



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MIIA-MARIA HEINÄMÄKI
PROSESSIAUTOMAATION TIETOTURVAN
HALLINTAJÄRJESTELMÄ

Diplomityö

Tarkastajat: professori (emeritus) Hannu Koivisto,
Tietoturva-asiantuntija Jari Seppälä
Tarkastajat ja aihe hyväksytyt
28. marraskuuta 2018

TIIVISTELMÄ

MIIA-MARIA HEINÄMÄKI: Prosessiautomaation tietoturvan hallintajärjestelmä
Tampereen teknillinen yliopisto
Diplomityö, 102 sivua
Marraskuu 2018
Automaatiotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Automaation tietotekniikka
Tarkastajat: professori (emeritus) Hannu Koivisto, tietoturva-asiantuntija Jari Seppälä

Avainsanat: Automaation tietoturva, tietoturvan hallinta, tietoturvan hallintajärjestelmä

Nykyään automaatio on laajalti verkottunut järjestelmä, joka yhdistää prosessitason, toiminnanohjaustason sekä kaikki niiden välillä olevat tasot yhdeksi kokonaisuudeksi. Automaatio voi koostua erityisesti automaatioon tarkoitetuista laitteista, mutta toisaalta siinä voidaan hyödyntää myös toimistoympäristöstä tuttuja IT-laitteita. Kun nämä erilaiset tekniikat sulautetaan yhteen, jotta pystytään vastaamaan nykyautomaation tarpeisiin, syntyy uusia tietoturva-asteita. Lisähaasteensa syntyy myös siitä, että tuotantolaitoksessa laitteet ja tekniikat saattavat olla eri aikakausilta eikä dokumentaatio välttämättä vastaa järjestelmän todellista tilaa.

Automaatiojärjestelmä ja automaation tietoturva sisältävät paljon muutakin kuin vain teknisiä ratkaisuja. Automaation kokonaisturvallisuuden hallinnan kannalta keskeisiä teki-joita yrityksessä ovat muun muassa turvallisuuspolitiikka, liiketoiminnan jatkuvuuden hallinta, riskinhallinta sekä kaikkien näiden soveltaminen prosessiautomaation tietoturvaan. Jotta tätä suurta kokonaisuutta pystytään hallitsemaan, käytössä täytyy olla tarkoituksenmukaiset toimintatapaohjeet.

Tämän tutkimuksen tavoitteena oli rakentaa prosessiautomaation tietoturvan hallintajärjestelmä, joka mahdollistaa systemaattisen ja liiketoimintaprosesseihin sulautetun tietoturvan hallinnan automaatioympäristössä. Tavoitteen saavuttamiseksi tehtiin kirjallisuustutkimus, jossa perehdyttiin automaation tietoturvan hallintajärjestelmämalleihin. Tarkoituksena oli kartoittaa prosessiautomaation tietoturvan hallintajärjestelmän kannalta oleelliset asiat. Tehdyn kirjallisuustutkimuksen pohjalta voitiin todeta, että tarjolla ei ole valmiita ratkaisuja automaation tietoturvan hallintaan, vaan jokaisen organisaation tulee räätälöidä omia tarpeitaan vastaava tietoturvan hallintajärjestelmä.

Tässä tutkimuksessa selvitettiin ensin kohteena olevan tuotantolaitoksen automaation tietoturvan senhetkinen tila, ja selvityksen perusteella laadittiin prosessiautomaation tietoturvan hallintajärjestelmä. Automaation tietoturvatilanteen kartoittamiseksi perehdyttiin muun muassa tuotantolaitoksen toimintatapoihin, organisaatorakenteeseen ja hallintomalleihin sekä olemassa oleviin toimintatapaohjeisiin ja muuhun dokumentaatioon. Kirjallisuustutkimuksen ja automaation tietoturvan tilakartoituksen pohjalta laadittiin tehtaan tarpeita vastaava prosessiautomaation tietoturvan hallintajärjestelmä.

ABSTRACT

MIIA-MARIA HEINÄMÄKI: Information Security Management System for Process Automation

Tampere University of Technology

Master of Science Thesis, 102 pages

November 2018

Master's Degree Programme in Automation Technology

Major: Information Technology in Automation

Examiners: Emeritus Professor Hannu Koivisto, Security Specialist Jari Seppälä

Keywords: Information security for Automation, Information Security Management, Information Security Management System

Automation systems consist of complicated networks that connect the process level to the enterprise resource planning level, and all levels between them to each other. The automation system may include specific automation technologies and also standard IT-technologies used in the office environment. Security challenges arise when these facilities and technologies are used together to meet the needs of the automation. The challenge is increased by the fact that in a production plant the facilities and the equipment may represent various periods of time and the documentation may often be out of date.

When it comes to the automation system and automation information security, attention must also be paid to other aspects than technical solutions. In order to control the entire field as well as possible, the enterprise must take into account e.g. security policy, management of business continuity, risk management as well as applying these issues to the information security for process automation. This is possible only if the enterprise has appropriate guidelines.

The aim of this thesis is to build an information security management system for process automation and thus make it possible to manage automation information security systematically, taking the business processes into account. This thesis includes a literature study on information security management systems for automation. The conclusion of this study was that there are no ready-made solutions; every organisation has to tailor the information security management system that is appropriate to its needs.

In the case study, the first step was to define the actual state of automation information security in the production plant. Based on the results of this step, an information security management system for process automation was built. The security state was defined using procedures, management frameworks, organisation structure and other documentation of the production plant. The objective was to build an information security management system that meets the needs of the production plant.

ALKUSANAT

Viisi kesää sähkö- ja automaatiokunnossapitotöitä Metsä Boardin Takon tehtaalla johti siihen, että sain tehdä myös diplomityöni Takolle. Tästä kiitos kuuluu sähkö- ja automaatiokunnossapidon väelle sekä Jouni Luukkoselle, jonka ideana syntyi työn aihe, ja joka toimi myös työni ohjaajana Takon puolella.

Tampereen teknillisen yliopiston puolelta haluan kiittää työni ohjaajia emeritus professori Hannu Koivistoa sekä tietoturva-asiantuntija Jari Seppälää. Heiltä saatu ohjaus ja palaute auttoivat diplomityöni loppuun saattamisessa.

Tämän lisäksi haluan kiittää kaikkia muita diplomityön vaiheissa mukana olleita, erityisesti Mariannaa ja äitiäni. Kiitos!

Tampereella, 21.11.2018

Miia-Maria Heinämäki

SISÄLLYSLUETTELO

1.	JOHDANTO	1
1.1	Ongelman asettelu	2
1.2	Rajaukset ja tavoitteet	4
1.3	Diplomityön rakenne	5
2.	PROSESSIAUTOMAATION TIETOTURVA JA TAKON AUTOMAATIOJÄRJESTELMÄ	6
2.1	Automaation tietoturva	6
2.2	Uhat, riskit ja liiketoimintavaikutukset	9
2.3	Metsä Board Tako	13
2.4	Esimerkkejä toteutuneista tietoturvahyökkäyksistä	17
2.5	Perusteluja diplomityön tarpeellisuudesta	18
3.	KIRJALLISUUSTUTKIMUS	20
3.1	Standardi SFS-IEC 62443-2-1	20
3.1.1	Riskianalyysi	23
3.1.2	Riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla	24
3.1.3	Automaation tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen	28
3.1.4	Standardin SFS 62443-2-1 yhteenveto	28
3.2	NIST:n kyberturvallisuuden kehysmalli	30
3.2.1	Tunnistusvaihe	31
3.2.2	Suojautumisvaihe	34
3.2.3	Havaitse	38
3.2.4	Reagoimisvaihe	39
3.2.5	Palautuminen	41
3.2.6	NIST:n kehysmallin yhteenveto	42
3.3	CPNI:n automaation tietoturvan kehysmalli	44
3.3.1	Hallinto ja tietoturvastrategia	45
3.3.2	Päätoiminnot	50
3.3.3	CPNI:n kehysmallin yhteenveto	56
3.4	Kirjallisuustutkimuksen tulos	57
3.4.1	Prosessiautomaation tietoturvan hallintajärjestelmän perustamis- ja käyttöönotto vaihe	57
3.4.2	Ihmisten sitouttaminen automaation tietoturvan hallintaan	58
3.4.3	Automaatiojärjestelmän elinkaaren hallinta ja tietoturva	59
4.	HALLINTAJÄRJESTELMÄSSÄ HYÖDYNNETTÄVÄT TAKON TOIMINTAMALLIT	61
4.1	Yritysturvallisuuspolitiikka	61
4.2	Liiketoiminnan jatkuvuudenhallinta	61
4.2.1	Yleistä jatkuvuudenhallinnasta	62
4.2.2	Jatkuvuudenhallintastrategia	63

4.2.3	Liiketoiminnan vaikutusanalyysi.....	64
4.2.4	Jatkuvuussuunnitelma.....	65
4.2.5	Tekninen toivutussuunnitelma.....	66
4.3	Riskienhallinta.....	67
4.4	Yleinen tietoturva.....	70
4.4.1	Tietoturvallisuuspolitiikka.....	70
4.4.2	Henkilöstön tietoturvaohje	71
4.4.3	Tietoturvan organisointi Metsä Group -konsernissa	71
4.4.4	Ohje tietoturvan auditointisuunnitelman tekoon	72
4.4.5	Tietoturvallisen elinkaarenhallinnan periaate.....	73
4.5	Automaation tietoturvaan ja laitehankintoihin liittyvä dokumentaatio	73
4.5.1	Tietoturva ja IT-laitehankinnat prosessiautomaatiossa	73
4.5.2	Tietoturvaohje automaatiotoimittajille	74
4.6	Yhteenveto toimintamalleista.....	75
5.	PROSESSIAUTOMAATION TIETOTURVAN HALLINTAJÄRJESTELMÄ ...	77
5.1	Hallintajärjestelmän perustaminen ja käyttöönotto.....	80
5.1.1	Liiketoimintaperustelu.....	80
5.1.2	Organisaatio- ja hallintomuutokset.....	82
5.1.3	Jatkuvuudenhallinta- ja riskinhallintastrategia	83
5.1.4	Sovellusalan kartoitus.....	83
5.1.5	Järjestelmän kehittäminen ja valvonta.....	84
5.2	Automaation tietoturvatietoisuuden ja -taitojen kehittäminen	84
5.2.1	Kouluttaminen	85
5.2.2	Ohjeistaminen.....	85
5.2.3	Työskentelysuhteiden kehittäminen	85
5.3	Automaatiojärjestelmän elinkaaren hallinta.....	86
5.3.1	Toimitusketjun riskinhallinta.....	88
5.3.2	Tietoturvavaatimusten sisällyttäminen toimitussopimukseen	88
5.3.3	Järjestelmän suunnittelu, toteutus ja käytöstä poisto.....	88
5.3.4	Automaation tietoturvan hallinta.....	89
5.3.5	Operatiivinen turvallisuus	95
5.4	Yhteenveto prosessiautomaation tietoturvan hallintajärjestelmästä	95
6.	YHTEENVETO JA POHDINTAA TYÖSTÄ	97
	LÄHTEET.....	99

KUVALUETTELO

<i>Kuva 1. Automaation pyramidimalli [34].....</i>	<i>2</i>
<i>Kuva 2. Automaatiosuunnittelun elinkaarimalli [muokattu lähteestä 36].....</i>	<i>8</i>
<i>Kuva 3. Riskikaavio [muokattu lähteestä 38, s. 31].....</i>	<i>11</i>
<i>Kuva 4. Tietoturvan hallinta [Muokattu lähteistä 41, s. 30 ja 17].</i>	<i>12</i>
<i>Kuva 5. MES –rajapinnat. [Muokattu lähteestä 37].....</i>	<i>15</i>
<i>Kuva 6. Tietoturvallisuuden hallintajärjestelmä [muokattu lähteestä 39, s. 37].....</i>	<i>22</i>
<i>Kuva 7. Automaation tietoturvan kehysmalli [muokattu lähteestä 27, s. 5].....</i>	<i>45</i>
<i>Kuva 8. Tietoturvan hallintomallin perustaminen [muokattu lähteestä 24, s. 3].</i>	<i>46</i>
<i>Kuva 9. Liiketoimintariskien hallinta [muokattu lähteestä 30, s. 3].....</i>	<i>47</i>
<i>Kuva 10. Automaatiojärjestelmän elinkaaren hallinta [muokattu lähteestä 29, s. 4].....</i>	<i>48</i>
<i>Kuva 11. Tietoisuuden ja tietoturvataitojen kehittäminen [muokattu lähteestä 28, s. 3].....</i>	<i>50</i>
<i>Kuva 12. Tietoturvaparannusten valinta ja käyttöönotto [muokattu lähteestä 33, s. 3].....</i>	<i>51</i>
<i>Kuva 13. Haavoittuvuuksien hallinta [muokattu lähteestä 32, s. 4].....</i>	<i>52</i>
<i>Kuva 14. Kolmansien osapuolien riskinhallinta [muokattu lähteestä 31, s. 3].</i>	<i>53</i>
<i>Kuva 15. Reagointipotentiaalin kehittäminen [muokattu lähteestä 25, s. 3].....</i>	<i>55</i>
<i>Kuva 16: Jatkuvuudenhallinnan elinkaari [muokattu lähteestä 15].</i>	<i>62</i>
<i>Kuva 17. Toivutusvaatimusten aikajana [muokattu lähteestä 8].....</i>	<i>64</i>
<i>Kuva 18. Riskienhallintaprosessi [muokattu lähteestä 22].</i>	<i>68</i>
<i>Kuva 19. Hallintajärjestelmän malli [muokattu lähteestä 4, s. 13].....</i>	<i>77</i>
<i>Kuva 20. Prosessiautomaation tietoturvan hallintajärjestelmä.</i>	<i>78</i>
<i>Kuva 21. Hallintajärjestelmän perustaminen ja käyttöönotto.</i>	<i>80</i>
<i>Kuva 22. Tietoturvataitojen ja tietoisuuden kasvattaminen.....</i>	<i>84</i>
<i>Kuva 23. Automaatiojärjestelmän elinkaarenhallinta.</i>	<i>86</i>
<i>Kuva 24. Tietoturvallisen elinkaarenhallinnan periaate [muokattu lähteestä 13].....</i>	<i>87</i>
<i>Kuva 25. Automaation tietoturvan hallinta.....</i>	<i>89</i>
<i>Kuva 26. Tietoturvan hallintajärjestelmä – arviointivaihe [muokattu lähteestä 39].....</i>	<i>91</i>
<i>Kuva 27. Tietoturvan hallintajärjestelmän elinkaari – kehitys- ja toteutusvaihe [muokattu lähteestä 39].....</i>	<i>92</i>
<i>Kuva 28. Tietoturvan hallintajärjestelmän elinkaari – ylläpitovaihe [muokattu lähteestä 39].....</i>	<i>93</i>

TAULUKKOLUETTELO

<i>Taulukko 1. Turvallisuuustasot [muokattu lähteestä 38, s.50].</i>	13
<i>Taulukko 2: NIST:n kyberturvallisuuden kehysmalli [muokattu lähteestä 4, s. 23].</i>	31
<i>Taulukko 3. Omaisuuden hallinta tunnistusvaiheessa [muokattu lähteestä 4, s. 24–25].</i>	32
<i>Taulukko 4. Tunnistusvaiheen liiketoimintaympäristö [muokattu lähteestä 4, s. 25].</i>	32
<i>Taulukko 5. Tunnistusvaiheen hallinto-osuus [muokattu lähteestä 4, s. 25–26].</i>	33
<i>Taulukko 6. Tunnistusvaiheen riskinarviointi [muokattu lähteestä 4, s. 26–27].</i>	33
<i>Taulukko 7. Tunnistusvaiheen riskinhallintastrategia [muokattu lähteestä 4, s. 27–28].</i>	34
<i>Taulukko 8. Toimitusketjun riskinhallinta [muokattu lähteestä 4, s. 28–29].</i>	34
<i>Taulukko 9. Suojautumisvaiheen identiteetin- ja pääsynhallinta [muokattu lähteestä 4, s. 29–31].</i>	35
<i>Taulukko 10. Suojautumisvaiheen tietoisuus ja koulutus [muokattu lähteestä 4, s. 31–32].</i>	36
<i>Taulukko 11. Suojautumisvaiheen tietoturva [muokattu lähteestä 4, s. 32–33].</i>	36
<i>Taulukko 12. Suojautumisvaiheen tietoturvaprosessit ja menettelyt [muokattu lähteestä 4, s. 33–36].</i>	37
<i>Taulukko 13. Suojautumisvaiheen huolto-osuus [muokattu lähteestä 4, s. 36].</i>	37
<i>Taulukko 14. Suojautumisvaiheen suojaava teknologia [muokattu lähteestä 4, s. 36–37].</i>	38
<i>Taulukko 15. Havaitsemisvaiheen poikkeukset ja tapahtumat [muokattu lähteestä 4, s. 37–38].</i>	38
<i>Taulukko 16. Havaitsemisvaiheen jatkuva turvallisuuden seuranta [muokattu lähteestä 4, s. 38–40].</i>	39
<i>Taulukko 17. Havaitsemisvaiheen havainnointiprosessit [muokattu lähteestä 4, s. 40].</i>	39
<i>Taulukko 18. Reagointivaihe reagointisuunnitelma [muokattu lähteestä 4, s. 41].</i>	40
<i>Taulukko 19. Reagointivaiheen tiedottaminen [muokattu lähteestä 4, s.41].</i>	40
<i>Taulukko 20. Reagointivaiheen analyysi [muokattu lähteestä 4, s. 42].</i>	40
<i>Taulukko 21. Reagointivaiheen lievennykset [muokattu lähteestä 4, s. 42–43].</i>	41
<i>Taulukko 22. Reagointivaiheen parannukset [muokattu lähteestä 4, s. 43].</i>	41
<i>Taulukko 23. Palautumisvaiheen toipumissuunnitelma [muokattu lähteestä 4, s. 43].</i>	42
<i>Taulukko 24. Palautumisvaiheen parannukset [muokattu lähteestä 4, s. 43].</i>	42
<i>Taulukko 25. Palautumisvaiheen viestintä [muokattu lähteestä 4, s. 44].</i>	42
<i>Taulukko 26. Riskien arviointi [muokattu lähteestä 22].</i>	69
<i>Taulukko 27. Riskimatriisi [muokattu lähteestä 22].</i>	69
<i>Taulukko 28. Riskimatriisin värikoodien selitykset [muokattu lähteestä 22].</i>	70
<i>Taulukko 29. Liiketoimintaperustelun osat [muokattu lähteistä 35 ja 39].</i>	81

LYHENTEET JA MERKINNÄT

APT	engl. Advanced Persistent Threat, kohdistettu hyökkäys
CPNI	engl. Centre for the Protection of National Infrastructure, Iso-Britannian valtiollisen infrastruktuurin suojauskeskus
ERP	engl. Enterprise Resource Planning, toiminnanohjausjärjestelmä
FAT	Factory Acceptance Test, Tehdastestaus
FSC	engl. Forest Stewardship Council, vastuullisen metsänhoidon sertifikaatti
ICS	engl. Industrial Control System, teollisuuden ohjausjärjestelmä
IEC	engl. International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio
IPC	engl. Interprocess communication, prosessien välinen kommunikointi
ISO	engl. International Organization for Standardization, Kansainvälinen standardisoimisliitto
LAN	engl. Local Area Network, lähiverkko
MES	engl. Manufacturing Execution System, tuotannonohjausjärjestelmä
NCSC	engl. National Cyber Security Centre, Iso-Britannian kansallinen kyberturvallisuuskeskus
NIST	engl. National Institute of Standards and Technology, Yhdysvaltojen kansallinen standardi- ja teknologiainstituutti
OHSAS	engl. Occupational Health and Safety Assessment Series, työturvallisuusjärjestelmäsertifikaatti
PEFC	engl. Programme for the Endorsement of Forest Certification, kansainvälinen metsäsertifiointijärjestelmä
PLC	engl. Programmable Logic Controller, ohjelmoitava logiikka
SANS	SANS-instituutti: tietoturvakoulutukset, sertifioinnit ja tutkimus
SESKO	sähkötekniikan alan kansallinen standardointijärjestö
SFS	Suomen standardisoimisliitto
TCP/IP	engl. Transmission Control Protocol/Internet Protocol, tietoliikenneprotokollaperhe

1. JOHDANTO

Vuonna 1865 Tammerkosken alajuoksulle perustettiin Suomen ensimmäinen puuhiomo. Hiomon rinnalle nousi paperitehdas, joka myöhemmin muutettiin kartonkitehtaaksi. Tänä päivänä hiomo on poistettu käytöstä, mutta tehdas, joka nykyisin tunnetaan nimellä Tako, työllistää yhä noin 210 henkilöä.

Metsä Group -konsernin Board liiketoimintayksikköön kuuluva Tako valmistaa laadukkaita taivekartonkeja muun muassa tupakka- ja elintarviketeollisuudelle. Tuotteita sitovat tiukat laatuvaatimukset, ja niille on myönnetty useita sertifikaatteja, joiden asettamat vaatimukset tuotteiden tulee täyttää. Toimintaa rajoittavat ja valvovat myös useat muut tahot, ja lisähaasteen toiminnalle tuo tehtaan sijainti kaupungin ydinkeskustassa, sillä ympäristövaatimukset ovat erityisen tiukat. Takon tehtaan korkean iän myötä automaation laitteistot ohjelmistoinen ovat elinkaariensa eri vaiheissa, mikä lisää järjestelmän eri osien integroinnin vaatavuustasoa.

Tämän päivän automaatio on verkottunutta ja siinä hyödynnetään suuria määriä tietoa. Automaatiossa ainoa uhka ei ole tiedon joutuminen väärin käsiin, vaan tietoturvan laiminlyönti voi suoraan uhata laitteita, ympäristöä tai jopa ihmisten terveyttä. Tästä syystä onkin erityisen tärkeää sitoa automaation tietoturva yhdeksi osaksi liiketoimintaprosesseja ja siten varmistua kokonaisvaltaisesta turvallisuudesta.

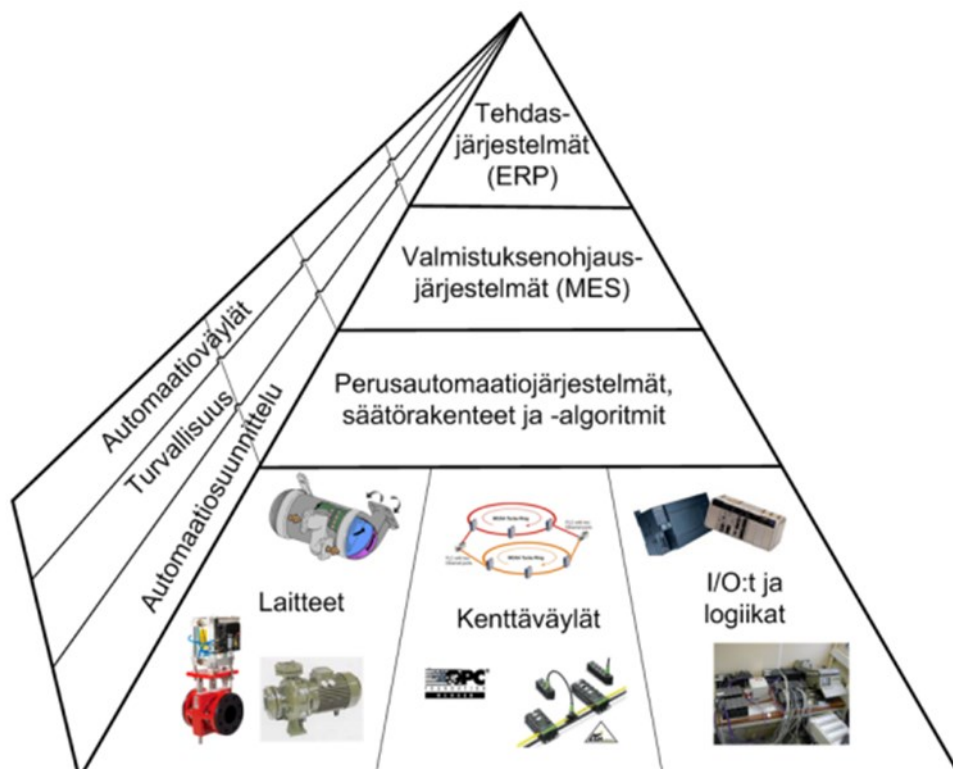
Automaation tietoturvasta ja sen hallinnasta on tehty paljon aiempaa tutkimusta, ja aihepiiriä tutkitaan yhä enenevässä määrin niin yksityishenkilöiden, yritysten kuin myös valtiollisten tahojen toimesta. Useiden vakavien teollisuusautomaatiota koskettaneiden tietoturvatapahtumien seurauksena on herätty aiheen ajankohtaisuuteen ja tärkeyteen. Suomen kielellä tutkimusta on kuitenkin tehty jokseenkin rajallisesti. Merkittäviä Suomessa tehtyjä tutkimuksia ovat muun muassa huoltovarmuuskeskuksen KYBER2020-hanke, johon kuuluvat KYBER-TEO [1] sekä KYBER-ENE -projektit. Näiden avulla pyritään jalkauttamaan kyberturvallisuusosaamista eri toimialoille. Keskeinen, hyvät pohjatiedot antava teos on vuonna 2005 julkaistu Teollisuusautomaation tietoturva [41]. Lisäksi valtiovarainministeriö ylläpitää digitaalisen turvallisuuden kehittämistä ja ohjausta koskevaa ohjeistusta (VAHTI-toiminta), jota yritykset voivat hyödyntää.

Yksi suuri aihepiirin tutkimukseen liittyvä ongelma on se, että iso osa teoksista on englanninkielisiä, hyvin teknisiä, yksityiskohtaisia ja laajoja kokonaisuuksia, jolloin niihin perehtyminen on raskasta, aikaa vievää ja vaatii teknistä osaamista. Yksi tämän tutkimuksen tavoitteista onkin saada koottua keskeinen tieto yksiin kansiin niin yksinkertaisesti ja

helppolukuisesti, että jokainen teknisen taustan omaava henkilö pystyy lukemaan ja ymmärtämään teoksen sisällön, etsimään sen avulla tarvittavat lisätiedot ja soveltamaan lukemansa tiedot käytäntöön. On myös ymmärrettävä, että yksikään teos ei pysty tarjoamaan valmiita ratkaisuja vaan jokaisen organisaation täytyy räätälöidä automaation tietoturva vastaamaan omia tarpeitaan.

1.1 Ongelman asettelu

Takon tehtaan korkeasta iästä johtuen tehdasautomaatio on peräisin eri aikakausilta ja automaatiojärjestelmän eri osien integraatio on toteutettu kullekin aikakaudelle ominaisella tavalla. Aiemmin tietoturvaa ei pidetty kovin suurena uhkana, koska automaatiojärjestelmien integrointi toteutettiin käyttäen tekniikoita, jotka eivät mahdollistaneet tieturvahyökkäyksiä siinä laajuudessa kuin uudet integrointitekniikat [35, kpl 3]. Tämän päivän automaatio on lähentynyt IT-puolen kanssa, ja näiden kahden muodostama kokonaisuus saattaa sisältää harmaita alueita, joiden vastuualueet ovat epäselviä. Tästä johtuen järjestelmään on voinut jäädä osa-alueita, joiden tietoturva ei ole riittävällä tasolla. Yhteisten sääntöjen puutteen ja verkottuneisuuden lisääntymisen myötä (kuva 1) automaatiojärjestelmän dokumentaatio ja tietoturva eivät ole välttämättä ajan tasalla.



Kuva 1. Automaation pyramidimalli [34].

Jos yrityksen automaatiojärjestelmä ei ole kohdannut merkittäviä tietoturvatapahtumia, uhkia ei välttämättä tiedosteta tai ne sivuutetaan, ja oletetaan tietoturvan olevan riittävällä

tasolla. Mahdollisten tuhojen laajuus saattaa olla hämärän peitossa eikä välttämättä hahmoteta, kuinka suurta vahinkoa automaatiojärjestelmään tehty hyökkäys saattaa aiheuttaa.

Nykyisin automaatioissa hyödynnetään paljon IT-puolen tekniikoita niiden helpon integroitavuuden ja edullisuuden vuoksi. Tässä huomioitavaa on se, että vaikka automaatiojärjestelmässä käytettäisiin samoja laitteita, ei tietoturva välttämättä voida toteuttaa samalla tavalla kuin IT-maailmassa. Kasvaneen integraatioasteen myötä automaatiojärjestelmät ovat yhteydessä IT-järjestelmien kanssa ja tiedolle asetetut turvallisuus-, luotettavuus- ja saatavuusvaatimukset saattavat muuttua siirryttäessä järjestelmän osien välillä. Tästä johtuen olisi tärkeää, että automaation tietoturvasta vastaavilla henkilöillä olisi riittävä osaaminen sekä IT-puolen että automaation laitteistoista sekä niille asetettujen vaatimusten eroista.

Tänä päivänä on yleistä, että automaatiojärjestelmän eri osakokonaisuudet ostetaan muualta, jolloin järjestelmään liittyy ulkopuolisia toimijoita. Tämä on jo itsessään riski, ja sopimusteknisistä asioista huolehtiminen onkin ensiluokkaisen tärkeää, jotta varmistetaan siitä, että toiset ja kolmannet osapuolet huolehtivat omien järjestelmiensä ja niiden liityntöjen tietoturvasta. Dokumentaation tulee olla ajan tasalla sekä ulkopuolisen toimijan osalta että yrityksen sisällä. Tarkka dokumentaatio helpottaa ymmärtämään automaatiojärjestelmän rakenteen. Jos rakennetta ei ymmärretä, ei myöskään sen tietoturvasta voida huolehtia asianmukaisesti.

Automaation tietoturva ei tarkoita pelkästään teknisiä ratkaisuja ja prosessin turvallisuutta, vaan valtaosa siitä koostuu ihmisen toimintatavoista. Kenties suurin uhka automaatiojärjestelmän tietoturvalle on ihmisten tietämättömyys ja välinpitämättömyys. Tästä johtuen olisi tärkeää huolehtia siitä, että kaikilla asianosaisilla on riittävä tietämys automaation tietoturvasta. Lisäksi saatavilla pitäisi olla yksiselitteinen ohjeistus kaikesta automaation tietoturvaan liittyvästä toiminnasta, jotta toiminta olisi johdonmukaista ja turvallista.

Kuten huomioitavien asioiden määrästä voidaan päätellä, prosessiautomaation tietoturva on laaja kokonaisuus, jossa haasteeksi osoittautuu kokonaisuuden hallinta. Myös tietoturvan nykytilan kartoitus on haastavaa, koska kartoitettavia osa-alueita on lukuisia, ja määrän tuomien haasteiden lisäksi myös ristivaikutusten huomiointi nostaa vaikeustasoa.

Monesti yrityksissä ei ole budjetoitu riittävästi resursseja automaation tietoturvaan, koska siihen liittyviä liiketoimintariskejä ei tiedosteta. Vastuualueet organisaation sisällä saatavat olla määritelty puutteellisesti, jolloin joitain tietoturvan osa-alueita saattaa jäädä huomioimatta. Riskien hallintaa koskevat päätökset ja siten myös priorisointi, resursointi ja budjetointi kuuluvat yritysjohdolle. On huolehdittava siitä, että yritysjohto saa tarvitta-

van informaation oikeiden päätösten tekemiseen. Huomioitavaa on myös, että tietoturvanhallinta ei ole kertaluontoinen korjaustoimenpide, vaan dynaaminen prosessi, joka vaatii jatkuvaa huomiota ja resursseja [18, 39].

1.2 Rajaukset ja tavoitteet

Tämän työn tavoitteena on kartoittaa prosessiautomaation tietoturvan nykytila, ja erityisesti pureutua tietoturvan hallinnassa esiintyviin ongelmiin. Kun ongelmat on kartoitettu, luodaan prosessiautomaation tietoturvan hallintajärjestelmä, joka pyrkii korjaamaan ongelmakohdat ja lisäämään automaation tietoturvan hallittavuutta ja siten kohentamaan automaation tietoturvan tilaa.

Työn tutkimuksellisenä tavoitteena on selvittää, miten prosessiautomaation tietoturvaa voidaan hallita. Tavoitteeseen pääsemiseksi tutustutaan kirjallisuudessa esiintyviin hallintajärjestelmämalleihin ja niiden sisältöihin, jotta pystytään muodostamaan kuva siitä, mistä tietoturvan hallinta muodostuu. Tämän tiedon avulla muodostetaan keinot prosessiautomaation tietoturvan nykytilan kartoittamiselle ja samalla saadaan kerättyä pohjatiedot sille, miten prosessiautomaation tietoturvan hallintajärjestelmä voidaan rakentaa.

Kun on kartoitettu, mistä automaation tietoturva ja sen hallinta muodostuu, voidaan kartoittaa Takon prosessiautomaation tietoturvan nykytila. Nykytilan kartoittamiseksi tutustutaan muun muassa tehtaan toimintatapoihin ja hallintomalleihin. Tämän lisäksi käydään läpi olemassa oleva automaation tietoturvaan liittyvä dokumentaatio sekä muu dokumentaatio, jota voidaan hyödyntää automaation tietoturvan hallinnassa. Jotta prosessiautomaation tietoturvan hallintajärjestelmästä saataisiin mahdollisimman hyvin konsernin toimintatapojen mukainen kokonaisuus, pyritään hallintajärjestelmän muodostamisessa hyödyntämään mahdollisimman paljon olemassa olevia toimintatapamalleja sekä muuta olemassa olevaa dokumentaatiota.

Kirjallisuustutkimukseen valikoitui julkaisuja kolmelta eri toimijalta, jotka ovat Suomen Standardoimisliitto (SFS), Yhdysvaltojen kansallinen standardi- ja teknologiainstituutti (engl. National Institute of Standards and Technology, NIST) ja Iso-Britannian valtiollisen infrastruktuurin suojauskeskus (engl. Centre for the Protection of National Infrastructure, CPNI). SFS on julkaissut kansainvälisen standardointiliiton automaation tietoturvaa koskevaa aineistoa suomeksi, NIST on Yhdysvalloissa toimiva järjestö, jolla on ohjeistus kyberturvallisuudesta, ja CPNI on vastaava järjestö Isossa-Britanniassa. Näiden lisäksi tarjolla on muitakin vartenotettavia teoksia, ohjeistuksia ja tutkimuksia, muun muassa SANS-politiikat (SANS-instituutti) ja huoltovarmuuskeskuksen KYBER-hankkeet.

Yksi tämän työn tavoitteista on herättää keskustelua ylemmässä portaassa ja saada sitä kautta resursseja prosessiautomaation tietoturvan hallintajärjestelmän perustamista ja käyttöönottoa varten. Pelkästään asenteiden muutos on iso askel oikeaan suuntaan, mutta

erityisen hyvin tämä työ on onnistunut, jos sen avulla saadaan resursseja tietoturvan hallintaan ja pystytään kehittämään henkilöstön toimintatapoja tietoturvallisempaan suuntaan.

Tarkasteltava aihealue on laaja, ja sen vuoksi tarkastelua joudutaan rajaamaan. Yksityiskohtien ja teknisten ratkaisujen sijaan työssä käydään asioita läpi yleisellä tasolla ja kartoitetaan suuntaviivat, joiden mukaan luodaan Takon kartonkitehtaan tarpeet huomioon ottava automaation tietoturvan hallintajärjestelmä.

1.3 Diplomityön rakenne

Toisessa kappaleessa tutustutaan työn kannalta oleellisiin taustatietoihin. Kappaleessa esitellään automaatiojärjestelmiä yleisellä tasolla, niihin liittyvää tietoturvaa sekä IT- ja automaatiojärjestelmien eroja tietoturvanäkökulmasta. Seuraavaksi tarkastellaan automaation tietoturvaan liittyviä uhkia ja riskejä sekä niiden hallintaa. Tämän jälkeen pureudutaan Takon liiketoimintaan sekä tehtaan prosessiautomaation tietoturvaan ja sen nykytilaan. Lopuksi tutustutaan muutamiin toteutuneisiin tietoturvahyökkäyksiin ja viimeiseksi kootaan yhteen perustelut tämän diplomityön tarpeellisuudelle.

Kolmannessa kappaleessa tehdään kirjallisuustutkimus Suomen standardisoimisliiton käsikirjasta SFS-IEC 62443-2-1 [39], Yhdysvaltojen kansallisen standardi- ja teknologia-instituutin kyberturvallisuuden kehysmallista [4] sekä Iso-Britannian valtiollisen infrastruktuurin suojauskeskuksen julkaisemasta teoskokonaisuudesta Security for Industrial Control Systems, joka koostuu kymmenestä julkaisusta [24–33]. Kirjallisuustutkimuksella pyritään kartoittamaan keinoja prosessiautomaation tietoturvan hallintaan, ja mitä osa-alueita hallintajärjestelmään kuuluu. Kappaleen lopussa suoritetaan yhteenveto, jossa vertaillaan teoksia ja kootaan yhteen niiden keskeinen sisältö, jota voidaan hyödyntää diplomityön muissa vaiheissa.

Neljännessä kappaleessa tarkastellaan Takon, Metsä Boardin ja Metsä Group -konsernin olemassa olevia toimintatapaohjeita sekä muuta dokumentaatiota niiltä osin kuin sitä voitaisiin hyödyntää tässä tutkimuksessa. Neljännessä kappaleessa käsiteltävät dokumentit valikoidaan kolmannen kappaleen kirjallisuustutkimuksen perusteella.

Viidennessä kappaleessa rakennetaan kolmannen ja neljännen kappaleen tuloksien pohjalta automaation tietoturvan hallintajärjestelmä. Hallintajärjestelmän rakentamisessa tarkoituksena on hyödyntää Metsä Group -konsernin olemassa olevaa dokumentaatiota mahdollisimman paljon, jolloin luotu hallintajärjestelmä noudattaisi konsernin linjausta ja välttyttäisiin päällekkäisyyksiltä.

Kuudennessä kappaleessa tehdään yhteenveto siitä, miten diplomityö onnistui ja saavutettiin sille asetetut tavoitteet. Lisäksi käydään läpi, mitä jatkotutkimuskohteita diplomityön perusteella nousi esiin ja pohditaan diplomityöntekoprosessia.

2. PROSESSIAUTOMAATION TIETOTURVA JA TAKON AUTOMAATIOJÄRJESTELMÄ

Tässä kappaleessa perehdytään prosessiautomaation tietoturvaan, miten järjestelmät ovat muuttuneet ajan saatossa, ja mitä vaikutuksia muutoksilla on ollut järjestelmien tietoturvaan. Lisäksi käydään läpi automaation tietoturvaan liittyviä uhkia, haavoittuvuuksia ja riskejä ja niiden vaikutuksia liiketoiminnalle. Tämän jälkeen tutustutaan lyhyesti Metsä Board -konsernin Takon tehtaan liiketoimintaan sekä tehtaan prosessiautomaatioon ja automaatiojärjestelmän rakenteeseen. Tässä yhteydessä esitellään tehtaan liiketoiminnan tavoitteet, sekä mitä vaatimuksia ja rajauksia toiminnalle ja siten myös automaation tietoturvalle on asetettu. Lisäksi listataan muutamia teollisten järjestelmien kohtaamia toteutuneita tietoturvahyökkäyksiä seurauksineen. Kappaleen lopussa perustellaan prosessiautomaation tietoturvan hallintajärjestelmän tarpeellisuutta.

2.1 Automaation tietoturva

Teollisuuden automaatiojärjestelmät hyödyntävät yhä enemmän standardoituja IT-ratkaisuja, kuten esimerkiksi Microsoftin Windows-käyttöjärjestelmiä, Web-pohjaisia sovelluksia, langattomia yhteyksiä sekä TCP/IP-tietoliikenneprotokollaperhettä (engl. Transmission Control Protocol/Internet Protocol) [6, s. 3; 38, s. 28; 27, s. 4]. Teknologiamuutoksien seurauksena ennen yksinoikeudella valmistettua laitteistoa korvataan hyllytävänä saatavana olevilla IT-ohjelmistoilla ja -laitteistoilla, jotka kytkeytyvät toisiinsa tehdasverkon välityksellä [6; 19, s. 234; 38, s. 28; 27, s. 4]. Tämä trendi laskee tuotteiden hintoja ja parantaa niiden saatavuutta, helpottaa tiedonkeruuta, toiminnan ja tuotannon ohjausta sekä automaatiojärjestelmän etäkäyttöä, mutta sillä on myös varjopuolensa. [19, s. 217; 35, s. 42]

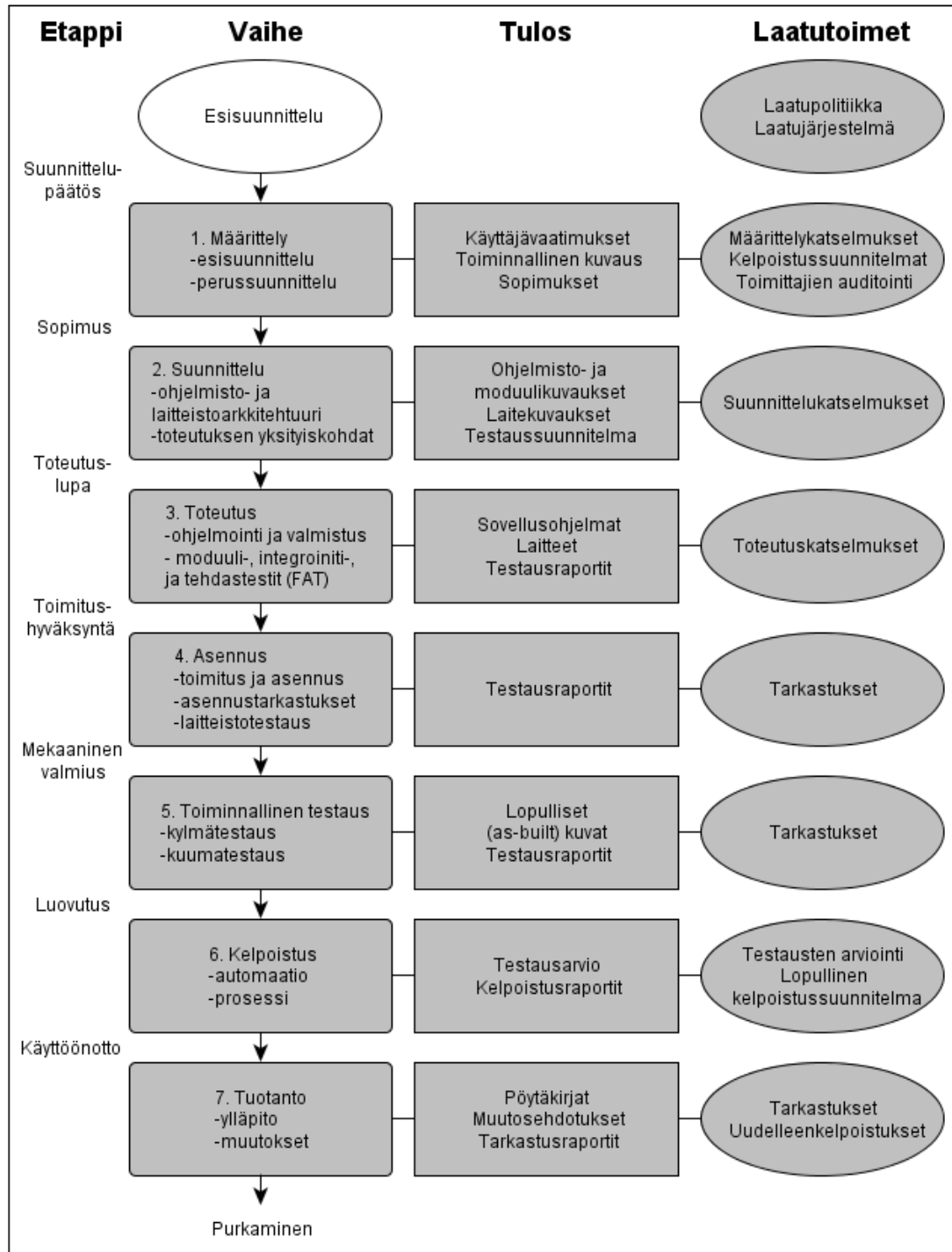
Automaatiojärjestelmien kehittyminen hyödyntämään IT-tekniologiaa altistaa ne uusille uhille, joita vastaan niillä ei välttämättä ole valmiuksia taistella. Automaatiolaitteiston kapasiteetti ei aina riitä pyörittämään virustorjuntaohjelmistoja, ja jo pelkästään reaaliaikaisuuden saavuttaminen saattaa olla laitteiston suorituskyvyn ylärajoilla. Yksi suorituskykyyn vaikuttava seikka on se, että automaatiolaitteiston elinkaaren voidaan arvioida olevan 15–20 vuotta, kun taas IT-laitteistolla se voi olla vain 3–5 vuotta. [35, s. 30] IT-laitteiston ohjelmistopäivitykset eivät sellaisenaan ole asennettavissa automaatiokäyttöön vaan kaikki päivitykset vaativat testauksia sekä suunnitelman asennusta varten [27, s. 4]. On tärkeää huomioda, että IT- ja automaatiojärjestelmien tiedoille asetetut prioriteetit eroavat toisistaan. IT-järjestelmälle tärkeää on tietojen luottamuksellisuus, kun taas automaatiojärjestelmälle on tärkeää, että tieto on saatavilla ja se on eheää [35, kpl 3]. Jos tiedolle asetetut vaatimukset eivät toteudu, voi seurata esimerkiksi tuotannon menetyksiä

tai poikkeamia laadussa, mikä merkitsee taloudellisia tappioita. Tämän lisäksi myös järjestelmien riskit eroavat toisistaan merkittävästi. IT-järjestelmässä riski kohdistuu itse järjestelmään ja sen sisältämiin tietoihin, mutta automaatiojärjestelmään tehty tietoturvahyökkäys voi uhata myös muun muassa ympäristöä tai ihmisen terveyttä ja turvallisuutta [35, kpl 3; 27, s. 4]. Tästä johtuen olisikin erityisen tärkeää huolehtia automaation tietoturvasta sen erityistarpeet huomioon ottaen. Lisätietoa automaatio- ja IT-järjestelmien eroavaisuuksista löytyy julkaisusta *Guide to Industrial Control Systems Security* [35, kpl 3], missä aihetta käsitellään erittäin kattavasti.

Lisääntynyt verkottuminen ja IT-tekniikoiden käyttö altistaa automaatiojärjestelmän samoille uhille, jotka ovat tuttuja koti- ja toimistoverkoista, mutta vastaavasti samojen tietoturvatoimien soveltaminen ei välttämättä ole mahdollista automaatioympäristössä. [6, s. 4; 27, s. 4] Esimerkiksi automaatioasemaan asennettu viruskuvauspäivitys, jota ei ole testattu, saattaa aiheuttaa yhtä suurta tuhoa kuin järjestelmään päässyt virus [35, kpl 3; 6].

Automaatiojärjestelmien kasvanut verkottuneisuus ja lisääntyneet yhteydet ulkoisiin palveluihin on huomioitu jo vuonna 2007 ilmestyneessä Suomen automaatioseuran julkaisussa *Automaatiosuunnittelun prosessimalli* [2]. Automaatiojärjestelmään liittyy lukuisia ulkoisia toimijoita, mikä tekee siitä monitoimijaympäristön. Tämä vaikeuttaa tietoturvan hallintaa entisestään, sillä automaatiojärjestelmän omistajan vastuulle jää huolehtia siitä, että myös ulkoisten toimijoiden toimintatavat täyttävät tietoturvalle asetetut vaatimukset.

Elinkaarimallin (kuva 2) hyödyntäminen automaatiojärjestelmähankinnoissa on hyvä työkalu luotettavuuden takaamiseksi [36]. Elinkaarimalli, jossa huomioitaisiin automaation tietoturva, ei ole vielä toistaiseksi vakiinnuttanut paikkaansa automaatiohankkeiden työkaluna, mutta potentiaalia siitä kyllä löytyisi. Elinkaarimallia hyödyntämällä pystytäisiin tehokkaasti sulauttamaan automaation tietoturva osaksi automaatiohankintoja.



Kuva 2. Automaatiosuunnittelun elinkaarimalli [muokattu lähteestä 36].

Sen lisäksi, että elinkaarimalli tarjoaa valmiit puitteet tietoturvalisille järjestelmähankinnoille, se myös huolehtii erilaisin testein ja kelpoistuksin siitä, että järjestelmän kokonaisturvallisuus ja laatuvaatimukset toteutuvat. Samalla kelpoistusraportit, tarkastuspöytäkirjat ynnä muu dokumentaatio tulee hoidetuksi asianmukaisesti.

2.2 Uhat, riskit ja liiketoimintavaikutukset

Kuten edellisestä kappaleesta käy ilmi, lisääntynyt verkottuneisuus ja IT-tuotteiden yleistyminen automaatiojärjestelmissä on tuonut mukanaan lisää tietoturvahkia. Näitä uhkia voidaan arvioida esimerkiksi niiden toteutumistodennäköisyyden mukaan. Haavoittuvuudet ovat puolestaan järjestelmälle ominaisia heikkouksia, jotka voivat kasvattaa uhkien todennäköisyyksiä tai pahentaa niiden seurauksia. Ihmisten toiminta, prosessit sekä teknologia pitävät kaikki sisällään uhkia ja näin ollen myös riskejä.

Automaatiojärjestelmässä on fyysisiä, loogisia sekä ihmisiin liittyviä suojattavia kohteita. Fyysisiä kohteita ovat esimerkiksi rakennukset, laitteet ja kaikki fyysiset esineet, jotka osallistuvat tuotantoprosessiin, muun muassa ohjausjärjestelmät. Loogisilla kohteilla tarkoitetaan tietoa, esimerkiksi automaatiologiikkaa ja prosessikohtaista tietämystä. Ihmiin liittyviä kohteita ovat puolestaan ihmiset ja heidän tuotantoprosessiin liittyvät taitonsa ja taitonsa, jotka voivat olla uhattuna esimerkiksi onnettomuuden aiheuttaman ruumiillisen vamman vuoksi. [38, s. 32]

Standardin IEC/TS 62443-1-1:fi [38, s. 32] mukaan automaatiojärjestelmä on jaettu pienempiin osajärjestelmiin, jotka koostuvat edellisessä kappaleessa mainituista suojattavista kohteista. Jokaisen suojattavan kohteen arvo tulisi määrittää laadullisesti tai määrällisesti, jotta riskianalyysia tehtäessä tiedetään mahdollisen menetyksen arvo. Menetystä arvioitaessa on huomioitava välittömän vahingon lisäksi myös välilliset seuraamukset. Toisin sanoen, jokaisen suojattavan kohteen kohdalla tulisi arvioida tietoturvan pettämisestä seuraavia liiketoimintavaikutuksia.

Tietoturvahilla tarkoitetaan mahdollisia järjestelmään kohdistuvia tekoja, jotka voivat olla tahallisia tai tahattomia. Usein tietoturvahat mielletään tahallisiksi hyökkäyksiksi, mutta todellisuudessa tavallisimpia uhkien aiheuttajia ovat puutteellisista tiedoista aiheutuvat vahingot tai kelpuuttamattomat muutokset, kuten esimerkiksi testaamaton ohjelmistopäivitys [38, s. 35]. Järjestelmän omistajan on huomioitava sekä tahalliset että tahattomat hyökkäykset hallinnoidessaan automaatiojärjestelmän tietoturvaa.

Standardin SFS-IEC 62443-2-1 [39] mukaan tietoturvahkia voivat aiheuttaa esimerkiksi:

- jännityksen etsijät
- tyytymättömät työntekijät
- vahinko (esim. oma-aloitteinen työntekijä tekee virheen)
- kiire, ei huomioida olemassa olevia politiikkoja
- varkaat
- terroristit
- vihollismaat tai -ryhmät.

Esimerkkejä tietoteknisistä uhista:

- järjestelmään tunkeutuminen
- haittaohjelmat
- kohdistetut hyökkäykset (engl. Advanced Persistent Threat, APT)
- puskuriylikuodot
- sähköposti
- palvelunestohyökkäykset
- haittaohjelmien torjunta (nämä saattavat hidastaa prosessia tai päivittämättöminä olla uhka)
- virustorjuntaohjelmien erot
- käyttöjärjestelmät.

Muun muassa yllä listatut uhan aiheuttajat ja tietotekniset uhat voivat aiheuttaa automaatiojärjestelmään tietoturvahäiriöitä. Standardin SFS-IEC 62443-2-1 [39, s. 40] mukaan automaatiojärjestelmän tietoturvahäiriöistä johtuvia seuraamuksia voivat olla esimerkiksi:

- tuotannon väheneminen tai menettäminen
- työntekijän tai ulkopuolisen henkilön vahingoittuminen tai kuolema
- laitevaurio
- ympäristövahinko
- viranomaismääräysten tai -vaatimusten rikkominen
- tuotteen turmeltuminen
- rikos- tai siviilioikeudellinen vastuu
- liiketalousuuden tai luottamuksellisen tiedon menettäminen
- maineen menetys tai asiakkaan luottamuksen menettäminen
- taloudellinen vahinko.

Jotta tietoturvahäiriöiltä vältyttäisiin, uhkia vastaan tulee suojautua erilaisin vastatoimenpitein. Esimerkkejä vastatoimenpiteistä ovat:

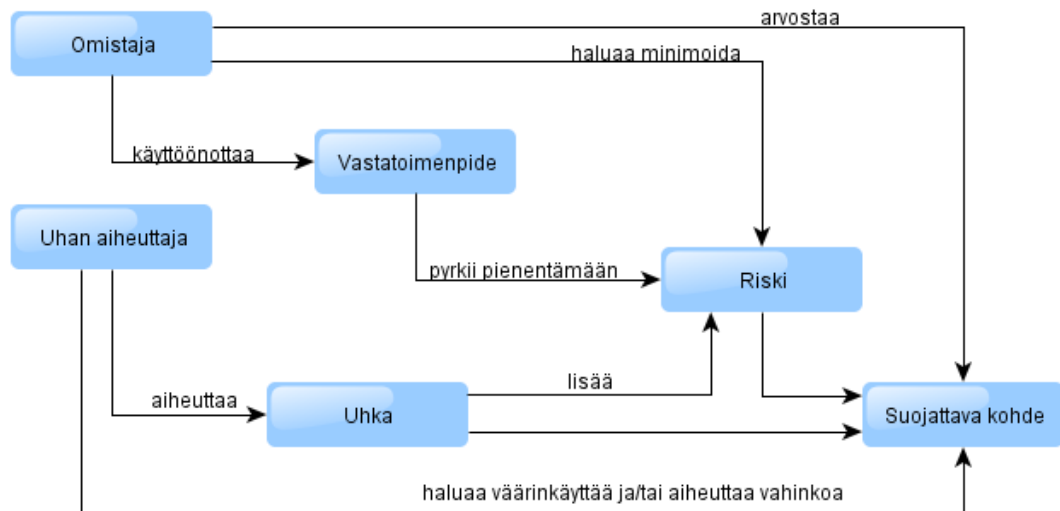
- fyysinen tietoturva
- pääsyn hallinta
- todentaminen
- salaus
- toimintojen tarkkailu.

Lisää vastatoimenpiteitä löytyy muun muassa standardista IEC/TS 622443-1-1:fi [38, s. 38]. Lisäksi standardissa IEC/TR 622443-3-1:fi [40] käsitellään suojautumisteknologioita hyvin yksityiskohtaisesti.

Uhkien ja niihin liittyvien seurausten sekä haavoittuvuuksien perusteella voidaan määrittää riski, eli menetyksen odotusarvo [38, s. 34]. Automaation tietoturvan hallinnan kannalta oleellista on hallita järjestelmän riskejä. Yksi tapa riskinhallintaan on määrittellä

suojattavien kohteiden riskinsietotasot. Riskinsietotasojen muutoksia tulee seurata ja niihin tulee reagoida tarvittavin vastatoimenpitein. Riskinsietotasoihin ja vastatoimenpiteisiin liittyvät päätökset ovat yritysjohton vastuulla.

Kuvassa 3 kootaan riskiin liittyvät elementit ja toimenpiteet eri elementtien välillä.



Kuva 3. Riskikaavio [muokattu lähteestä 38, s. 31].

Kuvan tarkoituksena on havainnollistaa, mitä motiiveja eri tekijöillä on suojattavaan kohteeseen liittyen ja miten ne vaikuttavat suojattavaan kohteeseen liittyvään riskiin. Jokaisen suojattavan kohteen kohdalla on syytä arvioida riskin suuruutta, mitkä tekijät riskiin vaikuttavat, ja miten riskiä pystytään hallitsemaan. Kuva ei huomioi suojattavan kohteen vaikutusta muihin suojattaviin kohteisiin, mikä olisi kokonaisuuden kannalta tärkeä huomioitava seikka. Jatkotoimenpiteenä uhkien, riskien ja vastatoimenpiteiden arvioinnille olisi oleellista pohtia, mitä vaikutuksia edellä mainituilla asioilla on organisaation liiketoiminnalle sekä jatkuvuudenhallinnalle.

Automaation tietoturvan hallinnassa tulee ottaa huomioon kaikki aiemmin tässä kappaleessa mainitut asiat. Standardin ISO/IEC 17799 [17] mukaan tietoturvan hallintajärjestelmä koostuu kuvan 4 mukaisista osa-alueista.



Kuva 4. Tietoturvan hallinta [Muokattu lähteistä 41, s. 30 ja 17].

Kuvasta nähdään, että suojattavia kohteita ei pystytä kokonaan suojaamaan, vaan osa jää aina, tarkoituksellisesti tai pakosta suojaamatta. Tärkeää olisi, että suojaamattomat kohteet valitaan tietoisesti riskianalyysin perusteella. Toinen huomionarvoinen seikka on se, että suurin osa suojaustoimenpiteistä on toimintatapoja ja vain osa teknisiä ratkaisuja.

Automaation tietoturvan hallinnassa voidaan hyödyntää vyöhykejajattelua yksittäiseen laitteeseen tai järjestelmään perustuvan ajattelun sijaan. Tällöin automaatiojärjestelmä jaetaan loogisiin vyöhykkeisiin, joille voidaan määrittää tavoitteellinen tietoturvaso. Tietoturvasot mahdollistavat suojattavien kohteiden tietoturvan kvalitatiivisen arvioinnin, jolloin suojattavien kohteiden tietoturvaa voidaan vertailla ja hallita. [38, s. 50] Kuitenkin automaation tietoturvan hallinnalla pyritään kokonaisvaltaiseen automaation turvallisuuteen, jolloin parempi lähestymistapa olisi tietoturvasojen sijasta määrittää tavoitteelliset turvallisuustasot, jotka koostuvat turvallisuudesta ja luotettavuudesta.

Automaatiojärjestelmän turvallisuudella tarkoitetaan sitä, että järjestelmä ei vahingoita ihmisiä, ympäristöä, laitteistoa tai tuotantoa. Luotettavuus kostuu toimintavarmuudesta ja saatavuudesta. Toimintavarmuus kuvaa sitä todennäköisyyttä, millä järjestelmä toimii ilman vikatilanteita, ja saatavuus kuvaa sitä osuutta ajasta, jonka järjestelmä on käytettä-

vissä tarkoitukseensa. Tietoturva onkin vain kokonaisturvallisuuden osatekijä ja sen vaikutusta automaatiojärjestelmän turvallisuuteen tulee arvioida osajärjestelmäkohtaisesti, mutta myös arvioiden ristivaikutuksia osajärjestelmien välillä sekä koko järjestelmäkokonaisuuden osalta.

Muokkaamalla tietoturvasolähestymistapaa siten, että arvioidaankin turvallisuustasoa, organisaation tulee määrittää tarvittavien turvallisuustasojen määrä. Suositeltavaa on, että niitä olisi vähintään kolme esimerkiksi taulukon 1 mukaisesti.

Taulukko 1. *Turvallisuustasot [muokattu lähteestä 38, s.50].*

Turvallisuustaso	Kvalitatiivinen kuvaus
1	alhainen
2	keskinkertainen
3	korkea

Turvallisuustasoja on kolmentyyppisiä:

- suojattavan kohteen tavoitteellinen turvallisuustaso
- suojattavan kohteen saavuttama turvallisuustaso
- suojattavan kohteen korkein mahdollinen saavutettavissa oleva turvallisuustaso.

Määritettyjen liiketoimintavaikutusten sekä riskinsietotason perusteella valitaan suojattavan kohteen tavoitteellinen turvallisuustaso. Suojattavan kohteen ominaisuudet määrittävät, mikä on korkein mahdollinen saavutettavissa oleva turvallisuustaso. Tämän on oltava suurempi tai vähintään yhtä suuri kuin tavoitteellinen turvallisuustaso, jotta kohteen saavuttama turvallisuustaso voi olla riittävän korkea.

Prosessiautomaation tietoturvan hallinnalla pyritään edistämään automaatiojärjestelmän turvallisuutta, jolloin tietoturvan hallintajärjestelmän tulee huomioida tietoturvan lisäksi liiketoiminnan jatkuvuus, sekä kriisitilanteisiin reagointikyky. Automaation tietoturvan hallintajärjestelmän suunnittelussa suositeltavaa olisi ottaa liiketoimintalähtöinen lähestymistapa, mikä huomioi tietoturvahyökkäyksistä aiheutuvat liiketoimintavaikutukset ja miten niitä pystyttäisiin minimoimaan.

2.3 Metsä Board Tako

Takolla valmistetaan korkealaatuista taivekartonkia kahdella kartonkikoneella. Valmis kartonki leikataan asiakkaiden tilausten mukaiseen muotoon kahdella pituusleikkurilla sekä viidellä arkkileikkurilla. Leikattu kartonki pakataan arkin- tai rullanpakkauslinjalla, jonka jälkeen se lastataan rekkaan, joka vie valmiin tuotteen varastoterminaaliin odottamaan toimitusta asiakkaalle. Kartongin valmistuksen lisäksi Takolla tuotetaan myös höyryä ja sähköä voimalaitoksen tiloissa.

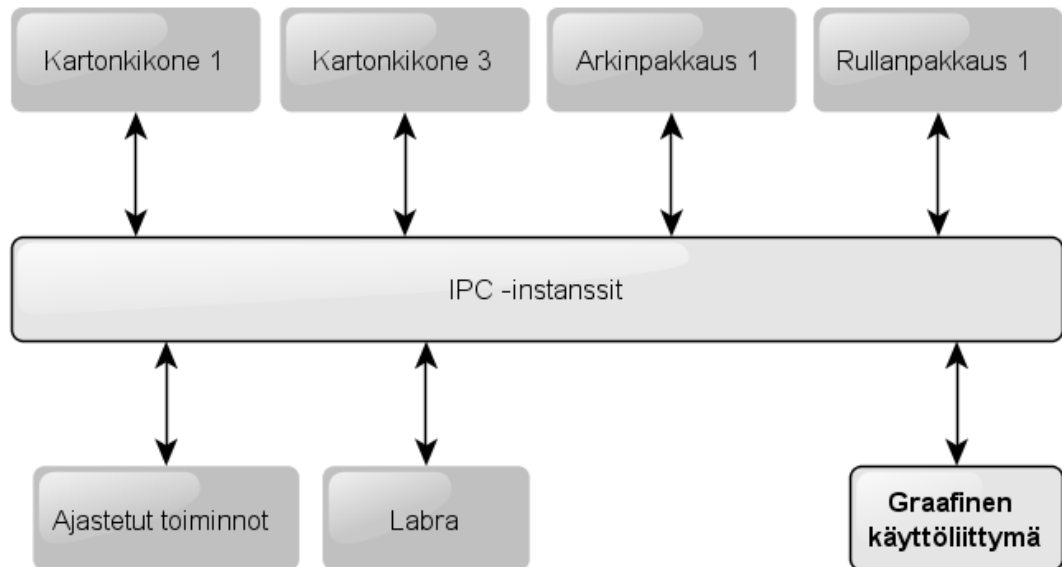
Massaosastolla pulpperoidaan ja laimennetaan kartongin raaka-aineena käytettävä kartonkimassa, ja pastakeittiöllä valmistetaan kartongin päällystykseen käytettävät päällystysaineet. Kaikki edellä mainitut sekä lukuisat pienemmät osajärjestelmät liittyvät toisiinsa automaatioverkon välityksellä.

Kartonkikoneiden vuosittainen tuotantokapasiteetti on noin 210 000 tonnia [21]. Maksimikapasiteetin saavuttamiseksi ei riitä, että pelkästään tuotantoon vaadittavat koneet ja laitteet ovat toimintakunnossa vaan kaikkien automaatiojärjestelmän osa-alueiden täytyy toimia moitteetta. Onkin erityisen tärkeää, että automaation tietoturvaan panostetaan, sillä tunkeutuminen mitättömältä tuntuvaan osajärjestelmään saattaa johtaa tehtaan tuotannon pysähtymiseen, tuotteen laadun alenemiseen tai muuhun liiketoiminnan kannalta negatiiviseen tapahtumaan.

Takon tehdasautomaatio on verkottunut siten, että lähes mistä tahansa järjestelmän osasta on yhteys mihin tahansa toiseen järjestelmän osaan. Sen lisäksi, että alimman tason kentälaitteet voivat olla yhteydessä toisiinsa, ne voivat olla yhteydessä myös ylemmän tason tuotannonohjaus-(engl. Manufacturing Execution System, MES) sekä toiminnanohjausjärjestelmien (engl. Enterprise Resource Planning, ERP) kanssa, kuten jo ensimmäisen kappaleen kuvasta 1 nähdään. Tuotannonohjausjärjestelmällä on suuri rooli tehtaan tuotannon jatkuvuudessa, sillä sen tulee taata tehtaan jatkuva käynti myös, jos jostain syystä toiminnanohjausjärjestelmä ei ole toiminnassa tai yhteys siihen katkeaa.

Tehtaan prosessinohjausjärjestelmä on ostettu ulkopuoliselta toimittajalta. Ulkopuolisia toimittajia on hyödynnetty laajalti myös muissakin tehtaan automaation osajärjestelmissä, kuten esimerkiksi mittapalkkien ja katkokameroiden sekä laboratorion laadunvalvonnassa. Takolla, kuten muissakin organisaatioissa, ulkopuoliset toimittajat tuovat omat haasteensa automaatiojärjestelmien tietoturvaan, sillä heidän järjestelmiensä ja toimintatapojensa tietoturvan taso tulee olla Takon vaatimusten mukainen ja lisäksi vaatimusten toteutumista pitää pystyä valvomaan. Koska prosessiautomaatio on monitoimijaympäristö, on erittäin tärkeää määrittää toimittajakohtaiset tietoturva-vaatimukset huolellisesti ja liittää ne jokaisen toimittajan ostosopimukseen.

Kuvasta 5 nähdään, miten tuotannonohjausjärjestelmän IPC-instanssit (engl. interprocess communication) ovat yhteydessä tehtaan automaatiojärjestelmän kanssa.



Kuva 5. MES –rajapinnat. [Muokattu lähteestä 37].

Kuva havainnollistaa, kuinka tuotannonohjausjärjestelmä kommunikoi molempien kartonkikoneiden kanssa, sekä lisäksi pakkauslinjojen kanssa. Tuotannon laatua seurataan kartonkikoneiden sekä laboratorion laadunvalvontalaitteiden avulla ja nämä laadunvalvontatiedot siirtyvät tuotannonohjausjärjestelmään, jolloin kartongin laatua pystytään tarkkailemaan, ja leikkaussuunnitelmiin voidaan vaikuttaa laatu tietojen perusteella. Valmiin kartongin laatu tiedot ovat jäljitettävissä pakkausetikettien perusteella. Tuotannonohjausjärjestelmän tietoja voidaan tarkastella ja muokata graafisen käyttöliittymän kautta. [20]

Yllä mainittujen järjestelmien lisäksi Takon tehtaassa automaatiojärjestelmään liittyy monia muitakin osajärjestelmiä, jotka eivät välttämättä ole suorassa yhteydessä tuotannonohjausjärjestelmään. Tiedonhallintaan ja dokumentointiin on olemassa oma tiedonhallintajärjestelmä, ja kunnossapidolla on käytössä erilaisia koneiden ja laitteiden kunnon seurantaan tarkoitettuja järjestelmiä. Leikkureiden ohjaus on toteutettu ohjelmoitavilla logiikoilla, ja kompressorien ohjauksiin on oma järjestelmänsä. Näiden lisäksi tehtaalla on käytössä muun muassa taloautomaatiota sekä kulunvalvontajärjestelmä.

Voimalaitosta tarvitaan tuottamaan sähköä ja höyryä kartonkikoneiden tarpeisiin. Voimalaitoksen tuottaman sähkön lisäksi sähköä otetaan myös verkosta. Kompressorien ohjausjärjestelmän ja kompressorien tuottaman paineilman täytyy olla käytettävissä, ja tiedonkulun kaikkien tehtaassa kenttälaitteiden ja ohjausjärjestelmien välillä täytyy toimia luotettavasti. Leikkureiden pitää pystyä leikkaamaan, ja pakkauslinjojen pakkaamaan samassa tahdissa ajatun tuotannon kanssa rajallisesta tampuurirautojen määrästä ja säilytystiloista johtuen.

Tehtaan laatujärjestelmien tulee olla toiminnassa, jotta kartongin laatua pystytään seuraamaan ja reagoimaan laatumuutoksiin. Kartongin tulee olla jäljitettävissä käytännössä valmiista rullasta aina kartonkimassan valmistukseen käytettyyn tukkierään saakka.

Kartonginvalmistusprosessi on monimutkainen ja monisäikeinen kokonaisuus, jonka jokainen säie vaikuttaa lopputulokseen. Takon tehdas on saanut sertifikaatteja, ja siten toiminta on tarkoin säänneltyä [21]. Esimerkiksi lopputuotteissa käytettävän puuraaka-aineen alkuperä pystytään jäljittämään, ja täten todentamaan, että metsien hoito täyttää niille annettujen sertifikaattien mukaiset vaatimukset. Tehtaalle myönnettyjä sertifikaatteja ovat:

- laatujärjestelmä: ISO 9001
- ympäristöjärjestelmä: ISO 14001
- elintarviketurvallisuusjärjestelmä : ISO 22000
- työturvallisuusjärjestelmä: OHSAS 18001
- energianhallintajärjestelmä: ISO 50001
- PEFC ja FSC -merkin käyttöoikeus.

Takon tehtaalla on maine huippulaadukkaan taivekartongin valmistajana. Toiminnan ja hyvän maineen varmistamiseksi tulee huolehtia yllämainittujen sertifikaattien vaatimusten täyttymisestä. Lisäksi tehtaan sisäisiin tavoitteisiin kuuluu esimerkiksi korkean tuotantoasteen saavuttaminen, sekä tapaturmien vähentäminen. Tavoitteet vuodelle 2018 ovat [16]:

- vuosituotanto: 215 000 tonnia
- laatu: valituskorvaukset alle 0,5 % liikevaihdosta
- työturvallisuus: 0 työtapaturmaa.

Edellä mainittujen tavoitteiden saavuttamiseksi on ehdottoman tärkeää huolehtia myös automaation tietoturvasta, sillä tietoturvahäiriöistä voi seurata pahimmassa tapauksessa uhka ihmisten tai ympäristön turvallisuudelle, laiterikkoja, yrityksen julkisuuskuvan heikkeneminen, tuotannon menetyksiä, laadun alenemaa tai muita liiketoimintaan negatiivisesti vaikuttavia asioita. Lähes poikkeuksetta tietoturvahäiriöt johtavat taloudellisiin tappioihin, esimerkiksi tuotannon menetyksestä johtuen. Myös harvinaisemmat seuraamukset, esimerkiksi työtapaturmat ja niistä koituvat vakavat seuraukset, tulee ottaa huomioon automaation tietoturvan hallinnassa. Automaatiojärjestelmän tietoturvan pettäminen voi siis aiheuttaa tuotannon menetyksien lisäksi lukuisia muita seuraamuksia. Tietoturvatapahtumat mielletään helposti ihmisten aiheuttamiksi, mutta kaikessa toiminnassa tulee huomioida myös esimerkiksi luonnonilmiöiden, kuten ukkosen aiheuttamat tietoturvauhat sekä esimerkiksi laiterikot.

Takon automaatiojärjestelmään liittyy lukuisien ulkoisten toimijoiden lisäksi talon oma IT-osasto sekä automaatio-osasto. Lisäksi myös osa IT-palveluista on ostettu ulkoisilta

toimijoilta. Tällä hetkellä Takon tehtaan automaation tietoturva ja laitehankinnat tehdään Metsä Groupin toimintaohjeen mukaisesti. Sen mukaan IT-puolen vastuulla on arvioida verkkoon liitettävien laitteiden tietoturvaa, yhteensopivuutta ja elinkaaren hallintaa ja arvion pohjalta suositella, miten tietoturva ja laite- ja lisenssihankinnat toteutetaan. Hyödyntäen IT-puolen suositusta, automaatiopuolen vastuuhenkilö neuvottelee automaatio-toimittajan kanssa sovellettavan menetelmän. [5]

Käyttöönoton yhteydessä automaatio-toimittaja, automaation vastuuhenkilö sekä IT-puolen vastuuhenkilö toteavat laitteiston, sovellusten ja tietoturvan toiminnan vaatimustenmukaisuuden. IT-puolen vastuulle jää päivittää asennetut laitteistot työasemalistoille. [5]

Tietoturvan ylläpito voidaan toteuttaa kahdella tapaa, riippuen siitä, onko kyseessä toimittajan huoltosopimukseen liittyvä järjestelmä vai IT-puolen vastuulla oleva järjestelmä. Mikäli järjestelmä liittyy toimittajan huoltosopimukseen, automaatio-toimittaja raportoi automaatiopuolen vastuuhenkilölle tietoturvasta ja siihen liittyvistä toimenpiteistä seurantalaverieissa tai muun raportointimenettelyn kautta. Automaatio vastaa tarvittavan tiedon kulusta IT-puolelle. [5]

Mikäli järjestelmä on Takon IT-puolen vastuulla, huolehtii IT-puoli järjestelmän viruskantojen päivityksistä. Korjaustiedostojen asennukset, varmistukset, versioiden korotukset yms. suunnitellaan yhteistyössä toimittajan ja automaatiopuolen kanssa. [5]

Prosessiautomaation tietoturvaprosessin ylläpidosta ohjeistetaan siten, että automaatiopuolen vastuuhenkilön tulee huolehtia tietoturvaprosessin toimivuudesta. IT-puolen vastuulla on prosessiautomaation LAN-verkkoon (engl. Local Area Network) liitettyjen laitteiden listojen ylläpito ja listan tilanteen arviointi ja raportointi. Listoja käsitellään asiainsaisten kesken seurantalaverieissa. [5]

Tietoturvaprosessin ylläpidosta vastaa prosessiautomaation kohdalla tehtaan automaatiopäällikkö. IT-puoli pitää yllä listaa kaikista LAN-verkkoon liitettyistä prosessiautomaation laitteista, ja listaa käydään läpi yhdessä automaatiopuolen yhdyshenkilön kanssa. IT-puoli raportoi luettelon tilanteesta automaatiopäällikölle kvartaaleittain tai tarpeen mukaan. Automaatioluettelot käydään läpi myös IT-puolen seurantalaverieissa. [5]

2.4 Esimerkkejä toteutuneista tietoturvahyökkäyksistä

Halutun turvallisuustason saavuttamiseksi laitteistoa ja ohjelmistoja täytyy suojata niihin kohdistuvilta tietoturvahyökkäyksiltä, joiden määrä on kasvanut räjähdysmäisesti TCP/IP –protokollaperheen käytön ja toimistolaitteiden yleistyttyä automaatiossa. Seuraavaksi käydään läpi joitain esimerkkejä toteutuneista, huomiota saaneista tietoturvahyökkäyksistä.

Yksi merkittävimpiä hyökkäyksiä on vuonna 2009 havaittu **Stuxnet**-mato, joka hyökkäsi Iranin ydinaseohjelmaa vastaan. Se pyrki häiritsemään uraanin rikastusprosessia ja rikkoamaan sentrifugeja yli vuoden ajan, ennen kuin se löydettiin. Se kerkesi myös levitä maailmanlaajuisesti, pääpainon ollessa Iranissa. Stuxnet hyödynsi Windows-pohjaisten koneiden haavoittuvuuksia ja onnistui leviämään niiden kautta koneisiin, joissa oli asennettuna Siemensin S7 PLC-ohjausjärjestelmä (engl. Programmable Logic Controller) ja onnistui sitä kautta pääsemään käsiksi Vaconin taajuusmuuttajien parametreihin ja muuntaamaan niitä siten, että taajuutta nostettiin ja laskettiin sentrifugien hajottamiseksi käyttäjien huomaamatta. [19, s. 24; 3]

Huomionarvoista Stuxnetissa on se, että automaatiojärjestelmä ei ollut liitettynä internetiin, ja siitä huolimatta mato pääsi leviämään suurelle alueelle [3, s. 3]. Muita merkittäviä tietoturvatapahtumia teollisuuden aloilla ovat olleet esimerkiksi:

Black Energy -kyberhyökkäys, joka aiheutti Ukrainan sähköverkon osittaisen alasajon vuonna 2015.

Havex-vakoiluohjelma, jonka kohteena olivat ICS-järjestelmät (engl. Industrial Control System) eri teollisuuden aloilla ja joka levisi arviolta 2000 toimipisteeseen vuonna 2013.

Petya, **NotPetya** ja **WannaCry** -kiristysohjelmat, joista ensiksi mainittu levisi laajasti haitaten muun muassa tanskalaista Moller-Maersk -varustamon liiketoimintaa aiheuttaen satojen miljoonien dollarien vahingot vuonna 2017.

Mainittakoon, että tietoturvahyökkäykset voivat olla joko kohdistettuja tai kohdistamattomia. Toisin sanoen on hyvin todennäköistä joutua hyökkäyksen kohteeksi, jos ei suorana kohteena, niin kohdistamattoman hyökkäyksen kohteena yhtenä muiden joukossa.

2.5 Perusteluja diplomityön tarpeellisuudesta

Edellä kuvatut esimerkit osoittavat, että nykypäivänä yksikään yritys ei saisi laiminlyödä automaatiojärjestelmiensä tietoturvaa. Tietoturvahyökkäysten lisäksi turvallisuutta voivat uhata lukuisat muut aiemmin kappaleessa 2.2 esitellyt uhkatekijät. Tietoturvahäiriöillä voi olla vakavia seuraamuksia Takon tehtaalle. Näistä esimerkkeinä mainittakoon:

- tuotannon väheneminen tai menettäminen
 - kustannukset, jos tuotanto pysähtynyt
 - maineen menetys, jos toimitukset myöhästyvät
- työntekijän tai ulkopuolisen henkilön vahingoittuminen tai kuolema
 - korvausvastuu
 - vakuutusmaksut
- laitevauriot
 - tuotantohäiriöt
 - laatu poikkeamat
 - korjauskustannukset
- ympäristövahinko
 - korvausvelvoitteet
 - mahdolliset lupien menetykset
 - maineen tahrautuminen
- viranomaismääräysten tai –vaatimusten rikkominen
 - rangaistustoimenpiteet
 - mahdollisten lupien menetys
- tuotteen turmeltuminen
 - korvaukset asiakkaalle
 - maineen menetys
- rikos- tai siviilioikeudellinen vastuu
 - rangaistustoimenpiteet
 - maineen menetys
- liikesalaisuuden rikkominen tai luottamuksellisen tiedon paljastuminen
 - taloudelliset menetykset
 - maineen menetys
 - tietosuojarikkomukset
- maineen menetys tai asiakkaan luottamuksen menettäminen
 - asiakkaiden menetys
 - tilauskannan pieneneminen
- taloudellinen vahinko
 - välillinen tai välitön seuraamus lähes kaikista tietoturvatapahtumista.

Lista on pitkä, ja siitä voidaan päätellä, että laiminlyöty tietoturva saattaa vaikuttaa monella tapaa negatiivisesti yrityksen liiketoimintaan. On syytä paneutua automaation tietoturva-asioihin yrityksen sisällä, koska tietoturvaa ei voida ulkoistaa. Näin siksi, että ulkopuolisen on lähes mahdotonta päästä perille koko automaatiojärjestelmän kokonaisuudesta, hallita sen tietoturvaa reaaliaikaisesti ja kantaa vastuu liiketoiminnan jatkuvuudesta. Joka tapauksessa viime kädessä vastuu tietoturvamenettelyjen käyttöönotosta, valvonnasta ja kehityksestä on yritysjohdolla. [1, s. 69]

3. KIRJALLISUUSTUTKIMUS

Automaation tietoturvasta sekä kyberturvallisuudesta löytyy paljon ohjeistusta, erityisesti yhteiskunnan huoltovarmuuskriittisille kohteille. Takon kartonkitehtaan toimintaa ei luokitella yhteiskunnan kannalta kriittiseksi, joten voidaan perustellusti todeta, että aiheeseen paneutuminen ei vaadi yhtä laajaa ja yksityiskohtaista selvitystä kuin huoltovarmuuskriittisissä kohteissa. Automaation tietoturvaa ja kyberturvallisuutta koskevia ohjeita, standardeja ja suosituksia laaditaan kansallisella ja kansainvälisellä tasolla muun muassa valtioiden, erilaisten yritysten ja järjestöjen toimesta.

Tavoitteena oli löytää kirjallisuudesta sopivia malleja prosessiautomaation tietoturvan hallintajärjestelmän luomiseen ja sovittaa ne konsernin olemassa oleviin menettelytapoihin. Kirjallisuustutkimukseen valikoitui kolme alalla keskeisen aseman saavuttanutta teosta:

- SFS-IEC 62443-2-1 Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten, Suomen standardoimisliitto, 2013 [39]
- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2017 [4]
- Security for Industrial Control Systems, Framework Overview ja oheisjulkaisut, Centre for the Protection of National Infrastructure, 2015 [24–33].

Ensin mainittu sisältää toimintatapaohjeen sekä tarvittavat elementit tietoturvallisuuden hallintajärjestelmän luomiseen. Kahdessa muussa esitellään kehysmallit, joilla automaation tietoturvaa voidaan parantaa ja hallita. Teokset on julkaistu Suomessa, Yhdysvalloissa ja Isossa-Britanniassa, ja jokaisen teoksen takana on arvostettu kansallinen järjestö. Kussakin teoksessa on hiukan erilainen lähestymistapa, mikä tuo monipuolisuutta tähän tutkimukseen. SFS-standardin valintaa puolsi se, että siinä esitellään kattavasti aihetta suomen kielellä. NIST:n kyberturvallisuuden menettelytapamalli on tuore julkaisu, joka pääsi tutkimukseen mukaan erityisesti selkeän ja hyvin jäsennellyn rakenteensa ansiosta. Teos on myös hyvin kattava, koska se käsittelee kriittisen infrastruktuurin kyberturvallisuutta, ja siinä olevat mallit ovat erittäin yksityiskohtaisia. CPNI:n teollisia ohjausjärjestelmiä koskeva julkaisusarja päätyi tutkimukseen selkeän rakenteensa ja tarjolla olleen sisältöön perehdyttävän oheismateriaalinsa ansiosta.

3.1 Standardi SFS-IEC 62443-2-1

Suomen standardoimisliitto SFS ry on standardoinnin keskusliitto Suomessa, ja SESKO on sähköteknisen alan standardointijärjestö. SFS-IEC 62443-2-1 on osa SFS-käsikirja 631-3 kokonaisuutta, jossa perehdytään automaation tietoturvallisuuteen. SFS 631-3 on SFS:n ja SESKO:n yhteistyönä vuonna 2013 laatima teos, joka perustuu kansainvälisen

sähköalan standardointiorganisaation IEC:n (engl. International Electrotechnical Commission) maailmanlaajuisiin standardeihin. Tässä kirjallisuustutkimuksessa paneudutaan käsikirjan toiseen osaan: SFS-IEC 62443 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvaluus. Osa 2-1: Tietoturvaluusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten.

SFS-IEC 62443-2-1 tarjoaa raamit teollisuusautomaatio- ja ohjausjärjestelmän tietoturvaluuden hallintajärjestelmälle. Standardia ei ole tarkoitettu sitovaksi ohjeeksi, vaan se muodostaa pohjan laadittavalle järjestelmälle ja antaa ohjeistusta siihen, mitä elementtejä järjestelmän tulisi karkeasti sisältää. Jokaisen organisaation tulee tarkastella mallissa annettuja ohjeita oman järjestelmänsä ja sen asettamien vaatimusten näkökulmasta. SFS-käsikirjan mukaan tietoturvaluuden hallintajärjestelmä koostuu kuvan 6 elementeistä:



Kuva 6. Tietoturvallisuuden hallintajärjestelmä [muokattu lähteestä 39, s. 37].

Tietoturvallisuuden hallintajärjestelmän tarkoituksena on suojata teollisuusautomaatio- ja ohjausjärjestelmää tietoturvallisuutta vastaan kohdistetuilta hyökkäyksiltä. Tietoturvallisuuden hallintajärjestelmä koostuu kolmesta pääluokasta, jotka jakautuvat elementtiryhmiin ja edelleen yksittäisiin elementteihin. Pääluokat ovat:

- riskianalyysi
- riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla
- tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen.

Pääluokat ja sitä kautta yksittäiset elementit ovat sidoksissa toisiinsa kuvan 6 nuolien mukaisesti.

3.1.1 Riskianalyysi

Riskianalyysi-luokkaan kuuluvat seuraavat elementit:

- liiketoimintaperustelu
- riskien tunnistaminen, luokittelu ja arviointi.

Liiketoimintaperustelun tarkoituksena on todentaa organisaation teollisuusautomaatio- ja ohjausjärjestelmän asettamat vaatimukset tietoturvallisuusriskien hallinnassa. Vaatimuksia voidaan perustella tietoturvallisuuden häiriintymisestä seuraavilla taloudellisilla menetyksillä, turvallisuus- tai ympäristöseurauksilla tai esimerkiksi maineenmenetyksellä. Tämä elementti osoittaa teollisuusautomaatio- ja ohjausjärjestelmien tietotekniikan erityistarpeet tietoturvallisuuden suhteen, sekä ilmentää tietoturvan tärkeyttä.

Liiketoimintaperustelu on oleellinen osa tietoturvallisuuden hallintajärjestelmän perustamista, sillä sen avulla pyritään saamaan johdon tuki prosessille ja sitä kautta vaadittavia investointeja ja resursointeja. [39, s. 16] Liiketoimintaperustelusta voi lukea tarkemmin standardista SFS-IEC 62443-2-1 [39, s. 38–42].

Riskien tunnistaminen, luokittelu ja arviointi – Kartoitetaan organisaation automaatiojärjestelmää uhkaavia tietoturvallisuusriskejä, arvioidaan niiden todennäköisyyksiä sekä vakavuutta. Oleellista on luokitella ja analysoida tietoturva-uhkia, haavoittuvuuksia ja seuraamuksia hyväksytyjä menetelmiä käyttäen. [39, s. 16–17]

Ensimmäisenä sovitaan, millä tavalla riskejä ryhdytään arvioimaan ja analysoimaan, jotta kaikki riskit tulevat käsiteltyä samoin perustein ja ne pystytään luotettavasti asettamaan keskinäiseen tärkeysjärjestykseen. Organisaation tulisi luokitella automaatiojärjestelmänsä loogisiin osajärjestelmiin, jotta automaatiojärjestelmästä saataisiin helpommin hallittava kokonaisuus. Lisäksi olisi luotava yksinkertaistetut verkkokaaviot, ja sovittua menetelmää hyödyntäen arvioitava laitteiston ja verkkojen tietoturvariskien luonnetta ja tärkeysluokkaa. Myös haavoittuvuudet tulisi asettaa tärkeysjärjestykseen ja huomioida riskiarvioita tehtäessä. [39, s. 16–17]

Tarkoituksena olisi saada tietoturvallisuuden riskinarvioinnista luotua dynaaminen prosessi, johon on integroitu fyysiset riskit, terveys-, turvallisuus- sekä ympäristöriskit. Riskien arviointia tulisi suorittaa järjestelmän elinkaaren kaikissa vaiheissa, ja iteroida tarvittaessa. Riskianalyysistä tulisi kerätä riittävä dokumentaatio, jotta sitä pystytään suorittamaan yhdenmukaisesti ja seuraamaan järjestelmän tilaa. [39, s. 16–17]

3.1.2 Riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla

Toinen pääluokka, riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla, jakaantuu kolmeen elementtiryhmään:

- tietoturvapoliittika, -organisaatio ja -tietoisuus
- valikoidut tietoturvavastatoimenpiteet
- toteuttaminen.

Tietoturvapoliittika, -organisaatio ja -tietoisuus

Tämän elementtiryhmän tehtävänä on kuvata tietoturvapoliittikkojen kehitysprosessia, tietoturvaorganisaation rakentamista sekä tietoturva-asioiden tuomista organisaation kaikkien sidosryhmien tietoisuuteen. Ryhmä koostuu seuraavista elementeistä:

- tietoturvallisuuden hallintajärjestelmän sovellusala
- organisaation perustaminen tietoturvaa varten
- henkilöstön koulutus ja tietoturvatietoisuus
- liiketoiminnan jatkuvuussuunnitelma
- tietoturvapoliittikat ja -menetelmät.

Tietoturvallisuuden hallintajärjestelmän sovellusala – Kartoitetaan kaikki teollisuusautomaatio- ja ohjausjärjestelmään liittyvät osapuolet, kuten esimerkiksi liiketoimintakumppanit, asiakkaat ja toimittajat. Lisäksi kartoitetaan kaikki tietoturvallisuuden hallintajärjestelmään liittyvät järjestelmät, prosessit ja muut organisaatiot ja dokumentoidaan ja arvioidaan ne. Sovellusalan kartoitus antaa selkeät rajat tietoturvallisuuden hallintajärjestelmän kattavuudesta ja selventää hallintajärjestelmän tavoitteita. [39, s. 18–19]

Organisaation perustaminen tietoturvaa varten – Jotta tietoturvasta vastaava organisaatio saadaan perustettua, tarvitaan ylemmän johdon tuki tietoturvallisuusohjelmalle. Toimiva automaation tietoturvaorganisaatio vaatii monitieteellistä osaamista, ja näin ollen vanhat vastuunjaot eivät välttämättä enää toimi. Eri osaamisalueilta vaaditaan yhteistyötä ja vastuut täytyykin määrittää siten, että kaikki osa-alueet toimivat yhteen, eikä järjestelmän osia jää huomioimatta. Jotta resurssit saadaan ohjattua oikeisiin paikkoihin, täytyy mennä organisaation hierarkiassa niin ylös, että valtuuksia riittää määrätä työtehtäviä ja vastuita laaja-alaisesti jokaiselle automaatiojärjestelmän sidosryhmälle. [39, s. 19]

Henkilöstön koulutus ja tietoturvatietoisuus – Tulee huolehtia siitä, että henkilöstölle annetaan riittävät tiedot työnsä suorittamiseksi tietoturvallisesti ja mahdolliset uhat ja haavoittuvuudet huomioiden. Kouluttamalla ja lisäämällä tietoisuutta varmistetaan se, että teollisuusautomaatio- ja ohjausjärjestelmien tietoturvallisuudesta huolehtiminen on rutiininomainen osa työtä. Olisikin tärkeä ymmärtää, että automaation tietoturvalle tulisi

antaa suuri painoarvo kuin turvallisuudelle ja toiminnalliselle eheydelle, sillä automaation tietoturvan pettäminen saattaa johtaa yhtä vakaviin, ihmisiä, laitteita tai ympäristöä uhkaaviin seuraamuksiin. [39, s. 19–20]

Liiketoiminnan jatkuvuussuunnitelma – Määritellään, miten yrityksen keskeiset liiketoiminnot pystytään ylläpitämään ja/tai uudelleenkäynnistämään häiriötilanteesta toivuttaessa. Kun jatkuvuussuunnitelma on tehty yksityiskohtaisesti ottaen huomioon kaikki järjestelmät ja osajärjestelmät sekä niiden liiketoimintatarpeet, varmistutaan siitä, että toimuminen tietoturvaluuhäiriöistä tapahtuu nopeimmalla mahdollisella tavalla. Jatkuvuussuunnitelmaan kirjataan mahdolliset keskeytykset ja niitä koskevat toipumismenettelyt sekä vaikutukset muihin järjestelmiin, jos jokin järjestelmän osa menetetään. Oleellista on myös luoda jatkuvuussuunnitelmalle testaussuunnitelma sekä tarkastuskäytännöt päivitysten suhteen. [39, s. 20–21]

Tietoturvapoliittikat ja -menettelyt – Tarkoituksena on muun muassa tuoda ilmi, miten organisaatiossa määritellään tietoturva sekä riskinsietokyky, miten tietoturvasuohjelmaa hyödynnetään ja kuinka sen päivittämisestä huolehditaan. Ylemmän tason politiikkojen ja riskinhallinnan työkalujen hyödyntäminen automaation tietoturvapoliittikkoja suunniteltaessa olisi suotavaa, sillä siten ne noudattavat organisaatiossa vallitsevaa linjaa. Tietoturvamenettelyt johdetaan tietoturvapoliittikoista ja niiden avulla todennetaan, miten politiikat pannaan käytäntöön. [39, s. 21–22]

Valikoidut tietoturvavastatoimenpiteet

Tässä elementtiryhmissä käsitellään tietoturvasuuden hallintajärjestelmälle ominaisia tietoturvamekanismien päätyyppejä ja se koostuu kuudesta elementistä:

- henkilöstöön liittyvä tietoturva
- fyysinen ja ympäristöön liittyvä turvallisuus
- verkon segmentointi
- pääsyn hallinta – käyttäjätilien hallinnointi
- pääsyn hallinta – todennus
- pääsyn hallinta – valtuutus.

Tämän elementtiryhmän kuvaus ei ole täydellinen listaus valituista tietoturvavastatoimenpiteistä, sillä vastatoimenpiteet riippuvat vahvasti riskiarvioista sekä riskien hallintaprosessista. Kuitenkin on tärkeää huomioida seuraavat vastatoimenpiteet jo tietoturvasuuden hallintajärjestelmää rakennettaessa, sillä niillä on iso vaikutus politiikkoihin sekä arkkitehtuuriin. [39, s. 22–23]

Henkilöstöön liittyvä tietoturva – Huolehditaan siitä, että organisaation sisäiset tietoturvavastatut tuodaan julki henkilöstölle, ja siitä, että henkilöstö on soveltuvaa kantamaan

vastuun omasta toiminnastaan, eikä uhkia sitä kautta synny. Luodaan henkilöstöä koskevat tietoturvapoliittikat, joista organisaation käytännöt käyvät ilmi ja sitoutetaan henkilöstö noudattamaan niitä. [39, s. 23–24]

Fyysinen ja ympäristöön liittyvä turvallisuus – Tavoitellun tietoturvatason perusteella luodaan suojaus valtuuttamattomalta pääsylvä, vahingolta, väärinkäytöltä ym. sekä ympäristöolosuhteita vastaan. Suojaus estää valtuuttamattoman fyysisen pääsyn käsiksi automaatiojärjestelmään ja sen laitteisiin. Lisäksi organisaation hallussa olevat yhteydet on suojattava. Suojauksen pitävyyttä on valvottava esim. auditoinneilla tai automaattisin hälytyksin, ja varauduttava tilanteisiin, joissa fyysinen turvallisuus on uhattuna. [39, s. 24–25]

Verkon segmentointi – Automaatiojärjestelmä jaotellaan siten, että saman tietoturvatason laitteet jaetaan omiin vyöhykkeisiinsä. Joka vyöhykkeeseen sovelletaan ennalta määriteltyjä tietoturvakäytäntöjä, joiden avulla huolehditaan siitä, että haluttu tietoturvan taso saavutetaan. Erityisesti tulisi huolehtia siitä, että tarpeeton tietoliikenne automaatiojärjestelmän laitetasolle suodatetaan tai estetään kokonaan. Verkon segmentoinnilla pyritään eristämään järjestelmän osia toisistaan, jolloin yhden osajärjestelmän tietoturvatapahtumat eivät pääse vaikuttamaan muihin osajärjestelmiin ja häiritsemään muiden osajärjestelmien toimintaa. Kuten muutkin vastatoimet, segmentointi suoritetaan riskinarvioon pohjautuen, eikä segmentointi aina ole välttämätön toimenpide pienen riskitason järjestelmissä. [39, s. 25–26]

Pääsyn hallinta – käyttäjätilien hallinnointi – Huolehditaan siitä, että vain asiaankuuluvilla henkilöillä on käyttäjätilit pääsyoikeuksilla järjestelmän eri osiin, laitteisiin, verkkoon jne. Käyttäjätilit tulee dokumentoida asianmukaisesti ja niiden myöntämisestä, muuttamisesta ja päättämistä tulee laatia selkeät säännöt, joiden noudattamista katselmoidaan säännöllisesti. [39, s. 26–27]

Pääsyn hallinta – todennus – Todennuksella pyritään tunnistamaan luotettavasti käyttäjätilin haltija. Eri profiileilta voidaan velvoittaa eri vahvuiset todennusmenetelmät sen mukaan, kuinka suuret vaikutukset mahdollisella luvattomalla pääsylvä olisi. Käyttäjätilin lukitsemista todennuksen epäonnistuessa riittävän monta kertaa tulee myös harkita tarkoin, sillä estynyt pääsy järjestelmään saattaa olla yhtä suuri uhka kuin luvaton pääsy. Automaatiojärjestelmäympäristössä voidaan yhdistää fyysisen todennuksen menetelmiä yhdessä elektronisten todennuskäytäntöjen kanssa ja siten parantaa todennuksen luotettavuutta. Kriittisiin järjestelmän osiin kohdistuneista pääsy-yrityksistä tulisi pitää lokia ja seurata kirjautumistietoja mahdollisten luvattomien pääsy-yritysten havaitsemiseksi. Eri-tyistä tarkkuutta tulisi noudattaa etäyhteyksien suhteen, ja etäyhteyksien hallinnan sääntöjen tulisi olla selkeät ja niiden noudattamista olisi seurattava. [39, s. 27–28]

Pääsyn hallinta – valtuutus – Henkilöstölle jaetaan valtuutuksia heidän työrooliensa mukaan siten, että kenelläkään ei ole ylimääräisiä valtuutuksia, mutta että myös jokaisella

on riittävät valtuudet työnsä suorittamiseen. Valtuutuksien jakamiseen tulee laatia koko henkilöstön kattava selkeä ohjeistus. Todennuksen jälkeen sovellus myöntää käyttäjälle valtuutuksen tehdä tiettyjä työtehtäviä. [39, s. 28–29]

Toteuttaminen

Viimeinen automaation tietoturvallisuuden hallintajärjestelmän riskin käsittely -osion elementtiryhmä on toteuttaminen, ja siinä käsitellään tietoturvallisuuden hallintajärjestelmän toteutukseen liittyviä asioita. Se koostuu seuraavista elementeistä:

- riskien hallinta ja riskinhallinnan toteuttaminen
- järjestelmän kehittäminen ja ylläpito
- tietojen ja dokumenttien hallinta
- häiriötilanteisiin varautuminen ja niihin reagoimisen suunnittelu.

Riskien hallinta ja sen toteuttaminen – Käsitellään havaittuja riskejä valitsemalla, kehittämällä ja toteuttamalla vaatimustenmukaiset vastatoimet. Eli pienennetään riski organisaation riskinsietokyvyn mukaiselle tasolle läpi koko organisaation. [39, s. 30]

Järjestelmän kehittäminen ja ylläpito – Huolehditaan siitä, että järjestelmä täyttää halutun tietoturvaprofiilin tunnusmerkit automaatiojärjestelmän kehittyessä tai muuttuessa. Lisäksi tarvittaessa tehdään uudet riskiarviot ennalta määrättyjen kriteerien mukaisesti. Tähän elementtiin kuuluvat muun muassa vastatoimenpiteiden sekä tietoturvapoliittikkojen ja –menettelyiden päivitykset ja ylläpito. Monesti tietoturvallisuuden hallintajärjestelmän ylläpito koetaan haasteellisemmaksi kuin sen perustaminen, joten onkin ensiarvoisen tärkeää sopia järjestelmän ylläpitomenettelyistä jo perustamisvaiheessa. Otetaan käyttöön muutostenhallintajärjestelmä sekä luodaan säännöt paikkaustenhallinnalle, vi-rustorjunnalle sekä varmuuskopioille. [39, s. 30–31]

Tietojen ja dokumenttien hallinta – Tulee kehittää dokumenttien hallintaprosessi, joka kattaa järjestelmän koko elinkaaren. Oleellista olisi, että dokumentit löytyvät ja että ne olisivat ajantasaisia. Dokumenttien säilytystä, luokittelua ja päivityksiä varten täytyy laatia selkeät säännöt, joiden avulla dokumenttien hallintaprosessi etenee jouhevasti. Järjestetään myös katselmoiteja sääntöjen noudattamisesta. [39, s. 31–32]

Häiriötilanteisiin varautuminen ja niihin reagoimisen suunnittelu – Mitä toimenpiteitä organisaatiossa on tehty häiriötilanteiden havaitsemiseksi ja kuinka havaittuihin häiriöihin reagoidaan. Häiriötilanteisiin reagoimissuunnitelman tulisi koskea kaikkia automaatiojärjestelmän osia ja siitä tulisi ilmetä organisaation menetelmät häiriötilanteisiin reagoimiseen, sisältäen tiedotus- ja dokumentointijärjestelyt, tutkimukset, toipumissuunnitelmat sekä häiriötilanteita seuraavat jatkomenettelyt. [39, s. 32–33]

3.1.3 Automaation tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen

Kolmas pääluokka koskee tietoturvallisuuden hallintajärjestelmän seuranta ja parantamista. Se koostuu kahdesta elementistä:

- noudattamisen valvonta
- tietoturvallisuuden hallintajärjestelmän katselmoinnit, parantaminen ja ylläpitäminen.

Noudattamisen valvonta – Varmistutaan siitä, että järjestelmä todella on käytössä suunnitellussa laajuudessaan. Seurataan, että määritellyistä politiikoista pidetään kiinni, ajantasaiset dokumentoinnit ja raportit huolehditaan aikatauluissa ja sovittuja menettelyjä noudatetaan. Asian suhteen voidaan sopia esimerkiksi auditoinneista, joissa mahdolliset puutteet noudattamisessa tulisivat ilmi. [39, s. 34]

Tietoturvallisuuden hallintajärjestelmän katselmointi, parantaminen ja ylläpitäminen – Varmistutaan siitä, että tietoturvallisuuden hallintajärjestelmä täyttää tavoitteensa järjestelmään kohdistuneista muutoksista huolimatta. Tietoturvallisuuden hallintajärjestelmälle tulisi suorittaa katselmoiteja säännöllisin väliajoin, jotta voidaan varmistua sen tehokkaasta toiminnasta. [39, s. 34–35]

3.1.4 Standardin SFS 62443-2-1 yhteenveto

Standardissa SFS 62443-2-1 [39] esitellyn automaation tietoturvallisuuden hallintajärjestelmä -mallin tarkoitus on ohjeistaa ja antaa viitekehys hallintajärjestelmän käyttöönotolle. Teoksessa painotetaan sitä, että malli ei sellaisenaan pysty täyttämään organisaation tarpeita, vaan että jokaisen organisaation on räätälöitävä omia tarpeitaan vastaava hallintajärjestelmä. Hallintajärjestelmä luodaan täyttämään organisaatiokohtaiset erityisvaatimukset. Hallintajärjestelmän muodostuminen riippuu pitkälti organisaation prosessiautomaation tietoturvatointojen nykytilasta, minkä perusteella pystytään määrittämään parannustarpeet. [39, s. 15]

Isossa konsernissa hallintajärjestelmää voidaan hyödyntää eri toimipisteissä, kunhan se määritellään tarpeeksi muodollisesti ja siten, että sitä on helppo soveltaa eri toimipisteiden vaatimusten mukaiseksi [39, s. 16]. Metsä Groupilla on runsaasti konsernitason politiikkoja ja toimintamalleja, erityisesti tietoturvaan liittyen, ja niitä voidaan hyödyntää automaation tietoturvallisuuden hallintajärjestelmässä, ja jatkumona automaation tietoturvallisuuden hallintajärjestelmää voitaisiin soveltaa eri toimipisteissä, sillä, oli hallintajärjestelmä tai ei, samat politiikat ja toimintaohjeet koskettavat eri toimipisteitä. Hallintajärjestelmän toimintojen avulla vain hallinnoitaisiin politiikkojen ja toimintamallien toteu-

tumista, ja siten varmistuttaisiin automaation tietoturva vaatimusten täyttymisestä. Konsernitason politiikkojen ja toimintamallien lisäksi tulisi myös paikallisesti luoda tarvittavat politiikat ja toimintamallit.

Standardin [39] hallintajärjestelmämallissa pohjana on riskilähtöinen ajattelu, jossa painotetaan riskianalyysia sekä riskin käsittelyä. Tämä on hyvä lähestymistapa automaation tietoturvallisuuden hallintaan, sillä riskianalyysin kautta voidaan tunnistaa ja priorisoida riskit, ja käsitellä riskejä hallintajärjestelmässä määritellyin toimenpitein tärkeysjärjestyksessä. Riskianalyysivaiheessa liiketoimintaperustelussa määritetään myös liiketoimintavaikutuksia, mikä on erittäin tärkeää, jotta pystytään näyttämään riskien mahdolliset vaikutukset liiketoiminnalle ja sitä kautta saamaan resurssit vastatoimenpiteiden toteuttamiseen. Liiketoimintaperustelu onkin äärimmäisen tärkeä työkalu, jotta saadaan yritysjohdon tuki automaation tietoturvallisuuden hallintajärjestelmälle ja myöhemmin riskien pienentämiseen hallintajärjestelmän riskinkäsittelyvaiheessa määritetyin vastatoimenpitein.

Riskilähtöisen ajattelun lisäksi Standardin SFS 62443-2-1 [39] automaation tietoturvallisuuden hallintajärjestelmässä oltaisiin voitu painottaa enemmän liiketoiminnan jatkuvuudenhallintaa, koska jos liiketoiminta loppuu, loppuu riskinhallintatarve. Nyt hallintajärjestelmä käsittelee liiketoimintavaikutuksia liiketoimintaperustelu-elementissä, ja jatkuvuussuunnitelma-elementissä tunnistetaan menetelmiä kriittisten toimintojen ylläpitämiseksi. Lisäksi häiriötilanteisiin varautumista käsitellään yhdessä elementissä. Varsinaista jatkuvuudenhallinta-osiota hallintajärjestelmässä ei siis ole vaan siinä käsitellään vain joitain jatkuvuuden hallinnan osa-alueita erillisinä palasina.

Järjestelmä siis koostuu riskianalyysi sekä riskin käsittely -osuuksista sekä kolmannesta automaation tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen -osiosta. Kolmannen osa-alueen huomiointi on erittäin oleellista järjestelmän toimivuuden kannalta, sillä sen avulla pystytään seuraamaan järjestelmän toimintaa, ja saavutetaanko järjestelmän avulla haluttuja tuloksia ja tarpeen vaatiessa kehittämään toimintaa. Myös järjestelmään liittyvien politiikkojen ja toimintamallien noudattamista seurataan ja noudattamatta jättämiseen reagoidaan. Standardissa [39] mainitaan, että automaation tietoturvallisuuden hallintajärjestelmän ylläpito on usein vaikeampaa kuin itse järjestelmän perustaminen ja käyttöönotto [39, s. 30]. Tästäkin syystä seuranta on erityisen tärkeää, koska siten pystytään varmistumaan, että järjestelmän ylläpidosta on huolehdittu.

Eräs silmiinpistävä huomio standardin [39] automaation tietoturvallisuuden hallintajärjestelmässä on se, että järjestelmä ei huomioi tarpeeksi sitä, että automaatio on monitoimijaympäristö. Kolmannet osapuolet ja heidän mukanaan tuomat riskit olisivat vähintään oman elementin arvoinen kokonaisuus. Asiaa sivutaan muiden elementtien yhteydessä, mutta siihen oltaisiin voitu pureutua paljon syvemmälle, esimerkiksi dokumentoinnin,

jäljitettävyyden, vastuunjaon sekä sopimusteknisten asioiden näkökulmasta. Myös yhteistyön tärkeyttä ei ole huomioitu lainkaan. Sillä pystyttäisiin helpottamaan monen ihmisen työtä organisaation sisällä tai jopa laajemmalla alueella.

Automaation tietoturvallisuuden hallintajärjestelmää perustettaessa ja käyttöönotettaessa on tärkeää, että sitä varten on perustettu oma organisaationsa. Standardin [39] mallissa tämä on huomioitu omana elementtinään: Luodaan organisaatio tietoturvallisuutta varten. Organisaation perustamiseen kuuluu vastuiden määrittelyt, riittävän poikkitieteellistä osaamista omaavan henkilökunnan järjestäminen hallintajärjestelmän luomiseen ja ylläpitämiseen. Nämä ovat usein kompastuskiviä automaation tietoturvallisuuden hallinnassa ja siksi onkin hyvä, että ne ovat erikseen huomioitu hallintajärjestelmässä. Organisaation perustamista käsitellään tarkemmin standardissa SFS 62443-2-1 [39, s. 66–69].

3.2 NIST:n kyberturvallisuuden kehysmalli

Seuraavaksi käydään läpi, millaisia lähestymistapoja yhdysvaltalainen National Institute of Standards and Technology (NIST) tarjoaa automaation tietoturvaan. NIST on julkaissut teoksen Framework for Improving Critical Infrastructure Cybersecurity [4], jossa esitellään kyberturvallisuuden kehysmalli kriittisen infrastruktuurin kyberturvallisuuden kehittämiseen. Vaikka Takon kartonkitechdas ei edusta yhteiskunnan kannalta kriittistä infrastruktuuria, NIST:n teos on mukana tutkimuksessa sen selkeän ja helposti ymmärrettävän rakenteensa ansiosta.

NIST:n kehysmalli tarjoaa perustan kyberturvallisuuteen liittyvien riskien hallintaan, mutta Takon tehtaan tarpeisiin se on ehkä tarpeettoman tarkka. Tällaisen yksityiskohtaisen mallin käytöstä on kuitenkin sikäli hyötyä, että jokaista kehysmallin vaihetta, kategoriaa ja alakategoriaa on pohdittava todella perusteellisesti sen määrittämiseksi, mikä on Takossa tarpeen ja mikä ei. Jos joku kohta tuntuu tarpeettomalta, perustellaan, mistä syistä sitä ei tarvita.

NIST on jakanut kriittisen infrastruktuurin tietoturvan riskinhallinnan viiteen suurempaan kokonaisuuteen, jotka ovat tunnistaminen, suojautuminen, havaitseminen, reagointi sekä toipuminen. Jokainen kokonaisuus jakautuu kategorioihin ja kategoriat jakautuvat edelleen alakategorioihin. Kyberturvallisuuden kehysmallin rakenne esitetään taulukossa 2.

Taulukko 2: NIST:n kyberturvallisuuden kehysmalli [muokattu lähteestä 4, s. 23].

Toiminnon yksilöivä tunniste	Toiminto	Kategorian yksilöivä tunniste	Kategoria
ID	Identify = Tunnista	ID.AM ID.BE ID.GV ID.RA ID.RM ID.SC	Asset Management = Omaisuuden hallinta Business Environment = Liiketoimintaympäristö Governance = Hallinto Risk Assessment = Riskin arviointi Risk Management Strategy = Riskinhallintastrategia Supply Chain Risk Management = Toimitusketjun riskinhallinta
PR	Protect = Suojaa	PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT	Identity Management and Access Control = Identiteetinhallinta ja pääsynhallinta Awareness and Training = Tietoisuus ja koulutus Data Security = Tietoturva Information Protection Processes and Procedures = Tietoturvaprosessit ja -menettelyt Maintenance = Huolto Protective Technology = Suojaava teknologia
DE	Detect = Havaitse	DE.AE DE.CM DE.DP	Anomalies and Events = Anomaliat ja tapahtumat Security Continuous Monitoring = Jatkuva turvallisuuden seuranta Detection Processes = Havainnointiprosessit
RS	Respond = Reagoi	RS.RP RS.CO RS.AN RS.MI RS.IM	Response Planning = Reagoimissuunnitelmat Communications = Tiedottaminen Analysis = Analyysi Mitigation = Lievennykset Improvements = Parannukset
RC	Recover = Palaudu	RC.RP RC.IM RC.CO	Recovery Planning = Toipumissuunnitelmat Improvements = Parannukset Communications = Tiedottaminen

Alkuperäisessä dokumentissa jokaisen alakategorian yhteydessä on annettu viitteet, mihin standardeihin tai toimintamalleihin perustuen kyseinen kohta voidaan toteuttaa [4, s. 24–44]. Siten tarvittava dokumentaatio käytännön työn toteutusta varten on helposti löydettävissä.

3.2.1 Tunnistusvaihe

Tunnistusvaihe jakaantuu kuuteen kategoriaan, joissa tarkastellaan organisaation omaisuutta, liiketoimintaympäristöä, hallintoa, riskien arviointia, riskien hallintaa sekä toimitusketjuja.

Ensimmäisenä tunnistusvaiheen osana on **omaisuudenhallinta**, jossa määritetään liiketoiminnan perusteena olevat laitteet, henkilökunta, data, systeemit ja välineet. Tämän kategorian alakategoriat ovat listattuna taulukossa 3. OmaisuuDENhallinta toteutetaan johdonmukaisesti yrityksen asettamien tavoitteiden ja riskinhallintastrategian mukaisesti. [4, s. 24–25]

Taulukko 3. OmaisuuDEN hallinta tunnistusvaiheessa [muokattu lähteestä 4, s. 24–25].

ID.AM Tunnistusvaihe – OmaisuuDEN hallinta	
ID.AM-1	Organisaation laitteiden ja järjestelmien inventointi
ID.AM-2	Organisaatiossa käytettyjen ohjelmistoalustojen ja sovellusten inventointi
ID.AM-3	Organisaation tietoliikenne sekä tietoaineistovirtojen kartoitus
ID.AM-4	Ulkoisten tietojärjestelmien listaus
ID.AM-5	Resurssien (esim. laitekanta, tietoaineisto, aika, henkilökunta ja ohjelmistot) priorisointi niiden luokittelun, kriittisyyden ja liikearvon perusteella
ID.AM-6	Kyberturvallisuusroolien ja -vastuiden määrittely koko henkilöstön ja ulkopuolisten sidosryhmien (esim. toimittajat, asiakkaat, kumppanit) suhteen

Seuraava kategoria perehtyy **liiketoimintaympäristöön**. Kategorian tarkoituksena on luoda ymmärrystä yrityksen tehtävistä, tavoitteista, sidosryhmistä sekä toiminnoista. Lisäksi asetetaan kaikki edellä mainitut tärkeysjärjestykseen. Tietoja hyödynnetään kyberturvallisuusvastuiden vastuunjaossa sekä riskinhallinnan päätöksenteossa. [4, s. 25] Liiketoimintaympäristön alakategorioiden sisällöt on listattu taulukkoon 4.

Taulukko 4. Tunnistusvaiheen liiketoimintaympäristö [muokattu lähteestä 4, s. 25].

ID.BE Tunnistusvaihe – Liiketoimintaympäristö	
ID.BE-1	Organisaation roolin määrittäminen toimitusketjussa ja siitä tiedottaminen
ID.BE-2	Organisaation aseman määrittäminen kriittisessä infrastruktuurissa sekä organisaation omalla teollisuuden alalla ja niistä tiedottaminen
ID.BE-3	Organisaation tehtävien, tavoitteiden ja toimintojen priorisointi ja niistä tiedottaminen
ID.BE-4	Kriittisten palveluiden toimittamiseen liittyvien riippuvuuksien ja kriittisten toimintojen määrittäminen
ID.BE-5	Kriittisten palveluiden toimitusta tukevien sietokykyvaatimusten määrittäminen kaikissa toimintatiloissa (esim. pakotettuna/hyökkäyksen alaisena, palautumisen aikana, normaalioloissa)

Tunnistusvaiheen **hallintokategorian** alakategoriat ovat listattuna taulukkoon 5. Kategorian avulla pyritään parantamaan tietoisuutta ja ohjeistamaan kyberturvallisuusriskien hallintaa selvittämällä politiikat, ohjeistukset sekä prosessit, joiden avulla hallitaan ja seurataan organisaatiota koskevia sääntöjen, lakien, riskien sekä ympäristön asettamia vaatimuksia ja operatiivisia vaatimuksia. [4, s. 25–26]

Taulukko 5. Tunnistusvaiheen hallinto-osuus [muokattu lähteestä 4, s. 25–26].

ID.GV Tunnistusvaihe – Hallinto	
ID.GV-1	Organisaation tietoturvallisuuskäytäntöjen määrittäminen
ID.GV-2	Tietoturvallisuusroolien ja -vastuiden koordinointi ja kohdistaminen sisäisiin rooleihin sekä roolien ja vastuiden jakaminen ulkoisten kumppaneiden kanssa
ID.GV-3	Perehtyminen kyberturvallisuutta koskeviin lainsäädännöllisiin vaatimuksiin, mukaan lukien yksityisyyteen ja kansalaisvapauksiin liittyvät velvoitteet, ja niiden hallinta
ID.GV-4	Kyberturvallisuusriskien huomioiminen riskinhallinta- ja johtamisprosesseissa

Riskinarviointikategoria muodostuu kuudesta alakategoriasta (taulukko 6). Kategorian toimintojen avulla pyritään lisäämään tietoisuutta kyberturvallisuudesta, jotka voivat kohdistua organisaation toimintaan, omaisuuteen ja ihmisiin. Tunnistusvaiheessa kartoitetaan uhkien vaikutusta organisaation tavoitteisiin pääsemiseen, tehtävien suorittamiseen, imagon ylläpitoon sekä maineen säilyttämiseen. [4, s. 26–27]

Taulukko 6. Tunnistusvaiheen riskinarviointi [muokattu lähteestä 4, s. 26–27].

ID.RA Tunnistusvaihe – Riskinarviointi	
ID.RA-1	Omaisuuteen kohdistuvien haavoittuvuuksien tunnistaminen ja dokumentointi
ID.RA-2	Kyberuhkiin liittyvän tietouden hankkiminen tietoa jakavilta forumeilta sekä muista lähteistä
ID.RA-3	Sisäisten ja ulkoisten uhkien tunnistus ja dokumentointi
ID.RA-4	Kyberuhkien aiheuttamien liiketoimintavaikutusten määrittäminen sekä niiden todennäköisyyksien arviointi
ID.RA-5	Uhkien, haavoittuvuuksien, todennäköisyyksien ja vaikutusten hyödyntäminen riskien määrittämisessä
ID.RA-6	Riskeihin vastaamisen määrittäminen ja priorisointi

Seuraava kategoria on **riskinhallintastrategia**. Kategorian sisältö koostuu organisaation prioriteettien, rasitteiden, riskitoleranssien ja olettamusten listaamisesta ja niitä koskevien sääntöjen laatimisesta. Tuloksia hyödynnetään päätöksenteossa operatiivisten riskien suhteen. [4, s. 27–28] Alakategoriat ovat listattuna taulukossa 7.

Taulukko 7. Tunnistusvaiheen riskinhallintastrategia [muokattu lähteestä 4, s. 27–28].

ID.RM Tunnistusvaihe – Riskinhallintastrategia	
ID.RM-1	Riskinhallintaprosessien määrittäminen, hallitseminen sekä hyväksyttäminen organisaation sidosryhmien kanssa
ID.RM-2	Organisaation riskinsietokyvyn määrittäminen ja selkeä esiintuominen
ID.RM-3	Organisaation riskinsietokyvyn määrittämisen ilmaiseminen sen roolin perusteella kriittisessä infrastruktuurissa sekä alakohtaisen riskianalyysin perusteella

Toimitusketjun riskinhallinta -kategoria koostuu viidestä alakategoriasta (taulukko 8). Tässä kategoriassa perehdytään organisaation asettamiin prioriteetteihin, rasitteisiin, riskitoleransseihin sekä olettamuksiin liittyen toimitusketjuihin. Tulosten avulla tuetaan päätösten tekoa toimitusketjuihin kohdistuvien riskien suhteen. Organisaatiolla tulee olla käytössään prosessit, joiden avulla kartoitetaan, arvioidaan ja hallitaan toimitusketjujen riskejä. [4, s. 28–29]

Taulukko 8. Toimitusketjun riskinhallinta [muokattu lähteestä 4, s. 28–29].

ID.SC Tunnistusvaihe – Toimitusketjun riskinhallinta	
ID.SC-1	Toimitusketjun kyberturvallisuuteen liittyvien riskinhallintaprosessien määrittäminen, arviointi, hallinta ja sopiminen organisaation sidosryhmien kanssa
ID.SC-2	Informaatiojärjestelmiin, komponentteihin ja palveluihin liittyvien toimittajien ja ulkopuolisten kumppaneiden tunnistus, priorisointi ja arviointi käyttäen toimitusketjun kyberturvallisuuden riskinhallintaprosessia
ID.SC-3	Toimittajilta ja ulkopuolisilta kumppaneilta vaaditaan sopimus asianmukaisen toimenpiteiden käyttöönotosta, jotta tietoturvaohjelman tai toimitusketjun kyberturvallisuuteen liittyvän riskinhallintasuunnitelman tavoitteet saavutetaan.
ID.SC-4	Toimittajat ja ulkopuoliset toimijat arvioidaan säännöllisesti, jotta varmistetaan, että he pitävät kiinni velvoitteistaan. Raportit auditoinneista, yhteenvetot testituloksista tai muut vastaavat arvioinnit toimittajista tai palveluntarjoajista toimeenpannaan
ID.SC-5	Reagoinnin ja palautumisen suunnittelu ja testaus toimittajien ja ulkopuolisten tuottajien kanssa

Tunnistusvaiheen toiminnot toimivat koko muun kehysmallin perustana. Huolellinen kartoitustyö edesauttaa siinä, että organisaatio osaa keskittyä ja panostaa resursseja oikeisiin asioihin ja pystyy siten hallitsemaan kyberturvallisuutta.

3.2.2 Suojautumisvaihe

Suojautumisvaiheessa kehitetään ja otetaan käyttöön suojatoimenpiteet, joilla varmistetaan tuotettavien palveluiden saatavuus. Vaihe muodostuu kuudesta kategoriasta, jotka

ovat identiteetin- ja pääsynhallinta, tietoisuus ja koulutus, tietoturva, tietoturvaprosessit ja menettelyt, huolto sekä suojaava teknologia.

Identiteetin- ja pääsynhallinta -kategorian kuusi alakategoriaa ovat listattuna taulukossa 9. Tässä kategoriassa käsitellään pääsynhallintaa fyysisiin ja loogisiin omaisuuksiin. Pääsyä rajoitetaan määrittämällä valtuutetut käyttäjät, prosessit ja laitteet ja sallimalla pääsy vain valtuutetuille käyttäjille. Käyttäjän identiteetistä varmistutaan identiteetin hallinnan avulla. Pääsynhallinnassa sovelletaan valtuuttamattoman pääsyn aiheuttaman riskin suuruuden arviota. [4, s. 29–31]

Taulukko 9. Suojautumisvaiheen identiteetin- ja pääsynhallinta [muokattu lähteestä 4, s. 29–31].

PR.AC Suojautumisvaihe – Identiteetin- ja pääsynhallinta	
PR.AC-1	Tunnuksien ja valtuuksien antaminen sallituille laitteille, käyttäjille ja prosesseille, ja tunnusten hallinta, verifiointi, peruutus ja auditointi.
PR.AC-2	Omaisuuden hallinta ja suojaus rajaamalla fyysistä pääsyä
PR.AC-3	Etäyhteyksien hallinta
PR.AC-4	Käyttölupien ja valtuutusten hallinta, joka käsittää pienimmän oikeuden periaatteen ja tehtävien erottelun
PR.AC-5	Verkon eheyden suojaaminen, joka käsittää verkon eristämisen tarvittaessa
PR.AC-6	Tunnuksen tarkistus ja liittäminen valtuuksiin sekä vahvistaminen tehtyjen toimintojen yhteydessä tarvittaessa
PR.AC-7	Käyttäjät, laitteet ja muu omaisuus todennetaan (esim. yksiasteinen tai useampiasteinen todentaminen) tapahtumiin liittyvien riskien mukaan (esim. yksilön tietoturvaan liittyvät riskit ja muut organisaation riskit)

Suojautumisvaiheen toinen kategoria on **tietoisuus ja koulutus**. Kategorian tarkoitus on huolehtia, että organisaation henkilökunnalle sekä yhteistyökumppaneille tarjotaan riittävästi koulutusta kyberturvallisuusasioissa. Huolehditaan siitä, että he suorittavat asiaankuuluvaa harjoittelua ja testausta tietoturvavelvollisuuksista ja vastuista ja osaavat toimia politiikkojen ja sovittujen sääntöjen mukaisesti. [4, s. 31–32] Kaikki kategorian alakategoriat löytyvät taulukosta 10.

Taulukko 10. Suojautumisvaiheen tietoisuus ja koulutus [muokattu lähteestä 4, s. 31–32].

PR.AT Suojautumisvaihe – Tietoisuus ja koulutus	
PR.AT-1	Kaikkien käyttäjien informointi ja koulutus
PR.AT-2	Etuoikeutetut/laajemmat valtuudet omaavat käyttäjät ymmärtävät roolinsa ja vastuunsa
PR.AT-3	Ulkopuoliset sidosryhmät (esim. toimittajat, asiakkaat, kumppanit) ymmärtävät roolinsa ja vastuunsa
PR.AT-4	Ylin johto ymmärtää kyberturvallisuusroolit ja -vastuut
PR.AT-5	Fyysisestä turvallisuudesta ja tietoturvallisuudesta vastaava henkilökunta ymmärtää kyberturvallisuusroolit ja vastuut

Tietoturvakategoria koostuu kahdeksasta alakategoriasta, jotka ovat listattuna taulukossa 11. Informaatiota ja asiakirjoja hallitaan organisaation riskinhallintastrategian mukaisesti siten, että varmistetaan riittävästä informaation luotettavuudesta, eheydestä sekä saatavuudesta. [4, s. 32–33]

Taulukko 11. Suojautumisvaiheen tietoturva [muokattu lähteestä 4, s. 32–33].

PR.DS Suojautumisvaihe – Tietoturva	
PR.DS-1	”Data-at-rest”: varastoidun tiedon suojaaminen
PR.DS-2	”Data-in-transit”: siirtyvän tiedon suojaaminen
PR.DS-3	Omaisuuksien hallinta sovittujen sääntöjen mukaisesti poiston, siirtojen ja luovutuksen aikana
PR.DS-4	Riittävä kapasiteetti, jotta varmistetaan käytettävyys
PR.DS-5	Suojausten toteuttaminen tietovuotojen ehkäisemiseksi
PR.DS-6	Eheystarkistusmenetelmien käyttö ohjelmiston, laitteiston ja tietojen eheyden tarkistamiseksi
PR.DS-7	Kehitys- ja testausympäristöt ovat erillään tuotantoympäristöstä
PR.DS-8	Laitteiston eheyden tarkistaminen eheystarkistusmenetelmien avulla

Taulukosta 12 voidaan tarkastella **tietoturvaprosessit ja menettelyt** -kategorian alakategorioita ja niiden sisältöä. Kategorian pääpainona ovat tietoturvan hallintaan liittyvät prosessit, ohjeistukset sekä politiikat. Tarkoituksena on huolehtia, että yllä mainitut asiat ovat ajan tasalla ja että niitä käytetään. [4, s. 33–36]

Taulukko 12. Suojautumisvaiheen tietoturvasprosessit ja menettelyt [muokattu lähteestä 4, s. 33–36].

PR.IP Suojautumisvaihe – Tietoturvasprosessit ja menettelyt	
PR.IP-1	Tietotekniikka- tai teollisuusvalvontajärjestelmien peruskokoonpanon luominen ja ylläpito, mikä käsittää asianmukaiset turvallisuusperiaatteet
PR.IP-2	Järjestelmäkehityksen elinkaaren määrittäminen järjestelmien hallintaa varten
PR.IP-3	Kokoonpanomuutosten ohjausprosessien käyttöönotto
PR.IP-4	Varmuuskopioiden ottaminen, ylläpito ja testaus määrääjien
PR.IP-5	Organisaation fyysistä toimintaympäristöä koskevien politiikkojen ja säädösten noudattaminen
PR.IP-6	Tiedon hävittäminen sovittujen käytäntöjen mukaan
PR.IP-7	Suojausprosessien jatkuva parantaminen
PR.IP-8	Suojaustekniikoiden tehokkuudesta tiedottaminen asianomaisille osapuolille
PR.IP-9	Reagointisuunnitelmat (Tapahtumiin reagointi ja liiketoiminnan jatkuvuus) ja toipumissuunnitelmat (häiriötilanteesta palautuminen ja katastrofista toipuminen) on tehty ja niitä hallitaan
PR.IP-10	Reagointi- ja toipumissuunnitelmien testaus
PR.IP-11	Kyberturvallisuus on osa henkilöstökäytäntöjä (esim. käyttäjätilien/-oikeuksien poisto, henkilöstön seulonta)
PR.IP-12	Haavoittuvuuksien hallintasuunnitelman kehittäminen ja toteuttaminen

Huoltokategoria kuvaa toimintoja, joilla huolehditaan automaatiojärjestelmän asianmukaisesta huollosta ja muista huoltoon liittyvistä toimenpiteistä. [4, s. 36] Huoltokategorian kaksi alakategoriaa ovat listattuna taulukkoon 13.

Taulukko 13. Suojautumisvaiheen huolto-osuus [muokattu lähteestä 4, s. 36].

PR.MA Suojautumisvaihe – Huolto	
PR.MA-1	Organisaation omaisuuden huollon ja korjaamisen suorittaminen ja kirjaaminen viipymättä ja hyväksytyillä ja valvotuilla välineillä
PR.MA-2	Organisaation omaisuuteen kohdistuva huolto etäyhteyden kautta hyväksytään, kirjataan ja suoritetaan siten, että luvaton pääsy on estetty

Suojaavan teknologian kategoria ja sen alakategoriat ovat listattuina taulukossa 14. Teknisiä tietoturvaratkaisuja hallitaan siten, että varmistetaan järjestelmien ja omaisuuden riittävästä turvallisuudesta ja sietokyvystä. Toimitaan aiheeseen liittyvien politiikkojen, ohjeiden ja sopimusten mukaisesti. [4, s. 36–37]

Taulukko 14. Suojautumisvaiheen suojaava teknologia [muokattu lähteestä 4, s. 36–37].

PR.PT Suojautumisvaihe – Suojaava teknologia	
PR.PT-1	Auditointi-/lokitiedostojen määrittäminen, dokumentointi, toteutus ja tarkistus yrityskäytäntöjen mukaisesti
PR.PT-2	Siirrettävien tietovälineiden suojaaminen ja käytön rajoittaminen yrityksen käytäntöjen mukaisesti
PR.PT-3	Minimitoiminnallisuuden -periaatteen toteuttaminen määrittämällä järjestelmät toteuttamaan vain välttämättömiä toimintoja
PR.PT-4	Yhteys- ja ohjausverkkojen suojaaminen
PR.PT-5	Järjestelmien toiminta ennalta määritetyissä toimintatiloissa, jotta taataan käytettävyyttä (esim. pakko, hyökkäys, palautuminen, normaalit toiminnot)

Suojautumisvaiheen toimintojen tarkoituksena on rajoittaa tai hillitä mahdollisten kyberturvallisuustapahtumien seurauksien vakavuutta.

3.2.3 Havaitse

Havaitsemisvaiheessa kehitetään ja otetaan käyttöön sopivat toimenpiteet, jotta osattaisiin tunnistaa kyberturvallisuustapahtumia. Vaiheen kategorioita ovat poikkeamat ja tapahtumat, jatkuva turvallisuuden seuranta sekä havainnointiprosessit.

Havaitsemisvaiheen ensimmäinen kategoria on **poikkeamat ja tapahtumat**. Poikkeavia toimintoja havainnoidaan oikea-aikaisesti ja ymmärretään mahdollisten poikkeavien tapahtumien aiheuttamat vaikutukset. [4, s. 37–38] Kategorian alakategoriat ovat listattuna taulukkoon 15.

Taulukko 15. Havaitsemisvaiheen poikkeukset ja tapahtumat [muokattu lähteestä 4, s. 37–38].

DE.AE Havaitsemisvaihe – Poikkeamat ja tapahtumat	
DE.AE-1	Käyttäjien ja järjestelmien verkkotoimintojen ja oletettujen tietovirtojen perustoimintojen laatiminen ja hallinta
DE.AE-2	Havaittujen tapahtumien analysointi hyökkäyskohteiden ja -menetelmien selvittämiseksi
DE.AE-3	Tapahtumatiedon kerääminen ja korrelointi useista lähteistä ja useilta sensoreilta
DE.AE-4	Tapahtumien vaikutuksen määrittäminen
DE.AE-5	Uhkien hälytysten raja-arvojen määrittäminen

Jatkuva turvallisuuden seuranta -kategoriassa käsitellään, kuinka automaatiojärjestel-

mää ja omaisuutta valvotaan diskreetein intervalein mahdollisten kyberturvallisuustapahtumien varalta. Näin varmistetaan suojaavien toimenpiteiden tehokkuudesta. Taulukoon 16 on listattu kategorian alakategoriat. [4, s. 38–40]

Taulukko 16. Havaitsemisvaiheen jatkuva turvallisuuden seuranta [muokattu lähteestä 4, s. 38–40].

DE.CM Havaitsemisvaihe – Jatkuva turvallisuuden seuranta	
DE.CM-1	Verkon valvominen mahdollisten kyberturvallisuustapahtumien havaitsemiseksi
DE.CM-2	Fyysisen ympäristön valvominen mahdollisten kyberturvallisuustapahtumien havaitsemiseksi
DE.CM-3	Henkilökunnan toimintojen valvominen mahdollisten kyberturvallisuustapahtumien havaitsemiseksi
DE.CM-4	Vahingollisen koodin havaitseminen
DE.CM-5	Luvattoman mobiilikoodin havaitseminen
DE.CM-6	Ulkoisen palveluntuottajan toiminnan valvominen mahdollisten kyberturvallisuustapahtumien havaitsemiseksi
DE.CM-7	Valtuuttamattoman henkilökunnan, yhteyksien, laitteiden ja ohjelmiston valvonta
DE.CM-8	Haavoittuvuusskannausten suorittaminen

Havainnointiprosesseihin liittyvät alakategoriat löytyvät taulukosta 17. Tämän kategorian tarkoituksena on luoda toimivat havainnointiprosessit ja testata niiden toimivuus. Havainnointiprosesseilla varmistetaan oikea-aikaisuus sekä riittävä valveutuneisuus poikkeavien tapahtumien suhteen. [4, s. 40]

Taulukko 17. Havaitsemisvaiheen havainnointiprosessit [muokattu lähteestä 4, s. 40].

DE.DP Havaitsemisvaihe – Havainnointiprosessit	
DE.DP-1	Havaitsemiseen liittyvien roolien ja vastuiden määrittäminen hyvin, jotta varmistetaan luotettavuus
DE.DP-2	Havaitsemistoiminnot ovat kaikkien sovellettavien vaatimusten mukaisia
DE.DP-3	Havaitsemistoimintojen testaaminen
DE.DP-4	Tapahtumien havaitsemistietojen viestiminen asianomaisille osapuolille
DE.DP-5	Havaitsemisprosessien jatkuva parantaminen

Havaitsemisvaiheen toiminnoilla pyritään varmistamaan kyberturvallisuustapahtumien oikea-aikainen havaitseminen

3.2.4 Reagoimisvaihe

Kehysmallin yksi tärkeä osa on reagointivaihe. Vaiheen tarkoituksena on kehittää ja käyttää tarvittavat aktiviteetit tilanteisiin, joissa havaitaan kyberturvallisuustapahtuma.

Vaiheen kategorioita ovat reagoimissuunnitelma, tiedottaminen, analyysi, lievennykset sekä parannukset.

Taulukosta 18 nähdään, että **reagoimissuunnitelma** -kategoria koostuu yhdestä alakategoriasta. Reagoimissuunnitelmaan kootaan reagoimisprosessit ja -ohjeet ja huolehditaan niiden käyttönotosta ja päivityksistä. Reagoimissuunnitelman tarkoituksena on varmistaa oikea-aikainen reagointi havaittuun kyberturvallisuustapahtumaan. [4, s. 41]

Taulukko 18. Reagointivaihe reagoitisuunnitelma [muokattu lähteestä 4, s. 41].

RS.RP Reagointivaihe – Reagoimissuunnitelma	
RS.RP-1	Reagoimissuunnitelman toteuttaminen tapahtuman aikana tai sen jälkeen

Toinen reagoimisvaiheen kategoria on **tiedottaminen**, joka koostuu viidestä alakategoriasta (taulukko 19). Reagointitoiminnoista keskustellaan sisäisten ja ulkoisten sidosryhmien kanssa, jotta saavutetaan yhtenäiset toimintasuunnitelmat. [4, s.41]

Taulukko 19. Reagointivaiheen tiedottaminen [muokattu lähteestä 4, s.41].

RS.CO Reagointivaihe - Tiedottaminen	
RS.CO-1	Henkilökunta tietää roolinsa ja toimintojen järjestyksen, kun reagointia tarvitaan
RS.CO-2	Tapahtumista raportoiminen laadittujen kriteerien mukaisesti
RS.CO-3	Tietojen jakaminen reagoimissuunnitelmien mukaisesti
RS.CO-4	Koordinoinnin suorittaminen sidosryhmien kanssa reagoimissuunnitelmien mukaisesti
RS.CO-5	Vapaaehtoinen tietojen jakaminen ulkopuolisten sidosryhmien kanssa, jotta saavutetaan laajempi tietoisuus kyberturvallisuustilanteesta

Analyysikategorian viisi alakategoriaa on listattuna taulukkoon 20. Analyysia tehdään, jotta varmistetaan siitä, että reagointitoiminnot ovat asianmukaisia ja palautuminen tapahtuu mahdollisimman tehokkaasti. [4, s. 42]

Taulukko 20. Reagointivaiheen analyysi [muokattu lähteestä 4, s. 42].

RS.AN Reagointivaihe – Analyysi	
RS.AN-1	Havaitsemisjärjestelmistä tulleiden ilmoitusten tulkitseminen
RS.AN-2	Tapahtuman vaikutuksen ymmärtäminen
RS.AN-3	Todistusaineiston tulkinta
RS.AN-4	Tapahtumien luokittelu reagoimissuunnitelmien mukaisesti
RS.AN-5	Prosessien laatiminen, jotta voidaan vastaanottaa, analysoida ja vastata sisäisten ja ulkoisten lähteiden ilmi tuomiin haavoittuvuuksiin (esim. sisäinen testaus, tietoturvailmoitukset tai tietoturvatutkijat)

Lievennyskategoria koostuu kolmesta alakategoriasta, jotka ovat listattuna taulukkoon 21. Lievennystoimenpiteiden tarkoituksena on rajoittaa kyberturvallisuustapahtuman vaikutuksien leviämistä, sekä lieventää vaikutuksia ja lopulta selvittää tapahtuma. [4, s. 42–43]

Taulukko 21. Reagointivaiheen lievennykset [muokattu lähteestä 4, s. 42–43].

RS.MI Reagointivaihe – Lievennykset	
RS.MI-1	Tapahtumien vaikutusten rajoittaminen
RS.MI-2	Tapahtumien vaikutusten lieventäminen
RS.MI-3	Uusien tunnistettujen haavoittuvuuksien lieventäminen tai dokumentointi hyväksytyiksi riskeiksi

Reagoimisvaiheen viimeinen kategoria on **parannukset** (taulukko 22). Organisaation reagoimistoimintoja kehitetään opittujen asioiden osalta. Menneitä ja tämän hetkisiä kyberturvallisuustapahtumia ja niihin liittyviä havaitsemis- ja reagoimistoimintoja hyödynnetään reagoimistoimintojen päivittämisessä. [4, s. 43]

Taulukko 22. Reagointivaiheen parannukset [muokattu lähteestä 4, s. 43].

RS.IM Reagointivaihe – Parannukset	
RS.IM-1	Reagoimissuunnitelmiin lisätään ns. kantapään kautta opitut asiat
RS.IM-2	Reagoimisstrategioiden päivittäminen

Reagoimistoiminnoilla pyritään pienentämään kyberturvallisuustapahtuman aiheuttamia vaikutuksia.

3.2.5 Palautuminen

Kehysmallin viimeinen vaihe on palautuminen. Vaiheen sisältöön kuuluu kehittää ja ottaa käyttöön soveltuvat toiminnot jatkuvuus- ja toipumissuunnitelmiin. Tavoitteena on huolehtia sietokyvystä ja palauttaa suorituskyky tai palvelut, jotka ovat kärsineet kyberturvallisuustapahtumasta. Palautumisvaihe muodostuu kolmesta kategoriasta, jotka ovat toipumissuunnitelma, parannukset ja viestintä.

Toipumissuunnitelma-kategoria koostuu yhdestä alakategoriasta (taulukko 23). Kategoriassa määritetään palautumisprosessit ja -ohjeet, otetaan ne käyttöön ja huolehditaan niiden päivityksistä. Toipumissuunnitelmaa noudattamalla varmistetaan järjestelmien nopeasta palautumisesta kyberturvallisuustapahtuman vaikutuksilta. [4, s. 43]

Taulukko 23. Palautumisvaiheen toipumissuunnitelma [muokattu lähteestä 4, s. 43].

RC.RP Palautumisvaihe – Toipumissuunnitelma	
RC.RP-1	Toimitaan toipumissuunnitelman mukaan kyberturvallisuustapahtuman aikana ja/tai sen jälkeen

Palautumisvaiheen seuraava kategoria on **parannukset**. Toipumissuunnitelmaa parannellaan aiemmista kyberturvallisuustapahtumista opittujen asioiden pohjalta. Kategorian alakategoriat on listattuna taulukkoon 24. [4, s. 43]

Taulukko 24. Palautumisvaiheen parannukset [muokattu lähteestä 4, s. 43].

RC.IM Palautumisvaihe – Parannukset	
RC.IM-1	Toipumissuunnitelmiin lisätään ns. kantapään kautta opitut asiat
RC.IM-2	Toipumisstrategioiden päivittäminen

Palautumisvaiheen ja samalla koko kehysmallin viimeinen kategoria on **viestintä** (taulukko 25). Palautumistoiminnoista sovitaan yhdessä sisäisten ja ulkoisten toimijoiden kanssa, kuten Internetin palveluntarjoajien, hyökkäysten uhrien, toisten tietoturvastaa-
vien sekä toimittajien kanssa. [4, s. 44]

Taulukko 25. Palautumisvaiheen viestintä [muokattu lähteestä 4, s. 44].

RC.CO Palautumisvaihe – Viestintä	
RC.CO-1	Tiedotusasioiden hallinta
RC.CO-2	Maineen korjaaminen tapahtuman jälkeen
RC.CO-3	Palautumistoiminnoista tiedottaminen sisäisille sidosryhmille sekä johtoportaan ja johtotiimeille

Palautumisvaiheen toimintojen tarkoituksena on varmistua tehokkaasta palautumisesta normaaleihin toimintoihin ja minimoida kyberturvallisuustapahtuman aiheuttamat vaikutukset.

3.2.6 NIST:n kehysmallin yhteenveto

Kriittisen infrastruktuurin kyberturvallisuuden hallintaan tarkoitettu NIST:n kehysmalli valittiin tutkimukseen, koska sen rakenne on erittäin selkeä, malli on kattava ja siinä annetaan lähdeviitteet jokaiseen mallin kohtaan taulukkomuodossa, jolloin jatkotutkimuksen tekeminen on helposti toteutettavissa. Järjestelmän jako viiteen suurempaan kokonaisuuteen ja siitä edelleen pienempiin osiin, tekee järjestelmästä helposti hallittavan kokonaisuuden. Kyberturvallisuuden hallintajärjestelmän käyttöönottoa ajatellen huomionarvoinen seikka on se, että NIST:n kehysmallissa ei ole huomioitu liiketoimintaperustelua, vaan siinä oletetaan, että resurssit kyberturvallisuuden hallintaan ovat olemassa. Näin ei

kuitenkaan monesti ole ja liiketoimintaperustelun tekeminen olisi ollut hyvä lisä kehysmalliin. Erityisesti jos kehysmallia sovelletaan ei-kriittisen infrastruktuurin järjestelmään, voi olla vaikea saada yritysjohto vakuutettua hallintajärjestelmän tai muiden toimenpiteiden toteuttamisen tarpeellisuudesta, jolloin liiketoimintaperustelua tarvitaan.

Yksi toimenpide, mihin liiketoimintaperustelu voi olla tarpeen, on organisaatio- ja hallintomuutokset, joilla varmistetaan, että politiikat, ohjeet, vastuunjaot ym. mahdollistavat toimivan kyberturvallisuuden hallinnan. Mallissa käydään kattavasti läpi näitä asioita, ja huolehtimalla, että tarvittavat organisaatio- ja hallintomuutokset on tehty, pystytään kyberturvallisuuden hallinnan toimenpiteitä toteuttamaan siihen varatuin henkilöstöresurssein sekä velvoittavien politiikkojen ja vastuiden nojalla.

NIST:n mallin tunnistusvaihe on erittäin kattava, ja jos tunnistusvaihe tehdään huolellisesti, kaikki toiminta siitä eteenpäin helpottuu. Järjestelmän kyberturvallisuuden hallinta on mahdollista vain, jos itse järjestelmä tunnetaan. Myös ulkoiset toimijat, osajärjestelmät sekä yhteydet ja tietovirrat jne. kartoitetaan eli monimuuttujaympäristö on huomioitu tässä mallissa.

Kuten SFS:n hallintajärjestelmän mallissa, myös tässä mallissa on paneuduttu hyvin riskeihin ja riskien hallintaan, myös toimitusketjujen osalta. Riskianalyyseissä käydään läpi liiketoimintavaikutuksia, mutta tässäkin mallissa liiketoiminnan jatkuvuudenhallinta ei ole omana kokonaisuutenaan vaan jatkuvuudenhallinnan osana on ripoteltu mallin eri osa-alueisiin. Muun muassa reagointi- ja toipumissuunnitelmien olemassaoloa, hallintaa ja testausta käsitellään kohdissa PR.IP-9 ja PR.IP-10, mutta yhtenäistä ohjeistusta jatkuvuudenhallintaan malli ei anna. Reagointi- ja toipumisvaiheen toteutukselle on kummallakin mallissa omat pääkohtansa, missä käsitellään muun muassa toimintaa häiriötilanteissa ja siitä toipuessa. Nämä kohdat onkin käsitelty kattavasti huomioiden asioita monipuolisesti esimerkiksi kiinnittämällä huomiota siihen, miten tilanteista voidaan oppia, ja että yksi osa toipumista on organisaation maineen palauttaminen.

Malli huomioi hyvin myös eri henkilöstöryhmät ja heidän erilaiset tarpeet kyberturvallisuuden liittyen. Kaikille osapuolille tulee tehdä selväksi heidän kyberturvallisuusvastuunsa ja antaa riittävä ohjeistus vastuiden täyttämiseksi. Myös eri rooleissa olevien henkilöiden koulutustarve eroaa ja tämä tulee huomioida koulutuksien järjestämisessä. Yhteistyön tärkeys mainitaan mallissa ja kuten myös tietojen jakaminen ja sen hyödyt.

Tietoturvatapahtumia pyritään havainnoimaan ja ennakoimaan havainnointivaiheen toimenpiteiden avulla. Lisäksi niiden avulla pystytään mittaamaan suojaavien toimenpiteiden toimivuutta. Molemmat edellä mainitut asiat ovat hyviä kyberturvallisuuden hallintaa helpottavia asioita.

NIST:n malli ei sisällä kuin muutaman kriittiselle infrastruktuurille sovellettavan kohdan, jotka ovat turhan tarkkoja Takon tarpeisiin. Näitä olivat ID.BE -vaiheen kohdat 2 (Organisaation aseman määrittäminen kriittisessä infrastruktuurissa), 4 (Kriittisten toimintojen

määrittäminen) ja 5 (Kriittisten palveluiden toimitusta tukevien tietokäyttövaatimusten määrittäminen), sekä ID.RM-3 (Organisaation riskinsietokyvyn määrittämisen ilmaiseminen sen roolin perusteella kriittisessä infrastruktuurissa), joissa kaikissa käsiteltiin kriittistä infrastruktuuria. Tosin ID.BE -vaiheen toiminnot voi pienin muutoksinkin jättää käyttäväksi, koska niissä käsitellään toiminnan jatkuvuutta ja tehdään roolia toimitusketjussa. Muuten malli olisi hyödynnettävissä sellaisenaan, ja mikäli mahdollista sen voisi sulauttaa osaksi automaatiojärjestelmän elinkaarta. NIST:n Framework for Improving Critical Infrastructure Cybersecurity -dokumentissa [4, s. 11] sanotaan, että tämän kehysmallin ei ole tarkoitus korvata olemassa olevia prosesseja vaan sitä voidaan hyödyntää täyttämään kyberturvallisuusaukot sulauttamalla malli olemassa oleviin prosesseihin.

3.3 CPNI:n automaation tietoturvan kehysmalli

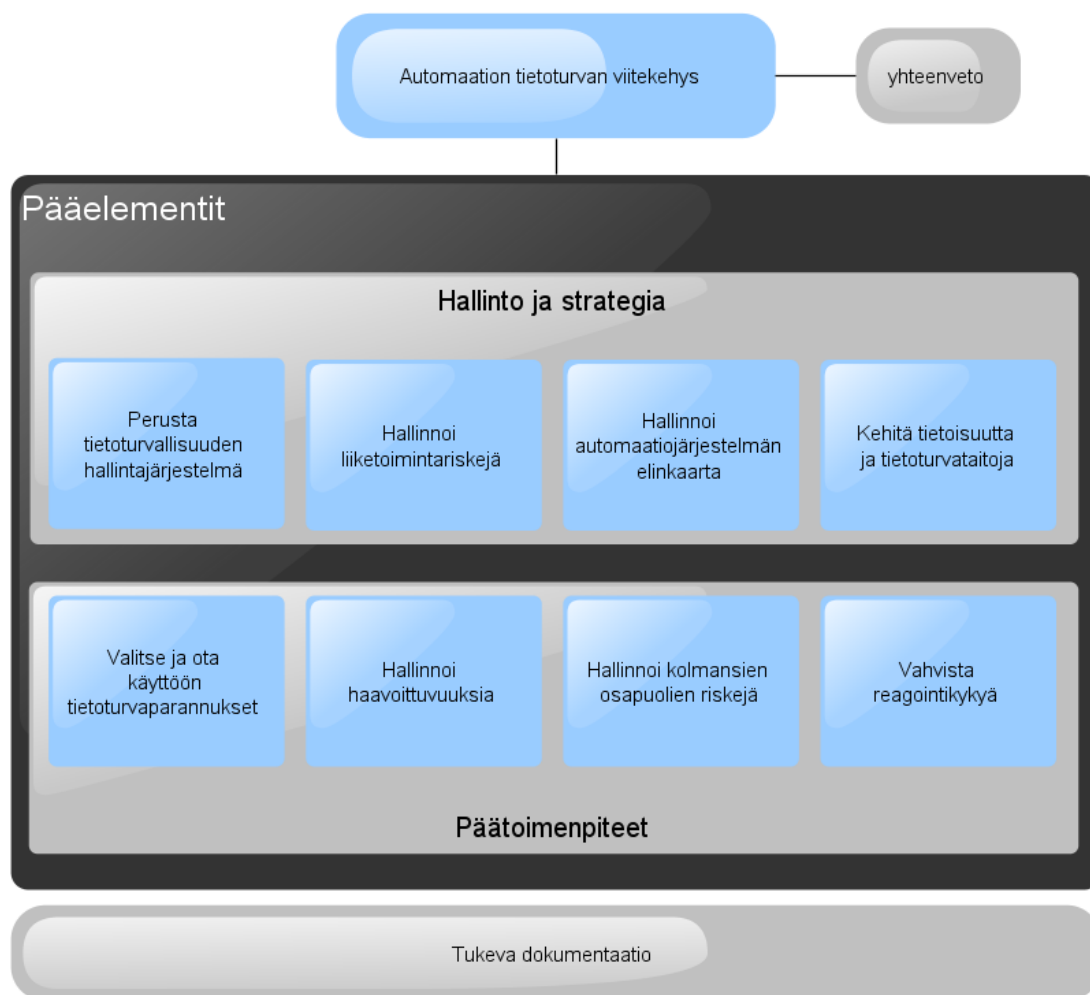
CPNI on Ison-Britannian valtiollinen virasto, joka tekee töitä kansallisen kyberturvallisuuskeskuksen NCSC:n (engl. National Cyber Security Centre) ja eri ministeriöiden ja virastojen kanssa edistääkseen Ison-Britannian kyberturvallisuusohjelmaa, jolla torjutaan kyberturvallisuusuhkia.

CPNI on koonnut omaa dokumentaatiota kyberturvallisuutta koskien. Tässä tutkimuksessa keskitytään CPNI:n laatimaan kehysmalliin, joka koostuu yleiskuvauksesta [27], yhteenvedosta [26] sekä yksityiskohtaisemmista tiedoista kehysmallin kahdeksasta pääelementistä [24–25, 28–33]. Kehysmallin tarkoituksena on tarjota hyvä toimintamalli kyberturvallisuudesta huolehtimiseen [27].

CPNI:n kehysmallin on tarkoituksena toimia räätälöidyn automaation tietoturvan hallintajärjestelmän ytimenä, eli se ei anna valmista ratkaisua automaation tietoturvan hallintaan, vaan tarjoaa raamit kehitystyölle. Kehysmallissa esitetään ohjenuorat, joiden mukaan kehysmalli on rakennettu:

- suojaa, havaitse, reagoi
- syvyysuuntainen puolustus
- tekninen suojaus, suojaavat menettelytavat sekä liikkeenjohdolliset suojaustoimenpiteet.

Näiden kolmen ohjenuoran avulla on pyritty kokoamaan mahdollisimman tehokas kehysmalli automaation tietoturvan hallitsemiseen. [27, s. 6] Kehysmallin kokonaisrakenne esitetään kuvassa 7.



Kuva 7. Automaation tietoturvan kehysmalli [muokattu lähteestä 27, s. 5].

Kehysmalli on jaettu kahteen pääelementtiin; hallinto ja tietoturvastrategia sekä päätöimenpiteet. Nämä elementit jakautuvat kumpikin neljään pienempään kokonaisuuteen, joista jokaisella on oma roolinsa tietoturvan parantamisessa. Lisäksi kehysmalliin kuuluu joukko tukevia elementtejä, joita käsitellään myöhemmin.

3.3.1 Hallinto ja tietoturvastrategia

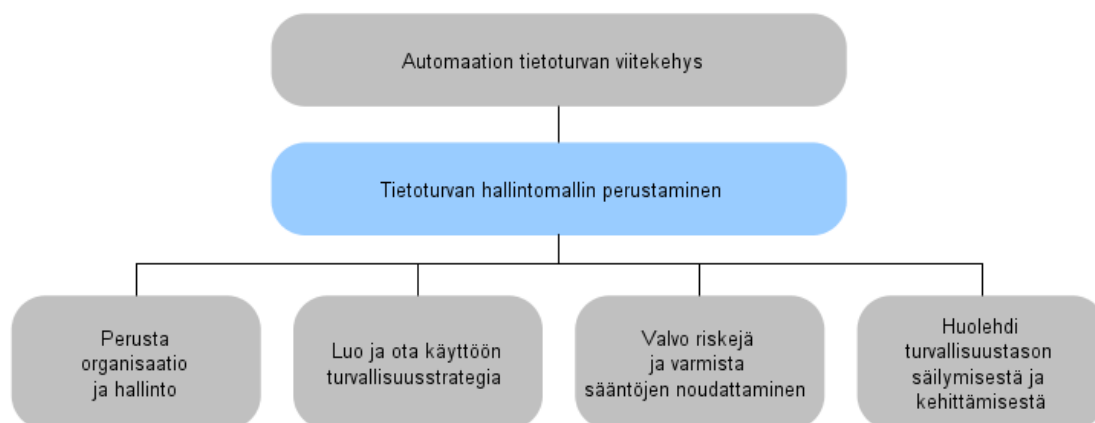
Ensimmäisen pääelementin tarkoituksena luoda toimiva hallintomalli, joka huolehtii siitä, että automaatiojärjestelmän tietoturvariskejä hallinnoidaan jatkuvatoimisesti yhteöllä tavalla ja tarkoituksenmukaisesti. Hallinto ja tietoturvastrategia -elementin osat ovat:

- toimivan tietoturvan hallintomallin perustaminen
- liiketoimintariskien hallinta
- automaatiojärjestelmän ja sen koko elinkaaren hallinta
- tietoisuuden ja tietoturvataitojen kehittäminen.

Hallinto ja tietoturvastrategia –vaiheen osa-alueita käydään pintapuolisesti läpi CPNI:n Framework Overview –dokumentissa [27, s. 7–15].

Tietoturvan hallintomallin perustaminen

Tietoturvan hallintomallin perustaminen jakaantuu kuvan mukaisiin alakohtiin (kuva 8).



Kuva 8. Tietoturvan hallintomallin perustaminen [muokattu lähteestä 24, s. 3].

Ensiksi **perustetaan organisaatio ja hallinto** toteuttamaan automaation tietoturvaa. Tätä varten on saatava ylemmän johdon tuki automaation tietoturvan hallintaa varten sekä määritettävä automaation tietoturvaan liittyvät roolit ja vastuut koko organisaation mitta-kaavassa.

Määritetään lainsäädännölliset vaatimukset ICS-turvallisuuteen liittyen ja nimetään vastuullinen taho ICS-turvallisuusriskien varalle. Organisaation koosta riippuen kyseessä voi olla yksittäinen henkilö tai useampia henkilöitä, jotka ovat yhden tahon alaisuudessa. Organisaatio- ja hallintomallin perustamista käsitellään laajemmin CPNI:n Establish Ongoing Governance -dokumentissa [24, s. 4–6].

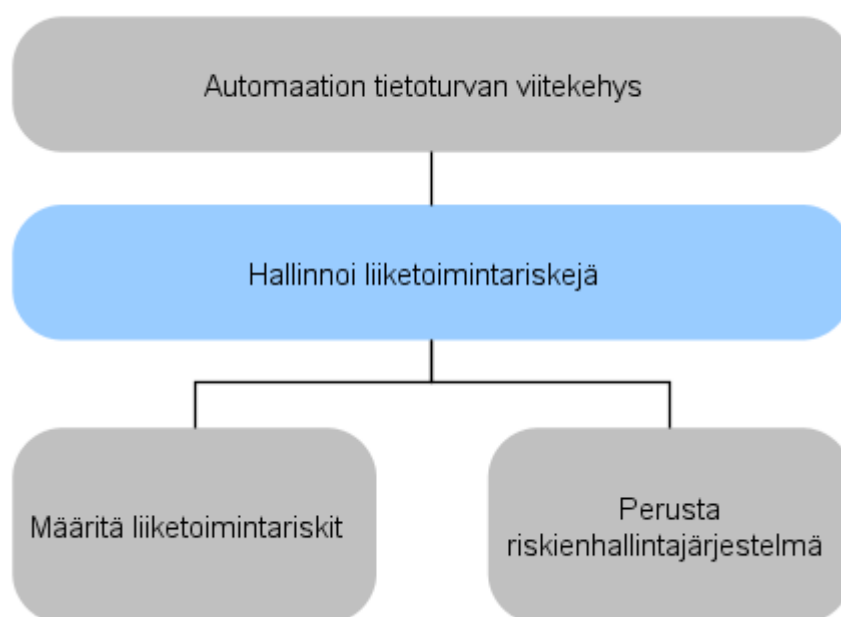
Toisessa vaiheessa **luodaan ja otetaan käyttöön turvallisuusstrategia**. Tarkoituksena on määrittää strategia, joka on linjassa liiketoiminnan ja operatiivisten tarpeiden kanssa ja minkä avulla asetetaan automaatiojärjestelmälle tietoturvallisuustavoitteet ja toimenpiteet, joiden avulla tavoitteet voitaisiin saavuttaa. Automaation tietoturvan hallintajärjestelmälle on myös edunmukaista rakentaa liiketoimintaperustelu, jonka avulla perustellaan järjestelmän perustamistarve. Automaation tietoturva koskevat muodolliset politiikat ja säännöt määritellään, dokumentoidaan, hoidetaan asianomaisten saataville sekä hallinoidaan muutoksia. Myös politiikkojen ja sääntöjen tulisi noudattaa organisaation yleistä linjausta sekä vaatimuksia ja tukea liiketoimintatavoitteita ja ne tulisi hyväksyttävä kaikilla asiaankuuluvilla osapuolilla. Turvallisuusstrategian luomiseen ja käyttöönottoon annetaan lisäohjeistusta CPNI:n Establish Ongoing Governance -dokumentissa [24, s. 7–13].

Kolmantena kohtana on **valvoa riskejä ja varmistua sääntöjen noudattamisesta**. Eli riskien muutoksia seuraamalla varmistutaan siitä, että turvallisuusstrategia pysyy asianmukaisena ajan kuluessa. Myös sääntöjen ja politiikkojen ajantasaisuutta varten täytyy sopia seurantasysteemistä. Tätä aihetta käsitellään CPNI:n Establish Ongoing Governance -dokumentissa [24, s. 14–16].

Neljäntenä **huolehditaan turvallisuustason säilymisestä ja kehittämisestä**. Hallintajärjestelmään täytyy luoda jatkuva prosessi, jonka avulla automaation tietoturvajärjestelmän säännöllisistä tarkistuksista ja jatkuvasta kehittämisestä varmistutaan. Esimerkiksi vuosittaiset uhkien päivitykset ja lakimuutosten tarkistus voisi tulla kyseeseen. Turvallisuustason seuranta ja kehittämistä käsitellään CPNI:n Establish Ongoing Governance -dokumentissa [24, s. 17–18].

Liiketoimintariskien hallinta

Hallinto ja tietoturvastrategia -pääelementin toinen alakohta on liiketoimintariskien hallinta, joka jakaantuu kahteen osaan kuvan 9 mukaisesti. Tarkoituksena on tutustua tarkasti riskeihin, jotka uhkaavat organisaation liiketoimintaa, ja niiden pohjalta kartoittaa ja toteuttaa organisaation kannalta riittävä tietoturva. [30, s. 3]



Kuva 9. *Liiketoimintariskien hallinta [muokattu lähteestä 30, s. 3].*

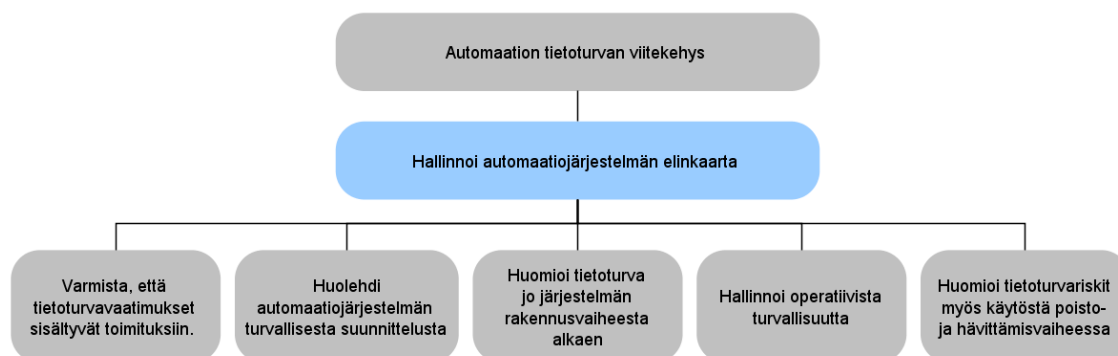
Ensimmäinen kohdista käsittelee **liiketoimintariskien määrittämistä**. Sen ensimmäinen toimenpide on saavuttaa riittävä ymmärrys automaatiojärjestelmästä. Tämän jälkeen kartoitetaan kaikki mahdolliset järjestelmää uhkaavat tekijät ja tietoturvahyökkäyksestä ai-

heutuvat mahdolliset seuraukset. Myös järjestelmän haavoittuvuudet tulee selvittää. Liiketoimintariskien määrittämiseen annetaan lisätietoa ja työkaluja CPNI:n Manage the Business Risk -dokumentissa [30, s. 4–12].

Toisessa kohdassa **perustetaan riskinhallintajärjestelmä**. Liiketoimintariski on yhtälö, joka muodostuu uhista, haavoittuvuuksista ja seurauksista. Jos jokin edellä mainituista muuttuu, se saattaa muuttaa liiketoimintariskiä. Toisin sanoen vaaditaan jatkuvaa riskinhallintaprosessia, jonka avulla reagoidaan parametrien muutoksiin ja arvioidaan liiketoimintariskit uudelleen, jotta voidaan kehittää ja ottaa käyttöön tarvittavat tietoturvan parannukset. Riskinhallintajärjestelmän perustamista käsitellään CPNI:n Manage the Business Risk -dokumentissa [30, s. 13–15]

Automaatiojärjestelmän elinkaaren hallinta

Kolmantena alakohtana on automaatiojärjestelmän elinkaaren hallinta. Elinkaaren hallinta muodostuu viidestä elementistä, jotka ovat esillä kuvassa 10. Tarkoituksena on huolehtia siitä, että kaikki suoraan tai epäsuoraan automaation tietoturvaan vaikuttavat järjestelmät noudattavat tietoturvallista suunnittelua ym. prosessia koko elinkaarensa ajan. [29, s. 3]



Kuva 10. Automaatiojärjestelmän elinkaaren hallinta [muokattu lähteestä 29, s. 4].

Varmistetaan siitä, että tietoturva-vaatimukset sisältyvät toimituksiin – Tehdään suunnitelma, jolla veloitetaan toimittajat noudattamaan tiettyä linjausta tietoturva-asioiden suhteen, jotta suunnitteluprosessi olisi turvallinen ja järjestelmän tietoturva-vaatimukset toteutuisivat. Lisäksi huolehditaan siitä, että kaikki tietoturvaan liittyvät standardit, speksit ja valitut riskien lievennystoimet tulee mainittua sopimuksissa toimittajien kanssa. Tietoturva-vaatimusten sisällyttämistä toimituksiin käydään läpi CPNI:n Manage Industrial Control Systems Lifecycle -dokumentissa [29, s. 5–7].

Huolehditaan, että automaatiojärjestelmät ovat suunniteltu turvallisiksi – Projektissa tulee olla mukana tietoturva-asiantuntija, joka on vastuussa projektiin liittyvästä tietoturvan riskinhallinnasta ja raportoinnista ja huolehtii siitä, että suunnitteluprosessi to-

teutuu turvallisesti. Kaikkien projektin suunnitteluvaiheeseen liittyvien osapuolien, mukaan lukien alihankkijoiden sekä kolmansien osapuolien, täytyy olla riittävän valveutuneita tietoturva-asioissa. Tietoturvan asettamat vaatimukset tulee huomioida alusta asti ja liittää projektin suunnitelmiin. Järjestelmän elinkaaren aikana tietoturvaa täytyy pystyä tarkastelemaan tarkastuspisteissä, joita tulee olla riittävän usein. Tietoturvaa tulee hallinnoida jokaisessa suunnitteluprojektissa, joka suoraan tai välillisesti on kytköksissä automaatiojärjestelmään. Automaatiojärjestelmien turvallisen suunnittelun varmistamista esitellään tarkemmin CPNI:n Manage Industrial Control Systems Lifecycle -dokumentissa [29, s. 8–10].

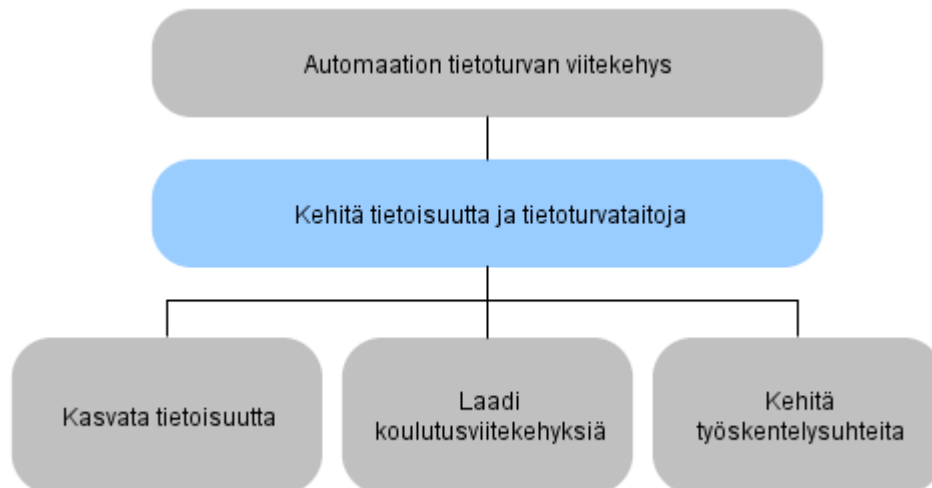
Hallinnoidaan tietoturvan toteutumista jo järjestelmän rakennusvaiheessa – Tietoturvakatselmuksia tulisi suorittaa läpi järjestelmän rakennusvaiheen esimerkiksi samaan aikaan, kun järjestelmän muuta turvallisuutta testataan. Kaikkien projektin rakennusvaiheeseen liittyvien osapuolien, mukaan lukien alihankkijoiden sekä kolmansien osapuolien, täytyy olla riittävän valveutuneita tietoturva-asioissa. Myös rakennusvaiheessa projektilla tulee olla osoitettuna henkilö, joka vastaa tietoturvan toteutumisen tarkastamisesta ja raportoinnista. CPNI:n Manage Industrial Control Systems Lifecycle -dokumentissa [29, s. 11–14] perehdytään yksityiskohtaisemmin tietoturvan toteutumisen seurantaan rakennusvaiheessa.

Hallinnoidaan operatiivista turvallisuutta – Varmistutaan siitä, että tietoturvaan liittyvät operatiiviset elementit on sulautettu liiketoiminnan joka päiväisiin operaatioihin. Kaikille kriittiseen järjestelmän osaan kiinni pääseville henkilöstön jäsenille tulee suorittaa taustatarkistukset, joita seurataan niin kauan kuin ko. henkilöillä on järjestelmän käyttö- tai pääsyoikeudet. Operatiivista turvallisuutta tulee seurata säännöllisesti koko järjestelmän elinkaaren ajan. Tietoturvaa tulee hallinnoida jokaisessa operatiivisen puolen projektissa sekä prosessissa, joka suoraan tai välillisesti on kytköksissä automaatiojärjestelmään. Lisätietoa operatiivisen turvallisuuden hallinnoinnista löytyy CPNI:n Manage Industrial Control Systems Lifecycle -dokumentissa [29, s. 15–16].

Muistetaan **huomioida tietoturvariskit myös käytöstä poisto- ja hävittämisvaiheessa**. Hävittämisvaiheessa projektilla tulee olla osoitettuna henkilö, joka vastaa tietoturvan toteutumisen tarkastamisesta ja raportoinnista. Hävittämisvaiheessa tulee huolehtia siitä, että kaikki järjestelmään liittyvä materiaali tuhoetaan asianmukaisesti, ettei tietokriittistä materiaalia pääse vääriin käsiin. Käytöstä poistoon ja hävittämiseen annetaan lisäohjeita CPNI:n Manage Industrial Control Systems Lifecycle -dokumentissa [29, s. 17–18].

Kehitä tietoisuutta ja tietoturvataitoja

Viimeinen osa-alue hallinta- ja strategielementissä on tietoisuuden ja tietoturvataitojen kehittäminen (kuva 11). Tavoitteena on kehittää ja ylläpitää henkilöstön tietoisuutta ja tietoturvataitoja, jotta he pystyvät tietoturvallisesti suoriutumaan työtehtävistään. [28, s. 3]



Kuva 11. Tietoisuuden ja tietoturvataitojen kehittäminen [muokattu lähteestä 28, s. 3].

Kasvata tietoisuutta – Yhteistyötä korkeamman portaan kanssa tulee lisätä, jotta ICS-riskit saadaan heidän tietoisuuteen ja sitä kautta tuki riskinhallinnalle. Myös muun henkilöstön automaation tietoturvaan liittyvää tietoisuutta tulee kasvattaa, jotta jokainen tuntee vastuunsa, tietää järjestelmään liittyvät uhat ja osaa varautua mahdollisiin uhkaaviin tilanteisiin ja ennaltaehkäistä niiden syntymistä. Tarvittaessa tulee tehdä liiketoimintaperustelu, jotta pystytään osoittamaan automaation tietoturvan hallintajärjestelmän tarpeellisuus. Lisätietoa tietoisuuden kasvattamisesta löytyy CPNI:n Improve Awareness and Skills -dokumentista [28, s. 4–7].

Perustetaan harjoituskehysmalleja – Koulutetaan IT-puolen osaajia ymmärtämään ja arvostamaan ICS-järjestelmän ominaisuuksia, IT-järjestelmän ja ICS-järjestelmän yhteneväisyyksiä ja eroavaisuuksia sekä niiden tietoturvan eroja ja yhteneväisyyksiä. Myös ICS-henkilökunnan tulisi tutustua riittävällä tasolla IT-järjestelmien toimintaan. Tätä aihetta käsitellään CPNI:n Improve Awareness and Skills -dokumentissa [28, s. 8–10].

Kehitetään työskentelysuhteita – Varmistutaan siitä, että IT- ja automaatiohenkilökunnan yhteistyö toimii ja riittävä tuki on aina saatavilla. Työskentelysuhteiden kehittämistä käydään läpi CPNI:n Improve Awareness and Skills -dokumentissa [28, s. 11–12].

3.3.2 Päätoiminnot

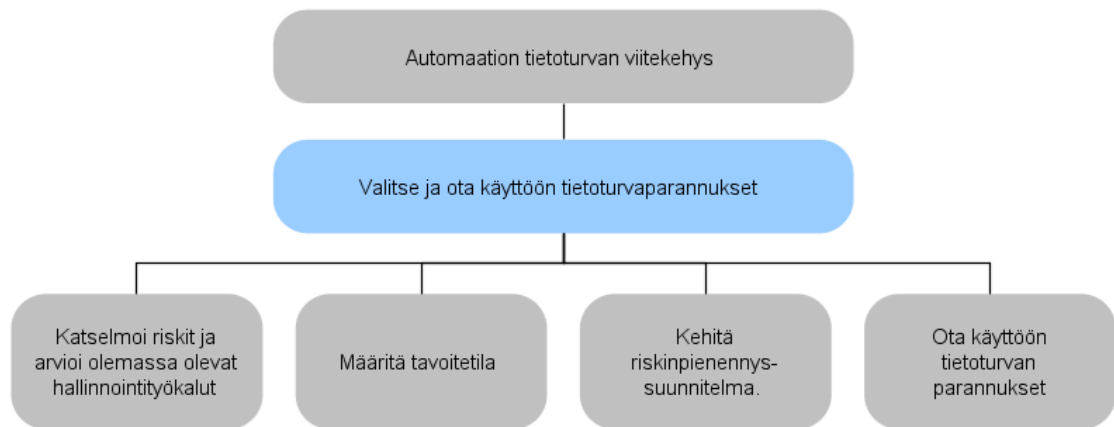
Automaation tietoturvan hallintaan liittyviä päätoimintoja ovat:

- valita ja ottaa käyttöön tietoturvaparannukset
- hallita haavoittuvuuksia
- hallita kolmasien osapuolien riskejä
- kehittää reagoitipotentiaalia.

Edellä mainitut päätoiminnot on esitelty pintapuolisesti CPNI:n Framework Overview – dokumentissa [27, s.16–23].

Valitse ja ota käyttöön tietoturvarapannukset

Liiketoimintariskin arvion perusteella organisaation tulisi valita ja ottaa käyttöön tekniset ratkaisut, menettelytavat sekä hallinnoida suojausmittareita parantaakseen ICS:n tietoturvaa. Tietoturvarapannusten valinta ja käyttöönotto jakaantuu kuvan 12 mukaisiin osiin. [33, s. 3]



Kuva 12. Tietoturvarapannusten valinta ja käyttöönotto [muokattu lähteestä 33, s. 3].

Katselmoi riskit ja arvioi olemassa olevat hallinnointityökalut – Tulee muodostaa monitieteellinen riskin ehkäisyryhmä. Tämän lisäksi katselmoidaan liiketoimintariskit ja arvioidaan tämänhetkisten kontrollimenetelmien tehokkuutta löydettyjä riskejä vastaan. CPNI:n dokumentissa Select and Implement Security Improvements [33, s. 4–5] tutustutaan paremmin riskikatselmoiintiin ja hallinnointityökalujen arviontiin.

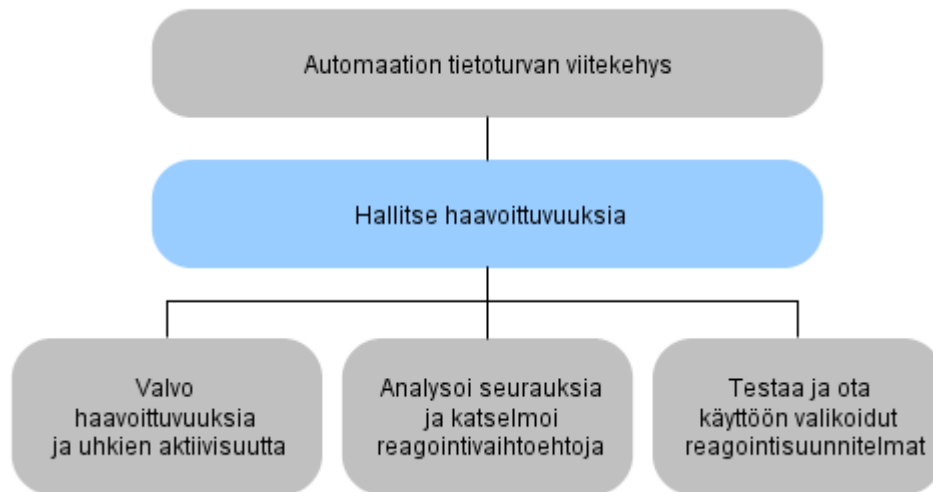
Määritetään tietoturvariskeihin liittyvä tavoitetilä. Sitä varten tulee hyväksyttää organisaation tavoitteellinen riskiprofiili ja luoda riskinpienennysstrategia. Lisäksi tulee kartoittaa tietoturvamittarit, joilla voidaan mitata riskejä. Tavoitetilan määrittäystä käydään läpi CPNI:n Select and Implement Security Improvements -dokumentissa [33, s. 6–7].

Kehitä riskinpienennysuunnitelma järjestämällä riskinpienennystyöpaja-tilaisuuksia, joissa kartoitetaan nopeasti ja helposti korjattavissa olevia tietoturvauhkia sekä pidemmän aikavälin ratkaisuja. Kartoitetaan myös, onko olemassa nopeita, vähin resurssein korjattavia riskejä. Työpajoja sekä kartoitustyötä hyödyntäen muodostetaan riskinpienennysuunnitelma. Riskinpienennysuunnitelman laatimista käsitellään tarkemmin CPNI:n dokumentissa Select and Implement Security Improvements [33, s. 8–11].

Tietoturvaparanusten käyttöön otto tapahtuu hyväksyttämällä ensin käyttöönotto-suunnitelmat. Tämän jälkeen voidaan suorittaa tietoturvaparanusten käyttöönotto. Asiaan paneudutaan laajemmin CPNI:n dokumentissa Select and Implement Security Improvements [33, s. 12–13].

Hallitse haavoittuvuuksia

Haavoittuvuuksien hallinta ei ole kertaluontoinen tehtävä vaan dynaaminen prosessi. Haavoittuvuudet kehittyvät ja muuttuvat ajan myötä ja tämän vuoksi niitä tulisi jatkuvasti arvioida, ja reagoida mahdollisiin muutoksiin. Mitä nopeammin tämä tapahtuu, sitä tehokkaampi haavoittuvuuksien hallinta yrityksellä on. Kuvasta 13 nähdään, miten haavoittuvuuksien hallinta voidaan toteuttaa. [32, s. 3]



Kuva 13. Haavoittuvuuksien hallinta [muokattu lähteestä 32, s. 4].

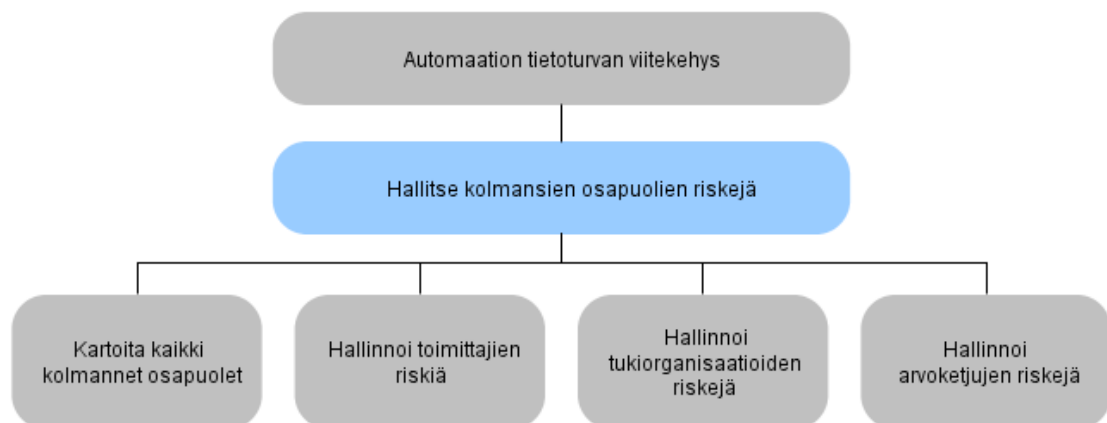
Valvo haavoittuvuuksia ja uhkien aktiivisuutta – Otetaan käyttöön haavoittuvuuksien hallintajärjestelmä, jotta voidaan varmistua siitä, että automaatiojärjestelmän haavoittuvuudet pysyvät minimissä. Lisäksi seuraamalla julkaisuja ja tiedotusta haavoittuvuuksista ja uhista pidetään huolta siitä, että kaikki automaatiojärjestelmää uhkaavat uudet haavoittuvuudet ovat tiedossa. Automaatiojärjestelmän uhkia arvioidaan säännöllisesti, ja tarkkaillaan, muuttuvatko riskiprofiilit. CPNI:n dokumentissa Manage Vulnerabilities [32, s. 5–8] tarkastellaan haavoittuvuuksien ja uhkien valvontaa yksityiskohtaisemmin.

Analysoi seurauksia ja katselmoi reagoitinvaihtoehtoja – Jos ilmenee uusia haavoittuvuuksia tai muutoksia uhkakuviin, niiden vaikutuksia automaatiojärjestelmään tulee analysoida. Jos muutoksilla on vaikutusta järjestelmään, tulee miettiä uusia suojauskeinoja, joilla voidaan kompensoida vaikutuksia. Seurausten analysointia ja reagoitinvaihtoehtojen katselmointia käsitellään CPNI:n Manage Vulnerabilities -dokumentissa [32, s. 9–11].

Testataan ja otetaan käyttöön valikoidut reagointisuunnitelmat. Ensin luodaan prosessit automaatiojärjestelmän korjaustiedostojen käyttöönotolle. Nämä prosessit tulisi huomioida myös käyttöönotoissa ja auditointityökaluissa. Näissä prosesseissa tulisi ottaa huomioon korjaustiedostojen kriittisyysarvioinnit, toimittajien sertifiikatit, testaus ennen käyttöönottoa sekä asteittainen käyttöönottoprosessi. Näin minimoidaan muutosten aiheuttamat häiriöt ja keskeytykset. Lisäksi varmistutaan siitä, että prosessi on integroitu tietoturvahälytysten ja haitallisten tietoturvatapahtumien kanssa siten, että se osaa reagoida niihin. Reagointisuunnitelmien testaukseen ja käyttöönottoon pureudutaan CPNI:n Manage Vulnerabilities -dokumentissa [32, s. 12–13].

Hallitse kolmansien osapuolien riskejä

Tämän vaiheen tarkoituksena on kartoittaa kaikki tärkeät kolmannet osapuolet sekä heihin liittyvät riskit, joilla voi olla vaikutusta organisaation automaatiojärjestelmään. Kun kartoitus on tehty, pyritään osapuolia ja riskejä hallitsemaan. Kuva 14 esittää, minkälaisiin osa-alueisiin kolmansien osapuolien riskinhallinta jakaantuu. [31, s. 3]



Kuva 14. Kolmansien osapuolien riskinhallinta [muokattu lähteestä 31, s. 3].

Ensimmäiseksi tulee **kartoittaa kaikki kolmannet osapuolet**, mukaan lukien toimittajat ja palveluntarjoajat ja kaikki muut toimijat jotka ovat jollain tavalla sidoksissa organisaation automaatiojärjestelmään. CPNI:n Manage Third Party Risks -dokumentti [31, s. 4–5] käsittelee kolmansien osapuolien kartoittamista tarkemmin.

Hallinnoi toimittajien riskiä – Varmistetaan, että tietoturvalausekkeet ovat yksityiskohdaisesti esitettyinä kaikissa hankintasopimuksissa aiempien sopimusten mukaisesti ja että ne välittyvät myös alihankkijoille asti. Tämän lisäksi tehdään jatkuvaa yhteistyötä toimittajien kanssa, jotta varmistutaan siitä, että toimittajien toimittamien järjestelmien tämänhetkiset ja tulevat haavoittuvuudet tulee huomatuksi myös tilaajaorganisaatiossa. Huolehditaan myös siitä, että organisaatiossa ymmärretään toimitetun automaatiojärjestelmän tietoturva-arkkitehtuuri ja mahdollinen etätuki ja sen tuomat haasteet. Myös toimittajien

täytyy ymmärtää organisaation automaatiojärjestelmän arkkitehtuuri, jotta he voivat toimittaa tietoturvallisen järjestelmän. [31, s. 6]

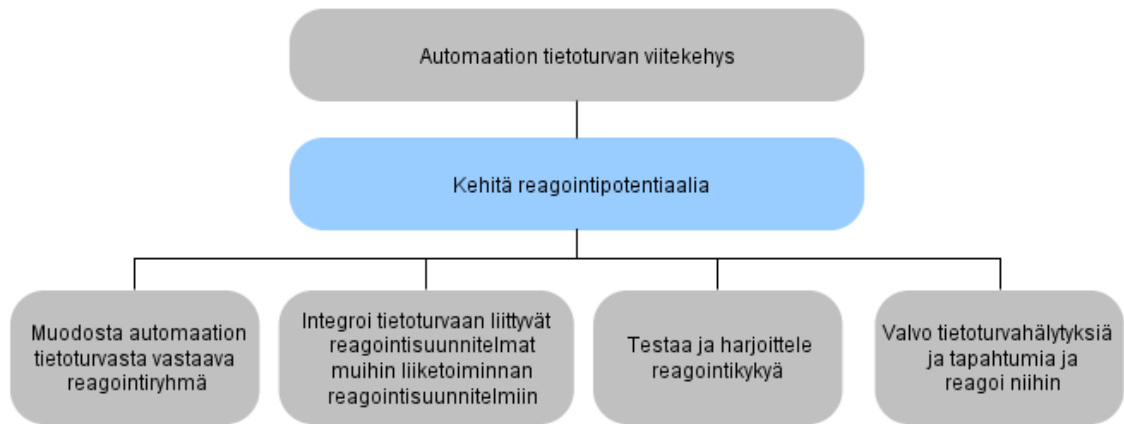
Toimittajilta tulee vaatia tietoturvaopastusta heidän toimittamiin tämän hetkisiin automaatiojärjestelmän osiin. Lisäksi tulee vaatia suunnitelma siitä, miten tulevaisuuden tietoturvaasteisiin aiotaan vastata. Huolehditaan myös siitä, että kaikki toimittajat asentavat asianmukaiset haittaohjelmien torjunnat heidän toimittamiinsa automaatiojärjestelmiin. Toimittajien kanssa tulee ottaa käyttöön tehokas ohjelmistojen patch-prosessi ja sopia järjestelmien kovennuksista. Lisäksi selvitetään kaikki ohjelmistokomponenttitekniologiat, mitä automaation osajärjestelmissä on käytössä, jotta kaikki haavoittuvuudet pysyvät hallinnassa. On myös tärkeää suorittaa säännöllisiä tietoturvakatselmuksia ja -auditointeja toimittajille järjestelmien priorisoinnin mukaan. Toimittajiin liittyvää riskinhallintaa käydään läpi CPNI:n Manage Third Party Risks -dokumentissa [31, s. 6–9].

Hallinnoi tukevien organisaatioiden riskejä tekemällä säännöllisiä riskiarvioita tukiorganisaatioille ja varmistamalla siitä, että kaikki vastatoimenpidevaatimukset on toteutettu. Tukiorganisaatioilta estetään pääsy automaatiojärjestelmään kunnes asianmukaiset mittarit tietoturvaohjeiden estämiseksi tai pienentämiseksi toteutuvat. Julkaistaan ja hyväksytään sopimus, jolla määritellään ehdot yhteyden muodostamiselle. Lisäksi tehdään yhteistyötä kaikkien tukiorganisaatioiden kanssa, jotta kaikki mahdolliset tietoturvatapaukset, joilla voisi olla vaikutusta organisaation automaatiojärjestelmän tietoturvaan, tulee raportoitua. Tulee myös lisätä kaikkien tukiorganisaatioiden tietoisuutta, jotta ne täysin ymmärtäisivät automaatiojärjestelmän rakenteen ja sitoutuisivat työskentelemään tietoturvaohjeistuksen puitteissa. Tätä aihetta käsitellään tarkemmin CPNI:n Manage Third Party Risks -dokumentissa [31, s. 10–12].

Hallinnoi arvoketjujen riskejä varmistamalla siitä, että kaikki arvoketjun organisaatiot ovat huolehtineet tietoturvastaan ja että he vakuuttavat että heidän tietoturvariskinsä ovat hallinnassa. Arvoketjujen riskinhallinnasta annetaan lisätietoa CPNI:n Manage Third Party Risks -dokumentissa [31, s. 13–14].

Kehitä reagoitipotentiaalia

Automaatiojärjestelmän uhat muuttuvat ja kehittyvät ajan myötä. Tietoturvan tasoa tulisi arvioida jatkuvasti, jotta pystytään reagoimaan vaaratilanteisiin. Tämän vuoksi tulisi ottaa käyttöön reagoinnin hallintajärjestelmä, jolla varmistutaan siitä, että muutokset riskeissä huomataan mahdollisimman nopeasti ja korjaaviin toimenpiteisiin ryhdytään ripeästi. Kuvasta 15 nähdään, miten reagoitipotentiaalia voidaan kehittää. [25, s. 3]



Kuva 15. Reagointipotentialin kehittäminen [muokattu lähteestä 25, s. 3].

Muodostetaan ICS:n tietoturvasta vastaava reagointiryhmä – Muodostetaan automaatiojärjestelmän tietoturvasta vastaava ryhmä, jonka vastuulla on huolehtia tietoturvatilanteisiin reagoimisesta. Ryhmän tulee muodostua eri liiketoiminta-alueiden osajista, jotta kaikki automaation tietoturvaan liittyvät osa-alueet tulevat huomioitua. Reagointiryhmän muodostamisesta ohjeistetaan CPNI:n Establish Response Capabilities -dokumentissa [25, s. 4–5].

Integroidaan tietoturvaan liittyvät reagointisuunnitelmat muihin liiketoiminnan reagoimissuunnitelmiin. Tämä tapahtuu huolehtimalla siitä, että automaatiojärjestelmälle on olemassa reagointisuunnitelma, liiketoiminnan jatkuvuussuunnitelma, katastrofisuunnitelma ja hätätilannesuunnitelma. Kyberturvallisuuden reagointisuunnitelman tulee olla integroituna muihin yllämainittuihin suunnitelmiin. Suunnitelmien integrointia käydään tarkemmin läpi CPNI:n Establish Response Capabilities -dokumentissa [25, s. 6–8].

Testataan ja harjoitellaan reagointikykyä varmistamalla, että kaikki kyberturvallisuuden liittyvät suunnitelmat tarkistetaan säännöllisesti ja että niiden toteuttamista harjoitellaan ja testataan. Aihetta käsitellään CPNI:n Establish Response Capabilities -dokumentissa [25, s. 9–10].

Tietoturvahälytyksiä ja -tapahtumia valvotaan ja niihin reagoidaan. Nämä toteutetaan luomalla järjestelmä, joka varoittaa asiaankuuluvaa henkilökuntaa tietoturvatapahtumista mahdollisimman pian hälytyksen tapahtuessa. Lisäksi luodaan ohjeet ja prosessit tietoturvatapahtumien valvontaa, arviointia ja niihin reagoimista varten. Tulee myös huolehtia siitä, että automaatiojärjestelmään kohdistuneet tietoturvatapahtumat raportoidaan, käydään läpi ja niiden perustella tehdään parannuksia reagoimissuunnitelmiin. Tietoturvahälytyksien ja -tapahtumien valvontaa ja niihin reagoimista tarkastellaan CPNI:n Establish Response Capabilities -dokumentissa [25, s. 11–16].

3.3.3 CPNI:n kehysmallin yhteenveto

CPNI:n kehysmalli on erittäin selkeä rakenteeltaan ja se huomioi oleelliset asiat monipuolisesti. Framework Overview -dokumentti [27] antaa hyvän, helppolukuisen ja helposti ymmärrettävän yleiskuvan kehysmallin rakenteesta. Jos lukija haluaa perehtyä tarkemmin dokumentaatioon, kehysmallin kahdeksasta eri osa-alueesta on jokaisesta omat dokumenttinsa, jotka paneutuvat aiheiden sisältöön tarkemmin. Dokumentteissa on myös hyvät lähdeviittaukset jatkotutkimusta varten. Tässäkin kehysmallissa painotetaan sitä, että malli ei tarjoa valmiita ratkaisuja vaan pohjan automaation tietoturvan hallintajärjestelmän kehittämiseen. Toisin sanoen, organisaation tulee itse räätälöidä mallin pohjalta organisaation tarpeille sopiva järjestelmä.

Kehysmallissa ensimmäisenä käsitellään hallintoa ja mitä kaikkea siihen liittyvää täytyy huomioida tietoturvan hallintajärjestelmän käyttöönotossa. Eli ensin käsitellään tarvittavia hallinnollisia muutoksia, tarvittavan tukioorganisaation perustamista sekä tietoturvastrategian luomista. Lisäksi tarkkaillaan riskejä, pidetään yllä tietoturvallista toimintaa ja kehitetään sitä. Kaikki nämä ovat oleellisia hallinnollisia seikkoja, jotka on hyvä huomioida jo automaation tietoturvan hallintajärjestelmän perustamisvaiheessa. Dokumentteissa mainitaan, että resursseja hallintajärjestelmää varten voidaan koittaa saada liiketoimintaperustelun avulla.

CPNI:n dokumentit ovat myös hyvin riskipainotteisia, ja riskianalyysiin ja riskinhallintaan on keskitytty laajalti ja lisäksi esimerkiksi haavoittuvuuksien hallinta on saanut paljon huomiota tässä kehysmallissa. Liiketoiminnan jatkuvuudenhallintaa ei sinänsä dokumenteissa käsitellä, mutta niissä mainitaan, että esimerkiksi automaation tietoturvaan liittyvät reagointisuunnitelmat tulee integroida liiketoiminnan jatkuvuuden hallinnan kanssa. Tämä on periaatteessa hyvä toimintamalli, mutta se edellyttää, että organisaation liiketoiminnan jatkuvuudenhallinta on entuudestaan kunnossa.

CPNI:n kehysmallissa huomioidaan hyvin se, että automaatio on monitoimijaympäristö ja siksi kolmansien osapuolien riskien hallintaan on paneuduttu perusteellisesti. Myös automaation tietoturva-vaatimusten sisällyttäminen hankintasopimuksiin on yhtenä osana hallintajärjestelmän elinkaarenhallinta -osiota. Kehysmallissa hyödynnetäänkin automaation elinkaarta ja pyritään saamaan tietoturva osaksi sitä.

Tietoturvan parannuskeinojen valinta ja käyttöönotto on otettu omaksi kokonaisuudekseen CPNI:n kehysmallissa. Onkin hyvä, että kyseiselle prosessille annetaan ns. valmis kaava, jonka mukaan toimia. Kun tietoturvaparannusten valintaan ja käyttöönottoon liittyvät oleelliset seikat on kertaalleen kartoitettu, niitä voidaan jatkossa hyödyntää järjestelmällisesti. Toisin sanoen, tietoturvaparannusten valinta ja käyttöönotto on pyritty automatisoimaan, jolloin vältetään tekemästä sama työ useampaan kertaan ja valinta ja käyttöönotto tapahtuu suoraviivaisesti vaatien mahdollisimman vähän resursseja.

Henkilöstön automaatioon liittyvän tietoturvatietoisuuden lisääminen ja tietoturvataitojen kasvattaminen ovat myös saaneet paljon huomiota CPNI:n kehysmallissa. Koulutusten ja ohjeistuksen lisäämisen lisäksi kehysmallissa painotetaan yhteistyön tärkeyttä. Organisaation eri osastojen yhteistyö ja tiedon jakaminen ovatkin suuressa roolissa, jotta saadaan perustettua toimiva automaation tietoturvan hallintajärjestelmä. CPNI:n dokumentti käsittelee tässä kohtaa vain organisaation sisäistä yhteistyötä, mutta yhteistyötä voisi laajentaa kattamaan myös toisia organisaatioita.

3.4 Kirjallisuustutkimuksen tulos

Kirjallisuustutkimuksessa tutustuttiin teoksiin SFS-IEC 62443-2-1 Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten [39], Framework for Improving Critical Infrastructure Cybersecurity [4] ja Security for Industrial Control Systems, Framework Overview sekä sen oheisjulkaisuihin [24–33]. Teosten pohjalta saatiin kattava katsaus siihen, mitä osa-alueita prosessiautomaation tietoturvan hallintajärjestelmän tulisi sisältää. Teoksissa painotetaan sitä, että niissä esitetyt mallit eivät ole valmiita ratkaisuja automaation tietoturvan hallintaan, vaan jokaisen organisaation tulee karhottaa omat tarpeensa ja niiden pohjalta teosten tietoja hyödyntäen räätälöidä organisaation tarpeita vastaava automaation tietoturvan hallintajärjestelmä. Yhteenvedona teoksista koostetut tiedot jaettiin kolmeen suurempaan kokonaisuuteen, jotka liittyvät hallintajärjestelmän perustamiseen, ihmisten sitouttamiseen automaation tietoturvan hallintaan sekä tietoturvan integroimiseen automaatiojärjestelmän elinkaareen.

3.4.1 Prosessiautomaation tietoturvan hallintajärjestelmän perustamis- ja käyttöönottoaihe

Tutkimuksen teoksissa [27, 39] sanotaan, että hallintajärjestelmän perustaminen ja siihen liittyvät toimenpiteet voivat vaatia liiketoimintaperustelun, jonka avulla saadaan yritysjohdon tuki ja vaadittavat resurssit. Kaikissa kolmessa teoksessa mainitaan, että hallintajärjestelmä vaatii toimiakseen myös sitä tukevan organisaation sekä hallintomuutoksia, jotka on syytä tehdä heti järjestelmän perustamisvaiheessa.

Jokaisessa teoksessa käsitellään kattavasti riskinhallintaa ja siihen liittyvää riskinhallintastrategiaa. Liiketoiminnan jatkuvuudenhallinta ja -hallintastrategia näyttelevät pienempää osaa, mutta niihin liittyviä osa-alueita liittyy jokaiseen kolmessa teoksessa esitettyyn malliin. Näin siksi, että liiketoiminnan jatkuvuudenhallintastrategia oletetaan olevan jo olemassa, ja tarkoitus on, että automaatiojärjestelmän jatkuvuudenhallintaan liittyvät elementit integroidaan jo olemassa olevaan jatkuvuudenhallintaan. Joka tapauksessa liiketoiminnan jatkuvuudenhallinta on tärkeä osa prosessiautomaation tietoturvaa ja se tulee huomioida prosessiautomaation tietoturvan hallintajärjestelmässä.

Eräs automaation tietoturvanhallinnan kannalta oleellinen asia on järjestelmätuntemus. Jotta automaatiojärjestelmän tietoturvaa voidaan hallita, täytyy automaatiojärjestelmä tuntea läpikotaisin, eli kaikki mahdollinen automaatiojärjestelmään liittyvä tulee tunnistaa ja dokumentoida. Laitteet, sovellukset, ihmiset, tietoverkot, tieto jne. Laitelistaaja ja dokumentaatiota täytyy myös ylläpitää ja niiden ajantasaisuutta tulee valvoa valvontamenettelyin.

Myös prosessiautomaation tietoturvan hallintajärjestelmän toimintaa tulee valvoa valvontamenettelyin. Näistä menettelyistä tulee sopia heti järjestelmän perustamisvaiheessa, jotta pystytään seuraamaan, että järjestelmä toteuttaa sille asetettuja vaatimuksia, ja että halutut tietoturvatavoitteet saavutetaan. Mikäli valvontamenettelyt paljastavat puutteita järjestelmän toiminnassa, tulee järjestelmää kehittää, ja ottaa käyttöön vaadittavat muutokset, joiden avulla vaatimukset ja tavoitteet täyttyvät.

3.4.2 Ihmisten sitouttaminen automaation tietoturvan hallintaan

Suuri uhka automaatiojärjestelmän tietoturvalle on ihmisten toiminta. Tästä syystä on tärkeää, että kaikki automaatiojärjestelmän parissa työskentelevät henkilöt ovat tietoisia riskeistä, heillä on riittävät taidot suorittaa työnsä tietoturva huomioiden ja he osaavat tarvittaessa etsiä automaation tietoturvaan liittyvät ohjeet ja toimintatapamallit ja noudattavat niitä.

Kaikissa kolmessa kirjallisuustutkimukseen osallistuneessa teoksessa käsitellään henkilöstön kouluttamista ja tietoturvatietoisuuden lisäämistä. Yksi huomioitava asia on se, että eri henkilöstöryhmille tulee järjestää erilaisia koulutuksia, joilla pystytään lisäämään niitä tietoturvatietoja ja -taitoja, joita ko. henkilöt työssään tarvitsevat. Myös sitä painotetaan, että tietoturvavastuut täytyy tiedottaa siten, että voidaan varmistua siitä, että jokainen asianosainen tietää omat vastuunsa ja velvollisuutensa.

Ohjeistuksien ja toimintamallien ajantasaisuus ja saatavuus on huomioitu kaikissa kolmessa teoksessa. Niiden avulla voidaan lisätä tietoisuutta ja taitoja, kunhan niiden päivityksistä on huolehdittu ja ne ovat niitä tarvitsevan henkilökunnan saatavilla. CPNI:n sekä NIST:n kehysmalleissa käsitellään hyvin myös yhteistyön tarpeellisuutta. Yhteistyöllä pystytään saamaan kokoon monitieteellistä osaamista, mikä on tarpeen automaation tietoturvan hallinnassa. Lisäksi yhteistyöllä voidaan helpottaa monen ihmisen työkuormaa, kun samoja asioita ei tehdä uudelleen monen ihmisen toimesta, vaan tietoa jaetaan. Yhteistyöllä on myös monia muita positiivisia vaikutuksia automaation tietoturvan hallintaan.

Kaikki ihmisten sitouttamiseen liittyvä toiminta tulee dokumentoida, sitä tulee arvioida, kehittää ja ylläpitää tarpeen mukaan. Henkilökunnan koulutuksista tulee pitää kirjaa, ja

heitä tulee uudelleen kouluttaa tarpeen vaatiessa. Ohjeistus, toimintamallit ym. tulee dokumentoida ja niiden ajantasaisuudesta tulee huolehtia. Eli myös ihmisten sitouttamisen valvontaan ja kehittämiseen on hyvä olla olemassa valvontamenettelyjä, joita hyödyntää.

3.4.3 Automaatiojärjestelmän elinkaaren hallinta ja tietoturva

Automaatiojärjestelmän elinkaari mainitaan erikseen vain CPNI:n kehysmallissa. Muissa malleissa asioita ei mitenkään sidottu elinkaareen vaan niitä on ripoteltu malleihin muun jaottelun pohjalta. Automaatioprojektien yksi tärkeimmistä vaatimuksista on kokonais-turvallisuus, joka voidaan saavuttaa hyödyntämällä automaation elinkaarimallia, johon on lisätty tietoturvanäkökulma. Elinkaarimallin hyödyntäminen takaa myös sen, että tarvittavien testien ja kelpoistusmenettelyiden avulla varmistetaan järjestelmän kokonais-turvallisuuden ja laatuvaatimusten toteutumisesta. Samalla kelpoistusraportit, tarkastus-pöytäkirjat sekä muu vaadittava dokumentaatio hoituu asianmukaisesti. Yksi esimerkki elinkaarimallista (kuva 2) löytyy tämän tutkimuksen sivulta 8.

Automaatiojärjestelmän elinkaareen kuuluvat esimerkiksi järjestelmän suunnittelu, käyttöönotto ja käytöstä poisto, jotka kaikki tulee suorittaa tietoturvallisesti. Näitä asioita käsitellään vain CPNI:n kehysmallissa. Kun elinkaaren eri vaiheissa noudatetaan tietoturvallisia toimintatapoja, varmistetaan siitä, että mahdollisten tietoturvatapahtumien negatiiviset seuraamukset pystytään minimoimaan.

Automaatio on aina monitoimijaympäristö, mikä luo omat haasteensa automaation tietoturvan hallintaan. Tämä tulee huomioida myös automaation elinkaaren hallinnassa, sillä automaatiohankintoihin liittyy usein ulkoisia toimijoita eli kolmansia osapuolia. Kolmannet osapuolet tulee kartoittaa ja niihin liittyviä riskejä hallita. Kolmannet osapuolet ja niihin liittyvät riskit on huomioitu kaikissa kolmessa käsitellyssä teoksessa, SFS:n mallissa hieman suppeasti ja NIST:n sekä CPNI:n teoksissa hyvinkin laajasti. Missään näistä kolmesta teoksesta kolmansia osapuolia ei ole sitoutettu automaation elinkaareen vaan asiat on ripoteltu malleihin erinäisin tavoin.

Kolmannet osapuolet tuovat mukanaan myös sopimusteknisiä asioita, jotka tulee huomioida hankintoja tehdessä. SFS:n mallissa sopimusteknisiin asioihin ei paneuduta lainkaan, NIST:n kehysmallissa vain sivutaan asiaa ja CPNI:n kehysmallissa asiaan paneudutaan huolellisimmin. Joka tapauksessa tietoturvan hallinnan varmistamiseksi on tärkeää huolehtia siitä, että automaation tietoturva-vaatimukset on sisällytetty hankintasopimukseen. Tämäkin vaihe on helposti sulautettavissa elinkaarimallin vaatimusten määrittely- sekä sopimusvaiheisiin.

Järjestelmän elinkaareen kuuluu operatiivista toimintaa, jonka tulee tapahtua tietoturva huomioiden. CPNI:n kehysmallissa operatiivinen turvallisuus on huomioitu omana kokonaisuutenaan, kahdessa muussa teoksessa operatiivisen turvallisuuden varmistamiseen on

annettu toimintamalleja välillisesti. Operatiivisella turvallisuudella pyritään varmistamaan siitä, että automaation tietoturvaan liittyvät operatiiviset asiat on sulautettu liiketoiminnan prosesseihin. Operatiivisen turvallisuuden toteutumista tulee valvoa säännöllisesti koko järjestelmän elinkaaren ajan.

Myös automaatiojärjestelmän elinkaareen liittyviä toimintamalleja tulee valvoa ja kehittää. Tämän perusteella voidaan päätellä, että perustamisvaiheessa kehitettävien valvontamenettelyjen tulee kattaa koko hallintajärjestelmä. Lisäksi myös valvontamenettelyjä täytyy valvoa ja kehittää, jotta niillä pystytään seuraamaan ja kehittämään järjestelmän tilaa luotettavasti.

4. HALLINTAJÄRJESTELMÄSSÄ HYÖDYNNETTÄVÄT TAKON TOIMINTAMALLIT

Turvallisuutta arvostetaan Metsä Group -konsernissa paljon, ja siihen on panostettu jo pidemmän aikaa. Nyt myös tietoturva on noussut turvallisuusajattelun rinnalle, ja erityisesti IT-puolella siihen on jo satsattu merkittävästi.

Metsä Group -konsernilla on olemassa politiikkoja, periaatteita ja ohjeistuksia automaation tietoturva-asioista sekä muuta mahdollisesti hyödynnettävissä olevaa dokumentaatiota liittyen turvallisuuteen, jatkuvuudenhallintaan, riskinhallintaan sekä IT-puolen tietoturvaan. Osa dokumenteista on toteutettu konsernitasolla ja osa on toimialakohtaista.

Tässä kappaleessa kootaan yhteen Takolla käytettävissä olevat toimintamallit ja muu dokumentaatio ja hyödynnetään niitä automaation tietoturvan nykytilan kartoituksessa. Lisäksi pohditaan, miten olemassa olevia toimintamalleja voidaan hyödyntää automaation tietoturvan hallinnassa, ja millaisia puutteita mahdollisesti jää.

4.1 Yritysturvallisuuspolitiikka

Yritysturvallisuus tarkoittaa yrityksen turvallisuusasioiden kokonaishallintaa. Yritysturvallisuudella tuetaan Metsä Groupin liiketoiminnallisia tavoitteita ja se on kiinteä osa organisaation toimintaa. Yritysturvallisuuden keskeinen päämäärä on huolehtia toiminnan häiriöttömästä jatkuvuudesta, ja lisäksi sillä suojataan henkilöstöä, muita sidosryhmiä, palveluja, tietoja, omaisuutta, toimintaympäristöä sekä konsernin mainetta vahingoilta, väärinkäytöltä ja rikolliselta toiminnalta. [44]

Metsä Groupin yritysturvallisuuspolitiikkaa sovelletaan kaikissa konsernin toimintayksiköissä eri puolilla maailmaa. Toimitusjohtajien on huomioitava paikallisen lainsäädännön mahdolliset vaikutukset periaatteita sovellettaessa. [44]

Yritysturvallisuuspolitiikkaa ohjaillaan yhdeksällä määräyksellä, jotka koskevat muun muassa lainsäädäntöön ja viranomaismääräyksiin liittyvien turvallisuusvelvollisuuksien noudattamista, turvallisuusriskien arviointia ja torjuntaa, turvallisuussuunnittelua, työtapoja, liikesalaisuuksia sekä toimi- ja tuotantotilojen suojausta. [44]

4.2 Liiketoiminnan jatkuvuudenhallinta

Liiketoiminnan jatkuvuudenhallinta on osa yrityksen keskeytysriskienhallintaa ja sen tehtävänä on luoda, kehittää sekä ylläpitää organisaation osaamista, sopeutumiskykyä ja toimimiskykyä. Näillä varmistetaan, että kriittisten tavoitteiden saavuttamiseksi vaadittavat prosessit ja resurssit ovat saatavilla jatkuvasti, myös häiriötilanteissa ja niiden jälkeen.

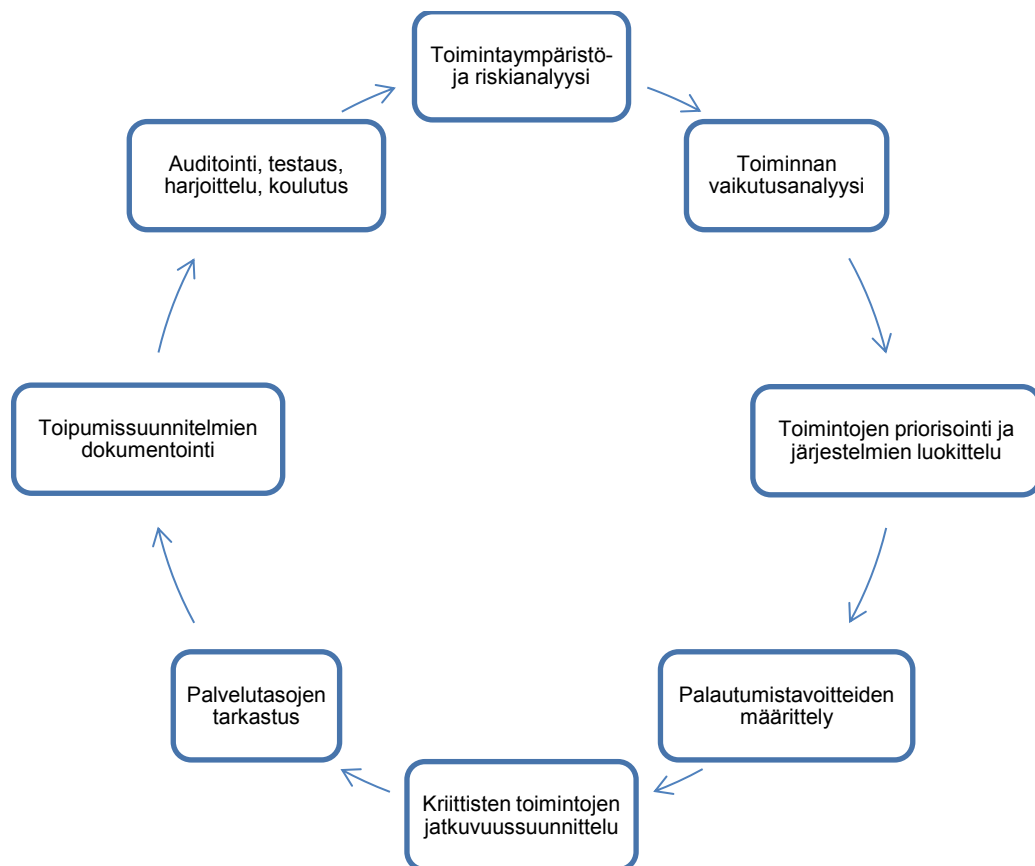
Jatkuvuudenhallinnan tulee olla dynaaminen prosessi, joka elää järjestelmän muutosten mukana. Se sisältää koulutuksia, harjoittelua, päivityksiä, muutosten hallintaa sekä toiminnan kehittämistä. Metsä Groupin intranetistä löytyy tietoa jatkuvuuden hallinnasta sekä dokumenttipohjia muun muassa jatkuvuudenhallintastrategialle, liiketoiminnan vaikutusanalyysille, jatkuvuussuunnitelmalle ja tekniselle toivutussuunnitelmalle. Seuraavat kappaleet käsittelevät dokumentteja yksityiskohtaisemmin.

4.2.1 Yleistä jatkuvuudenhallinnasta

Jatkuvuudenhallinta ja sen kehittäminen ovat kulloisenkin järjestelmän tai kohteen omistajan vastuulla. Oleellista on, että vastuuhenkilöllä on vastuutaan vastaavat valtuudet. Jatkuvuudenhallinnan dokumentissa mainitaan myös yhtälö

$$\text{ylemmän johdon sitoutuminen} = \text{omistajuus} + \text{raha} + \text{prioriteetti} + \text{resurssit}. \quad (1)$$

Jatkuvuudenhallintaan liittyvät muun muassa jatkuvuudenhallintastrategia, jatkuvuussuunnitelma, riskianalyysi, liiketoiminnan jatkuvuusanalyysi ja toipumissuunnittelu. Näistä kaikista löytyy dokumentaatiota sekä dokumenttipohjia, joita voidaan suoraan hyödyntää automaation tietoturvan hallinnassa. Kuvasta 16 nähdään jatkuvuudenhallinnan elinkaari. [15]



Kuva 16: Jatkuvuudenhallinnan elinkaari [muokattu lähteestä 15].

Jatkuvuussuunnittelu on jatkuva prosessi, mutta se tulee aloittaa projektiluontoisesti määrittelemällä vastuut, resurssit, prioriteetit, tavoitteet, vaatimukset, aikataulut sekä budjetti. Jatkuvuussuunnitelman kehittäminen ja käyttöönotto ovat kulloisenkin kohteen vastuuhenkilön tehtäviä. Huomionarvoista on, että vastuuta ei voi ulkoistaa. Jatkuvuussuunnitelmat ja niihin liittyvät muut suunnitelmat tulee tehdä kohteen suunnittelu- ja/tai käyttöönottovaiheessa eikä vasta silloin, kun järjestelmä on jo ns. tuotannossa. [15]

Jatkuvuudenhallintaan liittyviä asioita, joita tulisi pohtia ennen hallintaprosessin aloittamista:

- järjestelmän tai kohteen ja siten jatkuvuussuunnitelman omistaja
- jatkuvuussuunnitteluun osallistuvat tahot ja resurssit
- roolit ja vastuut koko elinkaaren loppuun saakka
- vaatimukset
- tavoitteet
- laajuus ja rajaukset
- prioriteetti
- budjetti
- aikataulu.

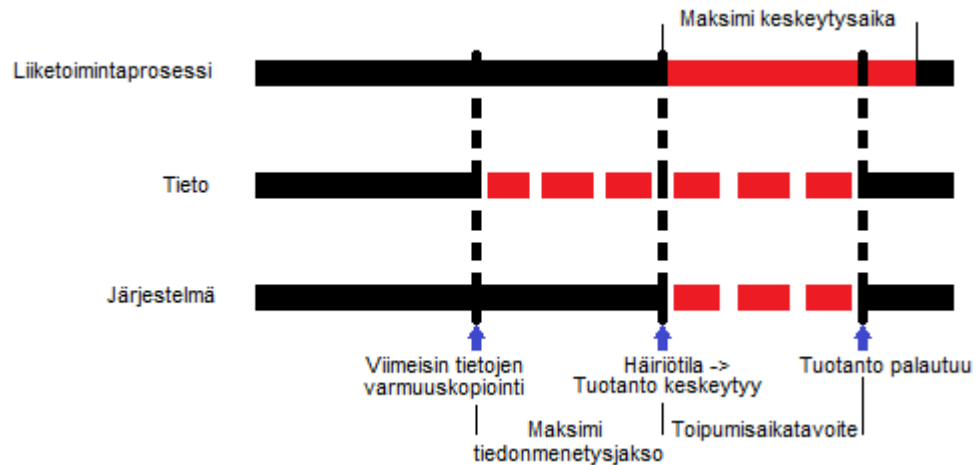
Näillä tiedoilla alustetaan jatkuvuudenhallinnan suunnitteluprosessia. [15]

4.2.2 Jatkuvuudenhallintastrategia

Metsä Groupin jatkuvuudenhallintastrategia -dokumenttipohjaa täytetään osajärjestelmä kohtaisesti. Sen tarkoituksena on luoda puitteet liiketoiminnan jatkuvuuden suunnitteluun ja hallintaan. Lisäksi sen avulla voidaan määrittää tekniset toipumistoimenpiteet esimerkiksi laitteistovikoja, inhimillisiä virheitä, luonnonkatastrofeja sekä tietomurtoja varten. [8]

Dokumentissa määritellään jatkuvuusstrategiaan liittyvät roolit ja vastuut organisaatiossa, käydään läpi liiketoiminnan vaatimuksia, sekä kuvataan itse jatkuvuudenhallintastrategia. Roolien ja vastuiden jako tulee tapahtua siten, että kaikilla järjestelmään liittyvillä osa-alueilla on omistaja, joka vastaa kohdealueensa jatkuvuudenhallinnasta. Järjestelmät pitää jakaa riittävän pieniin, tarkasti rajattuihin kokonaisuuksiin, jolloin vastuualueiden jatkuvuudenhallinta on selkeää. [8]

Liiketoiminnan vaatimukset -kohdassa kuvataan osajärjestelmää koskevat liiketoimintavaatimukset, kuten esimerkiksi jatkuvuus- ja toivutusvaatimukset. [8] Toivutusvaatimukseen liittyvää terminologiaa on esitetty kuvassa 17.



Kuva 17. Toivutusvaatimusten aikajana [muokattu lähteestä 8].

Toivutusvaatimusten aikajana selventää häiriötilan vaikutuksia liiketoimintaprosessiin, kyseisen prosessin tieto-omaisuuteen sekä tuotantojärjestelmään ajan suhteen. Maksimi keskeytysaika kuvaa ajanjaksoa, jonka sisällä tuotanto on saatava palautumaan, jotta häiriöstä ei aiheudu pysyviä haittoja liiketoiminnalle. Maksimi tiedonmenetysjakso määrittää, kuinka usein tietoa tulee varmuuskopioida, jotta tuotanto pystytään palauttamaan maksimi keskeytysajan puitteissa. Toipumisaikataavoite on aika, jonka kuluessa tuotanto saadaan palautettua ainakin osittain, siten että se täyttää ennalta määritetyn palvelutasotavoitteen. [8]

4.2.3 Liiketoiminnan vaikutusanalyysi

Liiketoiminnan vaikutusanalyysin tarkoituksena on määrittää liiketoiminnan kannalta kriittiset osa-alueet ja niihin liittyvät kriittiset resurssit. Tämä prosessi koostuu seuraavista toimenpiteistä:

- tunnistetaan kaikki liiketoiminnot
- tunnistetaan kaikki liiketoimintoja tukevat prosessit
- määritetään prosessien kriittisyydet liiketoimintaprosessissa
- määritetään prosessien kriittisyydet liiketoiminnalle
- arvioidaan liiketoimintavaikutukset ja toipumisaikataulut
- luokitellaan kriittiset prosessit.

Liiketoiminnan vaikutusanalyysi selvittää:

- tuotannon menetyksestä seuraavat taloudelliset tappiot
- katkojen aiheuttamat ei-taloudelliset seuraamukset
- yritystoiminnan kannalta kriittiset resurssit ja toiminnot
- tietojärjestelmien ja sovellusten tiedot ja priorisointi
- tiedon menetysten ja liiketoimintakatkojen vaikutukset
- yhteydet muihin liiketoimintaprosesseihin
- ulkoiset liittynät liiketoimintakumppaneihin.

Yllä listattujen tietojen perusteella voidaan arvioida liiketoiminnan kannalta kriittisiä osalualueita ja priorisoida toimintoja niihin liittyen. [10]

4.2.4 Jatkuvuussuunnitelma

Jatkuvuudenhallintasuunnitelma on tarkoitettu kriisitilanteessa järjestelmän jatkuvuus- ja toivutustoimenpiteistä vastaavien henkilöiden käytettäväksi. Sen tarkoituksena on ohjeistaa toimintaa häiriötilanteissa siten, että tuotantoa pystytään jatkamaan mahdollisimman pienin tappioin. [9]

Jatkuvuudenhallintasuunnitelmaan määritellään järjestelmän jatkuvuudenhallinnasta ja toivutuksesta vastaavat henkilöt ja organisaatiot. Lisäksi näiden vastuut eritellään kyseisessä dokumentissa. Toisin sanoen tähän dokumenttiin kirjataan kriisitilannetoiminnasta vastaava kriisiryhmä sekä toivutusryhmät, jotka vastaavat omien vastualueidensa toivutussuunnitelmien ylläpidosta ja toteuttamisesta. [9]

Jatkuvuudenhallintasuunnitelmassa käydään läpi, miten tulee toimia kriisitilanteessa. Aluksi sovitaan kriisiryhmän kokoon kutsumisen käytännöistä. Tämän jälkeen arvioidaan, miten vakavasta kriisistä on kyse, kuinka laajalle se on päässyt leviämään, ja mitä toivutustoimenpiteitä mahdollisesti vaaditaan, että tilanteesta päästään yli. [9]

Dokumentissa ohjeistetaan, mistä toivutuksessa tarvittava dokumentaatio löytyy, ja miten siihen pääsee käsiksi. Kriisiryhmän tehtävä on hankkia tarvittava dokumentaatio käytettäväksi toivuttamista varten. [9]

Seuraavaksi kriisiryhmä arvioi toivutusaikataulua. Tässä voidaan hyödyntää myös erillisissä toipumissuunnitelmissa tehtyjä aikamäärittelyitä. Jatkuvuudenhallintastrategiassa on määritetty pisin sallittu keskeytysaika sekä toipumisaikatavoite, joiden puitteissa tuotanto tulisi saada ajettua ylös. Mikäli toivutusaikatauluarvio ylittää toipumisaikatavoitteen, tulee kriisiryhmän informoida kyseisestä järjestelmästä vastaavaa johtoryhmää asiasta. [9]

Henkilöstön osalta tulee tunnistaa kriisin vaikutukset henkilöstöön. Resursoinnit tulee suorittaa etukäteen, ja lisäksi tulee pohtia, mistä mahdollinen lisähenkilöstö saadaan tarpeen vaatiessa. Henkilöstöä tulee informoida tilanteesta sisäisen viestintäsuunnitelman mukaan. Myös asiakasviestinnästä ja ulkoisesta viestinnästä tulee huolehtia. [9]

Tilojen käyttöä sekä verkon, järjestelmien ja laitteiden toimintaa tulee hallita suunnitelmien mukaisesti. Ensisijaisille tiloille tulee olla varalla toissijaiset tilat, jotka otetaan käyttöön tarvittaessa. Laitteistolle, järjestelmille ja verkoille, jotka pitävät sisällään muun muassa palvelimet, työasemat ja puhelimet sekä tietoliikenneyhteydet, on tehty hallintasuunnitelmat kyseiseen dokumenttiin. Mikäli kriisitilanne laajenee siten, että sen pelätään vaikuttavan muihinkin järjestelmiin tai niiden osiin, tulee kyseiset järjestelmät ajaa hallitusti alas. [9]

Tuotanto voidaan palauttaa osittain väliaikaistoimenpiteiden avulla, jolloin kyse on poikkeustilasta. Poikkeustilassa tuotanto voi tapahtua normaalia pienemmässä laajuudessa, kunnes koko järjestelmä on saatu palautettua normaalitilaan. Kun normaalitila saavutetaan, kriisiryhmän toiminta voidaan lopettaa. Kriisiryhmän johtajan tehtäväksi jää tilanteen jälkiraportointi johtoryhmälle. Jälkiraportoinnille löytyy ohjeistus jatkuvuudenhallintasuunnitelman liitteistä. [9]

4.2.5 Tekninen toivutussuunnitelma

Teknisessä toivutussuunnitelmassa määritellään kohteen toivuttamisen kannalta merkitykselliset asiat. Toivutussuunnitelma tulee koota sillä ajatuksella, että sen avulla toivuttamisen pystyy tekemään sellainen henkilö, jolle järjestelmä ja sen osat eivät välttämättä ole täysin tuttuja. [12]

Alkuun määritetään toivutusaika, eli kuinka kauan kestää saada järjestelmän tarjoamat palvelut uudelleen käyttöön, jos järjestelmä joudutaan kokoamaan alusta alkaen uudelleen sillä edellytyksellä, että järjestelmän toimintaan vaadittava infrastruktuuri on olemassa. Oleellista on myös erilaisten skenaarioiden kuvaaminen ja niiden toivutusaikatauluarvioiden pohtiminen. [12]

Kohteen, eli toivutettavan järjestelmän, yleistiedoissa esitetään kohteeseen liittyvät erityispiirteet sekä järjestelmän tai sen osien prioriteetit. Näillä saattaa olla vaikutusta toivutuksen toteutukseen. Tässä kohdassa käydään läpi kohteen vastuuhenkilöt, mitä tietoturvavaatimuksia kohteella on, sekä mitä tietoa järjestelmä pitää sisällään. Lisäksi kuvataan, mihin ylemmän tason toivutusalue suunnitelmaan kohde on sidoksissa. [12]

Yleistiedoissa myös listataan infrastruktuuri, joka vaaditaan järjestelmän toivuttamiseksi. Tämä käsittää esimerkiksi tietoliikenneverkot tai -laitteet, palvelimet, sovellukset, työasemat, sähköverkot. Lisäksi käydään läpi vaadittavat kohteeseen liittyvät ulkoiset palvelut ja liitännäisjärjestelmät. [12]

Toivutussuunnitelmaan kuvataan laitteiston nykytila sisältäen vähintään seuraavat kohdat:

- laitteisto
- käyttöjärjestelmä
- tietoliikenne
- varmistukset
- järjestelmän valvonta
- varajärjestelyt
- varusohjelmisto
- sovellusohjelmisto
- lisenssit
- vastuut.

Nykytilaa tulee päivittää säännöllisesti ennalta määritetyin aikaväleihin sekä muutosten yhteydessä. Toivutussuunnitelmaan ei ole tarpeen kuvata nykytilaa yksityiskohtaisesti, jos dokumentointi löytyy jostain muusta lähteestä. Oleellista on, että toivutussuunnitelmaan kuvataan jokaisen listatun kohteen osalta, mistä tieto on saatavilla, ja mikäli dokumentointia ei ole, kuvataan se kyseisen kohteen osalta toivutussuunnitelmaan. Tässä kohtaa täytyy huomioida myös se, miten tiedot löytyvät, mikäli verkko on alhaalla, ja ohjeistaa toiminta myös yhteydettömän tilanteen varalle. [12]

Toivutussuunnitelmassa käydään läpi myös muun muassa, mitä muuta tuotannon toimintaan liittyvää ohjeistusta mahdollisesti tarvitaan, sekä mitä muita tahoja tuotannon palauttamiseksi tarvitaan. Lisäksi käydään läpi, mitä toimenpiteitä varajärjestelyihin siirtymisen vaatii, ja miten tästä tiedotetaan. Mikäli esimerkiksi jatkuvuussuunnitelmaan on tehty suunnitelma tiedottamisesta, riittää, että viitataan siihen. [12]

Kaikki nykytilakohdassa listatut kohteet käydään läpi ja kuvataan, miten niiden toivutus tapahtuu, mistä tarvittava laitteisto saadaan, missä sovellusmediat sijaitsevat ja mikä on asentajan rooli. Lisäksi kuvataan muun muassa palvelimen palautus, käyttöönotto ja testaus, sekä koko kohteen testaus toivuttamisen jälkeen. [12]

Muita huomionarvoisia toivutussuunnitelmaan listattavia asioita ovat, kuinka dokumentaatiota, käyttäjätunnuksia, ohjelmistoja ja lisenssitietoja hallitaan ja säilytetään. [12]

4.3 Riskienhallinta

Yritysten liiketoimintaan sisältyy aina riskejä ja epävarmuutta. Osa riskeistä ja uhkatekijöistä on yrityksen vaikutuspiirin ulkopuolella, mutta riskienhallinnalla nekin pyritään ottamaan huomioon ja niihin varautumaan. Osaan riskejä pystytään vaikuttamaan ja niitä tulee käydä läpi riskienhallintaohjeiden mukaisesti ja suorittaa niille mahdollisesti ilmenneen tarpeen mukaan korjaustoimenpiteitä riskien pienentämiseksi.

Metsä Groupissa pyritään systemaattiseen, ennakoivaan ja jatkuvaan toimintaan riskienhallinnassa. Riskienhallintatyöllä tuetaan sisäistä valvontaa, mikä vuorostaan tukee liiketoiminnan johtamista ja päätöksentekoa. [22]

Metsä Groupin riskienhallintaperiaate sisältää ohjeet, säännöt sekä määräykset, joita konsernissa sovelletaan globaalisti. Sen keskeinen tavoite on määrätä suuntaviivat konsernin riskienhallintatyölle. Riskienhallinnalla pyritään reagoimaan liiketoiminta- sekä riskiympäristön muutoksiin, arvioimaan konsernin toimintaan kohdistuvia uhkia sekä mahdollisuuksia ja näin edistämään liiketoiminnan tavoitteiden saavuttamista. [22]

Riskienhallintaperiaatteessa on eritelty riskiympäristön neljä eri riskikategoriaa:

- strategiset riskit
- operatiiviset riskit
- rahoitusriskit
- vahinkoriskit.

Näiden kategorioiden riskienhallintaan tulee soveltaa konsernin politiikkoja ja ohjeita. Konsernin sisäiset vastuut riskienhallinnasta on listattuna riskienhallintapolitiikkaan. Dokumentin päivittämisestä vastaa erillinen riskienhallintayksikkö. [22] Kuvasta 18 nähdään konsernin riskienhallintaprosessi.



Kuva 18. Riskienhallintaprosessi [muokattu lähteestä 22].

Riskien arviointiin Metsä Group käyttää 5 x 5 -riskimatriisia, jonka toisella akselilla on riskin todennäköisyys ja toisella riskin vaikutukset. Näitä arvioidaan skaalalla yhdestä viiteen taulukon 26 mukaisesti.

Taulukko 26. Riskien arviointi [muokattu lähteestä 22].

Skaala	Riskin todennäköisyys	Riskin vaikutus
1.	Harvinainen	Merkityksetön
2.	Epätodennäköinen	Lievästi haitallinen
3.	Kohtalaisen todennäköinen	Kohtalaisen haitallinen
4.	Todennäköinen	Hyvin haitallinen
5.	Erittäin todennäköinen	Erittäin haitallinen



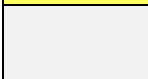

Riskin todennäköisyyden ja vaikutuksen perusteella voidaan sijoittaa riski riskimatriisiin (taulukko 27).

Taulukko 27. Riskimatriisi [muokattu lähteestä 22].

Erittäin todennäköinen	5								
Todennäköinen	4								
Kohtalaisen todennäköinen	3								
Epätodennäköinen	2								
Harvinainen	1								
		1	2	3	4	5			
		Merkityksetön	Lievästi haitallinen	Kohtalaisesti haitallinen	Hyvin haitallinen	Erittäin haitallinen			

Riskin arviointi ja riskiin suhtautuminen voidaan tehdä riskimatriisin värikoodien perusteella taulukon 28 mukaisesti.

Taulukko 28. Riskimatriisin värikoodien selitykset [muokattu lähteestä 22].

Vaikutus	Värialue	Riskin arviointi ja suhtautuminen riskiin
Merkittävä		Ei hyväksyttävissä oleva riski. Vaatii välittömiin korjaaviin toimenpiteisiin ryhtymistä
Suuri		Ei hyväksyttävissä oleva riski. Vaatii jatkuvia aktiivisia toimenpiteitä sekä valvontaa ja seurantaa.
Kohtalainen		Hyväksyttävä riski. Vaatii kuitenkin säännöllistä aktiivista valvontaa ja seurantaa sekä tarvittaessa toimenpiteitä
Pieni		Hyväksyttävä riski. Seuranta ja valvonta riittää.

Riskien arvioinnista ohjeistetaan, että riskiarvioiden päivityksistä tulee huolehtia säännöllisesti sekä lisäksi kontrolloida riskien arvioinnin perusteella vaadittujen toimenpiteiden toteutumista. Laitemuutokset velvoittavat myös uuden riskinarvion tekemiseen. Riskiarvioinnit sekä korjaavat toimenpide-ehdotukset dokumentoidaan ja käydään läpi asiansaisten kanssa. [22, 23]

4.4 Yleinen tietoturva

Metsä Groupilla on olemassa erilaisia toimintamalleja ja ohjeita yleisestä tietoturvallisuudesta. Tässä vaiheessa käsitellään vain viittä olennaisinta:

- tietoturvallisuuspolitiikka
- henkilöstön tietoturvaohje
- tietoturvan organisointi Metsä Group –konsernissa
- ohje tietoturvan auditointisuunnitelman tekoon
- tietoturvalisen elinkaarenhallinnan periaate.

Edellä mainittujen dokumenttien lisäksi Metsä Groupilta löytyy paljon lisäohjeistusta tietoturvanhallintaan.

4.4.1 Tietoturvallisuuspolitiikka

Metsä Groupin tietoturvallisuuspolitiikka velvoittaa kaikkia Metsä Groupin kuuluvia yhtiöitä sekä niiden henkilöstöä. Mikäli tarpeen, myös ulkopuoliset palveluntarjoajat ja muut sopimuskumppanit tulee velvoittaa noudattamaan tietoturvapolitiikan mukaisia tietoturvaperiaatteita ja määräyksiä. [43]

Tietoturvallisuudelle on asetettu neljä päätavoitetta, joista ensimmäisellä tavoitellaan tiedon saatavuudelle, eheydelle ja luotettavuudelle asetettujen vaatimusten täyttymistä koko tiedon elinkaaren ajalle. Toisena päätavoitteena on ennaltaehkäisy-, havainnointi- ja tor-

juntakyykyjen kehittäminen ja ylläpito, jotta voidaan välttyä liiketoimintaa ja tietoa uhkaavilta häiriöiltä dynaamisessa toimintaympäristössä. Kolmanneksi pyritään tekemään tietoturvallisuudesta ja tiedon suojaamisesta rutiininomaista toimintaa koko konsernin sisällä. Viimeisenä tavoitteena pyritään lisäämään henkilöstön tietoturvatietoisuutta. [43]

Dokumentissa määritellään yhdentoista kohdan politiikkamääräykset, joita tulee noudattaa ja joiden avulla organisaatio pyrkii saavuttamaan tietoturvan päätavoitteet. Lisäksi vastuut ja niiden jakovastuu on listattuna dokumenttiin. [43]

4.4.2 Henkilöstön tietoturvaohje

Tietoturvajärjestelyjen avulla pyritään varmistamaan, että tietoaineistojen, tietojärjestelmien ja palveluiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit huomioidaan ja niitä pienennetään. Tiedot, tietojärjestelmät ja verkot pidetään vain niiden henkilöiden saatavilla, jotka tarvitsevat niitä työtehtävissään. Sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja, joihin heillä ei ole oikeutta. Palvelujen on pystyttävä tunnistamaan ja todentamaan käyttäjät luotettavasti ja tuotettava kiistattomat lokitiedot. Ohje antaa tarkan toimintaohjeen käyttäjätunnusten ja salasanojen käytöstä. [7]

Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa joutua väärin käsiin, muuttua tai tuhoutua esimerkiksi haittaohjelmien tai laitevikojen vuoksi. Lisäksi niiden on oltava saatavilla silloin, kun niitä tarvitaan. [7]

Tietoturvaohjeessa annetaan ohjeet tietoaineistojen käsittelystä ja käsitellään kyberturvallisuutta lyhyesti yleisellä tasolla. Lisäksi annetaan ohjeet sähköpostitse tapahtuvien kohdistettujen hyökkäysten välttämiseksi, ja kuvataan, miten välttyä käyttäjän manipuloinnilta. Ohje opastaa myös päätelaitteiden (älypuhelinien ja kannettavien päätelaitteiden) tietoturvallista käyttöä. Lisäksi käsitellään myös sosiaalisen median ja pilvipalveluiden käyttöä. Kannettavat tallennusvälineet ovat suuri riski yritykselle, jos niitä ei ole suojattu. Muistitikun ja muiden ulkoisten muistivälineiden käsittelystä annetaan yksityiskohittaiset ohjeet. [7]

4.4.3 Tietoturvan organisointi Metsä Group -konsernissa

Dokumentin mukaan tietoturvallisuuteen liittyvät vastuut, roolit ja velvoitteet kuuluvat automaattisesti jokaisen työntekijän päivittäiseen työnkuvaan. Laadusta, tiedon suojaamisesta ja tietoturvallisuudesta on annettu periaatteet ja ohjeistus, joita jokaisen työntekijän tulee noudattaa. [14]

Organisaation tietojärjestelmille tai niiden osille, verkoille ja tiedolle määrätään omistaja, joka vastaa tietojen ja tietojärjestelmän lainmukaisesta suojaamisesta sekä asianmukai-

sesta ylläpidosta ja periaatteiden ja politiikkojen noudattamisesta. Vaikka tietojen käsittely tai tietojärjestelmien ylläpito tapahtuisi ulkoisen toimijan tekemänä, vastuu edellä mainituista asioista on silti organisaation sisältä määritellyllä henkilöllä. [14]

Tietoturvallisuuteen liittyvät vastuut Metsä Groupissa:

- tietoturvallisuuden kehittäminen ja riskienhallinta
- tietoturvavaatimusten määrittäminen, seuranta ja arviointi
- tietoturvallisuudesta raportointi
- tietoturvapoikkeamien ja niiden uhkien käsittely
- tietoturvayhteistyö (sisäinen ja ulkoinen)
- tietoturva-uhkien ennakoiminen ja uhkien seuraaminen
- tietoteknisten toipumis- ja jatkuvuussuunnitelmien laatiminen, päivitys ja katselmointi
- tietoturvaan liittyvien laitteiden, rekistereiden ja tietojärjestelmien omistajuus
- tietoturvaan liittyvien laite-, tietojärjestelmä-, palvelu-, ja ohjelmistoluetteloiden ylläpito
- lain mukaisten selosteiden ja kuvausten päivitys
- tietoturvallisuuteen liittyvien periaatteiden ja ohjeiden ylläpito sekä kehitys
- laitteiden ja tietojärjestelmien päivitystarpeiden seuranta, päivityspäätösten teko ja päivitysten asennus
- laitteiden ja tietojärjestelmien muutostarpeiden seuranta, muutospäätösten teko ja muutosten toteutus
- tietoturvallisuus, turvallisuussopimukset ja kumppanienhallinta kumppanuus- ja hankintatoiminnassa
- tietoturvallisuuden tilan säännöllinen arviointi, auditoinnit ja jatkuva parantaminen
- tietoturvallisuuskoulutusten suunnittelu, järjestäminen ja tietoturvaosaamisen ylläpito
- tietoturvallisuuden vuosikellon määrittäminen ja ylläpito.

Tietoturvan organisoimisen tavoitteena on määrittää kaikelle vastuuhenkilöt, ja jakaa järjestelmien tietoturvaan liittyvät tehtävät yksiselitteisesti. [14]

4.4.4 Ohje tietoturvan auditointisuunnitelman tekoon

Metsä Group ohjeistaa tietoturva-auditointisuunnitelman tekoa. Suunnitelma on oltava tehtynä ennen auditointia ja se on hyväksyttävä ennen auditoinnin aloittamista. Auditointisuunnitelmasta tulee käydä ilmi vähintäänkin seuraavat asiat:

- Miksi auditointi tehdään, ja mikä on sen tavoite?
- Mitä auditoidaan ja mitä ei? (rajataan auditoinnin laajuus)

- Miten auditointi toteutetaan?
- Miten auditoinnin riskejä hallitaan?
- Milloin auditointi suoritetaan? (vaiheistettu aikataulu auditoinnista)
- Ketkä auditoinnin suorittavat, ja mitä muita rooleja auditointiin liittyy?

Auditoinnilla pyritään valvomaan tietoturvatavoitteiden täyttymistä ja kehittämään toimintaa. [11]

4.4.5 Tietoturvallisen elinkaarenhallinnan periaate

Tietoturvallisen elinkaarenhallinnan periaatteen tavoite on kuvata yleiset vaatimukset kohteen tietoturvalliselle asentamiselle, testaukselle, ylläpidolle ja poistamiselle. Periaate sisältää sovellusalan määrittelyn, roolien ja vastuiden jaot, suunnittelun ja toteutuksen, testauksen, muutostenhallinnan ja jatkuvan parantamisen, käytöstä poiston sekä poikkeuksien käsittelyn. Tietoturvallisen elinkaarenhallinnan periaatteesta on johdettu Tietoturvallisen elinkaarenhallinnan muistilista, jossa listataan Metsä Groupin valitsema tärkeimmät kohdat tietoturvallisen elinkaarenhallinnan saavuttamiseksi.

Lisäksi politiikkoja, periaatteita ja ohjeita löytyy myös muun muassa lokien hallinnasta, pääsynhallinnasta, tietoliikenteen suodatuksista, päätelaitteiden tietoturvasta jne. [13]

4.5 Automaation tietoturvaan ja laitehankintoihin liittyvä dokumentaatio

Metsä Groupilla on käytössä toimintaohje, joka koskee tietoturvaa ja IT-laitehankintoja prosessiautomaatiossa. Lisäksi on olemassa yleisohje automaatiotoimittajille. Näiden lisäksi automaatioverkkoon liitetyistä laitteista tulee täydentää lomakepohja, josta käy ilmi kaikki oleellinen laitteen liittämiseksi tehdasverkkoon tietoturvallisesti.

4.5.1 Tietoturva ja IT-laitehankinnat prosessiautomaatiossa

Tietoturva otetaan huomioon jo hankintavaiheessa. Metsä Groupin tietoturvaohje, joka on aina ostosopimuksen liitteenä, annetaan toimittajalle sovellettavaksi jo ostovaiheessa. Paikallinen IT Service Manager tai IT-lähituki arvioi verkkoon liitettävät laitteet muun muassa tietoturvan, yhteensopivuuden ja elinkaarihallinnan suhteen, antaen suosituksen tietoturvasta ja laite- ja lisenssihankinnoista. Automaatiojärjestelmästä vastaava henkilö neuvottelee puolestaan toimittajan kanssa sovellettavan menetelmän. [42]

Tässä yhteydessä tietoturva tarkoittaa muun muassa laitteen liittämistä verkkoon, IP-osoitteita, palomuuriauvauksia, virustorjuntaa, Security Patchseja, varmuuskopiointia, varalaitteita, tukea jatkossa sekä elinkaaren hallintaa ja toipumissuunnitelmaa. [42]

Asennuksen ja käyttöönoton yhteydessä automaatiotoimittaja sekä tehtaan automaatiojärjestelmästä ja IT-järjestelmästä vastaavat tahot toteavat, että laitteisto, sovellus ja tietoturva toimivat halutulla tavalla. Sen lisäksi IT-puoli lisää asennetut laitteet työasemaluetteloon. [42]

Laitteen tietoturvan ylläpito jakautuu sen mukaan, onko kyseessä toimittajan huoltosopimukseen liittyvä järjestelmä vai IT-puolen vastuulla oleva järjestelmä. Ensiksi mainittujen kohdalla käytetään tietoturvan tilanteeseen, muutoksiin ja ongelmiin keskittyviä raportointeja ja seurantapalavereita, ja automaatiopuoli tiedottaa poikkeamista IT-puolelle. IT-puolen vastuulla olevien järjestelmien kohdalla viruskannat päivitetään automaattisesti, ja Security Patchit, varmuuskopiot, versiopäivitykset jne., suunnitellaan ja toteutetaan yhdessä automaatiopuolen ja toimittajan kanssa. [42]

Tietoturvaprosessin ylläpidosta vastaa prosessiautomaation kohdalla tehtaan automaatiopäällikkö. IT-puoli pitää yllä listaa kaikista LAN-verkkoon liitetyistä prosessiautomaation laitteista, ja listaa käydään läpi yhdessä automaatiopuolen yhdyshenkilön kanssa. IT-puoli raportoi luettelon tilanteesta automaatiopäällikölle säännöllisesti tai tarpeen mukaan. Automaatioluettelot käydään läpi myös IT-puolen seurantapalavereissa. [42]

4.5.2 Tietoturvaohje automaatiotoimittajille

Metsä Groupin automaatiotoimittajille tarkoitettussa tietoturvaohjeessa annetaan yleisluonteisia ohjeita koskien automaatiotoimituksia. Niissä määritetään vaatimukset, joita toimittajan tulee noudattaa Metsä Groupin IT-ympäristössä. Yksityiskohtaisempia ohjeita löytyy tarvittaessa Metsä Groupin intranetistä. Ohjeessa kuvataan myös Metsä Groupin tavanomainen verkkorakenne, jonka mukaan tehdasverkko tulisi rakentaa. [4]

Ohjeessa vaaditaan seuraavien toimenpiteiden noudattamista:

- Tuotantolaitoksen IT-palveluista vastaavaa tahoa tulee informoida kaikista muutoksista automaatioverkossa.
- Metsä Group vastaa tavanomaisten laitteiden sekä yleisesti käytettävien ohjelmistojen hankinnoista. Automaatiotoimittajan vastuulle jäävät erikoislaitteiden ja –ohjelmistojen hankinnat.
- Verkon segmentoinnista tulee huolehtia ohjeen mukaisella tavalla.
- Metsä Group vastaa palomuurien hankinnasta ja konfiguroinnista. Automaatioverkko tulee erottaa aina toimistoverkosta palomuurilla. Kaikki yhteyksien avaukset on neuvoteltava IT-palveluista vastaavan tahon kanssa.
- Automaatiotoimittajan täytyy suunnitella ja testata toimittamansa järjestelmä siten, että yleisten suojausohjelmistojen asennus ja päivitys ovat mahdollisia. Metsä Group päättää kumpi osapuoli suorittaa virusohjelman asennuksen ja päivityksen.
- Toimitetut järjestelmät ja sovellusalustat tulee testata ja koventaa turvallisiksi ennen toimitusta.

- Automaation ohjelmistoille on asetettu erityisvaatimuksia. Ensinnäkin automaation ohjelmistomuutokset eivät saa uhata tuotantoa. Toiseksi, lokikirjaustoimintojen tulee olla käytössä automaatiojärjestelmissä mukaan lukien toimittajien palomuurit. Lokitietoja tulee säilyttää asianmukaisesti.
- Kaikki versiopäivitykset tulee suunnitella ja toteuttaa käyttäen virallista muutosten hallintaprosessia, joka tulee hyväksyttävä kaikilla osapuolilla. Muutokset on testattava tarkasti ennen uuden version käyttöönottoa tuotannossa. Päivityksen epäonnistumiseen tulee varautua asianmukaisella varasuunnitelmalla. Tuotantolaitoksen muutoksista vastaavan tahon tulee puolestaan hyväksyä muutokset, jotta mahdolliset ongelmat tuotannossa pystytään ehkäisemään.
- Toimittajan täytyy käyttää yleisesti käytettyjä käyttöjärjestelmiä ja toimittajan täytyy suunnitella ja testata järjestelmät siten, että korjaustiedostot voidaan asentaa järjestelmään. Toimittajan tulee ilmoittaa korjaustiedoston julkaisemisesta, ja voiko korjaustiedoston asentaa järjestelmään. Korjaustiedoston voi asentaa toimittaja, tuotantolaitoksen oma henkilökunta tai kolmas osapuoli. Jos korjaustiedostoa ei voi asentaa, niin toimittajan on tarjottava vaihtoehtoja suojausratkaisua.
- Kaikki käyttäjätunnukset ja salasanat tulee määrittellä standardeissa esitettyjen suositusten mukaisesti. Toimitetuissa järjestelmissä käytettyjen käyttäjätunnusten ja salasanojen tulee noudattaa Metsä Groupin tietoturvapoliittikkaa. Metsä Groupilla on verkkoon kytkettyjen laitteiden nimeämistä varten menettelytapa, jota on ehdottomasti noudatettava.
- Liiketoimintaprosessin aikakriittisyys määrittää, kuinka usein varmuuskopioita tulee ottaa. Varasuunnitelmat on testattava säännöllisesti ja testaustulokset on dokumentoitava.
- Palvelinten virtualisointiin tulisi käyttää mahdollisuuksien mukaan Metsä Groupin olemassa olevia virtualisointiratkaisuja.
- Kaikesta tekemisestä tulee tuottaa asianmukainen dokumentaatio.
- Internetyhteydet sekä kolmansien osapuolien yhteydet tulee hyväksyttävä ja toteuttaa Metsä Groupin tietoturvapoliittikkaa noudattaen
- Järjestelmän valvonnasta, valvontatyökalujen asennuksista ja päivityksistä tulee huolehtia ja sopia tarkasti.
- Liiketoiminnan jatkuvuudesta tulee varmistua jatkuvuus- ja toipumissuunnitelmien avulla.

Tätä tietoturvaohjetta tulee noudattaa kaikissa automaatio- ja IT-projekteissa ja -asennuksissa, joissa Metsä Groupin verkkoon liitetään mitä tahansa laitteita. [4]

4.6 Yhteenveto toimintamalleista

Takolla on käytettävissä kattavasti toimintamalleja, ohjeita ja dokumenttipohjia, joita voidaan hyödyntää prosessiautomaation tietoturvan hallintajärjestelmän kehitystyössä sekä

itse hallintajärjestelmässä. Tähän tutkimukseen koottiin materiaalia liittyen yritysturvallisuuteen, jatkuvuuden hallintaan, riskien hallintaan, tietoturvaan ja automaation tietoturvaan.

Yritysturvallisuuspolitiikkaa voidaan käyttää yhtenä perusteena hallintajärjestelmän tarpeellisuudelle sekä siitä saadaan raamit turvallisuustyölle. Liiketoiminnan jatkuvuudenhallintaa käsitellään laajasti ja siihen annetaan hyvät työkalut konsernitasolta. Liiketoiminnan jatkuvuudenhallinta on todella tärkeä osa automaation tietoturvaa ja annettuja toimintamalleja ja ohjeita voidaan hyödyntää prosessiautomaation tietoturvan hallintajärjestelmän kehitystyössä.

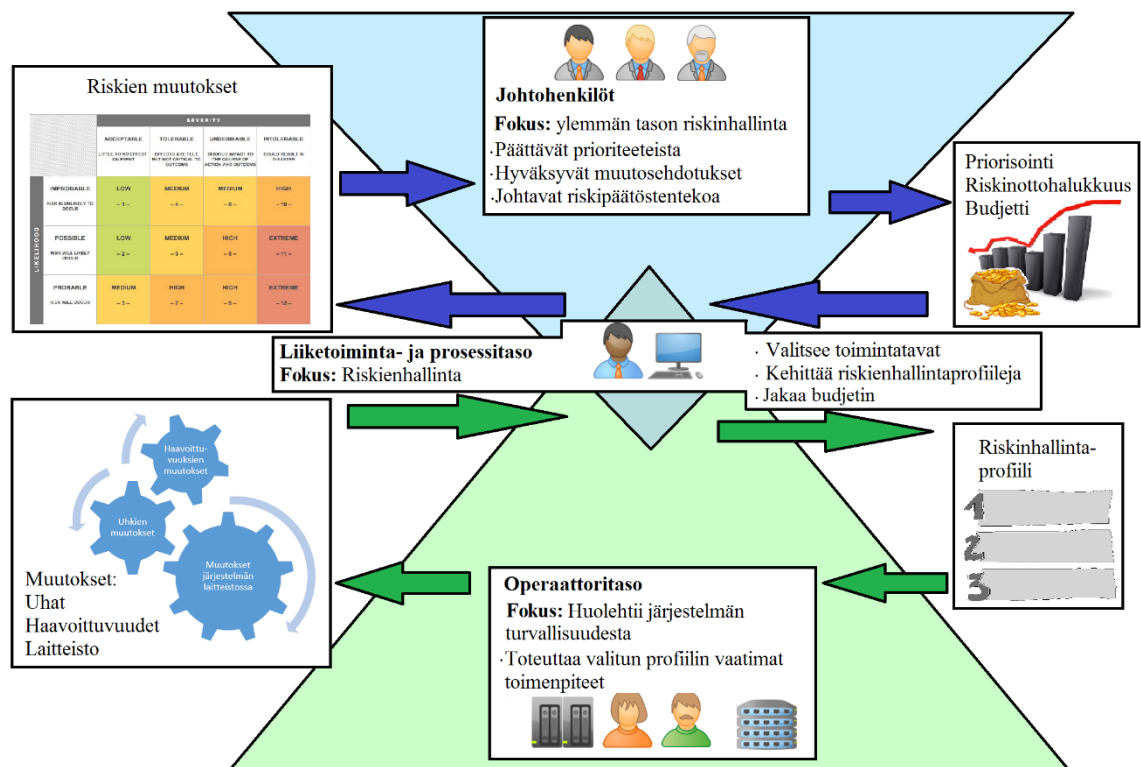
Yleistä tietoturvaa varten on olemassa politiikkoja, ohjeita ja toimintamalleja. Nämä täytyy ottaa huomioon prosessiautomaation tietoturvan hallintajärjestelmää kehitettäessä, ja osaa niistä voidaan sellaisenaan hyödyntää automaation tietoturvan hallinnassa. Esimerkiksi tietoturvan organisointi sekä auditointisuunnitelmien teko ovat erittäin tärkeitä vaiheita automaation tietoturvan hallinnassa ja nämä toimintaohjeet löytyvät jo konsernitasolta valmiina. IT-puolen ohjeistusta hyödynnettäessä tulee huomioida IT:n ja automaation eroavaisuudet.

Prosessiautomaation tietoturvalle ja IT-laitehankinnoille on olemassa valmis ohjeistus samoin kuin toimintaohje automaatiotoimituksia varten. Näitä voidaan sellaisenaan hyödyntää prosessiautomaation tietoturvan hallintajärjestelmässä.

5. PROSESSIAUTOMAATION TIIETOTURVAN HALLINTAJÄRJESTELMÄ

On tärkeää ymmärtää, että organisaatio ei voi ostaa kokonaisvaltaista tietoturvaa muualta vaan sen täytyy huolehtia ja vastata siitä itse. Automaatiojärjestelmän tietoturva on monisäikeinen ja laaja kokonaisuus, että ulkopuolisen on mahdotonta huomioida jokainen tietoturvaan liittyvä nyanssi, ottaa vastuu automaation tietoturvasta ja sitä kautta koko yrityksen toiminnan jatkuvuudesta. Siksi lopullinen vastuu automaation tietoturvasta on yrityksellä itsellään. Automaation tietoturvalle oleellista on ennaltaehkäistä ja ennakoita uhkia ja reagoida niihin, ja jos vahinko pääsee tapahtumaan, tulee virheistä ottaa opiksi.

Kuvassa 19 esitetään toimintakaavio tietoturvan hallinnasta. Kuvasta ilmenee, kuinka muutokset aikaansaavat päätöstentekoa muun muassa priorisoinnin, rahoituksen ja riskien suhteen. Muutosten seurauksena valitaan ja otetaan käyttöön uudet toimintatavat ja vastatoimenpiteet. Kuvan mallissa kaikki henkilöstöryhmät ovat sitoutettu tietoturvan hallintajärjestelmään ja prosessi on dynaaminen ja itseään toistava.



Kuva 19. Hallintajärjestelmän malli [muokattu lähteestä 4, s. 13].

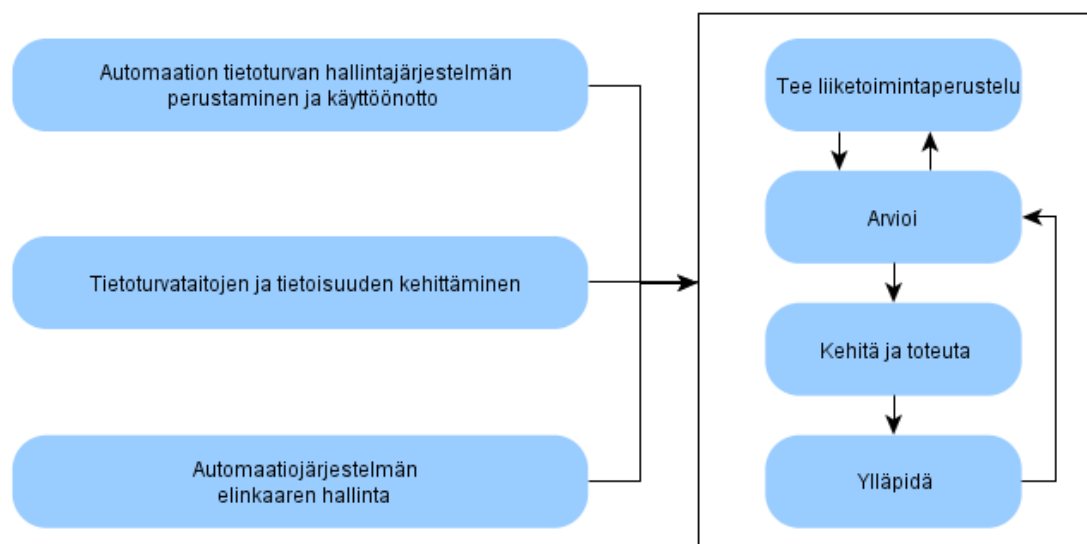
Johtohenkilöstö huolehtii ylemmän tason riskien hallinnasta, priorisoinnista ja muutosten hyväksynnästä sekä johtaa riskipäätöstentekoa. He myös määrittävät budjetin kaikelle toiminnalle.

Liiketoiminta- ja prosessitason henkilöstö valitsee toimintatavat, kehittää riskinhallinta-profiileja vastaamaan johtohenkilöstön ohjeistusta ja jakaa budjetin parhaaksi katsomallaan tavalla. Liiketoiminta- ja prosessitason henkilöstön päätehtävänä on hallita riskejä, informoida johtohenkilöstöä merkittävistä riskimuutoksista sekä päivittää riskinhallinta-profiileja, joiden mukaan operaattoritaso toteuttaa suojauksen toteutuksen ja ylläpitää järjestelmän turvallisuutta.

Operaattoritaso tarkkailee automaatiojärjestelmää ja erityisesti muutoksia, jotka koskevat esimerkiksi laitteistoa, uhkia tai haavoittuvuuksia. Kaikki muutokset informoidaan liiketoiminta- ja prosessitasolle, joka vastaavasti valitsee järjestelmän tilaan sopivan riskinhallintaprofiilin, jonka mukaan suojaus valitaan ja toteutetaan.

Edellä esitetyn mallin ideaa hyödyntäen, kappaleen kolme kirjallisuustutkimuksen teosten pohjalta, mutta myös muiden lähteiden tukemana, kootaan tähän kappaleeseen automaation tietoturvan hallintajärjestelmä ja asiat, jotka tulisi huomioida sen laatimisessa.

Tämän tutkimuksen pohjalta luodusta prosessiautomaation tietoturvan hallintajärjestelmästä muodostettiin mahdollisimman yksinkertainen ja helposti toteutettava kokonaisuus. Aiheen laajuus ja kompleksisuus aiheuttavat sen, että kokonaiskuvan hahmottaminen voi olla hankalaa ja tietoturvan toteutus ja siihen vaadittavien toimenpiteiden määrittäminen saattaa jäädä vajavaiseksi tai toisaalta aiheuttaa päällekkäisiä toimintoja. Tässä hallintajärjestelmässä on pyritty välttämään edellä mainitut ongelmat mahdollisuuksien mukaan. Tutkimuksen pohjalta luotu prosessiautomaation tietoturvan hallintajärjestelmä on kuvan 20 mukainen.



Kuva 20. Prosessiautomaation tietoturvan hallintajärjestelmä.

Järjestelmä koostuu kolmesta päävaiheesta, ja lisäksi jokaisen päävaiheen kohdalla toteutetaan kuvan oikeassa reunassa olevaa luuppia, joka toteuttaa samalla prosessiautomaation tietoturvan hallintajärjestelmän valvontamenettelyjä.

Automaation tietoturvan hallintajärjestelmän perustaminen ja käyttöönotto -vaiheen tarkoituksena on huolehtia siitä, että järjestelmä automaation tietoturvan hallintaa varten saadaan otettua asianmukaisesti käyttöön, sen ylläpidosta huolehditaan ja että sille saadaan varattua sen vaatimat resurssit. Hallintajärjestelmän perustamista ja käyttöönottoa käsiteltiin laajasti kirjallisuustutkimuksen teoksissa. Kirjallisuustutkimuksen sekä kokemuksen perusteella on ilmeistä, että hallintajärjestelmän perustamiseen ja käyttöönottovaiheeseen kannattaa paneutua, sillä hallintajärjestelmän perustaminen vaatii omat toimenpiteensä, ja ennen niiden toteuttamista on vaikeaa toteuttaa mitään muita automaation tietoturvan hallintaan liittyviä toimenpiteitä.

Tietoisuuden ja tietoturvataitojen kehittäminen -vaihe on järjestelmän kannalta erittäin tärkeä osio, sillä automaation tietoturvan hallinta muodostuu suurelta osin henkilöstön toimintatavoista. Yleisen tietoturvan osalta henkilöstön toimintaan on panostettu ja kiinnitetty huomiota todella paljon. Samaa panostusta ja tietoturvan jalkauttamista kaivataan myös automaatiopuolelle. Tämä käy ilmi analysoimalla tehtaan henkilöstön toimintaa, sekä myös suoraan kirjallisuustutkimuksesta. Henkilökunnan tietoturvatietoisuuden lisääminen sekä tietoturvataitojen kehittäminen ovatkin oleellisia asioita automaation tietoturvan hallinnassa.

Automaatiojärjestelmän elinkaaren hallinta valikoitui kolmanneksi osaksi prosessiautomaation tietoturvan hallintajärjestelmää, koska hallintajärjestelmän taustalla oli ajatus siitä, että automaation tietoturva integroitaisiin osaksi automaation elinkaarta. Tämän tutkimuksen sivulla 8 on esimerkki automaation elinkaarimallista (kuva 2), jota voidaan hyödyntää. Jos tietoturva saadaan sulautettua osaksi elinkaarimallia, tietoturvasta tulee luonnollinen osa automaatiota. Kirjallisuustutkimuksesta koottiin tärkeitä toimintoja, jotka voidaan sulauttaa elinkaareen, ja siten hallita automaatiojärjestelmän elinkaarta tietoturva huomioiden.

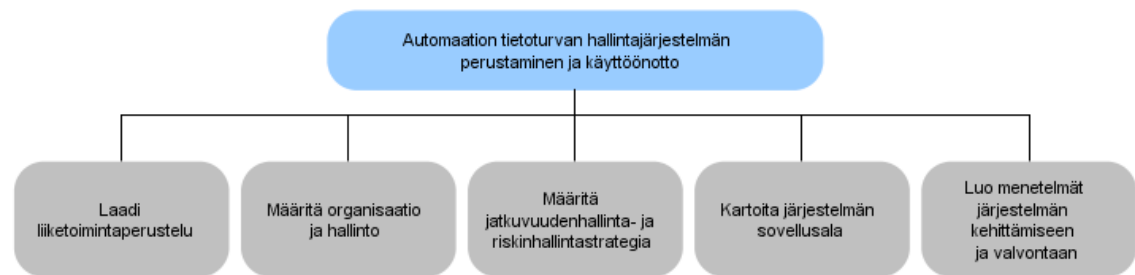
Kuvan vasemmanpuoleisista osioista automaation tietoturvan hallintajärjestelmän perustamisen ja käyttöönoton alkuvaiheet on suoritettava ensimmäisenä, jotta järjestelmä voidaan ottaa käyttöön, ja saadaan puitteet muiden vaiheiden toimintojen suorittamiseen.

Tämän jälkeen vasemman puoleisia osioita suoritetaan omina kokonaisuuksinaan yhtäaikaaisesti. Kaikkia osioita ja niiden sisäisiä toimintoja arvioidaan, niille tehdään mahdollisesti tarvittavat liiketoimintaperustelut muutosten läpiviemiseksi, jonka jälkeen tilannetta arvioidaan uudelleen. Tämän jälkeen kehitetään toimintoja tarpeen mukaan sekä toteutetaan kehitysratkaisuja. Ylläpitovaiheessa suoritetaan esimerkiksi muutosten valvontaa sekä aikamääreistä valvontaa. Kun automaation tietoturvaan sidonnaisissa kohteissa ta-

pahtuu merkittäviä muutoksia tai määräaika kuluu umpeen, siirrytään uudelleen arviointivaiheeseen ja näin luuppi toistaa itseään. Kuvailtu menettely on esitetty kuvan 20 oikeassa reunassa. Tätä menettelyä voidaan pitää prosessiautomaation tietoturvan hallintajärjestelmän valvontamenettelynä, joka kuuluu yhtenä osana automaation tietoturvan hallintajärjestelmän perustamiseen ja käyttöönottoon. Seuraavissa kappaleissa käydään läpi kuvan 20 prosessiautomaation tietoturvan hallintajärjestelmää vaihe vaiheelta.

5.1 Hallintajärjestelmän perustaminen ja käyttöönotto

Automaation tietoturvan hallintajärjestelmän perustamis- ja käyttöönottovaiheessa on viisi osa-aluetta: liiketoimintaperustelun laatiminen, organisaation ja hallinnon määrittäminen, riskinhallintastrategian määrittäminen, järjestelmän sovellusalan kartoittaminen sekä menetelmien luominen järjestelmän kehittämistä ja valvontaa varten (kuva 21).



Kuva 21. Hallintajärjestelmän perustaminen ja käyttöönotto.

Tietoturvan hallintajärjestelmän perustamisen ja käyttöönoton ensimmäinen edellytys on, että sille saadaan yritysjohton tuki. Tätä varten tarvitaan hyvä liiketoimintaperustelu, jolla vakuutetaan yritysjohto tai muut päättävissä asemassa olevat henkilöt siitä, että tietoturvan hallintajärjestelmä todella on tarpeen, ja että siihen satsatut eurot maksavat itsensä takaisin tulevaisuudessa. Liiketoimintaperustelussa voidaan vedota esimerkiksi yritysturvallisuuspolitiikkaan, joka Takolta löytyy entuudestaan. Toinen hyödynnettävissä oleva toimintamalli on liiketoiminnan vaikutusanalyysi. Liiketoimintaperustelun puuttuminen saattaa johtaa pahimmassa tapauksessa siihen, että tämän tutkimuksen tuloksena koottua prosessiautomaation tietoturvan hallintajärjestelmää ei oteta käyttöön. Tämän vuoksi seuraavaksi käsitellään liiketoimintaperustelua tarkemmin

5.1.1 Liiketoimintaperustelu

Liiketoimintaperustelun tärkeys käy ilmi kirjallisuustutkimuksen kautta ja sen tarpeellisuus tulee ymmärtää ja huomioida automaation tietoturvan hallintajärjestelmän perustamisessa. On tärkeää saada korkeampi johto ja päättäjät ymmärtämään automaation tietoturvaan liittyvät riskit, automaatio- ja IT-järjestelmien erot sekä automaation erityisvaatimukset.

Liiketoimintaperustelun tarkoituksena on lisätä asianosaisten tietoisuutta automaation tietoturvasta ja osoittaa aiheen vakavuus esimerkiksi taloudellisin perustein. Yksi mielenkiintoinen lähestymistapa liiketoimintaperusteluun löytyy CPNI:n julkaisusta Establish ongoing governance [24, s. 8]. Siinä tuodaan esiin mahdollisuus käyttää esimerkkitapausta, jonka avulla havainnollistetaan tämänhetkiset riskit sekä turvallisuuden kehitystarve. Esimerkkitapauksella kuvataan tilannetta, joka voisi tapahtua asianosaaisessa organisaatiossa, jolloin uhka realisoituu ja siihen suhtaudutaan sen vaatimalla vakavuudella. Esimerkkitapauksen myötä käyvät ilmi esitettyjen investointien ansiosta saavutetut riskitason parannukset. [24] Liiketoimintaperustelu voidaan myös johtaa esimerkiksi olemassa olevista turvallisuuden, yleisen riskinhallinnan tai viranomaismääräysten noudattamisen politiikoista [39, s. 38–39].

Liiketoimintaperustelun avulla automaation tietoturvan hallintajärjestelmän kannattavuus pyritään osoittamaan konkreettisesti, jotta saataisiin riittävät resurssit järjestelmän perustamiselle. Jatkossa, esimerkiksi järjestelmämuutosten yhteydessä, voi olla tarpeen laatia uusia liiketoimintaperusteluita, joiden avulla perustellaan muutosten tarpeellisuutta. [39]

Liiketoimintaperustelun tärkeimmät osat

Standardin SFS-IEC 62443-2-1 [39] ja NIST:n Guide to Industrial Control Systems Security -julkaisun [35] mukaan liiketoimintaperustelun tulee sisältää ainakin taulukon 29 mukaiset osat. Kuten taulukosta ilmenee, oleellista on asettaa tärkeysjärjestykseen liiketoimintaseuraukset sekä -uhat ja arvioida vaikutuksia vuositasolla. Standardin SFS-IEC 62443-2-1 [39, s. 38–42] mukaan neljäntenä osana on kustannukset, kun taas NIST [35, kpl 4] nostaa esiin liiketoimintahyödyt.

Taulukko 29. Liiketoimintaperustelun osat [muokattu lähteistä 35 ja 39].

	SFS	NIST
Tärkeysjärjestykseen asetetut seuraukset liiketoiminnalle	x	x
Tärkeysjärjestykseen asetetut uhat	x	x
Arvioitu vuosittainen vaikutus liiketoiminnalle	x	x
Vastatoimenpiteiden kustannukset	x	
Liiketoimintahyödyt		x

Tarkoituksena ei ole listata asioita taulukon mukaisesti vaan tärkeintä on, että kaikki mainitut osa-alueet tulisi käsiteltyä liiketoimintaperustelussa. Kun tehdään liiketoimintaperustelua automaation tietoturvan hallintajärjestelmän käyttöönotolle, tulisi huomio kiinnittää yhteen tai kahteen tärkeimpään ongelmaan ja niiden tunnistamiseen [39, s. 38–42]. Jatkossa, kun tietoturvan hallintajärjestelmä on otettu käyttöön, ja sen kehittyessä, käsiteltäväksi voidaan ottaa muitakin ongelmia.

Liiketoimintaperustelun tavoitteet, ja miten ne saavutetaan

Liiketoimintaperustelun avulla pyritään osoittamaan, millaisia liiketoimintavaikutuksia tietoturvaan vastaan tehdyt hyökkäykset aiheuttavat. Tavoitteena on perustella automaation tietoturvan hallintajärjestelmän tarpeellisuutta teknisten käsitteiden lisäksi myös liiketoimintakäsitteitä käyttäen.

Liiketoimintaperustelussa ei suoriteta yksityiskohtaista riskien arviointia, vaan sillä pyritään kuvaamaan tärkeimmät tai vakavimmat riskit, joiden avulla pohjustetaan tietoturvan hallintajärjestelmän tarpeellisuutta. Liiketoimintavaikutuksia ja uhan aiheuttajia on lisätty esimerkiksi standardissa SFS-IEC 62443-2-1 [39, s. 40]. Liiketoimintaperustelussa pyritään asettamaan liiketoimintavaikutukset ja uhat tärkeysjärjestykseen.

Liiketoimintaperusteluun voidaan sisällyttää osoitus siitä, että automaation tietoturvan hallintajärjestelmän avulla voidaan parantaa automaatiojärjestelmän luotettavuutta, saatavuutta ja kokonaisturvallisuutta. Nämä ovat erittäin olennaisia asioita tehtaan automaatiojärjestelmän toiminnan kannalta.

Tavoitteena on, että pystyttäisiin tekemään kvantitatiivista vertailua sen suhteen, mitä voi tapahtua, jos automaation tietoturvan hallintajärjestelmä otetaan käyttöön, suhteessa siihen, että sitä ei oteta käyttöön. Myös kvalitatiivista vertailua voidaan tehdä, mutta kvantitatiivinen vertailu on ehkä helpommin ymmärrettävissä. Tehokas ja havainnollinen kvantitatiivinen vertailutapa on taloudellinen, euromääräinen vertailu.

Tämän tutkimuksen sivuilla 10 ja 19 on luettelo tietoturvaan vastaan tehdyn hyökkäyksen mahdollisista liiketoimintavaikutuksista, joita voidaan hyödyntää liiketoimintaperustelussa. Tällöin luodaan skenaario siitä, että automaation tietoturvan hallintajärjestelmää ei ole otettu käyttöön, ja automaatiojärjestelmää vastaan on päästy hyökkäämään jollain tapaa. Skenaarioiden pohjalta jokaista liiketoimintavaikutusta voidaan arvioida esimerkiksi taloudellisesti. Toisaalta taas taloudellisesti voidaan arvioida myös automaation tietoturvan hallintajärjestelmän käyttöönotosta aiheutuvia kustannuksia. Näiden tietojen pohjalta voidaan suorittaa kvantitatiivinen vertailu.

Liiketoimintaperustelulla pyritään näyttämään toteen, että hallintajärjestelmään liittyvät tietoturvariskien lieventämisestä aiheutuvat kustannukset voidaan perustella hallintojärjestelmän avulla saatavilla taloudellisilla hyödyillä [39]. Liiketoimintaperustelusta tulee tehdä riittävän yksityiskohtainen, jotta se riittää päätöksentekoprosessin tueksi.

5.1.2 Organisaatio- ja hallintomuutokset

Kun hallintajärjestelmää otetaan ensimmäistä kertaa käyttöön liiketoimintaperustelun laatimisen jälkeen, eli kun tuki hallintajärjestelmälle on saatu, suoritetaan alustavat organisaatio- ja hallintomuutokset. Niiden avulla tietoturvan hallintajärjestelmälle määritetään ylemmän tason vastuuhenkilöt sekä strategiat ja toimintatapamallit, joiden varaan

hallintojärjestelmää voidaan alkaa rakentamaan. KYBER-TEO-projektissa käsitellään vastuunjakamista havainnollisesti ja projektissa esiintyvää vastuunjakomatriisia kannattaa soveltaa organisaation vastuiden jaossa [1 s. 22]. Lisäksi Metsä Groupilta löytyy ohjeistus IT-puolen tietoturvan organisointiin, jonka avulla automaation tietoturvaa voidaan organisoida [14].

Kun vastuuhenkilöt on ensimmäisen kerran määritetty, he voivat delegoida tehtäviä ja käynnistää strategioiden suunnittelun, järjestelmän sovellusalan kartoittamisen sekä kehittää olemassa olevaa organisaatiota ja hallintoa.

5.1.3 Jatkuvuudenhallinta- ja riskinhallintastrategia

Metsä Groupin jatkuvuudenhallintastrategiaa voidaan hyödyntää myös automaatiojärjestelmän kohdalla. Sen avulla luodaan puitteet liiketoiminnan jatkuvuuden suunnitteluun ja hallintaan. Lisäksi sen avulla voidaan määrittää reagoimis- ja toipumistoimenpiteet esimerkiksi laitteistovikoja, inhimillisiä virheitä, luonnonkatastrofeja sekä tietomurtoja varten. Jatkuvuudenhallintastrategiassa määritellään siihen liittyvät roolit ja vastuut organisaatiossa, käydään läpi liiketoiminnan vaatimuksia, sekä kuvataan itse jatkuvuudenhallintastrategia. Roolit ja vastuut tulee jakaa siten, että kaikilla järjestelmään osilla on omistaja, joka vastaa kohdealueensa jatkuvuudenhallinnasta.

Metsä Groupilla on olemassa myös riskinhallintastrategia, jota voidaan suoraan hyödyntää automaation tietoturvan tarkastelussa. Tähän liittyen on sovittava siitä, kuinka usein riskiarvioita päivitetään ja miten kontrolloidaan sitä, että arvioinneissa ilmenneet korjaustarpeet huomioidaan ja korjataan. Järjestelmämuutoksista seuraa uusi riskinarviointi, jonka avulla järjestelmä pysyy ajan tasalla tietoturvan suhteen. Riskinarvioinnit sekä korjaavat toimenpide-ehdotukset dokumentoidaan ja käydään läpi asianosaisten kanssa konsernin riskinhallintapolitiikan mukaisesti.

5.1.4 Sovellusalan kartoitus

Sovellusalan kartoituksella selvitetään kohteet, joihin automaation tietoturvan hallintajärjestelmää sovelletaan. Niitä ovat muun muassa järjestelmän laitteet, verkkoyhteydet ja järjestelmän parissa työskentelevä henkilöstö. Sovellusalan kartoituksessa voidaan käyttää apuna esimerkiksi NIST:n tunnistusvaiheen ohjeistusta, sillä siinä on listattu yksityiskohtaisesti tarpeellisia kohteita. Automaatiojärjestelmän sovellusalaan liittyvien tietojen ylläpitoa varten Takolta löytyy lomakepohja, joka tulee täyttää aina uusien hankintojen tai muutosten yhteydessä. Lomake sisältää oleelliset tiedot järjestelmämuutoksista (esim. laitteisto, palomuri, tietoturva-asetukset, etäyhteydet, vastuuhenkilöt, varmuuskopiointi jne.). Lomakkeen käyttö ja asianmukainen dokumentointi tulee ohjeistaa kaikille asianosaisille sekä valvoa lomakkeen käyttöä.

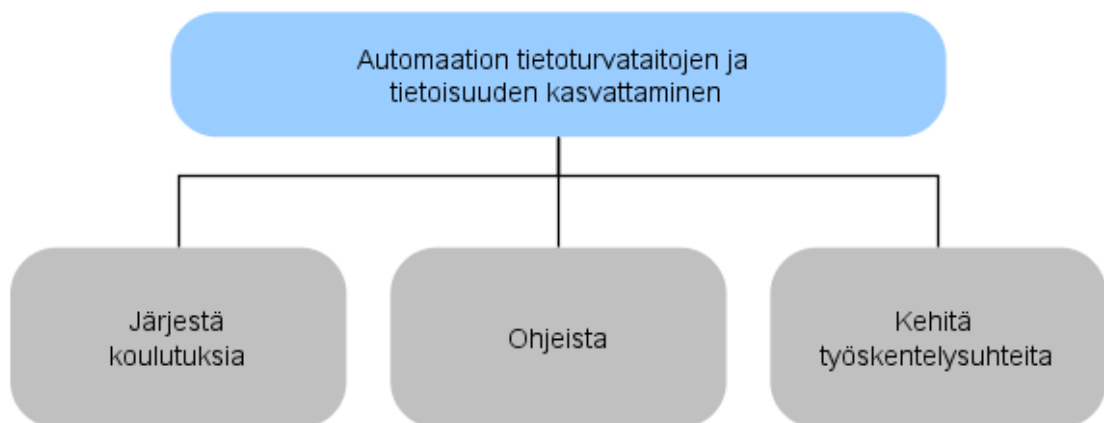
Kaiken kaikkiaan on syytä käydä läpi automaatiojärjestelmään liittyvä dokumentaatio ja varmistua dokumentaation riittävydestä ja ajantasaisuudesta. Olemassa olevan automaatiojärjestelmän dokumentaatiota voidaan päivittää täyttämällä edellä mainittua lomaketta systemaattisesti osajärjestelmäkohtaisesti.

5.1.5 Järjestelmän kehittäminen ja valvonta

Järjestelmän kehitys- ja valvontavaiheessa kehitetään menettelytavat, joilla valvotaan automaation tietoturvan hallintajärjestelmän noudattamista ja järjestelmän toimintaa, eli sitä toteuttaako järjestelmä sille asetetut vaatimukset, ja päästäänkö hallintajärjestelmän avulla haluttuihin tavoitteisiin. Jos havaitaan puutteita tai kehityskohtia, niihin puututaan, kehitetään ratkaisu ja toteutetaan vaadittavat parannukset. Takolla on olemassa ohjeistusta esim. tietoturva-auditoinneista [11]. Järjestelmän kehittäminen ja valvonta on sulautettu osaksi järjestelmää siten, että se toistaa kuvan 20 oikean reunan luuppia.

5.2 Automaation tietoturvatietoisuuden ja -taitojen kehittäminen

Suuri uhka automaatiojärjestelmän tietoturvaa vastaan on ihmisen toiminta [41 s.139]. Tietoturvataitojen ja tietoisuuden kehittäminen on automaation tietoturvan hallintajärjestelmän yksi tärkeä tavoite. Vaikka järjestelmä olisi tietoturvan osalta teknisesti mahdollisimman hyvin suojattu, voi ihminen toiminnallaan aiheuttaa suojauksen peittämisen. Henkilöstön koulutus ja tietoturvatietoisuuden lisääminen tähtää siihen, että henkilöstöllä on riittävät tiedot ja taidot työnsä suorittamiseksi tietoturvallisesti ja mahdolliset uhat ja haavoittuvuudet huomioiden. Jokainen henkilö, joka työskentelee jollain tavalla automaatiojärjestelmän kanssa, on perehdytettävä ja sitoutettava automaation tietoturvaan. Kuvasta 22 ilmenee, miten henkilöstön tietoturvataitoja ja tietoisuutta voidaan kasvattaa.



Kuva 22. Tietoturvataitojen ja tietoisuuden kasvattaminen.

Kouluttamalla ja lisäämällä tietoisuutta pyritään siihen, että automaation tietoturvasta huolehtiminen on rutiininomainen osa työtä. Tietoisuutta voidaan lisätä järjestämällä organisaation sisällä koulutusta ja ohjeistusta automaation tietoturvasta. Lisäksi on tärkeää varmistua siitä, että automaation tietoturvasta vastaavat henkilöt kommunikoivat riittävästi IT- sekä muun henkilökunnan kanssa, jolloin riittävä tuki puolin ja toisin on aina saatavilla ja työnjako ja tiedonkulku henkilöstön välillä toimii.

5.2.1 Kouluttaminen

Korkeamman portaan automaation tietoturvatietoisuutta tulee kasvattaa, jotta he tiedostavat automaatiojärjestelmän tietoturvariskit ja voivat kohdistaa tarvittavia resursseja prosessiautomaation tietoturvan hallintajärjestelmälle. Myös muun henkilöstön automaation tietoturvaan liittyvää tietoisuutta tulee lisätä, jotta jokainen tuntee vastuunsa, tietää järjestelmään liittyvät uhat ja osaa varautua mahdollisiin uhkaaviin tilanteisiin ja ennaltaehkäistä niiden syntymistä. Koulutuksia tulee järjestää eri henkilöstöryhmille (operaattorit, kunnossapito, suunnittelijat, IT-henkilöstö jne.) jokaisen ryhmän erilaiset tarpeet huomioiden [1, s. 26].

5.2.2 Ohjeistaminen

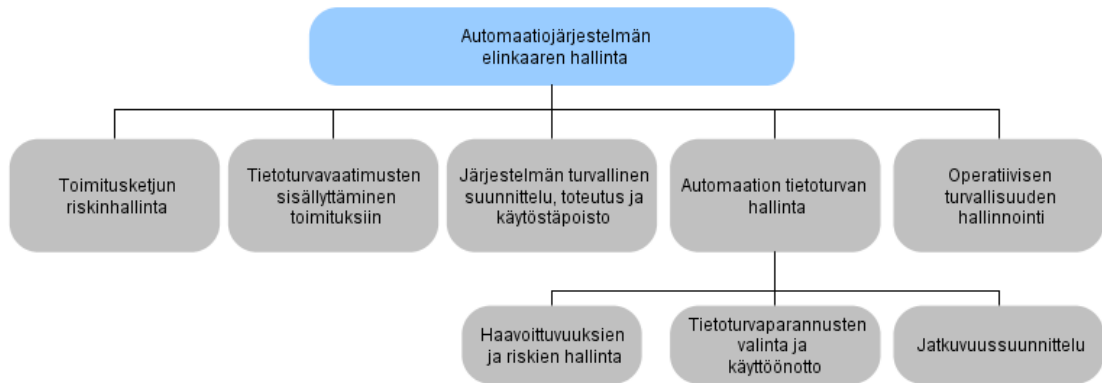
Metsä Groupilla on olemassa paljon erityisesti IT-puolen tietoturva-asioihin liittyvää ohjeistusta [7, 11, 13, 14, 43], jota voi osin hyödyntää myös automaatiopuolella. Tämän lisäksi on olemassa ohjeistusta myös suoraan automaation tietoturvaan [5, 42]. Ohjeiden ja toimintatapamallien käyttöä, dokumenttipohjien hyödyntämistä sekä dokumentointia tulee myös ohjeistaa. Lisäksi ohjeistuksen ja toimintatapamallien tulee olla kohdistettu eri henkilöstöryhmille siten, että ne vastaavat eri henkilöstöryhmien erilaisia tarpeita. Ohjeistuksia on päivitettävä, jotta ne noudattavat aina organisaation politiikkoja ja vastaavat senhetkistä tietoturvan tilaa.

5.2.3 Työskentelysuhteiden kehittäminen

Yhteistyötä Takon sisällä, eri osastojen välillä tulee lisätä, jotta automaation tietoturvaa pystytään hallitsemaan kokonaisvaltaisesti ja kaikki siihen liittyvät osa-alueet tulevat kateetuksi. Yhteistyö voidaan laajentaa kattamaan koko konsernin ja sen eri toimipisteet, jolloin tietoa jakamalla voidaan esimerkiksi välttyä tekemästä samoja asioita useampaan kertaan. Mikäli mahdollista, yhteistyötä voi olla myös konsernin ulkopuolelle.

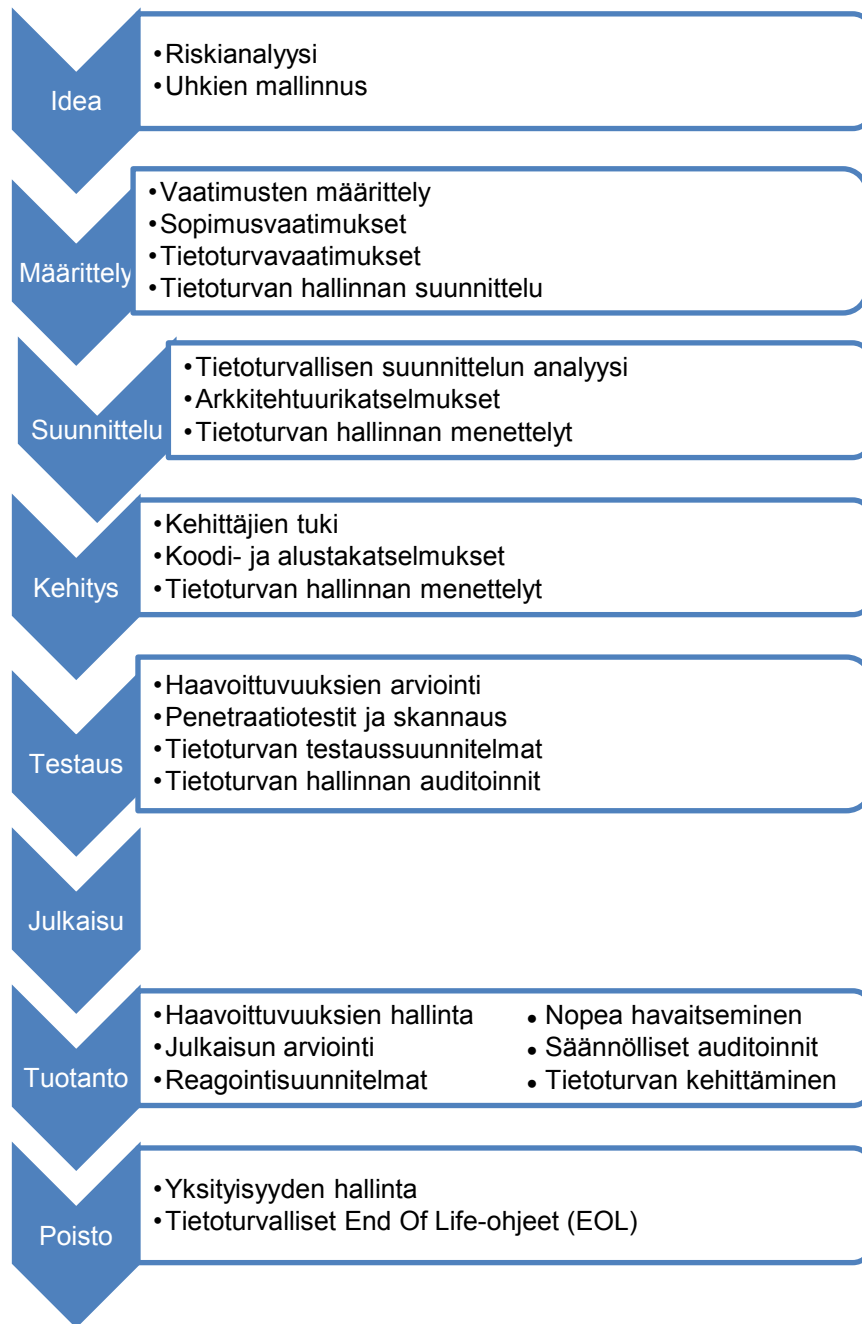
5.3 Automaatiojärjestelmän elinkaaren hallinta

Tavoitteena on tietoturvan sulauttaminen automaatiojärjestelmien elinkaareen. Eli se, että tietoturva huomioidaan automaatiohankinnoissa suunnittelusta aina käytöstä poistoon saakka. Automaatiojärjestelmän elinkaarenhallinta jakaantuu kuvan 23 mukaisiin osaluokkiin. Lisäksi automaation tietoturvan hallinta -osio jakautuu edelleen kolmeen pienempään alaosioon.



Kuva 23. Automaatiojärjestelmän elinkaarenhallinta.

Metsä Groupin Tietoturvallisen elinkaarenhallinnan periaate -dokumentissa [13] kuvataan Metsä Groupin linjaus siitä, miten tietoturva on sisällytetty elinkaarimallin eri vaiheisiin (kuva 24). Tietoturva tulee huomioida automaatiojärjestelmän koko elinkaaren ajan, jotta minimoidaan järjestelmähäiriöt ja varmistetaan riittävästä tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta [13].



Kuva 24. Tietoturvallisen elinkaarenhallinnan periaate [muokattu lähteestä 13].

Metsä Groupin tietoturvallisen elinkaarenhallinnan periaatemallista voidaan pienellä työllä muokata automaation tietoturvan erityistarpeet huomioon ottava ohjeistus automaatiojärjestelmän elinkaarenhallintaan.

Lisäksi Metsä Groupilla on olemassa ohjeistusta, politiikkoja sekä muuta dokumentaatiota, jota voidaan hyödyntää automaatiojärjestelmän elinkaaren eri vaiheissa. Automaatiohankintojen yhteydessä voidaan suoraan hyödyntää prosessiautomaation tietoturvaa ja IT-laitehankintoja koskevaa toimintaohjetta. Tämän toimintaohjeen mukaan ostosopimuksiin tulee liittää Metsä Groupin yleinen ohjeistus automaatiotoimittajille sekä verk-

koon liitettävien laitteiden kartoittamiseen käytettävä lomakepohja. Kun hankinnat toteutetaan ohjeen mukaan ja niiden laitteista kirjataan tiedot olemassa olevaan lomakepohjaan, osajärjestelmät rakentuvat johdonmukaisesti, ne ovat helposti jäljitettäviä ja dokumentointi pysyy ajantasaisena.

5.3.1 Toimitusketjun riskinhallinta

Toimitusketjun riskinhallinta alkaa toimitusketjun määrittämisellä. Ensin kartoitetaan kaikki teollisuusautomaatio- ja ohjausjärjestelmän toimitukseen liittyvät osapuolet kuten esimerkiksi ohjelmisto- ja laitetoimittajat. Seuraavaksi analysoidaan ja käsitellään toimitusketjuun liittyvät riskit Metsä Groupin riskinhallintaperiaatteen mukaisesti. Toimitusketjun riskinhallintaa käsitellään kaikissa kirjallisuustutkimuksen teoksissa sekä Metsä Groupin riskinhallintaa käsittelevissä toimintaohjeissa.

5.3.2 Tietoturva vaatimusten sisällyttäminen toimitussopimukseen

Automaatiojärjestelmätoimituksia varten tulee laatia lista tietoturva vaatimuksista, joiden tulee toteutua ja joita vasten järjestelmätoimituksen onnistumista voidaan arvioida. Tietoturva vaatimukset sisällytetään toimitussopimukseen ja niillä veloitetaan toimittajia noudattamaan organisaation määrittämää linjausta tietoturva-asioiden suhteen. Tällöin varmistetaan siitä, että koko toimitusprosessi on turvallinen ja järjestelmälle asetetut tietoturva vaatimukset toteutuvat. On myös tärkeää huolehtia siitä, että toimitussopimukseen on määritetty kaikki tietoturvaan liittyvät standardit, spesifikaatiot ja valitut riskien lievennystoimet tarpeellisessa laajuudessaan. Toimitusten sopimusehtojen ja tietoturva vaatimusten täyttymistä valvomaan tulee nimetä vastuuhenkilö, joka organisaation määrittämällä tavalla pitää huolta sopimusten noudattamisesta. Lisäksi toimittajille suoritetaan säännöllisiä tietoturvakatselmuksia ja –auditointeja järjestelmien priorisoinnin mukaan.

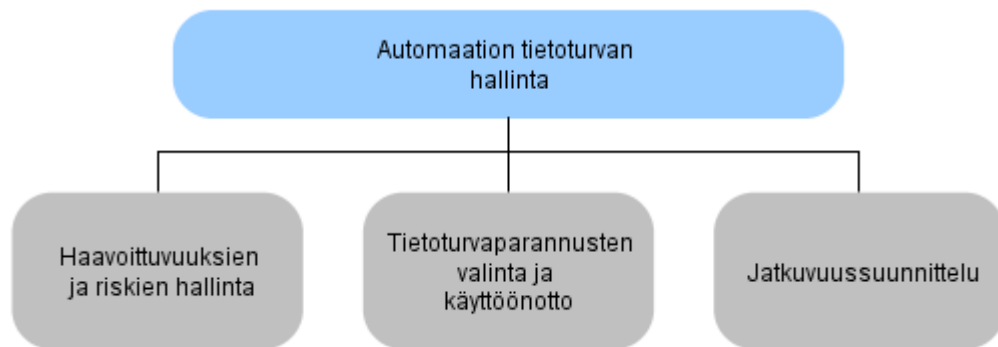
5.3.3 Järjestelmän suunnittelu, toteutus ja käytöstä poisto

Järjestelmä tulee suunnitella, ottaa käyttöön ja poistaa käytöstä tietoturva huomioiden. Suunnittelussa, järjestelmän toteutuksessa ja käytöstä poistossa on hyvä käyttää tietoturva-asiantuntijaa, joka huolehtii projektiin liittyvien tietoturvariskien hallinnasta ja niiden raportoinnista. Automaatiojärjestelmän suunnitteluun, toteutukseen ja käytöstä poistoon osallistuvien osapuolten tulee huomioida tietoturva kaikessa tekemisessään. Tietoturvakatselmuksia tulee suorittaa ennalta sovitun suunnitelman mukaisesti koko järjestelmän elinkaaren ajan, jotta varmistetaan riittävän korkeasta tietoturvan tasosta. Suunnittelu-, toteutus- ja käytöstä poisto –prosessien aikana on pidettävä huolta tietokriittisen materiaalin salassapidosta. Kun automaatiojärjestelmä tai sen osa tulee elinkaarensa päähän, myös tietoturvalliseen hävittämiseen tulee kiinnittää erityistä huomiota. Yksi var-

teenotettava keino tietoturvan toteutumiseksi käytöstä poistossa on laatia erillinen käytöstä poisto –suunnitelma, jossa eritellään järjestelmän kriittiset, erityistä huomiota hävittämävaiheessa vaativat osa-alueet.

5.3.4 Automaation tietoturvan hallinta

Kuvassa 25 esitetään vaiheet automaation tietoturvan hallintaan ja parantamiseen. Jatkuvuussuunnittelulle löytyy konsernitasolta kattava ohjeistus ja dokumenttipohjia [8, 9, 10, 12, 15]. Tietoturvan hallintaan valittiin käytettäväksi turvallisuustasot, joita käsitellään tässä tutkimuksessa sivuilla 12-13.



Kuva 25. Automaation tietoturvan hallinta.

Automaation tietoturvaa voidaan hallita hallitsemalla haavoittuvuuksia ja riskejä. Molemmat näistä ovat dynaamisia prosesseja, joiden suorittaminen tulee olla kiinteänä osana automaatiojärjestelmän elinkaarta. Haavoittuvuuksia tulee tunnistaa ja analysoida jatkuvasti ja reagoida uusiin tai muuttuneisiin haavoittuvuuksiin. Myös sisäisiä ja ulkoisia uhkia tulee arvioida ja seurata uhkakuvien muutoksia riittävän laajasti esimerkiksi alan foorumeilta ja muista lähteistä.

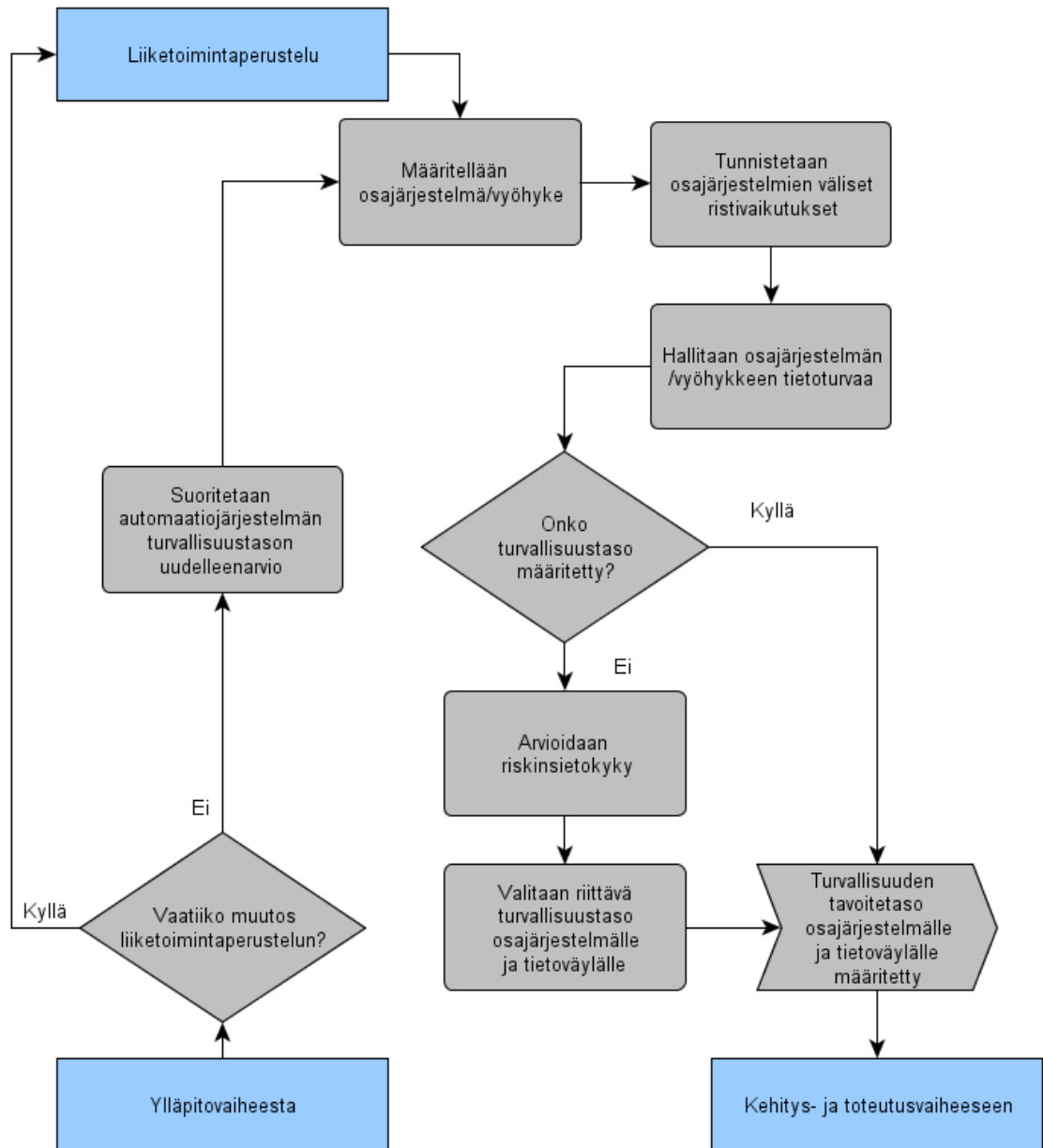
Uhkien ja haavoittuvuuksien seurauksia tulee luokitella niiden vakavuuden ja todennäköisyyden mukaan. Tämän luokittelun perusteella voidaan määrittää osajärjestelmän tai laitteen riskitaso ja sitä kautta turvallisuuden tavoitetaso. Määritettyjen riskitasojen perusteella osajärjestelmät voidaan priorisoida siten, että suurimman riskin järjestelmille, joiden tietoturvan taso on alhainen, annetaan resursseja turvallisuustason kohentamiseksi. Järjestelmän laitteistosta riippuu, kuinka korkea turvallisuustaso voidaan saavuttaa. Mikäli tarpeen, laitteistoa tulee muuttaa riittävän korkean turvallisuustason saavuttamiseksi.

Jotta riskit pysyvät hallinnassa, verkkoa, fyysistä ympäristöä sekä henkilöstön toimintaa tulee valvoa mahdollisten tietoturvatapahtumien varalta. Ulkoisten palveluntuottajien toimintaa tulee valvoa, sekä hallita mahdollisia etäyhteyksiä. Lisäksi voidaan mahdollisuuksien mukaan skannata verkkoa haavoittuvuuksien löytämiseksi. Kaikkeen poikkeavaan toimintaan tulee määrittää reagoimissuunnitelmat, joiden mukaan poikkeustilanteissa toimitaan. Reagoimissuunnitelmia käsitellään tarkemmin myöhemmin tässä kappaleessa.

Haavoittuvuuksien ja riskien hallinnasta täytyy tehdä riittävän laaja dokumentaatio, jotta kaikki tekeminen on jäljitettävissä ja siten haavoittuvuuksien ja riskien hallinnan sääntönmukaisuudesta ja loogisuudesta voidaan varmistua.

Tietoturvaparannusten valinta ja käyttöönotto -vaiheessa käydään läpi automaatiojärjestelmän osia prioriteetin mukaan. Tässä vaiheessa voidaan hyödyntää SFS-käsikirjasta muokattuja kaavioita (kuvat 26, 27 ja 28). Tällöin sovelletaan prosessiautomaation tietoturvan hallintajärjestelmän valvontamenettelyn vaiheita: arviointi, kehitys ja toteutus sekä ylläpito. Riippuen tarpeesta, voidaan ensin suorittaa liiketoimintaperustelu tai siirtyä suoraan arviointivaiheeseen.

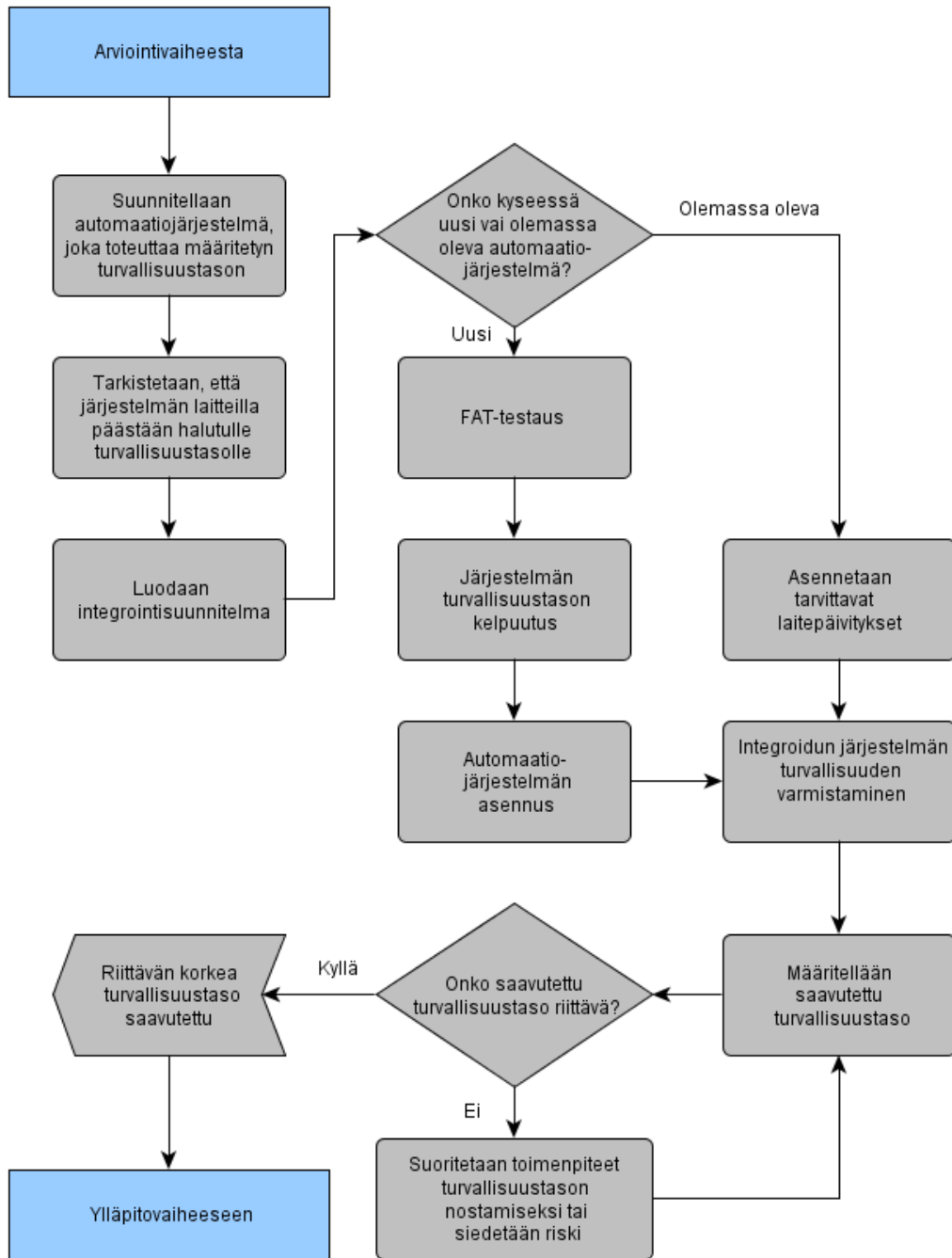
Arviointivaihe (kuva 26) alkaa määrittelemällä automaatiojärjestelmän osa, jonka tietoturvaa halutaan tarkastella sekä arvioidaan ristivaikutuksia muihin osajärjestelmiin. Jos tarkasteltavan järjestelmän osan turvallisuustasoa ei ole määritetty, suoritetaan riskin-sietokyvyn arviointi, jonka perusteella osajärjestelmälle ja sen tietoväylille valitaan riittävän korkea turvallisuustaso. Tämän jälkeen, tai jos turvallisuustaso oli ennalta määritetty, päästään arviointivaiheen tavoitetilään, jossa turvallisuuden tavoitetaso on määritetty.



Kuva 26. Tietoturvan hallintajärjestelmä – arviointivaihe [muokattu lähteestä 39].

Arviointivaiheeseen voidaan tulla myös ylläpitovaiheesta, jos järjestelmään tulee sellaisia muutoksia, joiden myötä turvallisuustaso tulee tarkistaa. Tässä kohtaa voi olla tarpeellista myös tehdä muutosta koskeva liiketoimintaperustelu, mikäli se vaaditaan resurssien varmistamiseksi, jonka jälkeen käydään läpi arviointivaiheen toiminnot. Arviointivaiheesta siirrytään kehitys- ja toteutusvaiheeseen.

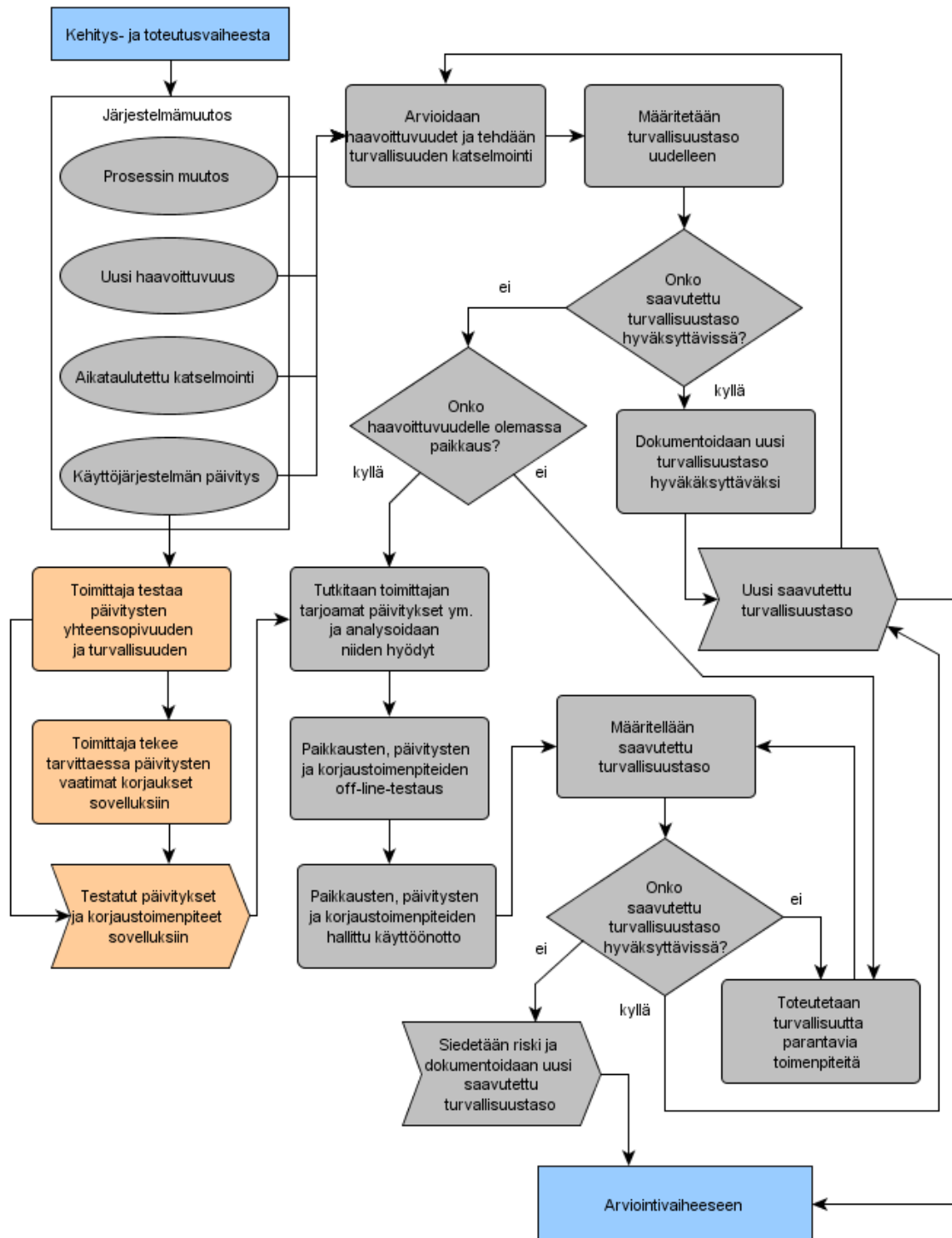
Kehitys- ja toteutusvaihe (kuva 27) aloitetaan suunnittelemalla automaatiojärjestelmän osa siten, että se toteuttaa määritetyn turvallisuustason asettamat vaatimukset ja että sen laitteilla voidaan päästä vähintään vaaditulle turvallisuustasolle. Tämän jälkeen tehdään integraatiosuunnitelma, jonka pohjalta osajärjestelmä sulautetaan yhteen muun automaatiojärjestelmän kanssa.



Kuva 27. Tietoturvan hallintajärjestelmän elinkaari – kehitys- ja toteutusvaihe [muokattu lähteestä 39].

Mikäli osajärjestelmä on täysin uusi, sille suoritetaan FAT-testaus (Factory Acceptance Test), turvallisuustason kelpuus sekä osajärjestelmän asennus ja integrointi. Jos järjestelmä on jo olemassa ja sitä vain muutetaan tai päivitetään, asennetaan tarvittavat laitepäivitykset ja suoritetaan integrointi. Integroidun järjestelmän turvallisuus testataan, jonka jälkeen määritetään saavutettu turvallisuustaso. Jos turvallisuustaso ei ole riittävä, suoritetaan tarvittavat parannukset tai siedetään jäljelle jäävä riski. Kehitys- ja toteutusvaiheen tavoitteeseen on päästy, kun saavutettu turvallisuustaso on hyväksyttävissä. Tämän jälkeen siirrytään ylläpitovaiheeseen.

Ylläpitovaiheessa (kuva 28) turvallisuustasoa uudelleen arvioidaan järjestelmämuutosten yhteydessä. Tällaisia voivat olla muun muassa prosessia koskevat muutokset, uudet haavoittuvuudet, aikataulutetut katselmointit tai käyttöjärjestelmien päivitykset.



Kuva 28. Tietoturvan hallintajärjestelmän elinkaari – ylläpitovaihe [muokattu lähteestä 39].

Muutoksen seurauksena arvioidaan haavoittuvuuksia sekä katselmoidaan muutosten vaikutukset tietoturvaan, minkä perusteella määritetään muutoksen jälkeinen saavutettu turvallisuustaso. Jos saavutettua turvallisuustasoa ei voida hyväksyä, tutkitaan, onko haavoittuvuudelle olemassa paikkaus. Jos järjestelmä tai sen osa on toimittajan vastuulla, muutostilanteessa toimittaja testaa päivitysten ja paikkausten yhteensopivuuden ja huolehtii riittävästä turvallisuudesta ja mahdollisista päivitysten vaatimista sovellusmuutoksista. Käyttäjän analysoitavaksi jäävät paikkauksesta seuraavat hyödyt ja/tai haitat. Paikkauksia ja päivityksiä testataan offline-tilassa ja testien onnistuttua ne otetaan hallitusti käyttöön. Paikkausten ja päivitysten käyttöönoton jälkeen määritellään saavutettu turvallisuustaso uudelleen.

Mikäli haavoittuvuudelle ei ole olemassa paikkausta tai paikkauksen käyttöönotto ei riitä nostamaan turvallisuustasoa tarpeeksi korkealle, täytyy suorittaa muita turvallisuutta parantavia toimenpiteitä, kunnes saavutetaan hyväksyttävissä oleva turvallisuustaso tai päätetään sietää jäännösriski. Toisaalta, jos järjestelmämuutoksista huolimatta turvallisuustaso säilyy hyväksyttävällä tasolla, voidaan saavutettu turvallisuustaso dokumentoida ja hyväksyä ja siirtyä ylläpitovaiheen tavoitteeseen, jossa uusi saavutettu turvallisuustaso hyväksytään. Ylläpitovaiheesta siirrytään edelleen arviointivaiheeseen.

Jatkuvuussuunnittelulla pyritään siihen, että tietoturvaluuhäiriöistä toipuminen tapahtuu sujuvasti ja minimoiden häiriön vaikutukset. Jatkuvuussuunnitelmassa on mietitty mahdollisia keskeytyksiä, niiden vaikutuksia muihin järjestelmiin sekä häiriötiloja koskevia toipumismenettelyitä. Myös jatkuvuussuunnitelmien ylläpidosta, päivittämisestä, tarkastuksista ja testaamisesta tulee huolehtia asianmukaisesti.

Metsä Groupin jatkuvuudenhallinnan periaatteita sekä olemassa olevaa dokumentaatiota käsiteltiin tämän tutkimuksen luvussa 4.2. Konzernissa on olemassa hyvät dokumenttipohjat jatkuvuussuunnitelmalle, jatkuvuuden hallinnan liiketoimintavaikutuksille sekä jatkuvuusstrategian tekoon. Jatkuvuussuunnitelmassa esitellään sovellusala, jaetaan vastuut sekä käydään läpi toiminta kriisitilanteessa. Liiketoimintavaikutuksia käsittelevässä dokumenttipohjassa esitellään aiheeseen liittyvä terminologia sekä arviointiskaalat, kuvataan liiketoimintaa, tehdään liiketoiminnan vaikutusanalyysi ja tarkastellaan häiriötilanteista toipumista. Jatkuvuudenhallintastrategiassa jaetaan roolit ja vastuut, listataan liiketoiminnan vaatimukset sekä itse jatkuvuudenhallintastrategia. Dokumenttien poikkiteollisen luonteen vuoksi on oleellista, että dokumenttien tekoon osallistuu riittävän laajalaisesti eri alojen osaajia.

Tärkeä osa jatkuvuussuunnittelua on reagointisuunnittelu, jonka tavoitteena on luoda ja ottaa käyttöön toimenpiteet, joita käytetään, kun havaitaan tietoturvahäiriöitä. Reagointitoimenpiteillä pyritään minimoimaan tietoturvahäiriöstä aiheutuvat haittavaikutukset. Reagointisuunnitteluun kuuluu reagointisuunnitelman teko, reagoinnista ja tietoturvahäiriö-

riöistä tiedottaminen, häiriötilanteiden ja niihin reagoinnin analysointi sekä virheistä oppiminen, negatiivisten vaikutusten minimointi sekä reagointisuunnitelman ylläpito ja tarvittavat päivitykset.

Toinen tärkeä jatkuvuussuunnittelun osa on toipumissuunnittelu. Konsernilla on olemassa toipumissuunnitelman dokumenttipohja, jota voidaan soveltaa automaatiojärjestelmään. Dokumentissa kuvataan muun muassa järjestelmän nykytila, oletettu toivutusaika, varajärjestelyt sekä toiminta ongelmatilanteissa.

5.3.5 Operatiivinen turvallisuus

Operatiivinen turvallisuus tarkoittaa sitä, että huolehditaan operatiivisten toimenpiteiden suorittamisesta rutiininomaisesti tietoturvallista toimintatapaa noudattaen. Tietoturvan toteutumista operatiivisissa toiminnoissa tulee valvoa järjestelmän koko elinkaaren ajan ennalta määritetyn suunnitelman mukaisesti. Operatiiviseen turvallisuuteen kuuluu myös se, että henkilöstön oikeuksia automaatiojärjestelmään rajataan siten, että käyttäjä saa vain työtehtävän kannalta välttämättömät käyttö- ja pääsyoikeudet. Operatiivinen turvallisuus on mukana järjestelmän koko elinkaaren ajan ja siksi se tulee huomioida myös prosessiautomaation tietoturvan hallintajärjestelmässä.

5.4 Yhteenveto prosessiautomaation tietoturvan hallintajärjestelmästä

Prosessiautomaation tietoturvan hallintajärjestelmä muodostettiin hyödyntäen kirjallisuustutkimuksen tuloksia, jotka koottiin kappaleeseen 3.4. Tämän lisäksi, jotta hallintajärjestelmästä saatiin Takon tarpeet huomioiva kokonaisuus, kartoitettiin prosessiautomaation tietoturvan sekä sen hallinnan nykytilaa. Tietojen pohjalta syntyi järjestelmä, jossa painotetaan kolmea osa-aluetta: prosessiautomaation tietoturvan hallintajärjestelmän perustamis- ja käyttöönottovaihetta, ihmisten sitouttamista prosessiautomaation tietoturvaan sekä tietoturvan integroimista prosessiautomaation elinkaareen.

Tutkimuksen perusteella panostamalla näihin kolmeen osa-alueeseen pystytään merkittävästi parantamaan prosessiautomaation tietoturvan hallintaa. Pelkästään hallintajärjestelmän perustamisvaiheen organisaatio- ja hallintomuutoksilla pystytään ohjaamaan työvoimaa ja resursseja automaation tietoturvan kannalta oikeiden asioiden pariin. Tarkka järjestelmän kartoitus mahdollistaa automaatiojärjestelmän tietoturvan paremman hallittavuuden ja strategiset muutokset muuttavat toimintatapoja oikeaan suuntaan.

Lisäämällä tietoisuutta ja tietoturvataitoja sitoutetaan automaatiojärjestelmän parissa työskentelevää henkilökuntaa toimimaan tietoturvallisesti. Tämä on erittäin tärkeä asia, sillä automaation tietoturvan hallinta muodostuu hyvin pitkälti toimintatavoista. Lisäksi jos tietoturva saadaan integroitua automaation elinkaareen, automaation tietoturvasta tu-

lee automaatioon sidottu luonnollinen prosessi, joka toteuttaa kaikki automaatiojärjestelmän elinkaaren vaiheet. Tällöin tietoturva tulee huomioitua suunnittelussa, vaatimusmäärittelyissä, sopimuksissa, testauksissa, jne. Hallintajärjestelmän toimivuus varmistetaan luomalla asianmukaiset valvontamenettelyt. Tarvittaessa järjestelmää tulee päivittää ja kehittää, jotta sen avulla saavutetaan halutut tavoitteet.

6. YHTEENVETO JA POHDINTAA TYÖSTÄ

Tämän työn tavoitteena oli kartoittaa Takon kartonkitehtaan prosessiautomaation tietoturvan hallinnan nykyinen tila, sekä sen perusteella luoda hallintajärjestelmä prosessiautomaation tietoturvalle. Tietoturvanhallinnan nykytilan kartoittamiseksi suoritettiin kirjallisuustutkimus, jotta pystyttäisiin hahmottamaan, mitä osa-alueita tietoturvan hallintaan kuuluu ja miten tietoturvan hallintaa voidaan arvioida. Samalla tutustuttiin myös siihen, miten prosessiautomaation tietoturvan hallintajärjestelmä voitaisiin perustaa ja ottaa käyttöön ja mitä osa-alueita hallintajärjestelmän tulee käsittää.

Kirjallisuustutkimuksessa tarkasteltiin standardia SFS-IEC 62443-2-1 [39], NIST:n kyberturvallisuuden kehysmallia [4] sekä CPNI:n automaation tietoturvan kehysmallia [24–33]. Teosten keskeinen sanoma on, että ne eivät tarjoa valmista ratkaisua automaation tietoturvan hallintaan vaan antavat raamit yrityksen tarpeita vastaavan hallintajärjestelmän rakentamiselle. Teosten mallit ovat hyvin toistensa kaltaisia ja kaikista nousee esille seuraavat toimenpiteet tietoturvan hallitsemiseksi: hallintajärjestelmän perustaminen ja käyttöönotto, toimintatapojen muutokset sekä vastatoimenpiteiden hallinta.

Kirjallisuustutkimuksen jälkeen perehdyttiin konsernin olemassa oleviin politiikkoihin, toimintamalleihin sekä muuhun dokumentaatioon, jota kokonaisvaltaisessa automaation tietoturvan hallinnassa voitaisiin hyödyntää. Tietoturvan hallinnan tilaa pyrittiin selvittämään myös seuraamalla ja analysoimalla henkilökunnan toimintatapoja sekä kartoittamalla automaatiojärjestelmää. Näin muodostui kuva siitä, mikä on prosessiautomaation tietoturvan hallinnan tila tällä hetkellä, ja mitä siihen liittyviä osa-alueita tulee parantaa.

Parannuskohteet olivat käytännössä samoja kuin kirjallisuustutkimuksessa painotetut. Tehtaan tietoturvasta on huolehdittu kattavasti ja se on hyvällä tasolla, mutta automaation tietoturvaan ja nimenomaan sen hallintaan tulee panostaa. Tämä voidaan ratkaista perustamalla ja ottamalla käyttöön automaation tietoturvan hallintajärjestelmä. Henkilökunta tulee sitouttaa noudattamaan järjestelmää – tähän tarvitaan toimintatapojen muutoksia. Lisäksi vastatoimenpiteiden hallintaa voidaan parantaa. Työkalut ovat olemassa, kunhan ne otetaan käyttöön.

Tutkimuksen tuloksena syntyi prosessiautomaation tietoturvan hallintajärjestelmä, joka on rakennettu automaation tietoturvan hallinnan nykytila huomioiden ja pureutuen erityisesti niihin osa-alueisiin, jotka kaipaavat lisähuomiota. Työn kannalta olisi ollut oleellista päästä perustamaan ja ottamaan käyttöön hallintajärjestelmä, mutta rajallinen aika ja resurssit tulivat vastaan, jolloin tutkimuksen tuloksena syntyneen tietoturvan hallintajärjestelmän toimintaa ei ole voitu vielä arvioida.

Toivottavaa on, että järjestelmä otetaan käyttöön, ja että käyttöönoton yhteydessä tehdään jatkotutkimusta kaikista hallintajärjestelmän päävaiheista seuraavista vaiheista, joihin ei pystytty tämän tutkimuksen puitteissa tarkemmin paneutumaan. Hallintajärjestelmän perustaminen ja käyttöönotto pitää aloittaa heti, ja tutkimusta sekä kehitystyötä järjestelmän parantamiseksi ja tarkentamiseksi voidaan tehdä samanaikaisesti. Näin prosessiautomaation tietoturvan hallinnan parannustyö saadaan aloitettua mahdollisimman pian.

Työn aihepiiri oli hyvin laaja ja siitä johtuen tutkimuksessa ei pystytty menemään juuri pintaa syvemmälle ja näin ollen jäljelle jäi monia jatkotutkimuksen kohteita. Alussa ajatuksena oli, että työn aikana löydetään automaatiojärjestelmän tietoturvan heikot kohdat ja mahdollisesti jopa toteutetaan suojausmenettelyt niiden korjaamiseksi. Pian kuitenkin selvisi, että jotta työstä olisi todellista hyötyä, se tulisi aloittaa aivan perusteista ja siten pyrkiä muuttamaan organisaation ja hallinnon toimintatapoja, jotta automaation tietoturva saadaan integroitua tehtaan kaikkiin toimintoihin. Alkuperäinen ajatus hioutui tavoitteeksi muodostaa runko prosessiautomaation tietoturvan hallintaan.

Työstä ei välttämättä ole välitöntä hyötyä työn tilaajalle, sillä sen seurauksena ei syntynyt välittömiä prosessiautomaation tietoturvan parannuksia. Sen sijaan työn tuloksena syntyi prosessiautomaation tietoturvan hallintajärjestelmä, jonka käyttöönotosta voi olla hyötyä pidemmällä aikavälillä. Sen avulla on mahdollista muokata yrityksen organisaatorakennetta ja toimintatapoja ja siten lisätä prosessiautomaation tietoturvan hallittavuutta.

LÄHTEET

- [1] P. Ahonen, et al. KYBER-TEO -tuloksia 2014-2016, Julkisten tulosten kooste, Teknologian tutkimuskeskus VTT Oy, Espoo, 2017, 148 s. Saatavissa: <http://urn.fi/URN:ISBN:978-951-38-8540-3>.
- [2] Automaatiosuunnittelun prosessimalli, Suomen automaatioseura ry, Helsinki, 2007, 43 s. Saatavissa: https://www.automatioseura.fi/site/assets/files/1367/automaatiosuunnittelun_prosessimalli.pdf.
- [3] N. Fallier, L. O Murchu, E. Chien, W32.Stuxnet Dossier, Symantec Corporation, 2011, 69 p. Saatavissa (viitattu 19.11.2018): https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
- [4] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, 2018, 55 p. Saatavissa: <https://doi.org/10.6028/NIST.CSWP.04162018>.
- [5] General guidelines for automation and other vendors, Metsä Group, 2014, 9 p. Rajoitettu saatavuus.
- [6] Good Practice Guide – Process Control and Scada Security, Centre for the Protection of National Infrastructure, London, 26 p.
- [7] E. Joffel, Henkilöstön tietoturvaohje, Metsä Group, Espoo, 2017, 13 s. Rajoitettu saatavuus.
- [8] E. Joffel, Jatkuvuudenhallintastrategia – esimerkkipohja, Metsä Group, Espoo, 2016, 11 s. Rajoitettu saatavuus.
- [9] E. Joffel, Jatkuvuussuunnitelma – esimerkkipohja, Metsä Group, Espoo, 2017, 27 s. Rajoitettu saatavuus.
- [10] E. Joffel, Liiketoiminnan vaikutusanalyysi (BIA) – esimerkkipohja, Metsä Group, Espoo, 8 s. Rajoitettu saatavuus.
- [11] E. Joffel, Ohje tietoturva-auditointisuunnitelmantekoon, Metsä Group, Espoo, 2017, 4 s. Rajoitettu saatavuus.
- [12] E. Joffel, Tekninen toivutussuunnitelma – esimerkkipohja, Metsä Group, Espoo, 2016. 8 s. Rajoitettu saatavuus.

- [13] E. Joffel, Tietoturvallisen elinkaarenhallinnan periaate, Metsä Group, Espoo, 2017, 8 s. Rajoitettu saatavuus.
- [14] E. Joffel, Tietoturvan organisointi Metsä Group –konsernissa, Metsä Group, Espoo, 2017, 5 s. Rajoitettu saatavuus.
- [15] E. Joffel, Yleistä jatkuvuudenhallinnasta, Metsä Group, Espoo, 2016, 8 s. Rajoitettu saatavuus.
- [16] J. Ikonen, Takon tavoitteet, Power Point –esitys, Metsä Board Tako, Tampere, 2017, 2 s. Rajoitettu saatavuus.
- [17] Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen standardisoimisliitto, ISO/IEC 17799:fi, Helsinki, 2006, 115 s.
- [18] Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen standardisoimisliitto, ISO/IEC 27001:fi, Helsinki, 2006, 34 s.
- [19] M. Lehto, P. Neittaanmäki, Cyber Security: Analytics, Technology and Automation, Springer, 2015, 268 p.
- [20] MES Integration Process Overview, Metsä Board, 2016, julkaisematon selvitys, 31 s.
- [21] Metsä Board: About Us, Tako Board Mill, verkkosivu. Saatavissa (viitattu 11.11.2018): <https://www.metsaboard.com/About-Us/Tako-board-mill/Pages/default.aspx>.
- [22] Metsäliitto –konsernin riskienhallintaperiaatteet, Metsä Group, 2007, 15 s. Rajoitettu saatavuus.
- [23] Riskienhallintaperiaatteet, Metsä Board Oyj, 2013, 14 s. Rajoitettu saatavuus.
- [24] Security for Industrial Control Systems – Establish Ongoing Governance, Centre for the Protection of National Infrastructure, London, 2015, 20 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [25] Security for Industrial Control Systems – Establish Response Capabilities, Centre for the Protection of National Infrastructure, London, 2015, 22 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [26] Security for Industrial Control Systems – Executive Summary, Centre for the Protection of National Infrastructure, London, 2015, 8 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.

- [27] Security for Industrial Control Systems – Framework overview, Centre for the Protection of National Infrastructure, London, 2015, 40 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [28] Security for Industrial Control Systems – Improve Awareness and Skills, Centre for the Protection of National Infrastructure, London, 2015, 18 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [29] Security for Industrial Control Systems – Manage Industrial Control Systems Lifecycle, Centre for the Protection of National Infrastructure, London, 2015, 27 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [30] Security for Industrial Control Systems – Manage the Business Risk, Centre for the Protection of National Infrastructure, London, 2015, 23 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [31] Security for Industrial Control Systems – Manage Third Party Risks, Centre for the Protection of National Infrastructure, London, 2015, 20 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [32] Security for Industrial Control Systems – Manage Vulnerabilities, Centre for the Protection of National Infrastructure, London, 2015, 20 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [33] Security for Industrial Control Systems – Select and Implement Security Improvements, Centre for the Protection of National Infrastructure, London, 2015, 23 p. Saatavissa: <https://www.ncsc.gov.uk/guidance/security-industrial-control-systems>.
- [34] J. Seppälä, Tietoliikenne sekä auditointi – Automaation turvallisuus -kurssin luentokalvot, Tampereen teknillinen yliopisto, 48 s. Rajoitettu saatavuus.
- [35] K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, Second Public Draft, National Institute of Standards and Technology, Maryland, USA, 2007, 157 p.
- [36] T. Tommila, Laatu automaatiassa – Parhaat käytännöt, Suomen Automaatioseura, Helsinki, 2001, 245 s. Saatavissa: <https://www.automatioseura.fi/site/assets/files/1367/laatuautomaatiassa.pdf>.
- [37] Tako Mill Interfaces, Metsä Board Tako, 2013, julkaisematon selvitys, 1 s.

- [38] Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit. Suomen standardisoimisliitto, IEC/TS 62443-1-1:fi, Helsinki, 2013, 77 s.
- [39] Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten. Suomen standardisoimisliitto, SFS-IEC 62443-2-1, Helsinki, 2013, 146 s.
- [40] Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille. Suomen standardisoimisliitto, IEC/TR 62443-3-1:fi, Helsinki, 2013, 94 s.
- [41] Teollisuusautomaation tietoturva, Suomen automaatioseura ry, Helsinki, 2005, 160 s. Saatavissa: <https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf>.
- [42] Tietoturva ja IT-laitehankinnat prosessiautomaatiossa – toimintaohje, Metsä Group, 2012, 2 s. Rajoitettu saatavuus.
- [43] Tietoturvallisuuspolitiikka, Metsä Group, 2017, 4 s. Rajoitettu saatavuus.
- [44] Yritysturvallisuuspolitiikka, Metsä Group, 2016, 2 s. Rajoitettu saatavuus.