotain vaatimusta ei ole noudatettu. Mikäli organisaation aikomuksena on sertifioida tuotekehitysprosessinsa standardin mukaisesti, toimivat dokumentit myös yhtenä todisteena siitä, että standardin vaatimukset on huomioitu tuotekehitysprosessissa. Verifioinnin ja validoinnin tukemiseksi organisaatiolla olisi hyvä olla käytössään myös sisäisiä mittareita ja keskeisiä indikaattoreita, joilla voidaan mitata, onko standardin vaatimukset täytetty ja ovatko tehdyt toimet toimivia (Kanniah & Mahrin 2016, 3027).

Olennainen tapa verifioida ja validoida tuotekehitysprosessia on tuotteen testaaminen. Tuotteelle voidaan toteuttaa erilaisia testauksia kehitysprosessin eri vaiheissa. Testauksilla varmistetaan, että tuote vastaa vaatimuksiaan, toteutetut toimet ovat toimivia ja tuote on ennen kaikkea mahdollisimman turvallinen. Standardi määrittelee neljä testausosaprosessia, jotka tuotteelle on suoritettava: turvallisuusvaatimusten testaus, uhkien lieventämisen testaus, haavoittuvuuksien testaus ja läpäisytestaus. Standardissa luetellaan useita eri testausmenetelmiä. Olennaisin asia verifioinnin ja validoinnin kannalta on, että testaukset suunnitellaan, toteutetaan, analysoidaan ja raportoidaan. Testauksen suunnittelussa mietitään, mitä halutaan testata, kuinka laajasti testataan, mitkä ovat testauksen tavoitteet, mitä rooleja ja vastuita testaukseen liittyy, aikataulu jne. Testaus onkin nähtävä verifioinnin ja validoinnin projektina, jolle toteutetaan ns. projektisuunnitelma. (Scarfone ym. 2008, 13.) Suunnittelun yhteydessä on myös huomioitava, että standardissa määritellään tarpeet testaajien riippumattomuudelle riippuen suoritettavasta testaustyypistä (testaajien riippumattomuus -osaprosessi). Näin ollen organisaation onkin määriteltävä suunnitelmassaan, kuka kyseisen testauksen suorittaa.

Pelkkä dokumentointi ei kuitenkaan riitä varmistamaan organisaation turvallista tuotekehitystä. Paperilla kaikki voi vaikuttaa hyvältä, mutta jos toimia ei viedä käytäntöön eikä niitä noudateta, on standardin soveltaminen ollut turhaa. Näin ollen organisaatiossa onkin huolehdittava, että kirjatut prosessit ovat

jalkautettu myös käytännöntyöhön ja näitä prosesseja noudatetaan. Tämä vaatii käytäntöjen kouluttamista henkilökunnalle ja säännöllistä käytäntöjen kertaamista. Tässä tuetaan mielestäni myös standardin vaatimusta turvallisuusasiantuntemuksesta. Kouluttamalla, informoimalla ja ylläpitämällä henkilökunnan tietotaitoa varmistetaan, että turvallinen tuotekehitysprosessi on osa organisaation toimintakulttuuria. Tätä edesauttamaan voidaan luoda suunnitelma käytäntöjen käyttöönottamiseksi ja kouluttamiseksi. Kannahinin ja Mahrinin tutkimuksen mukaan organisaation tavoitteet, toimintakulttuuri ja tietoisuus vaikuttavat turvallisen tuotekehityksen toteutumiseen (Kanniah & Mahrin 2016, 3026).

5.4 Ylläpidä ja kehitä

Turvallinen tuotekehitys täytyy nähdä jatkuvana prosessina, jolla ei ole alku- ja loppupäivämäärää. Näin ollen organisaation pitää huolehtia, että se arvioi kriittisesti omaa turvallisen tuotekehityksen elinkaari -prosessiaan säännöllisesti (jatkuvan parantamisen osaprosessi). Muuttuva maailma tuo mukanaan uusia uhkia ja uusia tapoja hyödyntää niitä, joten jatkuvaa parantamista vaaditaan, jotta voidaan jatkossakin taata tuotteen turvallisuus. Arvioinnissa on kiinnitettävä huomiota myös valmiiseen tuotteeseen päässeisiin haavoittuvuuksiin. (IEC 62443-4-1:2018, 26.) Käsiteltäessä valmiiseen tuotteeseen jääneitä turvallisuusongelmia voidaan arvioida samalla oman turvallisen kehitysprosessin toimivuutta ja tarpeita kehittää prosessia. Ilman tuotteen turvallisuusongelmiakin on huolehdittava, että turvallisen tuotekehityksen prosessia kehitetään ja parannetaan organisaatiossa johdonmukaisesti. Käytännössä organisaatiossa on oltava toimintasuunnitelma turvallisen tuotekehityksen arvioimiseksi ja kehittämiseksi. Yksi keino arvioida omaa toimintaa on auditoida omaa toimintaansa sisäisesti.

Useissa standardin vaatimuksissa vaaditaan, että kyseistä osaprosessia on tarkasteltava ja arvioitava säännöllisesti (mm. jatkuva parantaminen, uhkamallinnus, turvallisen suunnittelun käytännöt, turvallisuusongelmien hallinta). Näin ollen organisaatiossa onkin huolehdittava, että turvallisen tuotekehityksen arvioinnissa ja kehittämisessä huomioidaan myös jokainen osaprosessi itsessään, mutta myös osana kokonaisuutta. Näin varmistetaan, että yksittäiset osaprosessit vastaavat standardin vaatimuksia ja ne toimivat tarkoituksenmukaisesti. Lisäksi näin voidaan jatkossakin varmistaa tuotteen turvallisuus ja kehittää sen turvallisuutta entisestään. Tuotteen näkökannalta tämä tarkoittaa käytännössä, että jokaisen tuotemuutoksen tai käyttöympäristön tmv. muutoksen myötä tuotetta, osaprosesseja ja niihin liittyvää dokumentaatiota on arvioitava ja päivitettävä muutosten yhteydessä, esim. uusien uhkien ilmetessä tuot-

teen uhkamallinnusta päivitetään ja sen myötä toteutetaan tarvittavat muutokset. Tuotteen turvallisuudesta huolehtiminen luo laatua ja tuotteen laadukkuus tuo asiakkaita, sitoo asiakkaita sekä luo positiivisen yrityskuvan. Näin varmistetaan organisaation toiminnan jatkuvuus.

Organisaation olisi hyvä myös huomioida turvallisesta tuotekehitystä tukevat toiminnot ja arvioida niiden vaikutuksia aika ajoin. Ensinnäkin kehitystyössä käytettyjä työkaluja on syytä arvioida ajoittain, että ne vastaavat senhetkisen tuotekehitysprosessin tarpeeseen ja että työkalut ovat edelleen itsessään turvallisia. Lisäksi henkilöstön asiantuntemusta on ylläpidettävä ja kehitettävä koulutuksilla, jotta turvallisen tuotekehityksen asiantuntemus säilyy asianmukaisella tasolla. Myös organisaation sisäisten prosessien muutosten vaikutusta on arvioitava suhteessa turvallisen tuotekehityksen elinkaariprosessiin. Kaiken kaikkiaan organisaation on vahvistettava turvallisen tuotekehityksen käytäntöjään ja korostettava niiden merkitystä, jolloin käytännöt muuttuvat ajan saatossa yhä vahvemmaksi osaksi organisaation toimintakulttuuria (Kanniah ja Mahrin 2016, 3026–3027).

6 YHTEENVETO

ISA/IEC 62443-4-1 standardi on kokonaisvaltainen standardi, jossa jokainen vaatimus linkittyy jollain tasolla toisiinsa. Näin ollen ennen standardin käyttöönottoa on suositeltavaa perehtyä sen sisältöön kokonaisuudessaan ja arvioida standardin soveltuvuutta suhteessa omaan tuotteeseen ja tuotekehitysprosessiin. Standardi on mielestäni suhteellisen käytännönläheinen ja sen soveltaminen on riippuvainen organisaation toimialasta, kehitettävästä tuotteesta ja tuotteen tulevasta käyttöympäristöstä. ISA/IEC 62443-4-1 standardin ensisijainen hyöty on, että se tarjoaa organisaatioille viitekehyksen turvallisen tuotekehityksen elinkaaren käyttöönottoon, hallintaan ja kehittämiseen, mikä edesauttaa tietoturvallisten tuotteiden kehityksessä. Standardin käyttöönotto voi edesauttaa myös löytämään puutteita tai aukkoja omassa tuotekehitysprosessissa. Näin ollen tuotekehitysprosessia on mahdollista lähteä korjaamaan kohti turvallista tuotekehitysprosessia. Standardin ylläpitäminen vaatii myös jatkuvaa prosessin tarkastelua ja kehittämistä. Tämän ansiosta tuotekehitysprosessia voidaan siis parantaa entisestään. Prosessin kehittäminen vie organisaation toimintaa eteenpäin, kehittää laatua, tehostaa toimintaa ja tuo taloudellista hyötyä.

Tutkittuani ISA/IEC 62443-4-1 standardia olen todennut, että standardin käyttöönotto vaatii organisaatiolta resursseja ja aikaa paneutua tähän työhön. Lisäksi resurssien ja ajan määrä on riippuvainen suhteessa siihen, onko organisaation tarkoituksena sertifioida oma tuotekehitysprosessinsa vai vain pyrkiä noudattamaan standardin vaatimuksia omassa työssään. Sertifiointiprosessi voi olla iso kustannus organisaatiolle, mikä voi olla isokin kynnyskysymys lähteä sertifioimaan organisaatiota, prosesseja tai tuotteita. Ensimmäinen askel onkin lähteä pohtimaan sertifioinnin tuomia hyötyjä suhteessa sen aiheuttamiin kustannuksiin. Lisäksi on arvioitava esim. onko organisaatiolla mahdollisuutta toteuttaa sertifiointia nykyisten resurssien puitteissa, vaatiiko organisaation toimintaympäristö tai asiakaskunta tiettyjä sertifikaatteja organisaation toiminnasta tai onko sertifioinnille jotain lakisääteisiä perusteita tai vaatimuksia. Näkisin kuitenkin, että jos organisaatiolla on suunnitelmissa joskus tulevaisuudessa hankkia sertifiointi tai se muuten haluaa kehittää tuotekehitysprosessinsa ja tuotteensa tietoturvallisuutta, on standardin vaatimusten integroiminen omaan tuotekehitysprosessiin ennakolta yksi tapa säästää aikaa ja resursseja virallisessa sertifiointiprosessissa ja kehittää omaa tuotekehitysprosessia tietoturvallisemmaksi sekä siten parantaa oman tuotteen tietoturvallisuutta.

ISA/IEC 62443-4-1 standardin sertifioinnin ensisijainen hyöty on, että organisaatio voi osoittaa asiakkailleen ja yhteistyökumppaneilleen ns. virallisesti, että organisaatio noudattaa turvallisen tuotekehityksen vaatimuksia tuotekehityksen jokaisessa vaiheessa ja että organisaatiossa otetaan huomioon tuotteen kyber- ja tietoturvallisuus tuotteen koko elinkaaren ajan. Yleisesti ottaen voidaan myös ajatella, että kyber- ja tietoturvallisuus ovat organisaatiolle ensisijaisia tuoteominaisuuksia. (Mikhaleva 2022, 26–27.) Lisäksi on huomioitava, että sertifioinnin toteuttaa riippumaton kolmas osapuoli, jolloin sertifioinnin luotettavuus on korkeimmillaan. Näin ollen voidaan luottaa, että sertifiointi on toteutettu laadukkaasti ja varmasti standardin vaatimuksia noudattaen. Kuten sanottu, ilman sertifiointiakin standardin vaatimusten noudattaminen lisää tuotekehitysprosessin ja tuotteen tietoturvallisuutta, kunhan standardin vaatimukset ovat integroitu myös käytännöntyöhön.

Standardin käyttöönotossa voi olla myös riskinsä siinä mielessä, että organisaatio tuudittautuu ajatukseen, että tuote on täysin turvallinen, koska tuotekehitysprosessissa on seurattu turvallisen tuotekehityksen elinkaaren standardia (Tuptuk & Hailes 2018, 101). Standardin käyttöönotto ei kuitenkaan takaa, että tuote olisi myös tulevaisuudessa turvallinen. Muuttuva maailma, muuttuvat toimintamallit, kehittyvä teknologia ja ihmisten tietoteknisten taitojen lisääntyminen takaavat sen, että uusia uhkia ja haavoittuvuuksia ilmenee ja näin ollen myös tuote kohtaa uusia turvallisuusuhkia. Organisaatiossa onkin hyvä muistaa, että turvallinen tuotekehitys on jatkuva prosessi, joka vaatii seuraamista ja päivittämistä uusien uhkien tunnistamiseksi ja toimenpiteiden täytäntöönpanemiseksi tuotteen koko elinkaaren ajan.

Tämän opinnäytetyön tarkoituksena oli antaa kokonaiskuva turvallisesta tuotekehityksestä, ISA/IEC 62443-4-1 standardista ja standardin käyttöönotosta. Opinnäytetyön lopuksi voidaan todeta, että työssä annettiin kokonaisvaltainen kuva turvallisen tuotekehityksen elinkaaresta ja teollisuusautomaatio- ja ohjausjärjestelmien tuotteiden turvallisen tuotekehityksen standardista. Lisäksi työssä pystyttiin tuomaan yleisiä käytännön näkökulmia standardin käyttöönottoon ja tekemään tarkistuslista esitetyistä näkökulmista. Työelämän kannalta tavoitteeksi asetettiin, että opinnäytetyö tarjoaisi organisaatioille kokonaiskuvan turvallisesta tuotekehityksestä ja toimisi alkusysäyksenä standardin käyttöönotolle. Tähän tavoitteeseen päästiin ja näkisin, että tämä opinnäytetyö toimii hyvänä lähtökohtana standardiin perehtymiselle ja sen käyttöönotolle. Allekirjoittaneelle opinnäytetyön antina oli erityisesti ajattelumallin muutos. Muutos ajatella, että turvallisuus on tuotteen sisäänrakennettu ominaisuus, joka on huomioitava osana tuotekehitysprosessia, ja että tietoturva on koko tuotteen elinkaaren mittainen prosessi.

LÄHTEET

ANSI/ISA 62443-4-1-2018. *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.* 2018. International Society of Automation.

Automation Standards Compliance Institute. 2022. *SDLA-312.* Saatavissa: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/ISASecure%20Specifications/SDLA/SDLA%203.0.0/SDLA-312%20Sec%20Dev%20Lifecycle%20Assess(v6_3).pdf. Viitattu 22.1.2024.

Bartsch, S. 2011. *Practioner's Perspectives on Security in Agile Development.* Institute of Electrical and Electorinics Engineers. Saatavissa: https://doi.org/10.1109/ARES.2011.82. Viitattu 1.3.2024.

Conklin, L. 2024. *Threat Modeling Process*. OWASP Foundation. Saatavissa: https://owasp.org/www-community/Threat_Modeling_Process#asf-threat--countermeasures-examples. Viitattu 20.2.2024.

Cybersecurity & infrastructure security agency. 2021. *What is Cybersecurity?* Saatavissa: https://www.cisa.gov/news-events/news/what-cybersecurity. Viitattu 27.2.2024.

Cyber Security – Secure Development Lifecycle. 2021. Etteplan. Saatavissa: https://www.youtube.com/watch?v=XGlczq-VuM0. Viitattu 17.1.2024.

Dorsey, V. 2020. *The 6 stages of a holistic hardware security development lifecycle.* BNP Media. Saatavissa: https://www.securitymagazine.com/articles/93938-the-6-stages-of-a-holistic-hardware-security-development-lifecycle. Viitattu 27.2.2024.

Drake, V. 2024. *Threat Modeling*. OWASP Foundation. Saatavissa: https://owasp.org/www-community/Threat_Modeling#. Viitattu 18.1.2024.

Galarita, B. & Swanston B. 2024. *Information Security Vs. Cybersecurity: What's The Difference?* Forbes Media LLC. Saatavissa: https://www.forbes.com/advisor/education/it-and-tech/information-security-vs-cyber-security/. Viitattu 27.2.2024.

Gupta, A. K., Chandrashekhar, U., Sabnis, S. V. & Bastry, F. A. 2007. Building Secure Products and Solutions. *Bell Labs Technical Journal,* 12(3), 21–38. Saatavissa: https://doi.org/10.1002/bltj.20247. Viitattu 27.2.2024.

IEC 62443-4-1:2018. *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.* 2018. International Electrotechnical Commission.

IEC/TR 62443-3-1:fi. *Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille.* 2013. Suomen standardisoimisliitto SFS ry.

IEC/TS 62443-1-1:fi. *Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit.* 2012. Suomen standardisoimisliitto SFS ry.

International Society of Automation. 2024. *ISA99, Industrial Automation and Control Systems Security.* Saatavissa: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99. Viitattu 10.1.2024.

International Society of Automation. 2023. *Quick Start Guide: An Overview of ISA/IEC 62443 Standards. Security of Industrial Automation and Control Systems.* Saatavissa: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide.pdf. Viitattu 9.1.2024.

ISA Global Cybersecurity Alliance. 2020. *Security Lifecycles in the ISA/IEC 62443 Series. Security of Industrial Automation and Control Systems.* Saatavissa: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2022%20ISA%20Website%20Redesigns/ISA%20Secure/Files%20Repository%20For%20Learning%20Center/Articles%20Page/ISAGCA-Security-Lifecycles-whitepaper.pdf. Viitattu 15.1.2024.

Kanniah, S. L. & Mahrin, M. N. 2016. A Review on Factors Influencing Implementation of Secure Software Development Practices. *International Journal of Computer and Systems Engineering,* 10(8), 3022–3029. Saatavissa: https://doi.org/10.5281/zenodo.1127256. Viitattu 29.2.2024.

Kelly, J. & Sastre, D. 2023. Security by Design: Security principles and threat modeling. *Red Hat - blogi*. Saatavissa: https://www.redhat.com/en/blog/security-design-security-principles-and-threat-modeling#security-by-design-6. Viitattu 21.2.2024.

Liikenne- ja viestintävirasto Traficom. 2018. *Turvallinen tuotekehitys: Kohti hyväksyntää.* Helsinki. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf. Viitattu 17.1.2024.

Lipner, S. 2004. *The trustworthy computing security development lifecycle.* Institute of Electrical and Electronics Engineers. Saatavissa: https://doi.org/10.1109/CSAC.2004.41. Viitattu 27.2.2024.

Marty, K. 2019. *How to implement Cyber Security acc. to IEC 62443 – Ep.1 – Threat Analysis.* CertX AG. Saatavissa: https://certx.com/cybersecurity/how-to-implement-cyber-security-acc-to-iec-62443-ep-1-threat-analysis/. Viitattu 20.2.2024.

Marty, K. 2020. *How to implement Cyber Security acc. to IEC 62443 – Ep2. – Secure Design.* CertX AG. Saatavissa: https://certx.com/cybersecurity/how-to-implement-cyber-security-acc-to-iec-62443-ep-2-secure-design/. Viitattu 20.2.2024.

Microsoft. 2024a. *About Microsoft SDL*. Saatavissa: https://www.microsoft.com/en-us/securityengineering/sdl/about. Viitattu 17.1.2024.

Microsoft. 2024b. *Secure development documentation*. Saatavissa: https://learn.microsoft.com/en-us/azure/security/develop/. Viitattu 20.2.2024.

Microsoft. 2024c. *Threat Modeling Security Fundamentals.* Saatavissa: https://learn.microsoft.com/en-us/training/paths/tm-threat-modeling-fundamentals/. Viitattu 20.2.2024.

Microsoft. 2023. *Microsoft Security Development Lifecycle (SDL).* Saatavissa: https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle?source=recommendations#design. Viitattu 18.1.2024.

Mikhaleva, A. 2022. *Cybersecurity Standard Compliance in Development of Distributed Embedded Systems.* Espoo: Aalto University. Master's Programme in Computer, Communication and Information

Sciences. Master's thesis. Saatavissa: https://urn.fi/URN:NBN:fi:aalto-202212187148. Viitattu 5.2.2024.

Otieno, M., Odera, D., Ounza, J. E. 2023. Theory and practice in secure software development lifecycle: A comprehensive survey. *World Journal of Advanced Research and Reviews,* 18(3), 53–78. Saatavissa: https://doi.org/10.30574/wjarr.2023.18.3.0944. Viitattu 1.3.2024.

OWASP Foundation. 2006. *Development Guide: Security by Design Principles.* Päivitetty 3.8.2016. Saatavissa: https://wiki.owasp.org/index.php/Security_by_Design_Principles. Viitattu 18.1.2024.

OWASP Foundation. 2021. *OWASP Top 10:2021.* Saatavissa: https://owasp.org/Top10/. Viitattu 29.1.2024.

OWASP Foundation. 2024. *Secure Product Design Cheat Sheet.* Saatavissa: https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html#3-the-principle-of-zero-trust. Viitattu 21.2.2024.

Patel, S. 2018. *Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach.* Access Intelligence, LLC. Saatavissa: https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/. Viitattu 20.2.2024.

Purpose and Scope of the ISA99 Committee. 2023. International Society of Automation – ISA. Saatavissa: https://www.youtube.com/watch?v=rbcSL2qZjaA. Viitattu 10.1.2024.

Sanastokeskus TSK ry. 2018. *Kyberturvallisuuden sanasto.* Helsinki: Huoltovarmuuskeskus. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. Viitattu 27.2.2024.

Scarfone, K., Souppaya, M., Cody A. & Orebaugh, A. 2008. *Technical Guide to Information Security Testing and Assessment.* National Institute of Standards and Technology. Saatavissa: https://doi.org/10.6028/NIST.SP.800-115. Viitattu 1.3.2024.

SFS-ISO/IEC TR 33014:2020. *Information technology – Process Assessment – Guide for process improvement.* 2020. Suomen standardisoimisliitto SFS ry.

Sesko. 2024. *Teollisuuden kyberturvallisuus: IEC 62443 -sarja*. Saatavissa: https://sesko.fi/standardit/standardoinnin-aihealueita/kyberturvallisuus/teollisuuden-kyberturvallisuus-iec-62443-sarja/. Viitattu 12.1.2024.

The Security Development Lifecycle (SDL) Explained. 2016. Exida. Saatavissa: https://www.youtube.com/watch?v=mRe3vLBpCJI. Viitattu 17.1.2024.

Tuptuk, N., Hailes S. 2018. Security of smart manufacturing systems. *Journal of Manufacturing Systems* 47, 93–106. Saatavissa: https://doi.org/10.1016/j.jmsy.2018.04.007. Viitattu 5.2.2024.

LIITE 1/1

TARKISTULISTA ISA/IEC 62443-4-1 KÄYTTÖÖNOTOSTA

TEHTÄVÄ	**KYLLÄ**	**EI**
SUUNNITTELU		
1. Onko tuote määritelty?		
2. Onko standardin soveltuvuus arvioitu?		
3. Onko tuotekehitysprosessi määritelty ja dokumentoitu?		
4. Tukevatko organisaation yleiset prosessit ja käytännöt turvallista tuotekehitysprosessia?		
5. Onko kehitysympäristön tietoturva kunnossa?		
6. Onko organisaation roolit ja vastuut määritelty?		
7. Onko organisaation asiantuntemus arvioitu?		
8. Halutaanko toteuttaa sertifiointi? a) Onko sertifiointityyppi valittu? b) Onko sertifiointielin valittu?		
TOTEUTUS		
1. Onko tuotteen vaatimukset, rakenne, toiminnot, käyttötarkoitus ja -ympäristö määritelty huomioiden turvallisuusnäkökohdat?		
2. Onko tuote ja sen käyttö mallinnettu?		
3. Uhkamallinnus: a) Onko valittu sopiva uhkamallinnuksen viitekehys ja/tai työkalu? b) Onko uhkamallinnus toteutettu? c) Ovatko ilmenneet uhat arvioitu ja priorisoitu? d) Onko uhkien vastatoimet suunniteltu ja määritelty sallittu jäännösriskin taso?		
4. Onko standardin soveltuvat osat määritelty?		
5. Onko soveltuvat turvallisen suunnittelun käytännöt määritelty?		
6. Onko syväpuolustussuunnitelma suunniteltu ja mallinnettu?		
7. Onko toteutettu toimintasuunnitelma tuotteen turvallisuusongelmien ja tietoturvapäivitysten hallinnalle?		

LIITE 1/2

TEHTÄVÄ	**KYLLÄ**	**EI**
8. Onko käyttäjäopastus tehty? Onko informointikanavat perustettu?		
VERIFIOINTI JA VALIDOINTI		
1. Onko huolehdittu kehitysprosessin asianmukaisesta dokumentoinnista?		
2. Onko määritelty turvallisen tuotekehityksen sisäiset mittarit ja indikaattorit?		
3. Onko koko prosessia ja sen osaprosesseja tarkasteltu?		
4. Tuotetestaus: a) Onko testaukset suunniteltu ja arvioitu tarve testaajien riippumattomuudelle? b) Onko testaukset toteutettu? c) Onko testitulokset analysoitu? d) Onko tulokset raportoitu?		
5. Onko turvallinen tuotekehitysprosessi jalkautettu käytäntöön?		
YLLÄPITÄMINEN JA KEHITTÄMINEN		
1. Onko laadittu toimintasuunnitelma turvallisen tuotekehitysprosessin arvioinnista ja kehittämisestä?		
2. Onko tuotekehitysprosessin kehittämissuunnitelma otettu käytäntöön?		
3. Onko tuotteen tai sen käyttöympäristön tmv. muutokset huomioitu tuotekehitysprosessissa, tuotteessa ja tuotedokumentaatiossa? Onko tarvittavat muutokset toteutettu?		
4. Onko laadittu toimintasuunnitelma kehitysympäristön ja henkilöstön asiantuntemuksen arviointiin ja kehittämiseen?		
5. Onko arvioitu organisaation sisäisten prosessien muutosten vaikutukset suhteessa turvallisen tuotekehityksen prosessiin?		