Tampereen yliopisto

Patrik Ollikainen

AUTOMAATION TIETOTURVARAT-KAISU

Syvyyssuuntainen turvallisuussuunnittelu

Kandidaatintyö
Tekniikan ja luonnontieteiden tiedekunta
2023

TIIVISTELMÄ

Patrik Ollikainen: Automaation tietoturvaratkaisu: syvyyssuuntainen turvallisuussuunnittelu
Kandidaatintyö
Tampereen yliopisto
Teknisten tieteiden kandidaatin tutkinto-ohjelma
Huhtikuu 2023

Tämän kandidaatintyön tavoitteena on perehtyä syvyyssuuntaiseen turvallisuussuunnitteluun automaation tietoturvaratkaisuna kirjallisuuskatsauksen muodossa. Työn tarkoituksena on tutkia syvyyssuuntaisen turvallisuussuunnittelun rakennetta ja toteuttamista. Työssä on käytetty aineistona erilaisia kirjallisuus lähteitä. Työn alussa perehdytään automaatiojärjestelmän tietoturvavaatimuksiin ja reunaehtoihin sen toimivuuden kannalta. Syvyyssuuntaisella turvallisuussuunnittelulla pyritään löytämään ratkaisuja automaatiojärjestelmän tietoturvavaatimuksiin.

Tietoturvaratkaisuja suunniteltaessa automaatiojärjestelmiin tulee ottaa huomioon niille ominaiset vaatimukset. Korkealla prioriteetilla on automaatiojärjestelmissä saatavuus ja ihmisille tai ympäristölle turvallinen operointi. Pitkät elinkaaret automaatiojärjestelmän komponenteissa ja ohjelmistoissa asettaa järjestelmään haavoittuvaisuuksia, mitkä täytyy huomioida riskianalyysissä. Ohjelmistopäivitykset tulee testata huolellisesti ennen niiden asentamista järjestelmään ja ohjelmistoja päivittäessä tulee olla tietoinen kaikista toimintojen ja ohjelmistojen välisistä riippuvuussuhteista. Komponentti päivitykset tulee ajoittaa suunniteltuihin huoltokatkoihin järjestelmässä, jotta vältytään ylimääräisistä tuotannon seisauksista. Automaatiojärjestelmissä tietoliikenteen luotettavuuden säilyttäminen on tärkeää, koska muuten menetetään tiedon hyödyllisyys ja järjestelmän ohjauksista tulee epävakaita. Tietoturvatoimenpiteitä lisättäessä tiedon saatavuuden ja reaaliaikaisuuden pitää pysyä ennallaan järjestelmässä.

Syvyyssuuntainen turvallisuussuunnittelu perustuu tietoturvan kerroksellisuuteen, jossa eri turvaratkaisut muodostavat yhdessä toisiaan tukevan suojauksen. Kerroksien tarkoitus on luoda useita vastatoimia turvallisuuden parantamiseksi ja haavoittuvaisuuksien pienentämiseksi. Turvallisuussuunnittelun rakenne koostuu kolmesta osasta: teknisistä ratkaisuista, fyysisistä esteistä ja hallinnon käytänteistä. Organisaation riskienhallinnan tulee tunnistaa riskit ja niiden todennäköisyydet sekä määritellä kriittisimmät osat järjestelmästä. Organisaation tulee rajata tuotantoalueet fyysisin estein ja tuottaa kulunvalvontaa ja tilojen seurantaa tuotantoalueilla. Verkkoarkkitehtuuri tulee suunnitella jakamalla verkko luottamustasoihin. Tasojen välillä tulee olla luotettavuusrajoja ja kriittiset tasot järjestelmässä tulee segmentoida omiin osiinsa verkossa. Tietoturvan monitorointi ja kehittäminen tunnetuille ja tuleville uhille on edellytys sen jatkuvuudelle. Automaatiojärjestelmissä tulee olla jatkuvaa monitorointia ja uhkien havainnointia. Järjestelmän monitoroinnissa voidaan hyödyntää lokienhallintajärjestelmiä reaaliaikaisen tilannekuvan tuottamiseksi. Turvallisuussuunnittelussa kehitytään koko ajan paremmin tunnistamaan riskejä ja ennakoimaan niitä.

Avainsanat: Defense-in-Depth, Automaation tietoturva, Tietoturvallisuus.

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

DnD	Defense-in-Depth, syvyyssuuntainen puolustus
DMZ	Demilitarized zone, demilitarisoitu vyöhyke
ERP	Enterprise Resource Planning, toiminnanohjausjärjestelmä
IAS	*Industrial Automation Systems,* teollisuusautomaatiojärjestelmä
MES	*Manufacturing Execution Systems,* tuotannonohjausjärjestelmä
SIEM	Security Information and Event Management, tietoturvatieto- ja tapahtumahallintajärjestelmä
SIM	Security Information Management, tietoturvatietojen hallinta
SEM	Security Event Management, turvatapahtumien hallinta
VPN	Virtual Private Network, virtuaalinen erillisverkko

.

1. JOHDANTO

Tietoturvahyökkäykset ovat määrällisesti kasvaneet valtavasti ja niiden luonne on muuttunut yhä ammattimaisemmaksi. Lisäksi hyökkäystavat ovat muuttuneet tietojen kalastelusta enemmän järjestelmien haavoittuvuuksien hyödyntämiseen. Yleistyneet tietoturvahyökkäykset tuotantotoimia vastaan ovat saanet monet automaatio toimijat tietoiseksi heidän heikosta tietoturvansa tasosta. Organisaatiot ovat alkaneet panostamaan enemmän turvallisuussuunnittelun ja parantamaan järjestelmiensä turvallisuutta. Automaatiojärjestelmien tiukat vaatimukset kuitenkin asettavat paljon haasteita turvallisuussuunnittelun toteuttamiselle.

Tässä työssä on tavoitteena perehtyä syvyyssuuntaiseen turvallisuussuunnitteluun ja miten sitä olisi mahdollista hyödyntää automaatiojärjestelmissä. Työssä käsitellään automaatiojärjestelmien vaatimuksia ja esitetään ratkaisuja niiden toteuttamiseksi. Tarkoituksena on keskittyä tietoturvaan liittyviin vaatimuksiin ja niiden ratkaisuihin automaatiojärjestelmissä. Automaatiojärjestelmää on tarkoituksena käsitellä reaaliaikaisuuden, luotettavuuden ja saatavuuden näkökulmista.

Työssä perehdytään syvyyssuuntaisen turvallisuussuunnittelun rakenteeseen ja sen toteutukseen. Suunnittelutavan rakenteen tarkoituksena on muodostaa eri turvallisuuden osakokonaisuuksista yhdessä toimiva kerroksellinen turvallisuus kokonaisuus. Toteutuksen osakokonaisuuksia tarkastellaan koko organisaation osalta toiminnanohjauksen tasolta aina teknisiin laitteisiin asti. Lisäksi esitetään, kuinka organisaation turvallisuuskokonaisuutta ylläpidetään ja varmistetaan sen toimivuus jatkuvasti kehittyvissä järjestelmissä.

Syvyyssuuntaisella turvallisuussuunnittelulla organisaatio voi parantaa turvallisuuttaan luotettavammaksi ja vähentää toimintaan kohdistuvia riskejä. Ennen kuin organisaatio voi tehokkaasti toteuttaa turvallisuussuunnittelun on sen ensin tunnistettava kaikki riskit ja uhat, jotka kohdistuvat organisaation. Riskien ja uhkien vakavuus ja todennäköisyys tulee myös määritellä tarkasti riskiarvioiden avulla. Lisäksi organisaation on tunnistettava kriittisimmät toiminnot järjestelmästä eli suojattavat kohteet turvallisuussuunnittelun näkökulmasta.

2. AUTOMAATION TIETOTURVAVAATIMUKSET

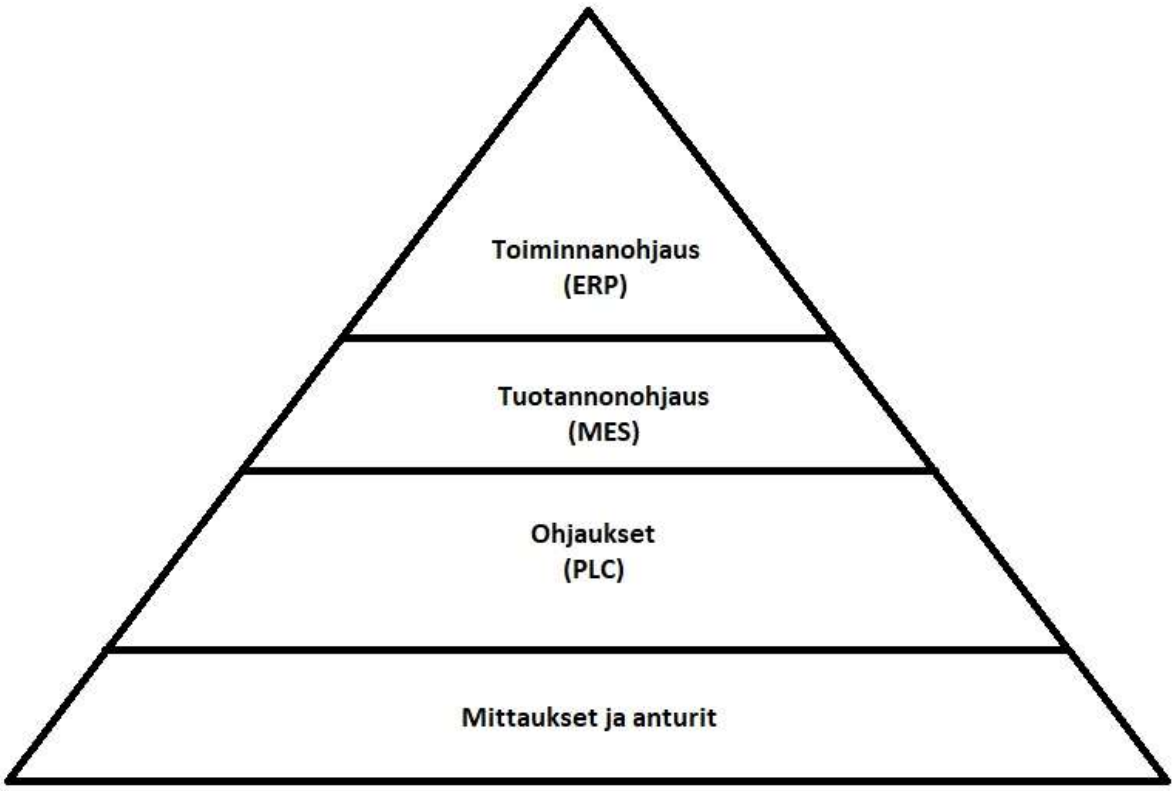
Automaatiojärjestelmät ovat kehittyneet valtavasti viimeisten vuosikymmenien aikana ja kehittyvät edelleen jatkuvasti, jolloin niiden tietoturvavaatimukset myös kasvavat huomattavasti. Pitkät elinkaaret automaatiojärjestelmissä myös asettaa haasteita turvallisuudella, kun jotkin osat järjestelmästä voivat olla todella vanhoja. Monesti suurissa automaatiojärjestelmissä tietoturvan taso on teknisiltä ratkaisuilta osin kunnossa, mutta muut tärkeät tietoturvan osa-alueet on jäänyt vähemmälle suunnittelulle tai jopa kokonaan jäänyt pois tietoturvavaatimuksista.

Tietoturvanvaatimukset kasvavat automaatiojärjestelmien laajentuessa. Monissa automaatiojärjestelmissä kuitenkin tietoturvan taso ei pysy muuttuneen toimintaympäristön tarpeiden tasolla, mikä lisää suuresti uhkia automaatiojärjestelmiin, kun niiden tietoturvassa on heikkouksia. Langattomiin yhteyksiin ja tietoliikenneverkkoihin kytketyt järjestelmät yleistyvät, jotka tuovat mukanaan lisää tietoturvia uhkia järjestelmiin. Etäyhteyksillä toimivat järjestelmät vaativat huomattavasti enemmän tietoturvaa ollakseen luotettavia. Tämän seurauksena pitää ottaa huomioon kenellä on oikeus kytkeytyä järjestelmään ja kuinka etäyhteyden muodostus toteutetaan luotettavasti.

Automaatiojärjestelmät voidaan jakaa eri tasoihin (Siemens ISA 2023), jotka yhdessä tuottavat toimivan automaatio kokonaisuuden. Kuvasta 1 nähdään, että ylimpänä tasona on toiminnanohjaus, josta menee tietoa alaspäin. Alimpana tasona kuvassa 1 on fyysisen maailman liitynnät, josta tulee dataa ylemmille tasoille. Tietoturvan näkökulmasta jokaisella tasolla tulee ottaa tietoturva huomioon ja se toteutetaan eri toimin tason mukaan. Alimmilla tasoilla tietoturva näkyy teknisinä ratkaisuina, kun taas ylempänä tietoturva pohjautuu ihmisten menettely tapoihin ja tietämykseen tietoturvan suhteen. Automaatiojärjestelmälle tietoliikenteen tietoturva on erityisen tärkeää eri tasojen välillä, jotta tietoa voidaan pitää luotettavana ja suojattuna. Automaatioympäristöissä korostuu erilaiset ominaisuudet, joista tärkeimmät ovat:

- Reaaliaikaisuus
- Luotettavuus
- Saatavuus

Joita käsitellään seuraavaksi hieman tarkemmin.



Kuva 1. Automaatiojärjestelmän tasot.

2.1 Reaaliaikaisuus

Reaaliaikaisuus tarkoittaa toiminnan tapahtumista tiettyyn takarajaan mennessä kuitenkin niin, että myös liian aikainen vaste on haitallinen järjestelmälle. Reaaliaikajärjestelmissä reaaliaikavaatimus määrittää toiminnan tapahtumista määritettyjen kahden ajanhetken välillä: aikaisimman ja viimeisimmän hetken, jolloin toiminnon tai tehtävän tulee valmistua. Reaaliaikajärjestelmissä kova reaaliaikaisuus tarkoittaa vaatimuksia, jotka tulee ehdottomasti saavuttaa. Mikäli kovan reaaliaikaisuuden raja ylitetään, järjestelmän toiminta on virheellistä ja datan hyödyllisyys menetetään. (Silvola 2006, s.34–35)

Nykyisissä automaatiojärjestelmissä reaaliaikaisuus vaatimukset kasvavat ja etenkin kovan reaaliaikaisuuden vaatimukset korostuvat. Automaatiojärjestelmien tietoturvan suurimpia haasteita on saada automaation mittaustason suuret reaaliaikaisuus vaatimukset luotettavaksi tietoturvan suhteen. Yksi yleinen automaatiojärjestelmissä käytetty tietoliikenne järjestelmä on Profinet (Hein 2013), joka täyttää automaatiojärjestelmien reaaliai-

kaisuus vaatimukset ja turvallisen tiedonsiirron. Vaatimukset Profinetin tietoturva ohjeistuksen mukaan (Müller 2018), jotka tulee täyttyä reaaliaikaisessa teollisuudenohjausjärjestelmässä ovat:

- Saatavuus
- Reaaliaikaisuuskyvyt
- Sujuvat käyttöönotto ja laitteiden vaihto-ominaisuudet
- Pitkäaikainen toiminta ilman ihmisen läsnäoloa
- Toimivuus turvallisten ja vanhojen laitteiden välillä.

Tietoturva toimenpiteitä lisättäessä tiedon saatavuuden ja reaaliaikaisuuden pitää pysyä ennallaan järjestelmässä. Uusien laitteiden integrointi järjestelmään sisältää tarvittavan turvatoimenpiteiden konfiguroinnin. Automaatiojärjestelmien pitkäaikainen toiminta ilman ihmisten läsnäoloa pakottaa siihen, että koko järjestelmää ei voida vaihtaa kerralla turvallisempaan. Sen sijaan tulee varmistua siitä, että uudet osat järjestelmässä toimii vanhojen laitteiden kanssa keskenään.

2.2 Luotettavuus

Luotettavuus on kaikki kaikessa automaatiojärjestelmissä. Automaatiojärjestelmää suunniteltaessa tulee huomioida tiedon luotettavuuden tärkeys. Automaatiojärjestelmän suunnittelua vietäessä eteenpäin tulee asettaa tietoturvavaatimukset riittävän suurelle tasolle. Järjestelmässä tulee ottaa myös huomioon mikä on riittävä taso, jos tietoturvavaatimukset ylimitoittaa riskeihin nähden, siitä seuraa ylimääräisiä kustannuksia. Kun tietoturvavaatimukset ovat kaikille osapuolille tiedossa kokonaisvaltaisesti, syntyy tietoturvallinen kokonaisuus. (Ahonen et al. 2021, s.59) Tietoturvaratkaisujen tärkeimpiä ominaisuuksia on luotettavuus automaatiojärjestelmissä ja mahdollisimman vähäinen tuotannon toiminnan häiritseminen.

Automaatiojärjestelmissä tietoliikenteen luotettavuuden varmistaminen on tärkeää, muuten tiedon hyödyllisyys menetetään ja järjestelmän ohjauksista tulee epävakaita. Luotettava tietoliikenne tuotetaan segmentoimalla järjestelmä hallittaviin kokonaisuuksiin ja turvallisilla etäyhteyksillä. Segmentoidussa järjestelmässä segmentit voidaan rajata toisistaan palomuurien avulla, jolloin yhden segmentin häiriö ei pääse vaikuttamaan toiseen segmenttiin suoraan. Eri luotettavuutta vaativien Segmenttien välille tulee suunnitella

luotettavuusrajat, jotta segmenttien toiminnan jatkuvuus on turvattu. Etäyhteyksien suhteen virtuaaliset erillisverkko (VPN) yhteydet on laajalti käytetty, mutta suoraa yhteyttä prosessiverkkoon ei tule sallia, vaan yhteyden tulee kulkea luotettavuusrajojen kautta. Pilvipalveluilla voidaan myös luoda lisää tietoturvaa tietoliikenteeseen. Monesti pilvipalveluiden vikasietoisuus on todella korkealla tasolla ja pilvipalvelualustat pitää sisällään uusimmat tietoturvakorjaukset. Pilvipalveluiden jatkuva kehittyminen pitää ne tietoturvakyvykkäinä uusille hyökkäyksille. (Ahonen et al. 2021, s.150–170)

2.3 Saatavuus

Tiedon saatavuuden ja tietoturvallisuuden ristiriitaisuus automaatiojärjestelmissä on jatkuvaa tasapainottelua. Automaatiojärjestelmät täytyy suunnitella riittävän tietoturvallisiksi ilman, että tiedon saatavuus kärsii liikaa. Tiedon saatavuuden varmentamisen lisäksi on huolehdittava myös laitteiden varaosien saatavuudesta. Kriittisiin osiin järjestelmässä sen käytettävyyden kannalta tulisi suunnitella kahdennusratkaisuja. Pitkät elinkaaret komponenteissa ja ylimääräisten käyttökatkojen välttely automaatiojärjestelmissä asettaa haasteita tietoturvallisuuden suunnittelulle.

Tietoturvapäivitysten asentaminen jatkuvasti käynnissä oleviin automaatiotuotannon prosesseihin ei ole mahdollista milloin tahansa. Usein järjestelmää ei voi pysäyttää ilman suurta vahinkoa tuotannolle, joten tietoturvapäivitykset pitää ajoittaa säännöllisiin huoltokatkoihin. Monesti tuotteet saattavat olla paljon arvokkaampia kuin tuotantoon liittyvä informaatio. Jolloin riskianalyysissä tulee miettiä tietoturvariskin todennäköisyyttä ja vakavuutta verrattuna sen torjumisesta aiheutuvaan tuotannon pysäytykseen. Tietoturvamenetelmien käyttöä vähentää paljon korkeat vaatimukset saatavuudelle. (Ala-Tala et al. 2005)

Automaatiojärjestelmät voivat olla monimutkaisia kokonaisuuksia, jolloin tunnistamattomat seuraukset aiheuttavat paljon haittaa. Kaikki tietoturvatoiminnot tulee testata huolellisesti ennen kuin ne voidaan lisätä automaatiojärjestelmiin. Ohjelmistoja päivittäessä tulee olla tietoinen kaikista toimintojen ja ohjelmistojen välisistä riippuvuussuhteista. Päivityslokin ylläpito on erittäin tärkeää automaatiojärjestelmien eheyden kannalta. Salasanojen osalta moniin automaatiotuotantoihin ei voida lisätä monimutkaisia salauksia tai autentikointeja tuotannon turvallisuuden vuoksi. Hätätapauksissa pitää olla nopea pääsy järjestelmään ja mahdolliseen manuaaliseen tuotannon alas ajoon. (Ala-Tala et al. 2005)

3. KERROKSELLINEN SUOJAUS

Automaatiojärjestelmälle ei ole yhtä oikeaa tietoturvaratkaisua, jolla järjestelmä olisi täydellisesti suojattu ja turvallinen. Organisaatioiden tulee jatkuvasti kehittää ja mukauttaa heidän turvallisuuttaan tunnetuille uhille sekä tuleville uusille uhille. Tärkeää on myös tunnistaa suojattavat kohteet organisaatiossa ja löytää sieltä kriittisimmät kohteet. Aina jossain kohtaan tulee myös taloudellinen puoli vastaan organisaatiolla tietoturvan suhteen, jolloin pitää tehdä valintoja suojaustoimenpiteissä ja valita kustannustehokkaimmat ratkaisut. Organisaation tulee ottaa myös huomioon laskelmoidut riskit, joissa voi olla virheitä. Lisäksi ei ole olemassa teknologiaa, jolla voisi estää ihmistä tekemästä virhettä vahingossa tai tahallaan. (ICS-CERT 2016, s. 2–3).

Syvyyssuuntaisen turvallisuussuunnittelun päällimmäinen sisältö on muodostaa järjestelmän tietoturva moneen eri kerrokseen, jolloin yhden osan pettäessä tulee aina uusi kerros vastaan. Alun perin käsite on peräisin sotilaallisesta strategiasta, jossa ideana oli hidastaa vastustajan etenemistä ja samalla valvoa heidän liikkeitään (ICS-CERT 2016). Syvyyssuuntainen suojaus ei ole yksiselitteinen, jossa tietyt tietoturvaratkaisut täyttämällä järjestelmäsi olisi turvattu. Sen sijaan se pyrkii suojelemaan koko organisaatiota hyödyntämällä organisaation kaikkia resursseja ja näin tuottamaan suojakerroksia yritykselle sen haavoittuvuuksien perusteella tietoturva hyökkäyksille. Eli tietoturva ei nojaudu yhteen suojausratkaisuun vaan on jaoteltu eri vyöhykkeisiin, joilla on kaikilla omat tietoturvatoimenpiteet ja toisiaan tukeva vaikutus.

3.1 Rakenne

Syvyyssuuntainen suojaus rakentuu osista, jotka yhdessä muodostavat tehokkaan tietoturvan organisaatioille. On hyvä huomata, että tietoturva ei ole pelkästään tekniikkaa. Tekniikka on vain yksi osa tietoturvan kokonaisuudesta, joka pitää sisällään fyysiset ratkaisut, riskianalyysin, riskienhallinnan, organisaation menettelytavat ja työntekijöiden tietämyksen tietoturvan suhteen.

Toiminnanohjauksen tasolla organisaatiolla tulisi olla kattava riskienhallintaohjelma. Kyberturvallisuuden huomioiminen miettimällä yrityksen käytänteitä ja menettelytapoja sekä ottamalla huomioon standardit ja suositukset. Ihmisten toiminnan huomioiminen suunnittelemalla toimintatavat ja käytänteet.

Tuotanto puolella tietoturvasuunnittelun lisäksi pitää myös suunnitella järjestelmät ihmisten kannalta turvallisiksi, mikä asettaa enemmän haasteita. Tuotannon tietoturva rakentuu turvallisuuden valvonnalla, joka pitää sisällään hyökkäyksien havaitsemisen, turvatarkastuksien kirjaamisen ja turvallisuustapahtumien valvonnalla. Fyysisellä turvallisuudella tuotanto alueella. Ulkoisten tekijöiden huomioon ottaminen tuottamalla tavarantoimittajien ja ulkoistusten hallintaa sekä myös pilvipalveluiden hyödyntämisellä. (ICS-CERT 2016, s. 4–6)

Teollisuusautomaatiojärjestelmän (IAS) puolesta verkkoarkkitehtuuriin tulee suunnitella yhteiset arkkitehtuurialueet, demilitarisoidut vyöhykkeet (DMZ) ja virtuaaliset lähiverkot. Oleellista on myös palomuurit, autentikointi ja palvelimien etäyhteydet ja isännät. Verkkolaitteiden haavoittuvuuksien hallintaa sekä huomioida kenttälaitteet ja virtuaalikoneet. (ICS-CERT 2016, s. 4–6)

3.2 Toiminta

Edellä mainittu rakenne automaation tietoturvaan vaatii toimiakseen monen eri alan osaamista ja tekniikkaa. Riskienhallinnan osalta organisaation tulisi tunnistaa riskit ja niiden todennäköisyydet. Lisäksi organisaation tulisi määritellä kriittisimmät osat järjestelmästä perustuen sen toimintaan ja tärkeyteen liiketoiminnan kannalta. Näiden jälkeen organisaation tulisi kehitellä turvallisuusjärjestelmä näiden perusteella, joka ottaa huomioon automaatiojärjestelmän eri tasojen tarpeet turvallisuuden osalta, sekä tehdä toimintasuunnitelma, kun on jouduttu mahdollisen tietoturvahyökkäyksen kohteeksi. Organisaation tulisi olla myös tietoinen, kuinka kauan kestää toipua hyökkäyksestä, jotta saadaan tuotanto takaisin toimintaan. Lopuksi organisaation tavoitteena olisi monitoroida ja kehittää järjestelmää jatkuvasti. (ICS-CERT 2016, s. 9–12)

Henkilöstön tietoturvaa parannetaan pitämällä koulutuksia ja varmistamalla henkilöstön tietoisuus tietoturvan suhteen. On pyrittävä saamaan tietoturva osaksi henkilöstön päivittäisiä toimintatapoja ja ajattelumallia sen sijaan, että se olisi jokin erillinen osa työskentelyä. Lisäksi tulee sopia yhteinen kieli tietoturvan suhteen organisaatiossa, jotta pystytään kommunikoimaan paremmin eri osastojen välillä. (Ahonen et al. 2021, s. 25)

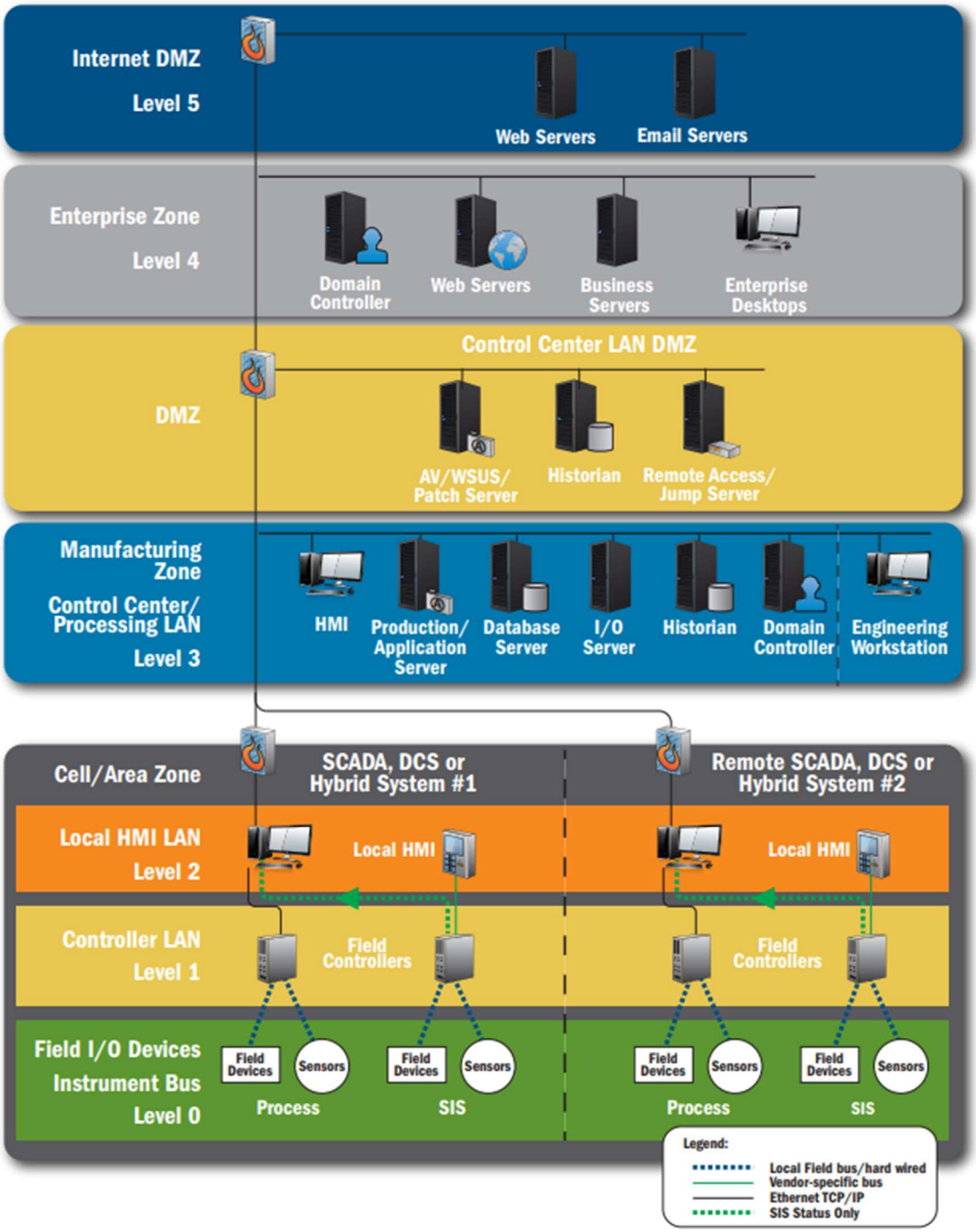
On olemassa lukuisia turvallisuus- ja riskistandardeja, joita organisaatio voi hyödyntää turvallisuuttaan parantaessa. Automaatiossa sovellettavia tietoturvastandardeja ovat IEC 62443 -sarja ja ISO/IEC 27000 -sarja. Standardien avulla tietoturvan kokonaiskuvan hahmottuminen helpottuu ja luodaan yhteinen terminologia tietoturvalle. Standardeja voi-

daan hyödyntää myös tietoturvan sertifioinnissa ja ulkoisten tekijöiden kanssa toimittaessa (Ahonen et al. 2021). Uuden järjestelmän suunnittelu helpottuu, kun hyödynnetään standardeja osana suunnittelua. Standardeilla voidaan tehostaa tuotantoa ja vähentää kuluja. Standardit auttavat myös organisaation laajentuessa maailmalle ja tuovat takuuta organisaation tuotannolle (ISA 2022). Monet automaatio-organisaatiot standardoivat järjestelmiään, mikä lisää kilpailuetua. Esimerkiksi Siemens tarjoaa palveluilleen Defense-in-Depth (DnD) -turvallisuuskonseptin, joka on tehty IEC 62443:n mukaisesti (Siemens 2022).

Organisaation tulee rajata tuotantoalueet fyysisin estein ja tuottaa kulunvalvontaa alueelle pääsemiseksi. Tuotantoalueen sisällä pitää olla jatkuvaa valvontaa ihmisten liikkeistä ja autentikoitu kulku kriittisimpiin kohteisiin. Tuotannonohjauksen huoneisiin ja laitteisiin tulee olla pääsy vain valtuutetuilla. Organisaation tulee kyetä havaitsemaan luvaton järjestelmien käyttöyritys. Automaatiojärjestelmän pitäisi sisältää erilaisia hälytysjärjestelmiä häiriöistä, kuten laitteiden virran katkaisuista, resetoinneista ja kaapeleiden muutoksista. Järjestelmän tulee olla tietoinen kaikista kytketyistä laitteista ja havaita, jos järjestelmään kytketään vieraslaite. Pitää olla suunnitelma käytänteille ja valvonnalle vierailijoiden osalta alueen sisällä sekä alihankkijoille tarkat toimintatavat alueella. (ICS-CERT 2016, s. 13–15)

Verkkoarkkitehtuuri tulee suunnitella ottamalla huomioon monet erilaiset toimijat verkossa. Hyvä verkkoarkkitehtuuri mukautuu organisaation jatkuvaan muutokseen. Verkkoarkkitehtuuri tulisi toteuttaa jakamalla verkon käyttäjät eri luottamustasoihin, kuten kuvassa 2 on esitelty. Verkko voidaan jakaa siten, että ylätasoilla on yritysverkko ja alatasoilla tuotantoverkko, jossa tarvitaan rajoitetumpaa pääsyä. Suurimpia haasteita verkkoarkkitehtuurin suunnittelulle on näiden kahden verkon yhdistäminen toimivaksi kokonaisuudeksi. Usein järjestelmien välillä on kommunikaatiohaasteita, kun yhteistä termistöä ei ole. Myös suuri ero näissä kahdessa verkkoarkkitehtuurissa on suunnitteluelinkaaret. (Ahonen et al. 2021, s. 103–124)

IEC 62433 -standardissa on esitelty tietoturvavyöhykejako automaatiojärjestelmille. Tietoliikenteen kannalta eri tasojen välissä tulisi olla luotettavuusrajoja, jotta tieto pysyisi eheänä. Tasojen välissä tulee olla myös palomuureja estämässä luvatonta pääsyä järjestelmään. Automaation ohjauksen tasolla tietoliikenteen pitää olla luotettavaa ja rajoitettua valtuutetuille tahoille. Kriittiset osat järjestelmästä tulisi segmentoida omiin osiinsa verkossa. (IEC 2022)



Kuva 2. Esimerkki suojatusta verkkoarkkitehtuurista (ICS-CERT 2016, s. 17).

Yritysverkkoon sisältyy yhteys internetiin, yritysviestintä, sähköpostipalvelimet, nimipalvelimet ja IT-järjestelmät. Tässä osassa verkkoa on monia erilaisia riskejä järjestelmien määrän ja liitettävyyksien vuoksi. Automaatiojärjestelmien turvallisuuden kannalta tätä osaa verkosta tulisi pitää epäluotettavana. Tuotantotaso (taso 3 kuvassa 2) yhdistää yritysverkon ja tuotantoverkon kokonaisuudeksi. Turvalliseen tiedonsiirtoon näiden kahden verkon välillä voidaan käyttää yhdyskäytäväratkaisuja, jolloin voidaan välittää tieto

eheänä ja tarkastettuna. Suurin osa monitoroinnista ja ohjauksesta tapahtuu tällä tasolla, joten sen tietoturvan prioriteetti on korkea. Se on kriittinen alue tuotannon hallinnan ja jatkuvuuden kannalta. Riskikohtina ovat liitettävyydet ulkoisiin järjestelmiin ja verkkoihin. (ICS-CERT 2016, s. 17–19) Suoria etäyhteyksiä tuotantoverkkoon ei saisi koskaan sallia, vaan niiden tulisi kulkea luotettavuusrajojen kautta. Etäyhteyksiä luotaessa pitää olla määriteltynä tarkat käytänteet ja tietoturvallisuusperiaatteet.

Alimmat tasot sisältävät ohjaukset, toimilaitteet ja anturit. Näiden tasojen prioriteetti on turvallisuuden kannalta erittäin korkea, koska niiden ohjaustoiminnot vaikuttavat fyysisiin päätelaitteisiin. Nykyään nämä laitteet hyödyntävät tiedonsiirrossa TCP/IP-protokollaa ja muita yleisiä protokollia. Mahdollinen hyökkääjä luultavasti haluaa päästä tuotantoverkkoon. Jokaisen tason suojaaminen ainutlaatuisilla suojauksilla luo kerroksisen puolustuksen hyökkääjää vastaan. Nämä suojaustoimet tarjoavat kerroksellisen puolustuksen ottamalla huomioon tasojen tietoturvavaatimukset.

Jokaisen verkkokerroksen eteen tulisi asettaa palomuuri, joka pitää tunkeutujat ulkona ja päästää läpi vain luvallisen liikenteen. Palomuurit tulee konfiguroida tarkasti ja pitää päivitettyinä, muuten palomuurit voivat sallia huomaamattoman luvattoman liikenteen järjestelmään. Toimistoverkon ja tuotantoverkon välissä olevan palomuurin tulisi sallia vain ehdottoman tarpeellinen tietoliikenne. Organisaation ulkopuolelta voidaan luoda yhteys organisaation verkkoon VPN-ratkaisulla. VPN-ratkaisussa tulee tarkasti määrittää, millaista tietoliikennettä VPN-yhteyden kautta sallitaan sekä VPN-yhteyden luotettava todentaminen. Nykyisissä VPN-laitteissa on palomuurin kaltaiset ominaisuudet, jolloin voidaan rajoittaa läpi päästettäviä tietoliikenneprotokollia. (Ahonen et al. 2021, s.74–76)

Nykyisten kriittisimpien järjestelmän osien tietoturvaa voi parantaa huomattavasti palomuurien lisäksi demilitarisoidulla alueella, jolla tarkoitetaan verkkoeristystä toimistoverkon ja tuotantoverkon eristämiseksi toisistaan. Huomioitavaa on se, että demilitarisoidun alueen yli ei saa sallia suoria yhteyksiä. Ollakseen erityisen luotettava demilitarisoitu alue tarvitsee useita palomuurirajapintoja. Tämä tekee verkosta monimutkaisemman ja lisää kustannuksia.

3.3 Jatkuvuus

Ennen kuin automaatiojärjestelmän tietoturvaa voidaan pitää luotettavana ja toimivana kaikkien tietoturvaratkaisujen jälkeen. Tulee järjestelmän tietoturvaa monitoroida ja ylläpitää kuten muutakin osaa järjestelmästä. Haavoittuvuus voi löytyä mistä tahansa järjestelmän osasta. Ilman valvontaa hyökkääjä voi murtautua järjestelmään ja päästä käsiksi kriittisiin osiin järjestelmästä ennen kuin sitä huomataan ollenkaan. Automaatiojärjestelmissä syntyy jatkuvasti tietoliikennettä molempiin suuntiin automaatiojärjestelmän tasoja, joten se vaatii osakseen monitorointia. Aktiivinen tietoliikenteen monitorointi pitää sisällään toiminnallisen tilan seurantaa, häiriöiden havainnointia ja kunnossapidon. Tietoliikennettä voidaan valvoa verkkoliikennepohjaisella havainnointimenetelmällä. Tietoturvauhkien jatkuvan kehityksen takia tietoturvavalvonnan tulee mukautua tilanteeseen jatkuvasti. (Ahonen et al. 2021, s. 177–183)

Monitoroinnin lisäksi uhkia voidaan havaita myös uhka- ja tiedostelutietoon perustuen erilaisilta tietoturvapalvelutoimijoilta. Lisäksi uhkien etsinnän tuloksena, jolloin järjestelmästä etsitään jälkiä hyökkäyksestä perustuen oletettuihin hyökkäystapoihin. Näin pyritään tunnistamaan uhat, joita ei ole havaittu aktiivisella monitoroinnilla. Uhkan havainnoinnin jälkeen on tärkeää olla ennalta sovitut toimenpiteet, kuinka uhkiin reagoidaan ja myös toimia niiden mukaisesti. Uhkia voidaan havaita myös asettamalla järjestelmään käyttäjätunnus tai tiedosto ansoja, joiden käytöstä nousee hälytys. (Ahonen et al. 2021, s. 179–183)

Järjestelmää voidaan monitoroida järjestelmän itsensä tuottaman lokitiedon perusteella. Lokienhallinnan haasteena on riittävän lokitiedon tuottaminen ja siirtäminen luotettavaan lokivarastoon. Tätä haastetta voidaan helpottaa keskitetyillä lokienhallintajärjestelmillä, kuten SIEM-järjestelmällä. Se voidaan jakaa kahteen toimintoon Tietoturvatietojen hallintaan (SIM) ja turvatapahtumien hallintaan (SEM). Tietoturvatietojen hallinta pitää sisällään lokitietojen keräämisen, raportoinnin ja analysoinnin. Ensisijaisesti isäntäjärjestelmistä ja sovelluksilta. Turvatapahtumien hallintaa tarjoaa reaaliaikaisen monitoroinnin ja tietoturvatapahtumien hallinnan. Se prosessoi loki ja tapahtuma tietoja turvalaitteista, verkkolaitteista ja sovelluksista reaaliajassa. SIEM-järjestelmää käytetään keräämään ja analysoimaan tietoturvatapahtumien dataa reaaliajassa, jolla luodaan reaaliaikainen tilannekuva tietoturvallisuudesta. Kun poikkeamat järjestelmässä huomataan nopeasti, voidaan niihin myös reagoida nopeasti. (Montesino et al. 2012)

Nopean teknologia kehityksen takia tietoturvan ylläpidon tulee olla järjestelmällistä, jolloin tietoturvapäivitysten hallinta nousee keskeiseksi osaksi tietoturvan jatkuvuutta. Tietoturvapäivityksien asentamiseen sisältyy epävarmuutta niiden soveltuvuudesta ja luotettavuudesta järjestelmään, joten ne täytyy testata ennen kuin ne voidaan asentaa järjestelmään. Nollapäivähaavoittuvuuksien kohdalla ohjelmisto kehittäjän julkaistessa tiedot haavoittuvuudesta ja sen korjauspäivityksestä. Asettaa järjestelmän omistaja itsensä haavoittuvaiseksi, koska tietoturvapäivitys tulee ensiksi huolellisesti testata. Tätä uhkaa voidaan torjua väliaikaisesti virtuaalisilla päivityksillä ennen todellista päivitystä. Huomioitavaa on se, että virtuaaliset päivitykset tarvitsevat ihmisten resursseja ja voidaan soveltaa vain tunnettuihin haavoittuvuuksiin. (Copty et al. 2019) Tietoturvapäivityksien hallintaprosessin tulisi sisältää tietoturvapäivitysten versiohistorian ja suunnitellut ajankohdat testattujen päivitysten asentamiselle.

4. YHTEENVETO

Tämän kandidaatintyön tavoite oli perehtyä syvyyssuuntaiseen turvallisuussuunnitteluun ja miten se pyrkii huomioimaan automaatiojärjestelmien vaatimukset etenkin tietoturvan näkökulmasta. Syvyyssuuntaisella turvallisuussuunnittelulla tarkoitetaan tässä työssä suunnittelumallia, jossa turvallisuus pyritään toteuttamaan kerrokselliseksi. Kerroksien tarkoitus on luoda useita vastatoimia turvallisuuden parantamiseksi ja riskien pienentämiseksi.

Tietoturvan tavoitteena on tehdä järjestelmästä hyökkääjälle erittäin hankala ja kallis kohde, jotta hyökkääjä ei näe kannattavaksi hyökätä järjestelmään. Lisäksi mahdollisen hyökkäyksen tullessa hidastaa hyökkääjän etenemistä syvemmälle järjestelmään, jotta se voidaan havaita ennen sen pääsyä kriittisiin osiin järjestelmästä. Tärkeää on myös tehdä järjestelmästä luotettava turvallisuus ratkaisuilla ja luotettavaa operoida.

Automaatiojärjestelmien vaatimukset asettavat paljon huomioitavaa turvallisuussuunnittelulle. Ensisijainen turvallisuus lähtökohta on suunnitella automaatiojärjestelmät turvallisiksi ihmisille operoida niitä tai niiden kanssa. Sen jälkeen tietoturvallista automaatiojärjestelmää suunniteltaessa tulee huomioida niiden täsmälliset rajat vaatimuksien suhteen. On korkeita reaaliaikaisuusrajoja, joista ei voida tinkiä tai tiedon hyödyllisyys putoaa nollaan. Todella tärkeää on säilyttää tiedon luotettavuus automaatiojärjestelmissä. Suunnitella tietoturvaratkaisut, joilla katetaan suurimmat riskit niin, että järjestelmän saatavuus pysyy halutulla tasolla.

On hyvä huomata organisaation turvallisuutta suunniteltaessa, että tekniikalla ei voida yksinään luoda luotettavaa turvallisuutta organisaation. Tekniikan lisäksi tulee myös suunnitella organisaatiolle kattava riskianalyysi ja riskienhallinta suunnitelma. Organisaatiolla tulee olla myös ennalta päätetyt menettelytavat ja toimintamallit eri tilanteisiin. Lisäksi organisaation tulee jatkuvasti ylläpitää työntekijöiden tietämystä tietoturvan suhteen. Liian usein organisaatiot keskittävät resurssinsa pääosin teknisiin ratkaisuihin ja muut turvallisuuden osa-alueet jäävät vähemmälle huomiolle, jolloin organisaatioon muodostuu selviä riskitekijöitä.

Kun lähdetään toteuttamaan syvyyssuuntaista turvallisuussuunnittelua niin se voidaan jakaa kolmeen osa-alueeseen: hallinnolliseen, fyysiseen ja tekniseen. Hallinnolliseen osaan kuuluu toiminnanohjauksessa vaadittu turvallisuussuunnittelu. Fyysiset ratkaisut sisältyvät tuotantoalueiden turvallisuuteen. Tekniset toteutukset koskevat koko organisaatiota ja etenkin sen sisällä tapahtuvaa tietoliikennettä.

Uskon, että tulevaisuudessa kerroksellinen turvallisuussuunnittelu tulee yleistymään entisestään automaatiojärjestelmissä. Kehitetään tehokkaampia ratkaisuja huomioimaan automaatiojärjestelmien korkeat vaatimuskriteerit. Koko ajan opitaan paremmin tunnistamaan riskejä ja ennakoimaan niitä.

Työn tavoitteena oli perehtyä syvyyssuuntaiseen turvallisuussuunnitteluun ja miten sitä olisi mahdollista hyödyntää automaatiojärjestelmissä. Työn tavoite toteutui tuomalla esiin turvallisuussuunnittelun kerroksellinen tarkoitus ja perehtymällä kaikkiin siihen liittyviin osa-alueisiin. Aiheesta oli hyvin tietoa saatavilla, jonka perusteella oli mahdollista perehtyä suunnittelutavan ominaisuuksiin. Automaatiojärjestelmien vaatimuksista työssä käsiteltiin tärkeimmät ominaisuudet, mutta tietoturvan korostaminen jäi vähäiseksi. Työn tavoitteesta työssä jäi kokonaan pois suunnittelutavan hyödyntäminen automaatiojärjestelmissä. Työtä olisi voinut laajentaa enemmän tavoitteen mukaiseksi käsittelemällä suunnittelutapaa automaatiojärjestelmässä. Työtä voisi jatkokehittää ottamalla tarkasteluun mukaan konkreettinen automaatiojärjestelmä, johon turvallisuutta pyrittäisiin kehittämään syvyyssuuntaisen turvallisuussuunnittelun mukaiseksi. Vaikka suunnittelutavan hyödyntäminen automaatiojärjestelmässä jäi käsittelemättä, tämä työ tarjoaa kattavan perehtymisen kyseiseen tietoturvaratkaisuun.

LÄHTEET

Ahonen, P., Seppälä, J., Suortti-Myyry, E. & Tyynelä, M. (2021) Automaation tietoturva: kriittisen tuotannon turvaaminen, Suomen Automaatioseura ry.

Ala-Tala, A., Havaste, A., Tuovinen, E. & Tyynelä, M. (2005) Teollisuusautomaation tietoturva: Verkottumisen riskit ja niiden hallinta, Suomen Automaatioseura ry, Turvallisuusjaosto. Saatavissa: https://researchportal.tuni.fi/en/publications/teollisuusautomaation-tietoturva

Copty, F., Kassis, A., Keidar-Barner, S. & Murik, D. (2019). Deep Ahead-of-Threat Virtual Patching. In: Fournaris, A., Lampropoulos, K., Marín Tordera, E. (eds) Information and Operational Technology Security Systems. IOSec 2018. Lecture Notes in Computer Science(), vol 11398. Springer, Cham. Luettu 10.1.2023. Saatavissa: https://doi-org.libproxy.tuni.fi/10.1007/978-3-030-12085-6_9

Hein, S. PROFINET Security Guideline, Version 2.0 2013. Luettu 15.10.2022. Saatavissa:https://www.prfbus.com/download/profinet-security-guideline

Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Publisher Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2016. Saatavissa: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

ISA Standards: Practical Solutions from Industry Experts, Luettu 21.11.2022. Saatavissa: https://www.isa.org/standards-and-publications/isa-standards

ISA/IEC 62443: Series of Standards. Luettu 14.3.2023. Saatavissa: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Montesino, R., Fenz, S. & Baluja, W. (2012) SIEM-based framework for security controls automation, Bradford: Emerald Group Publishing Limited. pp.248–263.

Müller, T., Walz, A., Kiefer, M., Doran, H. & Sikora, A. (2018) Challenges and prospects of communication security in real-time ethernet automation systems, Publisher: IEEE. Luettu 23.11.2022. Saatavissa: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/8402338

Siemens: Industrial Cybersecurity, Luettu 21.11.2022. Saatavissa: https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html

Siemens: ISA 95 Framework & Layers, Luettu 23.5.2023 Saatavissa: https://www.plm.automation.siemens.com/global/en/our-story/glossary/isa-95-framework-and-layers/53244

Silvola, Risto. *Reaaliaikaiset teollisuus-Ethernet -ratkaisut automaatiojärjestelmissä: diplomityö*. Tampere: Tampereen teknillinen yliopisto, 2006. Print. Saatavissa: https://andor.tuni.fi/permalink/358FIN_TAMPO/1j3mh4m/alma991835285305973