

TARTU ÜLIKOOL  
Loodus- ja täppisteaduste valdkond  
Arvutiteaduse instituut

# Automatiseeritud süsteemide ja tehnoloogiate küberturvalisuse riskide ja nende maandamise võimaluste analüüs

Tartu 2024



Kaasrahastatud Euroopa Liidu poolt. Avaldatud seisukohad ja arvamused on ainult autori(te) omad ega pruugi kajastada Euroopa Liidu või Euroopa küberpädevuskeskuse seisukohti või arvamusi. Euroopa Liit ega Euroopa küberpädevuskeskus nende eest ei vastuta.

## Resüme

Automatiseeritud süsteemid ja tehnoloogiad on nagu võrgustik, kus töötavad koos erinevad täituriid, näiteks tööstusrobotid ja arvutiseadmed. Tootmissektoris hõlmab see võrgustik mitmeid tegevusi alates projekteerimisest ja planeerimisest kuni tootmise, logistika, ladustamise ja müügini.

Need süsteemid võtavad enda peale ülesanded, mida tavaliselt teevad inimesed ja mis aitab suurendada efektiivsust ja tootlikkust erinevates tootmisprotsessi etappides. Automatiseeritud süsteemid ja tehnoloogiad võivad olla erineva tasemega, alates osaliselt käsitsi juhitud kuni täielikult automatiseeritud süsteemideni. Nende toimimisel on olulised müüja hooldus- ja vigade lahendamise põhimõtted ning on võimalik, et nende korralikuks toimimiseks on vaja kaugjuurdepääsu mehhanisme. Selleks, et organisatsioon suudaks säilitada oma konkurentsivõime, selles on selles keerulises keskkonnas oluline tagada, et kasutatavad andmed ja teave oleksid konfidentsiaalsed, terviklikud ja käideldavad. Arvestades digitaalse arengu kiirust, suurenevat vajadust nõudluspõhise tootmise järele ning tööjõu kulude kasvu, pole nende süsteemide turvalisus enam lihtsalt soovituslik, vaid on muutunud kriitiliseks investeeringuks.

Siiski on automatiseeritud süsteemide ja tehnoloogiate kasutamine ning teadlikkus nende küberturvalisuse riskidest ja võimalikest vastumeetmetest üsna piiratud. Operatiiv- ja turvaaspektides teavitatakse tihti suuliselt, ilma kehtiva turvapoliitikata ning turvalisusele pööratakse tähelepanu alles pärast turvaintsidentide toimumist. Organisatsioonid peavad olema teadlikud erinevatest turvastandarditest ja -eeskirjadest. Turvaintsidentidele reageerimine hõlmab tavaliselt andmete ja süsteemi taastamist kohalikust varukoopiast.

Analüüsis uuritakse automatiseeritud süsteemide ja tehnoloogiate kasutamist, kasutades intervjuusid, süstemaatilise kirjanduse analüüsi ja organisatsioonides läbi viidud küsitluse tulemusi. Analüüsi fookuses on kontekst ja olulised ressursid ning varad, mida tuleb kaitsta küberturvalisuse riskide eest. Konkreetsemalt vaadeldakse turvariskide juhtimise valdkonna mudelit, et selgitada automatiseeritud süsteemide nõrkusi, nendega seotud turvariske ning nende mõju andmete ja teabe konfidentsiaalsusele, terviklusele ja käideldavusele. Analüüsis esitatakse soovitused otsuste ja vastumeetmete kohta, mis aitavad maandada tuvastatud küberturvalisuse riske.

**Võtmesõnad:** Automatiseeritud süsteemid ja tehnoloogiad, kaitstud varad, küberturvalisuse riskid, STRIDE, vastumeetmed, turvanõuded ja kontroll, turvastandardid, ISSRM ja tootmisorganisatsioonid.

# Sisukord

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Sissejuhatus</b>   | <b>7</b>  |
| <b>2</b> | <b>Uurimismeetod</b>  | <b>8</b>  |
| 2.1      | Turvariskide haldamine . . . . .  | 8         |
| 2.2      | Uurimisküsimused . . . . .  | 13        |
| 2.3      | Intervjuud . . . . .  | 13        |
| 2.3.1    | Intervjuude teemad ja küsimused . . . . .   | 14        |
| 2.4      | Kirjanduse analüüs . . . . .  | 16        |
| 2.5      | Küsitlus . . . . .  | 21        |
| 2.6      | Ohud valiidsusele . . . . .   | 22        |
| <b>3</b> | <b>Automatiseeritud süsteemide ja tehnoloogia kontekst</b>                              | <b>25</b> |
| 3.1      | Automatiseeritud süsteemide ja tehnoloogiade definitsioon . . . . .                     | 25        |
| 3.2      | Tööstus 4.0 arhitektuuriline mudel . . . . .  | 27        |
| 3.3      | Väljakutsed . . . . .   | 29        |
| 3.4      | Intervjuude tulemused . . . . .   | 30        |
| 3.5      | Küsitluse tulemused . . . . .   | 32        |
| 3.6      | Arutelu . . . . .   | 33        |
| <b>4</b> | <b>Standardid</b>   | <b>35</b> |
| 4.1      | Tööstusrobotika ja -automaatika ohutus- ja turvastandardid . . . . .                    | 35        |
| 4.1.1    | Tööstusrobotika ja -automaatika standardid . . . . .                                    | 35        |
| 4.1.2    | Küberturbe koondpunkt: infotehnoloogia infrastruktuurist tööstusautomaatikani . . . . . | 36        |
| 4.2      | Küsitluse tulemused . . . . .   | 37        |
| 4.3      | Arutelu . . . . .   | 37        |
| <b>5</b> | <b>Automatiseeritud süsteemide ja tehnoloogiade varad</b>                               | <b>39</b> |
| 5.1      | Intervjuude tulemused . . . . .   | 39        |
| 5.2      | Kirjanduse analüüsi tulemused . . . . .   | 39        |
| 5.3      | Küsitluse tulemused . . . . .   | 41        |
| 5.4      | Arutelu . . . . .   | 42        |
| <b>6</b> | <b>Automatiseeritud süsteemide ja tehnoloogiade turvariskid</b>                         | <b>44</b> |
| 6.1      | Olukord Eesti küberruumis . . . . .   | 44        |
| 6.2      | Kirjanduse analüüsi tulemused . . . . .   | 45        |
| 6.3      | Küsitluse tulemused . . . . .   | 48        |
| 6.4      | Arutelu . . . . .   | 48        |
| <b>7</b> | <b>Turvalisuse vastumeetmed automatiseeritud süsteemides ja tehnoloogiates</b>          | <b>50</b> |
| 7.1      | Kirjanduse analüüsi tulemused . . . . .   | 50        |
| 7.2      | Küsitluse tulemused . . . . .   | 52        |

|           |  |           |
|-----------|--|-----------|
| 7.3       | Arutelu . . . . .  | 52        |
| <b>8</b>  | <b>Siseringi turvariskid tootmistellimuste töötlemisel</b>       | <b>61</b> |
| 8.1       | Konteksti analüüs . . . . .                                      | 61        |
| 8.2       | Tööstusspionaaž . . . . .  | 61        |
| 8.3       | Petturlik töö . . . . .  | 64        |
| 8.4       | Tahtlik sabotaaž . . . . .                                       | 66        |
| 8.5       | Tahtmatu kahju . . . . .   | 68        |
| 8.6       | Saadud õppetunnid . . . . .                                      | 69        |
| <b>9</b>  | <b>STRIDE turvaohutude analüüsimine tootmisettevõttes</b>        | <b>70</b> |
| 9.1       | Ettevõtte kirjeldus . . . . .                                    | 70        |
| 9.2       | Süsteemi kontekst . . . . .                                      | 71        |
| 9.3       | Turvariskide juhtimine . . . . .                                 | 74        |
| 9.3.1     | Võltsimine/teesklus/pettus ( <i>Spoofing</i> ) . . . . .         | 74        |
| 9.3.2     | Muukimine/rikkumine ( <i>Tampering</i> ) . . . . .               | 76        |
| 9.3.3     | Teabe avalikustamine ( <i>Information Disclosure</i> ) . . . . . | 78        |
| 9.3.4     | Teenustõkestus/ummistus ( <i>Denial of Service</i> ) . . . . .   | 79        |
| 9.3.5     | Õiguste vallutus ( <i>Elevation of Privilege</i> ) . . . . .     | 80        |
| 9.4       | Saadud õppetunnid . . . . .                                      | 82        |
| <b>10</b> | <b>Kokkuvõtvad märkused</b>                                      | <b>83</b> |
|           | <b>Viited</b>  | <b>84</b> |
|           | <b>Lisad</b>   | <b>88</b> |
|           | I. Terminid . . . . .  | 88        |
|           | II. Küsitluse küsimused ja vastuse variandid . . . . .           | 91        |
|           | III. Riski stsenaariumid . . . . .                               | 99        |

## Joonised

|    |   |    |
|----|---|----|
| 1  | ISSRM domeeni mudel, kohandatud allikast [11] [29] . . . . .  | 8  |
| 2  | ISSRM protsess, kohandatud allikast [11] [29] . . . . .   | 12 |
| 3  | Organisatsioonide tootmiskategooria . . . . .   | 23 |
| 4  | Vastajate rollid . . . . .  | 23 |
| 5  | RAMI 4.0 arhitektuuri mudel, kohandatud allikast [10] . . . . .   | 28 |
| 6  | Automatiseeritud tootmissüsteemide rakendamise variatsioonid . . . . .  | 31 |
| 7  | Automatiseerimise tasemed . . . . .   | 32 |
| 8  | Automatiseeritud tootmissüsteemide muudatused viimase 5 aasta jooksul . . . . .   | 33 |
| 9  | Automatiseeritud tootmissüsteemide rakendamise väljakutsed . . . . .  | 34 |
| 10 | Turvalisuse, eraelu puutumatus või ohutusega seotud õigusaktid, määrused ja/või standardid, mis puudutavad automatiseeritud tootmissüsteeme . . . . . | 38 |
| 11 | Automatiseeritud tootmissüsteemides kasutatavad andmed . . . . .  | 42 |
| 12 | IT-süsteemi kasutamise eesmärgid automatiseeritud tootmissüsteemides . . . . .  | 43 |
| 13 | Kirjanduse analüüsis tuvastatud turvaohud . . . . .   | 45 |
| 14 | Vastajate osutatud turvalisuse ohud . . . . .   | 48 |
| 15 | Ettevõtetes turvalisusega seotud teemade käsitus . . . . .  | 55 |
| 16 | Turvalisuse alane kooolitus ettevõtetes . . . . .   | 56 |
| 17 | Vastumeetmed turvasündmuste leevendamiseks . . . . .  | 57 |
| 18 | Infotöötlus funktsiooni (süsteemi varade), pettuse ohtude ja turvameetmete vastastikune sõltuvus . . . . .  | 57 |
| 19 | Infotöötlus funktsiooni (süsteemi varade), rikkumise ohtude ja turvameetmete vastastikune sõltuvus . . . . .  | 58 |
| 20 | Infotöötlus funktsiooni (süsteemi varade), teabe avalikustamise ohtude ja turvameetmete vastastikune sõltuvus . . . . .                               | 59 |
| 21 | Infotöötlus funktsiooni (süsteemi varade), ummistus ohtude ja turvameetmete vastastikune sõltuvus . . . . .   | 59 |
| 22 | Infotöötlus funktsiooni (süsteemi varade), õiguste vallutus ohtude ja turvameetmete vastastikune sõltuvus . . . . .                                   | 60 |
| 23 | Tellimuste töötlemise stsenaarium, kohandatud allikast [28] . . . . .   | 62 |
| 24 | Tootmise teostamise stsenaarium, kohandatud allikast [28] . . . . .   | 63 |
| 25 | Tööstusspionaaži riski mudel, kohandatud allikast [28] . . . . .  | 64 |
| 26 | Petturliku töö riski mudel, kohandatud allikast [28] . . . . .  | 66 |
| 27 | Tahtliku sabotaaži riski mudel, kohandatud allikast [28] . . . . .  | 68 |
| 28 | Ettevõtte X peamised protsessid, kohandatud allikast [26] . . . . .   | 71 |
| 29 | Müügiprotsess, kohandatud allikast [26] . . . . .   | 72 |
| 30 | Toote disaini protsess, kohandatud allikast [26] . . . . .  | 73 |
| 31 | Tootmisprotsess, kohandatud allikast [26] . . . . .   | 75 |
| 32 | Andmete rikkumise stsenaarium . . . . .   | 77 |
| 33 | Vahendusründe stsenaarium . . . . .   | 78 |
| 34 | Mikrovigade sisestamise stsenaarium . . . . .   | 81 |

## Tabelid

|    |  |    |
|----|--|----|
| 1  | Intervjueeritud ettevõtted . . . . .   | 14 |
| 2  | Kirjanduse analüüsi valitud allikad ja vastavad tulemused . . . . .  | 16 |
| 3  | Kaasamis-/väljaarvamiskriteeriumid valitud artiklite puhul . . . . .                                       | 17 |
| 4  | Seotud definitsioonid . . . . .  | 26 |
| 5  | Intervjuude tulemuste seostamine RAMI 4.0 varade kihiga; ”+“ viitab varade mainimisele . . . . .           | 39 |
| 6  | Süsteemi varade kaardistamine kirjandusest RAMI 4.0 varade kihiga; ”+“ viitab varade mainimisele . . . . . | 40 |
| 7  | RAMI 4.0 Vara kihtide varad . . . . .  | 41 |
| 8  | STRIDE taksonoomia kohane turvaehtude klassifikatsioon (1) . . . . .                                       | 46 |
| 9  | STRIDE taksonoomia kohane turvaehtude klassifikatsioon (2) . . . . .                                       | 47 |
| 10 | Turvanõuded [3] [4] ja kontrollid võltsimisriskide vähendamiseks . . . . .                                 | 50 |
| 11 | Turvanõuded [3] [4] ja kontrollid võltsimisohu vähendamiseks . . . . .                                     | 51 |
| 12 | Turvanõuded [3] [4] ja kontrollimeetmed teabe avalikustamise riskide vähendamiseks . . . . .               | 52 |
| 13 | Turvanõuded [3] [4] ja kontrollimehhanismid teenustõkestuse riskide maandamiseks . . . . .                 | 53 |
| 14 | Turvanõuded [3] [4] ja kontrollid õiguste vallutamise riskide maandamiseks . . . . .                       | 54 |
| 15 | Tööstusspionaaži riskijuhtimine, kohandatud allikast [28] . . . . .  | 63 |
| 16 | Petturlike töödega seotud riskijuhtimine, kohandatud allikast [28] . . . . .                               | 65 |
| 17 | Tahtliku sabotaaži riskijuhtimine, kohandatud allikast [28] . . . . .                                      | 67 |
| 18 | IP aadressi võltsimisega seotud riskijuhtimine . . . . .   | 74 |
| 19 | Andmete manipuleerimise riskijuhtimine . . . . .   | 77 |
| 20 | Vahendusrännaku riskijuhtimine . . . . .   | 79 |
| 21 | Teenustõkestuse rännaku riskijuhtimine . . . . .   | 80 |
| 22 | Mikrovigade sisestamise riskijuhtimine . . . . .   | 82 |

# 1 Sissejuhatus

Tänapäeval mõjutavad digitaliseerimine ja intelligentsed infrastruktuurid inimeste tööviise ja tööstussüsteeme oluliselt. Erinevates tootmisvaldkondades kasutatakse üha enam murrangulisi tehnoloogiaid nagu näiteks pilvepõhine andmetöötlus, plokiahelad, tehisintellekti (AI) ja masinõppe (ML) süsteemid ja automatiseeritud süsteemid. Nende tehnoloogiate laialdane kasutamine toob kaasa suure hulga andmete ja teabe loomise ning töötlemise, mida tuleb kasutada efektiivselt ja vajadusel teistele kättesaadavaks teha, et toetada õigete otsuste tegemist. Seetõttu peaks küberturvalisus olema digitaliseeritud protsesside ning automatiseeritud süsteemide ja tehnoloogiate puhul esmatähtis.

Eesti küberturvalisuse aastaraamat [17] toob esile murettekitava trendi, mille järgi on turvaohude ja -riskide arv märgatavalt suurenenud. Seda eriti institutsioonide ning teenust osutavate organisatsioonide seas. Kuna digitaliseerimine on jätkuvalt äri sektori fookuses, on organisatsioonide jaoks muutunud ülioluliseks oma turvameetmete tugevdamine. See hõlmab ettevalmistumist võimalikeks ohtudeks ning ennetavate strateegiatega riskide maandamiseks, et vältida halvimate stsenaariumite täitumist.

Käesolevas töös analüüsitakse automatiseeritud tootmissüsteemide konteksti, varasid, riske ja võimalikke vastumeetmeid. Eesmärgiks on saada ülevaade infoturbemeetmetest, mida tootmisüksustes rakendatakse. Erilist tähelepanu pööratakse väikestele ja keskmise suurusega ettevõtetele (VKE-d), kes juba kasutavad oma tootmisprotsessides erineval määral automatiseerimist. Selline rõhuasetus tuleneb sellest, et VKE-d on olulised majandusse panustajad [40], kuid sageli on neil piiratud ressursid arenenud ning turvalise infrastruktuuri loomiseks.

Analüüs on üles ehitatud järgnevalt: peatükis 2 selgitatakse uurimismeetodeid. Analüüsis järgitakse infosüsteemide turvalisuse valdkonna mudeli (ISSRM) põhimõtteid. Seda meetodit kasutatakse andmete kogumiseks läbi intervjuude, süstemaatilise kirjanduse analüüsi ja küsitluste automatiseeritud süsteemide ja tehnoloogiate turvaprobleemide kohta. Peatükis 3 määratletakse kontekst, kus arutatakse Tööstus 4.0 raamistiku referentsarhitektuuri mudeli üle, mis toob esile automatiseeritud süsteemide ja tehnoloogia põhikomponendid. Peatükis 4 antakse ülevaade asjakohastest standarditest. Peatükk 5 käsitleb varasid. Peatükk 6 käsitleb küberturvalisuse riske. Peatükis 7 tutvustatakse vastumeetmeid välja toodud riskide maandamiseks automatiseeritud süsteemides ja tehnoloogiates. Peatükid 8 ja 9 toovad välja kaks kasutusjuhtu, milleks on tootmistellimuste töötlemisel esinevate siseringi riskide analüüs ja tootmisprotsessides esinevate küberturvaohude analüüs. Peatükis 10 esitatakse kokkuvõtavad märkused.

## 2 Uurimismeetod

Selles peatükis määratleme uurimisküsimused ja kirjeldame uurimismeetodeid, mida rakendati automatiseeritud süsteemide ja tehnoloogiate küberturvalisust käsitlevate andmete kogumiseks ja analüüsimiseks. Töö aluseks on infosüsteemide riskijuhtimispõhine lähenemisviis. Valitud meetod on süstemaatiline viis konteksti ja varade määratlemiseks, turvariskide analüüsimiseks ning vastumeetmete valiku põhjendamiseks infosüsteemide riskide vähendamisel. Andmeid koguti kolme empiirilise uurimismeetodi abil:

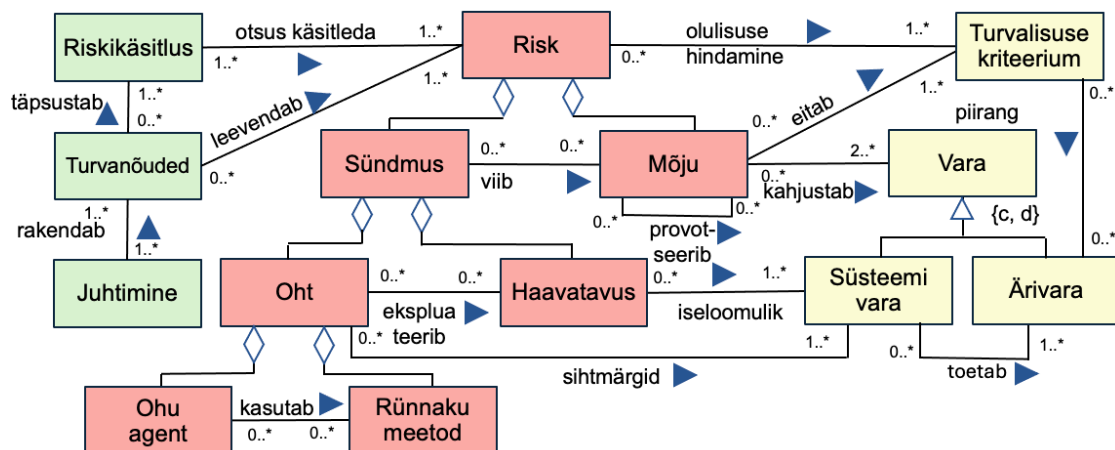
- intervjuud tootmisorganisatsioonide esindajatega,
- süstemaatiline kirjanduse analüüs,
- Eesti tootmisorganisatsioonides läbi viidud küsitlus.

Käesolevas peatükis kirjeldame uuringu etappe ja toome välja uuringu käigus kogutud andmed.

### 2.1 Turvariskide haldamine

Turvalisuse tagamine on protsess, mille eesmärk on vähendada tahtlikku kahju tekkimise riski olulistele varadele tasemeni, mis on süsteemi huvirühmadele vastuvõetav. See hõlmab ennetustööd ja pahatahtlikule tegevusele, väärkasutusele, ohtudele ja turvariskidele reageerimist[14].

Käesolevas analüüsis kasutame infosüsteemide turvariskide haldamise domeeni mudelit ISSRM (*Information Systems Security Risk Management*, vt Joonis 1) [11] [29]), mis koosneb kolmest peamisest kontseptsiooni grupist: varaga seotud kontseptsioonid, riskidega seotud kontseptsioonid ja riskikäsitlusega seotud kontseptsioonid. Ühe 2019 aastal läbi viidud uuringu [16] tulemuste kohaselt hinnati ISSRM'i üheks kõige pädevamaks mudeliks, mis rakendab ISO/IEC 27001 standardi nõudeid.



Joonis 1. ISSRM domeeni mudel, kohandatud allikast [11] [29]

**Varaga seotud kontseptsioonid** kirjeldavad, milliseid organisatsiooni varasid on oluline kaitsta ja millised kriteeriumid tagavad nende varade teatud turvalisuse taseme [11] [29]. Vara on midagi, millel on organisatsiooni jaoks väärtus ja mis mängib rolli organisatsiooni eesmärkide saavutamisel. Varad võib liigitada ärivaradeks ja süsteemi varadeks.

**Ärivar**a hõlmab teavet, protsesse, võimeid ja oskusi, mis on organisatsiooni ja tema põhiülesannete jaoks olulised ning tavaliselt on need immateriaalsed. Turvakriteerium (tuntud ka kui turvaomadus) iseloomustab turvavajadust ning on omadus või piirang, mis on seotud ärivaraga. Turvalisuse eesmärgid määratakse ärivarade turvakriteeriumide kaudu. Seega kirjeldavad turvakriteeriumid turvavajadusi, mida tavaliselt väljendatakse ärivarade konfidentsiaalsuse, tervikluse ja käideldavusega:

- **Konfidentsiaalsus** (*Confidentiality*) kirjeldab omadust, mille järgi ei tehta kättesaadavaks ega avalikustata informatsiooni volitamata isikutele, olemitele või protsessidele [11] [29]. Konfidentsiaalsus tegeleb teabe juurdepääsule ja teabe avalikustamisele seotud piirangute määramise ning säilitamisega. Muuhulgas hõlmab see vahendeid, mis tagavad privaatse ja konfidentsiaalse teabe kaitstuse. Konfidentsiaalsust võib ohustada näiteks võrguliikluse pealtkuulamine, mille tulemusena saavad selleks volitamata isikud juurdepääsu informatsioonile.
- **Terviklus** (*Integrity*) on ärivara täpsuse ja täielikkuse kaitstuse omadus [11] [29]. Täpsust võivad ohustada volitamata või soovimatud muudatused ja manipulatsioonid, samas kui täielikkust võib ohustada andmete muutmine või kustutamine. Terviklus kaitseb teavet ebaõige muutmise või hävitamise eest ning tagab teabe õigsuse ja autentsuse.
- **Käideldavus** (*Availability*) kirjeldab omadust, mille kohaselt midagi on kättesaadav ja kasutatav volitatud olemi nõudmisel või vajadusel [11] [29]. See tähendab, et on tagatud õigeaegne ja usaldusväärne juurdepääs teabele. Käideldavust võivad ohustada näiteks teenustõkestus rünnakud, kus süsteem on hõivatud libapäringutele vastamisega ning see takistab volitatud olemi juurdepääsu teabele.

**Süsteemi vara** on osa infosüsteemist või selle komponent, mis on organisatsiooni jaoks väärtuslik, kuna see toetab ärivarasid. Süsteemi vara võib hõlmata IKT-süsteemide komponente nagu riistvara, tarkvara või arvutivõrgud, aga ka isikuid või rajatisi, mis on süsteemiga seotud ja mängivad rolli selle turvalisuses. Infosüsteemide varad (välja arvatud tarkvara) on materiaalsed. Süsteemi varad võimaldavad organisatsiooni varade toimimist [29], hõlmates elemente, mis on vajalikud tehingute, teabe kogumise, säilitamise, hoolduse ja muude ärivaraga seotud funktsioonide jaoks. Steven Alter on oma teadustöös [2] välja toonud järgnevad infotöötlaste funktsioonid:

- **Teabe kogumine** erinevate vahendite abil, näiteks klaviatuuri, vöötkoodilugeja, digitaalse kaamera jne. Teabe kogumine võib toimuda mitmel erineval viisil, olenevalt sellest, millist tüüpi teavet kogutakse ja millist seadet või meetodit selleks kasutatakse.
- **Teabe edastamine** hõlmab teabe saatmist või jagamist erinevate vahendite abil, näiteks juhtmega või juhtmeta telefonid, internet jne. Teabe edastamine võib toimuda erinevate sidevahendite kaudu, olenevalt sellest, millist tüüpi teavet edastatakse.

- **Teabe hoiustamine** hõlmab teabe säilitamist erinevatel andmekandjatel või -vormingutes, näiteks kõvakettal, mälukaardil, andmebaasis jne. Teabe hoiustamine võib toimuda mitmel erineval viisil, olenevalt sellest, millist tüüpi teavet säilitatakse ja millist salvestusvahendit või -meetodit selleks kasutatakse.
- **Teabe pärimine** hõlmab teabe hankimist mis tahes füüsilisest seadmest või allikast. See võib hõlmata teabe küsimist või kogumist mis tahes seadmest või süsteemist, mis suudab andmeid genereerida või edastada. Pärimine võib toimuda erinevat tüüpi seadmetest, olgu selleks siis arvutid, nutiseadmed, masinad või muud füüsilised seadmed.
- **Teabe manipuleerimine** hõlmab teabe töötlemist, muutmist või analüüsimist erinevate meetodite abil. See võib hõlmata arvutusi, kombineerimist, statistiliste meetodite kasutamist ja muud teabe töötlemist. Teabe manipuleerimine võib toimuda tarkvara rakenduste, algoritmide või muude vahendite abil, olenevalt sellest, millist tüüpi manipuleerimist või analüüsi soovitakse teostada.
- **Teabe kuvamine** hõlmab teabe esitamist või väljastamist erinevatel seadmetel, näiteks monitoridel, printeritel jne. See protsess võimaldab kasutajatel või süsteemidel näha või saada juurdepääsu töödeldud või salvestatud teabele.

Kõik kuus funktsiooni - teabe jäädvustamine, edastamine, hoiustamine, pärimine, manipuleerimine ja kuvamine - on olulised süsteemi varade toimimiseks. Need funktsioonid võimaldavad andmete ja teabe kogumist, liikumist, töötlemist ning kuvamist vastavalt vajadustele ja protsessidele.

**Riskiga seotud kontseptsioonid** tutvustavad riski enda definitsiooni ja selle vahetute komponentide määratlusi [11] [29]. Risk on ohu ja ühe või mitme turvanõrkuse kombinatsioon, mis võib põhjustada varadele neid kahjustades negatiivset mõju. Ohu ja turvanõrkuse kombinatsioon moodustab riskisündmuse ning mõju on selle riski tagajärg. Mõju on riski potentsiaalne negatiivne tagajärg, mis väärab ärivaradele määratletud turvakriteeriumi ja kahjustab neid ohu realiseerumisel. Mõju võib avalduda infosüsteemide varade kihil, näiteks andmete hävimise või komponendi rikke kujul, või ärivarade kihil, väärtates turvakriteeriumid. Näiteks teabe konfidentsiaalsuse, protsesside tervikluse või andmete käideldavuse kadumisega. Lisaks võib üks mõju esile kutsuda erinevate mõjude ahelreaktsioone või teisi kaudseid mõjusid. Näiteks võib tundliku teabe konfidentsiaalsuse kadumine viia klientide usalduse vähenemiseni või sootuks kadumiseni.

**Riskisündmus** on ohu ja ühe või mitme nõrkuse kooslus. Nõrkus on omadus, mis paljastab mõne turvapuuduse infosüsteemi vara või varade rühma juures. Oht on intsident, mille on algatanud ohuallikas, kes kasutab ründemeetodit, et võtta sihikule üks või mitu infosüsteemi vara, kasutades ära nende nõrkusi. Ohuallikas on ohuagent, kellel on vahendid, et tahtlikult kahjustada infosüsteemi vara. Ohuagent tekitab ohu, seega on ta riski allikas. Ohuagenti iseloomustavad teadmised, ressurside olemasolu ja motivatsioon. Ründemeetod kirjeldab standardseid vahendeid, mida ohuallikas kasutab ohu tekitamiseks.

**Turvariskide analüüs** hõlmab ka turvaohude kaalumist. Käesolevas töös kasutame STRIDE (*Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege*) lähenemist [39], mis võimaldab tuvastatud ohtude kategoriseerimist iga mnemoonika

osa alla. Ohtude taksonoomia määratleb turvaohude tüübid esindatud elementide piires. STRIDE on akronüüm, mis lahti seletatuna tähendab järgmist:

- **võltsimine/teesklus/pettus** (*Spoofing*) - kellegi või millegi teisena esinemine,
- **muukimine/rikkumine** (*Tampering*) - millegi muutmine, mida ei peaks saama muuta,
- **salgamine** (*Repudiation*) - väitmine, et sa ei teinud midagi sõltumata sellest, kas see vastab tõe või mitte,
- **teabe avalikustamine** (*Information disclosure*) - teabe avaldamine osapooltele, kellel pole luba seda vaadata,
- **teenustõkestus/ummistus** (*Denial of service*) - rüüanded, mille eesmärk on takistada süsteemil ette nähtud teenust osutada,
- **õiguste vallutus** (*Elevation of privilege*) - programm või kasutaja suurendab enda õigusi ja saab teha asju (tehnilisi), mida ta ei peaks saama teha.

Need on loodud selleks, et aidata tarkvara arendajatel tuvastada tarkvara rünnakuid. Igale eelnevat ohule vastab turvanõue, mida see oht rikub:

- **võltsimine/teesklus/pettus** (*Spoofing*) - autentimine,
- **muukimine/rikkumine** (*Tampering*) - terviklus,
- **salgamine** (*Repudiation*) - salgamatus,
- **teabe avalikustamine** (*Information disclosure*) - konfidentsiaalsus,
- **teenustõkestus/ummistus** (*Denial of service*) - käideldavus,
- **õiguste vallutus** (*Elevation of privilege*) - autoriseerimine.

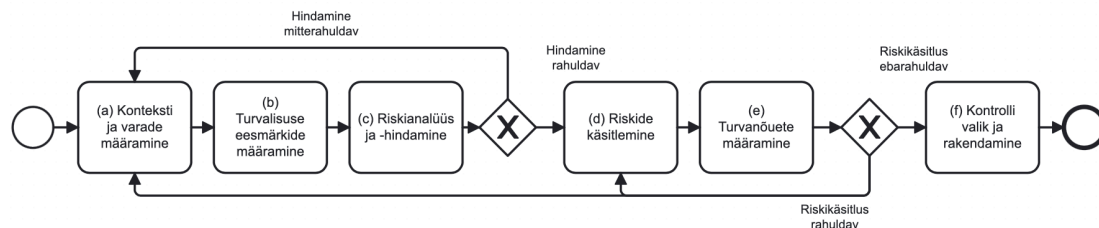
**Riskide käsitlemisega** seotud kontseptsioonid kirjeldavad riskikäsitluse kontseptsioone [11] [29]. Riski käsitlemise otsus on otsus, käsitleda tuvastatud riski. Käsitlus rahuldab turvavajaduse, mis on väljendatud üldises ja funktsionaalses mõttes ning täpsustatud turvanõuete suhtes. Riski saab käsitleda neljal eri viisil:

- **Riski vältimine** on otsus vältida riski tekkimist, võttes kasutusele meetmed, mis kõrvaldavad riski allikad või vähendavad nende mõju. See tähendab, et süsteemi funktsionaalsust muudetakse või sellest loobutakse, et vältida riski tekkimist või mõju.
- **Riski vähendamine** hõlmab meetmeid, mille eesmärk on vähendada riski teostumise tõenäosust, negatiivseid tagajärgi või mõlemat. Tavaliselt valitakse turvanõuded just riskide vähendamiseks.

- **Riski ülekandmine** on strateegia, mille käigus riski haldamise vastutus või osa sellest kantakse üle teisele osapooltele. See võib hõlmata lepinguliste tingimuste kehtestamist või kindlustuse sõlmimist, et leevendada võimaliku kahju mõju, mida riski teostumine võib kaasa tuua.
- **Riski säilitamine** kujutab endast otsust teadlikult aktsepteerida riski ja selle võimalikke tagajärgi, ilma et rakendataks täiendavaid meetmeid riski maandamiseks või vähendamiseks. Riski säilitamist võib pidada strateegiliseks valikuks, kui riski tekkimise tõenäosus on madal või kui riski mõju on talutav ning kulud riski maandamiseks või vältimiseks on suuremad, kui riski endaga kaasnevad kulud.

Turvanõue on tingimus keskkonna aspektidele, mille abil me soovime riskide taset vähendada [11] [29]. Turvanõuded täpsustavad riskide maandamise otsuseid. Kuigi riskide maandamise otsused võivad viia turvanõueteni, võib mõnikord olla vaja kohandada kolmandatele osapooltele esitatavaid turvanõudeid riskide ülekandmise otsuste kontekstis. Riski vältimine ja riski säilitamine ei vaja täiendavaid turvanõudeid. Iga turvanõue aitab katta ühte või mitut riskikäsitlemise aspekti analüüsitud süsteemis. Turva- või vastumeede on välja töötatud abinõu turvalisuse suurendamiseks läbi turvanõuete rakendamise. Turvameetmed võivad olla protsessid, poliitikad, seadmed, tavad või muud toimingud ja komponendid, mis aitavad vähendada riske.

**ISSRM-protsess** [11] [29] (Joonis 2) algab a) **organisatsiooni konteksti uurimisega ja selle varade kindlaks määramisega**. Selles etapis kirjeldatakse organisatsiooni, selle tegevuskeskonda ning süsteeme, mida organisatsioon kasutab. Seejärel tuleb varadele vajaliku kaitsetaseme alusel määrata b) **turvaeesmärgid**. Turvaeesmärgid on seotud ärivara konfidentsiaalsuse, teravikluse ja käideldavusega. Järgmine samm on c) **riskianalüüs**, mille käigus tuvastatakse ja hinnatakse võimalikke turvariske, mis võivad kahjustada varasid ja ohustada turvaeesmärke. Pärast riskianalüüsi tehakse otsused riskide d) **käsitlemise kohta** (riski vältimine, vähendamine, ülekandmine või säilitamine). Seejärel (e)) **selgitatakse välja tuvastatud riskide leevendamiseks vajalikud turvanõuded**. Lõpuks rakendatakse (f) **turvanõuded turvameetmetena**, mis on süsteemispetsiifilised vastumeetmed.



Joonis 2. ISSRM protsess, kohandatud allikast [11] [29]

Käesolevas analüüsis on kasutatud ISSRMi lähenemisviisi, et defineerida automatiseeritud süsteemide ja tehnoloogiate kontekst, riskid, turvanõuded ja vastumeetmed. Järgmises osas käsitleme uurimisküsimusi ja -meetodeid.

## 2.2 Uurimisküsimused

Automatiseeritud süsteemide ja tehnoloogiate analüüsi suunamiseks püstitame kuus uurimisküsimust:

1. Milline on automatiseeritud süsteemide ja tehnoloogiate kontekst?
2. Millised on automatiseeritud süsteemide ja tehnoloogiate väljakutsed?
3. Millised on automatiseeritud süsteemide ja tehnoloogiate alla kuuluvad kaitstavad varad?
4. Millised on automatiseeritud süsteemide ja tehnoloogiate turvariskid?
5. Millised turvanõuded ja meetmed on kohaldatavad automatiseeritud süsteemide ja tehnoloogiate riskide vähendamiseks?
6. Milliseid standardeid tuleks automatiseeritud süsteemide ja tehnoloogiate kasutamisel järgida?

Nendele küsimustele vastamiseks viisime läbi intervjuud valitud ekspertidega Eesti tootmisettevõtetest. Seejärel tegime süstemaatilise kirjanduse analüüsi. Lõpuks viisime läbi veebipõhise küsitluse ning kogusime andmeid Eesti tootmisettevõtelt. Kõigi kolme empiirilise uuringu aluseks on ISSRMi protsessi ja domeeni mudeli rakendamine.

## 2.3 Intervjuud

Intervjuude eesmärk oli uurida automatiseeritud süsteemide ja tehnoloogiate konteksti Eestis ning saada teavet infoturbe tavade praeguse olukorra kohta automatiseeritud tootmise valdkonnas. Selle uuringu tulemusi kasutati kahe teise empiirilise uuringu (st kirjanduse analüüs ja veebipõhine küsitlus) sisendina.

Intervjuud viidi läbi intervjuueeritavate emakeeles, mis hõlbustas loomulikku ja osavõtlikku dialoogi ning võimaldas neil tunda end mugavalt.

Intervjuude peamine eesmärk oli saada ülevaade hetkel kasutuses olevatest praktikatest. Selleks koostati struktureeritud küsimustik, et vältida vestluse kõrvalekaldumist uuritavast teemast. Sihilikult valiti suulised intervjuud kirjalike vastuste asemel, et vältida intervjuueeritavate vastuste ülemäärast silumist või ilustamist. Selle lähenemise eesmärk oli tagada tulemuste autentsus ja minimeerida vastuste kunstlikku kohandamist või moonutamist.

Ülevaatlike tulemuste saamiseks seati eesmärgiks läbi viia vähemalt kolm intervjuud. Kokku viidi edukalt läbi viis intervjuud. Intervjuude fookus oli suunatud väikestele ja keskmise suurusega ettevõtetele (VKEd) [12]. Et tagada arusaadavus eri keelte puhul, tõlgiti VKEde definitsioon eesti keelde. Tõlge oli oluline selleks, et tagada intervjuueeritavate arusaamine intervjuu ulatusest ja kontekstist.

Et tagada nende ühtsus, olid intervjuud poolstruktureeritud, kus arutelude juhtimiseks olid ette antud teemad ja alaküsimused. Selline lähenemisviis ei taganud mitte ainult intervjuude struktuurilist terviklikkust, vaid andis intervjuueeritavatele ka vabaduse spontaanselt jagada oma kogemusi ja vaatenurki. Osalejate nõusolekul salvestati iga intervjuu. Selline lähenemine hõlbustas täpsete

andmete kogumist, vältides vajadust samal ajal märkmeid teha, ja võimaldas intervjuerijal keskenduda täielikult intervjueritavale. Pärast iga intervjuud transkribeeriti helisalvestised sõnasõnalt ning kategoriseeriti vastavalt välja töötatud temaatilisele raamistikule, valmistades nii vastused ette analüüsiks. Vastuste analüüsimisel kasutati temaatilisi analüüsi meetodeid, mis võimaldasid vastuste kategoriseerimist ning nendes korduvate mustrite tuvastamist.

Tabel 1 kirjeldab intervjueritud ettevõtteid.

Tabel 1. Intervjueritud ettevõtted

|                        | <b>Töötajate arv 2022. aasta seisuga</b> | <b>Intervjueritava roll</b> | <b>Osa suuremast grupist</b> |
|------------------------|--|-----------------------------|------------------------------|
| <b>Intervjuu nr. 1</b> | 101 - 200                                | Tegevjuht                   | ei                           |
| <b>Intervjuu nr. 2</b> | 101 - 200                                | IT-juht                     | ei                           |
| <b>Intervjuu nr. 3</b> | 201 - 400                                | IT-spetsialist              | jah                          |
| <b>Intervjuu nr. 4</b> | 201 - 400                                | IT-juht                     | jah                          |
| <b>Intervjuu nr. 5</b> | 1 - 100                                  | Tegevjuht                   | ei                           |

### 2.3.1 Intervjuude teemad ja küsimused

- Automatiseeritud süsteemid ja seadmestiku käitlemine.
  - Milliseid automatiseeritud süsteeme teie tootmisprotsessides kasutatakse ning millised meetmed on võetud, et kaitsta neid volitamatu juurdepääsu või manipuleerimise eest?
  - Kas saaksite kirjeldada seadmestiku käitlemise ja hooldamise protseduure, sealhulgas tarkvara uuendamist, füüsilise turvalisuse tagamist ning võrgu isoleerimist?
  - Kuidas on teie ettevõttes korraldatud juurdepääsuõigused, eriti seoses kaugjuurdepääsuga või kolmandate osapoolte tarnijatega, kes suhtlevad kriitiliste süsteemidega?
- Üldine turvastrateegia.
  - Kas saaksite anda ülevaate oma ettevõtte küberturvalisuse strateegiast ja sellest, kuidas see on kooskõlas teie ärieesmärkidega?
  - Kuidas te hindate ja prioritseerite tootmissektorile omaseid küberriske ning milliseid raamistikke te kasutate riskide juhtimiseks?
  - Milliseid regulaarseid turvahindamisi või -auditeid viiakse läbi teie ettevõttes, et tagada vastavus kõige ajakohasemate standardite ja eeskirjadega?
- Ohuteadlikkus ja intsidentidele reageerimine.
  - Kas teie ettevõtte on kogunud küberohte või turvaintsidente? Kui jah, siis kuidas neid käsitleti ja milliseid olid õppetunnid?

- Kas saaksite kirjeldada oma ettevõtte intsidentidele reageerimise plaani ja seda, kuidas see on kohandatud teie tootmiskeskonna eripäraste probleemide lahendamiseks?
- Kuidas on korraldatud koostöö väliste osapooltega, nagu valitsus- või tööstusorganisatsioonid, et jagada ohuteavet ja parimaid tavasid?
- Andmevahetus ja terviklus.
  - Milliseid andmeid vahetavad teie ettevõtte süsteemid omavahel ja kuidas on need edastamise ajal krüpteeritud või muul viisil kaitstud?
  - Kas on mingi võimalus, et teie süsteemist saab andmeid varastada või nendega manipuleerida ning millised meetmed on rakendatud selliste juhtumite avastamiseks ja ennetamiseks?
  - Kuidas tagate andmete tervikluse ja käideldavuse, eriti süsteemi rikete või sihitud rünnakute korral?
- Töötajate koolitus ja väljaõpe.
  - Milliseid koolitus- ja teadlikkuse tõstmise programme kasutatakse töötajate koolitamiseks ja informeerimiseks uusimatest küberohtudest ja turvameetmetest?
  - Kuidas tagate, et turvateadlikkus on lõimitud ettevõtte kultuuri, eriti mitte-tehniliste töötajate seas, kes võivad kokku puutuda automatiseeritud süsteemidega?
- Nõuetele vastavus ja õiguslane teadlikkus.
  - Kas olete teadlikud õigusaktidest, standarditest või eeskirjadest, mis kehtivad teie tööstusharus seoses küberturvalisusega? Kuidas tagatakse nende nõuetele vastavus?
  - Millised protsessid on kehtestatud reguleerivate asutuste, õiguskaitseorganite või õigusnõustajate kaasamiseks küberintsidentide korral ning kuidas on ettevõtte siseselt määratletud vastutus?
  - Kuidas tasakaalustate turvalisuse vajadust muude äriliste kaalutlustega, nagu töö tõhusus, innovatsioon ja klientide usaldus?
- Tehnoloogia ja innovatsioon.
  - Kuidas peate sammu uute tehnoloogiate ja riskidega tootmissektoris ning kuidas need mõjutavad teie küberturvalisuse strateegiat?
  - Kas saate jagada oma kogemusi uuenduslike lähenemisviiside või tehnoloogiate kohta, mida olete rakendanud oma tootmisprotsesside turvalisuse suurendamiseks, nagu näiteks tehisintellekt, plokiahel või asjade internet?
  - Millised on teie tulevikuplaanid küberturvalisuse investeeringute ja arenduste osas, eriti arvestades töötleva tööstuse arenguid automatiseerimise ja ühenduvuse vallas?

## 2.4 Kirjanduse analüüs

Viisime läbi süstemaatilise kirjanduse analüüsi, järgides Kitchenham'i *et al.* [24] juhiseid. Eesmärk oli analüüsida kirjandust, mis käsitleb turvariske automatiseeritud süsteemides ja tehnoloogiates. Analüüsi käigus uurisime automatiseeritud tootmissüsteemide konteksti, määratlesime nende olemuse ja komponendid. Samuti tegime kindlaks nende turvavajadused, turvariskid, ning strateegiad ja meetmed (sealhulgas nõuded ja kontrollid) nende riskide vähendamiseks.

**Otsinguprotsess:** Teaduskirjanduse leidmiseks kasutasime digitaalseid raamatukogusid SCOPUS<sup>1</sup> ja Web of Science<sup>2</sup>. Otsingutes kasutasime võtmesõnu nagu "automatiseeritud tootmissüsteem", "küberturvalisus" ja "küberkaitse". Võtmesõnade ühendamiseks kasutasime Boole'i loogikaoperaatoreid vastavalt iga otsingumootori nõuetele. Tabelis 2 on välja toodud otsingu tulemused. Kokku leidsime 125 vastet (vt Tabel 2), millest valisime kaasamis- ja välistamiskriteeriumide alusel põhjalikumaks analüüsiks kümme (vt Tabel 3).

Tabel 2. Kirjanduse analüüsi valitud allikad ja vastavad tulemused

| Allikad                 | SCOPUS | Web of Science | Kokku |
|-------------------------|--------|----------------|-------|
| Tuvastatud              | 70     | 55             | 125   |
| Filter 1                | 29     | 23             | 52    |
| Filter 2 (lõplik valik) | 6      | 4              | 10    |

**Artiklite valik:** Viisime esialgsete tulemuste seas läbi analüüsi, mis hõlmas pealkirja, märksõnu, kokkuvõtet, tulemusi ja järeldusi. Sobilike tööde leidmiseks rakendasime uurimisküsimuste põhjal kahte filtrit:

1. Filter 1: Tabelis 3 on esitatud kaasamis- ja välistamiskriteeriumid, mille rakendamise tulemused on näha tabelis 2. Kriteeriumite rakendamise tulemusel leiti 52 sobivat teadustööd.
2. Filter 2: Esimese filtri läbinud tööde kvaliteeti hinnati vastavalt Kitchenhami kirjeldatud kvaliteedisuunistele [24], toetudes järgmistele küsimustele:
  - Kas artikkel hõlmab käesoleva analüüsi teemat ja ulatust?
  - Kas artiklis kirjeldatakse automatiseeritud tootmissüsteemide turvariske?
  - Kas artiklis on esitatud vastumeetmed kirjeldatud turvariskide vähendamiseks?

**Valitud tööd:** Esialgsest 125 artiklist jäeti kriteeriumide alusel välja 115 artiklit. Järele jäänud kümme artiklit analüüsiti põhjalikult, et neid kasutada uurimisküsimustele vastamiseks. Järgnevalt esitame ülevaate nendest valitud artiklitest, tuues esile nende vastavad kontekstid. Seejärel katalogiseerime igas artiklis viidatud standardid. Lõpuks pakume välja ühtse vaate igas artiklis käsitletud varadele, viies need vastavusse automatiseeritud süsteemide ja tehnoloogiate kontekstiga.

<sup>1</sup><https://www.scopus.com/home.uri>

<sup>2</sup><https://www-webofscience-com/wos/woscc/basic-search>

Tabel 3. Kaasamis-/väljaarvamiskriteeriumid valitud artiklite puhul

| Kaasamiskriteeriumid  | Väljastamiskriteeriumid   |
|---|---|
| Tööstusautomaatika valdkonna artiklid.  | Artiklid, mis keskenduvad automatiseeritud tootmissüsteemide turvalisuse mõnele kitsale valdkonnale.                      |
| Artiklid, mis konkreetselt keskenduvad turvariskide hindamisele või analüüsile. | Artiklid, mis keskenduvad automatiseeritud tootmissüsteemide ohutusabinõutele - tahtmatu kahju tekitamine sidusrühmadele. |
| Artiklid, mis esitavad lahendusi turvariskidele.                                | Artiklid, mis ei ole inglise keeles.  |
| Akadeemilised artiklid, mis on ülikooli kaudu täistekstina kättesaadavad.       | Artiklid, mis dubleerivad üksteist.   |

1. **Khalid et al.** "*Understanding vulnerabilities in cyber physical production systems*" [23]  
 Artikli eesmärk on süstemaatiliselt tuvastada riskiallikad ja esile tuua ohud küberfüüsilistes tootmissüsteemides, keskendudes ohutus- ja turvaaspektide integreerimisele. Eesmärk on aidata kaasa inimeste ja robotite koostöö (*Human-Robot Collaboration*) arengule ning integreerimisele tootmissüsteemidesse, eriti Tööstus 4.0 kontekstis. Uurimustöö keskseks kasutusjuhtumiks on autotööstus, kus tähtsateks töövahenditeks on suure kandevõimega raskerobotid. Artikkel uurib küberfüüsiliste tootmissüsteemide (*Cyberphysical production systems*) mudelit antud kasutusjuhtumi põhjal, kirjeldades üksikasjalikult tehnoloogianõudeid ja kasutatavat raamistikku. Simulatsiooni eesmärk on tuvastada süsteemi nõrkused, eriti küberrünnakute korral, mis võivad põhjustada ohutusprobleeme ja tõrkeid.

Artiklis tuvastatakse erinevad riskid ja ohud, mis on seotud küberfüüsiliste tootmissüsteemidega, eriti need, mis puudutavad raskete esemete töstmise robotite kasutamist tootmiskeskkonnas. Tulemused toovad esile nende süsteemide nõrkuse küberrünnakute suhtes ning nende võimaliku mõju ohutusele ja riketele. Simulatsiooniuringute abil näidatakse, kuidas küberrünnakud võivad ohustada ja häirida küberfüüsiliste tootmissüsteemide toimimist. Uuringu tulemused rõhutavad, et ohutus ja turvalisus peavad olema sügavalt integreeritud küberfüüsilistesse tootmissüsteemidesse, et kaitsta neid küberohtude eest ja tagada nende tõhus toimimine tööstuskeskkonnas.

2. **Urooj et al.** "*Risk Assessment of SCADA Cyber Attack Methods: A Technical Review on Securing Automated Real-Time SCADA Systems*" [41]  
 Artikkel võtab eesmärgiks luua põhjalik ülevaade SCADA (*Supervisory Control and Data Acquisition*) süsteemide ning tehnajuhtimissüsteemide küberturvalisuse riskihindamise meetoditest. Eesmärk on tuvastada võimalikud edasised uurimissuunad ja olemasolevad meetodid, mis keskenduvad automatiseeritud SCADA süsteemide riskide hindamise spetsiifikatele. Artiklis analüüsitakse mitmeid praegu kasutuses olevaid SCADA süsteemide küberturvalisuse riskihindamise meetodeid ning võrreldakse erinevaid lähenemisviise. Esitatakse nende meetodite peamised omapärased jooned ning analüüsitakse neid enamle-

vinud riskihindamise protsesside, analüüsimeetodite ja uurimisprobleemide seisukohast lähtuvalt.

Artiklis esile toodud peamised SCADA süsteemide riskid hõlmavad endas arvutivõrkude turvalisuse nõrkusi, krüptograafilisi puudujääke, SCADA süsteemide sätetest tulenevaid nõrkusi ja vigu juurdepääsu õiguste haldamisel. Autorid rõhutavad, et nende riskide vastu kaitsmiseks on oluline regulaarselt tugevdada turvameetmeid ja hoida süsteeme ajakohasena. Soovitatakse hoolikalt kavandada SCADA süsteemide võrgu arhitektuuri, et kaugkasutajatele oleks tagatud juurdepääs teabe seirele ja analüüsile vastavalt ettevõtte vajadustele, samas hoides juhtimissüsteeme isoleerituna välisest võrguliiklusest. Artiklis jõutakse järeldusele, et hetkel on küll olemas palju erinevaid riskihindamise meetodeid, kuid jätkuvalt eksisteerib puudusi. Eriti valdkondades nagu kasutajakontode krüpteerimine, rünnakute ning rikkumiste tuvastamine, inimfaktorid, hindamine ja kontroll ning tööriistade tugi. Autorid peavad vajalikuks luua kõiki riskijuhtimisprotsessi etappe hõlmav terviklik meetod.

3. **Thames et al.** "*Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems*" [27]

Artikli eesmärk on suurendada küberturvalisust CBDM (*Cloud-based Design and Manufacturing*) süsteemides. CBDM süsteemid on olulised kaasaegses tootarenduses ja tootmises ning vajavad oma mitmekesisuse ja internetipõhise küberfüüsilise olemuse tõttu tõhusaid küberturvalisuse meetmeid. Autorid pakuvad välja referentsarhitektuuri, mis kasutab globaalseid küberteabe vahetamise raamistikke dünaamilise küberturvalisuse tagamiseks CBDM süsteemides. Eriti tuuakse välja ülemaailmseid küberturbe teabe vahetamise platvorme, nagu näiteks TAXII (*Trusted Automated eXchange of Indicator Information*), mis aitab erinevatel organisatsioonidel jagada omavahel teavet pärast turvasündmusi.

Artiklis tutvustatakse DFAR (*Distributed Firewall and Active Response*) arhitektuuri, mis moodustab küberturvalisuse referentsraamistiku CBDM süsteemidele. DFAR toimib TDA (*Trusted Domain of Administration*) raames, kus iga olem on nii küberturvalisuse teabe tootja kui ka tarbija. Selle arhitektuuri eesmärk on dünaamiliselt kaitsta võrke, kasutades ära TAXII abil jagatud teavet. Artikkel demonstreerib, kuidas DFAR võib pakkuda praktilist, jagatud ja automatiseeritud küberturbe alast kaitset CBDM süsteemidele läbi globaalsete küberturbe teabe vahetamise platvormide.

4. **Clark et al.** "*Cybersecurity Issues in Robotics*" [8]

Artiklis keskendutakse robotite projekteerimise ja tootmise küberturvalisuse seni tähelepanuta jäänud aspektidele. Eesmärk on tuvastada praegused ja võimalikud tulevased küberturbe ohud robotitele eri kihtidel: riistvara, püsivara, operatsioonisüsteemid ja raketid. Lisaks uuritakse robotite vastu suunatud küberrünnakute majanduslikku mõju ja inimeste ohutusega seotud probleeme. Artiklis vaadeldakse erinevaid robotite tüüpe, nagu vanurite hooldusrobotid, droonid, automatiseeritud sõidukid ja tootmisrobotid, et avastada võimalikke nõrkusi.

Ohtude tõrjumiseks pakutakse välja mitmesuguseid vastumeetmeid, mis on suunatud robotsüsteemide eri kihtidele. Soovitatakse turvaprotseduure riistvara tootmise tarneahela

rünnakute korral ning tarnijate valideerimiseks. Püsivara ja operatsioonisüsteemide osas tehakse ettepanek leppida kokku standardeerimises ning luua konsortsium, mis teostaks platvormide turvalisuse järelvalvet. Rakenduste tasemel välja pakutud vastumeetmete hulka kuuluvad turvalise programmeerimise tavade järgimine ja tööriistade kasutamine, mis aitaks avastada ründeid rakenduse kasutamise ajal.

5. **Kutzler et al.** "*Boosting Cyber-Physical System Security*" [25]

Artiklis käsitletakse ettevõtete ja infrastruktuuri kasvava automatiseerimisega seotud probleeme ja riske, eriti küberturvalisuse kontekstis. Märgitakse, et praegused küberturvalisuse meetmed elutähtsates infrastruktuurides, näiteks võrgu- või sissetungi tuvastuse süsteemid, ei ole piisavad nende automatiseeritud süsteemide turvavajaduste rahuldamiseks. Samuti tuuakse välja, et puuduvad terviklikud vahendid ja lähenemisviisid, mis võimaldaksid hinnata võimalikke ohte automatiseeritud lahenduste kavandamisel.

Eesmärgiga kõrvaldada kirjeldatud puudused, töötasid artikli autorid AUTOSEC projekti raames välja täiustatud küberturvalisuse riskijuhtimise protsessi mudeli. See mudel põhineb USA Riikliku Standardi- ja Tehnoloogiainstituudi (NIST) elutähtsa infrastruktuuri küberturvalisuse parandamise raamistikul (*Framework for Improving Critical Infrastructure Cybersecurity*) ning hõlmab nii põhi kui ka tugi haldusfunktsioone. Mudeli eesmärk on olla kasutajasõbralik, ühilduv olemasolevate standarditega ning kohandatav erinevate tööstusharude kasutusjuhtudeks. Lisaks võetakse mudelis arvesse turvalisuse seisukohalt olulisi küberfüüsiliste süsteemide ainulaadseid omadusi, nagu kontekstiteadlikkus, dünaamiline topoloogia ja hajutatud organisatsiooniline struktuur.

6. **Quarta et al.** "*An Experimental Security Analysis of an Industrial Robot Controller*" [35]

Artiklis keskendutakse tööstusrobotika kontrollerite turvalisusele, mis on ülioluline automatiseeritud tootmis- ja logistikaprotsesside jaoks. Arvestades nende süsteemide kasvavat keerukust ja omavahelist seotust, on eesmärgiks süstemaatiliselt analüüsida ja hinnata nende süsteemide nõrkust küberrünnakute suhtes, mis on suhteliselt vähe uuritud valdkond. Artikkel käib välja domeenispetsiifilise ohuagendi mudeli, et uurida, kuidas tarkvara nõrkuste ära kasutamine võib viia füüsiliste tagajärgedeni. Antud lähenemine hõlmab tööstusrobotite standardarhitektuuri uurimist ja võimalike ründevektorite tuvastamist. Hinnatakse erinevate rünnakute mõju robotite funktsionaalsusele, nagu näiteks ohutusmeetmete õõnestamine ja liikumise täpsuse vähendamine.

Rõhutatakse tööstuslike robotite suurevat ohtu küberrünnakutele, mis tuleneb lõimitusest laiematesse IKT ökosüsteemidesse nende programmeerimiseks, hoolduseks ja integreerimiseks. Tuvastatakse mitmeid nõrkusi, mis võivad põhjustada olulisi häiringuid töös ja ohutuses, sealhulgas nõrk krüpteerimine, ebapiisav tervikluse kontroll ja puudulik juurdepääsukontrolli süsteem. Rõhutatakse vajadust kaitsta robotivõrke ja sidesüsteeme manipuleerimise eest ning pakutakse välja mitmeid vastumeetmeid nende riskide vähendamiseks. Jõutakse järeldusele, et hoolimata olemasolevatest turvameetmetest on vaja täiendavaid uuringuid ja parandusi sellistes valdkondades nagu volituste krüpteerimine, rünnakute ja rikkumiste tuvastamine ning inimfaktorid robotite programmeerimisel ja juhtimisel.

7. **Jablonski et al.** "A Case Study in the Formal Modeling of Safe and Secure Manufacturing Automation" [21]

Artiklis tutvustatakse juhtumiuuringut, kus kasutatakse formaalseid meetodeid ohutuse ja turvariskide hindamiseks automatiseeritud tootmissüsteemides. Põhirõhk on erinevate metodoloogiate tõhususe uurimisel ja hindamisel automatiseeritud tootmissüsteemidega seotud riskide tuvastamiseks, prioritseerimiseks ja leevendamiseks. Rakendatakse formaalseid meetodeid, nagu ühtne modelleerimiskeel (UML), lineaarne temporaalne loogika, arhitektuuri analüüsi- ning projekteerimiskeel (*Architecture Analysis & Design Language*) ning vea- ja ründe puud. Neid meetodeid kasutatakse automatiseeritud tootmissüsteemide käitumise ja omaduste modelleerimiseks ning analüüsimiseks, luues aluse tootmisseadmete formaalseks kontrollimiseks kogu tootmisprotsessi elukaare ulatuses. Näitena käsitletakse alumiiniumpurgi automatiseeritud tootmissüsteemi juhtumiuuringut, kus analüüsitakse selle töökäiku ja riskitegureid.

Artiklis antakse üksikasjalik kirjeldus 12 omavahel ühendatud jaamast koosnevast automatiseeritud tootmissüsteemist, mille eesmärgiks on materjalide töötlemine ja alamkomponentide tootmine. Rõhutatakse jaamadevaheliste loogikavoogude korraldamise keerukust ning sellega seotud ohutus- ja turvariske. Formaalse meetodite kasutamisel tuvastati võimalikud ohutus- ja turvaprobleemid automatiseeritud tootmissüsteemis, peamiselt keskendudes purkide kesti tootvatele komponentidele. Arhitektuuri analüüsi- ning projekteerimiskeele kasutuselevõtt võimaldas autoritel luua olekupõhiseid käitumisspetsifikatsioone, et defineerida süsteemiseseid andmevooge, leida vigu ning analüüsida rikkeid ning võimalikke ründeid. See lähenemine võimaldas struktureeritud analüüsida süsteemi nõrkusi, pakkudes ülevaadet vigade ja rünnakute tõenäosusest ning nende mõjust kogu süsteemi üldisele ohutusele ja turvalisusele.

8. **Chundhoo et al.** "Cybersecurity Risks in Meat Processing Plant and Impacts on Total Productive Maintenance" [7]

Artikkel uurib Austraalia lihatööstuse küberturbe riske, eriti neid, mis mõjutavad asjade interneti põhiseid lihatöötlemise süsteeme. Keskendutakse uurimisele, kuidas need ohud mõjutavad üldist lihatoodete kvaliteeti ja ohutust ning tootmisprotsesside tõhusust. Artikkel kasutab juhtumiuuringu lähenemisviisi, keskendudes ohumudelite abil tuvastatud asjade interneti põhise lihatöötlussüsteemi ohtude erinevatele tasemetele. Uuritakse võimalike küberrünnakute mõju süsteemi kontrolleritele, eriti protsessidele, mis on toodete kvaliteedi ja ohutuse tagamise seisukohast äärmiselt olulised.

Küberrünnakud asjade interneti süsteemidele mõjutavad negatiivselt seadmete üldist efektiivsust (OEE), mis on oluliseks näitajaks seadmete tulemusliku hooldussüsteemi (TPM) jaoks. Küberohtudest tulenevad kõikumised protsessi järjestustes või parameetrites, nagu toote temperatuur, võivad tekitada olulisi probleeme toote kvaliteedis. Nende riskide vähendamiseks tehakse ettepanek integreerida küberturvalisus olemasolevasse TPM raamistikku, et suurendada lihatööstusettevõtetes kasutusel olevate asjade interneti süsteemide vastupidavust ja turvalisust küberohtude vastu. Uuritakse ka TPM-i juurutamise probleeme ning lahendusi edukaks implementeerimiseks, rõhutades nõrkuste ennustamise tähtsust asjade interneti süsteemides, kus teostatakse OEE seiret.

9. **Shah et al.** "A survey on Classification of Cyber-attacks on IoT and IIoT devices" [38]

Artiklis keskendutakse asjade interneti seadmete ja tööstuslike asjade interneti seadmete, mis on muutunud lahutamatuks osaks tänapäeva elust ja tööstusest, turvalisusega seotud probleemidele. Nende seadmete integreerimine eri sektoritesse, eriti Tööstus 4.0 raames toimivas automatiseeritud tootmises, muudab need potentsiaalseteks küberrünnakute sihtmärkideks.

Artiklis antakse ülevaade tööstuslike asjade interneti süsteemide kihilisest ülesehitusest, käsitledes põhjalikult iga kihi komponente ja võimalikke rünnakuid. Selgitatakse, kuidas infotehnoloogia ja operatsioonitehnoloogia integreerimine tööstuslikku asjade interneti loob keerukaid turvaauke. Rõhutatakse jõuliste turvameetmete vajadust mitmesuguste küberrünnakute, sealhulgas pahavara, autentimisrünnakute, andmepüügi, SQL-süstimise, DNS-i võltsimise ja veebirakenduste rünnakute vastu.

Ohtude leevendamiseks soovitatakse rakendada tugevamaid paroole, regulaarselt tarkvara uuendada, luua segmenteeritud võrke, kasutada tugevamat krüpteerimist, muuta vaikumisi seadistusi, rakendada mitmefaktorilist autentimist, teha regulaarseid varukoopiaid ning kasutada virtuaalseid privaatvõrke. Lisaks rõhutatakse vajadust jätkata standardite loomisega ja teha edasisi teadusuuringuid andmeturbe valdkonnas, et tõhusamalt reageerida asjade interneti ja sellega seotud küberohtude kiiresti muutuvale maastikule.

10. **Pu et al.** "Security of Industrial Robots: Vulnerabilities, Attacks and Mitigations" [34]

Artiklis uuritakse tööstuslike robotite, mis on kriitilised komponendid intelligentsetes ja automatiseeritud tootmissüsteemides, turvaauke. Eesmärk on analüüsida ja teha kokkuvõtte tööstusrobotite nõrkustest, võimalikest küberrünnakutest ja olemasolevatest turvalahendustest, arvestades robotite turvalisuse suurendamisega seotud väljakutseid ja raskusi. Artikkel sisaldab põhjalikku analüüsi tööstusrobotite püsivara ja juhtimismoodulite nõrkustest ning nende turvalisuse võrdlust traditsiooniliste infotehnoloogiliste süsteemidega. Hindamisel käsitletakse mitmeid aspekte, sealhulgas ülesandeprogrammide nõrkusi, sidevõrkude nõrkusi ja juurdepääsukontrolli süsteemide puudusi. Lisaks vaadeldakse robotite sidevõrkude ja juhtimissüsteemide praeguseid turvameetmeid ja krüpteerimismeetodeid.

Tööstusrobotite nõrkuste hulgas tuvastatakse mitmeid probleeme, näiteks nõrk krüpteerimine, ebapiisav tervikluse kontroll ning puudulikud juurdepääsukontrolli süsteemid. Need nõrkused loovad võimalused erinevateks küberrünnakuteks, sealhulgas pahatahtlik programmeerimine, andmete manipuleerimine ja omavolilised toimingud. Artikkel toob esile selliste rünnete võimalikud tagajärjed, nagu tundlike andmete kompromiteerimine ja roboti töö segamine, mis võivad nende süsteemide küberfüüsilise olemuse tõttu põhjustada reaalselt kahju.

## 2.5 Küsitlus

**Küsimustik:** Küsitluse eesmärk oli saada ülevaade automatiseeritud süsteemide ja tehnoloogiate hetkeseisust ning nende turvalisuse tasemest Eestis. Selleks loodi veebipõhine küsimustik, mis koosnes 19 küsimusest. Küsimustiku sisu on toodud Lisas II.

Küsimustiku sisu hõlmas erinevaid teemasid, sealhulgas organisatsiooni suurust (küsimused 1 ja 2), tootmisvaldkonda (küsimus 3), vastaja rolli organisatsioonis (küsimus 4) ja teavet organisatsiooni automatiseerituse taseme kohta (küsimus 5). Küsimustik keskendus automatiseeritud tootmisele ja sellega seotud turvalisuse probleemidele.

Küsimustikus käsitletakse automatiseeritud tootmist seitsmes küsimuses. Soovisime saada ülevaadet organisatsiooni suhtumisest automatiseeritud tootmissüsteemide haldamisse (küsimus 6), nende süsteemides viimase viie aasta jooksul toimunud arengutest (küsimus 7), peamistest probleemidest nende kasutamisel (küsimus 8), hallatavast teabest (küsimus 9), infotehnoloogia kasutamise eesmärkidest automatiseeritud tootmisprotsessides (küsimused 10 ja 11) ning kas organisatsioon järgib mingit arhitektuuri raamistikku automatiseeritud süsteemide ja tehnoloogiate puhul (küsimus 12).

Turvalisuse probleeme käsitletakse viies küsimuses. Küsisime kuidas organisatsioonis käsitletakse turvalisusega seotud teemasid (küsimus 13), milliseid eeskirju ja standardeid järgitakse (küsimus 14), kas organisatsioonis on esinenud turvariske või -ohte (küsimus 15), milliseid vastu-meetmeid rakendatakse (küsimus 16) ja milliseid koolitusi organisatsioonis turvalisuse teemadel läbi viiakse (küsimus 17).

Kaks viimast küsimust olid avatud küsimused, kus valikvastuseid ei olnud ette antud. Küsimus 18 palus vastajatel jagada oma kogemusi automatiseeritud süsteemide turvalisusega teemadel, mis jäid eelnevate küsimustega katmata. Viimase küsimusega küsiti, kas vastaja on huvitatud tulevikus võimalikust koostööst.

**Küsitlus:** Küsitlus viidi läbi ajavahemikul 12. veebruarist kuni 31. märtsini 2024. aastal Eestis. Küsitluses osalema kutsuti Tartu Ülikooli arvutiteaduse instituudi uudiskirja ja sotsiaalmeediaplattformide kaudu, samuti läbi AIRE<sup>3</sup> uudiskirja, sotsiaalmeediakanalite ja isiklike sotsiaalmeediakontode. Küsitluse sihtrühmaks olid digitaliseerimise teekonnal olevad väikesed ja keskmise suurusega tootmisettevõtted (VKEd).

Küsitluses osales kokku 90 inimest, kellest 20 lõpetasid küsitluse, vastates kõikidele küsimustele. Nende 20 vastaja hulgas oli kaks mikroettevõtet, seitse väikest ettevõtet, üheksa keskmise suurusega ettevõtet ja kaks, mis kuulusid muudesse kategooriasse (vt Joonis. 3). 20st osalenud ettevõttest 8 olid osa suuremast kontsernist või konglomeraadist.

Küsitluse tulemused ei näidanud, et vastajad oleksid kuulunud ülekaalukalt ühte kindlasse sektorisse. Nagu näitab Joonis 3, olid vastajaid erineva taustaga. Sarnast mitmekesisust märgati ka vastajate rollides, nagu on näidatud Joonisel 4.

## 2.6 Ohud valiidsusele

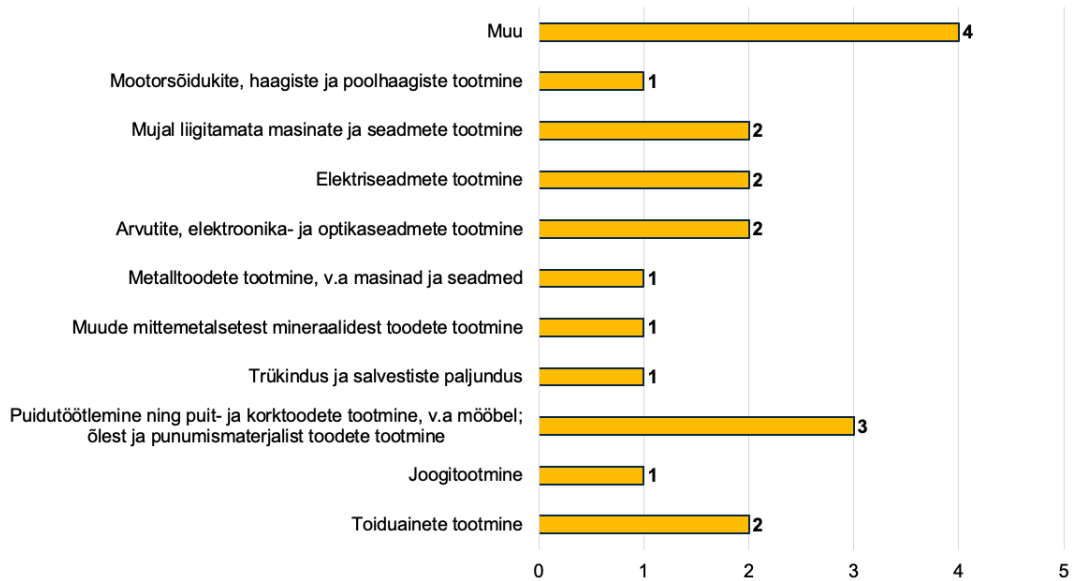
Alljärgnevalt vaatleme võimalikke probleeme, mis võivad ohustada käesoleva analüüsi valiidsust.

**Instrumendi valiidsus:** On oht, et intervjuude, kirjanduse analüüsi ning küsitluse läbi viimiseks kasutatud meetodid ja vahendid, nagu küsimustikud ja andmete kogumise vormid, võivad olla ebatäpsed. See tekitab küsimuse, kas saadud tulemused aitavad kaasa järelduste tegemiseks vajalike täpsete andmete ja teabe saamisele. On oht, et võimalikud piirangud nendes tööriistades võivad viia ebatäieliku või kallutatud andmekogumiseni, mis omakorda võib mõjutada käesoleva

---

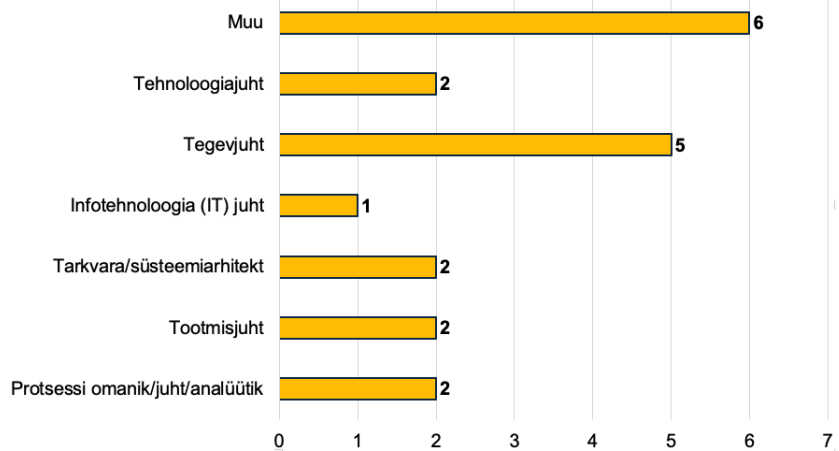
<sup>3</sup><https://aire-edih.eu/en/>

### Milline on teie organisatsiooni tootmiskategooria?



Joonis 3. Organisatsioonide tootmiskategooria

### Milline on teie positsioon/roll organisatsioonis?



Joonis 4. Vastajate rollid

töö üldiseid leide. Selle riski maandamiseks läbisid uurimisrühmas välja töötatud vahendid põhjaliku analüüsi ning koguti tagasisidet ka välistelt osapooltelt. Lisaks viidi läbi väike pilootanalüüs, et hinnata kasutatud küsimustikku.

**Järelduste valiidsus** puudutab uurimisandmetest tulenevate järelduste usaldusväärsust. See hõlmab andmete analüüsimisel kasutatud meetodite kontrollimist, eriti intervjuude vastuste tõlgendamisel ja kirjandusest saadud tulemuste sünteesimisel. Peamine risk seisneb kolmes

empiirilises etapis kogutud kvalitatiivsete andmete subjektiivses tõlgendamises ja täpsuses. Riski maandamiseks vaatasime läbi ja ühtlustasime andmed kõigis kolmes etapis, tagades nende kooskõla erinevatest vaatenurkadest (intervjuud, kirjandus ja küsitlused). Antud lähenemine võimaldas valideerida tehtud järeldusi, arvestades erinevaid perspektiive.

**Sisemine valiidsus** käsitleb uuringus kindlaks tehtud põhjuslikke seoseid. Süstemaatiline kirjanduse analüüs uurib seoseid erinevate uuringute tulemuste vahel. Intervjuude puhul keskendatakse intervjuude andmete ja uurimisküsimuste vahelistele seostele. Sisemine valiidsus võib olla ohustatud, kui need seosed ei ole selgesõnalised või ei ole empiiriliselt põhjendatud. See võib viia valede eeldusteni põhjus-tagajärg seoste kohta. Selle riski maandamiseks vaadeldi läbi empiiriliste uurimismeetodite etapid ja nende seosed sihtuuringute meetoditega.

**Väline valiidsus** on seotud uurimistulemuste üldistatavusega. See küsimus käsitleb, kas intervjuude, kirjanduse analüüsi ja küsitluse tulemusi saab kohaldada teiste kontekstide või elanikkonna rühmade suhtes. Peamine oht seisneb selles, et valitud kirjanduse spetsiifilisus ja intervjuueeritud ettevõtete omapärad võivad piirata järelduste laiemat rakendatavust või kehtivust erinevates organisatsioonilistes keskkondades. Siiski peame seda ohtu üsna piiratuks, kuna andmete allikad on hoolikalt üle vaadatud ning saadud tulemused ja järeldused on üldistatavad ka teistele kontekstidele.

### 3 Automatiseeritud süsteemide ja tehnoloogia kontekst

Selgitame käesolevas jaotises automatiseeritud süsteemide ja tehnoloogiate mõistet, mis võib hõlmata erinevaid vaatenurki alates tööstusrobotitest kuni automatiseeritud tootmislahendusteni. Lisaks tutvustame erinevaid automatiseerituse tasemeid ja tutvustame RAMI 4.0 mudelit – Tööstus 4.0 referentsarhitektuuri mudelit, et selgitada automatiseeritud süsteemide ja tehnoloogiate konteksti. Samuti toome esile mõningad väljakutsed, millega tootmisorganisatsioonid võivad potentsiaalselt kokku puutuda.

#### 3.1 Automatiseeritud süsteemide ja tehnoloogiate definitsioon

**Ajalooline ülevaade:** Artiklis [1] on koostatud põhjalik ülevaade automatiseeritud süsteemide ja tehnoloogiate ajaloost ning arengust. Algsed automatiseerimise kontseptsioonid tekkisid juba 1947. aastal ning neid hakati esmalt rakendama Fordi autode koosteliinidel [1]. Eesmärgiks oli tehnoloogia kasutamine tootmises efektiivsuse tõstmiseks. 1997. aastal käsitleti automatiseerimist kui tavapärastel inimeste poolt läbi viidud toimingute asendamist seadmetega, sealhulgas arvutitega [1]. See muutus mõjutas oluliselt töötingimusi ja inimese rolli tööstussektoris, kus otsestest operaatoritest said projekteerijad, hoolduspersonal või juhendajad. Aastal 2016 kirjeldati automaatikat kui süsteemi, mis täidab konkreetseid ülesandeid vastavalt ette nähtud programmile, ilma võimeta autonoomselt võtta vastu otsuseid või muuta oma toimingut. Sellised süsteemid toimivad vastavalt eelnevalt kindlaks määratud toimingutele, ilma et nad suudaksid neid toiminguid kohandada või muuta. Praegused tehnoloogilised pingutused tootmises keskenduvad tootmisliinide arendamisele, mis on võimelised kohanduma erinevate toodete ja erinevate tootmismahtudega [1].

**Definitsioon:** Pärast ajaloolise tausta ülevaadet automatiseeritud süsteemide ja tehnoloogiate kohta, toome Tabelis 4 välja peamised mõisted, alates tööstusrobotitest kuni automatiseeritud tootmissüsteemideni. Käesolevas analüüsis järgime järgmist definitsiooni:

**Automatiseeritud süsteemid ja tehnoloogiad** tootmissektoris on omavahel ühendatud toimimisseadmete (nagu tööstusrobotid ja arvutiseadmed) võrgustik, mis hõlmab endas projekteerimist, planeerimist, logistikat, tootmist, ladustamist ja müüki. Need süsteemid võimaldavad automatiseerida funktsioone, mida tavaliselt täidavad inimesed, suurendades seeläbi tõhusust ja tootlikkust tootmisprotsessi eri etappides.

Automatiseeritud süsteemid ja tehnoloogiad võivad olla erinevatel automatiseerimise tasemetel, nagu on defineeritud artiklis [15]. Automatiseerimise tasemed on järgmised:

- **Täielikult manuaalne** - käsitsi töö, mis ei kasutata mingeid tööriistu, vaid ainult töötajate lihasjõudu.
- **Staatiline käsitööriist** - käsitsi töötamine staatilise(te) tööriista(de) toel.
- **Paindlik käsitööriist** - käsitsi töötamine paindliku tööriista toel.
- **Automaatne käsitööriist** - käsitsi töötamine automatiseeritud tööriista toel.

Tabel 4. Seotud definitsioonid

| Termin   | Kirjeldus  | Allikas |
|--|--|---------|
| Tööstusrobotid   | Tööstusroboteid kasutatakse intelligentsetes ja automatiseeritud tootmiskeskondades, täites füüsilisi ülesandeid, näiteks asjade töstmist ja paigutamist. Nende ülesannete täitmist juhivad tootmissüsteemides teised seadmed, toetudes tootmisvõrgule.  | [34]    |
| Küber-füüsilised süsteemid (CPS)                               | Need süsteemid hõlmavad erinevaid riist- ja tarkvarakomponente, nagu mehaanilised täiturid, kontrollid, andurid, juhtimisloogika, püsivara ja operatsioonisüsteemid.   | [35]    |
| Manussüsteemid   | Need süsteemid on integreeritud laiemasse struktuuri ja loodud konkreetsete funktsioonide täitmiseks. Iga süsteem koosneb riist- ja tarkvarakomponentide ning mehaaniliste elementide kombinatsioonist. Robotid koosnevad mehaanilistest konstruktsioonidest, anduritest, ajamitest ja arvuti tarkvarast, mis jälgib ja kontrollib neid komponente.  | [8]     |
| Küberinfrastruktuuri elemendid (küber-füüsilistes süsteemides) | Näiteks arvutuslikud protsessid, kontrollalgoritmid, otsussüsteemid ja andmebaasid, ka füüsilised infrastruktuuri komponendid (st füüsilised protsessid ja elemendid). Need komponendid on omavahel ühendatud andurite ja täituri abil. Need süsteemid võivad intelligentsetes võrgustikus ühendada füüsilisi ja virtuaalseid protsesse ning omavad funktsionaalsust, et ise jälgida nii enda kui ka teiste küber-füüsiliste süsteemide seisundit.                                   | [25]    |
| Automatiseeritud tootmissüsteem                                | Need koosnevad omavahel seotud jaamadest, millest igaüks on spetsiaalselt struktureeritud materjalide töötlemiseks ja alamkomponentide või osaliselt valmis lõpptoote osade tootmiseks. Nende komponentide edasine töötlemine toimub järgmistes tööpiirkondades. Selleks, et tagada sujuv tootmisprotsess, on vaja hallata jaamadevahelisi loogikavoogusid. Sellist kontrolli pakub juhtimismehhanism, mis koordineerib tootmisahelas erinevate jaamade funktsioone sidevõrgu kaudu. | [21]    |

- **Staatiline masin/töökoht** - automaatne töö seadmega, mis on ette nähtud konkreetse ülesande täitmiseks.
- **Paindlik masin/töökoht** - automaatne töö seadmega, mida saab ümber seadistada erinevate ülesannete jaoks.
- **Täielikult automaatne** - automaatne töö, kus seade lahendab ise kõik tekkinud kõrvalekalded või probleemid.

## 3.2 Tööstus 4.0 arhitektuuriline mudel

Tööstus 4.0 arhitektuuriline domeenimudel (*Reference Architectural Model Industrie 4.0, RAMI 4.0*) on strateegiline raamistik, mis on välja töötatud Tööstus 4.0 algatuse raames [10]. RAMI 4.0 on tootmise ja tööstussektori digitaalse transformatsiooni juhtarhitektuur, mis on neljanda tööstusrevolutsiooni ajastul keskse tähtsusega.

Tööstus 4.0, mis sai alguse Saksamaa valitsuse algatusest, esindab tööstuses paradigma muutust, mis rõhutab digitaaltehnoloogia integreerimist tootmisprotsessidesse [33]. RAMI 4.0 töötasid koostöös välja Saksa Elektri- ja Elektroonikatootjate Liit (ZVEI), Saksa Standardiinstituut (DIN) ning VDI/VDE mõõtmiste ja automaatkontrollide selts. See arenes välja vajadusest standardiseerida ja struktureerida Tööstus 4.0 integreerimisprotsessi. RAMI 4.0 põhieesmärk on luua ühtne raamistik, mis hõlmab kõiki tööstusliku väärtusahela aspekte, tagades järjepidevuse, koostalitlusvõime ja tõhusa teabevahetuse digitaliseeritud tööstuskeskkondades. RAMI 4.0 on esitatud kolmemõõtmelise kaardina, kus teljed kujutavad tööstussüsteemi erinevaid kihte [22][42][31], alates füüsilistest varadest ja nende integreerimisest võrkudesse kuni andmeanalüüside ja ärimudelite rakendamiseni.

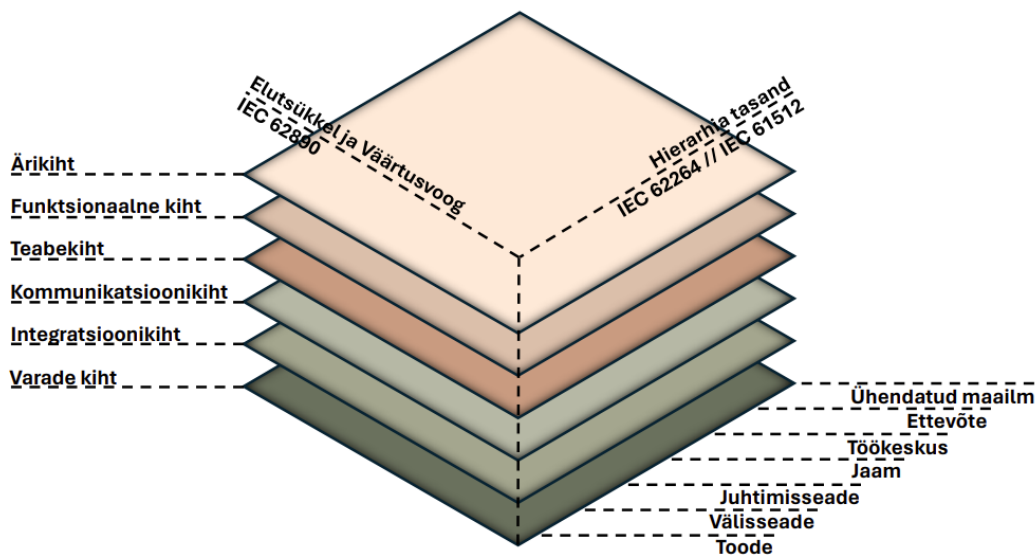
RAMI 4.0 eesmärk on olla paindlik, kergesti laiendatav ja liidetav teiste tootmisarhitektuuridega. Nagu kirjeldab artikkel [42], võib iga tootmisettevõtte leida oma koha selles kolmetasandilises arhitektuuris. Olulised standardid RAMI 4.0 kontekstis on:

- **IEC 62890**, mis käsitleb elutsükli staatust,
- **ISO/IEC 62264**, mis käsitleb ettevõtte juhtimissüsteemi integreerimist,
- **IEC 61512**, mis käsitleb partiide kontrollimist.

Muud seotud standardid on IEC 62541, IEC 61784, VDMA 24582, IEC 61987 ja ISO/IEC 20140 [42]. Varasemate tootmisarhitektuuride võrdluste põhjal peetakse RAMI 4.0 alusstandardiks [42], [31]. Autorid [22] on samuti määratlenud RAMI 4.0 kui standardiseeritud, kihipõhist ettevõtte arhitektuuri.

**RAMI 4.0 Hierarhia tasandi telg** on tuletatud Rahvusvahelise Elektrotehnilise Komisjoni (IEC) tehase projekteerimise referentsarhitektuurist. See liigitab tööstusprotsesside elemendid seitsmele tasandile:

- **Toode:** Toode on tulemus, mis tuleneb tootmisprotsessist.
- **Välisseade:** Need on riistvara komponendid, nagu andurid ja täiturid, mis koguvad keskkonna väärtusi.
- **Juhtimisseade:** Juhtimisseadmed, nagu programmeeritavad loogikakontrollerid (PLC-d) ja juhtimisarvutid (DC-d), võtavad vastu anduritest saadud andmed ja edastavad juhtimiskäskude süsteemi juhtimiseks.
- **Jaam:** See on koht, kus haldusõigustega kasutaja jälgib tööstustegevust ning haldab protsesse ja sündmusi, näiteks SCADA süsteem.



Joonis 5. RAMI 4.0 arhitektuuri mudel, kohandatud allikast [10]

- **Töökus:** Tagab andmete salvestamise, teabe ja analüüsi, mis põhineb ajaloolistel andmetel.
- **Ettevõte:** Kogu teabe haldamiseks ja kasumlike äriotsuste tegemiseks jälgitakse ettevõtte tasandit, mis hõlmab toodangu ja tellimuste jälgimist ning kulude ja tulude suhet, ning juhib tootmise planeerimist.
- **Ühendatud maailm:** Süsteem on ühendatud internetiga, tagamaks ühenduvus tarneahela protsesside ja välismaailmaga.

**RAMI 4.0 elutsükli väärtusvoo** mõõde käsitleb toote elutsükli kõiki etappe alates loomisest kuni utiliseerimiseni, hõlmates "Tüübi" ja "Instanti" ideed igas etapis. See rõhutab toodete ja varade jälgimise tähtsust nende kasutusaja jooksul, sealhulgas arenduse, tootmise, kasutamise ja utiliseerimise perioodidel. See aspekt aitab mõista toodete ja süsteemide muutuvaid nõudeid kogu nende elutsükli vältel.

**Arhitektuurikihid** RAMI 4.0 koosneb kuuest kihist, mis pakuvad terviklikku ülevaadet tööstussüsteemidest. Iga kiht täidab konkreetset funktsiooni, alustades süsteemi füüsilistest elementidest (nt varade kiht) kuni üldiste ärieesmärkide ja -mudeliteni (ärikiht). Selline kihiline lähenemine toetab tööstussüsteemide analüüsi ja projekteerimist, tagades, et kõik aspektid, alates riistvarast kuni andmeanalüüsini, on integreeritud. RAMI 4.0 erinevad kihid on järgmised:

- **Ärikiht:** See kiht hõlmab ettevõtte ärimudeleid, õiguslikku raamistikku ja tööstuslikke reaalajas jälgimisteenuseid, kasutades koondpaneeli ja kasutajaliidese rakendusi.
- **Funktsionaalne kiht:** Funktsionaalne kiht saab andmeid varade kihist ja teeb otsuseid andmeanalüüsi põhjal.
- **Teabekiht:** See kiht teostab erinevate sündmuste teabe eeltöötlust, tagab madalamatel kihtidel saadud andmete tervikluse ja kvaliteedi ning esitab seejärel struktureeritud andmed funktsionaalsetele ja ärikihtidele.
- **Kommunikatsioonikiht:** See kiht vastutab standardeid ja protokolle järgides võrkude omavahelise sidepidamise eest ning võimaldab varade ja integratsiooni kihtidel suhelda ülemiste kihtidega.
- **Integratsioonikiht:** See kiht edastab varadest genereeritud teavet ülemistele kihtidele, võimaldab varade juhtimist ja kontrollimist rakendus- ja funktsionaalkihtide kaudu ning sisaldab infotehnoloogia elemente.
- **Varade kiht:** See on kõige madalam kiht, mis hõlmab kõiki füüsilisi komponente, sealhulgas seadmeid ja lisaseadmeid.

RAMI 4.0 tasemed hõlbustavad traditsiooniliste tööstuslike operatsioonide kaardistamist digitaliseeritud Tööstus 4.0 paradigmasse, tagades, et iga komponendi roll on määratletud ja integreeritud kogu süsteemi.

Käesoleva analüüsi kontekstis keskendume varade kihile. Me võtame andmed valitud teadustöödest (vt Jaotis 2.4) vastavalt varade arhitektuuri kihis esitatud hierarhia tasanditele. Pärast tootmisprotsessiga seotud füüsiliste varade välja toomist saame luua konteksti teistele arhitektuuri kihtidele seoses teabe väärtusega.

### 3.3 Väljakutsed

Et püsida turul konkurentsivõimelised, peavad organisatsioonid tegelema mitmete väljakutsetega. Näiteks, nagu artiklis [20] on mainitud, võib **digitaalne transformatsioon**, tehnoloogia integreerimine äri- ja tootmisprotsessidesse, tekitada organisatsiooni rakenduste lõppkasutajatele vastuolulisi tundeid. Seega on IT-nõustajatele omaette väljakutseks digitaalsele transformatsioonile süsteemse lähenemisviisi leidmine, arvestades, kuidas iga tehnoloogia osa on integreeritud kogu protsessi.

**Pilvepõhised lahendused** võivad oluliselt kaasa aidata teabe turvalisusele ja juurdepääsu haldamisele [20], kuid nende integreerimine protsessidega võib olla keeruline, kuna erinevad pilvelahendused on loodud erinevalt. Vead rakendamisel võivad potentsiaalselt viia andmeleketeni. Lisaks sõltub organisatsiooni suurus, asukohast, tööstusharu eripärast, ärimudelist ja klientide profiilist, **millistele nõuetele peab organisatsioon vastama**. Tehnoloogiaalaste määruste täitmata jätmise võib kaasa tuua trahve ja karistusi, mis võivad tõsiselt mõjutada tootmisprotsesse.

**Integratsioonid ja uuendused** on digitaalse transformatsiooni oluline osa [20]. Süsteemide uuendamine ja uute tehnoloogiate integreerimine olemasolevasse infrastruktuuri võib olla keeruline, kuna rakenduste programmeerimisliidised võivad uute tarkvara süsteemidega olla ühitamatud

või uuendusprotsess võib võtta oodatust rohkem aega. **Automatiseerimine** on tööstuses vajalik protsesside kiirendamiseks, kulude vähendamiseks ja töötajate ohutuse tagamiseks. Uued automatiseerimislahendused mõjutavad töötajate igapäevast tööd, nõudes muuhulgas nende jaoks uute tehnoloogiate kasutama õppimist. **Tehisintellekt ja masinõpe** (AI/ML) toetavad automatiseerimisvahendite funktsionaalsust, kuid sobivate töövõtete leidmine konkreetsete ülesannete jaoks võib olla keeruline ja aeganõudev.

Organisatsioonid vajavad **andmete haldamise** strateegiaid, et kaitsta oma andmeid volitamata juurdepääsu ja manipuleerimise eest [20]. Andmelekkete korral võib organisatsioonidel olla keeruline jätkata oma tavapärast toimimist. Uute lahenduste ja tehnoloogiate kasutusele võtmine toob endaga kaasa **infrastruktuuri muudatusi**. Muutused võivad põhjustada häireid töös, millede lahendamine omakorda võib nõuda ajalisi ja rahalisi ressursse, kuna töötajad peavad muutustega kohanema. Infrastruktuuri muudatuste haldamine võib samuti olla kulukas ja aeganõudev protsess.

Organisatsioonidel võib olla **puudus kogunud spetsialistidest** [20], mistõttu nad kasutavad kas sisseostetud teenuseid või koolitavad töötajaid, et tagada pädevus automatiseerimisvahendite, protsesside, rakenduste jne haldamisel. Automatiseerimise algatuste **haldamine** (st planeerimine, organiseerimine ja implementeerimine) on keeruline protsess ning ebatõhus implementatsioon võib viia eelarve ületamiseni ja ulatuslike viivitusteni.

Andmekaitsealased rikkumised kujutavad peamist ohtu **andmeturbele** [20], mis omakorda mõjutab organisatsiooni rahalist seisundit ja konkurentsivõimet. Ohuagendid loovad pidevalt uusi strateegiaid, et organisatsioonides segadust tekitada. Kuna erinevatel organisatsioonidel on erinevad infoturbe vajadused, on andmete ja infotehnoloogia turvalisuse tagamine endiselt keeruline väljakutse.

### 3.4 Intervjuude tulemused

Selles jaotises antakse ülevaade intervjuude tulemustest. Intervjueeritavad rääkisid väljakutsetest, mida nende organisatsioonid kogevad seoses automatiseeritud süsteemide ja seadmete haldamisega, üldise turvalisuse strateegiaga, ohuteadlikkusega, intsidentidele reageerimisega, andmevahetusega, terviklusega, töötajate hariduse ja koolitustega, nõuetele vastavusega, õigusteadlikkuse ning tehnoloogia ja innovatsiooniga. Järgnevalt teeme kokkuvõtte intervjuude tulemustest.

**Automatiseeritud süsteemid ja seadmete käitlemine:** Ettevõtete protsesside automatiseerituse tase ulatub täielikult automatiseeritud protsessidest kuni täielikult manuaalsete protsessideni. Uuemad seadmed nõuavad sageli tõrkeotsinguks tarnija-spetsiifilist kaugjuurdepääsu, samas kui vanemad seadmed töötavad sageli vananenud tarkvara või püsivara peal, mida tunnistatakse riskina ning põhjendatakse investeerimisotsustega.

**Üldine infoturbe strateegia:** Ettevõtte suurus ja selle turvaalane valmisolek on omavahel seoses. Tavaliselt on suurematel ettevõtetel kehtestatud infoturbe poliitikad ja strateegiad, samal ajal kui väiksematel või alustavatel organisatsioonidel puuduvad sellised ametlikud protseduurid. Infoturbe meetmed, sealhulgas tarkvara uuendamine, kasutajate juurdepääsuõigused ja andmete varundamine, on kehtestatud ning neid hallatakse kas ettevõtte siseselt või ostetakse vastav teenus väljast sisse.

**Ohuteadlikkus ja intsidentidele reageerimine:** Vastajad teadvustasid, et on esinenud turvaintsidente, mis on viinud turvameetmete ajakohastamiseni. Siiski tõdeti, et tähelepanu turvalisusele on pärast vahejuhtumit aja jooksul vähenenud. Ettevõtte suurus tundub mõjutavat turvatestide läbiviimise tõenäosust ja sellele järgnevat reageerimist.

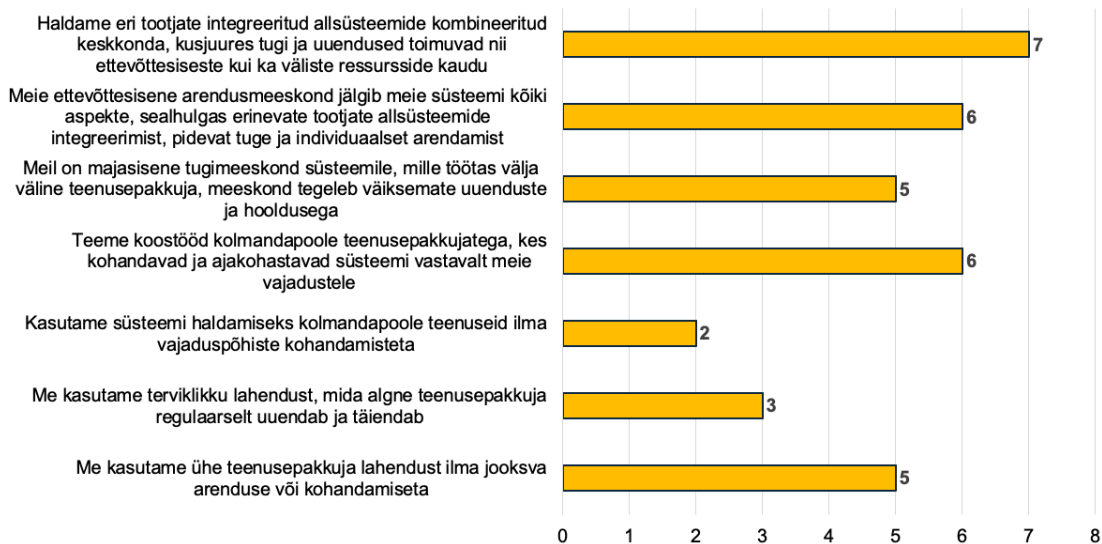
**Andmevahetus ja terviklus:** Ettevõtted kasutavad nii sise- kui ka pilvepõhiseid andmesalvestuslahendusi, mis näitab varieeruvat usaldustaset väliste andmesalvestusteenuste pakkujate suhtes. Juhtumid on näidanud, et sisemiste ja pilvepõhiste salvestusmeetodite kombineerimine pakub parimaid andmete taastamisvõimalusi. Väljakujunenud protsessid ja käitumismustrid takistavad suurematel ettevõtetel pilvepõhiste lahenduste kasutuselevõttu.

**Töötajate haridus ja koolitus:** Turvakoolituste ulatus ja regulaarsus varieeruvad ettevõtetelt. Suurematel ettevõtetel on sageli struktureeritud koolitusprogrammid, kuid kõik vastanud töid välja puudusi turvakoolitustes, mis on suureks nõrkuseks.

**Vastavus ja õigusteadlikkus:** Teadlikkus GDPR-ist ja konkreetsetest turvanormidest on olemas, kuid see on erineva tasemega ning on peamiselt probleemiks väiksemates ja alustavates ettevõtetes. See näitab vajadust selgitada, millised turvalisusega seotud õigusaktid on olemas ja kuidas neid järgida.

**Tehnoloogia ja innovatsioon:** Tehnoloogiate kasutusele võtmist mõjutavad majanduslikud kaalutlused. Märkimisväärselt eelistatakse tuntud Euroopa tarnijaid, eriti kohaliku või poolkohaliku tehnilise toe olemasolul. Läbirääkimised tarnijatega parimate tavade üle, eriti seoses kaugjuurdepääsuga, on tavalised, kajastades teadlikkust küberturvalisuse tähtsusest uutes tehnoloogiates.

**Kuidas teie organisatsioon rakendab ja haldab oma automatiseeritud tootmissüsteeme, arvestades, et need võivad koosneda erinevatest allsüsteemidest ja komponentidest, mis pärinevad erinevatelt tootjatelt?**



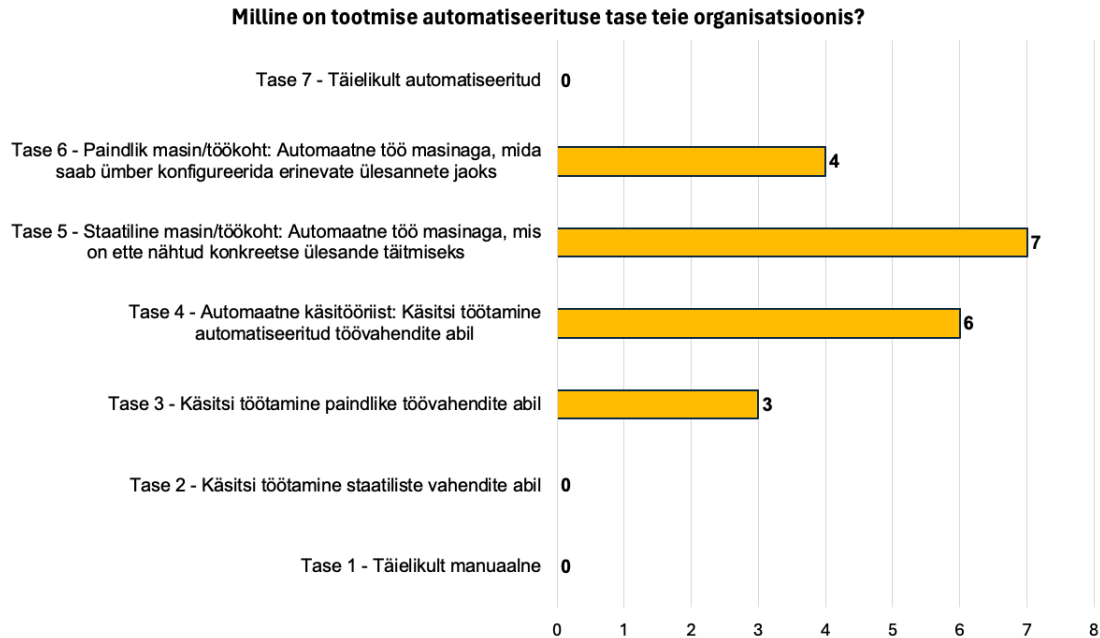
Joonis 6. Automatiseeritud tootmissüsteemide rakendamise variatsioonid

### 3.5 Küsitluse tulemused

Küsitluse tulemused näitavad suundumust integreerida erinevaid tehnoloogilisi lähenemisviise tootmisektoris ning eelistust hankida lahendusi ühelt pakkujalt. Nagu on kujutatud Joonisel 6, on levinud, et üks ettevõtte pakub mitmeid erinevaid lahendusi. See suundumus mitte ainult ei tõsta esile tootmise ökosüsteemi mitmekülgset ja segmenteeritud, vaid näitab ka liikumist ettevõtete tehnoloogiliste infrastruktuuride lihtsustamise ja ühtlustamise suunas. Selline lähenemine hõlbustab sujuvamat toimimist, parandab erinevate tehnoloogiliste komponentide koostalitlusvõimet ning vähendab potentsiaalselt mitmete tarnijate haldamise keerukust ja kulusid.

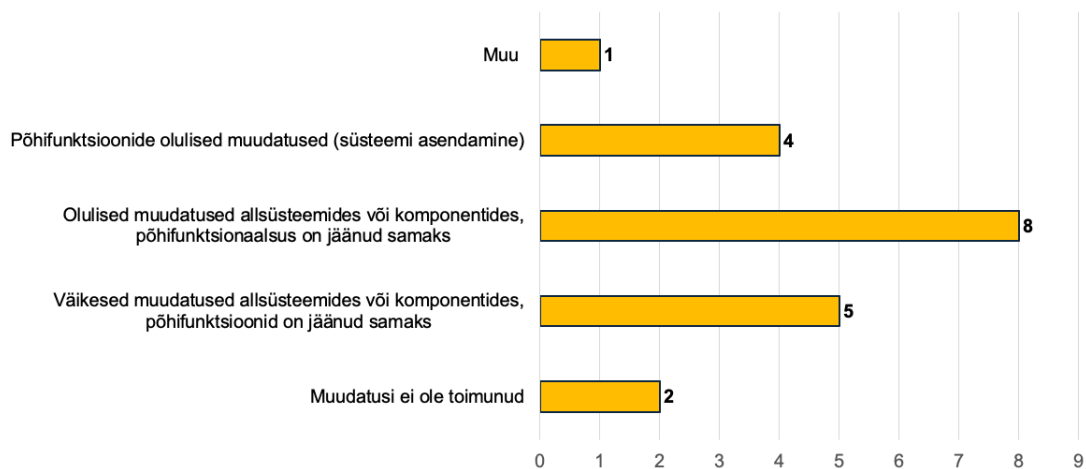
Joonisel 7 kujutatakse, kuidas vastajad hindasid automatiseerituse taset oma ettevõttes. Märgimiseväärtus on see, et kõik vastused jäid vahemikku 3-6, millest võib järeldada, et automatiseerimine toimub ulatuslikult kogu tööstuses. Enamus (7 vastust) märkisid, et nad kasutavad staatilisi seadmeid/töökohti, mis on spetsialiseerunud konkreetsetele ülesannetele (5. tase). 6 vastajat teatasid, et nad kasutavad automatiseeritud tööriistu, mis toetavad käsitsi tehtavat tööd (4. tase), ja 4 vastajat märkisid, et nad kasutavad seadmeid, mida saab kohandada erinevate ülesannete jaoks (6. tase). Samal ajal tunnistas enamus vastajaid, et viimase viie aasta jooksul on toimunud märkimisväärsed muutused (vt Joonis 8).

Tootmisprotsessi optimeerimine mitme erineva allsüsteemi vahel on välja toodud kõige suurema väljakutsena (11 vastust) automatiseeritud süsteemide ja tehnoloogia integreerimise, arendamise ja toetamise protsessis (vt Joonis 9). Sellele väljakutsele järgneb vajadus saavutada kõrge kvaliteediga süsteem, hallata turvalisust ja usaldusväärsust, tasakaalustada süsteemi tõhusus ja privaatsuse küsimused ning tagada andmete privaatsus ja turvalisus erinevate allsüsteemide ja tootjate integreerimisel (kõigil 8 vastust).



Joonis 7. Automatiseerimise tasemed

### Mil määral on teie automatiseeritud tootmissüsteem viimase 5 aasta jooksul muutunud?



Joonis 8. Automatiseeritud tootmissüsteemide muudatused viimase 5 aasta jooksul

## 3.6 Arutelu

Tulemused näitavad, et tootmisorganisatsioonid soovivad muuta oma töömeetodeid automatiseeritumaks. Ümberkujundamise tulemusena toimuvad arengud ja rakendatakse täiustatud lahendusi, mis näitab digitaliseerimise suurenevat tähtsust selles sektoris. See muutus pole ainult vastus efektiivsuse ja tootlikkuse suurendamise nõudmistele, vaid ka ennetav lähenemine tootmise tulevikule, kus on näha teataval tasemel automatiseerumist, andmete integreerimist ja nutikad tootmisviise.

Uute lahenduste integreerimine toob kaasa väljakutseid ja probleeme seoses erinevate tehnoloogiliste süsteemide ühtsesse raamistikku ühendamise ja integreerimisega. Need probleemid hõlmavad sageli ühilduvust, andmesilosid ja manussüsteemide haldamise keerukust. Sellise tehnoloogilise integreerimise eelised – alates suuremast tõhususest ja paremast andmeanalüüsist kuni kvaliteetsemate toodete väljatöötamiseni – kaaluvad üles esialgsed takistused ning raskused. Selline positiivne väljavaade rõhutab tootmise digitaalse ümberkujundamise väärtust, kinnitades tööstuse valmisolekut pikaajalise innovatsiooni ja konkurentsivõime saavutamiseks.

**Millised on teie organisatsiooni peamised väljakutsed automatiseeritud tootmissüsteemi, sealhulgas erinevate tootjate allsüsteemide integreerimisel, kasutamisel, arendamisel ja toetamisel?**



Joonis 9. Automatiseeritud tootmissüsteemide rakendamise väljakutsed

## 4 Standardid

Järgnevalt uurime analüüsitud artiklites viidatud standardeid, näidates nende keerukust ja sobivust erinevate automatiseerimise kasutusjuhtumite puhul. Uuring hõlmab mitmesuguseid standardeid, alates tööstusrobotika ohutusprotokollidest kuni pilvepõhiste tootmissüsteemide küberturvalisuse raamistikeni. Igal standardil on oluline roll kaasaegsete automatiseeritud süsteemide töökindluse ja usaldusväärsuse tagamisel. Käesoleval jaotisel on kaks eesmärki: anda põhjalik ülevaade ja pakkuda suuniseid tulevaste praktiliste rakenduste ning teadusuuringute jaoks tööstusautomaatika valdkonnas. Konkreetsemalt vaatleme, milliseid standardeid peaks automatiseeritud süsteemide ja tehnoloogia kasutamisel järgima.

### 4.1 Tööstusrobotika ja -automaatika ohutus- ja turvastandardid

Paljud standardid ja raamistikud on olulised tööstusautomaatika ja ohutuse valdkonnas, kujundades automatiseeritud süsteemide projekteerimist, rakendamist ja toimimist. Alates tööstusrobotika ohutusprotokollidest kuni pilvepõhiste tootmissüsteemide küberturvalisuse meetmeteni, mängivad need standardid võtmerolli süsteemide töökindluse ja usaldusväärsuse tagamisel. Nad pakuvad struktureeritud suuniseid ja meetodikaid, mis toetavad töö tõhusust, ohutust ja turvalisust erinevates automatiseerimissenaariumites.

#### 4.1.1 Tööstusrobotika ja -automaatika standardid

Teadusartiklid, mis on seotud tööstusrobotika ja -automaatika ohutusstandarditega [35, 23, 21, 41, 7], hõlmavad mitmesuguseid automatiseerimise stsenaariume, alates tööstusrobotitest kuni küberfüüsiliste tootmissüsteemideni. Need artiklid käsitlevad erinevate standardite ja raamistike kasutamist antud stsenaariumites. Selline mitmekesisus peegeldab automatiseerimise mitmekülgset eri tööstusharudes ning rõhutab vajadust mõista neid juhtpõhimõtteid terviklikult.

Quarta *et al.* [35] ja Khalid *et al.* [23] käsitlevad tööstusrobotika ja -automaatika ohutus- ja turvastandardeid. **ISO TS 15066** keskendub spetsiaalselt robotite koostöösüsteemidele, **ISO 12100** tegeleb üldiste ohutuspõhimõtetega ning **ISO 10218 osad 1 ja 2** keskenduvad konkreetsetele tööstusrobotite ohutusnõuetele. Need standardid pakuvad juhiseid tööstuslike robotite ohutuks projekteerimiseks, implementeerimiseks ja kasutamiseks. Lisaks defineerib **ISO 8373** tööstusroboti mõiste, rõhutades selle programmeeritavust, mitmetarbelisust ja rakendatavust tööstusautomaatikas.

Jablonski *et al.* [21] soovivad süsteemiarhitektuuri ja ohutusstandardeid keerukatele süsteemidele. AADL (**SAE AS5506C**) pakub raamistikku keerukate süsteemide modelleerimiseks ja analüüsimiseks, keskendudes peamiselt aspektidele nagu ajastus ja ohutus. Lisaks pakuvad AADL Behavior Model Annex (**SAE AS5506/2**) ja AADL Error Model Annex v2 (**SAE AS5506/1A**) täiendavaid vahendeid süsteemi käitumise ja veahaldusmehhanismide kirjeldamiseks, mis on olulised automaatsete süsteemide töökindluse ja ohutuse tagamiseks. Urooj *et al.* [41] ja Chundhoo *et al.* [7] osutavad üldistele riskijuhtimise standarditele, nagu (**ISO 31000**), mis pakub põhimõtteid, suuniseid ja protsesse riskide tõhusaks juhtimiseks.

Kuigi seni käsitletud standardid loovad kindla aluse tööstusautomaatika ohutuse ja süsteemi arhitektuuri jaoks, esineb nendes raamistikutes puudusi küberturvalisuse osas. Need puudused

muutuvad üha olulisemaks seoses küberohtude kiire arengu ja automaatikasüsteemide sügavama integreerumisega info- ja kommunikatsioonitehnoloogiatega. Hoolimata raamistike rõhuasetusest füüsilisele ohutusele ja operatiivsele efektiivsusele, on praegused standardid piiratud, kuna need ei võimalda piisavalt käsitleda automatiseeritud tootmissüsteemide küberturvalisuse ohtudest tulenevaid mitmetahulisi probleeme.

Antud asjaolu rõhutab vajadust täiendada meie arusaama küberturvalisusest, tuginedes infotehnoloogia süsteemidest saadud teadmistele ja tavadele. Järgneva peatüki eesmärk on aidata sellele kaasa, tutvustades infotehnoloogia sektori standardeid ja eeskirju, mida saab tõhusalt rakendada automatiseeritud tootmissüsteemide küberturvalisuse suurendamiseks. Nende teadmiste tutvustamisega püüame pakkuda terviklikumat lähenemisviisi automatiseeritud süsteemide kaitsmisele küberriskide eest, tagades nende kriitiliste süsteemide vastupidavuse ja usaldusvääruse arenevate ohtude ees.

#### **4.1.2 Küberturbe koondpunkt: infotehnoloogia infrastruktuurist tööstusautomaatikani**

Automatiseeritud tootmissüsteemide küberturvalisuse käsitlemisel on hädavajalik tunnistada aluspõhimõtet, et turvalisust ei saa lõplikult tagada, vaid pigem tuleb keskenduda nõrkuste tuvastamisele ja turvameetmete rakendamisele. See paneb aluse turvameetmete kriitilisele rollile, mis hõlmab mitmesuguseid juhtimis-, tegevus- ja tehnilisi strateegiaid, ning mis on mõeldud süsteemi konfidentsiaalsuse, tervikluse ja käideldavuse kaitsmiseks. Võimalike riskide vähendamiseks rakendatakse neid meetmeid eeskirjade, protseduuride ja tehniliste vahendite (nii käsitsi kui ka automatiseeritud) kombinatsiooni abil.

Küberturvalisuse raamistiku keskmes on standardid, mille eesmärk on tagada koostalitlusvõime, vastavus riiklike ja rahvusvaheliste eeskirjadega ning kehtestada miinimumnõuded süsteemide turvalisuse tagamiseks, sh käideldavuse, konfidentsiaalsuse ja tervikluse osas. Lisaks pakuvad küberturvalisuse põhialused (*de facto* standardid), mis tuginevad parimatele tavadele, organisatsioonidele suuniseid turvameetmete rakendamiseks ja riskianalüüsi läbiviimiseks. Näiteks nagu:

- **ISO/IEC 27000 perekond** - infoturve, küberturvalisus ja privaatsuse kaitse [19],
- **NIST küberturvalisuse raamistik** [32],
- **CIS kriitilised turvameetmed** [6],
- **E-ITS, Eesti Infoturbestandard** [37] mille üks kümnest moodulist, IND moodul, käsitleb eraldi tööstusautomaatikat,
- **Microsofti infoturbe põhialused**[30], mille põhiohk on Microsofti toodetel ja teenustel.

Raamistikud loovad ühise keele ja praktikad küberturbe riskide tõhusaks haldamiseks. Standardite ja määruste järgimine nõuab mitmetahulist lähenemist, sealhulgas auditeid, sertifitseerimisi ja enesehindamisi.

Kutzler *et al.* [25] soovib lisaks kasutada ka **raamistikku elutähtsate infrastruktuuride küberturvalisuse parandamiseks**, mis on koostatud NIST-i poolt. See raamistik juhendab ja

suunab tugevate küberturvalisuse strateegiate väljatöötamist, mis on eriti olulised elutähtsate infrastruktuuride, sealhulgas tootmissüsteemide, kaitsmiseks.

Kuid ka standardid ja raamistikud **TAXII** (usaldusväärne automatiseeritud indikaatorite teabevahetus), **STIX** (struktureeritud ohuteabe avaldamine) ja **CyBEX** (küberturvalisuse infovahetuse raamistik), millele viitab Schaefer *et al.* [27] on küberturbe alase teabe jagamiseks ja koostööks hädavajalikud, aidates organisatsioonidel end paremini kaitsta ja paremini reageerida erinevatele küberohtudele.

Tööstusautomaatikasüsteemide küberturvalisuse tugevdamise seisukohalt on oluline **ISA/IEC 62443** [18] standardite seeria. Selle seeria standardeid eristab tööstuslike juhtimissüsteemide turvalisusele keskendumine ning need on välja töötatud selliste sektorite nagu energia, tootmine ja transport eripärade lahendamiseks. IEC 62443 pakub raamistikku tööstusautomaatika ja juhtimissüsteemide kaitsmiseks. Standard kirjeldab struktureeritud lähenemist küberturvalisusele, hõlmates aspekte alates riskianalüüsist ja süsteemi kavandamisest kuni rakendamise ja hooldamiseni, tagades seeläbi nende süsteemide vastupidavuse küberohtude ees.

Lisaks olulistele tehnilistele ja tegevusstandarditele mängivad küberturvalisuse tavade kujundamisel olulist rolli ka õiguslikud raamistikud. Üks neist on **Isikuandmete Kaitse Üldmäärus (GDPR)** [13], Euroopa Liidu õigusraamistik, mis rõhutab isikuandmete kaitse tähtsust. GDPR kehtestab nõuded andmetööstustoimingutele, tagades isikuandmete privaatsuse ja turvalisuse erinevates sektorites, sealhulgas tootmises.

Isikuandmeid koguvate, töötlevate või säilitavate automatiseeritud tootmissüsteemide puhul ei ole GDPRi järgimine mitte ainult juriidiline kohustus, vaid ka küberturvalisuse hügieeni üks osa. Selles rõhutatakse vajadust rakendada andmekaitse meetmeid, näiteks andmete minimeerimist, krüpteerimist ja õigeaegselt leketest teatamist, mis on kooskõlas küberturvalisuse laiemate eesmärkidega, et kaitsta süsteemi terviklust ja konfidentsiaalsust. GDPRi ristumine tööstuslike küberturvalisuse standarditega, nagu näiteks IEC 62443, näitab kaasaegsete automatiseeritud süsteemide turvalisuse mitmekülgset olemust, kus andmete privaatsuse tagamine on muutunud üldise küberturvalisuse raamistiku lahutamatuks osaks.

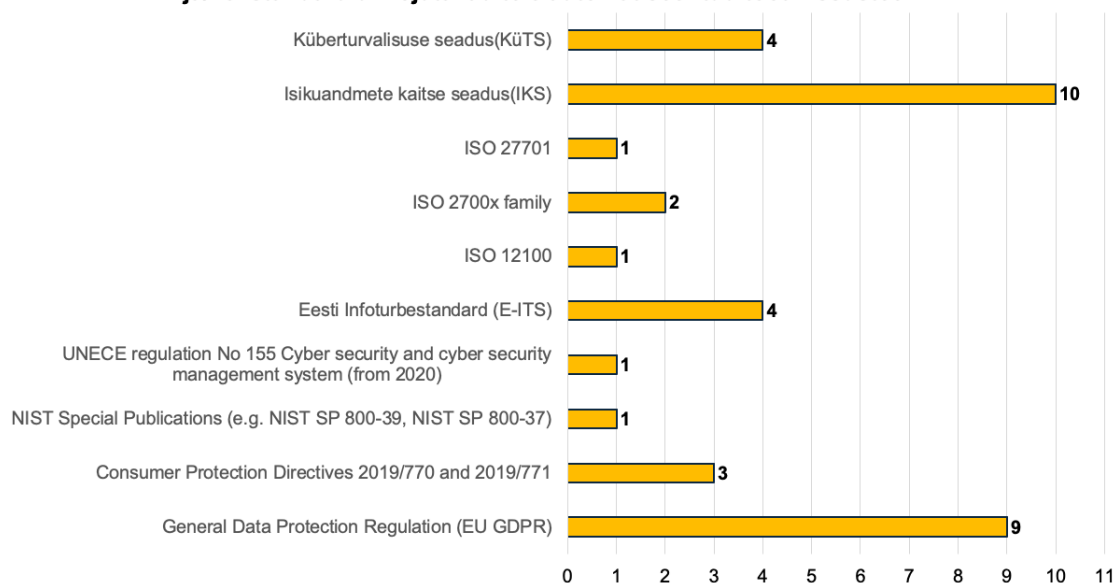
## 4.2 Küsitluse tulemused

Joonisel 10 on esitatud ülevaade sellest, millised turvalisust, privaatsust või ohutust käsitlevad õigusaktid, eeskirjad ja/või standardid mõjutavad vastajate organisatsioonides kasutatavaid automatiseeritud tootmissüsteeme. Kõige sagedamini on märgitud Euroopa tasemel heaks kiidetud isikuandmete kaitse üldmäärust, GDPR (9 vastust) ja Eesti Isikuandmete kaitse seadust, IKS (10 vastust). Küberturvalisuse seadus (KüTS) ja Eesti Infoturbestandard (E-ITS) jagavad kolmandat kohta, mõlemad 4 vastusega.

## 4.3 Arutelu

Turvalisuse, privaatsuse ja ohutusega seotud õigusaktid, määrused ja standardid pakuvad organisatsioonidele suuniseid automatiseeritud süsteemide ja tehnoloogiate parimate tavade kohta nende projekteerimisel, haldamisel ja hooldamisel. Need standardid aitavad defineerida turvapoliitikat, riskijuhtimise strateegiaid ja riskide maandamise meetmeid. Siiski näitavad küsitluse tulemused,

**Millised turvalisuse, privaatsuse või ohutusega seotud õigusaktid, määrused ja/või standardid mõjutavad teie automatiseeritud tootmissüsteemi?**



Joonis 10. Turvalisuse, eraelu puutumatuse või ohutusega seotud õigusaktid, määrused ja/või standardid, mis puudutavad automatiseeritud tootmissüsteeme

et vastajad keskenduvad peamiselt isikuandmete kaitse normidele, nagu Euroopas kehtiv Isikuandmete Kaitse Üldmäärus (GDPR) ja Eesti Isikuandmete Kaitse Seadus (IKS). Selline piiratud õigusteadlikkus rõhutab teadmiste ja kogemuste puudumist laiemate õiguslike raamistikega, mis reguleerivad digitaalset ja küberturbe maastikku.

See järeldus on eriti murettekitav ajal, mil digitaalsed toimingud on seotud erinevate regulatiivsete nõuetega, mis ei piirdu ainult isikuandmete kaitsega. Need eeskirjad hõlmavad mitmesuguseid tööstusspetsiifilisi vastavusstandardeid ja rahvusvahelisi küberturvalisuse protokolle, mis on äärmiselt olulised ettevõtete ja nende sidusrühmade huvide kaitsmisel.

## 5 Automatiseeritud süsteemide ja tehnoloogiate varad

Selles peatükis esitleme intervjuude, kirjanduse analüüsi ja küsitluse tulemusi automatiseeritud süsteemide ja tehnoloogiate varade kohta. Meenutame, et varad võivad olla ärivarad (nagu andmed, teave ja teenused) või süsteemi varad (nagu süsteemi komponendid või nende kombinatsioonid, mis toetavad ärivara). Turvaeesmärk määratletakse ärivara piirangutena kasutades turvakriteeriume (nagu konfidentsiaalsus, terviklus ja käideldavus). Selles peatükis uurime, millised on kaitstud varad automatiseeritud süsteemides ja tehnoloogiates.

### 5.1 Intervjuude tulemused

Käesolevas peatükis esitame intervjuueeritavate seisukohad selle kohta, kuidas nende ettevõtetes kasutusel olevaid automatiseeritud süsteeme ja tehnoloogiaid saab selgitada läbi RAMI 4.0 raamistiku. Tulemused on kokkuvõtlikult esitatud Tabelis 5, kus varad on vastavusse viidud RAMI 4.0 varade arhitektuuri kihiga. Tasub mainida, et intervjuud viidi läbi enne struktureeritud kirjanduse analüüsi ning seetõttu pole need väga detailsed, kuid annavad siiski ülevaate tootmisprotsessi varadest intervjuueeritavate ettevõtetes.

Tuleb märkida, et viies intervjuueeritav esindab alustavat ettevõtet, millel on allhanke põhine tootmisvõimekus. Ettevõtte ja ühendatud maailma taseme varad on selle ettevõtte jaoks esmatähtsad, kuna need on nende igapäevase toimingu lahutamatuks osaks. Teiste intervjuueeritavate puhul pöörati sarnast rõhku ettevõtte ja ühendatud maailma kihtidele, kuid tähelepanu pöörati ka madalama kihi varadele. Kõigil juhtudel haldasid seadmete tootjad tavaliselt kaitset välisseadmete ja juhtimisseadmete kihil, kuna neil oli kindel juurdepääs või nõuded seadmete tõrkeotsinguks kohapeal.

Tabel 5. Intervjuude tulemuste seostamine RAMI 4.0 varade kihiga; ”+“ viitab varade mainimisele

|                        | Toode | Välis-seade | Juhtimis-seade | Jaam | Töö-keskus | Ettevõtte | Ühendatud maailm |
|------------------------|-------|-------------|----------------|------|------------|-----------|------------------|
| <b>Intervjuu nr. 1</b> | -     | +           | +              | +    | +          | +         | +                |
| <b>Intervjuu nr. 2</b> | -     | +           | +              | +    | +          | +         | +                |
| <b>Intervjuu nr. 3</b> | -     | +           | +              | +    | +          | +         | +                |
| <b>Intervjuu nr. 4</b> | -     | +           | +              | +    | +          | +         | +                |
| <b>Intervjuu nr. 5</b> | -     | -           | -              | -    | -          | +         | +                |

### 5.2 Kirjanduse analüüsi tulemused

Selles jaotises võtame kokku ärivarade ja süsteemi varade kohta läbi viidud kirjanduse analüüsi tulemused. Alustuseks esitame Tabelis 6 kirjanduses tuvastatud süsteemi varade vastavused RAMI 4.0 raamistikus esitatud varade mõõtmega.

Tabel 6. Süsteemi varade kaardistamine kirjandusest RAMI 4.0 varade kihiga; ”+“ viitab varade mainimisele

| Artikkel                            | Toode | Välisseade | Juhtimisseade | Jaam | Töökeskus | Ettevõtte | Ühendatud maailm |
|-------------------------------------|-------|------------|---------------|------|-----------|-----------|------------------|
| Khalid <i>et al.</i> (2021) [23]    | -     | +          | +             | +    | -         | -         | -                |
| Urooj <i>et al.</i> (2022) [41]     | -     | +          | +             | +    | +         | -         | +                |
| Thames <i>et al.</i> (2014) [27]    | -     | +          | -             | -    | +         | +         | -                |
| Clark <i>et al.</i> (2017) [8]      | -     | +          | -             | +    | -         | -         | -                |
| Kutzler <i>et al.</i> (2021) [25]   | -     | +          | -             | +    | +         | -         | -                |
| Quarta <i>et al.</i> (2017) [35]    | -     | +          | +             | +    | -         | +         | +                |
| Jablonski <i>et al.</i> (2021) [21] | -     | +          | -             | +    | -         | -         | -                |
| Chundhoo <i>et al.</i> (2021) [7]   | -     | +          | -             | -    | -         | +         | -                |
| Shah <i>et al.</i> (2020) [38]      | -     | +          | +             | +    | +         | +         | -                |
| Pu <i>et al.</i> (2023) [34]        | -     | +          | +             | +    | -         | -         | -                |

**Toode** hõlmab tootmisprotsesside lõpptulemust, näiteks tarbekaupu või tööstustooteid, mis on ettevõtte tulude ja turupositsiooni seisukohalt keskse tähtsusega. Need tooted määratlevad brändi identiteedi ja on võtmetähtsusega klientide rahulolu tagamisel.

**Välisseade** hõlmab olulisi vahendeid, nagu robotid, andurid ja ajamid, mis on tootmisoperatsioonide täpsuse ja tõhususe seisukohalt üliolulised. Need seadmed mõjutavad toote kvaliteeti, tootmiskiirust ja kohandumisvõimet tootmisülesannetega.

**Juhtimisseade**, näiteks programmeeritavad loogikakontrollerid (PLC), kaugjuhtimispuldid (RTU) ja hajutatud juhtimissüsteemid (DCS), on hädavajalikud tootmisprotsesside automatiseerimisel, järjepidevuse tagamisel ja reaajas andmete haldamisel, võimaldades operatiivsete otsuste tegemist.

**Jaam** jälgib ja kontrollib konkreetseid tootmisprotsesse, kasutades töökohti ja operaatoriliideseid, mis võimaldavad tootmistegevuse teostamist ja jälgimist.

**Töökeskus** hõlmab organisatsiooni tehnoloogilist selgroogu, sealhulgas arvuteid, servereid ja koostöötarkvara, mis toetavad toiminguid nagu projekteerimine, planeerimine ja haldusülesanded.

**Ettevõtte**: (nt ERP-süsteemid, pilvepõhised andmetöötluslahendused ja ärianalüüsi vahendid) toetavad strateegilist otsustamist ja ressursside jaotamist.

**Ühendatud maailm** hõlmab arvutivõrkude infrastruktuuri, sealhulgas sise- ja välissidevõrke,

mis võimaldavad integreerida erinevaid äriprotsesse.

Süsteemi varade kaardistamine ärivaradele tähendab RAMI 4.0 kontekstis, et tuleb mõista nende varade olemuslikku väärtust, mida nad organisatsioonile loovad. Kuigi vaatlusalustes artiklites ei rõhutada selgesõnaliselt turvavajadust (ärivarade konfidentsiaalsuse, tervikluse või käideldavuse osas), eeldatakse, et kõik kolm kriteeriumit on olulised ja sõltuvad konkreetsetest turvariskidest (käsitlеме mitmeid näiteid Peatükkides 8 ja 9). Tabel 7 võtab kokku automatiseeritud süsteemide ja tehnoloogiate varad (süsteemi- ja ärivarad), liigitab need varad ning illustreerib iga kihi põhilised funktsionaalsed valdkonnad.

Tabel 7. RAMI 4.0 Vara kihtide varad

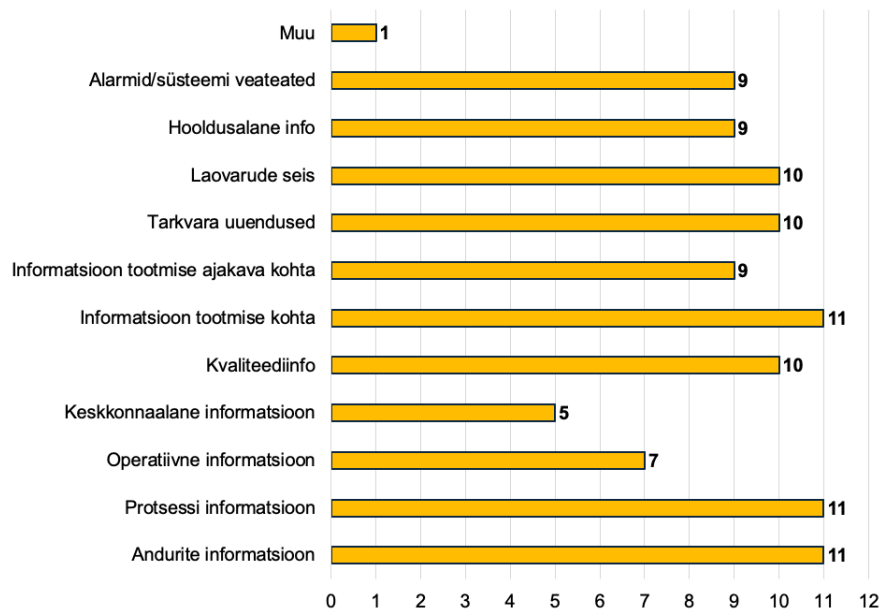
| Hierarhia tasemed | Süsteemi varad  | Ärivarad   |
|-------------------|---|--|
| Toode             | –   | –  |
| Välisseade        | Robotid, täiturid, andurid, mootorid, saatjad, sisseehitatud seadmed, füüsilised tootmiseseadmed, kaamerad, 3D-printerid.                         | Tootmisandmed, töötingimuste andmed, keskkonnategurite andmed, kvaliteedikontrolli andmed, tegevusandmed, visuaalsed andmed. |
| Juhtimis-seade    | Programmeeritav loogiline kontroller, kaugjuhtimispult, hajutatud juhtimissüsteem, väravad.   | Tootmisandmed, töötingimuste andmed, kvaliteedikontrolli andmed, automatiseeritud otsustusprotsess.                          |
| Jaam              | Tööjaam (digitaalne juhteseade), SCADA, operaatorid, operaatoripunktid.   | Operatiivandmed, operatsiooniprotsessid, operatsiooniteenused.   |
| Töökeskus         | Koostöötarkvara, IT hostid, arvutid, serverid, andmekeskused, posti- ja veebiteenused.  | Taotluse andmed, taotlusprotsess, rakendusteenused.  |
| Ettevõtte         | Ettevõtte ressursside planeerimise süsteemid (ERP), tootlikud hooldussüsteemid, müüjad, partnerid, ärirakendused, andmeanalüüs, pilvandmetöötlus. | Äriprotsess, tegevusressursside planeerimine, tarneahela protsess, ärirakenduste andmed.                                     |
| Ühendatud maailm  | Sisevõrk, robotvõrk, tööstuslik demilitariseeritud tsoon, avalik internet.  | Ärirakenduste andmed, tegevusandmed, teenused ja protsessid.   |

### 5.3 Küsitluse tulemused

Küsitluse tulemused rõhutavad üleminekut andmepõhisele otsuste tegemisele tootmisprotsessides. Joonis 11 kajastab vastuste spektrit, mis näitab, et enamik ettevõtteid kogub nüüd oma tootmistegevuses aktiivselt erinevaid andmeid. Lisaks sellele toob Joonis 12 esile infotehnoloogia süsteemide peamised rakendused tootmises, millest kõige levinumaks kasutusalaaks peetakse and-

mete säilitamist (17 vastust). Sellele järgnevad müügiprotsessi juhtimine (11 vastust) ja ettevõtte ressursside planeerimine (ERP) (12 vastust).

#### Millist teavet kasutatakse teie automatiseeritud tootmissüsteemis?



Joonis 11. Automatiseeritud tootmissüsteemides kasutatavad andmed

## 5.4 Arutelu

Andmepõhiste strateegiate kasutusele võtmine annab eelised **protsesside optimeerimisel ja tegevuskulude vähendamisel**. Andmete hoiustamise tähtsustamine rõhutab **andmete kui põhilise vara** rolli tootmise digitaalses ümberkujundamises. Erinevad andmete hoiustamise lahendused võimaldavad organisatsioonidel tohutul hulgal andmeid turvaliselt salvestada, hallata ja pärida, olles muude andmepõhiste toimingute selgrooks. Müügiprotsessi juhtimise roll kajastab **kliendiandmete ja suhtluse tootmisstrateegiasse integreerimise tähtsust**, tagades, et tootmine on kooskõlas turunõudluse ja klientide ootustega. ERP-süsteemide kasutamine tähendab **kompleksset lähenemist põhiliste äriprotsesside integreerimisele**, hõlbustades reaajas andmevahetust eri osakondade vahel, suurendades toimingute nähtavust ja parandades otsuste tegemise tõhusust.

Andmepõhiste strateegiate eeliste hulka kuuluvad toodete parem kvaliteet ja ennetav hooldus, mis minimeerib seisakuid, ennetades seadmete rikkeid enne nende tekkimist. See aitab kaasa tarneahela juhtimisele läbi prognoosimise ja varude kontrolli, ning klientide rahulolule, kohandades tooteid vastavalt konkreetsetele vajadustele ja eelistustele. Andmete kasutamine rõhutab tootmise strateegilist üleminekut intelligentsele, tõhusale ja kliendikesksele toimingutele.

Vara analüüsi tulemused näitavad tootmise arenevat maastikku, kus **andmetel põhinevad otsused ja infotehnoloogiline integratsioon** on muutumas tegevusstrateegiate keskseks osaks. Andmete kasutamine võimaldab tootjatel mitte ainult oma vahetuid protsesse optimeerida, vaid

**Millistel eesmärkidel kasutab teie organisatsioon infotehnoloogia (IT) süsteeme oma automatiseeritud tootmisprotsessides?**



Joonis 12. IT-süsteemi kasutamise eesmärgid automatiseeritud tootmissüsteemides

ka saavutada püsivat innovatsiooni, konkurentsivõimet ja kasvu digitaalses ja kliendikeskses turukeskkonnas.

## 6 Automatiseeritud süsteemide ja tehnoloogiate turvariskid

Käesolevas peatükis kirjeldame kirjanduse analüüsi ja küsitluse käigus tuvastatud turvariske ja -ohte. Turvarisk on ühe või mitme nõrkuse ärakasutamise ohu kombinatsioon, mis võib kaasa tuua negatiivse mõju süsteemile ja organisatsiooni varadele. Selles peatükis analüüsime eelkõige turvariske, millega automatiseeritud süsteemid ja tehnoloogiad kokku puutuvad.

### 6.1 Olukord Eesti küberruumis

Geopoliitilised pinged avaldasid olulist mõju Eesti küberruumile kogu 2023. aasta vältel, nagu on märgitud iga-aastases küberturvalisuse aastaraamatus [36]. Üks märkimisväärsemaid sündmusi, mis mõjutas ka automatiseeritud tootmise süsteemide kasutajaid, leidis aset novembris, kui Iisraeli ja Hamasi vaheline konflikt laienes Eestisse.

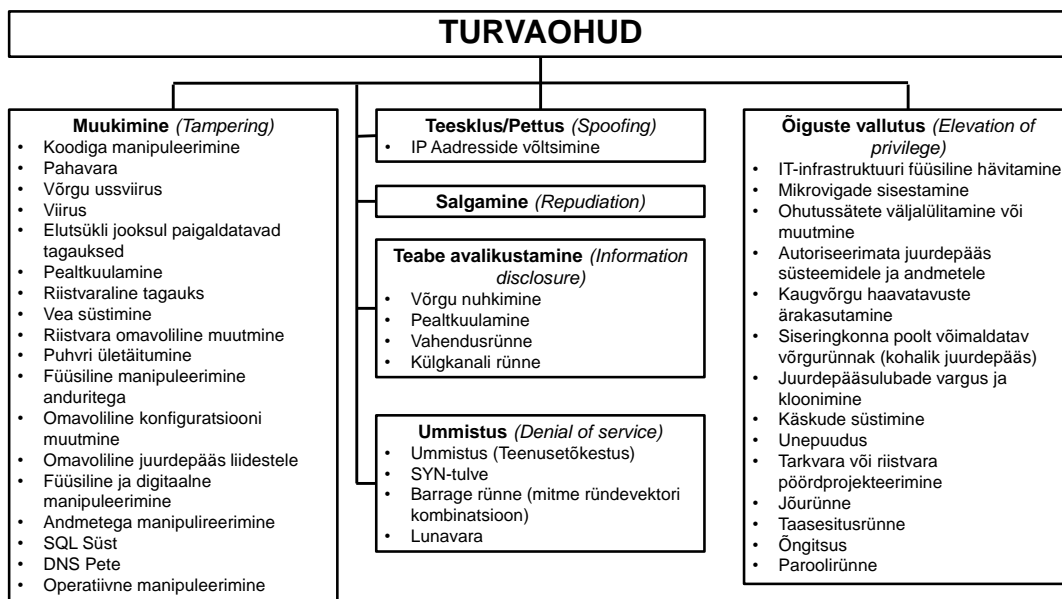
2023. aasta novembri lõpus toimunud küberrünnak häiris ühe kaugkütteettevõtte tööd, mõjutades kaheksat keskküttekatla juhtimissüsteemi. Kuigi vastavad üksused lülitati käsitsi tööle, et säilitada soojuse tootmine ja jaotamine, oli seadmetele tekitatud kahju piisavalt suur ning seadmed tuli välja vahetada. Sarnased küberrünnakud olid suunatud veel vähemalt kahe Eesti ettevõtte vastu, kellest üks tegutseb veevarustuse tagamisega ja teine ehitussektoris. Rünnakud ei olnud suunatud mitte konkreetselt Eesti ettevõtete ja asutuste vastu, vaid Iisraelis toodetud programmeeritavate loogikakontrollerite (PLC) vastu, sõltumata nende geograafilisest asukohast. Sarnast mustrit täheldati ka Ameerika Ühendriikides, peamiselt veevarustusettevõtete puhul. Ründajad, kes väitsid ennast olevat Iraani taustaga, väitsid, et tegemist on kättemaksuga Iisraeli ja Hamasi konflikti eest. See sündmuste seeria toob esile, kuidas ülemaailmsed geopoliitilised pinged ja sõjalised konfliktid võivad esile kutsuda küberrünnakuid ka kaugel asuvates riikides, nagu Eesti.

Kübermaastikul oli Eestis suurenenud aktiivsus seoses Ukrainas toimuva konfliktiga, kus teenusetõkestusrünnakud (DDoS) neljakordistusid. See küberrünnakute järsk kasv ületas 2023. aastal juba 2022. aastal täheldatud kõrge aktiivsuse taseme, püstitades uue rekordi: 2023. aastal registreeriti 484 teenusetõkestusrünnakut - 60% rohkem kui 2022. aastal. Vaid ühe kuuga ületas DDoS-rünnakute sagedus aastase koguhulga, mida täheldati enne Ukraina sõjategevuse eskaleerumist. Neist 139 rünnakut, mis moodustasid vähem kui kolmandiku, peeti mõjusaks, põhjustades tavaliselt lühiajalisi seisakuid või vähendades veebisaitide ja teenuste reageerimisvõimet.

Küberrünnakud muutusid 2023. aasta jooksul üha keerukamaks ja sihitumaks, kus ründajad kulutasid rohkem aega ettevalmistustele ja keskendusid konkreetsetele sihtmärkidele, et tagada märgatavad häired süsteemide töös. Sageli koosnesid rünnakud kahest etapist: esmalt lühike rünnak, mille eesmärk oli hinnata sihtmärgi kaitset, ning seejärel pikem ja intensiivsem rünnak, kui esimene rünnak oli edukas. Need DDoS-rünnakud olid sageli seotud Eesti toetusega Ukrainale või uute sanktsioonide väljakuulutamisega Venemaa vastu, mis viitab poliitilisele motiivile küberrünnakute taga. Taoline poliitiliselt motiveeritud rünnakute suundumus on jätkuvalt murettekitav.

## 6.2 Kirjanduse analüüsi tulemused

Kirjanduse analüüsi tulemusel kaardistati kokku 43 turvariski. Tulemused on esitatud Tabelites 8 ja 9 ja kokku võetud Joonisel 13. Enamik neist (19) olid määratletud kui muukimise/rikkumise ohud (*Tampering*), 15 olid õiguste vallutamise ohud (*Elevation of privilege*), 4 olid seotud teabe avalikustamisega (*Information disclosure*), 4 olid teenustökestus/ummistus ohud (*Denial of service*) ning 1 oli seotud võltsimise/teeskluse/pettusega (*Spoofing*). Vaadeldud kirjanduses ei tuvastatud ühtegi salgamisohu (*Repudiation*).



Joonis 13. Kirjanduse analüüsis tuvastatud turvaohud

Iga turvaohu käsitletakse turvariski kaudu (vt. Lisa III), seega sisaldab Lisa rünnakumeetodeid, ohtusid, nõrkusi ja nende mõjusid. Nagu on määratletud artiklis [11] [29], nende komponentide kombinatsioon määratleb süsteemi ja organisatsiooni varade turvariski. Järgnevalt toome mõned näited turvastenaariumidest.

**Võltsimine/teesklus/pettus (*Spoofing*):** IP-aadressi teesklus [38]: Selle stsenaariumi korral on oht võime maskeerida pahatahtlikku liiklust seaduslikuks, muutes andmepakettide lähte-IP-aadressi. Sellega võib mööda minna turvameetmetest, mis tuginevad autentimisel IP-aadressidele, või käivitada rünnakuid teiste sihtmärkide vastu, tekitades mulje, et liiklus pärineb usaldusväärsest allikast. Peamine nõrkus seisneb selles, et arvutivõrk ei suuda autentida ega kinnitada paketi tegelikku päritolu. IP-aadressi võltsimise mõju võib olla märkimisväärne, ulatudes loata juurdepääsust võrgule ja andmete rikkumisest kuni arvutivõrgu kaasamiseni kolmandate isikute vastu suunatud rünnakutesse. Selle ohu vähendamiseks tuleks rakendada tugevaid arvutivõrgu turvameetmeid, nagu pakettide filtreerimine ja sissetungi tuvastussüsteemid, kasutada võltsimisvastaseid meetodeid võrgu piirides ning jälgida pidevalt arvutivõrgu liiklust kahtlase toimingute suhtes.

Tabel 8. STRIDE taksonoomia kohane turvaohutude klassifikatsioon (1)

| Artikkel                            | Võltsimine<br>( <i>Spoofing</i> ) | Muukimine/rikkumine ( <i>Tampering</i> )   | Salgamine<br>( <i>Repudiation</i> ) |
|-------------------------------------|-----------------------------------|--|-------------------------------------|
| Khalid <i>et al.</i> (2021) [23]    | –                                 | Koodiga manipuleerimine, pahavara, võrgu ussviirus, viirus, elutsükli jooksul paigaldatavad tagauksed, pealtkuulamine, riistvaraline tagauks.  | –                                   |
| Clark <i>et al.</i> (2017) [8]      | –                                 | Koodiga manipuleerimine, pahavara, viirus, elutsükli jooksul paigaldatavad tagauksed, pealtkuulamine, riistvaraline tagauks, vea süstimine, riistvara omavoliline muutmine, puhvri ületäitumine. | –                                   |
| Kutzler <i>et al.</i> (2021) [25]   | –                                 | Koodiga manipuleerimine.   | –                                   |
| Quarta <i>et al.</i> (2017) [35]    | –                                 | Vea süstimine.   | –                                   |
| Jablonski <i>et al.</i> (2021) [21] | –                                 | Füüsiline manipuleerimine anduritega, omavoliline seadete muutmine, omavoliline juurdepääs liidestele.   | –                                   |
| Chundhoo <i>et al.</i> (2021) [7]   | –                                 | Füüsiline ja digitaalne manipuleerimine.   | –                                   |
| Shah <i>et al.</i> (2020) [38]      | IP Aadresside võltsimine.         | Pahavara, pealtkuulamine, andmetega manipuleerimine, SQL süstimine, DNS pete.  | –                                   |
| Pu <i>et al.</i> (2023) [34]        | –                                 | Pahavara, andmetega manipuleerimine, operatiivne manipuleerimine.  | –                                   |

**Muukimine/rikkumine (*Tampering*):** Tarkvara koodiga manipuleerimine [23][8][38]: Selle stsenaariumi korral püüab ohuagent manipuleerida tarkvara koodi, et luua tagauks edaspidiseks juurdepääsuks, takistada kriitiliste süsteemide funktsionaalsust või varastada tundlikke andmeid. Tugevate turvameetmete puudumine tarkvara arenduse elutsükklis, näiteks põhjalik koodi kontroll ja automatiseeritud turvatestimine, loovad nõrkuse, mida ohuagent saab ära kasutada. Sellise rünnaku mõju võib olla kaugele ulatuv, mõjutades mitte ainult tarkvara terviklust, vaid võib tuua ka märkimisväärset kahju organisatsiooni tegevusele ja mainele.

**Teabe avalikustamine (*Information disclosure*):** Arvutivõrgu nuhkimine [38]: Selle stsenaariumi korral hõlmab oht arvutivõrgu liikluse loata hõivamist ja analüüsimist. See on eriti tõhus selliste võrkude puhul, mis edastavad andmeid krüpteerimata kujul või millel on nõrgad turvaseaded. Peamine nõrkus seisneb selles, et andmed ei ole kaitstud edastamise ajal ning arvutivõrgu järelevalvemehhanismid on ebapiisavad. Arvutivõrgu nuhkimise mõju võib olla märkimisväärne, kuna see võib viia tundliku teabe ohustamiseni, mida saab kasutada edasiseks pahatahtlikuks tegevuseks.

Tabel 9. STRIDE taksonoomia kohane turvaohutude klassifikatsioon (2)

| Artikkel                            | Teabe avalikustamine ( <i>Information disclosure</i> ) | Teenustõkestus ( <i>Denial of service</i> )      | Õiguste vallutus ( <i>Elevation of privilege</i> )  |
|-------------------------------------|--|--|---|
| Khalid <i>et al.</i> (2021) [23]    | Pealtkuulamine.  | Ummistus (teenustõkestus).                       | IT-infrastruktuuri füüsiline hävitamine.  |
| Clark <i>et al.</i> (2017) [8]      | Pealtkuulamine.  | –  | –   |
| Quarta <i>et al.</i> (2017) [35]    | –  | –  | IT-infrastruktuuri füüsiline hävitamine, mikrovigade sissestamine, ohutussätete välja lülitamine või muutmine, autoriseerimata juurdepääs süsteemidele ja andmetele, kaugvõrgu nõrkuste ärakasutamine, siseringkonna poolt võimaldatav võrgu rünnak (kohalik juurdepääs). |
| Jablonski <i>et al.</i> (2021) [21] | –  | –  | IT-infrastruktuuri füüsiline hävitamine, juurdepääsulubade vargus ja kloonimine, käskude süstimine.   |
| Chundhoo <i>et al.</i> (2021) [7]   | Vahendusrünnak.  | SYN üleujutus, mitme ründevektori kombinatsioon. | Unepuudus.  |
| Shah <i>et al.</i> (2020) [38]      | Võrgu nuhkimine, pealtkuulamine, vahendusrünnak.       | Ummistus (teenustõkestus).                       | Tarkvara või riistvara pöördprojekteerimine, jõurünnak, taasesitusrünnak, õngitsus, paroolirünnak.  |
| Pu <i>et al.</i> (2023) [34]        | –  | Ummistus (teenustõkestus), lunavara.             | –   |

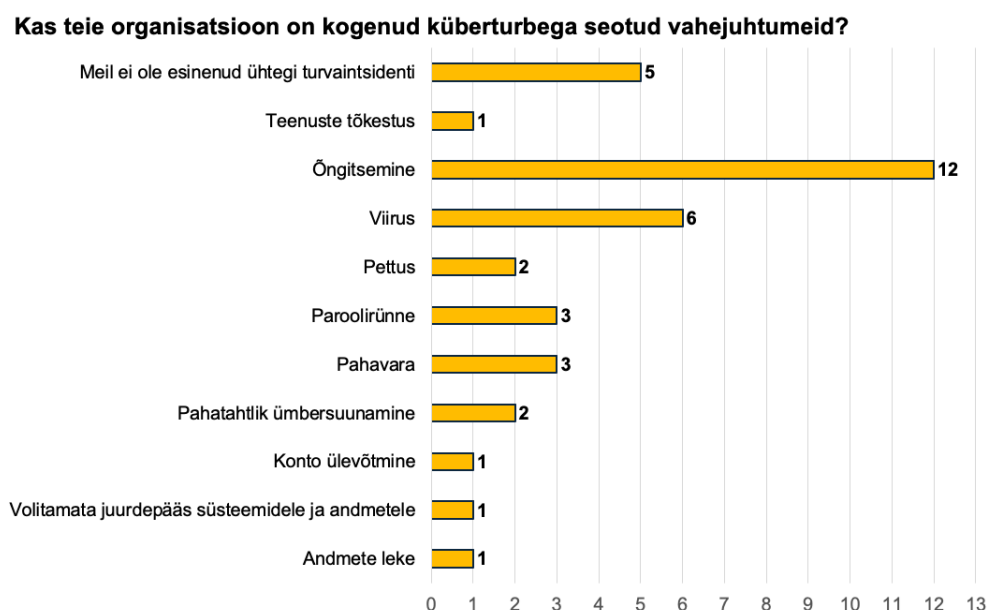
**Teenustõkestus/ummistus (*Denial of service*):** Teenustõkestus/ummistus [23][38] [34]: Selle stsenaariumi korral on rünnaku eesmärk kahjustada küberturvalisuse käideldavuse aspekti. Erinevalt teistest rünnakutest, mis varastavad või rikuvad andmeid, on rünnakute eesmärk eelkõige süsteemi ressurside üle koormamine, põhjustamaks häireid teenustes. Selles kontekstis on nõrkused sageli seotud ebapiisava valmisolekuga ootamatuteks arvutivõrgu liikluse piikideks. Näiteks ei ole olemas skaleeritavat infrastruktuuri või täiustatud ohu tuvastamise ja tõrjumise vahendeid. Mõju on märkimisväärne, eriti organisatsioonide jaoks, kes sõltuvad veebipõhisest kohalolekust ja veebipõhistest teenustest, kuna see mõjutab vahetult nende võimet tegutseda ja säilitada klientide usaldust. Nende riskidega tegelemiseks on vaja strateegilist kombinatsiooni, mis koosneb tugevast arvutivõrgu arhitektuurist, reaajas jälgimisvahenditest ja hädaolukorra

planeerimisest liikluse ülekoormuse stsenaariumide korral.

**Õiguste vallutus** (*Elevation of privilege*): Infotehnoloogia infrastruktuuri füüsiline hävitamine [23][35][21]): Selle stsenaariumi puhul iseloomustab rünnakut füüsiline tegevus, mis kahjustab või hävitab infotehnoloogilist vara. Seda tüüpi oht jäetakse küberturvalisuse planeerimisel sageli tähelepanuta, kuna keskendutakse pigem digitaalsetele ohtudele. Füüsiline turvalisus on aga üldise infotehnoloogia turvalisuse kriitiline aspekt. Nõrkused tulenevad tavaliselt ebapiisavatest kaitsemeetmetest, näiteks ebapiisavatest füüsilistest tõketest, järelvalvest või juurdepääsu piirangutest tundlikele aladele. Sellise rünnaku mõju võib olla tõsine ja kohene, mõjutades mitte ainult riistvara, vaid ka andmeid ja teenuseid, mis sõltuvad sellest riistvarast. Selle riski tõhus haldamine hõlmab tugevaid füüsilisi turvameetmeid ning põhjalikku hädaolukorra taastamise ja talitluspidevuse planeerimist, et vähendada mõju ja tagada kiire taastumine selliste intsidentide korral.

### 6.3 Küsitluse tulemused

Küsitluse käigus uurisime, kas ettevõtte on kogenud mingeid turvariske. Teatati 32 juhtumist (vt Joonis 14), kus kõige sagedamini esinesid andmepüügi rünnakud, millele järgnesid viirused ja muud ohud.



Joonis 14. Vastajate osutatud turvalisuse ohud

### 6.4 Arutelu

Turvaohte võib täheldada automatiseeritud süsteemide ja tehnoloogiate erinevates komponentides. Üks tõhus vahend sellise analüüsi läbiviimiseks on referents- või arhitektuuriraamistik, nagu

näiteks RAMI 4.0, mis pakub juhiseid süsteemi võimalike varakomponentide ja funktsionaalsete üksuste kohta. Teine lähenemine võib olla keskendumine teabetöötamise funktsioonidele, mis hõlmavad teabe kogumist, edastamist, salvestamist, pärimist, töötlemist ja kuvamist. Need funktsioonid moodustavad andmete ja teabe töötlemise perimeetri, kus ärivara, nagu andmed ja teave, võib muuta oma vormi ja seisundit, olles seeläbi haavatav ning seda on võimalik ära kasutada.

Oluline on mitte ainult tuvastada turvaohutuse sümptomeid, vaid ka uurida, miks oht oli võimalik (millised on süsteemi nõrkused), kuidas oht realiseerus (millised olid rünnaku meetodi sammud) ja kuidas see mõjutab süsteemi (kuidas see kahjustab süsteemi ja ärivara ning eirab turvakriteeriume).

Analüüsis rõhutatakse erinevate küberintsidentidega kokku puutuvate ettevõtete seas kasvavat trendi, kus enamik vastanutest nimetas õngitsusrünnakuid levinumaiks probleemiks. Sellele järgnevad tihedalt viiruste või pahavaraga nakatumised. Kuna organisatsioonid tuginevad info-tehnoloogia süsteemidele ja tootmisprotsessid on omavahel seotud, suureneb tõenäosus, et nad seisavad silmitsi turvaintsidentidega.

Tuginemine digitaaltehnoloogiale ja sidestatud toimingutele tekitab nõrkusi, mida küberründajad ära kasutavad, rõhutades kriitilist vajadust turvalaste vastumeetmete järele. Õngitsusrünnakute levik rõhutab töötajate pideva koolituse ja teadlikkuse tõstmise vajadust ning tähtsust, kuna need ohud on suunatud üksikisikutele läbi eksitavate e-kirjade või sõnumite<sup>4</sup>.

---

<sup>4</sup>Uuri lisa <https://cyberphish.eu/learn>

## 7 Turvalisuse vastumeetmed automatiseeritud süsteemides ja tehnoloogiates

Käesolevas peatükis tutvustame analüüsitud kirjanduses leitud turvameetmeid. Tuletame meelde, et turvariskide käsitlemise otsused hõlmavad riski säilitamist (st otsust mitte sekkuda või aktsepteerida risk), riski ülekandmist (st otsust jagada riskiga seotud kahjude koormust), riski vältimist (st otsust mitte sekkuda või loobuda riskist, muutes süsteemi või loobudes sellest) ja riski vähendamist (st meetmeid riskiga seotud tõenäosuse, negatiivsete tagajärgede või mõlema vähendamiseks). Riski vähendamise otsuse tulemuseks on turvanõuete väljaselgitamine ja turvakontrollide implementeerimine tuvastatud riskide vähendamiseks. Käesolevas peatükis esitatakse turvanõuded ja kontrollimeetmed, et vähendada automatiseeritud süsteemide ja tehnoloogiate turvariske.

### 7.1 Kirjanduse analüüsi tulemused

Tuginedes STRIDE raamistikule, mis on loodud ohu tuvastamiseks ja klassifitseerimiseks, kasutame STRIDE'i sihipäraste vastumeetmete väljatöötamiseks. Need vastumeetmed on mõeldud tuvastatud ohtude kõrvaldamiseks ja neutraliseerimiseks, tagades konkreetsetele turvanõuetele kohandatud kaitsemehhanismid. Riskide vähendamise strateegiad võivad erineda sõltuvalt automatiseeritud süsteemide ja tehnoloogiate tüübist, spetsiifikast, keerukusest ja valdkonnast.

Ohupõhiste nõuete väljaselgitamise lähenemisviis toetab turvanõuete liigitamist kolme rühma - ennetav (**E**), avastav (**A**) ja korrigeeriv (**K**). Me tähistame tuvastatud turvanõudeid atribuutidega E, A ja K. "Süsteem" mõiste turvanõuetes viitab automatiseeritud süsteemidele ja tehnoloogiatele ning nende komponentidele.

Tabelis 10 on esitatud nõue ja kontroll võltsimisrännaku leevendamiseks. Kuigi me keskendume ühele kontrollile, tunnustame, et muud vastumeetmed (nagu biomeetriline autentimine, volituste haldamise põhimõtted jne) võivad olla alternatiiviks mitmefaktorilise autentimise jaoks. Joonisel 18 on kujutatud sõltuvust teabe töötlemise funktsioonide (nagu teabe edastamine), IP-aadressi võltsimise ning selle vastumeetmete vahel.

Tabel 10. Turvanõuded [3] [4] ja kontrollid võltsimisriskide vähendamiseks

| Turvanõuded                                  | Turvakontrollid                   |
|--|-----------------------------------|
| SS1.R1: Süsteem peaks autentima kasutaja (E) | Mitmefaktoriline autentimine [34] |

Tabelis 11 on esitatud turvalisuse vastumeetmed võltsimisohu vähendamiseks. Enamik turvanõuetest viitab ennetavatele turvastrateegiatele (välja arvatud nõue ST3.R1, mis nõuab korrigeerivat turvastrateegiat). Määratud turvakontrolli meetmed hõlmavad teabevahetuse krüpteerimisprotokolle, riistvara ülevaatus, käskude valget nimekirja (lubatakse ainult eelnevalt kindlaks määratud käsud), privaatvõrkude kasutamist ning turvaliste programmeerimistavade rakendamist.

Vastumeetmed teabe avalikustamise riskide vähendamiseks on esitatud Tabelis 12. Enamik strateegiaid (välja arvatud nõue SID3.R.2) keskendub avastamisstrateegiatele. Kirjanduses soovi-

Tabel 11. Turvanõuded [3] [4] ja kontrollid võltsimisohu vähendamiseks

| <b>Turvanõuded</b>   | <b>Turvakontrollid</b>                         |
|--|--|
| <b>ST1.R1:</b> Süsteem peaks kasutama volituste andmiseks turvalisi protokolle (E)<br><b>ST1.R2:</b> Süsteem peaks suhtlema andmehoidlaga kanali kaudu, mis on kaitstud krüpteerimisprotokolliga (E)   | Sidepidamise krüpteerimisprotokollid [8], [34] |
| <b>ST2.R1:</b> Süsteemi komponendid peaksid järgima kvaliteedipoliitikat (E)<br><b>ST2.R2:</b> Organisatsioon peaks kontrollima füüsilist juurdepääsu ülekandekanalitele organisatsiooni rajatistes (E)  | Riistvara ülevaatus [8]                        |
| <b>ST3.R1:</b> Süsteem peaks teostama sisendandmete valideerimist (K)<br><b>ST3.R2:</b> Süsteem peaks määratlema piirangud kasutaja poolt sisestatud andmetele (E)<br><b>ST3.R3:</b> Süsteemi liidesed peaksid varjama tundlikke andmeid välise teabevahetuse ajal (E)<br><b>ST3.R4:</b> Süsteem peaks võimaldama sisendite edastamist ainult lubatud allikatest (E) | Käskude valgesse nimekirja kandmine [41]       |
| <b>ST4.R1:</b> Enne ühenduse loomist peaks süsteem läbi viima seadme autentimise (E)<br><b>ST4.R2:</b> Süsteem peaks tagama edastatud teabe konfidentsiaalsuse (E)<br><b>ST4.R3:</b> Süsteem peaks järgima traadita side võimaluste eeskirju (E)   | Virtuaalsete privaativõrkude kasutamine [34]   |
| <b>ST5.R1:</b> Organisatsiooni infoturbe töötajad peaksid enne süsteemi käivitamist läbi viima staatilisi koodianalüüse (E)<br><b>ST5.R2:</b> Organisatsiooni infoturbe töötajad peaksid käivitatava süsteemi jaoks läbi viima dünaamilise programmi analüüsi (E)  | Turvalise programmeerimise tavad [8]           |

tatakse rakendada lahendusi kasuliku koormuse tuvastamiseks, anomaaliade avastamiste häireid ja protokollide seisundi jälgimist.

Teenustõkestusriski vähendamiseks võib rakendada ennetavaid, avastavaid ja korrigeerivaid turvastrateegiaid, mida illustreerivad Tabelis 13 esitatud turvanõuded. Sellest tulenevalt soovitatakse kirjanduses kasutada sissetungi tuvastussüsteeme, andmepakettide lühiajalist nummerdamist, regulaarseid uuendusi ja parandusi, algatatud ja loodud TCP-ühenduste võrdlemist, andmeliikluse juhtimist ja piiranguid ning regulaarseid varukoopiaid.

Tabelis 14 on loetletud vastumeetmed õiguste vallutamise riskide vähendamiseks. Kirjanduses soovitatakse kahte turvakontrolli: kasutajate sõelumist ja kasutajate juurdepääsu haldamist. Need turvakontrollid saavutatakse turvanõuete rakendamisega, mis enamasti hõlmavad ennetavaid turvastrateegiaid, välja arvatud nõuded SEP1.R2 (korrigeeriv strateegia) ja SEP2.R4 (avastamisstrateegia).

Tuvastatud turvameetmed muutuvad pärast nende rakendamist autonoomsete süsteemide ja tehnoloogiate osaks. See tähendab, et neist saavad süsteemi varad, mis toetavad vastavaid äriarvaid. Organisatsioon peaks pidevalt jälgima nende turvalisuse taset ning seega potentsiaalselt

Tabel 12. Turvanõuded [3] [4] ja kontrollimeetmed teabe avalikustamise riskide vähendamiseks

| Turvanõuded  | Turvakontrollid  |
|--|--|
| <b>SID1.R1:</b> Infoturbe töötajad peaksid analüüsima süsteemi logisid vastavalt logihalduspoliitikale (A) | Võrgus edastatavate andmete tuvastamise lahendused [8] |
| <b>SID2.R1:</b> Süsteem peaks tuvastama volitamata ühendused võrku (A)                                     | Anomaalia tuvastamise häire [41]                       |
| <b>SID3.R1:</b> Süsteem peaks kontrollima edastatud andmete terviklust (A)                                 | Protokolli seisundi jälgimine [41]                     |
| <b>SID3.R2:</b> Süsteem peaks kaitsma kogu kasutaja sessiooni (E)  |  |

tuvastama ja hindama lisatud vastumeetmete turvariske.

## 7.2 Küsitluse tulemused

Turvaohude vastumeetmete kohta tehtud küsitluses tuuakse esile erinevaid strateegiaid, mida ettevõtte kasutavad oma varade kaitsmiseks. Nagu on näidatud Joonisel 15, kasutavad ettevõtte automatiseeritud turvalahendusi (10 vastust) ja küberturvalisuse eest vastutab IT-osakond (10 vastust). Töötajad osalevad koolitustel ja teadlikkuse tõstmise programmides (12 vastust). Viimast kinnitab ka Joonis 16, kus kasutatakse veebipõhiseid koolitusi ja vahendeid (8 vastust), korraldatakse korrapäraseid küberturvalisuse koolitusi töötajatele (7 vastust) ning korraldatakse spetsiaalseid koolitusi IT- ja infoturbe töötajatele (6 vastust). Samas näitavad tulemused ka seda, et mõnes ettevõttes ei korraldata ametlikke küberturvalisuse koolitusi (8 vastust).

Turvaintsidentide leevendamiseks on kõige populaarsemad meetmed regulaarsed tarkvara uuendused ja paranduste haldamine (15 vastust), tulemüürid ja sissetungi tuvastus- ja -tõrjesüsteemid (14 vastust), kasutajate õiguste piiramine ja juurdepääsukontrollid (13 vastust) ning viirusetõrje- ja pahavara vastased lahendused (13 vastust).

## 7.3 Arutelu

Turvariskide käsitlemise meetmed toetavad turvariskide ennetamise, avastamise ja korrigeerimise strateegiaid, vähendades turvariskide mõju. Organisatsiooni esimene samm peaks olema turvariskide käsitlemise otsus, mis hõlmab riski säilitamist, riski ülekandmist, riski vältimist või riski vähendamist. Seejärel aitab järgnev otsus kaasa turvastrateegiate täpsustamisele vastavalt turvanõuetele ja turvariskidele. Selles peatükis oleme esile toonud turvanõuded ja nende rakendamiseks vajalikud turvakontrollid. Joonistel 18–22 illustreerime infotöötlusfunktsiooni, turvariskide ja -ohtude ning turvalisuse vastumeetmete vahelist seost. Neid näiteid võib pidada kontrollnimekirjaks turvariskide vähendamise strateegiate määratlemisel.

Küsitluse tulemused turvaohude vastumeetmete kohta näitavad, et organisatsioonid rakendavad erinevaid strateegiaid oma vara kaitsmiseks. Organisatsioonide tavapoliitikasse on integreeritud mitmesugused turvameetmed, mis rõhutab mitmekülgse lähenemisviisi tähtsust küberriskide

Tabel 13. Turvanõuded [3] [4] ja kontrollmehhanismid teenustõkestuse riskide maandamiseks

| <b>Turvanõuded</b>  | <b>Turvakontrollid</b>                            |
|---|---|
| <b>SDS1.R1:</b> Süsteem peaks tuvastama süsteemi piirangute kahjustamise (A)  | Sissetungi tuvastamise süsteem [38]               |
| <b>SDS2.R1:</b> Süsteem peaks järgima andmehalduspoliitikat (K)   | Andmepakettide arv lühikese aja jooksul [38]      |
| <b>SDS3.R1:</b> Süsteem peaks järgima välissüsteemide kvaliteedipoliitikat (E)<br><b>SDS3.R2:</b> Süsteem peaks pärast tarkvara uuendusi jääma terviklikuks (E)<br><b>SDS3.R3:</b> Süsteem peaks käivitama ainult lubatud programme (E)   | Regulaarsed uuendused/parandused [41], [38], [34] |
| <b>SDS4.R1:</b> Süsteemil peaks olema sidepidamise varukanal (K)  | Võrrelda algatatud ja kestvaid TCP-ühendusi [38]  |
| <b>SDS5.R1:</b> Süsteem peaks kasutama kaugjuhtimiseks krüpteerimisprotokolliga kaitstud kanalit (E)<br><b>SDS5.R2:</b> Süsteem peaks tasakaalustama sissetulevat arvutivõrgu liiklust (K)  | Liikluse korraldamine ja piirangud [41], [38]     |
| <b>SDS6.R1:</b> Süsteem peaks kasutama varukoopiaid organisatsioonilise teabe taastamiseks (E)<br><b>SDS6.R2:</b> Organisatsioon peaks tagama andmete varundamise kaitse (E)<br><b>SDS6.R3:</b> Süsteemil peaks olema tsentraalne logide halduse kontroll (A)<br><b>SDS6.R4:</b> Süsteem peaks teostama toimingute logimist süsteemi komponentide kohta (A)<br><b>SDS6.R5:</b> Süsteem peaks säilitama süsteemi komponentide logide ajatemplite järjepidevuse (E) | Regulaarne varunduste genereerimine [34]          |

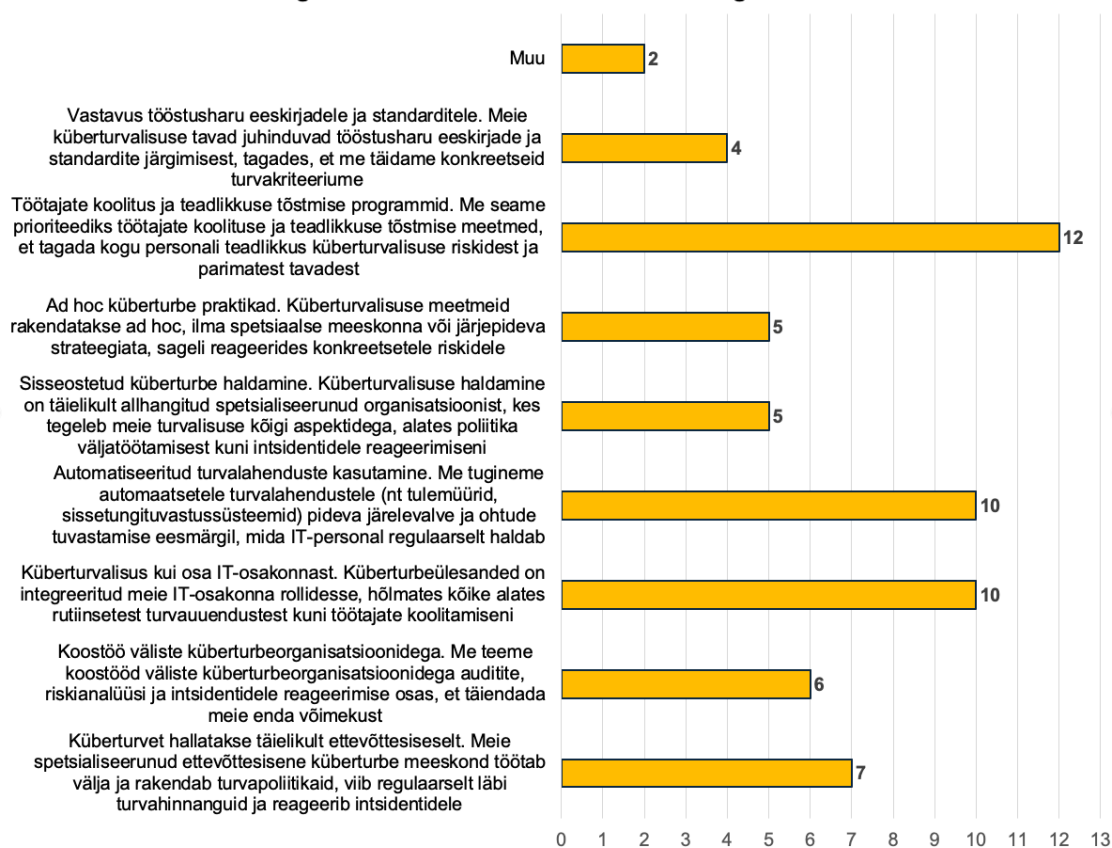
vastu võitlemisel. Näiteks infotehnoloogiliste süsteemide regulaarne uuendamine viimastele versioonidele ja kasutajate juurdepääsu kontrollimine on peamised meetmed, mida peetakse kohustuslikeks kõigis sektorites. Need meetmed on olulised organisatsiooni turvalisuse taseme tõstmisel ja nõrkuste vähendamisel.

Lisaks tehnilistele kaitsemeetmetele rõhutavad uuringu tulemused töötajate pideva küberturvalisuse koolituse olulisust. Arvestades digitaalse maastiku dünaamilist olemust, kus tehnoloogilised edusammud ja ohud arenevad kiiresti, on töötajate teavitamise ja valvsuse säilitamise tähtsus hindamatu. Regulaarsed koolitused loovad teadlikkuse kultuuri, mis varustab töötajaid teadmistega, et nad suudaksid tuvastada võimalikke turvaintsidente ja neile tõhusalt reageerida. Selline ennetav lähenemine küberturvalisuse koolitustele on hädavajalik, et vastu seista üha keerukamatele sihtrünnakutele, mis sageli kasutavad ära inimfaktoreid.

Tabel 14. Turvanõuded [3] [4] ja kontrollid õiguste vallutamise riskide maandamiseks

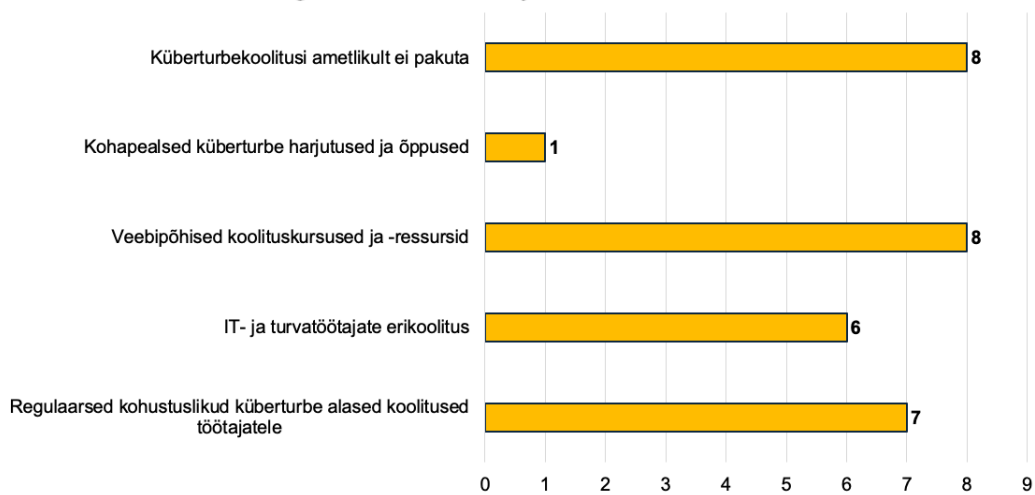
| Turvanõuded  | Turvakontrollid                                 |
|--|---|
| <p><b>SEP1.R1:</b> Organisatsioon peaks järgima kasutajate haldamise poliitikat (E)</p> <p><b>SEP1.R2:</b> Süsteem peaks eraldama eri kasutajate rollid (K)</p> <p><b>SEP1.R3:</b> Süsteem peaks autentima andmelao kasutajaid (E)</p> <p><b>SEP1.R4:</b> Süsteem peaks kaitsma mobiilsetes seadmes kuvatavaid tundlikke andmeid (E)</p> <p><b>SEP1.R5:</b> Süsteem peaks juhendama kasutajaid, kuidas määrata konkreetseid seadistusi süsteemiga suhtlemiseks kasutatavates mobiilsetes seadmetes (E)</p> | <p>Kasutajate kontroll ja isoleerimine [38]</p> |
| <p><b>SEP2.R1:</b> Süsteem peaks rakendama juurdepääsu kontrollimise mehhanismi (E)</p> <p><b>SEP2.R2:</b> Süsteem peaks autoriseerima juurdepääsu andmelao kasutajatele (E)</p> <p><b>SEP2.R3:</b> Süsteem peaks säilitama kasutajate kasutajatunnuseid turvaliselt (E)</p> <p><b>SEP2.R4:</b> Süsteem peaks registreerima juurdepääsu katsed oma liidestele (A)</p>  | <p>Kasutajatete juurdepääsu haldamine [38]</p>  |

### Kuidas teie organisatsioonis käsitletakse küberturbega seotud teemasid?



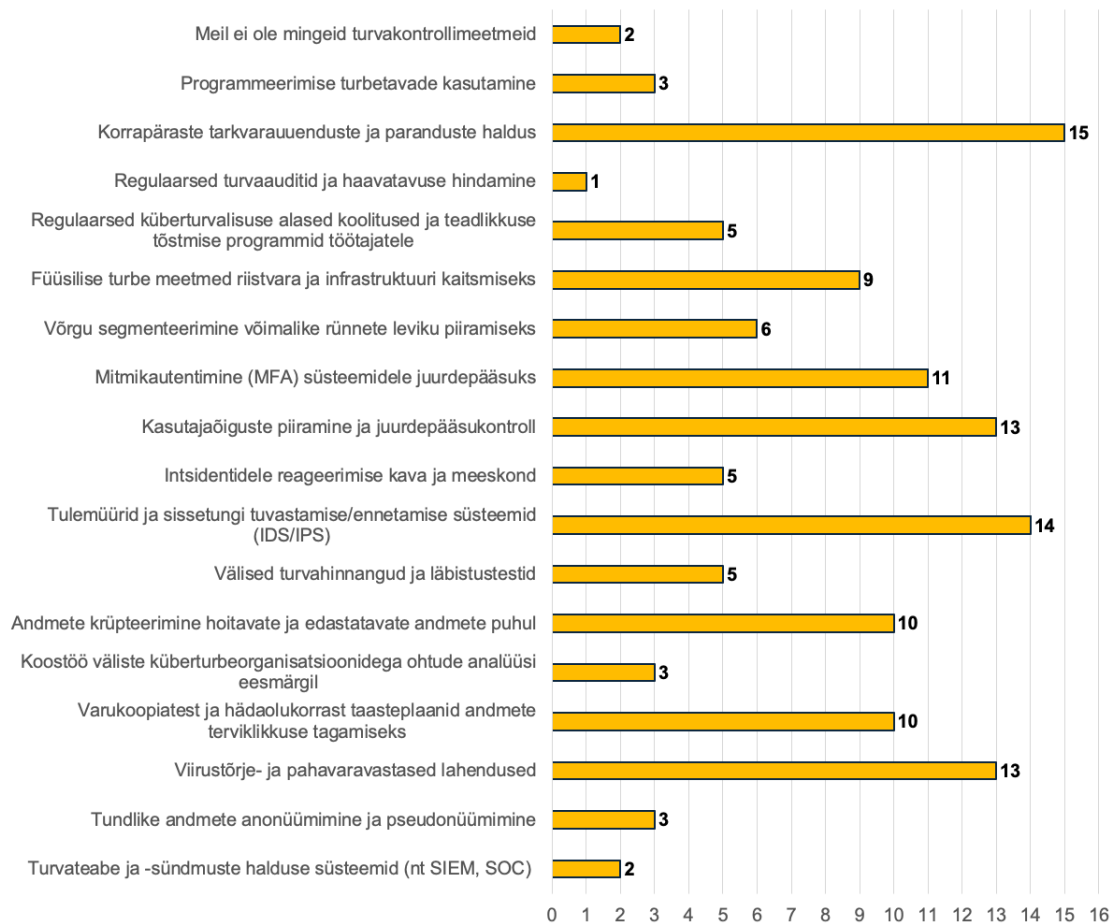
Joonis 15. Ettevõtetes turvalisusega seotud teemade käsitus

**Kuidas toimub teie organisatsioonis töötajate küberturbealane koolitamine?**

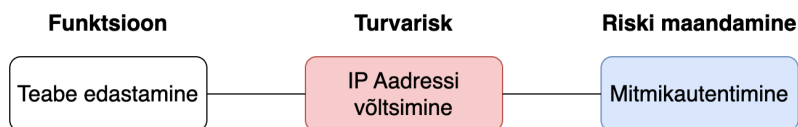


Joonis 16. Turvalisuse alane koolitus ettevõtetes

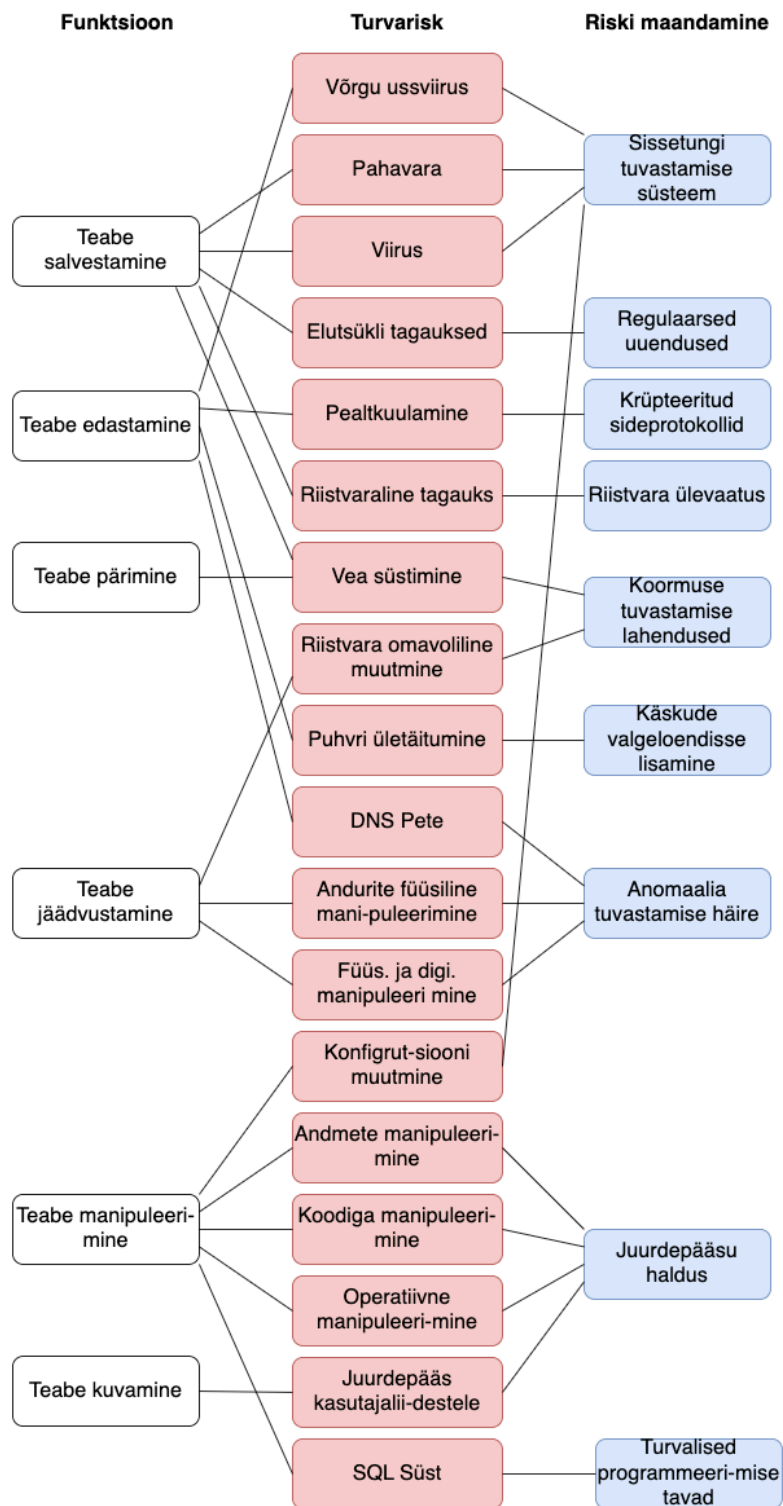
**Milliseid vastumeetmeid rakendab teie organisatsioon küberturbe intsidentide vähendamiseks?**



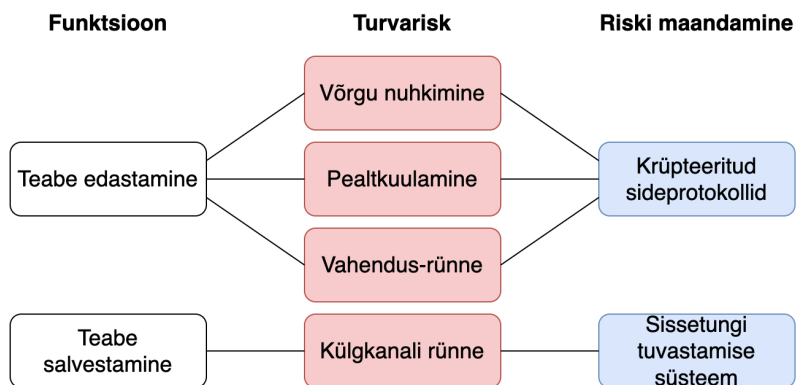
Joonis 17. Vastumeetmed turvasündmuste leevendamiseks



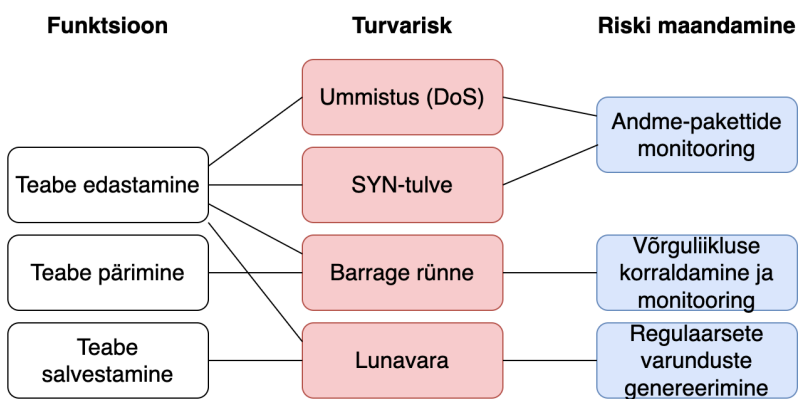
Joonis 18. Infotöötlus funktsiooni (süsteemi varade), pettuse ohtude ja turvameetmete vastastikune sõltuvus



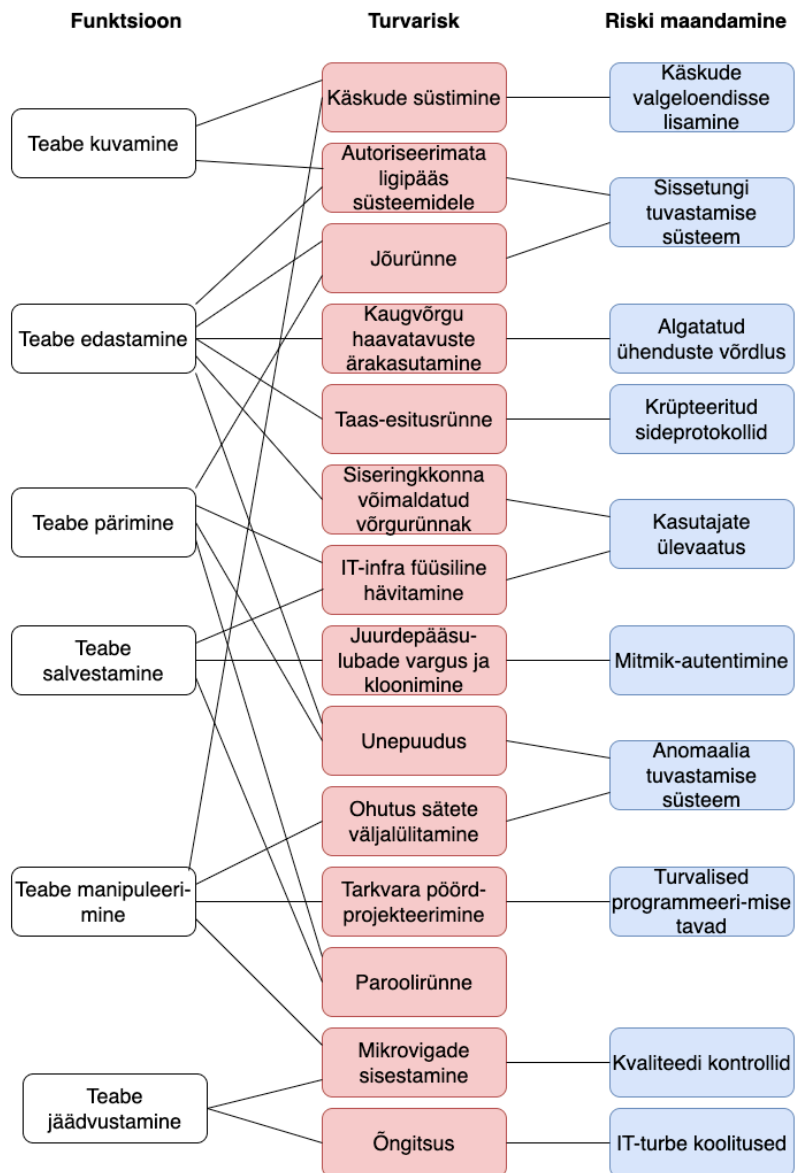
Joonis 19. Infotöötlus funktsiooni (süsteemi varade), rikkumise ohtude ja turvameetmete vastastikune sõltuvus



Joonis 20. Infotöötlus funktsiooni (süsteemi varade), teabe avalikustamise ohtude ja turvameetmete vastastikune sõltuvus



Joonis 21. Infotöötlus funktsiooni (süsteemi varade), ummistus ohtude ja turvameetmete vastastikune sõltuvus



Joonis 22. Infotöötlus funktsiooni (süsteemi varade), õiguste vallutus ohtude ja turvameetmete vastastikune sõltuvus

## 8 Siseringi turvariskid tootmistellimuste töötlemisel

Selles peatükis võetakse uuesti luubi alla juhtumiuuring [28] keskmise suurusega tootmisettevõttest, kus töötab umbes 80 inimest. Ettevõtte on spetsialiseerunud elektri- ja mootoriseadmete keerukate metallkomponentide täpsele CNC-töötlustele (st kõrgelt automatiseeritud mehaaniline tööriist, mis kasutab CAD või CAM vahenditega genereeritud programme). Selles peatükis illustreerime, kuidas saab rakendada peatükis 2.1 esitatud ISSRM-i lähenemist antud juhtumi puhul, keskendudes protsessidele, mis on seotud siseringi ohtudega. Analüüsi toetamiseks on juhtumi stsenaariumid esitatud äriprotsessi mudeli ja notatsiooni (BPMN)<sup>5</sup> abil.

### 8.1 Konteksti analüüs

Stsenaarium toob esile tellimuste vastu võtmise ja täitmisega seotud protsessid, pöörates erilist tähelepanu turvameetmete tõhustamisele. CNC-töötlemistellimuse täitmise põhiprotsess on näidatud Joonisel 23, ja tootmise teostamise alamprotsessid on esitatud Joonisel 24. Ettevõtte kasutab tellimuste elutsükli haldamiseks ettevõtte ressursside planeerimise süsteemi (ERP), mis haldab sisse tulevaid, käimasolevaid ja lõpetatud tellimusi. Erinevatel tasanditel töötavad töötajad, näiteks juhtivtöötajad ja tehase töötajad, sisestavad süsteemi andmeid. Tootmisprotsessi andmeid hoitakse kohalikes serverites, kuid andmete salvestamise süsteemil puudub järelvalve seni teadmata põhjustel.

Ettevõtte on juurutanud kiibipõhise süsteemi, mis jälgib töötajate kohalolekut, eesmärgiga tugevdada juhtimiselast järelvalvet. See süsteem pakub juhtkonnale ülevaadet töötajate kohaloleku harjumustest. Lisaks jälgib ettevõtte sissetulevat tööstusmaterjali. Siiski ei jälgita raisku läinud tööstusmaterjali ja vigaseid tooteid.

### 8.2 Tööstusspionaaž

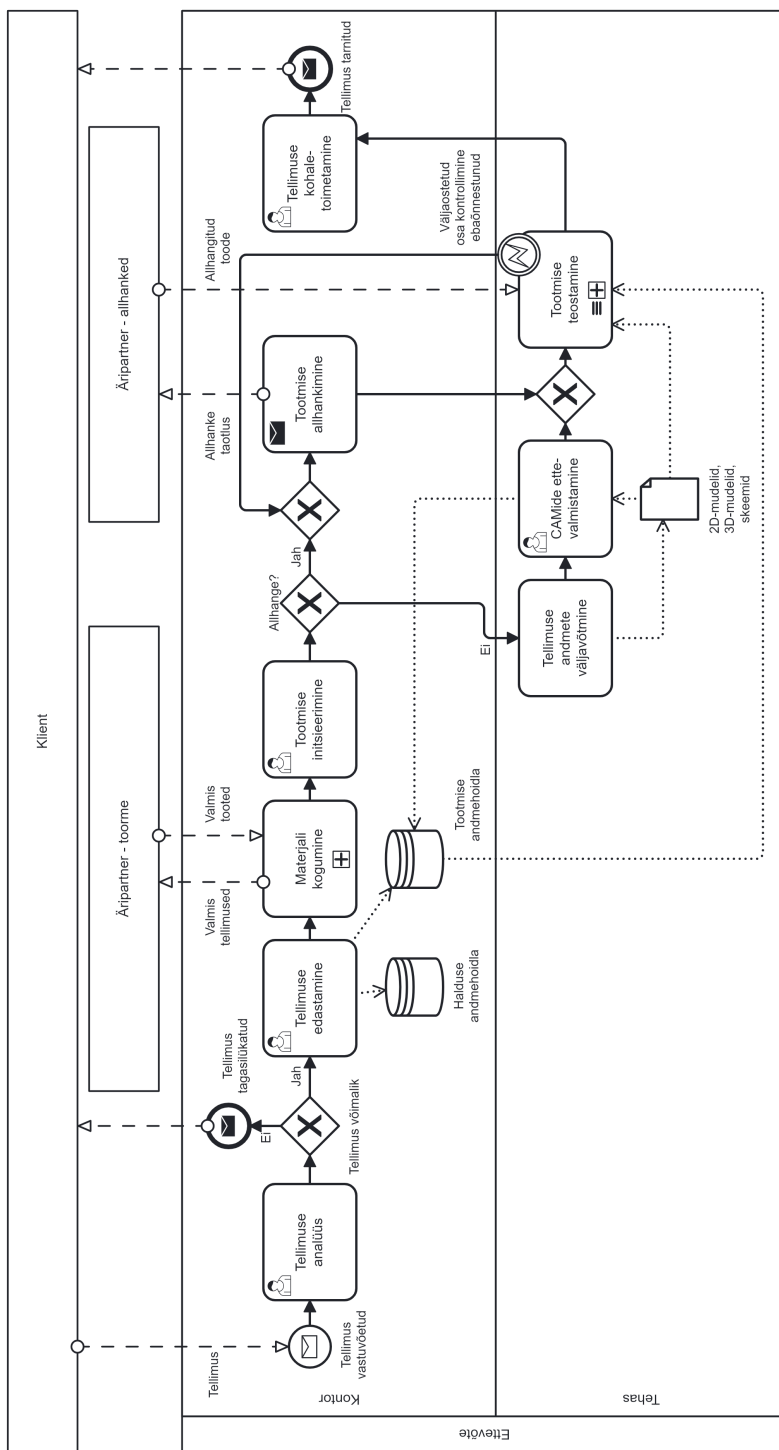
Tabel 15 illustreerib varade analüüsi, tööstusspionaaži riski ja võimalikku riski vähendamise lahendust.

**Varade identifitseerimine:** Selles stsenaariumis hoitakse tellimuste töötlemisega seotud andmeid, näiteks toote kujundusi ja mudeleid, serveris, mis on jaotatud kaheks peamiseks valdkonnaks:

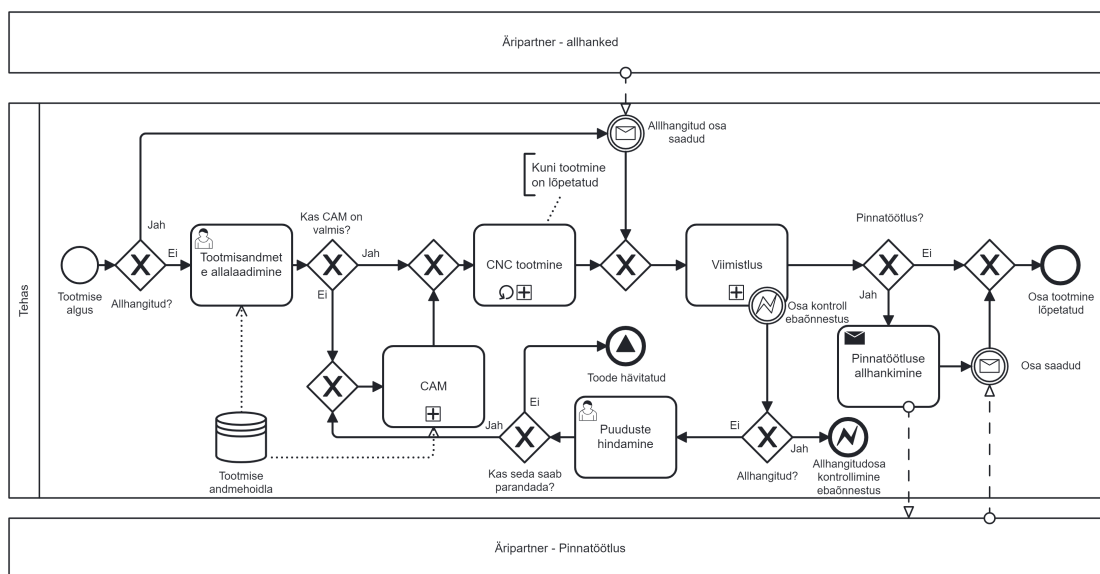
- **Haldus** hoiab andmeid jooksvate tellimuste, varukoopiate ja arhiivide kohta. Sellele alale ja selle kaustadele on juurdepääs ainult ettevõtte juhtkonnal.
- **Tootmine** haldab teavet käimasolevate tootmistellimuste kohta, sealhulgas toote tunnuseid, tehnilisi jooniseid, mudeleid ja koguseid. See osa on avatud kõigile ettevõtte töötajatele.

**Riskianalüüs:** Tundlik teave on kättesaadav kõigile ettevõtte töötajatele või väljastpoolt tulnud isikutele, kes esinevad ettevõtte töötajana. Nagu näidatud Joonisel 25, töötajad (st siseringi töötajad) võivad ühendada oma seadme ettevõtte võrku või kasutada juba olemasolevat

<sup>5</sup><http://www.omg.org/spec/BPMN/2.0/>



Joonis 23. Tellimuste töötlemise stsenaarium, kohandatud allikast [28]



Joonis 24. Tootmise teostamise stsenaarium, kohandatud allikast [28]

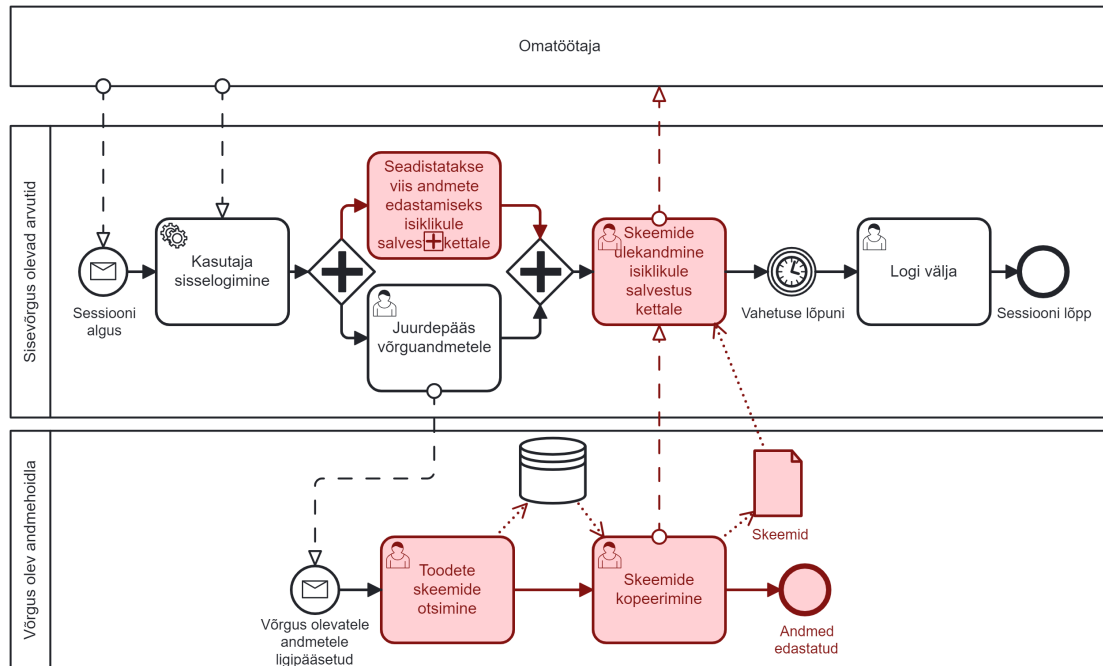
Tabel 15. Tööstusspionaazi riskijuhtimine, kohandatud allikast [28]

|                      |  |
|----------------------|--|
| <b>Ärivarava</b>     | Toodete skeemid  |
| <b>Süsteemi vara</b> | Tootmise kõvaketas   |
| <b>Risk</b>          | Siseringi töötaja, kellel on juurdepääs ettevõtte kõvakettale, avastab salvestatud toodete skeemid ja kopeerib need isiklikule salvestusseadmele, kasutades ära olukorda, kus juurdepääs ettevõtte kõvakettale ei ole piisavalt jälgitav ega analüüsitav. See toob kaasa andmete lekke, nende konfidentsiaalsuse kaotuse ning ettevõtte kõvaketta töökindluse ohu. |
| <b>Mõju</b>          | Andmete konfidentsiaalsuse kadu, varastatud andmed, andmete salvestussüsteemi (serveri) töökindluse kadu.  |
| <b>Nõrkus</b>        | Juurdepääsu ettevõtte andmete salvestussüsteemidele ei jälgita ega analüüsita nõuete kohaselt.   |
| <b>Ohu agent</b>     | Ettevõtte tootmise kõvakettale ligipääsuga siseringi töötaja.  |
| <b>Ründemeetod</b>   | Siseringi töötaja leiab ettevõtte kõvakettalt veel avaldamata toodete skeemid ja kopeerib need isiklikule salvestusseadmele.   |
| <b>Turvanõue</b>     | Turvasüsteem reageerib tööstusspionaazi kahtlustele.   |
| <b>Kontroll</b>      | Nõuete kohane andmete säilitamise jälgimise seadistamine, töötajate toimingute logimine ja protsesside kaeve genereeritud andmete kohta.   |

arvutit, näiteks tootmisüksuse kontrollimise arvutit. Sealt võivad nad ligi pääseda vähemalt tootmisserveritele ning otsida ja endale kopeerida väärtuslikke andmeid, mis neil leida õnnestub.

**Riski vähendamine:** Tööstusspionaazi leevendamiseks on oluline jälgida andmete hoiustamist, eriti haldus- ja tootmispiirkondades. Süsteem peaks jälgima, kes failidele juurde pääseb,

neid loeb või muudab. Analüüsid failide kasutamist ajas, saame aru töötajate tavapärasest käitumisest ja sellest, kes neid salvestusruume kasutavad. See teave võimaldab meil luua kasutajate käitumise mudelid. Seejärel saame rakendada tehnikaid, mis kontrollivad, kas praegune toiming vastab nendele mustritele. Selline kontrollsüsteem peaks olema ettevõtte serverites ja jälgima pidevalt kõiki toiminguid ja tuvastama toimingud, mis ei vasta normile. Kui leitakse midagi ebatavalist, võib kontrollsüsteem automaatselt otsustada, kuidas kõige paremini reageerida, arvestades toimingu riskantsust ja potentsiaalset kahju ettevõttele.



Joonis 25. Tööstusspionaaži riski mudel, kohandatud allikast [28]

### 8.3 Petturlik töö

Tabel 16 kujutab endast petturlike töödega seotud riskide juhtimist.

**Varade identifitseerimine:** Tiptasemel tootmine loob tavaliselt märkimisväärset lisandväärtust, kuid sellega kaasnevad suured kulud, sealhulgas vajadus kvalifitseeritud tööjõu ja spetsiifiliste seadmete järele. Töötajad, kes on teadlikud ettevõtte ressurssidest, võivad võtta riske, tuues sisse väliseid materjale ja kasutada ettevõtte aega ning seadmeid isiklikeks projektideks või töödeks konkurentidele, tihti ilma tööandja või reguleerivate asutuste teadmata. Selline tegevus kahjustab ettevõtte huve ning võib olla ebaseaduslik.

**Riskianalüüs:** Loata tööde tegemiseks, nagu näidatud Joonisel 26, peab keegi, kes soovib ettevõtte ressursse ära kasutada, tooma tootmispiirkonda väliseid materjale. Seejärel peab ta leidma meetodi, kuidas oma andmeid ettevõtte süsteemi sisestada, et neid saaks kasutada tootmise juhtimise arvutis. Kui saavutatakse kontroll vastava arvuti üle, on võimalik sisestada oma tootmise

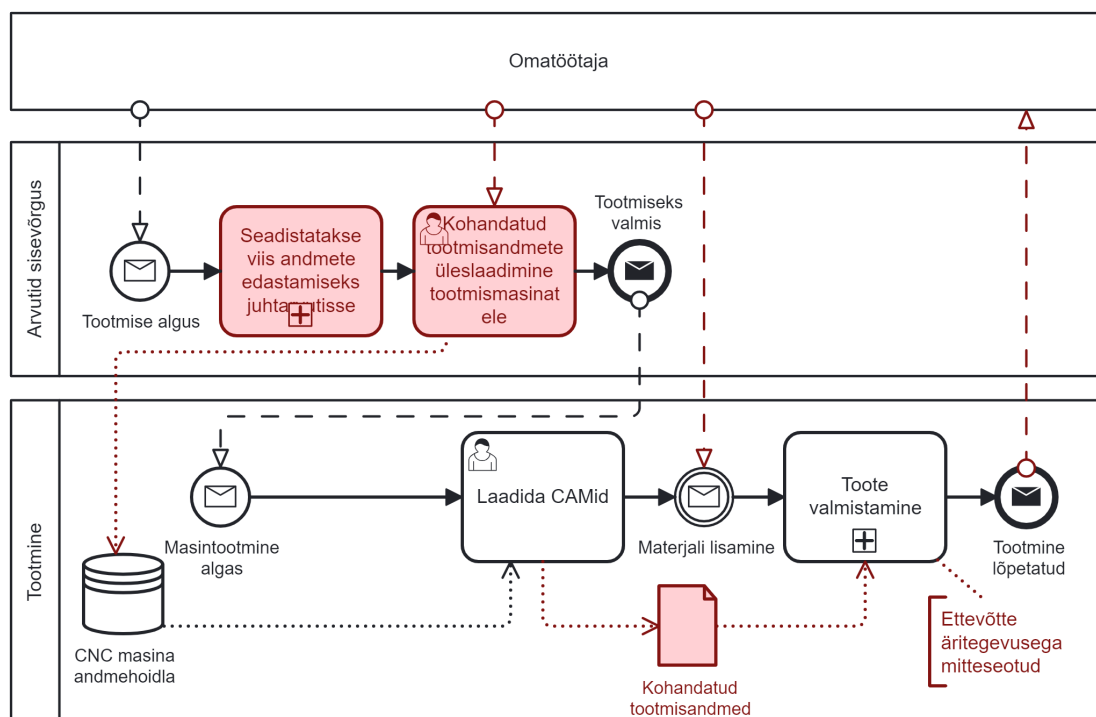
Tabel 16. Petturlike töödega seotud riskijuhtimine, kohandatud allikast [28]

|                      |   |
|----------------------|---|
| <b>Ärivarava</b>     | Tootmise protsess.  |
| <b>Süsteemi vara</b> | CNC-pingi, CNC-pingi mälu, tootmise juhtimise arvuti.   |
| <b>Risk</b>          | Siseringi töötaja, kes vastutab CNC-tootmise eest, laeb kohandatud tootmisandmed CNC-masina mällu. Seejärel kasutab ta väljastpoolt toodud materjali ja loob toote, mis ei ole seotud ettevõtte ärihuvidega. Seda lähenemisviisi kasutades kasutab siseringi töötaja ära asjaolu, et tootmise juhtimise arvuti ei saa asjakohast teavet aktiivsete tellimuste ja CNC-masinasse üles laetud andmete tervikluse kohta. Selle tulemusena võib toote tootmise üldine kättesaadavus, kvaliteet ja terviklus kannatada. |
| <b>Mõju</b>          | Üldine ligipääsetavus ja toote valmistamise terviklus väheneb.  |
| <b>Nõrkus</b>        | Tootmise juhtimise arvuti ei saa piisavalt teavet aktiivsete tellimuste ja CNC-masinasse üles laetud andmete kehtivuse kohta.   |
| <b>Ohu agent</b>     | CNC tootmise eest vastutav siseringi töötaja.   |
| <b>Ründe meetod</b>  | Siseringi töötaja laeb kohandatud tootmise andmed CNC-masina mällu, seejärel kasutab ta väljastpoolt toodud materjali ja lõpuks loob toote, mis ei ole seotud ettevõtte äritegevusega.  |
| <b>Turvanõue</b>     | Turvasüsteem tuvastab ettevõtte seadmete loata kasutamise.  |
| <b>Kontroll</b>      | Töötajate toimingute logimine, ettevõtte seadmetesse tehtavate andmeedastuste jälgimine, CNC-masinate kohalike logide analüüsimine ja protsessi kaeve kasutamine kogutud andmete põhjal.  |

juhised seadmesse, tavaliselt CNC-pinkidesse, näiteks kohandatud arvuti põhise tootmise (CAM-failid). Peale seadistamist kasutatakse seadet nagu tavaliselt, kuid oma andmete ja materjalidega, tootes esemeid, mis ei ole seotud ettevõtte ametlike toodetega.

**Riski vähendamine:** Andmete muutmise jälgimine ja aktiivsete tellimuste teabe registreerimine on süvaanalüüsi jaoks äärmiselt oluline. Nende andmete ühendamine ettevõtte seadmete logidega võimaldab tuvastada juhtumeid, kus töötajad võivad osaleda või püüavad osaleda projektides, mis ei vasta ühelegi käimasolevale tellimusele. See meetod pole aga alati töökindel, sest toiminguid kogumine kõikidest seadmetest võib olla keeruline. Üldiseks probleemiks on käsitsi kasutatavad seadmed, mis salvestavad toiminguid ainult lokaalselt.

Nende puuduste kõrvaldamiseks soovitame kasutada teavet kohaloleku- ja ERP-süsteemidest (ettevõtte ressurside planeerimine). See hõlmab üksikasju toodete töötlemise kohta, tööoperatsioonide järjestust ja töötajate poolt teatatud aega, mida nemad ja tootmisspetsialistid igale etapile kulutavad. Kuigi need andmed võivad olla puudulikud, tingituna nende kogumise viisist, on siiski võimalik kasutada protsesside avastamise meetodeid, et luua üldine pilt tüüpilisest tootmise töövoost, sealhulgas iga etapi keskmine kestus. Vastavuskontrolli abil saame tuvastada kõik olulised kõrvalekalded standardmudelist, hoiatades juhte potentsiaalselt kahtlaste toimingute eest, mis võivad vajada lähemat uurimist.



Joonis 26. Petturliku töö riski mudel, kohandatud allikast [28]

## 8.4 Tahtlik sabotaaž

Tabel 17 kujutab endast varade analüüsi, tahtliku sabotaaži riski ning võimalikku riski vähendamise lahendust.

**Varade identifitseerimine:** Kuna tootmine muutub üha enam automatiseerituks, suureneb ka tootmisprotsesside täpsus. Suurenenud täpsusega kaasneb aga ka protsesside keerukuse ja filigraansuse suurenemine. Kui turvameetmed ei ole piisavalt tugevad, võivad tootmiskeskonna erinevad komponendid muutuda sabotaaži sihtmärkideks. Selline sabotaaž võib olla tingitud ettevõtte rahulolematu töötaja, konkurendi või kättemaksu otsiva endise töötaja tegevusest.

**Riskianalüüs:** Selliste tegevuste tagajärjeks võib olla kriitiliste andmete, nagu CNC-pinkide või CAM-programmide, aktiivsete tellimuste üksikasjade või olulise tootmistarkvara, rikkumine või kustutamine. See võib põhjustada ka kallite seadmete füüsilist kahjustamist või märkimisväärse hulga materjalide raiskamist. Need juhtumid toovad kaasa otseselt kahju ning võivad põhjustada viivitusi tellimuste täitmisel, mis omakorda vähendab klientide usaldust. See võib lõppkokkuvõttes kaasa tuua olulise tulude kaotuse.

Sabotaaž kasutab ära ettevõtte infotehnoloogilise infrastruktuuri nõrkusi, mis sarnanevad tööstusspionaaži stsenaariumides esile toodud nõrkustele. Sabotaaži katsed võivad aga olla laialaialuslikumad, võttes sihikule laiema hulga ettevõtte süsteeme. Kui ohuagent pääseb juurde mis tahes osale ettevõtte infotehnoloogilisest arvutivõrgust, võib ta alustada sabotaažiga.

Näiteks, nagu on kujutatud Joonisel 27, võivad nad laadida ettevõtte andmehoidlast tootmisele

Tabel 17. Tahtliku sabotaaži riskijuhtimine, kohandatud allikast [28]

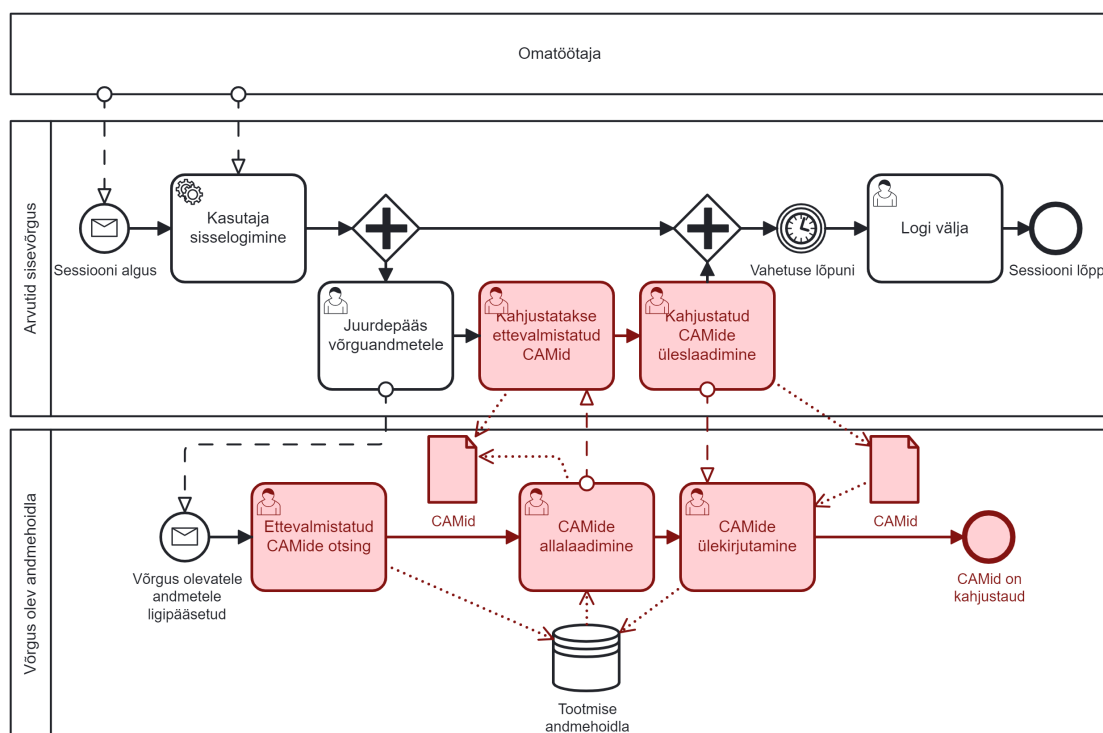
|                      |   |
|----------------------|---|
| <b>Ärivarava</b>     | Ettevalmistatud CAM-failid.   |
| <b>Süsteemi vara</b> | Tootmise arvuti kõvaketas.  |
| <b>Risk</b>          | Rahulolematu töötaja avastab ettevalmistatud CAM-failid ja kahjustab neid, kasutades ära olukorda, kus tootmises kasutatavat arvuti kõvaketast ei jälgita ega analüüsita nõuetekohaselt. Selle tulemusena on ettevalmistatud CAM-failide terviklus kahjustatud. |
| <b>Mõju</b>          | Ettevalmistatud CAM-failide terviklust on rikutud.  |
| <b>Nõrkus</b>        | Tootmises kasutatavat arvuti kõvaketast ei jälgita ega analüüsita nõuete kohaselt.  |
| <b>Ohu agent</b>     | Rahulolematu töötaja.   |
| <b>Ründe meetod</b>  | Ettevõtte töötaja leiab ette valmistatud CAM-failid ja kahjustab neid.  |
| <b>Turvanõue</b>     | Turvasüsteem peab takistama ette valmistatud CAM-failide omavolilist kahjustamist.  |
| <b>Kontroll</b>      | Andmete korrektse säilitamise jälgimise seadistamine, töötajate toimingute logimine ning protsesside kaevandamine genereeritud andmete kohta.   |

mõeldud CAM-failid alla mõnda arvutisse, neid muuta või kahjustada ning seejärel laadida need tagasi, asendades originaalfailid andmehoidlas.

**Riski vähendamine:** Nagu tööstusspionaaži stsenaariumi puhul, on väga oluline jälgida, kuidas andmeid tootmis- ja haldusosakondades käsitletakse, seekord keskendudes lisamistele, muudatustele ja kustutamistele. See samm aitab luua või genereerida mudeleid selle kohta, kuidas töötajad nende andmetega toimetavad, kasutades protsesside kaevandamist. Seejärel saaksime kohaldada vastavuskontrolle, et jälgida kõiki uusi andmetega tehtavaid toiminguid. Lisaks saame analüüsi täiustada, võrreldes andmesalvestuse toiminguprotokolle muu tootmisprotsessist pärit teabega, näiteks ERP-tarkvara üksikasjadega, kohaloleku andmete või tootmisseedmete logidega. See aitaks kahtlase toimingu tuvastada mitte ainult protsesside kaevandamise kaudu, vaid võimaldaks ka märgata võimalikke kahtlasi toiminguid selliste märkide kaudu nagu:

- ebatavalised mustrid töötajate kontrollimisel seoses aja ja asukohaga,
- seadme omavoliline või ebavajalik kasutamine,
- selliste toodete tootmise alustamine, mis ei ole ERP-süsteemi jooksvates tellimustes loetletud,
- ebatavaliselt suur tootmisvigade määr, mida ei ole võimalik parandada ja
- liiga palju raisku läinud materjali.

Erinevate andmeallikate integreerimine ja analüüsimine võimaldab tõhusamalt tuvastada võimalikke turvariske ning nendele reageerida.



Joonis 27. Tahtliku sabotaaži riski mudel, kohandatud allikast [28]

## 8.5 Tahtmatu kahju

**Varade identifitseerimine:** Kuigi töötaja tahtmatu kahju tagajärjed võivad olla sarnased tööstusspionaaži või tahtliku sabotaaži tagajärgedega, on sellistele juhtumitele reageerimine sageli erinev, arvestades suurt nõudlust oskustöölise järele tootmises, kus töötaja vallandamist peetakse üldiselt viimaseks abinõuks. Väga oluline on välja selgitada, kas kahju oli tahtlik või tulenes sellest, et töötaja langes sotsiaalse manipuleerimise, hooletuse või teatud seadmete või tarkvara vähesel tundmisel ohvriks.

**Riskianalüüs:** Tahtmatu kahju tekkimise oht võib ilmned mitmel viisil, kuid ühiseks teguriks peetakse heade kavatsustega töötajat, kellel on seaduslik juurdepääs ettevõtte süsteemidele ja kes:

- Teeb ettevõtte süsteemide kasutamisel juhusliku vea, näiteks kiirustades seadmete välja lülitamisega, mis jätab need ettearvatusesse seisundisse. See omakorda võib põhjustada kahju andmetele, tarkvarale või seadmetele endile.
- Laseb end eksitada ettevõtte välise osapoole poolt, aidates neid tahtmatult, näiteks järgides telefoni teel antud juhiseid, mis võivad viia kaugjuurdepääsuni ettevõtte süsteemidele, või vastates andmepüügi e-kirjale, mille tagajärjel antakse ründajale üle tundlikku teavet.

**Riski vähendamine:** Arvestades tahtlike ja tahtmatute kahjude erinevaid tulemusi, on protsessi analüüsile keskendumine loomulik lähenemisviis selle küsimuse käsitlemiseks. Tahtmatuid õnnetusi kujutavad mudelid on üldjuhul keerulisemad ja ebakorrapärasemad kui tahtlikku sabotaaži

kujutavad mudelid, millel on tavaliselt algusest peale selged ja määratletud eesmärgid. Kuna tahtmatuid kahjustusi esineb tootmises suhteliselt harva, võib piisavate andmete kogumine, et konstrueerida mudel, mis suudaks neid kahte tüüpi juhtumeid eristada, võtta aega kuid või isegi aastaid.

Alternatiivse strateegiana soovitame koguda süsteemi keskkonnast võimalikult palju andmeid ja säilitada neid eelnevalt kindlaks määratud aja jooksul. Kui tahtliku sabotaaži avastamiseks loodud süsteem märgib mis tahes toimingu kahtlaseks, võiks see kasutada protsessi avastamist, et luua ühekordne "rikastatud" mudel, kasutades kõiki olemasolevaid andmeid. Seda mudelit saaks seejärel esitada juhtkonnale, et otsustada, kas käitumine oli tahtlik. Aja jooksul, kui süsteem kogub andmeid varasematest juhtumitest, saab hakata määrama usaldusnivood selle kohta, kas toiming on tõenäoliselt tahtlik sabotaaž või mitte, täiustades võimet teha vahet nende kahe vahel.

## 8.6 Saadud õppetunnid

Selles peatükis näitasime, kuidas turvariskide juhtimise lähenemisviisi saab rakendada turvariskide väljaselgitamiseks tootmisvaldkonnas. Konkreetselt oli selles näites fookuses üks konkreetne turvariski liik, nimelt siseringi riskid. Rõhutame, et organisatsioon peab hindama erinevaid turvarünnakute stsenaariume, sealhulgas organisatsiooni töötajate poolt tekitatud turvaohтусid.

Käesolevas näites käsitleme nelja turvariski - tööstusspionaaži, petturlikku tööd, tahtlikku sabotaaži ja tahtmatut kahju. Potentsiaalselt võime neid rünnakuid vahetult siduda eelmises peatükis käsitletud kaitstavate varade, turvariskide ja riskide vastumeetmetega. Näiteks, kui arutame ERP-süsteemi kohaldamist, mis mängib olulist rolli RAMI 4.0 hierarhia tasandi telje ettevõtte tasandil, on tööstusspionaaži risk suunatud tootmissalvestusseadmele, mida võiks potentsiaalselt kaitsta kasutajate jälgimise ja/või kasutajate juurdepääsu haldamise kontrollide nõuete rakendamisega (vaata Tabel 14).

Esitatud juhtum illustreerib ka seda, et tootmisprotsessides võivad eksisteerida erinevad ärivarad ja neil võivad olla erinevad turvavajadused. Näiteks tuleks kaitsta teabe konfidentsiaalsust (nt toodete skeemide konfidentsiaalsust) tööstusspionaaži ohu eest; protsessi terviklust (nt tootmisprotsessi terviklust) tuleks kaitsta pettuse ohu eest; ja tootmisvahendi terviklust (nt CAM-i terviklust) tuleks kaitsta tahtliku sabotaaži ohu eest. See näide illustreerib, et ohu tegurid võivad potentsiaalselt olla suunatud erinevatele varadele automatiseeritud süsteemi ja tehnoloogiate arhitektuuri hierarhias.

## 9 STRIDE turvaehtude analüüsimine tootmisettevõttes

Alljärgnevalt väljatoodud viis juhtumit on pärit kirjanduse analüüsist, kus on tuvastatud erinevaid turvariske.

Analüüsi [26] näitel, on ettevõtte X Eestis asuv puidutööstusettevõtte, mis on Euroopa turul tegutsenud 20 aastat. Ettevõtte tootevalik laieneb igal aastal uute toodetega ning nad teenindavad peamiselt suuri jaemüügi ettevõtteid, kes kuuluvad mööblitööstuses äri-äri (B2B) sektorisse. Lisaks olemasolevale tootevalikule pakub ettevõtte X ka projekteerimis- ja arendusteenuseid, mis täiendavad nende tootmisvõimsust. Tellimused on nende tootmise aluseks - nad ei tooda ette varusid ning heaks kiidetud tellimused käivitavad tootmise planeerimise. Käesolevas peatükis järgime STRIDE taksonoomiat (vaata Peatükke 2 ja 6) ja analüüsime ettevõtte X protsesse, varasid, riske ning nende käsitlemise meetmeid.

### 9.1 Ettevõtte kirjeldus

Ettevõtte X jälgib iga tarneahela üksuse tegevust, keskendudes peamiselt ettevõtte siseprotsesside juhtimisele. Siiski kasutab ettevõtte perioodiliselt tootmise allhankeid, et tulla toime nõudluse kõikumisega. Peamised trendid, mis mõjutavad ettevõtet X, on järgmised:

- **Euroopa Liidu keskkonnahoidliku majanduskasvu eesmärgid:** Need eesmärgid rõhutavad keskkonnasäästlikkust, ressursside tõhusat kasutamist ning vastavust keskkonnasäästliku majanduse põhimõtetele.
- **Geopoliitilised väljakutsed:** Sõja kriis on sundinud Eesti ettevõtteid otsima alternatiivseid tarnijaid, mis omakorda mõjutab puidu impordi ja suurendab kulusid.
- **Tehnoloogilised arengud ja automatiseerimine:** Konkurentsivõime säilitamiseks kasutab puidutööstus, sealhulgas ettevõtte X, automatiseerimist ja robotiseerimist, eesmärgiga suurendada tootmise tõhusust.
- **Digitaalne transformatsioon:** Digitaalsete vahendite, sealhulgas tehisintellekti, masinõppe ja küberfüüsiliste süsteemide integreerimine toob kaasa murrangulisi muutusi nii andmetöötuses kui ka ettevõtte üldises juhtimises.
- **Tööjõu puudus:** Seda pidevat probleemi lahendavad osaliselt automatiseerimine ja digitaliseerimine, kuid nõudlus kvalifitseeritud spetsialistide järele püsib. Tööstuse tähtsuse ja puidu ökoloogilise kasulikkuse rõhutamist peetakse strateegiliseks sammuks, et meelitada ligi uusi talente.

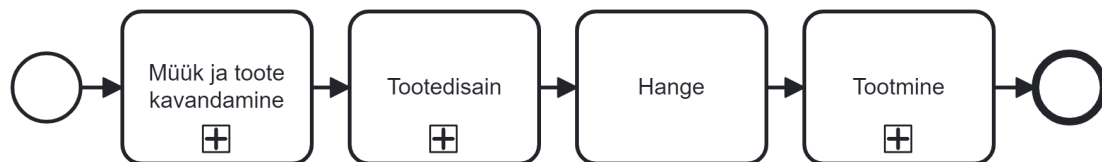
Ettevõtte X ärieesmärkideks on pakkuda konkurentsivõimelist hinda, tagades samal ajal, et toodete kvaliteet vastab kehtestatud standarditele, ning kindlustada toodete õigeaegne tarnimine, säilitades lühikesed tarneajad ja soodustades uute toodete kiiret arendamist.

## 9.2 Süsteemi kontekst

Ettevõtte X kasutab järgmisi tarkvaralahendusi:

- ERP süsteem ressursside planeerimiseks,
- SolidWorks projekteerimisülesannete täitmiseks,
- sisemine tarkvara toodete planeerimiseks ja
- MS Office tarkvara mitmesuguste tööülesannete täitmiseks.

Väärtusahelat kujutatakse põhiprotsesside kaudu, nagu on näidatud Joonisel 28, kus iga protsessi jälgib määratud protsessi omanik, kes vastutab selle juhtimise ja kontrolli eest. Nende protsesside omavahelist seotust soodustab sisendite ja väljundite vastastikune vahetamine, mis tagab teabe sujuva liikumise järgmistesse etappidesse. Nende peamiste protsesside toetamiseks kasutatakse infosüsteeme, näiteks ERP ja tootmise planeerimise tarkvara. Lisaks toetavad neid toiminguid sellised abivahendid nagu Excel ja SolidWorks; Excel toimib andmesalvestus- ja töötlemisvahendina ning SolidWorks'i kasutatakse peamiselt tootemudelite, koostejooniste, juhendite ja pakendi skeemide koostamiseks.

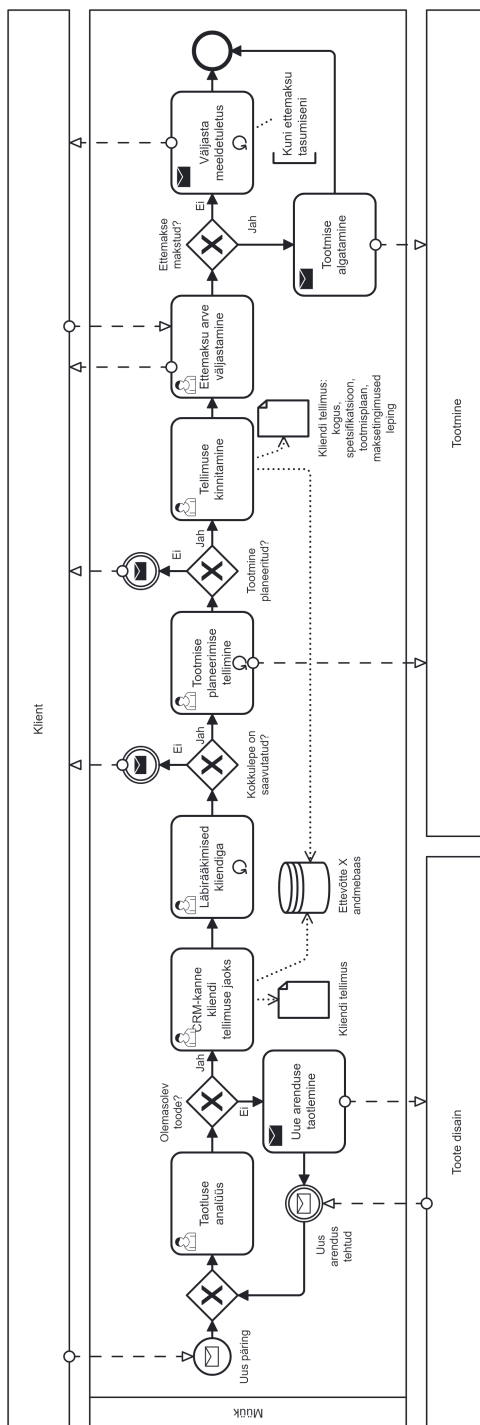


Joonis 28. Ettevõtte X peamised protsessid, kohandatud allikast [26]

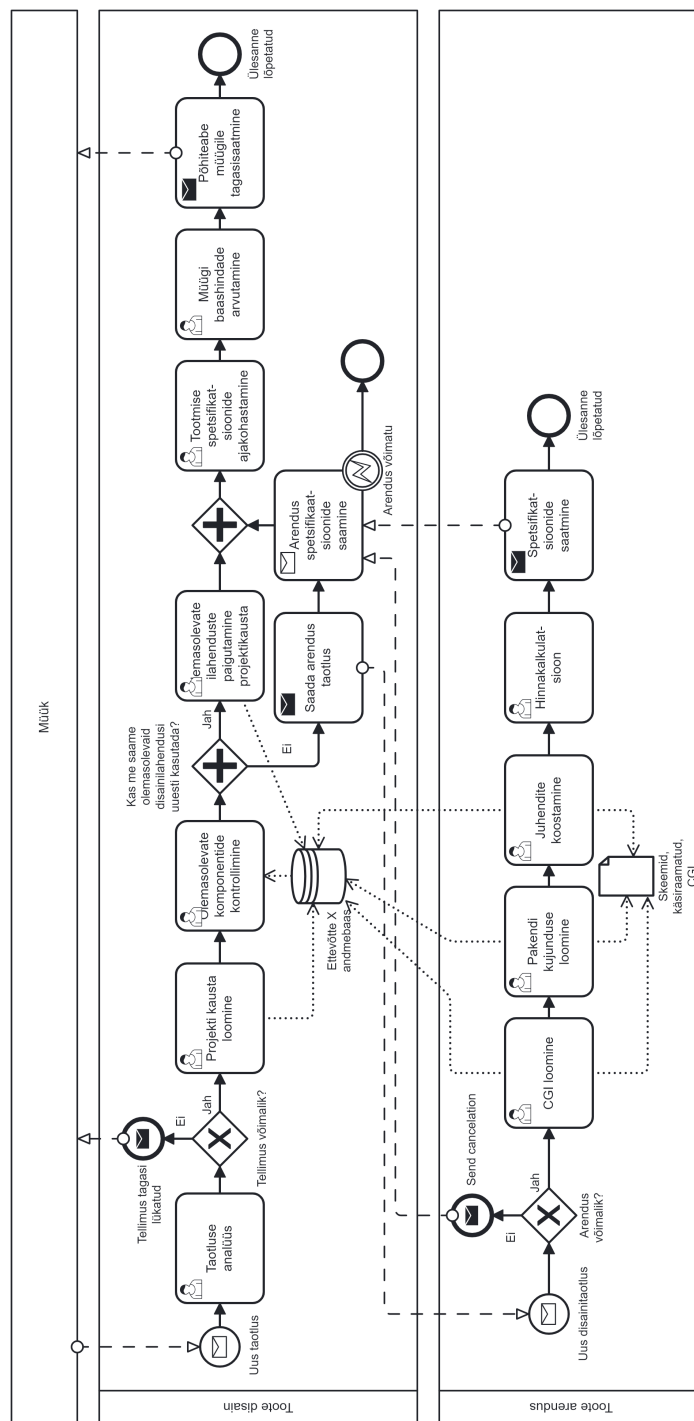
**Müük ja toote kavand:** Müügiosakonnal on mitu funktsiooni (vt Joonis 29): tootearenduse juhtimine, kliendibaasi haldamine, üldplaneerimine (pikaajaline) ja tellimuste haldamine. Kui ettevõtte saab kliendilt taotluse, alustab müügijuht projekti läbi vaatamisega, et otsustada, kas seda saab täita olemasoleva tootesarja abil või tuleb välja töötada uued tootmiselemendid. Pärast esialgset hindamist peab müügijuht kliendiga läbirääkimisi hindade üle ja koostab tootmisplaani. Tootmist alustatakse alles siis, kui klient on teinud ettemaksu, mida kinnitab ettemaksu arve tasumine.

**Toote disain:** Toote disainiprotsess, mis on kujutatud Joonisel 30, algab müügimeeskonna taotluste analüüsist. Kui on kinnitust leidnud, et taotlus on teostatav, võib alustada vajalike alamkataloogide ja projektifailide eraldamist. Selle protsessi käigus on mõistlik taaskasutada võimalikult palju juba konstrueeritud detaile, vähendades seeläbi arenduskulusid ja keerukust. Siiski võivad esineda olukorrad, kus tuleb välja töötada uusi detaile. Sellistel juhtudel esitatakse tootearendusmeeskonnale alampäring, kes koostab kõik vajalikud skeemid, kasutusjuhendid ja tootekirjeldused. Kui vajalik teave on kogutud, arvutatakse tootmise baashinnad ja saadetakse vastav info tagasi müügimeeskonnale. Mõnel juhul võidakse uue toote väljatöötamisel valmistada näidistoodet, kuid kuna see on pigem erandlik, ei ole seda juhtumit eraldi protsessina välja toodud.

**Tootmine:** Tootmisprotsessi võib jagada kolmeks alamkategorriaks:



Joonis 29. Müügiprotsess, kohandatud allikast [26]



Joonis 30. Toote disaini protsess, kohandatud allikast [26]

- uue toote tootmisprotsessi loomine,
- üksikasjalik planeerimine ja
- tootmise teostamine.

Siinkohal keskendume tootmise teostamise protsessile (vt Joonis 31).

Tootmise alustamise eelduseks on toote metaandmete olemasolu. Valmistamine koosneb erinevatest puidutööstustoimingutest ja algab toote profiili valimisega. Kõik tooted läbivad saagimise, masintöötluste, CNC-pingilõikamise, viimistlustööd ja pakendamise. Mõned tooted vajavad lisaks ka kokkupanekut. Protsess lõpeb tarneks valmisolekuga.

## 9.3 Turvariskide juhtimine

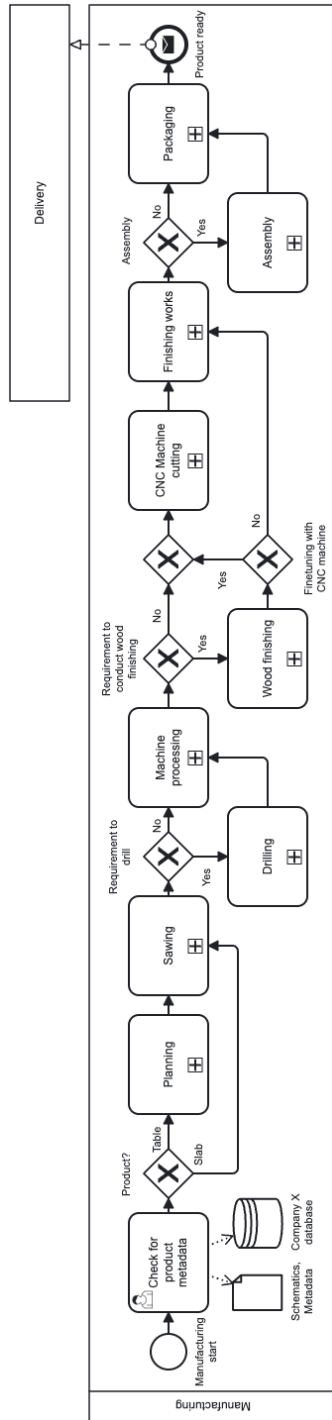
### 9.3.1 Võltsimine/teesklus/pettus (*Spoofing*)

Nagu on määratletud osas 2, tähendab teesklus paistmist millegi või kellegi teisena. Näiteks **IP-aadressi võltsimine** on olukord, kus ründaja maskeerib end usaldusväärseks seadmeks, võltsides IP-aadressi pakette. Seda tehnikat kasutatakse sageli IP-aadressil põhinevate turvameetmete vältimiseks, hõlbustades volitamata juurdepääsu võrkudele või käivitades teenustökestusrünnakuid (DDoS), mis sageli koormavad sihtmärki mitmest võltsitud allikast pärit liiklusega.

Ettevõtte võrgus võib IP-aadresside võltsimise oht tuleneda ebapiisavast võrgu piirdekaitsest või ebapiisavatest sisemistest turvameetmetest, näiteks pakettide filtreerimise või valideerimise mehhanismide kasutamata jätmisest. Ründajad võivad neid nõrkusi ära kasutada, et jäljendada siseseadmeid, saades seeläbi võimaluse võrguliikluse pealtkuulamiseks, muutmiseks või pahatahtlike andmete sisestamiseks. See võib viia andmete rikkumiseni, andmete omavolilise muutmise ja teenuste katkestamiseni, mis mõjutab tõsiselt organisatsiooni toimivust ja usaldusväärust.

Tabel 18. IP aadressi võltsimisega seotud riskijuhtimine

|                      |   |
|----------------------|---|
| <b>Ärivarava</b>     | Andmete saatmine sidevõrgu kaudu.   |
| <b>Süsteemi vara</b> | Arvutivõrgu infrastruktuur.   |
| <b>Risk</b>          | Ründaja maskeerib end seaduslikuks kasutajaks või seadmeks, võltsides IP-aadressi teavet oma võrgupakettides, eesmärgiga mööda minna IP-põhistest turvameetmetest.                                  |
| <b>Mõju</b>          | Autoriseerimata juurdepääs arvutivõrgu ressurssidele.   |
| <b>Nõrkus</b>        | Arvutivõrgu autentimise protokollide puudumine.   |
| <b>Ohu agent</b>     | Sobivate vahendite ning motivatsiooniga ründaja.  |
| <b>Ründe meetod</b>  | Ründaja möödub arvutivõrgu turvareeglitest.   |
| <b>Turvanõue</b>     | Süsteem peab tuvastama volitamata kaugühendused.  |
| <b>Kontroll</b>      | Tegeleb ebapiisavate kaugühenduse reeglitega, jälgides ja analüüsides TCP-ühendusi, et tuvastada lahknevusi algatatud ja kestvate ühenduste vahel, aidates avastada volitamata juurdepääsu katseid. |



Joonis 31. Tootmisprotsess, kohandatud allikast [26]

**Riski maandamine:** Meetmed IP-aadresside võltsimise vastu peavad olema mitmekülgsed. Ruuterites ja jaoturites sisenemis- ja väljumisfiltrite implementeerimine võib oluliselt vähendada võltsitud pakettide riski, mis sisenevad või väljuvad arvutivõrgust. Samuti aitab võrgu sissetungi tuvastamise süsteemide ja sissetungi tõkestamise süsteemide kasutuselevõtt tuvastada ja blokeerida võltsimisega seotud kahtlasi liiklusmustreid. Lisaks sellele võib krüpteerimisprotokollide kasutuselevõtt tundlike andmete edastamiseks ning turvaliste autentimismehhanismide kasutuselevõtmine vähendada pealtkuulamise mõju, tagades, et isegi kui andmed on tabatud, jäävad need volitamata osapooltele mõistetamatuks.

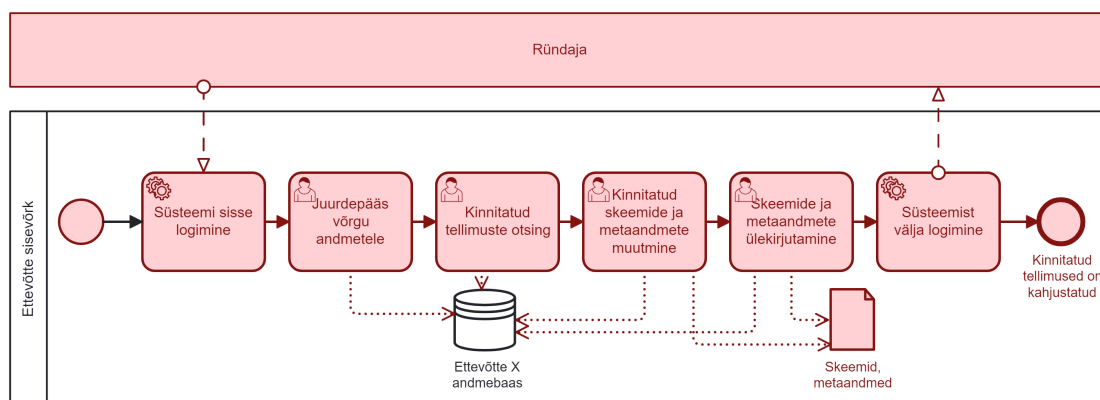
Lisaks sellele on väga oluline harida töötajaid riskidest, mis on seotud andmepüügi e-kirjadega või pahatahtlike veebisaitidega, mis võivad olla osa võltsimisrünnakust, mille eesmärk on paigaldada siseseadmesse pahavara. Selle ohu eest kaitsmiseks on oluline regulaarselt uuendada ja parandada arvutivõrgu seadmeid ja tarkvara.

Kokkuvõtlikult võib öelda, et IP-aadresside võltsimine kujutab endast olulist ohtu arvutivõrgu turvalisusele. Selleks, et seda ohtu tõhusalt maandada, on vajalik strateegia, mis hõlmab tehnilisi kaitsemeetmeid, töötajate teadlikkust ja turvapoliitikat. Ainult nende meetmete kombineeritud implementeerimine võimaldab avastada, ennetada ja adekvaatselt reageerida sellistele turvariskidele.

### 9.3.2 Muukimine/rikkumine (*Tampering*)

Muukimine või rikkumine tähendab millegi muutmist kettal, võrgus, mälus või mis tahes seadmes. Peatükis 6 oleme tuvastanud 18 muukimise/rikkumise ohtu. Ettevõtte X puhul võib kaaluda mitut ohtu. Kuna ettevõtte tugineb suurel määral eelnevalt loodud toodete skeemidele, muutub *andmete manipuleerimise* oht kõige mõjukamaks ohuks ja seda tuleks võtta tõsiselt. Joonisel 32 esitatud stsenaarium toob esile ohu, mida kujutab endast andmete manipuleerimine, alates väikestest parandustest kuni toote kujunduse täieliku võltsimiseni.

Ründaja võib kasutada õngitsusrünnet, et saada juurdepääsu ettevõtte süsteemidele. See võimaldab tal manipuleerida andmeid, mis on kinnitatud tootmiseks ja mida ei kontrollita uuesti. Selline tegevus kahjustab vahetult tootmisprotsessi, kuna esimene märk probleemist ilmneb alles tootmise käigus või isegi pärast seda, kui kõik tooted on juba valminud.



Joonis 32. Andmete rikkumise stsenaarium

Sellised omavolilised muudatused võivad kaasa tuua mitmeid probleeme, sealhulgas tootmisvigade tekkimist, rahalist kahju ja klientide usalduse kaotust. Praegune lähenemine, mis võimaldab kõigil töötajatel juurdepääsu nendele skeemidele, suurendab andmete juhusliku ja tahtliku manipuleerimise riski. Nii sise- kui ka välisründajad, olgu nad siis kahjulike kavatsustega ettevõtte töötajad või turvanõrkuste kaudu juurdepääsu saanud välised isikud, võivad neid kavandeid muuta. Nende motiivid võivad ulatuda ettevõtte toimimise häirimisest kuni konkurentidele eeliste andmiseni või isegi intellektuaalomandi varguseni.

Tabel 19. Andmete manipuleerimise riskijuhtimine

|                      |  |
|----------------------|--|
| <b>Ärivarava</b>     | Andmebaasi salvestatud andmed.   |
| <b>Süsteemi vara</b> | Andmebaas.   |
| <b>Risk</b>          | Ründaja muudab süsteemis või ülekandes olevaid kriitilisi andmeid, et rikkuda teavet, kahjustada otsustusprotsesse või saada rahalist kasu.  |
| <b>Mõju</b>          | Andmete terviklus on rikutud.  |
| <b>Nõrkus</b>        | Puudulik juurdepääsukontroll.  |
| <b>Ohu agent</b>     | Sobivate vahendite ning motivatsiooniga ründaja.   |
| <b>Ründe meetod</b>  | Ründaja saab juurdepääsu toote skeemidele ja muudab neid.  |
| <b>Turvanõue</b>     | Kasutajatele juurdepääsu põhimõtete kehtestamine ja jõustamine, mis reguleerivad nende õigusi.   |
| <b>Kontroll</b>      | Kõrvaldada tarkvara, süsteemide ja andmete puudulikud juurdepääsu kontrollid, rakendades poliitikaid ja süsteeme, mis haldavad ning jälgivad kasutajate õigusi, tagades, et juurdepääs on ainult volitatud töötajatel. |

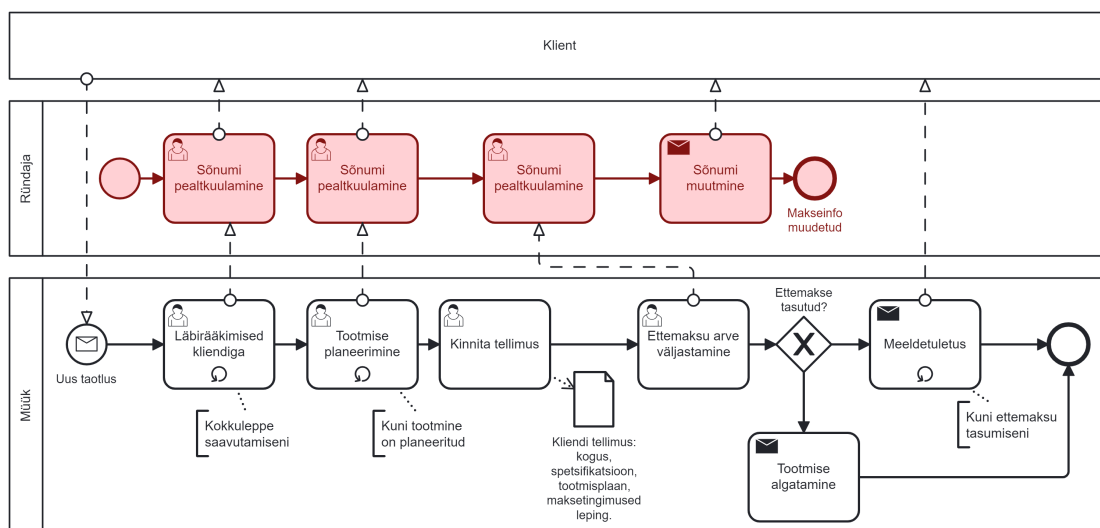
**Riski maandamine:** Selliste ohtude leevendamiseks on vaja rakendada kaitsestrateegiat. Juurdepääsu kontroll ja õiguste määramine rollide alusel võib riske märkimisväärselt vähendada, tagades, et muudatusi saavad teha ainult need töötajad, kes vajavad vastavat juurdepääsu seoses oma tööga. Lisaks võib järelvalvetehnoloogiate kasutuselevõtt aidata tuvastada volitamata või ebatavalisi toiminguid andmetega. Need süsteemid jälgivad, kuidas andmetele ligi pääsetakse ja kuidas neid muudetakse ning hoiatavad ebatavaliste mustrite esinemise korral.

Lisaks sellele võib digitaalsete markeeringute kasutamine toote skeemide puhul aidata faile jälgida ja autentida, muutes manipulatsioonide tuvastamise lihtsamaks. Andmetele juurdepääsu ja muudatuste korrapärane kontrollimine koos koolitusprogrammidega, mille eesmärk on teavitada töötajaid andmete turvalisuse tähtsusest ja manipuleerimisega seotud riskidest, tugevdab ettevõtte kaitset nende ohtude vastu.

### 9.3.3 Teabe avalikustamine (*Information Disclosure*)

Teabe avalikustamine tähendab teabe jagamist kellegagi, kellel ei ole sellele juurdepääsu õigust.

Arvestades ettevõtte X digitaliseerimist, on **vahendusrünnakute** oht üsna suur. Selliste rünnakute puhul sekkub kurjategija ja võib muuta kahe osapoole vahelist sidet. See ohustab ettevõtet X, eriti andmeedastuse ajal tarneahelas ja suhetes peamiste jaemüügi partneritega. Katkematu infovoog on väga oluline alates kliendi päringute analüüsist kuni lõplike tarnete lähetamiseni. Vahendusrünne võib segada suhtlust, näiteks müügijuhtide ja klientide vaheliste läbirääkimiste ajal, kus võidakse sisestada muudetud tingimusi või võltsitud maksejuhiseid, nagu on kujutatud Joonisel 33. Samuti on oht, et projekteerimise etappide ajal toimuvasse teabevahetusse müügi-, tootearendusmeeskondade ja väliste partnerite vahel sekkub väline pahatahtlik osapool, mis võib kaasa tuua spetsifikatsioonide muutmise või varastatud patenteeritud disainilahenduse, mis omakorda võib põhjustada rahalist kahju või tootmise sabotaaži.



Joonis 33. Vahendusründe stsenaarium

Ettemaksu arvete väljastamise ja maksmise protsess on veel üks haavatav valdkond. Kurjategijad võivad arveid vahelt püüdes neid muuta ja suunates makseid võltsitud kontodele. Ettevõtte X B2B kontekstis võib selline pettus tõsiselt mõjutada ettevõtte finantsolukorda ja ärisuhteid.

**Riskide maandamiseks** saab kasutada andmete krüpteerimist edastamisel, kasutajate autentimist ning arvutivõrgu ebatavalise aktiivsuse pidevat jälgimist. Lisaks on oluline töötajaid

regulaarselt koolitada, et tõsta nende teadlikkust küberturvalisusest ning tagada sidekanalite turvalisus. Need meetmed aitavad kaitsta ettevõtte X digitaalset suhtlust, tagades selle usaldusväärsuse ja töökindluse.

Tabel 20. Vahendusrännaku riskijuhtimine

|                      |  |
|----------------------|--|
| <b>Ärivarava</b>     | Kommunikeeritavad andmed.  |
| <b>Süsteemi vara</b> | Arvutiside võrk.   |
| <b>Risk</b>          | Ründaja kuulab pealt ja potentsiaalselt muudab kahe osapoolse vahelist suhtlust ilma nende teadmata.                           |
| <b>Mõju</b>          | Andmete konfidentsiaalsus ja terviklus on rikutud.   |
| <b>Nõrkus</b>        | Ebaturvalised ja/või krüpteerimata sidekanalid.  |
| <b>Ohu agent</b>     | Sobivate vahendite ning motivatsiooniga ründaja.   |
| <b>Ründe meetod</b>  | Ründaja kuulab pealt sidekanaleid.   |
| <b>Turvanõue</b>     | Kõik digitaalsed andmeedastused peavad olema krüpteeritud.   |
| <b>Kontroll</b>      | Tagage, et igasugune kasutatav andmeside on turvaline ja krüpteeritud, et vältida volitamata juurdepääsu ja andmete rikkumist. |

### 9.3.4 Teenustõkestus/ummistus (*Denial of Service*)

Teenustõkestus või ummistus on teenuse osutamiseks vajalike ressursside ammendumine. Näiteks **teenustõkestuse** rünnak seab ohtu igapäevase operatiivtegevuse, ujutades üle ettevõtte võrgu või süsteemid liigse liiklusega, mis takistab õiguspärase taotluste töötlemist. Sellised häired võivad segada ettevõtte X tarneahelat, viivitada tootmist ning häirida sidet jaemüügi partneritega, kahjustades seeläbi ettevõtte äritegevust.

Ettevõtte X sõltuvus digitaalsest raamistikust oma B2B tegevuses, alates tellimuste vastuvõtmisest kuni tootmise planeerimiseni ja tarnimiseni, muudab selle haavatavaks. Olulised süsteemid, nagu ERP ressursside planeerimiseks ja SolidWorks toodete projekteerimiseks, on igapäevase toimimise jaoks hädavajalikud. Rünnak nende süsteemide vastu võib põhjustada olulisi viivitusi, mis mõjutavad kõike alates tellimuste töötlemisest kuni valmistoodete väljasaatmiseni. Kuna ettevõtte X tootmisprotsess põhineb kinnitatud tellimustel, võivad viivitused tootmises kaasa tuua lepingu rikkumisi, rahalisi trahve või äritegevuse vähenemist.

Oht ei piirdu ainult välise ohuga, vaid see võib tuleneda ka kahjustatud sisemistest süsteemidest või ettevõtte võrgus olevatest asjade interneti seadmetest. Näiteks kui tootmisliini seade satub eduka rünnaku ohvriks, võib see oluliselt mõjutada tootmistegevuse tõhusust.

**Riski maandamine:** Selliste riskide vastu võitlemiseks peab ettevõtte X kasutusele võtma sissetungi tuvastamise süsteemid, et reguleerida sisse tulevat liiklust. Liikluse analüüsi vahendite kasutamine ja kiiruse piiramise implementeerimine võib aidata varakult avastada ja lahendada ebanormaalseid liiklusmustreid. Samuti võib varusüsteemide ja võrguteede loomine aidata hoida ettevõtet rünnaku ajal töökorras.

Tabel 21. Teenustõkestuse rünnaku riskijuhtimine

|                      |   |
|----------------------|---|
| <b>Ärivarava</b>     | Operatiivteenuste käideldavus.  |
| <b>Süsteemi vara</b> | Võrgu infrastruktuur.   |
| <b>Risk</b>          | Ründaja koormab organisatsiooni arvutivõrgu ressursse või teenuseid liigse liiklusega.  |
| <b>Mõju</b>          | Teenuse käideldavuse kadu.  |
| <b>Nõrkus</b>        | Ebapiisav võrgu läbilaske võime, filtreerimismehhanismide puudumine.  |
| <b>Ohu agent</b>     | Sobivate vahendite ning motivatsiooniga ründaja.  |
| <b>Ründe meetod</b>  | Ründaja koormab organisatsiooni ressursse liigse liiklusega.  |
| <b>Turvanõue</b>     | Süsteem peab rakendama reaajas sissetungi tuvastamise mehhanisme andmevoo jälgimiseks.  |
| <b>Kontroll</b>      | Andmepakettide voo jälgimine, mis võimaldab tuvastada ja reageerida võimalikele teenustõkestuse rünnakutele või muudele pahatahtlikele tegevustele. |

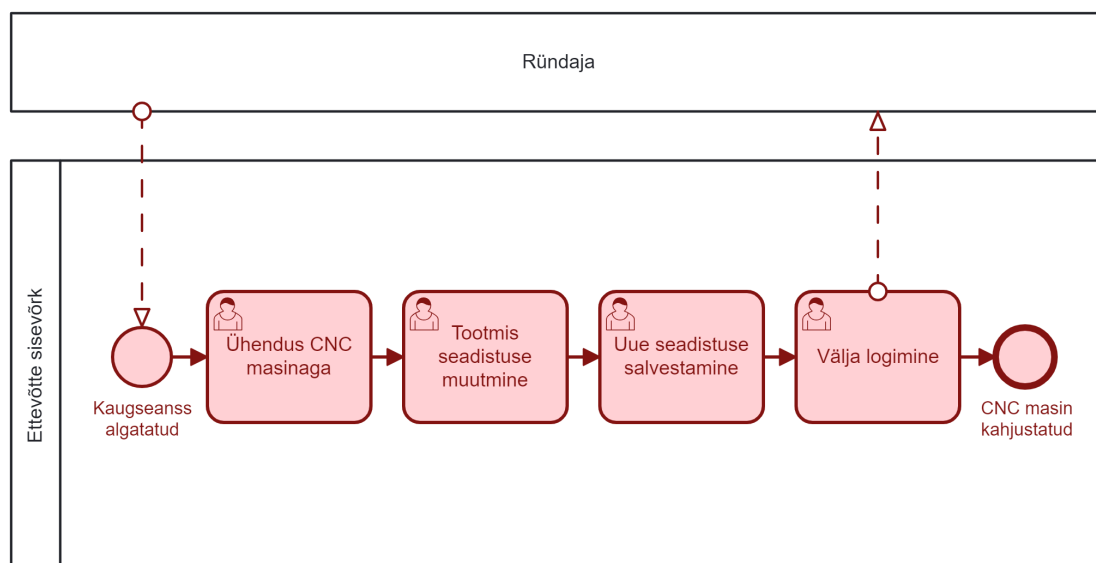
### 9.3.5 Õiguste vallutus (*Elevation of Privilege*)

Õiguste vallutus tähendab, et kellelgi lubatakse teha midagi, milleks tal õigust ei ole. Peatükis 6 tuvastasime 14 antud kategooria ohtu. Arvestades ettevõtte suurust on **mikrovigade sisestamise risk** arvestatava mõjuga tootmise kvaliteedile. See oht hõlmab pisikeste vigade tahtlikku sisse viimist toote disaini või tootmisprotsessidesse. Selline võltsimine võib drastiliselt kahjustada valmistoodete terviklust ja pikaajalisust, mis omakorda toob kaasa mainekahju, rahalised tagasilöögid ja ohutusprobleemid.

Ettevõtte X edu tugineb integreeritud tarneahelale ja digitaalsetele lahendustele, nagu ERP ressursside planeerimiseks ja SolidWorks toodete projekteerimiseks. Ettevõtte tava alustada tootmist ainult kinnitatud tellimuste alusel rõhutab vajadust täpsuse ja usaldusväärsuse järele iga toodetud üksuse puhul. Selles kontekstis võib mikroviiga tekkida ettevõtte andmeserveris olevate võltsitud digitaalsete failide või konstruktsiooni skeemide pahatahtlike muudatuste kaudu. Disaini ja arenduse digitaalne iseloom muudab sellised muudatused eriti peeneks ning ohtlikuks, kuna nad võivad olla sisestatud ja levida tootmistsükli jooksul ilma, et neid kohe avastataks.

Mikrovigade sisestamise võimalikud punktid on järgmised:

- **Projekteerimisfaas:** SolidWorks'i failide manipuleerimise kaudu toote konstruktsioonidesse vigade sisestamine.
- **Tootmise planeerimine:** Tootmise parameetrite või materjali spetsifikatsioonide muutmine ERP andmete kaudu.
- **Tootmise teostamine:** Originaalsetest konstruktsioonidest kõrvalekaldumine, muutes CNC-pingi seadeid.



Joonis 34. Mikrovigade sisestamise stsenaarium

CNC-põhine mehaaniline töötlemine on tootmisviis, kus eelprogrammeeritud arvuti tarkvara juhib tehase seadmete ja tööriistade liikumist. See võimaldab kasutada mitmesuguseid keerulisi seadmeid, nagu lihvimismasinad, treipingid, freesid ja CNC-freesid, täites kolmemõõtmelisi lõikamisülesandeid ühe käskude jada abil. Seadete muudatused võivad olla väga peensusteni viidud, kuid võivad põhjustada pikaajalisi kvaliteedi probleeme, mis ilmnevad alles pärast kvaliteedi kontrolli või teatud kasutusea möödumist. Näiteks võib ründaja, nagu kujutatud joonisel 34, kaugühenduse kaudu seadistada CNC-masinaid, muutes kvaliteedinäitajaid või isegi ohutussätteid. Artiklis [5] on väidetud "Kasutajale või protsessile antakse sageli täielik ligipääs mis tahes süsteemi ressurssidele, sealhulgas failisüsteemile või mäluasukohtadele. Näiteks rakendusel, mis on kirjutatud THINC-API peal, võib olla täielik ligipääsuõigus mis tahes süsteemi ressurssidele, sealhulgas sisekontrollerite seadetele. Sarnaselt võib Ethernet Q puhul kaugkasutajal olla võimalus kirjutada salvestuspunktid, mis on kaardistatud väljaspool käimasolevat protsessi."

**Riskide maandamine:** See hõlmab digitaalse turvalisuse meetmete rakendamist, et vältida volitamata juurdepääsu ja manipuleerimist projekteerimis- ja tootmisandmetega. Selle hulka kuuluvad juurdepääsu kontrollimehhanismid, digitaalsete failide auditikontroll, andmete krüpteerimine ja toodetud toodete kvaliteedi kontroll. Lisaks võimaldavad kvaliteedi tagamise meetmed varakult avastada ja parandada kõrvalekaldeid toote standarditest. Projekteerimis- ja tootmisprotsesside üksikasjalik läbivaatamine ja analüüsimeetodid võivad tuvastada mikrovigadele viitavaid kõrvalekaldeid.

Teadlikkuse ja avatuse kultuuri edendamine julgustab töötajaid olema tähelepanelikud võimalike turvaprobleemide või kahtlase käitumise suhtes. Pidev küberturvalisuse alane haridus rõhutab igapäevast rolli ettevõtte toimimise ja maine terviklikkuse säilitamisel.

Tabel 22. Mikrovigade sisestamise riskijuhtimine

|                      |   |
|----------------------|---|
| <b>Ärivarava</b>     | Toodetavad tooted.  |
| <b>Süsteemi vara</b> | Tootmiseadmed.  |
| <b>Risk</b>          | Ründaja lisab komponentidesse väikeseid defekte tootmise või hoolduse käigus.                 |
| <b>Mõju</b>          | Toodetava komponendi tervikluse kadu.   |
| <b>Nõrkus</b>        | Komponentide kontrolli- ja testimisprotokollide puudumine.                                    |
| <b>Ohu agent</b>     | Sobivate vahendite ning motivatsiooniga ründaja.  |
| <b>Ründe meetod</b>  | Ründaja sisestab CNC tööpinkide abil mikrovigu.   |
| <b>Turvanõue</b>     | Organisatsioon peab rakendama kvaliteedikontrolli protokolle ja testimisprotseduure.          |
| <b>Kontroll</b>      | Komponentide kontrollimine kvaliteedirikkumiste suhtes, mis võivad ohustada toote terviklust. |

## 9.4 Saadud õppetunnid

Selles peatükis tutvustasime tootmisettevõtet, keskendudes selle müügi, tootearenduse ja tootmistevõtmise protsessidele. Esiteks tõime välja, et ettevõtte seisab silmitsi sarnaste väljakutsetega, mida käsitleti Peatükis 3, hõlmates geopoliitilisi, tehnoloogilisi ja digitaalseid muutusi ning tööjõupuudust. Teiseks illustreerisime STRIDE taksonoomia kasutegureid turvariskide juhtimisel. Kuigi näites illustreerisime viit turvariski, võib STRIDE klassifikatsioon suunata analüütikute tähelepanu erinevatele turvariskidele organisatsioonis.

## 10 Kokkuvõtvad märkused

Tootmise valdkonnas on automatiseeritud süsteemid ja tehnoloogiad arenenud keerukateks valdkondlikeks süsteemideks, mis hõlmavad omavahel seotud Tööstuse 4.0 raamistikke. See areng rõhutab vajadust kaasaegsete turvameetmete järele, et tagada turvalised ja usaldusväärsed töövood.

Käesolevas analüüsis kasutatakse infosüsteemide turvariskide juhtimise (ISSRM) lähene-misviisi, et selgitada konteksti, varasid, turvariske ja nende vastumeetmeid automatiseeritud süsteemides ja tehnoloogiates. ISSRMi valdkonna mudel põhineb toetavate ja kaitstavate va-rade ning turvavajaduste süstemaatilisel kindlaksmääramisel. Samuti määratleb see turvariski kui ohu allika, rünnaku meetodi, nõrkuse ja mõju kombinatsiooni. Valdkonna mudelit rakenda-takse intervjuudes, süstemaatilises kirjanduse analüüsis ja Eesti organisatsioonides läbi viidud küsitluses.

Kogutud andmeid kasutatakse automatiseeritud süsteeme ja tehnoloogiaid kasutavate toot-misorganisatsioonide probleemide kindlaks tegemiseks. Peamiseks väljakutseks on määratletud andmete ja teabe turvalisus. Nende järelduste empiiriline kinnitamine saavutati intervjuude kaudu tootmisettevõtetega, mis näitasid, et hoolimata süsteemide ja seadmete jaoks hästi määratletud turvameetmetest on töötajad sageli turvariskide suhtes haavatavad. Käesolevas analüüsis rõhutatakse, et RAMI 4.0 on valdkondade vaheline arhitektuuriline raamistik, mis on rakendatav erinevates tootmisvaldkondades. RAMI 4.0 kaudu on võimalik tuvastada ärivarad ja süsteemi varad, mis võivad olla turvariskidele suhtes haavatavad.

STRIDE taksonoomia abil uuritakse automatiseeritud süsteemide ja tehnoloogiate turva-riskide. Kirjanduse analüüsi käigus tuvastati 43 turvariski, mis on süstemaatiliselt määratletud ISSRMi riskide hindamise meetodite abil. Enamus riskidest on seotud muukimise/rikkumise ja õiguste vallutamise-ga. Uuringu käigus ei leitud ühtegi salgamise riski. Tuvastatud turvariskide leevendamiseks on välja töötatud turvalisuse vastumeetmed, sealhulgas turvanõuded ja kontrollid. Uuringu tulemused viitavad ka sellele, et organisatsioonid ei kasuta mitte ainult tehnilisi turva-meetmeid, vaid korraldavad ka turvalisuse alaseid koolitusi ning osalevad nii kohapeal kui ka veebis toimuvatel kursustel.

Kirjanduse analüüs näitas, et olemasolevad turvastandardid keskenduvad peamiselt süsteemi ohutusele, kuid ei paku piisavalt terviklikke turvaprotokolle. Arutatud kasutusjuhtumid näitavad, kuidas tootmisorganisatsioonides võiks toimuda turvariskide haldamine. On oluline märkida, et turvasündmused võivad tuleneda mitte ainult välisohudest, vaid ka organisatsiooni enda seest.

Läbiviidud uuringud avavad tee põhjalikumate järelanalüüside tegemiseks. Täpsem uurimine konkreetsete andmetüüpide ja tootmisprotsesside kohta, mis reguleerivad tootmistoiminguid, on oluline, et tuvastada võimalikud ründevektorid ja välja töötada tõhusad tõrjestrategieid. Kuigi RAMI 4.0 pakub standardiseeritud raamistikku, nõuab selle praktiline implementeerimine tööstuses põhjalikumat uurimist. Seetõttu on vajalikud järelanalüüsid, et kontrollida RAMI 4.0-le kohandatud turvameetmeid, nende praktilist rakendamist stsenaariumides ning kaasaegsete tootmisprotsessides.

## Viited

- [1] Hasnaa Ait Malek, Alain Etienne, Ali Siadat, and Thierry Allavena. A Literature Review on the Level of Automation and New Approach Proposal. In Bojan Lalic, Vidosav Majstorovic, Ugljesa Marjanovic, Gregor Von Cieminski, and David Romero, editors, *Advances in Production Management Systems. The Path to Digital Transformation and Innovation of Production Management Systems*, volume 591, pages 408–417. Springer International Publishing, Cham, 2020. Series Title: IFIP Advances in Information and Communication Technology.
- [2] Steven Alter. *The Work System Method: Connecting People, Processes, and IT for Business Results*. Work System Method, 2006.
- [3] Mariia Bakhtina. Securing Passenger’s Data in Autonomous Vehicles. Master’s thesis, University of Tartu, 2021.
- [4] Mariia Bakhtina and Raimundas Matulevičius. Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 13(1):87–111, 2023.
- [5] Marco Balduzzi, Francesco Sortino, Fabio Castello, and Leandro Pierguidi. A Security Analysis of CNC Machines in Industry 4.0. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 132–152. Springer, 2023.
- [6] Center for Internet Security. CIS Critical Security Controls. URL: <https://www.cisecurity.org/controls> (viimati kontrollitud: 15.04.2024), 2024.
- [7] Vickram Chundhoo, Gopinath Chattopadhyay, Gour Karmakar, and Gayan Kahandawa Appuhamillage. Cybersecurity Risks in Meat Processing Plant and Impacts on Total Productive Maintenance. In *2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*, pages 1–5, Ballarat, Australia, December 2021. IEEE.
- [8] George W. Clark, Michael V. Doran, and Todd R. Andel. Cybersecurity Issues in Robotics. In *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, pages 1–5, Savannah, GA, USA, March 2017. IEEE.
- [9] Cybernetica AS. AKIT: Andmekaitse ja Infoturbe portaal, URL: <https://akit.cyber.ee/> (viimati kontrollitud: 30.04.2024), 2023.
- [10] Dr. Karsten Schweichhart. Reference Architectural Model Industrie 4.0 (RAMI 4.0), 2016.
- [11] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. *A Systematic Approach to Define the Domain of Information System Security Risk Management*, pages 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
- [12] EAS, Enterprise Estonia. Väike- ja keskmise suurusega ettevõtja (vke) definitsiooni selgitus vastavalt euroopa komisjoni määruse 800/2008/eÜ lisa 1-le, 2009.

- [13] European Union. General Data Protection Regulation. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04> (viimati kontrollitud: 15.04.2024), 2016.
- [14] Donald Firesmith. Engineering Safety and Security Related Requirements for Software Intensive Systems. In *ICSE Companion*, page 169, 2007.
- [15] J. Frohm, V. Lindström, and M. Winroth. Levels of Automation in Manufacturing. *Int. J. Ergon. Hum. Factors*, 30(19), 2008.
- [16] Ganji, D. and Mouratidis, H. and Gheytaasi, S.M. Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard. In *In Proc. of the 5th International Conference on Advances and Trends in Software Engineering (SOFTENG'19)*, pages 17–23, 2019.
- [17] Information System Authority. Cyber Security in Estonia 2023, URL: <https://www.ria.ee/en/media/2702/download> (viimati kontrollitud: 15.04.2024), 2023.
- [18] ISA Standards and Publications. ISA/IEC 62443 Series of Standards. URL: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> (viimati kontrollitud: 15.04.2024), 2024.
- [19] ISO, Organization for Standardization. ISO/IEC 27000 Family, Information Security Management. URL: <https://www.iso.org/standard/iso-iec-27000-family> (viimati kontrollitud: 15.04.2024), 2024.
- [20] Ugalde J. 15 Technology Challenges Businesses May Face in 2023. URL: <https://www.systems-x.com/blog/technology-challenges-businesses-face> (viimati kontrollitud: 15.04.2024).
- [21] Matthew Jablonski, Bo Yu, Gabriela Felicia Ciocarlie, and Paulo Costa. A Case Study in the Formal Modeling of Safe and Secure Manufacturing Automation. *Computer*, 54(9):59–71, September 2021.
- [22] Jan Kaiser, Duncan McFarlane, Gregory Hawkrige, Pascal André, and Paulo Leitão. A Review of Reference Architectures for Digital Manufacturing: Classification, Applicability and Open Issues. *Computers in Industry*, 149:103923, August 2023.
- [23] Azfar Khalid, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. Understanding Vulnerabilities in Cyber Physical Production Systems. *International Journal of Computer Integrated Manufacturing*, 35(6):569–582, June 2022.
- [24] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic Literature Reviews in Software Engineering – A Systematic Literature Review. *Information and Software Technology*, 51(1):7–15, January 2009.
- [25] Tobias Kutzler, Alexandra Wolter, Andy Kenner, and Stephan Dassow. Boosting Cyber-Physical System Security. *IFAC-PapersOnLine*, 54(1):976–981, 2021.

- [26] Laanemets, Hendrik. Normeerimise ja marsruudi loomise kontseptsioon ettevõtte x näitel, 2023.
- [27] J. Lane Thames. Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems. In Dirk Schaefer, editor, *Cloud-Based Design and Manufacturing (CBDM)*, pages 207–229. Springer International Publishing, Cham, 2014.
- [28] Martin Macak, Radek Vaclavek, Dasa Kusnirakova, Raimundas Matulevičius, and Barbora Buhnova. Scenarios for Process-Aware Insider Attack Detection in Manufacturing. In *Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22*, New York, NY, USA, 2022. Association for Computing Machinery.
- [29] Raimundas Matulevičius. *Fundamentals of secure system modelling*. Springer, 2017.
- [30] Microsoft. Microsoft Security Baselines. URL: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines> (viimati kontrollitud: 15.04.2024), 2024.
- [31] Akseer Ali Mirani, Gustavo Velasco-Hernandez, Anshul Awasthi, and Joseph Walsh. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors*, 22(15):5836, August 2022.
- [32] NIST, National Institute of Standards and Technology. NIST Cybersecurity Framework. URL: <https://www.nist.gov/cyberframework> (viimati kontrollitud: 15.04.2024), 2024.
- [33] Plattform Industrie 4.0. The background to Plattform Industrie 4.0. url: <https://www.plattform-i40.de/IP/Navigation/EN/ThePlatform/Background/background.html> (viimati kontrollitud: 15.04.2024), 2022.
- [34] Hongyi Pu, Liang He, Peng Cheng, Mingyang Sun, and Jiming Chen. Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations. *IEEE Network*, 37(1):111–117, January 2023.
- [35] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. An Experimental Security Analysis of an Industrial Robot Controller. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 268–286, San Jose, CA, USA, May 2017. IEEE.
- [36] Riigi Infosüsteemi Amet. Cyber Security in Estonia. URL: <https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis> (viimati kontrollitud: 15.04.2024), 2024.
- [37] Riigi Infosüsteemi Amet. Eesti Infoturbestandard. URL: <https://eits.ria.ee/> (viimati kontrollitud: 15.04.2024), 2024.

- [38] Yash Shah and Shamik Sengupta. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0406–0413, New York, NY, USA, October 2020. IEEE.
- [39] Adam Shostack. *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.
- [40] Statistikaamet. Eesti Tööstus. URL: <https://www.stat.ee/et/avastatistikat/valdkonnad/majandus/toostus> (viimati kontrollitud: 15.04.2024 ), 2023.
- [41] Beenish Urooj, Ubaid Ullah, Munam Ali Shah, HiraŠhahzadi Sikandar, and Abdul Qarib Stanikzai. Risk Assessment of SCADA Cyber Attack Methods: A Technical Review on Securing Automated Real-time SCADA Systems. In *2022 27th International Conference on Automation and Computing (ICAC)*, pages 1–6, Bristol, United Kingdom, September 2022. IEEE.
- [42] Baicun Wang, Fei Tao, Xudong Fang, Chao Liu, Yufei Liu, and Theodor Freiheit. Smart Manufacturing and Intelligent Manufacturing: A Comparative Review. *Engineering*, 7(6):738–757, June 2021.

# Lisad

## I. Terminid

- **AI** - *Artificial Intelligence* - intellektitehnika.  
Interdistsiplinaarne ala, enamasti loetakse informaatika haruks, tegeleb mudelite ja süsteemidega selliste ülesannete täitmiseks, mida tavaliselt seostatakse inimintellektiga, näiteks arutlemiseks ja õppimiseks [9].
- **B2B** - *Business-2-Business* - ettevõttelt ettevõttele.  
Turundusmudel, milles ettevõtte müüb tooteid, teenuseid või teavet teisele ettevõttele, näiteks tootja hulgimüüjale [9].
- **BPMN** - *Business Process Model and Notation* - äriprotsessimudel ja -notatsioon.  
Graafiline tähistussüsteem äriprotsessiskeemide tarbeks [9].
- **CAD** - *Computer-Aided Design* - raalprojekteerimine.  
Projekteerimistegevustik (sealhulgas joonestamine ja illustreerimine), mille puhul andmetöötlussüsteeme kasutatakse näiteks komponendi või toote projekteerimiseks, simuleerimiseks või täiustamiseks; võimaldab iga graafikaelementi täpselt dimensioneerida ja paigutada [9].
- **CAM** - *Computer-Aided Manufacturing* - raaltootmine.  
Tarkvara ja arvutiga juhitud seadmete kasutamine tootmisprotsessi automatiseerimiseks.
- **CNC** - *Computer numerical control* - arvjuhtimine.  
Tööpinkide arvutipõhine programmjuhtimine [9].
- **DCS** - *Distributed control system* - hajusjuhtimissüsteem.  
Tehnojuhtimissüsteem, milles otsustusloogika ei ole koondatud ühte keskusesse, vaid on hajutatud juhtimisobjekti eri osadesse [9].
- **DDoS** - *Distributed Denial-of-Service attack* - hajus ummistusrünne.  
Ummistusrünne, milles kasutatakse sihtsüsteemi või -võrgu liikluse mahu tunduvaks suurendamiseks suurt arvu ründavaid süsteeme, eriti zombivõrke [9].
- **ERP** - *Enterprise Resource Planning* - ettevõtte ressursside plaanimine.  
Ettevõtte ressursside plaanimist toetav tarkvara.
- **GDPR** - *General Data Protection Regulation* - isikuandmete kaitse üldmäärus.  
Euroopa Parlamendi ja EL Nõukogu määrus (EL) 2016/679, 27. aprill 2016 füüsiliste isikute kaitse kohta isikuandmete töötlemisel, selliste andmete vaba liikumise kohta [9]. Selle määrusega sätestatakse õigusnormid, mis reguleerivad füüsiliste isikute kaitset isikuandmete töötlemisel ja isikuandmete vaba liikumist ning selle eesmärk on kaitsta füüsiliste isikute põhiõigusi ja -vabadusi, eriti nende õigust isikuandmete kaitsele.

- **IEC** - *International Electrotechnical Commission* - rahvusvaheline Elektrotehnikakomisjon.  
Juhtiv rahvusvaheline elektrotehnika ja elektroonika standardimise organisatsioon, asutatud 1906. a. Londonis, liikmeid on 89 maalt (2021), teeb koostööd ISO ja ITUga [9].
- **IIoT** - *Industrial Internet of Things* - tööstuse esemevõrk, masinavõrk.  
Tööstusseadmete esemevõrk [9].
- **IKT** - info- ja kommunikatsioonitehnoloogia.  
Ressursid informatsiooni hõiveks, töötamiseks, talletuseks ja levituseks; termin hõlmab ka sidetehnoloogiat.
- **ISO** - *International Organisation for Standardization* - Rahvusvaheline Standardiorganisatsioon.  
Valitsusväline rahvusvaheline organisatsioon, mis ühendab standardiasutusi, asutatud 1947, peakorter on Genfis, 165 liikmesorganisatsiooni (2020); ISO standardid saavad tihti seaduse jõu lepingute kaudu või liikmesmaade standardite kaudu [9].
- **ISSRM** - *Information Systems Security Risk Management* - infoturbe riskijuhtimine.  
Infoturbe valdkonna mudel, mis hõlmab turvariskide süstemaatilist tuvastamist, hindamist ja juhtimist infosüsteemide kontekstis.
- **IoT** - *Internet of Things* - esemevõrk.  
Kokkuühendatud olemite, inimeste, süsteemide ja teaberessursside taristu koos teenustega, mis töötlevad füüsilisest ja virtuaalsest maailmast pärinevat teavet ja reageerivad sellele [9].
- **NIST** - *National Institute of Standards and Technology* - Riiklik Standardi- ja Tehnikainstituut.  
USA kaubandusministeeriumi allasutus, kes töötab välja testimismeetodeid, teeb tehnilisi analüüse, koostab standardeid riigiasutustele ja nende partneritele ning annab välja infoturbe metoodika- ja juhendmaterjal [9].
- **PLC** - *Programmable Logic Controller* - programmeeritav kontrolleri.  
Eriotstarbeline mikroarvuti, programmeeritav mikroprotsessoriga juhtseade tehniliste protsesside juhtimiseks, eelkõige tööstusautomaatikas [9].
- **RAMI 4.0** - *Reference Architectural Model Industrie 4.0* - tööstuse arhitektuuri referentsmudel.  
Kolmemõõtmeline mudel, mis näitab kuidas struktureeritult läheneda Tööstus 4.0-le. RAMI 4.0 ühendab kõik elemendid ja IT-komponendid ühte kiht- ja elutsükli mudelis.
- **RTU** - *Remote Terminal Unit* - kaugterminaliseade.  
Mikroprotsessoriga juhitud elektrooniline seade, mis kogub andmeid ja juhib protsesse näiteks tööstuslike rajatiste või infrastruktuuri jaotusvõrkude osades. Need seadmed võivad koguda andmeid andurilt, toimetada neid edasi keskele juhtimissüsteemile ning võtta vastu käsklusi ja juhtimisfunktsioone kesksüsteemilt.

- **SCADA** - *Supervisory Control and Data Acquisition* - superviisorsüsteem.  
Liik tehnajuhtimissüsteeme: - automatiseerib tehniliste protsesside järelevalvet ja nende hierarhilise juhtimise ülataset - teenindab operaatorikeskusi andmeside ja kaugjuhtimise abil [9].
- **STRIDE** - *Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege* - võtslimine/teesklus/pettus, muukimine, salgamine, teabe avalikustamine, teenustõkestus/ummistus ja õiguste vallutus.  
Turvariskide hindamise raamistik, mis koosneb erinevatest turvariskide kategooriatest.
- **SYN flood** - SYN-tulve.  
Kahjurkliendilt serverile suunatud ummistusrünne: põhineb massilisel SYN-paketi kordamisel, tekitades massilisel poolelijäävaid TCP-kätlusi; kätluse nurjab kviteeringu puudumine või aadressivõltsing [9].
- **Tööstus 4.0** - 4. tööstusrevolutsioon, mida iseloomustab tööstuse digitaliseerimine, suurandmete ja andmeanalüütika tekkimine ning kasutamine, esemevõrgu ning masinõppe kasutuselevõtt.
- **VKE** - väike- ja keskmise suurusega ettevõtted. [12]
- **VoIP** - *Voice over IP* - kõne IP-protokolli kaudu.  
Metoodika ja tehnoloogiaharu kõneside- ja multimeediumiseansside korraldamiseks IP-protokollil põhinevates arvutivõrkudes, eriti Internetis [9].

## II. Küsitluse küsimused ja vastuse variandid

1. Milline on teie organisatsiooni suurus?
  - Keskmine
  - Väike
  - Mikro
  - Muu
2. Kas teie organisatsioon on osa suuremast grupist või kontsernist?
  - Jah
  - Ei
3. Milline on teie organisatsiooni tootmisklassifikatsioon?
  - Toiduainete tootmine
  - Joogitootmine
  - Tekstiilitootmine
  - Rõivatootmine
  - Nahatöötlemine ja nahktoodete tootmine
  - Puidu töötlemine ning puit- ja korktoodete tootmine, v.a mööbel; õlest ja punumis-  
materjalist toodete tootmine
  - Paberi ja pabertoodete tootmine
  - Trükindus ja salvestiste paljundus
  - Koksi ja puhastatud naftatoodete tootmine
  - Kemikaalide ja keemiatoodete tootmine
  - Põhifarmaatsiatoodete ja ravimpreparaatide tootmine
  - Kummi- ja plasttoodete tootmine
  - Muude mittemetalsetest mineraalidest toodete tootmine
  - Metallitootmine
  - Metalltoodete tootmine, v.a masinad ja seadmed
  - Arvutite, elektroonika- ja optikaseadmete tootmine
  - Elektriseadmete tootmine
  - Mujal liigitamata masinate ja seadmete tootmine
  - Mootorsõidukite, haagiste ja poolhaagiste tootmine
  - Muude transpordivahendite tootmine

- Mööblitootmine
- Muu

4. Milline on teie positsioon/roll organisatsioonis?

- Projektijuht
- Protsessi omanik/juht/analüütik
- Tootmisjuht
- Süsteemianalüütik
- Tarkvara/süsteemiarhitekt
- Infotehnoloogia (IT) juht
- Infoturbejuht
- Tegevjuht
- Tehnoloogiajuht
- Muu

5. Milline on tootmise automatiseerituse tase teie organisatsioonis?

- Tase 1 - Täielikult manuaalne
- Tase 2 - Käsitsi töötamine staatiliste vahendite abil
- Tase 3 - Käsitsi töötamine paindlike töövahendite abil
- Tase 4 - Automaatne käsitööriist: Käsitsi töötamine automatiseeritud töövahendite abil
- Tase 5 - Staatiline masin/töökoht: Automaatne töö masinaga, mis on ette nähtud konkreetse ülesande täitmiseks
- Tase 6 - Paindlik masin/töökoht: Automaatne töö masinaga, mida saab ümber konfigureerida erinevate ülesannete jaoks
- Tase 7 - Täielikult automatiseeritud

6. Kuidas teie organisatsioon rakendab ja haldab oma automatiseeritud tootmissüsteeme, arvestades, et need võivad koosneda erinevatest allsüsteemidest ja komponentidest, mis pärinevad erinevatelt tootjatelt?

- Me kasutame ühe teenusepakkuja lahendust ilma jooksva arenduse või kohandamiseta.
- Me kasutame terviklikku lahendust, mida algne teenusepakkuja regulaarselt uuendab ja täiendab.
- Kasutame süsteemi haldamiseks kolmandapoolse teenuseid ilma vajaduspõhiste kohandamisteta.

- Teeme koostööd kolmandapoolse teenusepakkujatega, kes kohandavad ja ajakohastavad süsteemi vastavalt meie vajadustele.
- Meil on majasisene tugimeeskond süsteemile, mille töötab välja väline teenusepakkuja, meeskond tegeleb väiksemate uuendustega ja hooldusega.
- Meie ettevõttesisene arendusmeeskond jälgib meie süsteemi kõiki aspekte, sealhulgas erinevate tootjate allsüsteemide integreerimist, pidevat tuge ja individuaalset arendamist.
- Haldame eri tootjate integreeritud allsüsteemide kombineeritud keskkonda, kusjuures tugi ja uuendused toimuvad nii ettevõttesiseste kui ka väliste ressursside kaudu.
- Muu

7. Mil määral on teie automatiseeritud tootmissüsteem viimase 5 aasta jooksul muutunud?

- Muudatusi ei ole toimunud
- Väikesed muudatused allsüsteemides või komponentides, põhifunktsioonid on jäänud samaks
- Olulised muudatused allsüsteemides või komponentides, põhifunktsionaalsus on jäänud samaks
- Põhifunktsioonide olulised muudatused (süsteemi asendamine)
- Muu

8. Millised on teie organisatsiooni peamised väljakutsed automatiseeritud tootmissüsteemi, sealhulgas erinevate tootjate allsüsteemide integreerimisel, kasutamisel, arendamisel ja toetamisel?

- Andmekaitse ja turvalisuse tagamine erinevate allsüsteemide ja toodete integreerimise käigus
- Süsteemi tõhususe ja privaatsuse tasakaalustamine keerulises tootmiskeskonnas
- Tööstuse eeskirjade ja standardite puudulikkuse või ebajärjekindluse jälgimine erinevates allsüsteemides
- Tootmise protsesside optimeerimine mitmete erinevate allsüsteemide puhul
- Süsteemi turvalisuse ja töökindluse haldamine enne kasutuselevõttu ja kasutamise käigus
- Koostalitlusvõime tagamine erinevate allsüsteemide vahel ja/või väliste süsteemide või teenusepakkujatega
- Aruka tootmise ühtse riikliku või kogu tööstusharu hõlmava strateegia puudumine
- Ressursipiirangute haldamine seadmetes ja tootmisliini allsüsteemides
- Erinevate võrkude ja sideprotokollidega seotud probleemide lahendamine

- Süsteemi kvaliteediomadustele, nagu skaleeritavus, tõhusus ja kohandatavus erinevatele platvormidele ja operatsioonisüsteemidele, esitatavate kõrgete ootuste täitmine
- Muu

9. Millist teavet kasutatakse teie automatiseeritud tootmissüsteemis?

- Andurite informatsioon
- Protsessi informatsioon
- Operatiivne informatsioon
- Keskkonnaalane informatsioon
- Kvaliteediinfo
- Informatsioon tootmise kohta
- Informatsioon tootmise ajakava kohta
- Tarkvara uuendused
- Laovarude seis
- Hooldusalane info
- Alarmid/süsteemi veateated
- Muu

10. Milliseid automatiseeritud süsteeme te kasutate?

- Avatud tekstiga vastus

11. Millistel eesmärkidel kasutab teie organisatsioon infotehnoloogia (IT) süsteeme oma automatiseeritud tootmisprotsessides?

- Me ei kasuta oma tootmisprotsessides IT-süsteeme.
- Digitaalsete andmete salvestamiseks ja haldamiseks.
- Kliendisuhete ja müügiotsuste haldamiseks.
- Ettevõtte ressursside planeerimise (ERP) jaoks.
- Digitaalsete teenuste või toodete pakkumine otse lõppkasutajatele.
- Andmete vahetamiseks väliste IT-süsteemide või partneritega.
- Tootmise planeerimiseks ja ajakava koostamiseks.
- Tarneahela juhtimiseks, sealhulgas logistika ja varude kontrolliks.
- Kvaliteedikontrolliks ja nõuetele vastavuse järelevalveks.
- Ennetavaks hoolduseks ja varade haldamiseks.
- Tootmiseseadmete reaalajas jälgimiseks ja kontrollimiseks.

- Inimressursside haldamiseks.
  - Teadus- ja arendustegevuseks, sealhulgas tootekujunduseks ja simulatsiooniks.
  - Muu
12. Kas teie organisatsiooni automatiseeritud tootmisprotsesside arhitektuur on kooskõlas mudeliga RAMI 4.0 (Reference Architecture Model Industrie 4.0)? Kui ei, siis palun täpsustage mudel või arhitektuuriraamistik, mida te järgite, või kirjeldage oma tootmisprotsessi arhitektuuri struktuuri.
- See ei ole kooskõlas ühegi arhitektuuri või raamistikuga.
  - Jah, see on kooskõlas RAMI 4.0-ga.
  - Muu
13. Kuidas teie organisatsioonis käsitletakse küberturbega seotud teemasid?
- Küberturvet hallatakse täielikult ettevõttesiseselt. Meie spetsialiseerunud ettevõttesisene küberturbe meeskond töötab välja ja rakendab turvapoliitikaid, viib regulaarselt läbi turvahinnanguid ja reageerib intsidentidele.
  - Koostöö väliste küberturbeorganisatsioonidega. Me teeme koostööd väliste küberturbeorganisatsioonidega auditite, riskianalüüsi ja intsidentidele reageerimise osas, et täiendada meie enda võimekust.
  - Küberturvalisus kui osa IT-osakonnast. Küberturbeülesanded on integreeritud meie IT-osakonna rollidesse, hõlmates kõike alates rutiinsetest turvauuendustest kuni töötajate koolitamiseni.
  - Automatiseeritud turvalahenduste kasutamine. Me tugineme automaatsetele turvalahendustele (nt tule müürid, sissetungituvastussüsteemid) pideva järelevalve ja ohtude tuvastamise eesmärgil, mida IT-personal regulaarselt haldab.
  - Sisseostetud küberturbe haldamine. Küberturvalisuse haldamine on täielikult allhangitud spetsialiseerunud organisatsioonist, kes tegeleb meie turvalisuse kõigi aspektidega, alates poliitika väljatöötamisest kuni intsidentidele reageerimiseni.
  - Ad hoc küberturbe praktikad. Küberturvalisuse meetmeid rakendatakse ad hoc, ilma spetsiaalse meeskonna või järjepideva strateegiata, sageli reageerides konkreetsetele riskidele.
  - Töötajate koolitus ja teadlikkuse tõstmise programmid. Me seame prioriteediks töötajate koolituse ja teadlikkuse tõstmise meetmed, et tagada kogu personali teadlikkus küberturvalisuse riskidest ja parimatest tavadest.
  - Vastavus tööstusharu eeskirjadele ja standarditele. Meie küberturvalisuse tavad juhinduvad tööstusharu eeskirjade ja standardite järgimisest, tagades, et me täidame konkreetseid turvakriteeriume.
  - Muu

14. Millised turvalisuse, privaatsuse või ohutusega seotud õigusaktid, määrused ja/või standardid mõjutavad teie automatiseeritud tootmissüsteemi?

- General Data Protection Regulation (EU GDPR)
- Consumer Protection Directives 2019/770 and 2019/771
- NIST Special Publications (e.g. NIST SP 800-39, NIST SP 800-37)
- UNECE regulation No 155 Cyber security and cyber security management system (from 2020)
- Estonian Information Security Standard (E-ITS)
- NIS2 directive
- ISO 10218
- ISO 12100
- ISO TS 15066
- ISO 2700x family
- ISO 27701
- ISO 31000
- Isikuandmete kaitse seadus(IKS)
- Küberturvalisuse seadus(KüTS)
- Ma ei tea
- Muu

15. Kas teie organisatsioon on kogenud küberturbega seotud vahejuhtumeid?

- Meil ei ole esinenud ühtegi turvaintsidenti
- Õngitsemine
- Konto ülevõtmine
- Andmetega manipuleerimine(nt tahtlik andmete muutmine)
- Pettus
- Kaugühenduse haavatavuste ärakasutamine
- Teenuste tõkestus
- Lunavaranõue
- Viirus
- Andmete leke
- Pahatahtlik ümbersuunamine
- Volitamata juurdepääs süsteemidele ja andmetele

- Paroolirünne
- Pahavara
- Muu

16. Milliseid vastumeetmeid rakendab teie organisatsioon küberturbe intsidentide vähendamiseks?

- Viirustõrje- ja pahavaravastased lahendused
- Varukoopiastest ja hädaolukorrast taasteplaanid andmete terviklikkuse tagamiseks
- Tulemüürid ja sissetungi tuvastamise/ennetamise süsteemid (IDS/IPS)
- Regulaarsed küberturvalisuse alased koolitused ja teadlikkuse tõstmise programmid töötajatele
- Andmete krüpteerimine hoitavate ja edastatavate andmete puhul
- Korrapärase tarkvarauuenduste ja paranduste haldus
- Välised turvahinnangud ja läbistustestid
- Tundlike andmete anonüümimine ja pseudonüümimine
- Kasutajaõiguste piiramine ja juurdepääsukontroll
- Koostöö välise küberturbeorganisatsioonidega ohtude analüüsi eesmärgil
- Intsidentidele reageerimise kava ja meeskond
- Meil ei ole mingeid turvakontrollimeetmeid
- Regulaarsed turvaauditid ja haavatavuse hindamine
- Plokiahela või muude kõrgtehnoloogiate kasutamine turvalisuse suurendamiseks
- Füüsilise turbe meetmed riistvara ja infrastruktuuri kaitsmiseks
- Turvateabe ja -sündmuste halduse süsteemid (nt SIEM, SOC)
- Mitmikautentimine (MFA) süsteemidele juurdepääsuks
- Programmeerimise turbetavade kasutamine
- Võrgu segmenteerimine võimalike rünnete leviku piiramiseks
- Muu

17. Kuidas toimub teie organisatsioonis töötajate küberturbealane koolitamine?

- Regulaarsed kohustuslikud küberturbe alased koolitused töötajatele.
- IT- ja turvatöötajate erikoolitus.
- Veebipõhised koolituskursused ja -ressursid.
- Välised õpitoad ja seminarid.
- Kohapealsed küberturbe harjutused ja õppused

- Küberturbekoolitusi ametlikult ei pakuta
  - Muu
18. Kui soovite jagada midagi küberturbega seonduvat, võite seda vabalt teha. Laiendage või lisage konteksti mis tahes konkreetsele teemale, mis teie arvates vajab rohkem tähelepanu.
- Avatud tekstiga vastus
19. Kas me võime teiega tulevikus võimaliku koostöö osas ühendust võtta? Kui jah, siis palun jätke oma e-posti aadress.
- Avatud tekstiga vastus

### III. Riski stsenaariumid

| Riski ID | Rünne   | Oht  | Nõrkus  | Süsteemi vara   | Ärivarava  | Mõju   |
|----------|---|--|---|---|--|--|
| 001      | Oma-töötaja rünne [23], [35], [34] tahtlikult või tahtmatult. | Siseringi töötaja manipuleerib operatiivkäsklusi.                    | Töötajate taustakontrolli puudumine.  | <b>RAMI 4.0:</b> välisseade, jaam, töökeskus, ettevõtte.<br><b>Siht:</b> töötaja [23].  | Tegevusandmed, tootmisparameetrid.   | Kaob ärivara terviklus, kaob süsteemi vara töökindlus.   |
| 002      | Andmetega manipuleerimine [23].                               | Ohuagent rikub andmeid ja muudab turvapoliitikat.                    | Ebapiisav andmete valideerimine ja tervikluse kontroll, nõrk poliitika juhtimine ja järelvalve.   | <b>RAMI 4.0:</b> töökeskus, ettevõtte.<br><b>Siht:</b> serverid, andmekeskused.   | Turvapoliitika haldussüsteem, turvalisuse eeskirjad, turvalisuse protokollid, turvalisuse haldussüsteem. | Ohustab ärivara konfidentsiaalsust ja terviklust; rikub turvameetmete ja süsteemi varade tõhusust ja usaldusväärsust [23].               |
| 003      | Koodiga manipuleerimine [23], [8], [38].                      | Ohuagent sisestab pahatahtlikku koodi või muudab olemasolevat koodi. | Ebapiisavad koodikontrolli protsessid; automatiseeritud turvakontrolli puudumine; ebapiisav juurdepääsukontroll koodihoidlatele [38], [34]. | <b>RAMI 4.0:</b> välisseade, juhtimisseade, tööjaam, ettevõtte.<br><b>Siht:</b> püsivara, rakendusserverid, lähtekoodi repositooriumid. | Rakendustarkvara ja seadme püsivara [23].  | Kompromiteeritud rakenduse funktsionaalsus [23], [38], [34], võimalikud andmekaitse rikkumised, volitamata juurdepääs süsteemidele [34]. |

|     |                                 |  |   |  |   |   |
|-----|---------------------------------|--|---|--|---|---|
| 004 | Pahavara [23], [8], [34], [34]. | Ohuagent paigutab organisatsiooni võrku pahavara viiruse, ussi, tagaukse, lunavara või nuhkvara kujul. | Ebapiisav lõppseadmete turvalisus; regulaarsete süsteemi uuenduste ja paranduste puudumine; ebapiisav võrgu segmenteerimine ja turvalisus [34]; nõrgad e-posti ja veebi filtreerimise põhimõtted. | <b>RAMI 4.0:</b> töökeskused, serverid, ühendatud maailm (lõppkasutaja seadmed).<br><b>Siht:</b> serverid, lõppkasutaja seadmed. | Süsteemi ja rakenduste käideldavus ja jõudlus; organisatsioonilised ja kliendiandmed. | Tegevuse katkemine süsteemi kahjustamise või rikke tõttu, andmete vargus või kaotus, finantskahju, õiguslikud ja nõuetele vastavuse tagajärjed, maine kahjustumine.   |
| 005 | Võrgu ussviirus [23].           | Ise paljunev uss imub võrku, levib kiiresti seadmetesse ja süsteemidesse ilma kasutaja sekkumiseta.    | Uuendamata tarkvara või operatsioonisüsteemid, avatud arvutivõrk, ebapiisav võrgu segmenteerimine [34], ohu tuvastamise mehhanismide puudumine.   | <b>RAMI 4.0:</b> töökeskused, serverid.<br><b>Siht:</b> ruuterid, serverid.  | Võrgu infrastruktuur, võrguseadmetesse salvestatud andmed.                            | Võrgu jõudluse halvenemine, süsteemi rikked [21], [38], volitamata juurdepääs andmetele [23], [34], äritegevuse katkemine.  |
| 006 | Viirus [23], [8].               | Ründaja paigaldab organisatsiooni süsteemidesse arvutiviiruse.   | Ajakohastatud viirusetõrjetarkvara puudumine, töötajate ebapiisav väljaõpe [41], nõrgad e-posti ja allalaadimiste turvapoliitika ning ebapiisavad süsteemi uuendamise eeskirjad.                  | <b>RAMI 4.0:</b> kõik.<br><b>Siht:</b> mistahes vara koos tarkvaraga.  | Andmete ja tarkvara terviklus ja käideldavus.   | Individuaalse ja organisatsioonilise tootlikkuse katkemine [23], [21], [38], tundlike andmete kadumine või rikkumine [34], süsteemi taastamis- ja remonditöödest tulenev rahaline kahju ja kahju organisatsiooni mainele [8], [35], [38]. |

|     |  |   |  |   |  |   |
|-----|--|---|--|---|--|---|
| 007 | Ummistus (teenuse tõkestus) [23], [34].                        | Ohuagent koormab organisatsiooni võrguressursse või -teenuseid liigse liiklusega.   | Ebapiisav võrgu ri-balaius, kiiruse pii-ramise või liikluse filtreerimise mehha-nismide puudumine, ebapiisavad teenuse tõkestuse kaitsestra-teegiad [34].  | <b>RAMI 4.0:</b> võrgu infrastruktuur.<br><b>Siht:</b> ruuterid, jaotu-rid, serverid [23].                          | Veebi teenused [34], klientide juurde-pääs digitaalsetele platvormidele, toimingute tõhusus.           | Teenuse käideldavuse kadu, mis toob kaasa talitlushäireid [38], [34], klientide usalduse ja rahulolu kahjustamine [35], [38], tulude vähe-nemine seisakute ajal [35], ja suuremad kulud seoses võrgu paranda-mise ja kaitsevõime tugevdamisega.                       |
| 008 | Arenduse elutsükli jooksul paigal-datavad tagauksed [23], [8]. | Ohuagent paigaldab tarkvara või riistva-ara arenduse elutsükli ajal tagauksed, mis võimaldavad hilise-mas etapis volitamata juurdepääsu või volitamata kontrolli. | Ebapiisavad turva-meetmed arendus- ja tarneahela protsessis, kolmandate osapoolte tarnijate põhjaliku kontrolli puudumine, ebapiisavad auditid ja nõrgad juurde-pääsukontrollid arenduskeskkondade-le. | <b>RAMI 4.0:</b> aren-dusvahendid ja -keskkonnad.<br><b>Siht:</b> tarkvara, riist-vara, tarneahela inf-rastruktuur. | Toote terviklus ja turvalisus, usaldus organisatsiooni toodete ja teenuste vastu, intellek-tuaalomand. | Volitamata juurdepääs süsteemidele ja and-metele [34], toote ja sellega seotud süs-teemide kahjustamise potentsiaal, klientide ja teiste osapoolte usalduse vähenemine [35], [38], õiguslikud ja regula-tiivsed tagajärjed ning märkimisväärne finants-ja mainekahju. |

|     |   |  |   |  |  |   |
|-----|---|--|---|--|--|---|
| 009 | IT-infras-<br>tuktuuri<br>füüsiline<br>hävitami-<br>ne [23],<br>[35], [21]. | Kriitilise IT-riistvara<br>ja -infrastruktuuri<br>tahtlik füüsili-<br>ne hävitamine<br>ohuagentide (N:<br>töötajad, töövõtjad<br>või sissetungijad)<br>poolt.  | Ebapiisavad füüsili-<br>sed turvameetmed<br>IT-infrastruktuuri<br>asukohtades (and-<br>mekeskused, serveri-<br>ruumid), järelevalve-<br>ja juurdepääsukont-<br>rolli süsteemide<br>puudumine, ebapii-<br>savad hädaolukorra<br>taastamise ja ta-<br>litluspidevuse<br>planeerimine. | <b>RAMI 4.0:</b> integrat-<br>siooni, kommunikati-<br>siooni ja funktsio-<br>naalsed kihid.<br><b>Siht:</b> füüsiline IT-<br>riistvara [23], [35],<br>[21], serverid, ruute-<br>rid, jaoturid.   | Operatiivandmed,<br>äritegevuse toime-<br>pidevus, toodete ja<br>teenuste terviklus ja<br>käideldavus. | Kriitiliste IT-teenuste ja<br>andmete kaotus, märki-<br>misväärne seisak ja ärite-<br>gevuse häirimine, tundli-<br>ke andmete võimalik kao-<br>tus, kõrged taastamis- ja<br>asenduskulud ning orga-<br>nisaatsiooni maine võima-<br>lik kahjustamine.             |
| 010 | Pealt-<br>kuulamine<br>[23], [8],<br>[34].                                  | Loata pealtkuula-<br>mine ja pealtkuu-<br>lamine isiklikuks<br>kasutamiseks<br>mõeldud digi-<br>taalsides, näiteks<br>e-kirjad, kõned või<br>andmeedastused,<br>välis- või sisemiste<br>osalejate poolt. | Krüpteerimata si-<br>dekanalid [34],<br>nõrk võrguturve,<br>ebapiisav turvaliste<br>sideprotokollide<br>kasutamine [41], eba-<br>piisav lõppseadmete<br>turvalisus.   | <b>RAMI 4.0:</b> kommu-<br>nikatsiooni ja vara<br>kihid.<br><b>Siht:</b> ruuterid, jaotu-<br>rid, Wi-Fi juurdepää-<br>su punktid, kommu-<br>nikatsiooni süsteem<br>(e-mail) VoIP süstee-<br>mid. | Teabe konfident-<br>siaalsus, konfident-<br>siaalsed ärisuhted,<br>intellektuaalomand.                 | Tundliku teabe rikkumi-<br>ne, mis toob kaasa and-<br>mete rikkumise, konku-<br>rentsielise kaotus, või-<br>malikud õigus- ja nõuete-<br>le vastavuse rikkumised,<br>klientide ja sidusrühma-<br>de usalduse vähenemise<br>ning maine kahjustamise<br>[35], [38]. |

|            |   |  |  |   |  |   |
|------------|---|--|--|---|--|---|
| <b>011</b> | Riistvara tagaukse kasutamise [23], [8] | Ohuagent võib kahjustatud tarneahela kaudu või tootmise käigus paigaldada riistvara komponentidesse tagaukse, mis võimaldab volitamata juurdepääsu või volitamata kontrolli. | Riistvara tarnijate ebapiisav kontroll, riistvara põhjaliku turvakontrolli puudumine enne kasutuselevõttu, ebapiisav järelevalve tootmisprotsessi üle ja nõrk tarneahela turvalisus. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> füüsilised komponendid. | Füüsilise tehnoloogia infrastruktuuri terviklus ja turvalisus. | Loata juurdepääs kriitilistele süsteemidele ja kontroll nende üle [34], organisatsiooni võrgu ulatuslik kahjustamine [23], klientide usalduse ja ärilise maine kahjustamine, õiguslikud ja nõuetele vastavuse probleemid ning märkimisväärne rahaline kahju [35], [38]. |
| <b>012</b> | Vea süstimine [8], [35].                | Ohuagent põhjustab tahtlikult vigu süsteemi riist- või tarkvaras, et põhjustada süsteemi talitlushäireid.  | Riist- ja tarkvara vastuvõtlikkus välistele manipulatsioonidele, ebapiisav vigade taluvuse testimine, töökindlate veakäitlus- ja valideerimismehhanismide puudumine.                 | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> sardsüsteemid.          | Süsteemi usaldusväarsus ja turvalisus, andmete terviklus.      | Süsteemi funktsionaalsuse kahjustamine, andmete rikkumine, turvameetmete õonestamine, organisatsiooni usaldusväärsuse ja klientide usalduse kahjustamine.   |

|     |                                      |  |  |  |   |   |
|-----|--------------------------------------|--|--|--|---|---|
| 013 | Riistvara omavõimeline muutmine [8]. | Ohuagent muudab füüsiliselt riistvara komponente või manipuleerib nendega. | Riistvara ebapiisav füüsiline turvalisus [34], võltsimise tuvastamise mehhanismide puudumine, ebapiisav riistvara tervikluse järelevalve ja puudulik kontroll riistvara hoolduse üle [38]. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> sardsüsteemid.   | Süsteemi usaldusväärsus ja turvalisus, andmete terviklus.   | Autoriseerimata juurdepääs süsteemile [34], mis toob kaasa andmete rikkumise või süsteemi kahjustamise, tegevuse katkemise, võimaliku spionaaži ja mainekahju [35], [38].               |
| 014 | Puhvri ületäitumine [8].             | Ohuagent kasutab ära puhvri ülevoolu nõrkust tarkvara programmis.          | Tarkvara, mis ei halda mälu nõuetekohaselt, piiride ja kontrollimise puudumine koodis, eaturvaliste programmeerimiskeelete või teekide kasutamine, mis võimaldavad puhvri ületäitumist.    | <b>RAMI 4.0:</b> funktsionaalne kiht.<br><b>Siht:</b> tarkvara rakendused, operatsiooni süsteemid, püsivara. | Tarkvarasüsteemide terviklus, kättesaadavus ja konfidentsiaalsus, andmete konfidentsiaalsus ja terviklus. | Autoriseerimata juurdepääs [34], võimalikud süsteemi töö katkestused, andmete rikkumine, võrgu turvalisuse kahjustamine ning organisatsiooni maine ja usalduse kahjustamine [35], [38]. |

|     |  |   |  |   |                                     |   |
|-----|--|---|--|---|-------------------------------------|---|
| 015 | Riistvarasse tootmikro- vigade sises- tamine [35].               | Ohuagent lisab toot- mise või hoolduse käigus riistvara komponentidesse mikroskoopilisi defekte.  | Kontrolli- ja tes- timisprotokollide puudumine, ebapiisav järelevalve tootmis- ja hooldusprotsesside üle, tuginemine kolmandate isiku- te kontrollimata komponentidele või teenustele.     | <b>RAMI 4.0:</b> integrat- siooni kiht.<br><b>Siht:</b> sardsüsteemid, kiibid, mikroprotses- sorid, trükiplaadid.                     | Riistvara komponen- tide terviklus. | Riistvara funktsionaal- suse kahjustamine, organisatsiooni kvalitee- di ja usaldusväarsuse ning maine kahjustami- ne, kulude suurenemine [35], [38].                                |
| 016 | Ohutus- sätete väljalülita- mine või muutmine [35].              | Ohuagent lülitab füüsiliselt välja või muudab ohu- tussätteid, et luua ohtlikud tingimused või võimaldada volitamata füüsilist juurdepääsu. | Ebapiisav füüsiline turvalisus [34] ja ohutussätete järele- valve, ohutusseadete regulaarse kontrolli ja katse puudumine.  | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> füüsilise juurdepääsu kont- rollimise ruumid (jaamad), ohutus- /hädaolukorra süsteemid. | Tööohutus, persona- li heaolu.      | Suurenenud õnnetusjuh- tumite ja füüsiliste vi- gastuste oht, võimalikud talitlushäired, elutähtsate infrastruktuuride kahjus- tamine, õiguslik vastutus [35], [38].                |
| 017 | Autorisee- rimata juur- depääs süsteemi- dele ja andmetele [35]. | Ohuagent pääseb ligi organisatsiooni süsteemidele või andmetele.  | Nõrgad autenti- mismehhanismid, ebapiisav juurde- pääsukontroll [41]), [38], [34], mitmefak- torilise autentimise puudumine, halb paroolide haldamine ja ebaturvalised võrguteenused [34]. | <b>RAMI 4.0:</b> funktsio- naalne kiht.<br><b>Siht:</b> andmebaasid, serverid, kasutajate haldussüsteemid, haldusvahendid.            | Andmete konfident- siaalsus.        | Andmete rikkumine, süs- teemi seadete või äriand- mete omavoliline muut- mine, õiguslike ja regu- latiivsete nõuete rikku- mine, maine kahjustami- ne ja rahaline kahju [35], [38]. |

|            |  |   |  |  |   |  |
|------------|--|---|--|--|---|--|
| <b>018</b> | Kaugvõrgu nõrkuste ärakasutamise [35].         | Ohuallikas kasutab organisatsiooni kaugvõrgu juurdepääsu nõrkusi ja saab juurdepääsu sisevõrgule.   | Ebapiisav võrgu segmenteerimine, vananenud või parandamata võrgutarkvara [34], ebaturvalised kaugjuurdepääsu protokollid [41], ebapiisavad tulemüürireeglid ja sissetungi avastamise/kaitsetsüsteemide puudumine [34]. | <b>RAMI 4.0:</b> kommunikatsiooni kiht.<br><b>Siht:</b> tulemüürid, ruuterid, jaoturid, kaugjuurdepääsu serverid, väravad. | Võrgu terviklus ja turvalisus, edastatavate andmete konfidentsiaalsus ja terviklus. | Loata juurdepääs sisevõrkudele [34], võrguteenuste katkemine, võimalik andmete pealtkuulamine ja vargus, tundliku teabe ohustamine ning sellest tulenev finants- ja mainekahju organisatsioonile [35], [38]. |
| <b>019</b> | Omatöötaja poolt võimaldatud võrgurünnak [35]. | Ohuagent, kellel on füüsiline juurdepääs organisatsiooni ruumidesse, ühendub füüsiliselt sisevõrku. | Ebapiisav füüsiline juurdepääsukontroll võrguportidele ja -seadmetele, halb võrgu segmenteerimine, kohaliku võrguliikluse ebapiisav jälgimine, tugeva autentimise puudumine [41], [38], [34].                          | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> füüsiline võrgu riistvara.   | Võrgu süsteemide terviklus, siseside konfidentsiaalsus.                             | Võrguturbe kahjustamine, pahavara sissetoomine, loata jälgimine, IT-teenuste häirimine ja sellest tulenev kahju toimimisele, rahaline ja maine kahjustamine [35], [38].                                      |

|            |   |  |   |   |  |   |
|------------|---|--|---|---|--|---|
| <b>020</b> | Füüsiline anduritega manipuleerimine [21].  | Ohuagent takistab, häirib või kahjustab füüsiliselt andureid.  | Füüsiliste kaitsemeetmete puudumine tundlike andurite juures [38], ebapiisav manipuleerimise tuvastamine, toimetuleku ebaõnnestumine ja nõrgad intsidentidele reageerimise protokollid. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> sensorid, kaamerad, ajamid.   | Andmete terviklus, operatiivteadlikkus.          | Olukorra teadlikkuse kadumine, ebaõiged andmed, füüsilise kahju või protsessi häirete tekkimise võimalus ning organisatsiooni tegevuse järjepidevuse säilitamise ohustamine [38]. |
| <b>021</b> | Juurdepääsulubade vargus ja kloonimine[21]. | Ohuagent varastab volitatud töötajalt füüsilise juurdepääsu kaardi või kloonib neid, et pääseda piiratud juurdepääsuga kohtadesse. | Ebapiisavad füüsilised turvameetmed, kaartide juurdepääsu järelevalve puudumine, nõrgad autentimisprotsessid ja kadunud või varastatud kaartide viivitamatu deaktiveerimise puudumine.  | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> identifikatsiooni märgid.   | Füüsiliste ruumide turvalisus, töötajate ohutus. | Volitamata juurdepääs, mis võib viia varguse või sabotaažini [34], rajatiste ohustatud turvalisus, risk töötajate ohutusele.  |
| <b>022</b> | Käskude süstimine [21].                     | Ohuagent kasutab tarkvara eaturvalist sisendi valideerimist, et sisestada volitamata käske.  | Ebapiisav sisendi valideerimine ja puhastamine, protsesside täitmine ülemääraste õigustega, tõhusa rakenduskihi turvakontrolli puudumine ja eaturvalised kodeerimistavad.               | <b>RAMI 4.0:</b> funktsionaalne kiht.<br><b>Siht:</b> rakendustarkvara, operatsioonisüsteemid, rakenduskeskkonnad (veebiserverid, andmebaasid). | Tarkvararakenduste terviklus ja käideldavus.     | Volitamata süsteemitegevus, mis viib andmete rikkumiseni, süsteemi ohustamiseni ja teenuste katkestamiseni; organisatsiooni maine ja usalduse kahjustamine [35], [38].            |

|     |   |   |   |   |  |   |
|-----|---|---|---|---|--|---|
| 023 | Omavoliline seadete muutmine [21].            | Ohuagent saab juurdepääsu seadete liidestele või -failidele ja teeb lubamatuid muudatusi.                             | Ebapiisav juurdepääsukontroll seadetele, muudatuste haldamise ja järelevalve puudumine, liiga suured kasutajakontode õigused ning seadete muudatuste ebapiisav auditeerimine. | <b>RAMI 4.0:</b> funktsionaalne kiht.<br><b>Siht:</b> rakendustarkvara, operatsioonisüsteemid, rakenduskeskkonnad (veebiserverid, andmebaasid). | IT-süsteemide terviklus ja turvalisus.       | Operatiivse toimimise häirimine valesti seadistatud süsteemide tõttu, regulatiivsete nõuete täitmata jätmine, võimalikud andmekaoad ja usalduse kaotamine [35], [38].         |
| 024 | Volitamata ligipääs liidestele [21].          | Ohuagent kasutab süsteemide nõrkusi, et saada volitamata juurdepääs, mis viib kontrollini füüsiliste protsesside üle. | Nõrgad autentimismehhanismid [41], [38], [34], parandamata tarkvara, ebapiisav võrgu segmenteerimine.   | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> juhtimissüsteemid, konsolid, SCADA süsteemid.   | Tööprotsesside terviklus ja käideldavus.     | Riskid, mis tulenevad kontrolli kaotamisest tööstusprotsesside üle [21], [38], [34], omavolilised muudatused seadistustes, andmete võltsimine ja vara füüsiline kahjustamine. |
| 025 | Füüsiline ja digitaalne manipuleerimine [38]. | Ohuagent muudab füüsiliselt või manipuleerib digitaalselt seadmeid, tarkvara või andmeid.                             | Ebapiisav füüsiline turvakontroll, ebapiisav andmete ja tarkvara tervikluse kontroll, võltsimise tuvastamise ja vältimise mehhanismide puudumine, nõrk juurdepääsude haldus.  | <b>RAMI 4.0:</b> vara ja funktsionaalne kiht.<br><b>Siht:</b> rakendustarkvara, füüsilised seadmed.   | Andmete ja operatsioonisüsteemide terviklus. | Volitamata muudatused, mis põhjustavad süsteemi talitlushäireid [21], [38], [34], andmete rikkumine või kadumine, uute nõrkuste tekkimine.                                    |

|     |                           |  |  |  |  |   |
|-----|---------------------------|--|--|--|--|---|
| 026 | Unepuudus [38].           | Ohuagent saadab pidevalt päringuid süsteemile, seadmele või komponendile, takistades selle üleminekut vähese energia tarbimise olekusse (puhkeolekusse). | Kiiruse piiramise või päringute filtreerimise puudumine seadmetes, ebapiisavad energiahaldusprotokollid ning ebapiisav süsteemi jõudluse ja seisundi jälgimine.                              | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> IoT-seadmed, serverid, võrguseadmed.   | Riistvara käideldavus ja terviklus, toimimise tõhusus. | Suurenenud energia tarbimine, mis toob kaasa suuremad tegevuskulud [35], [38], seadmete vähenenud eluiga pideva töö tõttu, võimalikud süsteemirikked või talitlushäired ja süsteemi üldise jõudluse vähenemine.                           |
| 027 | SYN-tulve [38].           | Ründaja saadab sihtserverile kiiresti järjestikuseid SYN-päringuid, kuid ei vasta serveri SYN-ACK-vastustele.  | Ebapiisav SYN-tulvakaitse serverites, kiiruse piiramise puudumine, ebapiisav võrgu infrastruktuur suure andmemaahu käsitlemiseks, halb SYN-pakettide filtreerimine.                          | <b>RAMI 4.0:</b> vara ja kommunikatsiooni kiht.<br><b>Siht:</b> veebiserverid, rakendusserverid, võrgu infrastruktuur.       | Interneti-teenuste käideldavus, toimimise tõhusus.     | Serveri seisak või vähenenud jõudlus, teenu-se osutamise takistamine seaduslikele kasutajatele, võimalik tulude vähenemine, suuremad tegevuskulud [35], [38] liikluse korraldamiseks ja koormuse leevendamiseks.                          |
| 028 | Vahendusrünne [38], [34]. | Ohuagent kuulab pealt ja potentsiaalselt muudab kahe osapoole vahelist suhtlust ilma nende teadmata.   | Ebaturvalised või halvasti krüpteeritud sidekanalid [41], [34], nõrgad autentimisprotokollid [41], [34], lõppseadmete turvalisuse puudumine [34] ja vastuvõtlikkus DNS või ARP võltsimisele. | <b>RAMI 4.0:</b> vara ja kommunikatsiooni kihid.<br><b>Siht:</b> veebi- ja rakendusserverid, võrgu kommunikatsiooni-seadmed. | Edastatud andmete konfidentsiaalsus ja terviklus.      | Andmete rikkumine, mis hõlmab tundlikku teavet, volitamata juurdepääsu süsteemi mandaatidele, võimalikku manipuleerimist andmetega, mis toob kaasa ebaõiged otsused või toiminguid, kasutajate usalduse kaotuse ja mainekahju [35], [38]. |

|            |  |   |  |   |   |  |
|------------|--|---|--|---|---|--|
| <b>029</b> | Uhterünnak [38].                                       | Ohuagent suunab võrguliikluse ümber pahatahtliku sõlme (neeldaja) kaudu, mis võimaldab tal võrgu kaudu liikuvaid andmeid pealt kuulata, analüüsida või nendega manipuleerida. | Kompromiteeritud võrgu marsruutimisandmed, võrgu uuenduste nõrk autentimine [34], vastuvõtlikkus marsruutimisprotokollide rünnakutele ja ebapiisav võrgu seire.  | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> võrgu infrastruktuur.                     | Võrguliikluse terviklus ja konfidentsiaalsus. | Tundlike andmete pealt kuulamine ja ohustamine [34], võrguteenuste häirimine või halvemine, volitamata juurdepääs võrgusüsteemidele ja üldine võrguturbe kahjustumine.   |
| <b>030</b> | Barragerünnak (mitme ründevektori kombinatsioon) [38]. | Ohuagent käivitab koordineeritud rünnaku, kasutades samaaegselt või järjestikuseid erinevaid rünnakumeetodeid, mille eesmärk on alistada kaitse.                              | Ebapiisavad mitmekihilised kaitsemehhanismid, ohu reaalsajas tuvastamise ja reageerimise võimekuse puudumine, ebapiisav koolitus [41] ja valmisolek keerukateks rünnaku stsenaariumideks ning nõrk süsteemide vaheline side ja kontroll. | <b>RAMI 4.0:</b> funktsionaalne, Kommunikatsiooni ja varade kiht.<br><b>Siht:</b> kõik. | Äritegevuse käideldavus ja terviklus.         | Mitme süsteemi kiire ohustamine, suuremad raskused ohtude tuvastamisel ja leevendamisel, märkimisväärsed häired toimingutes, võimalikud andmekaitse rikkumised ning märkimisväärne kahju organisatsiooni mainele ja usaldusele [35], [38]. |

|            |  |   |   |  |  |   |
|------------|--|---|---|--|--|---|
| <b>031</b> | Tarkvara või riistavara pöördprojekteerimine [34]. | Ohuagent analüüsib tarkvara või riistvara, et mõista selle ülesehitust, funktsionaalsust ja võimalikke nõrkusi.   | Kaitsevahendid pöördprojekteerimise vastu on ebapiisavad, näiteks tarkvara varjutamistehnikad [34], ja riistvara füüsilised turvameetmed.         | <b>RAMI 4.0:</b> funktsionaalne ja varade kiht.<br><b>Siht:</b> tarkvara rakendused, püsivara, riistvara.    | Intellektuaalomand.                            | Toodete loata kopeerimine või muutmine, konkurentsieelise õõnestamine, võimalikud turvarikumised, mis põhinevad avastatud nõrkustel, ning turuosa ja kaubamärgi terviklikkuse vähenemine. |
| <b>032</b> | Jõurünne [34].                                     | Ohuagent kasutab automatiseeritud meetodeid, et süstemaatiliselt proovida paroolide või krüpteerimisvõtmete kombinatsioone, kuni leitakse mõni, mis võimaldab volitamata juurdepääsu. | Nõrgad parooli poliitika [41], konto lukustusmehhanismide puudumine, ebapiisav krüpteerimise tugevus [41], autentimiskatsete ebapiisav jälgimine. | <b>RAMI 4.0:</b> funktsionaalne ja äri kiht.<br><b>Siht:</b> autentimissüsteemid, kasutajakontode andmebaas. | Andmete konfidentsiaalsus, süsteemi terviklus. | Loata juurdepääs tundlikele süsteemidele ja andmetele, võimalus edasiseks pahatahtlikuks tegevuseks.  |

|     |                       |   |  |   |   |   |
|-----|-----------------------|---|--|---|---|---|
| 033 | Võrgu nuhkimine [34]. | Ohuagent kasutab pakettide nuhkimise vahendeid võrguliikluse pealtkuulamiseks ja analüüsimiseks, eesmärgiga hõivata tundlikku teavet, näiteks paroole, sessiooni tunnuseid või võrgu kaudu edastatavaid konfidentsiaalseid andmeid. | Krüpteerimata võrguliiklus [41], nõrgad võrgu seaded [34], võrgu seire ja sisestungi tuvastussüsteemide puudumine ning turvamata juhtmeta võrguühendused.        | <b>RAMI 4.0:</b> kommunikatsiooni kiht.<br><b>Siht:</b> võrgu infrastruktuur. | Andmete konfidentsiaalsus, sidevõrgu terviklus  | Tundliku teabe avalikustamine, võimalikud hilisemad sihitud rünnakud, võrgu turvalisuse õõnestamine ning organisatsiooni maine ja usalduse kahjustamine [35], [38]                    |
| 034 | Taasesitusrünne [34]. | Ohuagent püüab kehtivate andmete edastamist (nt autentimise tunnused) ja edastab need uuesti, et saada volitamata juurdepääs või sooritada tehing pettuse teel.   | Järjenumbrate või ajatemplite puudumine või ebapiisav sideprotokollides implementeerimine [41], [34], ebapiisavad krüpteerimismehhanismid ja nõrk seansi haldus. | <b>RAMI 4.0:</b> kommunikatsiooni kiht.<br><b>Siht:</b> võrgu infrastruktuur. | Andmete konfidentsiaalsus, sidevõrgu terviklus. | Volitamata juurdepääs süsteemidele või andmetele, petturlike tehingute tegemine, turvaliste sidekanalite kahjustamine ning kasutajate ja sidusrühmade usalduse vähenemine [35], [38]. |

|     |                                     |  |   |   |   |   |
|-----|-------------------------------------|--|---|---|---|---|
| 035 | IP aadresside võltsimine [34].      | Ohuagent maskeerib end seaduslikuks kasutajaks või seadmeks, võltsides IP-aadressi teavet oma võrgupaketites, eesmärgiga mööda minna IP-põhistest turvameetmetest, kehastades teisi seadmeid või viies läbi peegeldatud rünnaku. | Võrgu autentimisprotokollide puudumine [41], [34], ebapiisav pakettide filtreerimine, nõrk võrgu seadistus ja ebapiisav võrguliikluse jälgimine kõrvalekallete suhtes.                      | <b>RAMI 4.0:</b> kommunikatsiooni kiht.<br><b>Siht:</b> võrgu infrastruktuur.         | Andmete konfidentsiaalsus, sidevõrgu terviklus. | Volitamata juurdepääs võrgu ressursidele, teenuste häirimine, võimalikud edasised võrgu põhised rünnakud, andmete tervikluse kahjustamine ja organisatsiooni maine kahjustamine [35], [38].                                   |
| 036 | Andmete manipuleerimine [34], [34]. | Ohuagent muudab süsteemis või transiidis olevaid kriitilisi andmeid, eesmärgiga rikkuda teavet, õõnestada otsustusprotsesse või saada rahalist kasu.   | Ebapiisav andmete tervikluse kontroll, tugeva juurdepääsu kontrolli puudumine, andmete nõrk krüpteerimine transiidi ajal [41], [34], andmete muutuste ebapiisav kontrollimine ja jälgimine. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> andmebaasid, faili hoiustamissüsteemid. | Andmete terviklus ja käideldavus.               | Muudetud andmete põhjal tehtud ebaõiged otsused, usalduse vähenemine andmete usaldusväärsuse suhtes, manipuleeritud andmetest tulenev finantskahju (nt finantstehingutes), võimalikud õiguslikud ja regulatiivsed tagajärjed. |

|     |                     |   |  |   |  |  |
|-----|---------------------|---|--|---|--|--|
| 037 | Õngitsus [34].      | Ohuagent petab kasutajaid, et nad paljastaksid tundlikku teavet, näiteks sisse logimise andmeid või isiklike andmeid, maskeerudes digitaalses suhtluses usaldusväärseks üksuseks. | Kasutajate teadlikkuse ja koolituse puudumine [41], ebapiisavad e-posti filtreerimise- ja turvameetmed, ebapiisavad digitaalsuhtluse kontrollmehhanismid [34].                                   | <b>RAMI 4.0:</b> äri ja kommunikatsiooni kihid.<br><b>Siht:</b> e-posti süsteemid, kasutaja seadmed, interneti sirvi-<br>jad. | Andmete konfidentsiaalsus.                           | Volitamata juurdepääs kontodele ja tundlikele andmetele, võimalikud edasised turvarikkumised, pettusest või andmevargusest tulenev rahaline kahju, organisatsiooni maine kahjustamine [35], [38], ja usalduse vähenemine suhtluskanalite suhtes. |
| 038 | SQL süstimine [34]. | Ohuagent kasutab ära veebirakenduse andmebaasi päringutarkvara nõrkust, sisestades pahatahtlikku SQL-koodi.   | Ebapiisav sisendi valideerimine, ettevalmistatud avalduste või parameetriga päringute puudumine andmebaasi interaktsioonis, ebapiisav kasutaja sisendi puhastamine ja nõrk andmebaasi seadistus. | <b>RAMI 4.0:</b> informatsiooni kiht.<br><b>Siht:</b> veebirakenduste serverid, andmebaasid.                                  | Andmete terviklus, konfidentsiaalsus ja käideldavus. | Volitamata juurdepääs tundlikele andmetele, andmebaasi võimalik rikkumine või kadumine, privaatse teabe avalikustamine, andmete tervikluse kadumine, õiguslikud ja nõuetele vastavuse probleemid ning organisatsiooni maine kahjustamine.        |

|     |                        |   |  |  |                            |  |
|-----|------------------------|---|--|--|----------------------------|--|
| 039 | DNS pete [34].         | Ohuagent rikub DNS (domeenini-mede süsteemi) vahemälu vale teabega, suunates kasutajaid nende teadmata pahatahtlikele veebilehtedele või serveritele.   | DNS-serverite nõrgad turvameetmed, DNS-päringute valideerimise puudumine, vananenud või parandamata DNS-tarkvara ja ebapiisavad võrgu turvaprotokollid [34], [34].   | <b>RAMI 4.0:</b> kommunikatsiooni kiht.<br><b>Siht:</b> võrgu infrastruktuur.      | Veebiliikluse terviklus.   | Kasutajad suunatakse teadmatult pettuse veebilehtedele, mis viib andmepüügi rünnakute või pahavaraga nakatumiseni, tundliku teabe ohustamiseni, seadusliku veebiliikluse katkestamiseni ja organisatsiooni usaldusväärsuse võimaliku kahjustamiseni. |
| 040 | Külgkanali rünne [34]. | Ohuagent kasutab ära krüptosüsteemi füüsilist raketamist, näiteks ajastusandmeid, energiatarbimist, elektromagnetilisi lekkeid või isegi heli, et saada teavet aluseks olevate andmete või krüptograafiliste võtmete kohta. | Krüptosüsteemid, mis ei ole kavandatud füüsilise lekke vastu, riistvara ebapiisav varjestus, andmeoperatsioonide müra puudumine ja kriitilistele süsteemidele füüsilise juurdepääsu ebapiisav järelevalve. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> krüptograafilised seadmed, serverid. | Andmete konfidentsiaalsus. | Krüptograafilise teabe kahjustamine, mis toob kaasa andmete rikkumise, andmete krüpteerimistavade õõnestamise, tundliku teabe võimaliku paljastamise ja usalduse kaotamise turvameetmete vastu.  |

|            |                                   |   |   |   |   |   |
|------------|-----------------------------------|---|---|---|---|---|
| <b>041</b> | Paroolirünne [34].                | Ohuagent üritab saada volitamata juurdepääsu süsteemidele või andmetele kasutajate paroolide murdmise või äraarvamise teel.   | Nõrgad kasutajate parooli poliitika [41]), [38], [34], mitmefaktorilise autentimise puudumine, ebapiisav kasutajate koolitus [41] turvaliste paroolide kasutamise osas ja ebapiisavad kontode lukustusmehhanismid.                              | <b>RAMI 4.0:</b> funktsionaalne ja varade kiht.<br><b>Siht:</b> kasutaja kontod.  | Andmete konfidentsiaalsus ja terviklus.     | Volitamata juurdepääs kriitilistele süsteemidele ja andmetele, võimalus edasiseks pahatahtlikuks tegevuseks võrgus, kasutajate volituste kahjustamine, tööhäired ja organisatsiooni maine kahjustamine. |
| <b>042</b> | Operatiivne manipuleerimine [34]. | Ohuagent saavutab kontrolli operatsioonisüsteemide üle või muudab nende seadeid, mille tulemuseks on ebaõiged toimingud, protsesside häirimine või seadmete füüsilise kahjustamine. | Ebapiisavad juurdepääsukontrollid operatiivsüsteemidele, süsteemi toimingute järelevalve ja hoiatusteadete puudumine, ebapiisav eraldatus IT- ja operatsioonitehnoloogia (OT) võrkude vahel ning nõrgad autentimismehhanismid [41], [38], [34]. | <b>RAMI 4.0:</b> varade kiht.<br><b>Siht:</b> tööstuslikud juhtimissüsteemid (ICS), programmeeritavad loogikakontrollerid (PLC), SCADA süsteemid. | Tööprotsesside terviklus, personali ohutus. | Tööprotsesside katkemine, seadmete või infrastruktuuri võimalik füüsiline kahjustamine, töötajate ohutusriskid, tööseisakud ja rahaline kahju [35], [38].   |

|            |                |   |  |  |                                   |  |
|------------|----------------|---|--|--|-----------------------------------|--|
| <b>043</b> | Lunavara [34]. | Ohuagent krüpteerib organisatsiooni andmed või süsteemid ja nõuab tasu andmete dekrüpteerimise eest, takistades juurdepääsu andmetele ja takistades toiminguid. | Ebapiisav lõppseadmete turvalisus [34], andmete regulaarse varundamise puudumine, töötajate ebapiisav väljaõpe [41] pahavara ohtude, e-posti ja veebi turvalisuse põhimõtete ning uuendamata süsteemide kohta. | <b>RAMI 4.0:</b> vara ja informatsiooni kihid.<br><b>Siht:</b> andmete hoidmissüsteemid, lõppkasutajate seadmed, serverid. | Andmete terviklus ja käideldavus. | Juurdepääsu kaotamine kriitilistele andmetele ja süsteemidele, tööseisak, võimalikud andmekaitse rikkumised, rahaline kahju lunaraha maksmise ja taastamispüüdluste tõttu ning maine kahjustamine. |
|------------|----------------|---|--|--|-----------------------------------|--|