TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anto Veldre, 175103IDSR

Eesti infoturbestandardi protsessimudeli evalveerimine

Diplomitöö

Juhendaja: Kristjan Karmo
MBA

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Anto Veldre

17.05.2021

Annotatsioon

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 49 leheküljel 8 jaotises. Töö põhiosas on 7 joonist ja 4 tabelit, lisades on kokku 10 joonist. Töö sisaldab nii infosüsteemi analüüsi kui ka uurimustöö elemente. Lõputöö uurimisobjekt on Eesti infoturbestandard (E-ITS), mis on rakendamiseks kohustuslik paljudele avaliku sektori asutustele. Käsitlusalaks on standardi kaks olulist juhendit – "ISMS nõuded" ja "Rakendusjuhend". Töö vaatleb standardi juhiseid asutusele kohustusliku infoturbealase meta-äriprotsessina ning uurib selle äriprotsessi mudelit. Töö käigus analüüsisin etalonturvet puudutavaid materjale ning eelnevaid teadustöid. Äriprotsessi mudeli koostasin kahes erinevas notatsioonis (BPMN ja FRAM). Analüüsisin mudelit ning dokumenteerisin mudelist tulenevad järeldused 22 leiu kujul. Mudeli ja leidude põhjal sõnastasin soovitused standardi omanikule. Esitasin arutlused võimaliku ISMS tööriista kohta ning standardi majandusliku ja korraldusliku optimeerimise teemadel. Töö illustreerib uudse FRAM metoodika kasutusvõimalusi infosüsteemide ja infoturbe valdkonnas.

Abstract

Evaluation of a Process Model of the Estonian Information Security Standard

The thesis is in the Estonian language and contains 49 pages of body text, 7 figures and 4 tables in 8 chapters. Addenda contain 10 more figures. The thesis offers both research as well as elements of information systems analysis. The thesis deals with the correctness of the procedures described in the new Estonian InfoSec Standard (E-ITS, 2021), describes the known issues of the previous standard - ISKE, and then analyses the concept of a supporting tool from the information systems viewpoint. The scope is limited to the two pivotal manuals, ISMS Requirements and Implementation Guide, which are the structural equivalents of the BSI 200-1 and 200-2 standards from BSI IT-Grundschutz (The Baseline Protection Manual) offered by BSI (*Federal Office for Information Security, Germany*).

The author created own models based on the full-text descriptions of the processes in the Standard and analysed these in detail. To discover the possible irregularities, two distinct notions are used, BPMN and FRAM. The suitability of the FRAM notation is discussed in regard of certain parts of the model. An ERD concept model for the domain is proposed. 22 findings were raised as a result of holistic analysis of the model. Improvements compared to the ISKE are documented. Recommentations are given that the owner of the Standard can rely on, during the next iterations of the Standard. Useful background information is presented that the interested implementers can make use of.

Earlier models from the author are referenced in Addendum 1. A short Estonian language description of the FRAM (Functional Resonance Analysis Method) is offered as Addendum 2, to compensate the fact the method is not yet widely known in Estonia.

Sisukord

Jooniste loetelu

Tabelite loetelu

Lühendite ja mõistete sõnastik

BSI IT Grundschutz	Saksa Liidumaa infoturbeinstituudi (BSI) poolt välja töötatud etalonturbe raamistik, on aluseks nii ISKEle kui E-ITSile. Sisaldab mh standardeid BSI 200-1 ja BSI 200-2
BPR	*business process re-engineering* – äriprotsesside parendamine v ümberkorraldamine
E-ITS	Eesti infoturbestandard (põhineb etalonturbel, asendab ISKE)
emergents	(*emergence*) – teravalt silmapaistev olukord, kus olem ilmutab omadusi, mida pole tema ühelgi osal ning mis ilmnevad üksnes nende osade koosmõjul
ERD	*entity relation diagram*, olemi-suhte diagramm
etalonturve	Etalonturve on keskselt ettevalmistatud tüpiseeritud turva-meetmestik, mis rakendatakse varadele (sihtobjektidele), eesmärgiga saavutada vajalik tüüpne turvatase saavutamiseks ja säilitada seda
FISC	(*Center for Financial Industry Information Systems*) – finantsala infoturbeamet ja selle infoturbestandard Jaapanis
FRAM	*Functional Resonance Analysis Method* – prof Erik Hollnageli poolt välja töötatud analüüsimeetod (ja notatsioon) õnnetuste ja intsidentide uurimiseks ning riskide tuvastamiseks
Informationsverbund	Saksakeelne vaste asutuse kõigi infosüsteemide kogumile, nö superinfosüsteemile. E-ITS terminoloogias: kaitseala
ISKE	„Infosüsteemide kolmeastmeline etalonturve" – Eestis seni kehtinud infoturberaamistik (standard)
ISMS	Information Security Management System – infoturbe halduse süsteem
kaitseala	Turvapoliitika käsitlusala, mille ulatuses rakendatakse turvameetmed
kohaldusmäärang	*statement of applicability* (SOA), ISO 27001 sõnavara kohaselt 114 üldsõnalist meedet sisaldav Lisa A, sisuliselt ülemise taseme kontrollnimekiri
lateraalne	Küberkaitses tähistab lateraalne küberohu horisontaal-liikumist kaitstavate süsteemide vahel. Süsteemidünaamikas ja küberneetikas tähisatab lateraalne kõrvalekaldumist rangelt korraldatud mõtteviisist.

MFN	Mittefunktsionaalsed nõuded (NFR – *non-functional requirements*)
RIA	Riigi Infosüsteemi Amet
RUP	*Rational Unified Process*, Rationali unifitseeritud protsess tarkvaraarenduses
sihtobjekt	(*das Zielobjekt*) E-ITS uustermin varade tähistamiseks. E-ITS meede rakendub ühele või mitmele sihtobjektile.
SOA	(*statement of applicability*) – kohaldusmäärang. ISO 27000 definitsioon: dokumenteeritud deklaratsioon, mis kirjeldab organisatsiooni ISMS puhul asjakohaseid ja kohaldatavaid meetmete eesmärke ja meetmeid
sotsiotehniline süsteem	Süsteem, mis moodustub ühelt poolt tehnoloogiast ja teiselt poolt üksikinimestest (töötajatest) ja neist koosnevast organisatsioonist
STS	*socio-technical system* – sotsiotehniline süsteem.
tööriist	Täpsustamata funktsionaalsusega infosüsteem, mis pakub arvutituge ISMS, ISKE, E-ITS või etalonturbe protsesside evitamisel, käitamisel, vastavuskontrollil, auditeerimisel või sertifitseerimisel.
WAI	*work as imagined* - FRAM termin uue süsteemi kirjeldamisel
WAP	*work as performed* - FRAM termin olemasoleva süsteemi kirjeldamiseks

1 Sissejuhatus

Eestis algab peatselt üleminek etalonturbe süsteemilt ISKE Eesti Infoturbestandardile (E-ITS) [1] .

Majandus- ja kommunikatsiooniministeerium (MKM) on aastateks 2019–2022 vastu võtnud "Küberturvalisuse strateegia" [2] . Tegevussuund 1.1 "Tehnoloogilise vastupanuvõime tõhustamine" näeb ühe meetmena ette baasturvanõuete laiapindset rakendamist. Strateegia leheküljel 23 öeldakse: "Täna on endiselt probleemiks ISKE keerukus ning selle rakendamist hindavad eriti väiksemad kohuslased, sh kohalikud omavalitsused, ülejõukäivaks, eeskätt administratiivselt. Lisaks valitsusasutustele vajavad suuniseid ja tuge küberriskide haldamisel ning andmekaitse-ja infoturbenõuete täitmisel ka väikeettevõtjad, vabakond ja üksikisikud. Vajalikus ulatuses baasturbenõuete rakendatavuse tagamiseks on vaja riigi täiendavat tuge, et süsteemselt tagada lihtsa tööriista, juhendmaterjalide ja koolituste kättesaadavus. Sihiks on luua ajakohane, süsteemne ja laialt kasutusel olev baasturbenõuete süsteem, mis hõlmab nii infoturbe kui andmekaitse miinimumnõudeid.". Strateegia (lk 35) defineeritb mõõdikuna "ametlikult kinnitatud IKT turvapoliitika kasutamine ettevõtetes". Kui aastal 2015. aastal oli see tingimus täidetud enamal kui 16,9% ettevõtetest (v.a. mikroettevõtted), siis 2022. aastaks oodatakse näitaja suurenemist 25%-ni. Strateegia mainib ühe tähtsama eesmärgina, et infoturve peab muutuma riskipõhiseks. Terminoloogia korrastamist pole strateegias eraldi eesmärgina tõstatatud, kuid probleemi on tunnetatud ning alates lk 42 esitatakse ala võtmeterminid.

Septembris 2020 kiitis Eesti valitsus heaks infosüsteemide turvameetmete süsteemi määruse muutmise eelnõu [3] . Majandusministeeriumi pressiteade [4] teavitas, et on alanud ISKE asendamiseks mõeldud uue standardi loomine: "Kui seni pidid Eesti asutused riigi infosüsteemi kuuluvate andmekogude turvalisuse tagamiseks rakendama infosüsteemide kolmeastmelise etalonturbe[1] süsteemi, siis pärast muudatust on lubatud alternatiivina kasutada ka ISO/IEC 27001 standardit (edaspidi ISO standard)". Tänaseks

1 Töö autori märkus: selle all mõeldakse ISKEt, vt Jaotis 3.2

on E-ITS materjalid koostatud ning avaldatud asjakohases portaalis [1] . Üleminek ISKElt hakkab toimuma järk-järgult, tähtajad reguleeritakse seadusaktidega.

Ühena meeskonnaliikmetest osalesin Eesti Infoturbestandardi väljatöötamises (riigihange nr 203534 [5] juuni 2019 – jaanuar 2021). Tööde kirjelduse punkt 5.2 püstitas kvaliteedinõude: "Eesti olukorda ja vajadusi arvesse võttes kõikide tellija edastatavate materjalide läbi töötamine ja analüüsimine, kasutades selleks erinevate valdkondade parimat ekspertteadmist". Nõuete detailse spetsifikatsiooni asemel püstitas tööde kirjeldus järgmise eesmärgi: "[..] on mõistlik välja töötada Eesti oma infoturbestandard, mis asendab senist ISKE-t ja mis võimaldab kontrollitumat tuge ISO 27000 seeria vastavate standardite (nt 27001 ja/või 27002) nõuete rakendamisel ja vastavuse saavutamisel. Sarnastel põhimõtetel on BSI reforminud ka IT-Grundschutz standardit, mida on otstarbekas kasutada sisendina Eesti infoturbestandardi koostamisel."

1.1 Taust

Diplomitöö laad jääb infosüsteemide analüüsi ja uurimuse vahepeale. Kasutan kirjeldamisel mina-vormi, et eristada standardi loomise käigus kollektiivselt tehtut isiklikust panusest diplomitöös. Töö käigus avastatud ning lõppjärelduse seisukohast olulised faktid tähistan nummerdatud leidudena (näiteks **Leid 01**). Töö pealkirjas kasutatud termin "evalveerimine" tähendab "Eesti keele seletava sõnaraamatu" [7] kohaselt hindamist, väärtuse või hinna määramist ning seda tuleb eristada formaalsest verifitseerimisest. Töö on mahukas, kuivõrd selle käigus oli vaja süstematiseerida ja kõrvutada väga erinevaid valdkondi puudutavaid uurimusi.

1.2 Motivatsioon

Standardi loomise käigus hakkasin infoturbestandardit tajuma riikluse ja rahvuskultuuri seisukohast olulise verstapostina. Projekti vältel kogunes hulk teadmust, taustinfot, kaalutlusi ning ka lõpetamata ideid, mis ei mahtunud standardisse, kuid mille valdamine tähendab olulist ajavõitu nii E-ITS rakendajale kui ka edasiarendajale. Projekti lõpus tundsin soovi ja kohustust akumuleeritud teadmiste edasiandmiseks ja -arendamiseks.

Infosüsteemide analüüsi erialal õpitu koos varasema spetsialiseerumisega infoturbele lõi võimaluse standardi keskseid teemasid edasi käsitleda. Himanen oma raamatu [6] esimeses osas "Tööeetika" tunneb imetlust selle üle, kui võimas jõud on protestantlik tööeetika. Soovin, et standardi rakendaja Himaneni järgijana ei piirduks küsimusega “mida pean tegema?”, vaid esitaks kohe ka järgmise küsimuse “miks ma seda teen?”.

E-ITSi juhendite kirjutamist raskendas olukord, kus protsessi alusmõisted ei olnud üheselt defineeritud. Kahes võõrkeeles täistekstina esitatud ning toortõlgitud protsessi-kirjeldus ei andnud mulle kui analüütikule selget arusaama protsessi detailidest ja otsustuskohtade täpsetest kriteeriumitest. Juhendite protsesse ühte üldvaatesse koondades põrkusin mõistete ontoloogias esineva ühestamatusega ning keerukusega protsessi osade hierarhilisel liigitamisel. Pärast projekti lõppemist on mul tekkinud võimalus märgatud probleeme edasi uurida.

Töö kajastab minu isiklikke seisukohti, mis ei pruugi ühtida standardi omaniku, Riigi Infosüsteemi Ameti (RIA) seisukohtadega. Olen teinud jõupingutusi, et töös esitatud materjal, faktid ja väited oleksid võimalikult täpsed. Mõned esialgsed faktivead, mis selgusid minu ja RIA vahelises suhtluses, on lõppversioonis parandatud. RIA on andnud nõusoleku töös kasutada riigihanke täitmise käigus loodud, kuid standardi koosseisu mitte jõudnud mudelimustandeid ning loetleda standardi loomisel lahendatud küsimusi (vt jaotis 3.3) märkusega, et RIA nõusolek selle teabe kasutamiseks ei tähenda RIA nõustumist diplomitöös sisalduvate väidetega.

1.3 Uurimisobjekt

Töö uurimisobjektiks on Eesti infoturbestandardi protsessi mudel. Eksisteerivad kaalukad põhjused Eesti infoturbestandardi protsesside analüüsiks. Teema on oluline ja innovatiivne, avalik sektor paneb standardi kasutuselevõtule suuri ootusi. Standardi kohuslaste[1] arvu hinnatakse sadadesse. Kindlasti vajab standardi sisu levitamist, edasiarendamist ja sügavamat analüüsi.

1 Praktikas jaotuvad E-ITS kohuslased kahte suurde gruppi (jaotuskõveral on kaks tõusu, üks kummaski servas) – väike kogus võimekaid IT maju, ministeeriume ja X-teel keskset teenust pakkuvaid organisatsioone vs suur kogus oluliselt vähem võimekaid väikerakendajaid.

Töö eesmärgiks on täiendada standardi osapoolte senist teadmust vaikimisi (*default*) eelduste osas, kuivõrd need ei pruugi tegelikkuses kehtida, samuti senisest täpsemini tuvastada standardi protsesside potentsiaalselt masintoetatavad osad. Veel on eesmärgiks anda avalikult edasi teadmust, mis hõlbustaks tõhusa tööriista teket. Kogueesmärgiks on soodustada Eesti infoturbestandardi kiiret ja efektiivset rakendamist ning ühtlasi selle edasist täiustamist.

Etalonturbe standardi avalikult kättesaadavat formaalset mudelit ei eksisteerinud teadaolevalt ei Grundschutzi, ISKE ega E-ITSi osas. Tegevussoovitused ja juhised olid varem väljendatud vaid täisteksti kujul. Eesmärkide saavutamise eeldusena tuleb mul seega kõigepealt koostada infoturbestandardi rakendusprotsessi formaalne mudel – kirjeldada tegevusjärgnevusi, mida rakendaja peab standardi rakendamiseks sooritama – ning seejärel analüüsida mudelit standardi järgmise iteratsiooni täiustamise eesmärgil. Analüüsi käigus uurin standardi protsesside korrektsust ning tuvastan võimalikud loogikavead, nii need vähetõenäolised, mis on sinna pärandunud BSI IT Grundschutzi protsessidest kui ka need, mis võivad olla tekkinud kohandamise tulemusel.

Mudel koondab kahe E-ITS juhise – ISMS nõuete [12] ja rakendusjuhendi [13] – korraldused. Riskihaldusjuhendi [14] puhul vaatlen vaid liidestust sellega, protsesse käsitlemata. Mudelis kirjeldan vaid protsessi neid osi, mis on kõigile asutustele ühised. Vaatluse alt jäävad välja asutuse äriprotsessid ja varade kooslus (kui olemuselt unikaalsed) ning neist tulenev konkreetne meetmevalik etalonturbe kataloogist.

Ülesande lahendamise käigus valin modelleerimisvahendid, loon mudeli, analüüsin seda ning kirjeldan analüüsist koorunud soovitused. Diplomitöö maht piirab analüüsi vaid ülesande kõige olulisemate tahkudega. Ülesande täielikku keerukust võimaldab hinnata ISKE tööriista rahvusvahelist piirmäära ületava hanke ebaõnnestumine 2017. a., kui pakkumusi ei esitatudki.

Töö uurimisobjektiks on **Mudel 01** (Joonis 1), mille eelnevalt koostasin etalonturbe raamistiku täisteksti põhjal ning mida oma töös tõlgendan. Minu kui analüütiku teekond analüüsitava alusmudelini on kirjeldatud Lisas 1. Selline lähenemine sisaldab subjektiivsuse riske. Mudel sõltub analüütiku võimest täisteksti mõista, pädevusest mustrite tuvastamisel ning lõpuks, analüütiku subjektiivsest tõlgendusest iseenda

mudelile. Akadeemilisuse nõue toob kaasa vajaduse materjali töötlemisel kasutada aktsepteeritud metoodikaid. Metoodika valiku küsimusi käsitletakse Jaotises 4.

1.3.1 Uurimisküsimused

Uurimisküsimuste püstitamisel arvestan järgmist taustinfot.

(a) Standardi etalonturbemeetod pärineb ISKEga samast algallikast – BSI IT Grundschutz [8] . ISKE ja E-ITS käsitluse erinevused seletuvad BSI etalonturbe-meetodi pideva täiustumisega ning lokaalsete muudatuste ja täienduste olemasoluga etalonturbe Eesti versioonis.

(b) Eksisteerib visioon "etalonturbe tööriistast". Tööriista all mõistan tugisüsteemi, mis toetab infoturberaamistiku või infoturbestandardi praktilist rakendamist asutuses. BSI esitab nimekirja [9] ühest riiklikust ning kümnetest kommertsiaalsetest IT Grundschutzi rakendamise tööriistadest. RIA on korduvalt läbi viinud "ISKE tööriista" hankeid, millest osad (aastatel 2007, 2015 [10] ja 2017 [11]) ebaõnnestusid. Küberturvalisuse strateegia (lk 23) nõuab "riigi [..] tuge, et süsteemselt tagada lihtsa tööriista [..] kättesaadavus". Tööriista võimaliku disaini kohta on tehtud ettepanekuid magistri- ja doktoriväitekirjades.

Töö käigus otsin vastuseid järgmistele uurimisküsimustele:

UK1 – millised on olnud teadaolevad probleemid ISKE (kui E-ITS eellase) rakendamisel;

UK2 – kas E-ITS tegevustiku juhised ja korraldused moodustavad korrektse ning omavahel seotud süsteemi;

UK3 – millised nõuded tuleb esitada E-ITS tööriistale.

Püstitasin järgmised uurimishüpoteesid:

UH1 – standardi rakendamisel väikeasutuses[1] kulub aega ja ressursse otstarbekalt;

1 väikeasutus - vähem kui 50 töötajaga asutus. Analoogia mikro- või väikeettevõttega (MVE) – vastavalt 9 või vähem töötajat vs 10-49 töötajat.

UH2 – standardi rakendamise protsess on sisemiselt konsistentne, selles pole loogikavigu, rahuldamata sõltuvusi ega dokumenteerimata eeldusi;

UH3 – standardi protsessi keerukus pole ülemäärane.

1.4 Ülevaade töö jaotistest

Jaotises 1 "Sissejuhatus" kirjeldan asjaolusid, mis viisid diplomitöö teema valikuni, samuti piiranguid, motivatsiooni ja töö ülesehitust. Määratlesin uurimisobjekti, püstitasin uurimishüpoteesid ja uurimisküsimused.

Jaotises 2 "Ülevaade kaasaegse infoturbe probleemidest" kirjeldan küberturbeohtusid ja nende levikut tänapäeva maailmas. Keskendun seisukohale, et globaalvõrgus Internet on turvaline ja ohutu tegutseda üksnes juhul, kui kasutaja järgib väga ulatuslikku komplekti infoturbesoovitusi, eelistatult mõnda infoturbestandardit.

Jaotises 3 "Infoturberaamistikud. Etalonturve." annan lühikese ülevaate infoturbe-standarditest ning keskendun seejärel etalonturbele. Vaatlen etalonturbe raamistikke IT Grundschutz, ISKE ja E-ITS.

Jaotises 4 "Meetodi valikuprotsess" kirjeldan oma esialgset valikut notatsiooni ning analüüsimetoodika osas. Valisin välja Eestis suhteliselt tundmatu FRAM-metoodika, mida kirjeldan Lisas 2.

Jaotises 5 "Töö käik (süntees)" kirjeldan mudeli järjestikust arendamist. Töö käigus selgub, et eeldused FRAM metoodika kasutamise osas ei olnud realistlikud. Küll aga võimaldasid FRAM-mudeli olemuslikud eelised mul mõista protsessimudeli keerukuse allikat ning näitasid teed keerukuse ületamiseks.

Jaotises 6 "Tulemused / Järeldused" kirjeldan töö tulemusi võrrelduna lähteülesandega.

Jaotises 7 "Soovitused" esitan soovitused, mis hõlbustavad standardi omanikul ja teistel huvipooltel (*stakeholders*) edasist arendust ning ülesande koostamist seonduva tööriista väljatöötlusele.

Jaotises 8 "Kokkuvõte" esitan lühikokkuvõtte diplomitööst.

Lisas 1 esitan minu poolt standardi valmimise vältel konstrueeritud mudelid ning mudelitega kaasnevad mõttekäigud.

Lisas 2 esitan lühiülevaate FRAM meetodist, kuivõrd töö tugineb FRAM meetodile olulisel määral ning meetod ise oli seni eesti keeles kirjeldamata.

2 Ülevaade kaasaegse infoturbe probleemidest

Töös analüüsin standardi protsesse abstraktse avaliku sektori organisatsiooni, E-ITS kohuslase vaatepunktist. Praktikuna olen märganud, et infoturvanõudeid alahinnatakse vaatamata tugevale vajadusele (vt nt *RUP security extension* [15]). Olen näinud, kuidas infoturvanõuded taandatakse mittefunktsionaalseteks nõueteks (MFN), mis aga näiteks *Open Security Architecture* initsiatiivi [16] liigituse järgi on kõigest üks neljast turva-nõuete tüübist. Minu kogemusel peatab turvanõuete mittearvestamine või mittejärgimine infosüsteemi funktsioneerimise sama edukalt kui eksimus süsteemi funktsionaalse osa analüüsis või teostuses.

Minu vaade infoturbest on oluliselt laiem kui ühe asutuse üks infosüsteem. Asutuse infosüsteemide kogum moodustab omavahel tihedalt ühendatud terviku, seda nii sünergia kui andmevahetuse seisukohast. Negatiivne mõjur (nagu küberoht), mis suudab infosüsteemi töö peatada, on sageli lateraalne ning suudab liikuda süsteemide vahel. Enamikes organisatsioonides käitatakse sisemisi universaalteenuseid (andmebaas, failitalletus), millele toetuvad praktiliselt kõik infosüsteemid. Ilmselt just seetõttu käsitleb IT Grundschutz organisatsiooni Infosüsteemi[1] ühtse suure tervikuna ning mitte eraldiseisvate infosüsteemidena. Niisugune püstitus osutab, et kuigi ühe infosüsteemiga piirduv turva-analüüs on jätkuvalt vajalik, ei ole see enam piisav.

Eesti infoturbestandardi tiimina sõnastasime me eraldi väärtusena BSI IT Grundschutzi ühe alusmõtte, et olukorras, kus enamik organisatsioone kasutavad ühetaolist standardtarkvara, tarbivad ühetaolist Internetti, milles enamik ohtusid polegi organisatsioonispetsiifilised, vaid on samuti ühetaolised, sellises olukorras saavad ühetaolised olla ka meetmed, millega neid ohtusid erinevates organisatsioonides tõrjutakse. Selline alusmõte loob hea teoreetilise aluse etalonturbe süsteemidele üldse. Lisaks aga, ning see on käesoleva diplomitöö seisukohalt oluline, võimaldab kirjeldatud mõttekäik infoturvaanalüüsi teatud määral üldistada, muuta seda geneerilise(ma)ks ning osas, mis ei puuduta konkreetse ettevõtte spetsiifilisi äririske, ka universaalse(ma)ks.

1 Infosüsteem suure algustähega vastena saksakeelsele terminile *der Informationsverbund.*

Oma töös vaatlen standardit informatsioonisüsteemi-ülese metaäriprotsessina, mis korraldab avaliku sektori asutuse infoturvet. Sellest vaatepunktist kujutab töö endast eeltööd standardi äriprotsessi uuendamisele (BPR – *business process re-engineering*). Teine võimalik vaatepunkt on standardi käsitlemine äriprotsessi sõnalise kirjeldusena - sellest vaatenurgast saan oma töös esitada eelanalüüsi seda äriprotsessi toetavale IT-vahendile, nn tööriistale.

2.1 Sotsio-tehnilised süsteemid

ITU oma veebiartiklis [17] refereerib fakti, et Eesti paikneb globaalses küberturbe-indeksis viiendal kohal. Tasakaalustatud teaduslikku selgitust Eesti küberedule on mõnevõrra raskem leida.

Tar oma doktoriväitekirjas [18] (alates lk 52) säärase tasakaalustatud käsitluse esitab, loetledes üleüldise küberturvalisuse saavutamise võtmetegurid – proaktiivne turvakultuur, turvapoliitika olemasolu, sisekontrolli olemasolu, isiklikud väärtused ja uskumused ning veel ka turvakoolitus. Tar (lk 67) kirjeldab Fred Emery ja Eric Tristi poolt 1960-ndatel püstitatud sotsiotehniliste süsteemide teooriat ning toob sisse kübervaldkonna uurimustes haruldase sotsiotehnilise süsteemi mõiste. Tari käsitluse eeliseks kohaliku küberteaduse ees on asjaolu, et universaalsetele järeldustele on tuldud ilma Eesti-spetsiifiliste argumentideta.

Hollnagel [19] vaatleb sotsiotehnilisi süsteeme teistsuguse nurga alt, hinnates olemasolevate metoodikate võimekust sääraseid süsteeme kirjeldada. Hollnagel pakub kasutamiseks välja uudse FRAM metoodika, mis on võimeline korraga arvesse võtma sotsiotehnilise protsessi mõlema osapoole (nii masinate kui inimeste) tugevaid ja nõrku külgi. Metoodika on varustatud kaasneva modelleerimistarkvaraga.

Leian, et Hollnageli FRAM suudab pakkuda täiendust või alternatiivi klassikalistele protsessikäsitlustele, näiteks lahendada kitsikusi, mis mul analüütikuna tekkisid IT Grundschutzi protsesside kirjeldamisel.

3 Infoturberaamistikud. Etalonturve.

Infoturbelahendusi saab jagada reaktiivseteks (sündmusjuhitud kaitse) ja proaktiivseteks (valmistumine). Kõige efektiivsemad on lahendused, mis sisaldavad mõlema lähenemise kombinatsiooni. Toimivatel infoturbestandarditel ja -raamistikel (ISO/IEC 27001 [20] , FISC [21] , BSI IT Grundschutz [8] , ISKE[1] [22]) sisaldub nõuetes järelkontrolli kohustus – seda kas auditeerimise või sertifitseerimise kaudu, ning ühtlasi kohustus ümbritsevat olukorda pidevalt seirata. Kvaliteedisüsteemidele omaselt on infoturbestandardid tagasisidestatud, mistõttu suudavad reaalajalähedaselt arvesse võtta ümbritseva keskkonna muutusi – infoturbe haldussüsteemi (ISMS – *information security management system*) abil. Tegelikkuses eksisteerib oluliselt rohkem infoturberaamistikke (nt COBIT, HIPAA, PCI DSS, ka ITIL-i mõned osad), neid ma ei vaatle.

Tänapäeva maailma liiderkultuuriks on kujunenud anglo-ameerika ärikultuur. Infoturbes on viimase 10 aasta jooksul omandanud olulise tähenduse standard ISO/IEC 27001 koos selle aluseks oleva kahjukeskse lähenemise ning riskipõhise mõtlemisega. Saksamaal ja Eestis on populaarsust kogunud etalonturve. E-ITS Lühijuhend [1] selgitab etalonturbe tähendust: "tüüpjuhtude riskianalüüs on juba ette keskselt ära tehtud standardi koostaja poolt. Riskide vähendamiseks pakutakse standardi rakendajale valmis tüüpmeetmed, mis paiknevad etalonturbe kataloogis."

Hea infoturbestandard eeldab väljatöötlust ulatuses, mida iseloomustavad suurusjärgud kümneid tuhandeid töötunde ning kümneid miljoneid eurosid. See selgitab Eesti ees seisvat probleemi – väikeriik ei ole originaalväljatöötluseks võimeline. Teiseks oluliseks kriteeriumiks on erinevused rahvuskultuuris ja -tavades ning keeleregistris [23] . Infoturbestandardid erinevad oma suunitluse, sügavuse, lähenemisnurga ja kõnetamis-viisi poolest. Eestis alles harjutakse mõttega, et inglise või saksa keelest materjale tõlkides ei osutu tekst sihtgrupile arusaadavaks põhjusel, et vastavad grammatilised konstruktsioonid pole ülekantavad; et kasutatud oskussõnade tähendusväli on

1 ISKEt ning selle alust – BSI IT Grundschutzi - saab olemuselt lugeda infoturbestandarditeks.

teistsugune või nagu selgitab Lyubymova jt uurimus ([24] , lk 7, loetelu), "puudub vastavat keelekihti kasutav sotsiaalne grupp". Sisu ülekandmisel võõrast ärikultuurist esineb ka kultuurilisi raskusi. Kui valdavalt protestantlik saksa töökultuur eeldab BSI IT Grundschutzi tuhandeid täpseid ja detailseid juhiseid, siis anglo-ameerika turvakultuur eeldab lühikest ja abstraktset kogumit ülemise taseme metanõuetest, milleks nt ISO/IEC 27001 puhul on selle Lisa A - 114 ühiku pikkune kohaldusmäärang. Terminoloogilist ühtsust ja tõlkekvaliteeti võib lähenemiskultuuri lõhe kõrval lugeda juba pisiprobleemiks. Nii näiteks avastasin, et tõlgitud ministandardite "US-CCU küberturbe kontroll-küsimustik" [25] ja "CIS-meetmed" [26] tõlkekvaliteet on madal ja kohati takistab sisu mõistmist.

Leid 01[1]: eesti keelde tõlgitud infoturbealaste materjalide keeleline ja kultuuriline kvaliteet on tihti madal.

3.1 BSI IT Grundschutz

BSI (saksa k. *Bundesamt für Sicherheit in der Informationstechnik*, inglise k. *Federal Office for Information Security*) on Saksa Liidumaa riiklik infoturbeorganisatsioon, mis asutati 1991. aastal [27] .

IT Grundschutz [8] on BSI poolt loodud ning perioodiliselt uuendatav infoturbe standard – (ingl.k *IT Baseline Protection Manual*). Esmaversioon avaldati aastal 1994, uuendused on iga-aastased, hetkel kehtib versioon 13. 90-ndatel konkureeris tegevuspõhine IT Grundschutz kahjupõhise standardiga BS7799 (hilisema ISO 27001 eellane), mille väljaandjaks oli teine sarnase nimega organisatsioon – BSI - British Standards Institution [28] .

IT Grundschutz raamistik kätkeb endas etalonturbe kataloogi (Kompendium) ja nelja standardit:

- BSI 200-1 (kirjeldab infoturbe halduse süsteemi ja infoturbe korraldus)
- BSI 200-2 (kirjeldab etalonturbe protsessi, meetmevalikut ja käitust)

1 Nüüd ja edaspidi - ülevaate ja analüüsi käigus tehtud olulised tähelepanekud registreerin nummerdatud leidudena. Leidude koondvaade on esitatud jaotise 5.8 tabelites.

- BSI 200-3 (kirjeldab riskihaldust)
- BSI 100-4 (kirjeldab äri jätkuvust)

IT Grundschutz kui vundament on olnud inspiratsiooniks nii ISKEle kui ka E-ITSile. Viimastes Grundschutzi versioonides on esitusviisi oluliselt kaasajastatud. Elemendid on korraldatud hierarhiliselt ning neid tutvustatakse järk-järgult. See vähendab näivat keerukust ning kasutaja frustratsiooni seoses mahuga. IT Grundschutz on alates aastast 2006 teinud jõupingutusi ISO/IEC 27001 nõuete inkorporeerimiseks [29] , mistõttu need standardid täna pigem ühilduvad kui vastanduvad.

Märgin BSI etalonturbe probleemina ära asjaolu, et eri alamstandardites (BSI 200-1/2/3) püstitatud korraldusi ja nõudeid oli keeruline ühendada koondvaatesse või esitada hierarhiliselt korrektselt (vt ka Lisa 1, Mudel A). Nii näiteks ei selgu, kas varade arvelevõtt kuulub riskihalduse, etalonturbe või ISMS meetodi koosseisu, ehkki inventuur on kõigi nende tegevuste kohustuslikuks eelduseks. Saksamaale omases piisavalt suures ettevõttes ei ole selline sektsioneeritus probleemiks, kuivõrd erinevate alamteemadega (riskihaldus, käitus, infoturve) tegelevad erinevad allüksused. Küll aga võib probleem tekkida Eestis, kus Rahandusministeeriumi andmete [30] kohaselt leidub paarikümne töötajaga asutusi piisavalt.

Leid 02: BSI eri standardites (200-1, 200-2) püstitatud korralduste ja nõuete agregeerimine ning ühtsesse hierarhilisse koondvaatesse ühendamine on komplitseeritud.

3.2 ISKE

ISKEl on olnud eriline ja tänuväärne roll infoturbe distsipliini teadvustamisel Eestis. Lühendi ISKE tähendus RIA veebi ühe tüviteksti [31] kohaselt on "InfoSüsteemide Kolmeastmeline Etalonturve". ISKEt käsitlen põhjalikumalt, kuivõrd just ISKE oletatavad või tegelikud puudused on olnud E-ITS-standardi valmimise motivaatoriks.

Lühidalt ISKE ajaloost: turvastandardite kaardistamisel tutvusid Cybernetica AS tollased töötajad BSI poolt CD-ROM-kandjal levitatava IT Grundschutziga, ning see mõjutas oluliselt infoturbealaseid mõttemalle Eestis [32] . Cybernetica hinnangus [33]

(2003) leiti, et etalonturve kui meetod võiks Eestile sobida. Seeba oma magistritöös ([34] lk 11-13) kirjeldab ISKE saamislugu põhjalikumalt.

Võtmeisikuteks ISKE väljatöötamisel olid Monika Oit, Ahto Buldas, Vello Hanson ja Valdo Praust[1]. Turvastandard Eestile valiti 15 turvastandardi seast, kuid läbi vaadati neid üle 30. Turvaklasside idee autoriks oli Ahto Buldas. BSI alumise turvataseme muutis Vello Hanson vastavuses Eesti oludega pisut nõrgemaks, jättes sinna hinnalt odavamad ja seetõttu kättesaadavamad meetmed (tase L). Kesktaseme meetmed võeti Grundschutzi dokumentatsioonist üle sisuliselt üks-ühele (tase M). Oluliselt panustati kõrgtaseme (H) meetmetesse, need töötas välja Valdo Praust. Nii näiteks, kõrgtaseme süsteemide auditeerimisnõuded osutusid BSI nõuetest karmimateks. Valdo Praust lisas BSI kriteeriumitele (konfidentsiaalsus, terviklus, käideldavus) hiljem kategooria R (käideldamatusest tingitud kahjud).

Hindan, et tollaste otsuste üheks varjatud motivaatoriks oli ka 1996. a aset leidnud ning Imre Perliga seostatav andmelekkeskandaal [35] .

ISKE rakendusjuhendi esimene versioon valmis 2003. aasta oktoobrikuus. Valitsus võttis ISKEle ametliku staatuse andnud määruse [36] vastu 12.08.2004. Auditeerimiskohustus tekkis ISKE-kohuslastel alates 01.01.2008.

3.2.1 ISKE kriitika

ISKEt on palju kritiseeritud. Suurimaks puuduseks on nimetatud tema tohutut mahtu. Seeba [34] võrdleb ISKE umbes 5000-t lehekülge A4 teksti standardi ISO/IEC 27001 22 leheküljega.

Kivimaa oma doktoritöös (2013, lk 252) [37] vaatleb ISKEt turbekulutuste optimaalsuse seisukohast ning esitab ISKE ratsionaalse optimumi puudused: "1. ISKE turvameetmete loetelu aluseks on võetud üks-üheselt turvameetmed Saksa Liitvabariigi infoturbe mudelist BSI (~1000 turvameedet) ning juurde lisatud kõrge taseme meetmed (~500). St Eesti riigiasutus oma ~100 korda väiksemate ressurssidega peaks olema suuteline teostama oluliselt enam turvameetmeid kui Saksa riigiasutus? Ilmselgelt küllaltki

1 Refereeritud intervjuu põhjal ühega projekti osalistest

lootusetu olukord – suure mehe ülikond päris kindlasti ei sobi väikesele mehele. Praktikas jätavad Eesti riigiasutused ressursside puudusest tingitult sadu BSI/ISKE turvameetmeid lihtsalt realiseerimata (info ISKE auditítest). 2. Ratsionaalne optimum on vägagi kaugel tegelikust optimaalsest". Tsitaadist ja selle analüüsist tulenevad järgmised leiud:

Leid 03: Kulutuste problemaatika kui üks ISKE läbitöötamata aspekte.

ISKE määrus näeb ette, et ISKE rakendub andmekogudele ja mitte asutusele või infosüsteemile. See aga tähendab, et varemalt puudus vajadus vaadelda asutust tervikuna ning et katmata jäid lateraalsed küberohud.

Leid 04: ISKE rakendub andmekogudele, E-ITS rakendub kogu asutusele (sh äriprotsessidele).

2018.a hindas Riigikontoll ISKE rakendamist [38] kohalikes omavalitsustes (KOV). Aruande punktis 43 öeldakse: "[..] selgub, et kohustuslikku turvameetmete süsteemi ei ole suutnud täies ulatuses ükski KOV rakendada. KOVid on seda põhjendanud ISKE töömahukusega. Selgituste kohaselt käib ISKE dokumentatsiooni väljatöötamine ja ka kogu IT-taristu haldamine ISKE rakendusjuhendi ja meetmete kataloogi järgi KOVidele üle jõu. KOVid on teinud RIA küsitlustes ettepaneku ISKEt kohaldada etapiviisi või vähendatud mahus. Kuigi ISKE rakendamise seisu selgitamiseks on tehtud küsitlusi, pole rakendamist takistavaid asjaolusid seni analüüsitud".

Edasi, Riigikontrolli aruande punktis 53 tsiteeritakse audiitorfirma PWC eksperdihinnangut „Kohalike omavalitsuste IT juhtimise, e-teenuste analüüs ja arendusettepanekud“ aastast 2015: "[..] üldiselt on väikestes KOVides IT antud mõne teise valdkonna spetsialisti vastutusalasse ning keskmise suurusega KOVides koosneb IT-teenistus kuni paarist spetsialistist. Lisaks kirjeldati, et peamiselt suudetakse pakkuda IT tehnilist tuge, aga spetsialiseerumist (sh infoturbele) on vähe ning keerukamate tehniliste probleemide puhul on vajadus välise abi järele." Riigikontrolli aruanne ei too välja ISKE rakendamata jätmise sügavamaid põhjusi, mistõttu pole ka teada, kas tegu on objektiivse keerukusega või rakendaja universaalse õigustusega oma seadusliku kohustuse täitmatajätmiseks.

Puudub teave selle kohta, kas või mis ulatuses on ISKEle omistatud hinnanguid üldse kellegi poolt süsteemselt kaardistatud.

3.2.2 ISKE tööriist

ISKE kriitika teiseks keskseks küsimuseks peale ISKE keerukust on kujunenud ISKE tööriist. Elojärvi oma diplomitöös [39] sedastab: "Sampo on maagiline artefakt, mis toob omanikule õnne ja hea elu". Analüütikuna märkan Sampo sarnasust ISKE tööriista avalikult eeldatava spetsifikatsiooniga. Vaikimisi eeldatakse ISKE tööriistalt, et see toetaks rakendajat meetmete elukaare tagamisel ning infoturbeprotsesside läbiviimise dokumenteerimisel. Vajadusele tööriista järele viitab nii Kivimaa – "astmelise infoturbe ekspertsüsteemi" nime all, kulude vähendamise potentsiaaliga 10x – kui ka Seeba, kes esitab ISO 27001-ga ühilduva, riskihaldust arvesse võtva, tööprotsesse toetava ning neid ISMS tarbeks dokumenteeriva süsteemi "*ISMS tool*" (infoturbehalduse tööriista) disaini.

Kivimaa (lk 243) toob välja emergentsed seosed meetmekataloogi ja infoturbe-protsesside vahel, väites et "koolituse taseme tõstmine on otstarbekam, kui parema ja kallima tulemüüri hankimine". Seeba oma Tabelis 1 esitab mitut erinevat laadi ISMS tööriistade teoreetilise võrdluse – sh kasu tavalisest Exceli tabelist võrrelduna töövoopõhise süsteemiga. Kuna Seeba esitab kvalitatiivsed hinnangud skaalal 1..5, siis ei tule ilmutatult välja säärase tööriista konstrueerimise hind.

Näen seoses ISKE tööriistaga kolme alamvaldkonda. Üheks on masintugi ülipikkadele nimekirjadele, mis Seeba andmetel on osaliselt juba realiseeritud, teiseks masintugi vastavusele (*compliance*), kus ta pakub välja disaini. Hindan kolmandaks ja seni vähe uuritud valdkonnaks etalonturbe protsesside a) keerukust ja b) osade tihedaid omavahelisi seoseid. Need kaks tunnust on mulle paraku eelnevalt tuttavad kui Perrow raamatus [40] kirjeldatud tehnogeensete katastroofide alustingimused.

Leid 05: ISKEl puudub kulutuste formaalne mudel.

ISKE rakendamine eeldab spetsiifilist taustteadmust etalonturbe meetodist endast, samuti eelnevat põhjalikku tutvumist materjalidega, mis geneerilise infoturbejuhi lugemislaualt puuduvad.

Leid 06: Infoturbejuht kui keskne ressurss mahuga 1850 töötundi aastas.

Vajadus esmatutvuseks ISKE materjalidega on põhjus, miks Kivimaa hinnang – 1-2 inimkuud astmelise infoturbe mudeli rakendamisele – on pigem alahinnatud. Infoturbejuht on asutuses kriitiline ressurss, ainuke omataoline. Infoturbejuht on juhiks, koordinaatoriks, vastutajaks ja ühtlasi ka pudelikaelaks kõigile turbetegevustele, mida sooritavad teised töötajad. Peterson ([41] , Fig 7.4) kasutab säärase mustriga ressursi kirjeldamisel terminit "*shared channel*".

Leid 07: Infoturbejuht kui keskne ja kriitiline ressurss (*shared channel*).

3.3 E-ITS

E-ITSi aluseks olev etalonturbe mudel tugineb jätkuvalt ja väga suures osas BSI IT Grundschutzi materjalidele. Standardi väljatöötamisel võtsime aluseks Grundschutzi 2019. aasta versiooni ning üksikuid materjale ka 2021. aasta versioonist. Eesti e-riigi tugevused (X-tee, ID-kaart) peegelduvad E-ITSi esmaversioonis osaliselt ning nende süvendatud käsitlemine on standardi omaniku tegevuskavas.

Teen kindla järelduse, et E-ITS on senist ISKE kogemust olulisel määral arvesse võtnud ning et suur hulk ISKE tegelikke või eeldatud puudusi on E-ITSis kõrvaldatud. Seni puudub ülevaade, missuguseid ISKE ja IT Grundschutzi teadaolevaid puudusi on E-ITS üritanud arvesse võtta. Olgu minu töö üheks tulemiks esmane loetelu sellistest asjaoludest. Järgneb loend teemadest, mida standardi koostamise edenedes arutasime ja milliste osas võtsime töögrupis vastu kokkuleppeid.

1. Mitmeid mahukaid kontseptsioone ja mudeleid selgitasime lugejale jooniste (visuaali) abil (vs senised pikad tekstid). Paljud joonised on originaaljoonised, kuid ka Grundschutzist pärit joonised on detailsemalt läbi töötatud.

2. Erilist rõhku panime ühtesobivusele ISO/IEC 27001 nõuetega, kuni selleni välja, et juhendi "ISMS nõuded" ja ISO standardi teatud peatükkide vahel on vastavus.

3. Avastasime, et saksakeelses tekstis nõuete (*Anforderungen*) ja meetmete (*Umsetzungshinweise*) sisu dubleerib üksteist liiga suurel määral. E-ITS etalonturbe kataloogis on mahu vähendamiseks esitatud üksnes meetmed (need saadi nõuete ja "teostussoovituste" kombineerimisel).

4. Nõuete all tuleb edaspidi mõista E-ITS infoturbe haldussüsteemi (ISMS) nõudeid, seda väljendab ka vastava juhise nimetus.

5. Meetmete ja nõuete ühildamise tõttu tuli leida asendus nendevahelist vastavust verifitseerivatele sammudele (*Grundschutz-Check*).

6. Auditeerimisprotsess ([1] , Auditeerimisjuhend) on korraldatud uudselt ja Eesti väiksust arvestades.

7. Me ei võtnud E-ITS-i üle mooduleid, mis Eesti oludes lisaväärtust ei annaks, nagu näiteks IBM z-server ja faks.

8. Üks kolmest etteantud alustamisviisist – tuumikuturve (*core protection*) – on võrreldes BSI ebapiisava interpretatsiooniga kirjeldatud oluliselt täpsemini.

9. Nägime vaeva Grundschutzi keele ja ärikultuuri lähendamiseks Eestile. Sõnastasime meetmed uuesti ja eesti keeles, pidades seejuures eelkõige silmas IT Grundschutzi tekste ja nende mõtet. Saavutasime mahu olulise kokkuhoiu. Kohandamine toimus heas usus, eeldefineeritud reeglid puudusid (vrdl **Leid 01** ja Küberturvalisuse strateegia [2] lk 40).

10. Avastasime, et indo-euroopa keelte modaalverbid, mida standardid kultuslikult kasutavad kohustuse määra edasiandmiseks, ei ole eesti keelde süsteemselt ega kadudeta tõlgitavad. Seetõttu kasutame E-ITS tekstides kohustuse määra edasiandmiseks ka vähem rangeid vahendeid.

11. Meetmete selge eestikeelse väljendamise huvides võtsime arvesse moodustajate pragmaatilisi funktsioone, eelkõige teema-reema kontseptsiooni [42] .

12. Tegime katset paigutada mõistesüsteem korrektsesse ontoloogiasse. Mõnel juhul õnnestus tekkinud probleemid lahendada, kuid mitte alati. Näiteks Eesti seadustega määratletud legaalterminil "infovara" ei ole inglise keeles sama spetsiifilist tähendust. Saksa keeles on sõnale "oht" kolm eristuvat vastet. Ingliskeelse termini "access" vasteks on vastavalt kontekstile kas "(juurde)pääs" või "pöördus", kusjuures õige vaste valimiseks on vaja originaalteksti mõista

sisuliselt. Standard väldib terminite "küber-", "infovara" ja "teenus" kasutamist kõikjal kus võimalik.

13. Lõime terminoloogiat ning korrastasime vana. Tegemist oli erakordselt ajamahuka tegevusega. Eesti keel sõltub suurest hulgast liiderkeele mõistetest, mida keelkondadevahelised loomulikud semantilised erinevused ei võimalda kadudeta üle võtta. Probleem pole uus – selle olemasolu markeeris Riikoja juba 1961. aastal, eessõnas Wieneri "Küberneetika..." [43] eestikeelsele tõlkele: "Nii esineb siin selliseid võõrsõnu, millele asemele ühemõttelist eestikeelset vastet ei leidugi". Olen veendunud, et rahvuskultuuri ja keele säilimise huvides tuleks terminoloogiatöö Eestis kuulutada riiklikult oluliseks teemaks, koos asjakohase finantseerimisega.

14. IT Grundschutzi Põhiturbejuhendi taolise dokumendi koostamist selle riigihankega ei tellitud.

15. Standardi koostamise käigus seadsime endale kvaliteedinõude, et standardi tekstid oleksid arusaadavad ka noortele ja erialase kõrghariduseta inimesele. Seda nõuet õnnestus täita lauseehituse ja jutustamise viisi osas ning vähem terminoloogia osas.

4 Meetodi valikuprotsess

Standardi protsesside analüüsiks vajasin notatsiooni ja metoodikat. Tegin järelduse, et notatsioon ja meetod on omavahel tihedalt seotud (näiteks nagu UML ja RUP). Notatsioon pidi olema piisavalt paindlik väljendamaks sotsiotehniliste süsteemide iseärasusi ning samas piisavalt range, võimaldamaks järgnevat analüüsi, valideerimist ning vajadusel ka verifitseerimist.

Alustasin notatsiooni valikust. Määravaks said senised frustreerivad kogemused standardi protsesside tõlkimisel BPMN-notatsiooni. Keskendusin UML, BPMN, FRAM ning Petri võrkude notatsioonile.

4.1 UML

Fowleri raamatut [55] uurides tõdesin, et UML keel oma tohutute võimalustega keskendub ennekõike tehiste kirjeldamisele ning ei pruugi sellisena sobida sotsio-tehnilise süsteemi kirjeldamiseks. Aktiivsusdiagrammi võimekus erinevate suhtlus-liikide väljendamisel on ebapiisav. Kasutusloodiagramm väljendab pigem inimese ja masina vahelisi suhtlusakte, seejuures vaid kõige ülemisel tasemel. Standardi protsessid aga kirjeldavad põhiliselt inimese ja inimese vahelist koostööd. Ülejäänud UML diagrammid (sh seisundidiagramm) on selgelt orienteeritud tarkvaralisele lõpp-produktile ning need pigem ei sobi inimestevahelise vaba suhtluse ega asutusesisese töökorralduse kirjeldamiseks, kuivõrd töökorralduses puuduvad elemendid nagu komponent, klass ja implementatsioon.

4.2 BPMN

BPMN keel on spetsiifiliselt ette nähtud äriprotsesside kirjeldamiseks.

Ojava magistritöö [35] refereerib BPMN saamislugu ja otstarvet: "BPMN loodi 2004. aastal Business Process Management Initiative'i poolt. Peamine eesmärk oli luua üheselt mõistetav märgisüsteem, mida mõistaksid nii ärianalüütikud, arendajad kui ka ettevõtte töötajad, kellel ei ole IT-alaseid spetsiifilisi teadmisi. Suure huvi tõttu adopteeriti BPMN standardina 2006. aastal. Hetkel kehtib versioon BPMN 2.0. BPMNi tugevused seisnevad selle sobivuses erinevatele pooltele. Ärivaldkonna eksperdid saavad tuvastada protsessi graafilise kujutise õigsuse ning selles leiduvad kitsaskohad, nagu pudelikaelad, katkestavad tingimused ja tsüklid. Analüütikutel on võimalik koguda andmeid ressursside kasutuse kohta, et tuvastada, kas protsessi on võimalik optimeerida või mitte, ning arendajad huvituvad võimalustest tõlkida diagramm masinloetavasse keelde jagamis- või käivituseesmärkidel. Sellisteks keelteks on enamasti XPDL või BPEL.".

Vähem on teada BPMN puudustest, mis takistavad tal oma eesmärki täita. Minu kogemuste põhjal võib BPMN vähem sobida selliste protsesside kirjeldamiseks, kus esineb osade tugev läbipõimumine, või toimingute asünkroonsus.

4.3 FRAM

FRAM akronüümina tähistab funktsionaalse resonantsi analüüsimeetodit (*Functional Resonance Analysis Method*). Meetodi looja Hollnageli hinnangu kohaselt on meetod eriti sobiv just sotsiotehniliste süsteemide analüüsiks. FRAM pole Eestis seni tuntud. Annan ülevaate FRAM mudeli notatsioonist ja analüüsivõimekusest Lisas 2.

4.4 Petri võrgud

Petri oma doktoriväitekirjas 1962. aastal kirjeldas tollal uudse mudeli ja sellele vastava notatsiooni [45] 1962. aastal. Vastavalt ülestähendatud graafe nimetatakse kaasajal Petri võrkudeks.

Vaatlen Petri võrke piiratud kontekstis, et nendega on võimalik mudelite õigsust matemaatiliselt valideerida. Tutvusin paarikümne teadustööga ning jõudsin üldistatud

järelduseni, et oluliseks tingimuseks äriprotsessi mudeli kontrollimisel Petri võrkude abil on vastava translaatori olemasolu. Ma ei tuvastanud ühtki teadaolevat translaatorit, millega oleks võimalik mudeli ülekandmine tuntud modelleerimisvahenditest (Bizagi Modeler, Camunda Modeler) ning leidsin, et sellise vahendi arendus väljuks analüüsi õppekava raamidest.

Minu hinnangul tuleks töödeldavate andmekategooriate (näiteks sihtobjektide klassifikatsiooni) paljususe tõttu BPMN mudeli testimisel eelistada värvitud Petri võrke (CPN – *Coloured Petri Networks*). Lisaks õppisin, et valideerimismudelite aeg on paratamatult diskreetne.

Leid 08: Valideerimismudelite aeg on diskreetne, mitte reaalaeg nagu E-ITS tegevustel.

4.5 Valikukriteeriumid

Otsisin notatsioonisüsteemi ja metoodikat, mis rahuldaks järgmisi tingimusi:

(a) eksisteerib formaalne **notatsioon**, mis võimaldab mudeleid üles tähendada, eelistatult nii graafilise kui struktuurse (XML) arvutitoega;

(b) eksisteerib **meetod** ülestähendatud mudelite **analüüsiks**, sh keerukuse ja/või loogikavigade analüüsiks (NB! Notatsioon ja analüüs ei pea pärinema samast allikast või koolkonnast; tingimuseks on meetodi suutlikkus mudelit töödelda);

(c) metoodika peab hästi **sobima** uuritava kompleksvaldkonnaga (infosüsteemid, infoturve, sotsiotehnilised süsteemid).

Juhul kui sääraseid metoodikaid leidunuks mitu, tulnuks nende vahel valida.

Selgitan loetletud tingimuste tausta. E-ITS lepingu täitmise käigus koostasin mitmeid graafilisi mudeleid, mis (mõnevõrra muudetud kujul) said standardi osaks ning ühtlasi mõned mudelid, mis lepingu tööde tulemitesse ei kuulunud. Tingimus (a) oli vajalik, et juba eksisteerivaid ning mittestandardselt kirjapandud mudeleid edasi arendada. Tingimus (b) oli vajalik, et piirata uuritav valdkond vastavusse diplomitöö iseärasuste ja mahuga. Tingimus (c) oli tingitud uurimisvaldkonna paiknemisest IT mitme alamharu piiridel. Seos infosüsteemidega väljendub eelkõige asjaolus, et infosüsteemid ja neis

töödeldavad andmed on põhiliseks E-ITS standardi poolt kaitstavaks objektiks. Seos infoturbega (mis *pro forma* sisaldub ka infosüsteemide analüüsi distsipliinis) on ilmutatud – see on valdkond, mida E-ITS kui standard reguleerib. Inimkäitumise ja sotsiotehniliste süsteemide käsitlus infosüsteemi analüüsi rakendustaseme õpetamisel piirdub Andreas Capell'i kuulsa projektijuhtimise karikatuuriga [46] (*„I know that's what I said, but it's not what I meant!"*). Organisatsiooniteoorias võimaldab inimkäitumise iseärasusi põhjalikumalt arvestada mõiste – sotsiotehnilised süsteemid.

4.6 Esialgne meetod

Valikukriteeriume a) ja b) rahuldasid BPMN ja FRAM. Valikukriteeriumit c) rahuldas üksnes FRAM. Esialgseks meetodiks valisin FRAMi. Töö käigus selgus, et kaasneva tarkvara võimekus FRAM mudelite analüüsil on piiratud ning üksnes FRAM ei võimaldaks ülesannet lõpuni lahendada. Seetõttu pidin töö käigus osaliselt tagasi pöörduma klassikaliste meetodite (BPMN) ja kontseptsioonide (ERD) kasutamisele.

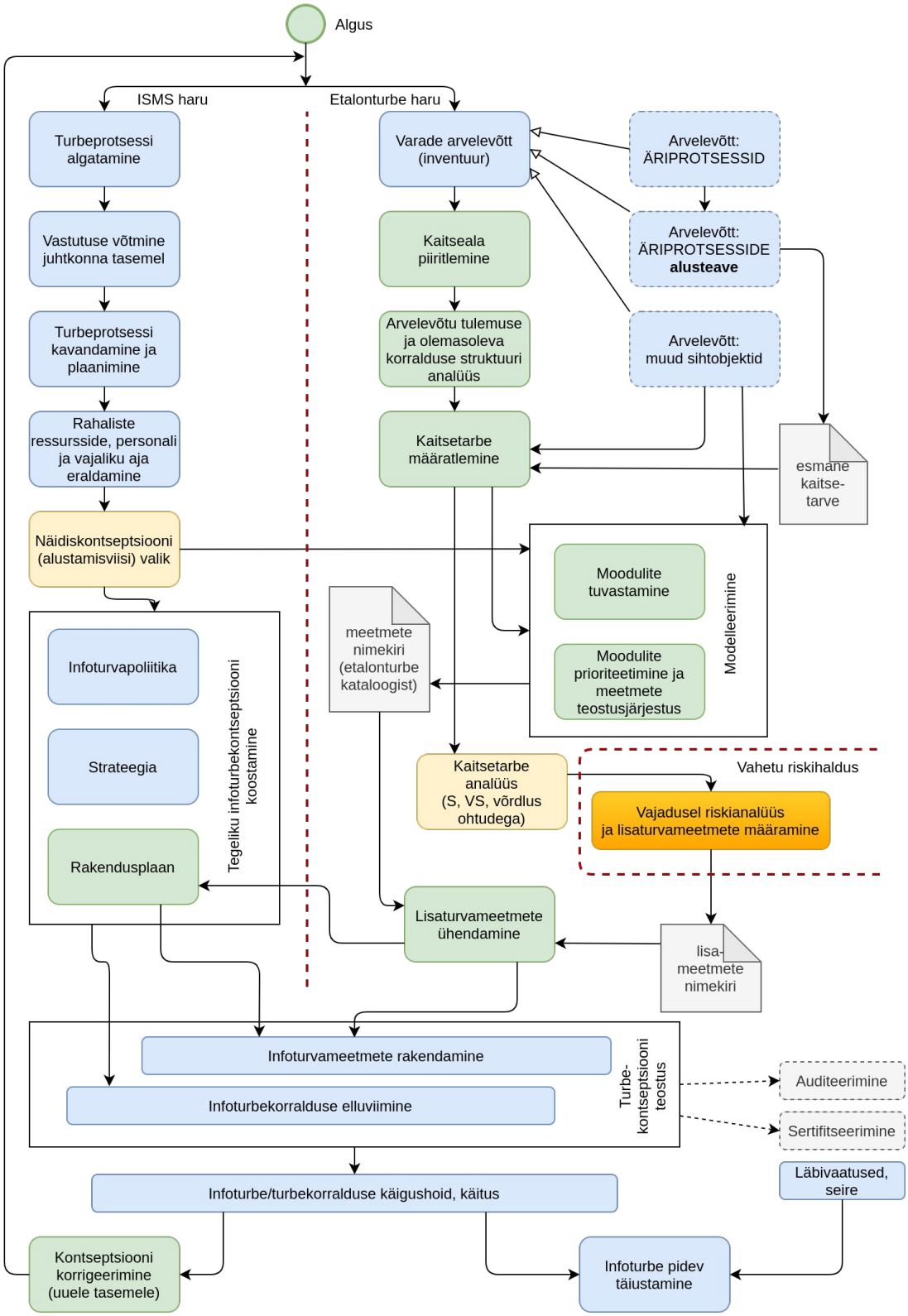
5 Töö käik (süntees)

Ärianalüüsi alustatakse tüüpiliselt ärisõnastiku koostamise ja ärireeglite kirjeldamisega. Infoturbestandardi lepingu täitmise käigus olin eelnevalt saanud kogemuse, et mitmesaja lehekülje pikkuse täisteksti korrektne tõlkimine ärireegliteks on liiga mahukas ning ühtlasi – teksti sisemiste vastuolude tõttu – ka erakordselt keeruline. Keele- ja kultuuriprobleemide tõttu saanuks ärisõnastiku kvaliteet kõigest rahuldav ning kindlasti mitte ideaalne. Võtsin analüütikuna vastu otsuse, et standardi tekstis ilmnenud vastuolud silun juhiste sobiva sõnastusega. Küll aga oli võimalik tagada piisavalt üldise mudeli kvaliteet. See on põhjus, miks keskendusin eelkõige mudeli konstrueerimisele (tegevusjärgnevus on esitatud Lisas 1, sellega on soovitav tutvuda enne käesoleva jaotise lugemist).

Neis tingimusis on võimalik analüüsile allutada E-ITS protsessi mudel, mida tinglikult nimetan **Mudeliks 01**. See mudel kujunes minu varasemate mudelite edasiarendamise tulemusel (vt Lisa 1 **Mudel F**). Joonis 1 esitab sama skeemi uuesti kui **Mudeli 01**.

Mudelis kasutan lihtsustatud BPMN notatsiooni. Palju ruumi nõudvate hargnemiste ja koondumiste vältimiseks kasutan mitteametlikku võtet, kus lüüside (*gateways*) tingimused varjan elemendi semantika taha, näiteks: valik, piiritlemine, ühendamine. Mudelis on kolm tegutsemisharu. Esimene neist on infoturbe haldussüsteemi algatamine (nn ISMS haru), teine on etalonturbe haru. Kolmas haru on riskihaldus, mida mudel käsitleb üksnes liidestuse näitlikustamise otstarbel. Punased punktiirjooned tähistavad tegevusharude vahelisi piire. BSI protseduuridest ei selgu, kuhu kuulub inventuur, kuid kuna inventuuril ja etalonturbel on ühine andmestik, otsustasin analüütikuna käsitleda inventuuri etalonturbe koosseisus. Mudel illustreerib harudevaheliste suhete keerukust ning sisaldab kokku 28 tegevust (tegevusgruppe loetlemata). Vahetulemusi on ilmutatult kujutatud kolm, tegelikkuses on neid oluliselt enam.

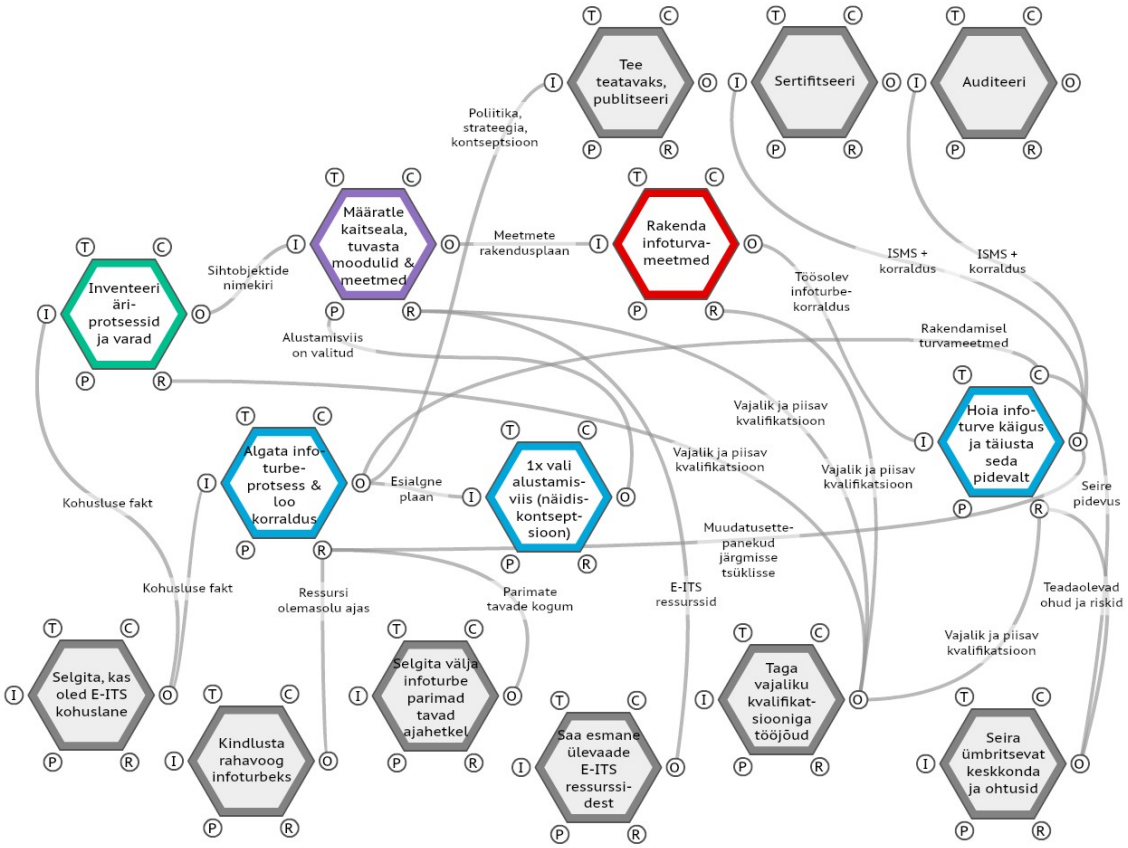
Edasi hakkan **Mudelit 01** ümber joonistama erinevates aktsepteeritud notatsioonides ja vahe-eesmärk on baasmudelit enne tema analüüsimist testida.



Joonis 1. Mudel 01 - standardi protsess detailselt

5.1 Järk 1 - FRAM mudeli näide

Joonise 2 esitab mudeli **Mudel 02.** Tegemist on lihtsustatud mudeliga, mille ainsaks eesmärgiks lugeja esmatutvus FRAM notatsiooniga. FRAM meetodi kirjeldus ja mudeli notatsioon on selgitatud Lisas 2, millega tuleks tutvuda enne edasilugemist.



Joonis 2. Mudel 02 - E-ITS kaksikprotsessi (ISMS + etalonturve) lihtsustatud mudel

Atomaarseks elemendiks FRAM notatsioonis on kuusnurk (*hexagon*), mis väljendab üht eraldivõetud tegevust (*activity*). FRAM nimetab kuusnurki funktsioonideks. Kuusnurkade vahelised ühendusjooned väljendavad saadusi (BPMN mõistes andmeobjekte) – need võivad olla loogilised tingimused, andmed vms. FRAM ei ole kulgmudel – iga funktsioon võib käivituda enne kui eelnev funktsioon lõpetab või isegi alustab. Seetõtu puuduvad skeemil tegevuse alguse ja lõpu markerid. Selline iseärasus sobib hästi BSI IT Grundschutz protsessiga, kus lõpumarkerit tuvastada ei õnnestu.

Näitena sisendite toimimisest ei saa mudelis järgmised tegevused alata enne, kui on välja selgitatud, kas organisatsioon on E-ITS kohuslane või mitte – saaduseks on „kohustuse fakt". See tundub ebaoptimaalne, kuid just selline on FRAM mudelite loogika. Ühtlasi ei saa ükski FRAM notatsioonis esitatud skeem lõppeda saadusega (meie näites tüvitekstid „poliitika, strateegia, kontseptsioon"), vaid peab kindlasti lõppema tegevusega – „Tee teatavaks, publitseeri". See tähendab, et seosed ülejäänud äriloogikaga (sisuliselt joonistevahelised ühenduspunktid (*off-page connectors)*) tuleb samuti väljendada kuusnurkadega. Joonisel 2 olen sellised ühenduslülid värvinud halliks ning FRAM terminoloogias nimetatakse neid taustfunktsioonideks (*background functions*). Skeemi loogikast nähtub, millised neist liidestest on eeldused (puudub sisend) ning millised on väljundid. Väiksema FRAM diagrammi mõningaseks ebamugavuseks on, et ühenduselementide kogus võib ületada sisuliste elementide kogust. Nii näiteks, antud skeemil on liidestena kujutatud kuut eeldustegevust ja kolme järeltegevust (kokku 9), kuid sisuliste elementide arv skeemil on kõigest 6.

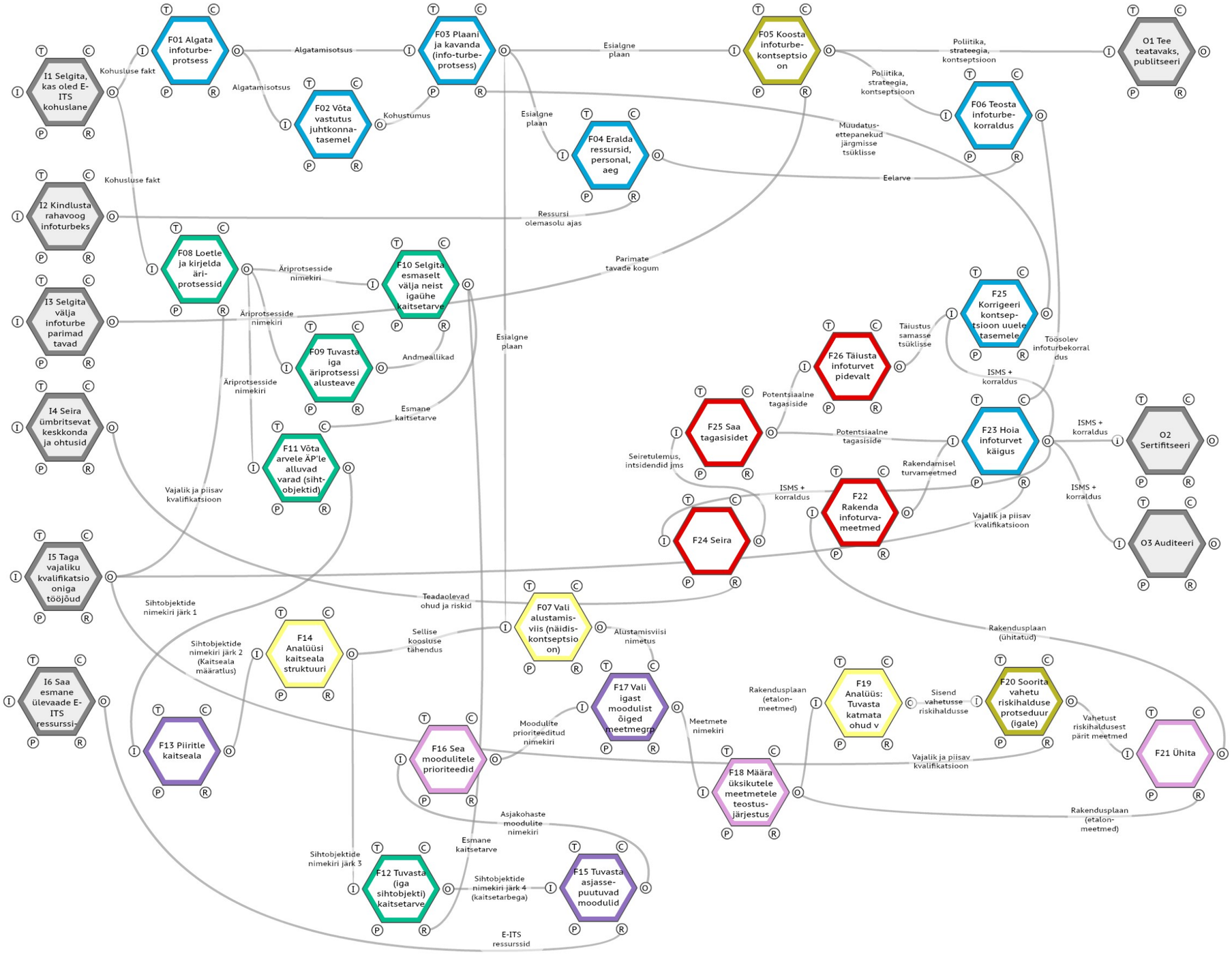
Metoodiline juhendmaterjal [49] rõhutab (lk 7), et FRAM mudel tuleb konstrueerida põhimõttel "ulatus enne sügavust" (*breadth before depth*). Tõlgendan seda nõuet kui väidet, et äsjakirjeldatud lihtsustatud mudelit tuleb pidada kunstlikuks.

Jõudsin järeldusele, et mudelit pole õige lihtsustada funktsioonide varjatud grupeerimise abil (miski, mis on teistes notatsioonides täiesti lubatud tegevus). FRAM kuusnurgal on viis erineva otstarbega sisendit ning funktsioone grupeerides kaoksid olulised detailid.

Kuigi skeemi tegevusloogika Joonisel 2 edeneb vasakult paremale, tuli eeldused skeemi lihtsustamiseks paigutada skeemi alaosasse ning tulemused joonise ülaosasse. See on ebaharilik praktika, mis võimaldas oluliselt lihtsustada ühendusjoonte kulgu ja joonise loetavust. Juba järgmises FRAM mudelis ma säärast lihtsustust väldin.

5.2 Järk 2 - FRAM mudeli koostamine

Järgmisena esitan E-ITS protsessi täieliku mudeli FRAM notatsioonis. Joonis 3 kujutab **Mudelit 03**. Joonisel 2 kujutatud funktsioonid on siin detailiseeritud (lahti volditud). Skeemil on 6 sisendit (eeldust), kolm väljundtegevust ning 27 funktsiooni. FRAM mudel on heas vastavuses Joonisel 1 kujutatud originaalmudeliga.



Joonis 3. Mudel 03 - Etalonturbe kaksikprotsess (ISMS + etalonturve) FRAM notatsioonis

Joonisel 3 paiknevad mudeli kuus sisendtegevust (eeldused, *off-page connectors*) lehe vasakus servas ning kolm väljundtegevust (samuti *off-page connectors*) lehe paremas servas. Kuusnurkade värvid kujutavad endast katset märgistada vastavate tegevuste sooritajaid (või sooritamiseks vajalikku kvalifikatsiooni). Hiljem mudeli analüüsil mõistsin, et mõnigi tegevus vajab sooritamiseks korraga mitut kvalifikatsiooni. Samuti nõuavad ühe tegevustepilve tegevused vahelduvalt erinevaid kvalifikatsioone (näiteks infoturbe- vs protsessijuhtimise oskusi). Selle kõige tõttu osutub värvidega kodeerimine konkreetses mudelis väheefektiivseks (värvid on joonisel siiski säilitatud).

Leid 09: IT Grundschutzi tegevustiku paljusid elemente on lihtsam ja loomulikum kirjeldada FRAMi funktsioonidena kui BPMN tegevustena.

Leid 10: BSI rollimudel ja rolli definitsioon lähtub vastavuse ja juriidilise vastutuse põhimõtetest. Esineb lahknevus mõistega tegutseja (*actor*) UML/BPMN tähenduses.

Joonisel 3 kujutatud mudel ei väljenda absoluutset tõde, vaid on minu kui analüütiku subjektiivne *bona fide* tõlgendus. Infosüsteemide analüüsi alal on subjektiivsus täiesti normaalne nähtus, kuid sageli unustatakse see fakt otsesõnu deklareerimata.

5.2.1 Esmased järeldused FRAM mudeli koostamise põhjal

FRAM mudelit **Mudel 03** analüüsides jõudsin huvitavate järeldusteni. Esiteks, sisenditüüp T (*time*) ei leia minu mudelis üldse kasutust. mis võib olla tingitud sellest, et standardi protsesside omavaheline ajastus pole ülearu kriitiline (etalonturbe rakendamine kestab aastaid). See järeldus on õige siiski vaid seni, kuniks analüüsi käsitlusalast puuduvad konkreetsed meetmed, Alusohtude kataloog ning kuniks skeem ei sisalda Auditeerimisjuhendi või asutuse infoturbestrateegia poolt seatavaid tähtaegu. Sisenditüübid C (*control*), P (*pre-condition*) ja R (*resource*) leiavad kasutust vaid vähesel määral. Tegu on esmase mudeliga, mis vajab tulevikus kindlasti täiendamist arvestamaks standardi ülejäänud osades esitatud piiranguid ja tingimusi.

Skeemi liik kui „*not a workflow*" ja funktsioon atomaarse ühikuna tunduvad olevat optimaalselt valitud, kuivõrd näiteks BPMN poolt alati nõutava „stop" sündmuse/ikooni

puudumine Joonisel 3 on täiesti loomulik ega põhjusta FRAM mudelis vähimatki probleemi[1].

Leid 11: Töötajate kvalifikatsioon on BSI materjalide kohaselt peaaegu kõigi tegevuste eelduseks.

FRAM mudel vähe sellest, et võimaldab seda nõuet selgelt noteerida, osutab üheselt, et töötajate kvalifikatsiooni ebapiisavus blokeerib etalonturbe rakendamise. **Mudelis 03** Joonisel 3 on eeldus I5 "Taga vajaliku kvalifikatsiooniga tööjõud" selguse huvides ühendatud siiski vaid kolme kriitilise tegevusega. Funktsioonimudelilt on otseselt näha, et töötajate ebapiisava kvalifikatsiooni korral infoturbetegevused peatuvad.

Leid 12: FRAM mudeli kohaselt on jätkusuutlik rahastamine etalonturbe vältimatu eeldus.

Minu FRAM mudeli esimestes versioonides see eeldus puudus ning vastavuses FRAM ideoloogiaga tuli mul analüüsi käigus mudelit inkrementaalselt täiendada. Põhiline ressurss etalonturbes kulub meetmete rakendamisele, mida töö ei vaatle ning töötasudeks (funktsioon kulutatud ajast). Funktsioonimudelilt on otseselt näha, et ka ebapiisava rahastamise korral infoturve lihtsalt peatub.

Kokkuvõttes võimaldab FRAM notatsioon mul skeemil selgelt märgata asjaolusid, mis näiteks BPMN diagrammil poleks üldse ilmsed. Kindlasti pole etalonturvet võimalik rakendada ilma piisavalt kvalifitseeritud töötajate või jätkusuutliku rahastamiseta, kuid FRAM puhul paistab see asjaolu otse skeemilt. Seega andis FRAM notatsioon etalonturbe tegevustiku ülesmärkimisel mõningaid koheseid ja ootamatuid tulemusi.

5.3 Järk 3 - FRAM mudeli valideerimine

Mudeli 03 valideerisin järgnevalt tarkvara FMI [47] vahenditega. Mudel valideerimist ei läbinud, tegevus peatus pärast funktsiooni F16 "Sea moodulitele prioriteedid". Funktsioon F17 "Vali igast moodulist õiged meetmegrupid" ei aktiveerunud, kuivõrd funktsiooni F03 "Plaani ja kanvanda infoturbeprotsess" ressursisisendis R puudusid "Muudatusettepanekud järgmisse tsüklisse" ning omakorda funktsioon F07 "Vali

1 väite tõesus kestab siiski vaid formaalse valideerimiseni

alustamisviis" ei saanud aktiveerida funktsiooni F17 juhtsisendit C. Validaatori väljundteateid on kujutatud Joonisel 4. Sarnane viga kordus hiljem seoses funktsiooniga F25 "Saa tagasisidet". Vigu analüüsides selgus, et probleem on BSI poolt nõutud tagasisides.

```
Summary of FMIlog
Begin initialisation
--- MODEL INITIALISATION COMPLETED.
BEGIN CYCLE 1
Function <F01 Algata infoturbe-protsess> has been activated.
Function <F08 Loetle ja kirjelda äri-> has been activated.
BEGIN CYCLE 2
Function <F02 Võta vastutus juhtkonna-tasemel> has been activated.
Function <F09 Tuvasta iga äriprotsessi alusteave> has been activated.
BEGIN CYCLE 3
Function <F10 Selgita esmaselt välja neist igaühe kaitsetarve> has
been activated.
BEGIN CYCLE 4
Function <F11 Võta arvele ÄP'le alluvad varad (siht-objektid)> has
been activated.
BEGIN CYCLE 5
Function <F13 Piiritle kaitseala> has been activated.
BEGIN CYCLE 6
Function <F14 Analüüsi kaitseala struktuuri> has been activated.
BEGIN CYCLE 7
Function <F12 Tuvasta (iga sihtobjekti) kaitsetarve> has been
activated.
BEGIN CYCLE 8
Function <F15 Tuvasta asjasse-puutuvad moodulid> has been activated.
BEGIN CYCLE 9
Function <F16 Sea moodulitele prioriteedid> has been activated.
BEGIN CYCLE 10
No functions were actived during this cycle.
```

Joonis 4. Viga FRAM Mudeli 03 valideerimisel

IT Grundschutzi etalonturbeprotsess näeb ette tagasisidestamist nii enne järgmist iteratsiooni kui ka sama iteratsiooni vältel. See tekitab probleeme kõige esimesel valideerimisel, kui tagasisidet veel eksisteerida ei saa. Teisalt, formaalset mudelit, mis sisaldab lõputuid tsükleid, polekski võimalik lõpuni valideerida.

Tegin järelduse, et tegemist pole mudeli vigadega, vaid et FMI validaatoris puudub spetsiifilise lisatingimuse võimalus: "ignoreeri esimesel läbimisel". Mudeli muutmisel ja Grundschutzi poolt nõutud tagasiside kõrvaldamisel valideerimine õnnestub. Isendistatud mudeli automaatanalüüsi FMV tasuta versioon ei paku ning ühtlasi puudub akadeemilise litsentsi võimalus. Huvitava faktina vajab mainimist, et validaator leiab funktsiooni, millel lõpetada vaatamata asjaolule, et FRAM notatsioon lõpumärki ei sisalda.

Leid 13: BSI tagasisidestamisnõude tõttu tekivad mudelisse lõimi lukustavad tsüklid. Ühtlasi korelleerub see eelmiste leidudega küsimuses, et protsessimudelil puudub lõpp.

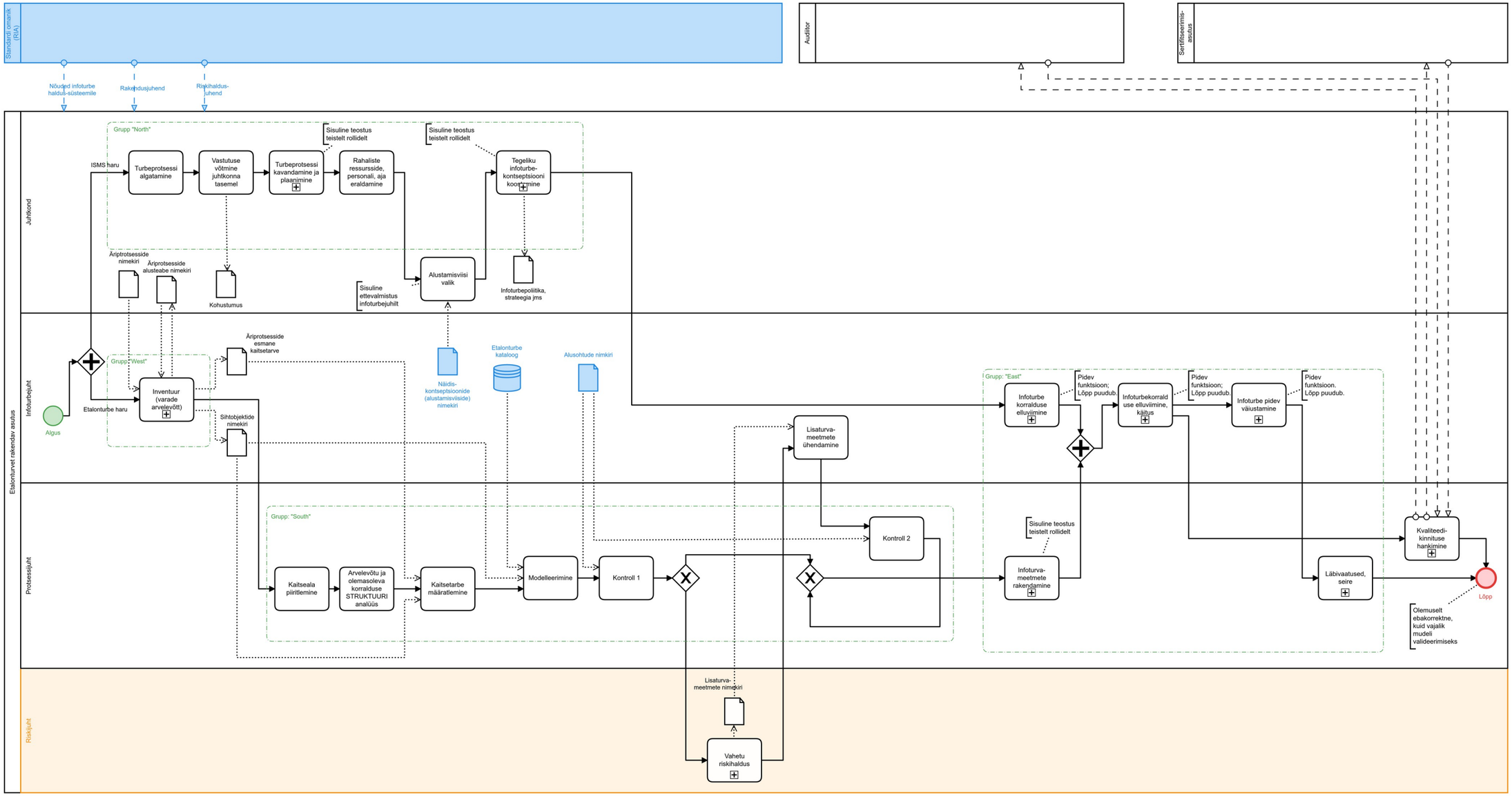
IT Grundschutz protsessi tsükliline ja raskesti automaat-valideeritav ülesehitus nõuab eraldi diskussiooni väljaspool seda tööd.

5.4 Järk 4 - BPMN mudel

BPMN notatsiooni teadaolevate probleemide tõttu hoidusin BPMN mudeli koostamisest pikalt. Lõpuks õnnestus tekkinud modelleerimisprobleemidele leida tehnilised lahendused – näiteks lahendada hierarhiaprobleemid BPMN koreograafia (*choreography*) vahenditega. FRAM notatsiooni kogemusele tuginedes leian, et funktsiooni iseloomuga elementide kujutamiseks ei tohiks BPMN-i üldse kasutada, kuigi tehniliselt on see võimalik. Lisaks märgin, et Leide 11 ja 12 poleks BPMN diagrammi põhjal olnud võimalik tuletada.

BPMN notatsioonis **Mudel 04** on esitatud Joonisel 5. Koostasin selle **Mudeli 01** (Joonis 1) ja **Mudeli 03** (Joonis 3) põhjal.

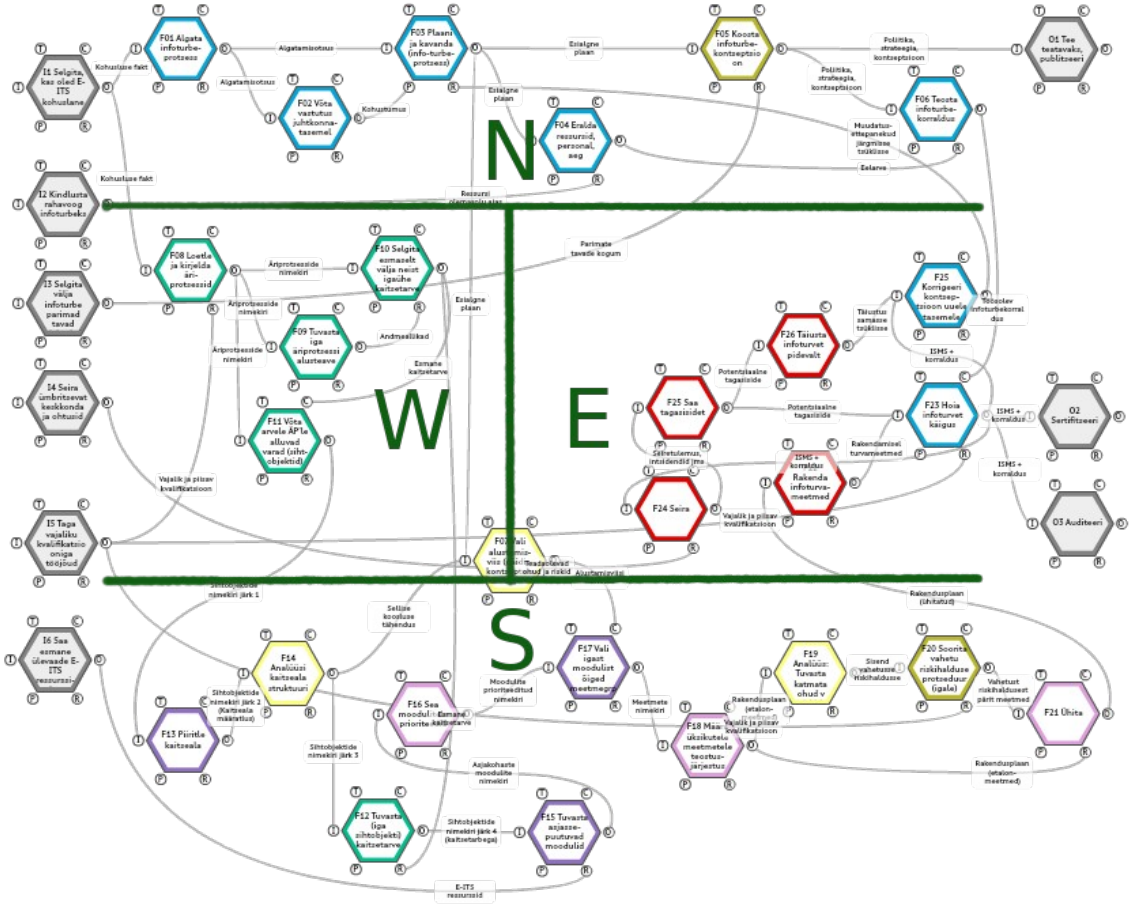
Mudelil nähtavaid iseärasusi ei ole.



Joonis 5. Mudel 04 - Etalonturbe ja ISMS kaksikprotsess BPMN notatsioonis

5.5 Järk 5 - funktsioonigruppide moodustamine mudelites

Järgnevalt pööran tähelepanu asjaolule, et mudelitel **Mudel 03** ja **Mudel 04** on elemendid jaotatud nelja funktsionaalsesse gruppi. Arvutitarkvara Camunda Modeler võimaldab gruppe markeerida, seetõttu Joonis 5 sisaldab **Mudeli 04** gruppe ilmutatult. Arvutitarkvara FMV tasuta versioon funktsioone gruppidesse koondada ei luba, seetõttu **Mudel 03** kasutab elementide eraldamiseks gruppidevahelist vaba ruumi. Kannan nelja grupi paigutuse FRAM mudelile **Mudel 03**, mida illustreerib skeem Joonisel 6.



Joonis 6. FRAM mudeli jaotus neljaks grupiks

Sellise jaotuse korral tekib neli funktsioonigruppi, tinglike nimedega *North*, *East*, *South* ja *West* (ingliskeelsed ilmakaarte nimetused). Gruppide tähendust analüüsin jaotises 5.7.

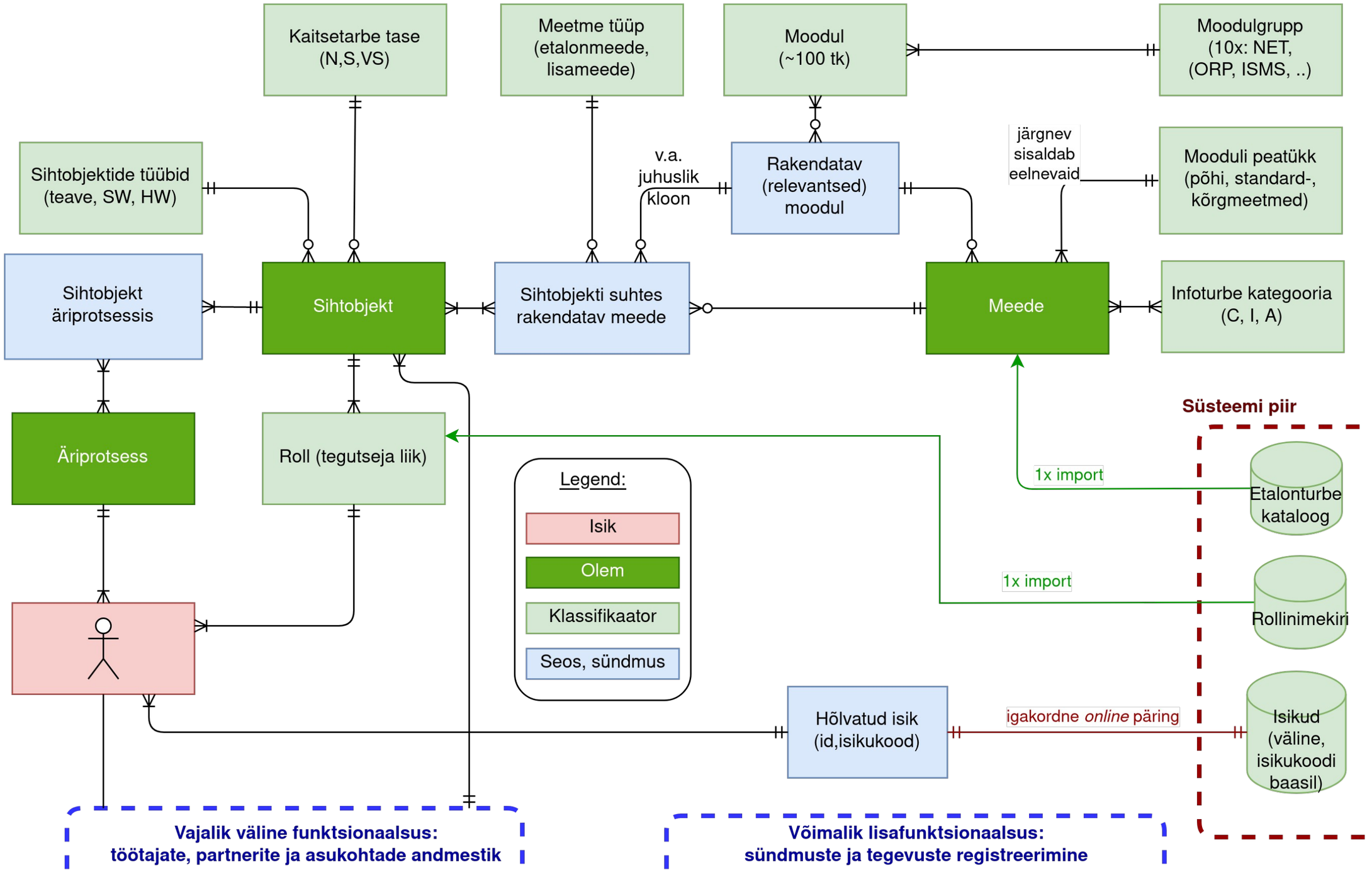
5.6 Järk 6 - andmemudeli koostamine

Hõlbustamaks potentsiaalse E-ITS tööriista disaini, koostan visandi selle võimalikust kontseptuaalsest andmemudelist. **Mudel 05** on esitatud Joonisel 7.

Andmemudel on hierarhia seisukohast ülilihtne. On vaid 3 (kolm) eset/asja ning vaid üks isik/tegutseja/tegija (*actor*). Tegija rolli liigitamisel pole protsessi õnnestumise seisukohast tähtsust, oluline on tegutseja tegelik kvalifikatsioon ja turvaaspekt. Organisatsiooni turve nõuab pääsuõiguste olemasolu ning seejärel tekib ka võimalus vastavust demonstreerida. Võtmeküsimuseks on tegutseja tegelik kvalifikatsioon ja arusaam probleemist, mida ta "tööriista" abil lahendama asub. Probleem seisneb asjaolus, et BSI poolt välja pakutud rollide nimekiri ([1] , "Rollisõnastik") tegija funktsiooni markeerimiseks ei sobi. Grundschutzi seisukohast on oluliseks seaduslikkus, pädevus, pääsuõigused ja vastavus ning roll defineeritakse just sellest vaatepunktist. Tegemist on kultuurilise nähtusega, mille senine eestindamisviis tuleb lugeda ebaõnnestunuks ja "tööriista" disaini otseselt komplitseerivaks. Skeemi lihtsuse huvides jätsin Mudelis 05 selle dilemma kajastamata.

Leid 14: BSI protsesside modelleerimisel tekivad raskused "rolli", "tegutseja" (*actor*) ning tegutsejalt nõutava kvalifikatsiooni eristamisel. Probleemi teadaolev lahendus on saksa bürokraatia, mis aga Eesti oludesse ei sobi.

Keerukus potentsiaalse tööriista loomisel seisneb minu arvates oluliselt mujal kui ärisõnastikus või ärireeglites. Nimelt, infoturbe või protsessi valideerimise küsimustes pole infosüsteemide analüüsimeetodid optimaalsed. Infoturbeküsimustes liigub hierarhiline tase fookuspõhimõttel üles-alla, mistõttu kõrvuti toimingutest üks (näiteks veebilehele sisenemine) võib paikneda väga ülemisel äritasemel kuid juba järgmine tehnilise disaini väga alumisel tasemel (võtmevahetus turvalise sidekanali püstitamiseks). Seevastu BPMN on äritaseme mudel, mis teostust ei käsitle, ning seetõttu jäävad analüütikul olulised detailid märkamata. Need ilmneksid ootamatusena alles implementatsiooni käigus. Minul infoturbeanalüütikuna on lihtsam kontseptuaalse ja loogilise mudeli vahelist piiri ignoreerida.



Joonis 7. Mudel 05 – valdkonna kontseptuaalmudel

5.7 Järk 7 - tuvastatud artefaktide vaatlus

Järgnevalt käsitlen funktsioonigruppe, mis tekkisid jaotises 5.5 sooritatud grupeerimise tagajärjel. Grupid tähistasin ingliskeelsete ilmakaarte nimetustega *South*, *East*, *South*, *West*. Analüüsin neis gruppides sooritatavat funktsionaalsust. Analüüsin FRAM mudelit (Joonis 3 ja Joonis 6) ja BPMN mudelit (Joonis 5) ühtse tervikuna.

Põhijäreldusena märgin, et IT Grundschutzi protsesside kirjeldamine üksnes BPMN mudeli ega üksnes FRAM mudeli abil ei tundu otstarbekas. IT Grundschutzi protsesside adekvaatseks kirjeldamiseks on kindlasti vaja kasutada segatehnoloogiat, mille puhul protsessi teatud osad (eelkõige eeldused – Leid 11 ja Leid 12 asjaolude tõttu – ning funktsionaalne grupp *East*) oleksid kirjeldatud FRAM-tehnoloogias, kuid ülejäänud osi (grupid *North*, *South* ja *West*) saab hõlpsasti kirjeldada hästituntud BPMN tehnoloogias. Järgnevalt analüüsin E-ITS tööriista võimalikku teostust ning grupeerin soovitused funktsioonigruppide *South*, *East*, *South*, *West* kaupa. Need soovitused kujutavad endast ühtlasi IT Grundschutzi protsesside ärianalüüsi ning on edaspidi kasutatavad standardi äriprotsessi parendamise alusmaterjalina.

5.7.1 Grupp *North* – juhtkonnategevused

ISMS käivitamise keerukus on väiksem kui tüüpilisel äriprotsessil. Tegemist on lihtsate toimingute kronoloogilis-põhjusliku jadaga, mille tagajärjel võtab juhtkond vastutuse asutuse infoturbe eest. Muud tulemid peale infoturvapoliitika (Grundschutzi kohustuslik dokument) on korralduslikud. Nõuded protsessigrupile tulenevad põhiosas vastavusnõuetest.

Arvutituge juhtkonnategevustele pigem ei vajata (piisab dokumendihaldussüsteemi olemasolust, mis avalikus sektoris eksisteerib *a priori*). Funktsioonigrupi arvutitoe teostusjärjekord saab seetõttu olla madala prioriteediga.

5.7.2 Grupp *West* – varade arvelevõtt

Protsessigrupp *West* kujutab endast mõne väga olulise andmestruktuuri järk-järgulist täitmist. Raskuspunkt on loendatavate esemete ontoloogial ja klassifikaatorite täpsusel.

Sihtobjektide tüpoloogia kinnist loetelu ei ole seni õnnestunud tuvastada, selle loomiseks infosüsteemi analüütikust ei piisa. Oluline on märkida, et IT Grundschutzi terminoloogia kohaselt, äriprotsess ei ole vara. Põhiprobleem avaldub asjaolus, et etalonturbe metoodika eeldab äriprotsesside eelnevat kaardistatust, see eeldus aga ei osutu Eesti avalikus sektoris sageli tõeseks. E-ITS ei õpeta äriprotsesse kaardistama, asutus peab abi hankima mujalt.

Leid 15: Etalonturbe üheks varjatud eelduseks on äriprotsesside kaardistatus. Äriprotsesside kaardistamine on olulise aja- ja tööjõukuluga tegevus, mis on aga paljudel asutustel sooritamata, seetõttu pidurdub etalonturbe rakendamine juba kohe alguses. Otstarbekas oleks siduda avaliku sektori äriprotsesside kaardistamine kvaliteedijuhtimise ning juhtimisküpsuse teemadega.

On selgeks vaidlemata, kas "teenus" on vara. Seeba artikli "Mis on äriprotsess ja mis on teenus" kohaselt (vt E-ITS portaal, sektsioon "koolitus ja KKK"), E-ITS ei tegele teenustega, ei loetle neid ega käsitle teenuste tagamist või teenusprotsesside korraldamist. Seetõttu puuduvad vastavad tegevused minu protsessimudelis.

Pole detailideni selge algoritm, mille abil suhtestada äriprotsesse esmase (kiiresti ja jämedalt hinnatud) kaitsetarbega. Veel pole selge, millise detailsusega täidab äripool esmase ligikaudse info põhjal neid E-ITS tööriista andmestruktuure, kuhu kogunevad äriprotsessiga seotud sihtobjektid. Küsimus on äriala ning IT-ala inimeste erinevas lähenemises. Minu hinnangul on kuulub kaitsetarbe esmane hindamine äripoole, mitte IT ülesannete hulka. Tööriista disain eeldab selgust äripoole kohustuste osas.

Inventuuri teeb keeruliseks asjaolu, et äriprotsessi kaitsetarve saab esmase hinnangu tema poolt vajatava teabe (andmeallika, andmekogu vms) kaitsetarbe alusel. Pole selge äriomaniku kvalifikatsioon andmeallikate tuvastamisel ja haldamisel (haldamata jätmine eiraks määrust "Infosüsteemide turvameetmete süsteem" [3]). Ent just esmane hinnang kaitsetarbele (lisaks äriprotsessi määratlemise kvaliteedile) paneb aluse inventuuri kvaliteedile ja hakkab hiljem mõjutama etalonturbe rakendamise üldist kvaliteeti.

Arvutitugi hoiab inventuuri protsessis aega kokku, kuid arvestades, et äriprotsesse on asutuses tüüpiliselt kuni paarikümmend, ei ole ajavõit märkimisväärne. Pigem on mõtet investeerida meeskonna kvalifikatsiooni.

5.7.3 Grupp *South* – meetmete haldus

Selle grupi toimingute äriloogika keerleb ümber vähese arvu ülioluliste andmestruktuuride, millessse kogutavat teavet järkjärgult väärindatakse läbi suure koguse hästidefineeritud protseduuride. Äriloogikale tuleb esitada mitmelõimelisuse (*multi-threading*) nõue, et protseduurid toimuksid konkurentselt ega lukustaks grupi *East* tegevusi. Näide: pärast seda kui näiteks kolm meedet tuhandest on tuvastatud ning sooritamata on isegi veel prioriteetimine, on tuvastatud meetmeid tegelikult juba võimalik rakendada. Puudub vajadus oodata kõigi meetmete kaardistamist ja sisustamist.

Leid 16: Andmestruktuuride lukustumine võib kaasa tuua järgnevate tegevuste pidurdumise. Juhul kui grupp *South* protseduurid pole õigesti (mitmelõimeliselt) projekteeritud, siis nad takistavad grupi *East* funktsioonide käivitumist. See toob kaasa põhjendamatu viivituse meetmete rakendamisel.

Arvutustabelil (näiteks Excel) ilma VBA pealisehituseta puudub mitmelõimelisus ning selle andmed pigem ei vastaks normaalkujule (loe: ei tagaks keerukaid seoseid).

Leid 17: Arvutustabeli perspektiivitus ISKE/ISMS tööriistana. Kirjeldan etalonturbe kontekstis põhjusi, miks arvutustabel ilma VBA vahenditeta ei sobi oluliste andmestruktuuride hoidmiseks: ülipikad nimekirjad, raskused korrektse andmedisainiga (1NF-3NF), mitmelõimelisuse puudumine. Samas on arvutustabel ainuke tehniline vahend, mida väikeettevõte on iseseisvalt võimeline välja töötama. Leid rõhutab ootusi kõigile soovijatele kättesaadava ja keskselt väljatöötatud tööriista järele.

Arvutitugi võimaldab grupi *South* toimingutes ajalist kokkuhoidu määral, mis minu hinnangul on mõõdetav inimkuudes. Arvutitoest ühtlasi oleneb, kas pädevusnõue (töötajate kvalifikatsioon) ja vastavusnõue (võime sooritatud tegevusi ka juhtkonnale ning audiitorile presenteerida) on tagatud.

Kontseptuaalmudeli olulisemad tabelid (vt jaotis 5.6 , Joonis 7) on: "Sihtobjekt äriprotsessis" ning "sihtobjekti suhtes rakendatav meede". Arvutitugi peab realiseerima järgmised kriitilised funktsioonid:

- klassifikaatorite ja pikkade nimekirjade haldamine – annab olulise ajavõidu. Süsteem haldab varasid, nende liike, parameetreid, seoseid, kuuluvust gruppidesse, kaitsetarvet jm parameetreid, allutatust konkreetsetele meetmele (vt joonisel 7 esitatud **Mudel 05**). Käsitsitöö on sellise mahu puhul minu hinnangul ebaoptimaalne ja ületab inimolendi suutlikkust;

- tugi äriprotsesside ja sihtobjektide suhtestamise toimingutele (tööalane jõupingutus koos ajakuluga);

- tugi meetmete ja sihtobjektide omavahelisele suhtestamisele (sama märkus);

- tugi meetmete teostusjärjekorrale ja prioriteetimisele.

Heal tasemel teostatud arvutitugi toetab vastavusnõuete haldamist (mida kirjeldab Seeba [34] ning võimaldab ellu viia nii etalonturbe kui ka ISMS protsesse.

Võimalikud probleemid. Osa meetmeid ja isegi mõned ORG ja ISM grupi moodulid moodulid rakenduvad tervele organisatsioonile, nii näiteks vajadus järgida mingit nõuet "igal töökohal". Sellise üldistuse tõlkimine infosüsteemile arusaadavaks on praktikas keeruline. Hindan, et automaatse toe pakkumine säärastele nõuetele on keeruline.

Leid 18: Moodulid gruppides ORP ja ISMS rakenduvad kogu organisatsioonile. Seega tuleb enne tööriista disaini alustamist sisustada üldsuskvantor.

IT Grundschutz ei esita meetmete omavahelise sõltuvuse tabelit (ajaline, põhjuslik). Osad sõltuvused tulenevad meetme semantikast (näide: Linuxi server, postiserver). Võimalik, et semantiliste sõltuvuste arvestust polegi võimalik automatiseerida.

Leid 19: Grundschutz ei esita meetmete omavahelise sõltuvuse tabelit (ajaline, põhjuslik), samast kui nende omavaheline prioriteetimine võib vajada asjakohast otsust. Lahendus sõltub sõnastuste semantikast ning seda ei pruugi üldse eksisteerida.

5.7.4 Grupp *East* – rakendamine, käitus, jätkupidevus

Funktsioonigrupi *East* tegevusi on otstarbekas noteerida pidevalt toimivate funktsioonidena (vt FRAM mudelite alane diskussioon eespool). Auditeerimist ja sertifitseerimist on otstarbekam käsitleda eraldi organisatsiooni põhiprotsessidest (nagu

Joonisel 5). BPMN notatsiooni koreograafiaelemendid annavad selleks võimaluse (vt **Mudel 04** Joonisel 5.

Arvutitugi on põhiliselt seotud vastavusnõuetega. Arvutitugi muudab vastavus-protsessid, sh auditeerimiseks valmistumise, oluliselt odavamaks (vt [34] lk 22, "Specification of the layer-based ISMS"). Otsustetugi ning kuluarvestus on pigem faktipõhine – säilitab ajatempliga varustatud vastused küsimustele "mis juhtus?", "kes tegi?", "mida tegi?". Vastav lisafunktsionaalsus viidatud kontseptuaalmudelil Joonisel 7.

5.7.5 Grupiväline funktsioon – alustamisviisi valik

Etalonturbe äriprotsessi elementi "alustamisviisi valik" on filosoofiliselt keeruline liigitada ükskõik millisesse neljast grupist. Tegemist on projekteerija praktilise otsusega.

5.8 Järk 9 – leiud

Esitan minu poolt analüüsi käigus tehtud leiud. Leiud puudutavad BSI IT Grundschutzi mudelit selle eestindatud variandis ning minu kui analüütiku tõlgenduses. Enamik leide on universaalsed nii Grundschutzi, ISKE kui E-ITS puhul, erisused on vajadusel käsitletud.

Leiud 20-23 on kirjeldatud jaotises Lisa 1 – Varased mudelid. Ülejäänud leiud on kirjeldatud töö põhiosas. Leiud on temaatiliselt grupeeritud. Leide saab kasutada järgnevaks analüüsiks, tööriista disainil ning ka metaäriprotsessi riskihalduse alusmaterjalina. Kasutamise hõlbustamiseks on tabelid markeeritud värviga.

Tabelisse 1 on koondatud leiud, mis käsitlevad etalonturbe ressursivajadust. Tabeli eesmärgiks on seada küsimuse alla vaikimisi ettekujutus või selle puudumine etalonturbe rakendamise kohta ning hõlbustada eelarvestamist ning planeerimist.

Tabel 1. Leidude koond – ressursivajadus

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 03	ISKE, rahastamine	3.2.1, lk 23	Kulutuste problemaatika kui üks ISKE läbi-töötamata aspekte.	Ebaselgus kulumudeli osas on asutustel takistanud ISKE rakendamist.
Leid 04	ISKE vs E ITS	3.2.1, lk 23	ISKE rakendub üksnes andmekogudele, E-ITS rakendub kogu asutusele (sh äriprotsessidele).	E-ITS protsessid on ISKE omast keerukamad, järelikult kulukamad.
Leid 05	ISKE, rahastamine	3.2.2, lk 25	ISKEl puudub kulutuste formaalne mudel.	Ebaselgus kulumudeli osas on asutustel takistanud ISKE rakendamist.
Leid 06	ISKE, E-ITS, infoturbejuht	3.2.2, lk 25	Infoturbejuht kui keskne ressurss mahuga 1850 töötundi aastas	Suure osa sellest võtab esmatutvus etalonturbe materjalidega. Selgitab, miks väiksemates asutustes jääb ISKE sageli rakendamata.
Leid 07	ISKE, E-ITS, infoturbejuht	3.2.2, lk 25	Infoturbejuht kui keskne ja kriitiline ressurss (*shared channel*)	Kriitiliselt koormatud ressurss aeglustab rakendamist väikses asutuses.
Leid 12	Etalonturve, rahastamine	5.2.1, lk 39	FRAM mudeli **Mudel 03** kohaselt on jätkusuutlik rahastamine etalonturbe vältimatu eeldus.	FRAM mudel osutab ressurssivajadusele otseselt.

Tabelisse 2 on koondatud leiud, mis puudutavad võimalikke korralduslikke probleeme. Need leiud pakuvad huvi eelkõige etalonturvet rakendavale asutusele. Leid 17 diskuteerib lihtsate tugivahendite kasutatavuse üle ning loodetavasti stimuleerib edasist diskussiooni etalonturbe universaalse tööriista võimalikkuse ja otstarbekuse üle.

Tabel 2. Leidude koond – korralduslikud probleemid

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 01	ISKE (Grundschutz)	3, lk 20	Tõlgitud infoturbealaste materjalide keeleline ja kultuuriline kvaliteet on tihti madal.	Paljud senised tõlke-materjalid, sh ISKE, on eestlasele raskesti mõistetavad.
Leid 11	E-ITS	5.2.1, lk 39	Töötajate kvalifikatsioon on BSI materjalide kohaselt peaaegu kõigi tegevuste eelduseks.	FRAM mudel osutab, et töötajate kvalifikatsiooni ebapiisavus blokeerib etalonturbe rakendamise.

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 15	E-ITS	5.7.2, lk 49	E-ITS etalonturbe varjatud eelduseks on äriprotsesside eelnev kaardistatus.	Enamikel asutustel on äriprotsessid kaardistamata, see pidurdab E-ITS rakendamist kohe alguses. Lisateemad: juhtimisküpsus, kvaliteedijuhtimine avalikus sektoris
Leid 17	ISKE, E-ITS	5.7.3, lk 51	Arvutustabeli (Excel) perspektiivitus ISKE/ISMS tööriistana (nimekirjade maht, andmedisaini normaalkuju eiramine, mitmelõimelisuse puudumine).	Väikeasutused vajavad keskselt väljatöötatud tööriista ega ole võimelised seda ise konstrueerima (ressursi puudumine, oskused).

Tabelisse 3 on koondatud leiud, mis kirjeldavad etalonturbe juhiste modelleerimisel tekkivaid funktsionaalseid keerukusi. Need leiud suunavad etalonturbe tööriista projekteerijat kohasemate analüüsistrateegiate ning projekteerimisvahendite valikule.

Tabel 3. Leidude koond – BSI etalonturbe mudeli iseärasused

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 02	Grundschutz, ISMS tööriist	3.1, lk 21	BSI eri standardites (200-1, 200-2) püstitatud korralduste ja nõuete agregeerimine ning ühtsesse hierarhilisse koondvaatesse ühendamine on komplitseeritud.	Protseduuride modelleerimine on keeruline. Võib ette näha keerukust ISMS tööriista disainil.
Leid 10	Grundschutz, E-ITS, ISMS tööriist	5.2, lk 36	BSI rollimudel ja rolli definitsioon lähtub vastavuse ja juriidilise vastutuse põhimõtetest.	UML / BPMN mudelite semantika kohaselt tegutseja (*actor*) mõiste tähendab hoopis muud. ISMS tööriista väära disaini risk.
Leid 14	Grundschutz, E-ITS, ISMS tööriist	5.6, lk 46	BSI protsesside modelleerimisel tekivad raskused "rolli", "tegutseja" (actor) ning tegutsejalt nõutava	Saksamaal on probleem lahendatud tugeva bürokraatiaga, mis aga Eesti oludesse ei sobi. Vigase äriloogika risk. ISMS tööriista

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
			kvalifikatsiooni eristamisel.	projekteerija ei tohiks "rolli" ja "tegutsejat samastada.
Leid 23	Grundschutz, ISMS tööriist	Lisa 1, lk 68	Liidestus kolme meetodi (etalonturve, ISMS, riskihaldus) vahel on möödapääsmatu.	Eesti oludes, väikeses asutuses, ei õnnestu neid teemasid jagada mitme osakonna vahel. Toetav tööriist peab olema ühtne, integreeritud.

Lõpuks, Tabelis 4 on ära toodud hajusad mitteilmsed faktoidid, milliste teadmisest võib analüütikul ja projekteerijal olla kasu nõuete väljatöötamisel ja tööriista projekteerimisel. Selles tabelis ei eristata etalonturbe tööriista ja ISMS tööriista.

Tabel 4. Leidude koond – ISMS tööriista arendust mõjutavad asjaolud

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 08	ISMS tööriist, etalonturbe tööriist	4.4, lk 30	Valideerimismudelite aeg on diskreetne, mitte reaalaeg nagu E-ITS tegevustel.	ISMS tööriist vajab disainimist reaalaja-süsteemina.
Leid 09	ISMS tööriist, etalonturbe tööriist	5.2, lk 36	IT Grundschutzi tegevustiku paljusid elemente on lihtsam ja loomulikum kirjeldada FRAMi funktsioonidena kui BPMN tegevustena.	Etalonturbe äriprotsessis on tegevusi, mille noteerimiseks sobib funktsioonipõhine FRAM oluliselt paremini kui tegevuse põhine BPMN.
Leid 13	Grundschutz, ISMS tööriist	5.3, lk 40	BSI tagasisidestamisnõude tõttu tekivad mudelisse lõimi lukustavad tsüklid.	Raskused mudeli valideerimisel, vajatakse mitmelõimelisuse lisanõuet tööriista disainil.
Leid 16	ISMS tööriist, etalonturbe tööriist	5.7.3, lk 51	Andmestruktuuride lukustumine võib kaasa tuua järgmiste tegevuste pidurdumise.	Keerukus ISMS tööriista disainil (vaja esitada mitme-lõimelisuse nõue). Meetmete halduse protseduurid ei tohi pidurdada meetmete. rakendamise tegevusi. Viivitusrisk E-ITS rakendamisel.
Leid 18	Grundschutz, ISMS tööriist, etalonturbe tööriist	5.7.3, lk 51	Moodulid gruppides ORP ja ISMS rakenduvad kogu organisatsioonile.	Infosüsteemide disaini faasis raskesti sisustatavad nõuded. On raske määratleda, mida "kõik" tähendab.

Leid	Kategooriad	Kirjeldatud jaotises	Kirjeldus	Tähendus
Leid 19	Grundschutz, ISMS tööriist, etalonturbe tööriist	5.7.3, lk 51	Grundschutz Kompendium ei esita meetmete omavahelise ajaliste või põhjuslike ristsõltuvuste tabelit.	Automaatsed võimalused ISMS tööriistas meetmeid ajaliselt reastada on piiratud.
Leid 20	Grundschutz, ISMS tööriist	Lisa 1, lk 68	Pole selge, millisesse kolmest meetodist (etalonturve, ISMS, riskihaldus) kuulub inventuur.	Disaini filosoofiline keerukus, raskused tööriista ühtsusega
Leid 21	Mõisted	Lisa 1, lk 68	Pole selge, kas äriprotsess on vara.	Kannatab enne tööriista disaini koostatava ärisõnastiku täpsus, ilmneb teostusvigade risk.
Leid 22	Grundschutz, ISMS tööriist	Lisa 1, lk 68	BSI protsessid on iteratiivsed, neil puudub formaalne lõpumarker.	Protsessimudelites on lõpumarker nõutud. Selle puudumine raskendab formaalset valideerimist.

Leidude kõrval võivad projekteerijale huvi pakkuda ka jaotises 3.3 loetletud kokkulepped, mis juba ongi oluliselt tõstnud E-ITS tekstide kvaliteeti.

6 Tulemused / Järeldused

Tööplaan nägi ette järgmised tulemid ja need on saavutatud:

- Standardi kahe põhijuhendiga määratletud protsess on kirjeldatud formaalse mudeli abil.
- Mudel on analüüsitud, tuvastatud piirangud ja puudujäägid.
- On antud soovitused standardi järgmiseks iteratsiooniks.

Lisaks on tekkinud koolituseks sobiv lisamaterjal

Uurimisküsimus UK1 – "millised on olnud teadaolevad probleemid ISKE rakendamisel" on analüüsitud ning leitud vastused süstematiseeritud.

Töö esialgne kava sisaldas küsitlusplaani ning küsitluse tulemuste analüüsimist. Konsultatsioonidel standardi omanikuga sain teada, et postiloendis korraldatud küsitluse vastused on mittestruktureeritud ning kõikuva kvaliteediga ning kuivõrd nad sisaldavad asutuste infoturbeinfot, ka ligipääsupiiranguga. Pärast arutelusid loobusin ka mõttest korraldada infoturbejuhtidele uus küsitlus, kuivõrd vahepeal E-ITS avaldati ning ISKE reaalsus on rakendajatel segunemas ootustega E-ITS suhtes. Selles olukorras küsitlus ei andnuks enam objektiivseid tulemusi.

Vastused uurimisküsimusele UK1 tuletasin Riigikontrolli aruannet lugedes, ISKEt puudutavate teadustöödega tutvudes ning omaenda mudeleid analüüsides. ISKEt puudutavad leiud on esitatud Tabelis 1 (ressursivajadus) ja Tabelis 2 (vajadus tööriista järele). Väikeasutus ei ole võimeline ise looma tõhusat arvutituge ISKE protsessidele.

Uurimisküsimuse UK2 – "kas E-ITS tegevustiku juhised ja korraldused moodustavad korrektse ning omavahel seotud süsteemi" – aluseks olevad asjaolud on analüüsitud ning vastatud. Etalonturbe ja ISMS tegevuste keerukus on märkimisväärne, juhised on esitatud täpsusega, mis on rakendajale arusaadavad, kuid modelleerimiseks ebapiisavad.

Eelkõige iseloomustavad seda probleemi Tabelis 3 esitatud leiud. Modelleerimise käigus tekkivad küsimused on keerulised, nõuavad filosoofilist lähenemist ning iseseisvaid otsusi. Minu hinnangul, protsessi mõningad osad vajavad tavalist äriprotsessi-põhist lähenemist, kuid ülejäänud osad funktsionaalsuse põhist lähenemist. Soovitan standardi omanikule selle aluseks oleva mudeli edasist formaliseerimist ning koostööd BSI-ga juurdepääsuks sealsetele mudelitele.

Uurimisküsimus UK3 – "millised nõuded tuleb esitada E-ITS tööriistale" – on analüüsitud ja vastused koondatud Tabelisse 4. Olen sinna kokku koondanud leiud, mis mõjutavad säärase tööriista disaini. Küsimusele vastamiseks tutvusin etalonturbesüsteeme käsitlevate teadustöödega ning analüüsisin loodud mudeleid.

Uurimishüpoteesi UH1 – "standardi rakendamisel väikeasutuses kulub aega ja ressursse otstarbekalt" – pole mul olemasolevate andmete põhjal võimalik ei kinnitada ega ümber lükata. Tabelisse 1 ja osalt ka Tabelisse 2 koondatud leidudest järeldub, et kulumudelit kui säärast pigem ei eksisteeri ning säärase konstrueerimist ei olnud ka selle töö käsitlusalas. Soovitan standardi omanikul teha jõupingutusi mudeli formaliseerimiseks. Ühtlasi peaks rakendajateni viima selge seisukoha, et kulumudeli vähene uuritus ei ole piisav põhjus rakendamise edasilükkamiseks.

Uurimishüpoteesi UH2 – "standardi rakendamise protsess on sisemiselt konsistentne, selles pole loogikavigu, rahuldamata sõltuvusi ega dokumenteerimata eeldusi" – loen tõeseks pisemate reservatsioonidega. Üksikud raskused on objektiivsed, tingitud põhiliselt keele- ja kultuurierinevustest. Avastasin, et BSI on etalonturbe, infoturbe halduse süsteemi ja riskihalduse metoodikad kokku sulatanud viisil, mida on objektiivselt väga keeruline modelleerida, peamiseks põhjuseks asjaolu, et funktsioonid ja tegevused paiknevad mudelis läbisegi. Tuvastasin, et sellest keerukusest võimaldab olulisel määral üle saada FRAM metoodika kaasamine analüüsi.

Uurimishüpoteesi UH3 – "standardi protsessi keerukus pole ülemäärane" pole mul võimalik tõeseks tunnistada. Kuigi standardi tekstis sisaldub nii minu enda kui ka standardi omaniku arvukaid lihtsustusi, leidub keerukuses endiselt vähendamis-potentsiaali, millega standardi omanik saab jätkuvalt tegeleda. Enamikel juhtudel puudub vajadus tegeliku keerukuse vähendamiseks, kuid optimeerida tuleb kirjeldusi ja esitusmetoodikat. Minu järeldusel standardi protsess juba ongi oma hierarhilisuse ja

sisseviidud kultuurikohanduste tõttu (vt jaotis 3.3) rakendajale oluliselt mõistetavam ja mugavam kui ISKE protsess.

6.1 Tagasivaade töö käigule

Väga iseloomulikult meid ümbritsevale reaalsele maailmale ei realiseerunud esialgne tööplaan ning pidin seda käigult modifitseerima. Tööd planeerides võtsin riski, mis seisnes Eestis tundmatu metoodika – FRAM – kasutamises põhimeetodina. See risk realiseerus, sest alles töö käigus selgusid FRAM meetodi tegelikud piirangud. Kuid just FRAM-metoodika kasutamine andis võtme teatud tüüpi keerukuse tuvastamiseks standardi protsessides. Pärast keerukuse asjaolude tuvastamist (protseduuride ja funktsioonide kasutamine vaheldumisi, lõputud tsüklid, varjatud sõltuvused) osutus võimalikuks naasta klassikalise ärianalüüsi meetodite juurde. Töös kasutasin mudeli loomiseks paralleelselt FRAM ja BPMN notatsioone ning need täiendavad teineteist.

7 Soovitused

Soovitused on suunatud eelkõige standardi omanikule (RIA) ja valdkonna koordinaatorile (MKM). Tehtud töö põhjal saan soovitada järgmisi tegevusi.

- Uurida ISKE ja E-ITS tegelikku efektiivsust. Otsida tõestust hüpoteesile, et etalonturbe rakendamine vähendab infoturbeintsidentide arvu asutuses.
- Teaduslikult uurida keele- ja kultuuriprobleeme tehnikakirjanduse tõlkimisel. Koostöös Eesti keele instituudiga töötada välja metoodika tehniliselt keeruliste lõpptekstide tegeliku loetavuse ja arusaadavuse automaathindamiseks.
- Luua infoturbestandardi rakendamise kulumudel ning selle põhjal tuletada reaalselt vajalik eelarveline kate (töötundide arv, nõutav kvalifikatsioon) asutuse kohta eeldusel, et tegevusi automatiseeriv tööriist on loodud ning ka ilma selleta.
- Uurida võimalust BSI'lt standardite BS 200-1 ja 200-2 (ka valmiva 200-4) protsessi formaalsete alusmudelite hankimiseks. Alternatiivina sooritada mudelite pöördkonstrueerimine täisteksti põhjal, nagu on tehtud minu töös.
- Võtta sõnavarasse sotsiotehnilise süsteemi mõiste, mis võimaldab mehhaanilisi protseduure eristada inimtööjõule omasematest tööfunktsioonidest. Arvestada neid erisusi standardi protsesside mudeli koostamisel ja tööriista väljatöötlusel.
- Formaliseeritud kujul hallata Eesti standardi protsessidesse sisseviidud erinevusi võrreldes BSI mudeliga (hetkel tuumikuturve, auditeerimisprotseduur jne).
- Ette näha mudeli formaalne verifitseerimine. Selle eel tuleks mudel teisendada matemaatiliselt täpsele kujule, näiteks mingit tüüpi Petri võrguks (CPN).
- Fikseerida väljendi "E-ITS tööriist" semantiline ja tehniline tähendus.
- Algatada standardi rakendustegevusi automatiseeriva tööriista väljatöötlus. Eelinfona saab arvestada jaotises 5.8 kirjeldatud piiranguid ja iseärasusi.

8 Kokkuvõte

Töö eesmärgiks oli evalveerida Eesti Infoturbestandardi (E-ITS) protsesse, mida pole varem formaalselt kirjeldatud ega mudeli põhjal analüüsitud. Uurisin, millised on etalonturbe senise standardi (raamistiku) ISKE tegelikud ja oletatavad puudused, hindasin standardi põhiprotseduuride korrektsust ning uurisin etalonturbe tööriistadele esitatavaid nõudeid, eeldusi ja piiranguid.

Töö käigus tõlkisin standardi põhiliste protsesside sõnalised juhised mudeli kujule ning analüüsisin seda mudelit. Koostasin mudeli kahes erinevas tehnoloogias, BPMN notatsioonis ja FRAM notatsioonis. Esitasin valdkonna kontseptuaalse analüüsi ERD skeemi kujul. Analüüsisin mudelist tulenevaid järeldusi, millel on tähendus nii avaliku sektori asutustes kohustuslikule turvalisuse meta-äriprotsessile kui ka potentsiaalse etalonturbe tööriista disainile.

Dokumenteerisin standardi arenduse käigus saavutatud olulised kokkulepped, mis näitavad, millised eelmise standardi (ISKE) probleemidest uus standard (E-ITS) lahendab. Dokumenteerisin analüüsi käigus tehtud 22 leidu. Oma analüüsi põhjal andsin soovitused standardi omanikule. Jõudsin järeldusele, et standardi täisteksti edasine uurimine teaduslike meetoditega on perspektiivne ja vajalik arengusuund.

Seos töö ülesande ja tulemuse vahel moodustus mittelineaarselt, sündmusjuhitava tegevuse käigus, lateraalse mõtlemistehnika (de Bono [50]) abil. Oluliste tulemusteni jõudsin Eestis seni vähetuntud FRAM-metoodikat kaasates.

Kasutatud kirjandus

[1] Eesti infoturbestandard, portaal [Võrguressurss] https://eits.ria.ee/ (Külastatud: 17.05.21)

[2] Majandus- ja kommunikatsiooniministeerium, Küberturvalisuse Strateegia 2019-2022 (avalik versioon) [Võrguressurss] https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (Külastatud: 17.05.21)

[3] Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ muutmine [Võrguressurss] https://www.riigiteataja.ee/akt/115092020012 (Külastatud: 17.05.21)

[4] MKM pressiteade 14.09.2020 : "Laieneb riigi infosüsteemi kuuluvate andmekogude turvalisuse tagamiseks lubatud infoturbestandardite ring." [Võrguressurss] https://www.mkm.ee/et/uudised/riigi-infosusteem-teeb-suuri-samme-rahvusvahelise-koostoo-edendamiseks (Külastatud: 17.05.21)

[5] Riigihangete portaal, riigihange nr 203534 „Eesti infoturbestandardi väljatöötamine”, 2019 [Võrguressurss] https://riigihanked.riik.ee/rhr-web/#/procurement/1535697/general-info (Külastatud: 17.05.21)

[6] Pekka Himanen "Häkkerieetika ja informatsiooniajastu vaim", tõlge eesti keelde, Tallinn, Kunst, 2003. ISBN: 9949-407-00-1

[7] [EKSS] "Eesti keele seletav sõnaraamat" 2009 [Võrguressurss] http://eki.ee/dict/ekss/index.cgi?Q=evalveerima (Külastatud: 29.04.2021)

[8] Bundesamt für Sicherheit in der Informationstechnik, BSI IT Grundschutz [Võrguressurss] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (Külastatud: 17.05.21)

[9] BSI, "Alternative -Grundschutz-Tools", [Võrguressurss] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/alternative-it-grundschutztools_node.html (29.04.2021)

[10] EU hanke aruanne "ISKE tööriista arendamine", Riigihange nr 163923, 2015 [Võrguressurss] https://www.mercell.com/nb-no/anbud/52074243/eu-hanke-aruanne-iske-tooriista-arendamine-anbud.aspx (Külastatud: 17.05.21)

[11] RIA presentatsioon "Infopäev 2016-06-03", [Võrguressurss] http://kov.riik.ee/wp-content/uploads/2016/07/3.-juuni-2016-Infop%C3%A4ev-01-ISKE-n%C3%B5uded.pdf (Külastatud: 17.05.21)

[12] Eesti infoturbestandard, "ISMS nõuded" [Võrguressurss] https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/isms-noouded/ (Külastatud: 17.05.21)

[13] Eesti infoturbestandard, "Rakendusjuhend" [Võrguressurss] https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/rakendusjuhend/ (Külastatud: 17.05.21)

[14] Eesti infoturbestandard, "Riskihaldusjuhend" [Võrguressurss] https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/riskihaldusjuhend/ (Külastatud: 17.05.21)

[15] Shirazi, Mohammad Reza & Jaferian, Pooya & Elahi, Golnaz & Baghi, Hamidreza & Sadeghian, Babak. (2005). RUPSec: An Extension on RUP for Developing Secure Systems - Requirements Discipline. 208-212. [Võrguressurss] https://www.researchgate.net/publication/221017730_RUPSec_An_Extension_on_RUP_for_Developing_Secure_Systems_-_Requirements_Discipline/ (Külastatud: 17.05.21)

[16] Open Security Architecture, veebisait, artikkel "IT Security Requirements" [Võrguressurss] https://www.opensecurityarchitecture.org/cms/definitions/it_security_requirements (Külastatud: 17.05.21)

[17] Estonia ranks fifth in the global cybersecurity index [Võrguressurss] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx (Külastatud: 29.04.2021)

[18] Nicholas L.K. Tar. 2017.When Cyber Systems Crash: Attitudes Towards Cyber Utilization And Security.Doctoral dissertation. NovaSoutheastern University. Retrieved from NSUWorks, College of Arts, Humanities and Social Sciences – Department of ConflictResolution Studies. (69) [Võrguressurss] https://nsuworks.nova.edu/shss_dcar_etd/69 (Külastatud: 29.04.2021)

[19] Erik Hollnagel, FRAM - the Functional Resonance Analysis Method : modelling complex socio-technical systems. Ashgate 2012, ISBN: 978-1-4094-4551-7

[20] Eesti standardimis- ja akrediteerimiskeskus, standard ISO/IEC 27001:2017 [Võrguressurss] https://www.iso.org/isoiec-27001-information-security.html (Külastatud: 17.05.21)

[21] The Japanese Center for Financial industry information systems (FISC), FISC security guidelines [Võrguressurss] https://www.fisc.or.jp/english/ (Külastatud: 17.05.21)

[22] ISKE juhendid ja materjalid, Riigi infosüsteemi amet [Võrguressurss] https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html (Külastatud: 17.05.21)

[23] Wikipedia, artikkel "Register (keeleteadus)" [Võrguressurss] https://et.wikipedia.org/wiki/Register_(keeleteadus) (Külastatud: 17.05.21)

[24] Svitlana Lyubymova, jt, On Lacunarity in Translation of Culture Specific Concepts, 2018 [Võrguressurss] https://www.uco.es/ucopress/ojs/index.php/tl/article/download/11033/10143/ (Külastatud: 27.04.21)

[25] John Bumgarner; Scott Borg; US-CCU küberturbe kontroll-küsimustik, 2007 [Võrguressurss] https://www.ria.ee/sites/default/files/content-editors/KIIK/us_ccu_kontrollkusimustik_081211.pdf (Külastatud: 17.05.21)

[26] Center for Internet Security, CIS-meetmed, versioon 7.1, 2019 [Võrguressurss] https://www.ria.ee/sites/default/files/content-editors/kuberturve/cis20_meedet_eesti_keeles.pdf (Külastatud: 17.05.21)

[27] Bundesamt für Sicherheit in der Informationstechnik, Historie des BSI [Võrguressurss] https://www.bsi.bund.de/DE/Das-BSI/BSI-Historie/bsi-historie_node.html (Külastatud: 17.05.21)

[28] Wikipedia, artikkel "BSI Group" [Võrguressurss] https://en.wikipedia.org/wiki/BSI_Group (Külastatud: 17.05.21)

[29] Wikipedia, artikkel "IT Grundschutz" [Võrguressurss] https://de.wikipedia.org/wiki/IT-Grundschutz (Külastatud: 17.05.21)

[30] Rahandusministeerium, avaliku sektori asutused, asutuste liikide lõikes[Võrguressurss] https://www.rahandusministeerium.ee/sites/default/files/avaliku_sektori_asutused_asutuse_liikide_loikes_.xlsx (Külastatud: 17.05.21)

[31] Riigi infosüsteemi amet, tüvitekst, ISKE üldvaade [Võrguressurss] https://www.ria.ee/et/kuberturvalisus/infosusteemide-turvameetmete-susteem-iske.html (Külastatud: 17.05.21)

[32] Buldas, A., Oit, M., Praust, V.: Turvaklasside kirjeldused. Tehniline aruanne. Dok. DO–X-09-0498. Küberneetika AS (1998)

[33] Hanson, V., Praust, V., Infosüsteemide turbe etalonmeetmete süsteemi koostamine. Aruanne. Dok. CY-AA-A-054-031029. Cybernetica AS (2003)

[34] Mari Seeba, magistritöö, Infoturbe halduse tööriista spetsifikatsioon rakendamiseks töövoohalduse platvormil, ingl.k., 2019 [Võrguressurss] https://dspace.ut.ee/handle/10062/66393 (Külastatud: 17.05.21)

[35] Armin Berlin "See seaduslik ebaseaduslik info…", ajakiri Luup 1998, nr. 21, lk. 44–47

[36] Riigi Teataja, "Infosüsteemide turvameetmete süsteemi kehtestamine" [Võrguressurss] https://www.riigiteataja.ee/akt/791875 (Külastatud: 17.05.21)

[37] Jüri Kivimaa, doktoritöö, A cost optimizing model for IT security, 2013 [Võrguressurss] https://www.ester.ee/record=b3004315~S1*est (Külastatud: 17.05.21)

[38] Riigikontrolli aruanne Riigikogule "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes", Tallinn, 5. juuni 2018 [Võrguressurss] https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2466&FileId=14236 (Külastatud: 17.05.21)

[39] Roope Rafael Elojärvi, "Maailmanpylväs Rovaniemelle - Tornisuunnitelma", Diplomityo - Arkkitehtuurin kolutusohjelma, 2014 [Võrguressurss] https://et.wikipedia.org/wiki/Sampo (Külastatud: 29.04.2021)

[40] Charles Perrow, Normal Accidents: Living with High-Risk Technologies. Revised Edition, Princeton University Press, 1999. ISBN-13: 978-0691004129

[41] James L. Peterson, Petri Net Theory and the Modelling of Systems, Prentice-Hall, Englewood Cliffs, New Jersey, (April 1981), Chapter 7, Figure 7.4 "The buffered producer/consumer with a shared channel." [Võrguressurss] http://jklp.org/profession/books/pn/7.html (Külastatud: 17.05.21)

[42] Mati Erelt, Tiiu Erelt, Kristiina Ross, Eesti keele käsiraamat, 2007, "Moodustajate semantilised ja pragmaatilised funktsioonid" [Võrguressurss] http://www.eki.ee/books/ekk09/index.php?id=359&p=5&p1=1 (Külastatud: 17.05.21)

[43] Norbert Wiener, Küberneetika ehk juhtimine ja side loomas ning masinas, Eesti Riiklik Kirjastus, Tallinn, 1961

[44] Ron Ojava, magistritöö, Simulatsiooni abil kontrollitud BPMN standardi protsessimustrid õppenäidetena, 2017 [Võrguressurss] https://digikogu.taltech.ee/et/Download/d91545fd-08db-4651-a113-e719b21b537f (Külastatud: 17.05.21)

[45] C. A. Petri, Ph.D. Dissertation: ”Kommunikation mit Automaten.” , Institut für Instrumentelle Mathematik, Bonn, 1962 [Võrguressurss] https://edoc.sub.uni-hamburg.de/informatik/volltexte/2011/160/ (Külastatud: 17.05.21)

[46] Andreas Cappell, karikatuur „Project Management” [Võrguressurss] https://www.flickr.com/photos/cappellmeister/5921913 (Külastatud: 17.05.21)

[47] Erik Hollnagel, tarkvara FRAM Model Interpreter (FMI) kasutusjuhend, 28/07/2020 [Võrguressurss] https://functionalresonance.com/onewebmedia/FMI%20basicPlus%20V3.pdf (Külastatud: 17.05.21)

[48] FRAM-meetodi infosait [Võrguressurss] https://functionalresonance.com/ (Külastatud: 17.05.21)

[49] The Functional Resonance Analysis Method, metoodiline juhendmaterjal, A brief Guide on how to use the FRAM, Erik Hollnagel, 6/1/2018, [Võrguressurss] https://functionalresonance.com/onewebmedia/Manual%20ds%201.docx.pdf (Külastatud: 17.05.21)

[50] de Bono, Edward. (1970). Lateral thinking: Creativity step by step. NY: Harper & Row, ISBN-10: 0141938315

[51] Erik Hollnagel; Jeanette Hounsgaard; Lacey Colligan; FRAM– the Functional Resonance Analysis Method, a handbook, 2014 [Võrguressurss] - https://functionalresonance.com/onewebmedia/FRAM_handbook_web-2.pdf (Külastatud: 17.05.21)

[52] Stråls säkerhets myndigheten, Erik Hollnagel, uurimus, An Application of the Functional Resonance Analysis Method (FRAM)to Risk Assessment of Organisational Change, 2013 [Võrguressurss] https://inis.iaea.org/collection/NCLCollectionStore/_Public/44/057/44057156.pdf (Külastatud: 17.05.21)

[53] Erik Hollnagel, Safety-II in Practice, ISBN-13: 9781138708921, Appendix "A FRAM Primer", 2017 [Võrguressurss] https://functionalresonance.com/onewebmedia/FRAM%20Primer.pdf (Külastatud: 17.05.21)

[54] Wikipedia, artikkel "BPMN" [Võrguressurss] https://et.wikipedia.org/wiki/BPMN (Külastatud: 17.05.21)

[55] Martin Fowler, „UMLi kontsentraat: objektmodelleerimise standardkeele UML 2.0 lühijuhend : 3. redaktsioon”, Cybernetica, 2007, ISBN-10: 9949153360, [Võrguressurss] https://www.kriso.ee/umli-kontsentraat-objektmodelleerimise-standardkeele-uml-20-db-9789949153367.html (Külastatud: 17.05.21)

[56] Askdifference portaal, kirje: Purpose vs. Function - What's the difference?, 07.05.2020 [Võrguressurss] https://www.askdifference.com/purpose-vs-function/ (Külastatud: 17.05.21)

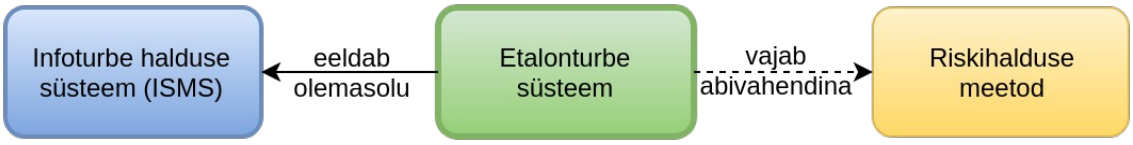
[57] Tarkvara FRAM Model Visualiser (FMV) kasutusjuhend, ver 2.1, 2020 [Võrguressurss] https://functionalresonance.com/onewebmedia/FMV_instructions_0.4.0.pdf (Külastatud: 17.05.21)

[58] Tarkvara FMV allalaadimiskoht, versioon 2.1 [Võrguressurss] http://zerprize.co.nz/FRAM/index.html (Külastatud: 17.05.21)

[59] Tarkvara FMI allalaadimiskoht, versioon 12.07.2019 [WWW] https://functionalresonance.com/onewebmedia/FMI_BasicPlus_Windows.zip (Külastatud: 17.05.21)

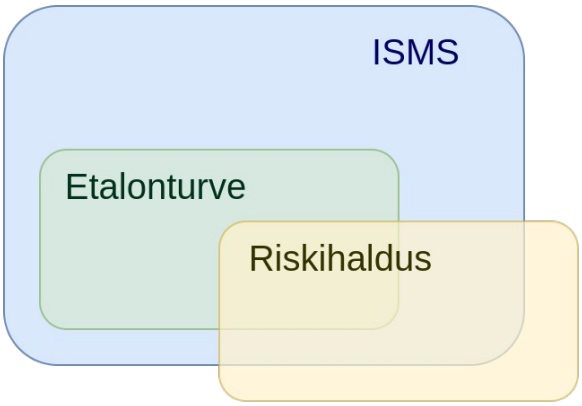
Lisa 1 – Varased mudelid

2020. aastal koostasin 2019. aasta IT Grundschutzi põhjal mõned selgitavad skeemid, mis hõlbustasid standardi koostajate omavahelist kommunikatsiooni ning ning andsid vastuse BSI kolme meetodi (riskihaldus, etalonturve, ISMS) omavaheliste suhete kohta. Neid suhteid on kujutatud joonistel L1_Joonis 1 (**Mudel A**) ning L1_Joonis 2 (**Mudel B**).



L1_Joonis 1. Mudel A – Etalonturbe välised seosed

Ei õnnestunud tuvastada, kuidas paigutuvad kolm meetodit omavahel hierarhiasse või kas tähtsaim neist (eeldatavalt riskihaldus vs etalonturve) paikneb hierarhia tipus. L1_Joonis 2 väljendab seisukohta, et etalonturvet saab käsitleda ühe alamosana infoturbe halduse süsteemist. Seevastu riskihaldus kujutab endast oluliselt laiemat distsipliini, hõlmates aspekte, mida ei kata ei etalonturve ega ISMS. Võimatus BSI protseduure hierarhiliselt normaliseerida on oluline järeldus, millel põhinevad E-ITS mitmed hilisemad otsused ning ühtlasi Leid 20.



L1_Joonis 2. Mudel B – kolme meetodi omavaheline suhe

Leid 20: Pole selge, millise meetodi koosseisu kolmest – riskihaldus, etalonturve, ISMS – kuulub inventuur. Varade arvelevõtmist nõuavad kõik kolm meetodit, ning protsesside hierarhiliseks kujutamiseks tuleks tuvastada inventuuri täpne koht protsessis.

Välistasin dilemma otsusega, et inventuur paikneb sõltumatult, eraldi, olles neljas meetod, mida vajadusel välja kutsutakse. Tegu on hierarhiaprobleemiga, BSI'l pole õnnestunud kolme meetodit ühte hierarhiasse sulatada. Lisaks selgus, et BSI materjalid ei anna konkreetset vastust küsimusele, kas äriprotsess on vara.

Leid 21: Pole selge, kas äriprotsess on vara. Eeldame, et ei ole. Otsus mõjutab ISKE tööriista disaini.

Ülevaade E-ITS protsessidest

Lisas 1 kirjeldatud mudelid pärinevad perioodist, kui standardi lõppversioon ei olnud veel valminud. Rakendusjuhendi hetkeversioon [13] defineerib rakendajale kohustuslikud kaheksa peamist sammu jaotistes 8-10, sealsel Joonisel 7. Siinses analüüsis vajame varasema versiooni detaile - minu mudelis oli sammude arv suurem.

Vajadus mudeli järgi tulenes asjaolust, et formaliseeritud mudelit (XML, graaf) ei eksiteerinud teadaolevalt ei Grundschutzi ega ISKE tarbeks. Asjaolu, et mudel (pisut muudetud kujul) on standardi koosseisus, osutab vajadusele säärase mudeli järele.

Järgnevate mudelite käsitlusala piirasin dokumentidega "ISMS nõuded" ja "Rakendus-juhend". Need dokumendid sisaldavad korralduslikke protsesse, mis on ühised igale rakendavale asutusele. Mõningad kontseptsioonid varases mudelis peegeldavad BSI algse mudeli idiosünkraasiat (auditeerimine enne sertifitseerimist) ning on E-ITS lõplikus versioonis lahendatud teisiti.

Mudelid on üles tähendatud BPMN-notatsioonile lähedases lihtsustatud notatsioonis. Käsitlesin mudelist väljaspool asuvana asutusespetsiifilist osa:

- konkreetse asutuse äriprotsessid (loetelu v kirjeldus);
- konkreetse asutuse varad (E-ITS terminoloogias: sihtobjektid, nende nimekiri);

- konkreetsed moodulid, mis modelleerimise käigus tunnistatakse asjakohaseks;
- konkreetsed modelleerimise käigus määratud infoturvameetmed;
- rakendamise võimalik ajakava.

Rakendusjuhend

Mudel C on tuletatud sõnalistest protsessijuhistest ning seda kujutab L1_Joonis 3. Infoturbe abitegevusi (koolitus, intsidendihaldus) pole kujutatud, kuivõrd neid reguleerivad teised, praegusest fookusest väljapoole jäävad juhendid.

Leid 22: BSI protsessid on iteratiivsed, neil puudub formaalne lõpumarker. See tekitab probleeme mudeli valideerimisel.

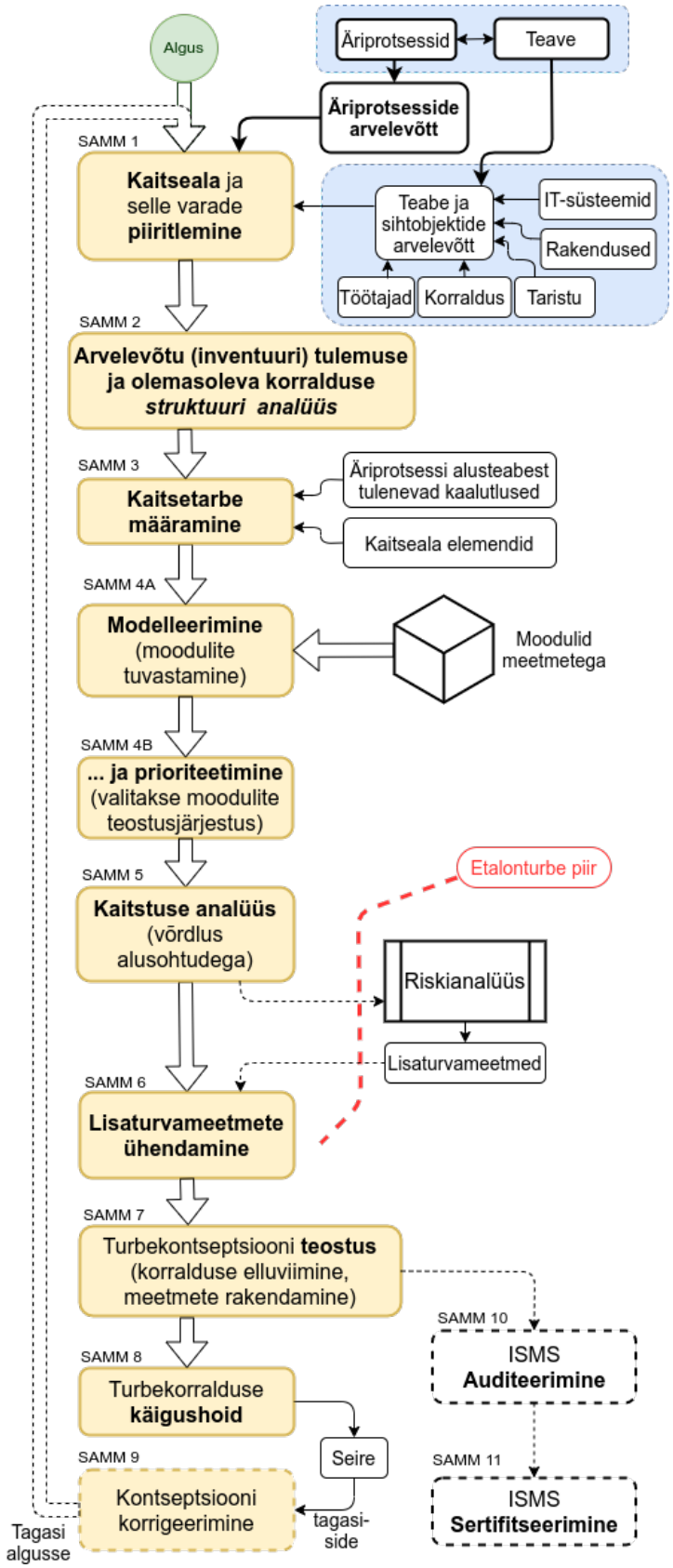
L1_Joonis 3 esitab **Mudeli C**, millel vastavuses BSI protsessiga puudub LÕPP.

ISMS nõuded

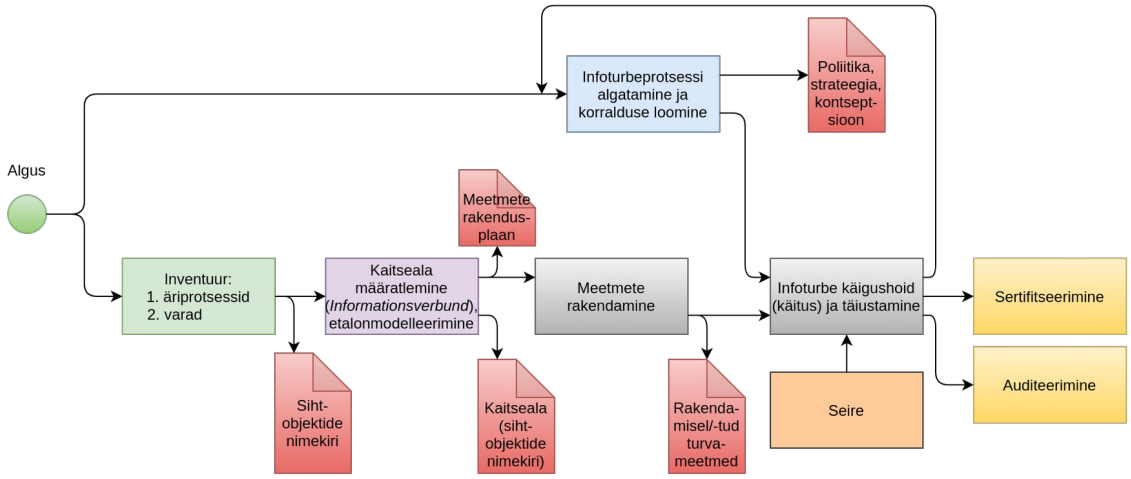
BSI tarvitab standardite näiva keerukuse langetamiseks meetodit, mille kohaselt eri allüksuste/osakondade poolt sooritatavad tegevused on lahutatud erinevateks standarditeks. Samas, IT Grundschutzi juhendid ei ole sõltumatud. Kuigi standard BSI 200-1 on etalonturbest suhteliselt iseseisev ning korraldab terve hulga tegevusi infoturbe haldussüsteemi käivitamiseks ja käituseks, esineb puhutisi otseseid puuteid etalonturbe protsessiga. Kaudne puutumus leiab aset ka läbi ORG moodulgrupi moodulite, seda aspekt jääb hetkel vaatluse alt välja.

Leid 23: Liidestus kolme meetodi (etalonturve, ISMS, riskihaldus) vahel on möödapääsmatu.

L1_Joonis 4 kujutab **Mudelit D** ning esitab ühtse, väga lihtsustatud, algajale sobiva ning enamikest detailidest abstraheeruva vaate ISMS Nõuete ning Rakendusjuhendi kaksikprotsessi (etalonturve+ISMS) ülevaatejoonisena. Kokkupuutepunktideks on inventuur ja käitus. Lõpumarker puudub ka joonisel L1_Joonis 5. BSI ettekujutuse kohaselt, pärast teatava infoturbetaseme saavutamist "tuleb minna järgmisele ringile".



L1_Joonis 3. Mudel C – Rakendusjuhendi protsessi ülevaade (autori varane versioon)



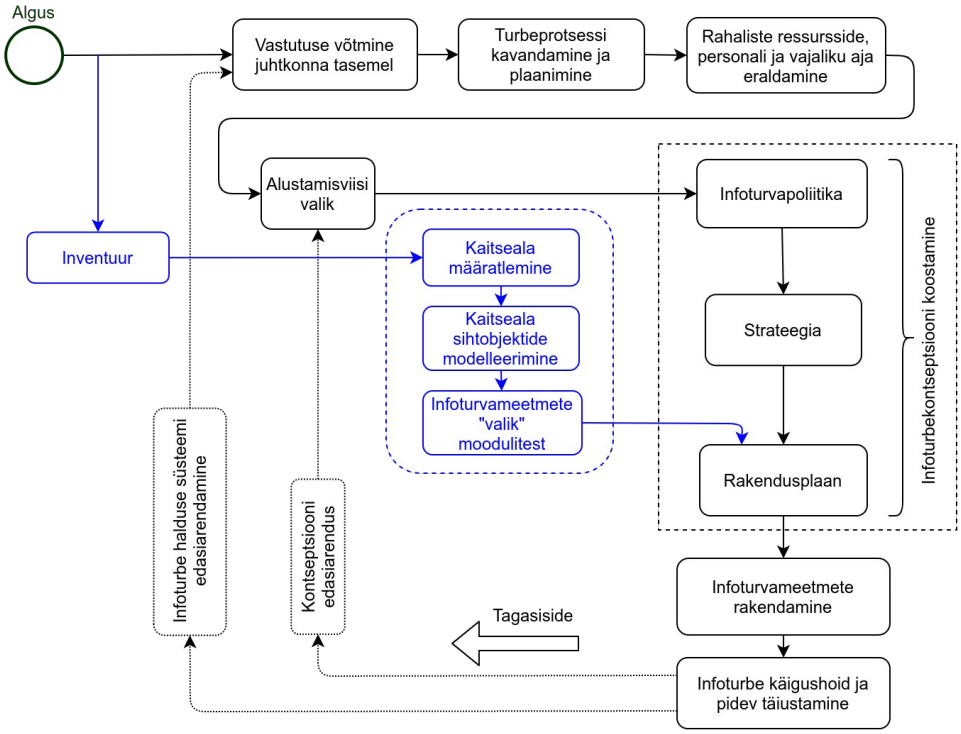
L1_Joonis 4. Mudel D – etalonturbe ja ISMS kaksikprotsess

Eesti oludes, väikeses asutuses, ei õnnestu nõuete ja rakenduse teemasid mitme osakonna vahel jagada. Toetav tööriist peab olema ühtne, integreeritud.

Kuivõrd sertifitseeritakse ja auditeeritakse infoturbe halduse süsteemi ja mitte rakendatud meetmekomplekti, siis sertifitseerimise ja auditeerimise tegevusi võib lugeda pigem ISMS kui etalonturbe tegevusteks (hiljem olen jõudnud seisukohale, et need asuvad üldse väljaspool põhiprotsessi). Neid samme pole otstarbekas protseduurimudelist välja jätta, muidu kaob rakendajal siht ja stiimul.

Osutamaks ISMS ja etalonturbe kaksikprotseduuri keerukusele, koostasin **Mudeli E**. See lõppkasutajale orienteeritud skeem kasutab lihtsustatud BPMN notatsiooni ning on standardi vastava joonise ([13] , joonis 8) aluseks.

Mudelit E kujutab L1_Joonis 5. Skeem võimaldab defineerida ISMS protsessi (värvitud mustaks) ja rakendusjuhendi (värvitud siniseks) samm-sammuliste protseduuride liidespunktid ning vaadelda E-ITS protsessi ühtse tervikuna. Sel mudelil on inventuur katseliselt paigutatud etalonturbe kossseisu.



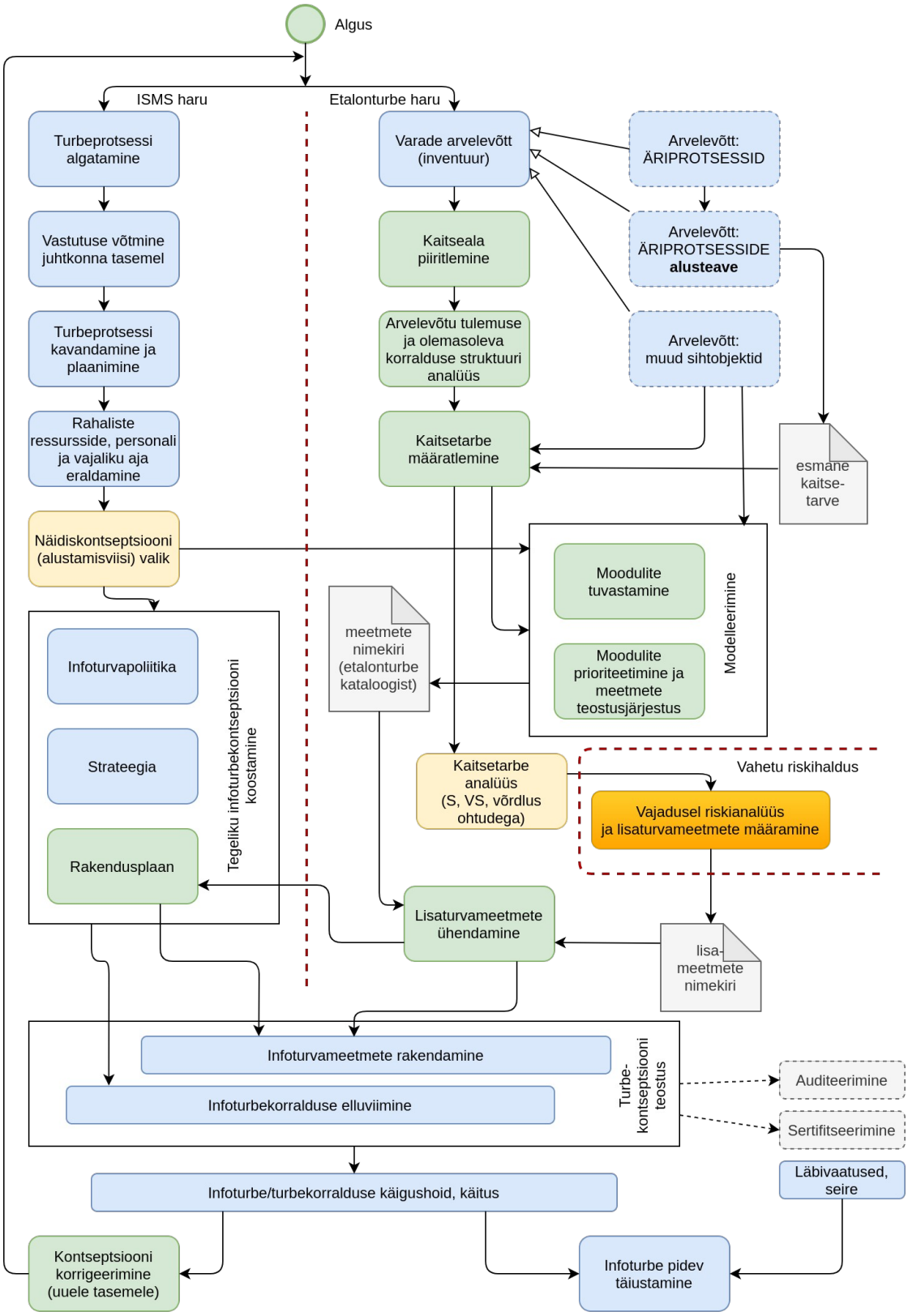
L1_Joonis 5. Mudel E – etalonturbe ja ISMS metoodika sulandumine

Viimase varase mudelina (**Mudel F**) on joonisel L1_Joonis 6 tegevustiku täielik skeem See katab ISMS nõuded (BSI 200-1) ja etalonturbe rakendusjuhendi (BSI 200-2) ning osutab liidestusele riskihalduse (BSI 200-3) protsessiga.

L1_Joonis 6 kasutab BPMN-lähedast notatsiooni ning sisaldab kokku 28 tegevust (tegevusgruppe loetlemata) ning näitab tegevustiku suurt keerukust. Olen ilmutatult kujutanud kolm vahetulemust, tegelikkuses on neid rohkem. Sel joonisel kujutatu ongi E-ITS protseduuri **originaal**, mida kasutan diplomitöös analüüsi sisendina. Skeem valmis väljaspool standardi loomise töid.

L1_Joonis 6 eraldab kolm meetodit (ISMS, etalonturve, riskihaldus) punaste punktiirjoontega. Inventuur on kujutatud etalonturbeprotsessi osana kaalutlusel, et andmestik on neil ühine. Endiselt puudub protsessil lõpumarker.

Selles lisas esitatud mudelid olid vajalikud BSI IT Grundschutz protsessiga seotud esialgse keerukuse sujuvaks ületamiseks ning üksikute varaste leidude väljatoomiseks.



L1_Joonis 6. Mudel F – kaksikprotsess detailselt

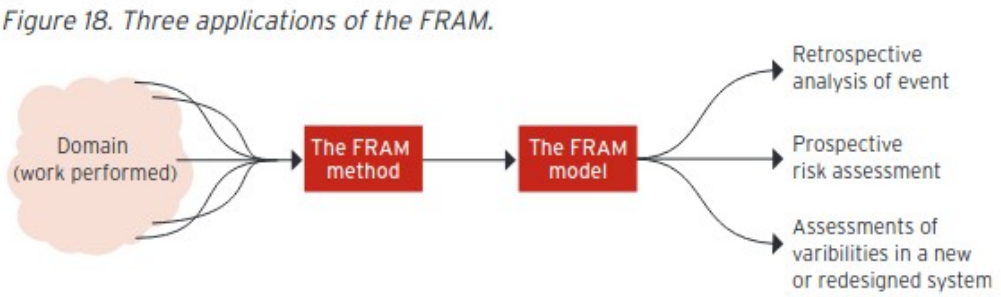
Lisa 2 – FRAM-metoodika lühikirjeldus

FRAM (*functional resonance analysis method*) on Eestis seni avalikkusele tundmatu meetod. Seetõttu on käesoleva diplomitöö mõistmiseks möödapääsmatu FRAM-meetodi eelnev eestikeelne lahtiseletamine.

Olen selle jaotise koostanud allikate [47] , [48] , [49] , [50] , [52] , [53] põhjal. Esitan FRAMi kohta käivad põhiväited mitte tsitaatidena, vaid omaenda sõnastuses. Lühikirjeldus kujuneb üldistamise teel, alustan praktilistest faktidest ja laiendan seda alusteooriale.

FRAM meetodi väljatöötajaks on professor Erik Hollnagel (*University of Southern Denmark, Denmark*) ning selle väljatöötamisajaks loetakse aastat 2004. Meetodi põhiteos „FRAM: The Functional Resonance Analysis Method. Modelling Complex Socio-technical Systems" [19] publitseeriti aastal 2012. Meetod ise on avalik, seda ja kaasnevat arvutitarkvara saab kasutada tasuta.

Klassikaline infosüsteemide analüüs (näiteks Rational Unified Process) näeb ette, et kõigepealt koostatakse huvigruppide visioonidele vastav mudel (*work as imagined – WAI*) ning alles seejärel realiseeritakse mudeli alusel reaalne objekt. Seega on tegu mudelini viiva meetodiga (*model-cum-method*, nn mudeliga meetod). VAstupidiselt eelmisele, FRAM on meetod ilma mudelita (*method-sine-model*) kuivõrd analüüsib mudeli asemel vahetut reaalsust (*work as performed - WAP*). Mudel moodustub FRAM puhul alles analüüsi käigus, vt L2_Joonis 2.



L2_Joonis 1. FRAM handbook[FC], Figure 18

FRAM tähistab ühtaegu nii innovatiivset ohutusparadigmat, üleskirjutusviisi (notatsiooni) kui ka loodava mudeli uurimiseks kasutatavat analüüsimeetodit. FRAMi mudel on allika [49] kohaselt ette nähtud selleks, et a) töökindlal ja süsteemsel viisil, b) kasutades hästimääratletud vormingut; luua reaalse olukorra peegeldus (mudel) ning seejärel) analüüsida: i – kuidas vastav olukord on üles ehitatud, ii – kuidas teda üldiselt konstrueeritakse, iii – kuidas teda saab konstrueerida.

FRAM-i kasutusalad ei piirdu õnnetuste (*accidents*) analüüsiga ega ohutuse juhtimise süsteemidega. FRAM on kasutatav ka toimingute (*activities*) analüüsiks, süsteemidisainiks vms. Eriti hästi sobib FRAM sotsiotehniliste süsteemide kirjeldamiseks, kuivõrd ta eristab tegevuse subjektidena tehnoloogiat, inimest ning isegi (inimestest koosnevat) organisatsiooni. Seetõttu suudab FRAM arvesse võtta inimeste poolt toimepandud unikaalseid ja mittekorratavaid kõrvalekaldeid protseduuridest.

L2_Joonis 1 kajastab võimalikku motivatsiooni FRAM meetodi kasutamiseks. Käesolevas diplomitöös on FRAM meetodiga loodav mudel kasutusel nii riskihalduse eesmärgil kui ka tutvumiseks variatiivsuse allikatega. FRAM mudel, mis sisuliselt on vaid olemasoleva olukorra ülestähendus, vajab selget eristamist analüüsist ja eksperimentidest, mida vastava mudeli põhjal hiljem võidakse sooritada. Ühtlasi on võimalik, et mõni läbiviidav analüüs annab lisainfot ning kutsub esile mudeli inkrementaalse parandamise. FRAM sobib konkreetsete, raskeid tagajärgi kaasa toonud õnnetuste (*accidents*) uurimiseks, aga ka turvalisuse ja ohutuse uurimiseks üldisemalt.

FRAM-mudeli notatsioon

FRAM mudeli notatsioon erineb üldtuntud UML ja BPMN notatsioonidest märkimisväärselt. FRAM nimetab ühte elementi funktsiooniks, BPMN tegevuseks (*activity*) .

Üheks kitsaskohaks infosüsteemide arenduses levinud mudelite puhul on asjaolu, et elemente siduvad ühendused kannavad väga erinevaid semantilisi kategooriaid ning alati ei selgu skeemilt, milliseid täpselt. Nii näiteks võivad BPMN tegevusvoo elemente

nagu sündmused (*events*), tegevused (*activities*) ja lüüsid (*gateways*) siduda järgmised kategooriad [54] : jadavoog (*sequence flow*), sõnumivoog (*message flow*), seos (*association*).

FRAM mudeli puhul on seoste ühestamatus lahendatud elegantselt. FRAM atomaarsel ühikul on kokku viis erineva otstarbega sisendit ning üks väljund. L2_Joonis 2 kujutab FRAM üht elementi (funktsiooni) kuusnurgana, mille tippudes on konkreetse funktsiooni sisendid ja väljund. Iga säärast tippu nimetatakse **aspektiks**.

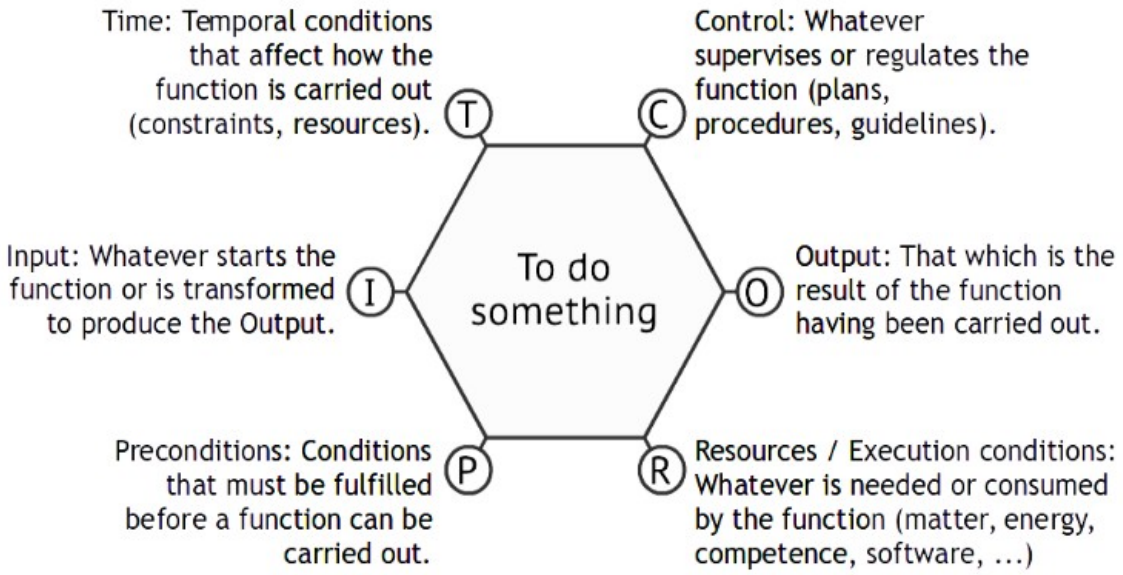


Figure 2: The six aspects used to characterise functions
L2_Joonis 2. FRAM, A Handbook, (2014) [65], Fig. 2

Põhimõttelise erinevusena BPMNist ja UMList, on FRAMi notatsiooni atomaarseks ühikuks (rakukeseks) mitte tegevus (*action*) ega toiming (*task*), vaid **funktsioon**. Funktsioon mõistena on mõnevõrra laiem kui BPMN tegevus (activity) või toiming (task) ning ühtlasi laiem kui UML komponentdiagrammi komponent või oleku-diagrammi seisund. Funktsioon sarnaneb enim BPMN toiminguga (*task*), väljendades mida on vaja teha, samas lisamata, kuidas või mis vahenditega see toiming sooritatakse. FRAM semantika kohaselt, funktsioon väljendab toimingut koos sinna juurde kuuluva metainformatsiooniga (kommentaar, tegija liik, seosed, aspektide variatiivsus). Rakukeste vahelised ühendusteed (seosed) märgivad ülesvoolufunktsiooni tulemust, selle poolt loodud saadusi (*deliverables*) (sh BPMN andmeobjektid). FRAM esitusviis

ei ole kulgmudel ([49] , lk 7), teisisõnu, järgnev (allavoolu, *downstream*) funktsioon võib ajaliselt käivituda varem, kui eelmine (ülesvoolu, *upstream*) oma tegevuse lõpetab ning samas võib ta mitte käivituda isegi juhul kui "eelmine" funktsioon on töö lõpetanud (see juhtub siis, kui mõnesse teise sisendisse jääb saabumata oluline sisendinformatsioon).

Harjumatu on ka FRAM mudeli konstrueerimispõhimõte – graaf ehitatakse üles laiuti (*breadth before depth*) – kõik funktsioonid paigutatakse joonisele ning alles seejärel asutakse mudeli üksikuid funktsioone täitma metainformatsiooniga. FRAM mudeli ühestki tipust ei tohi lähtuda ühendust, mis viiks "eikusagile". Kuivõrd kõik ühendusjooned on varustatud vastava saaduse unikaalse nimega, siis on skeemil lubatud nii 1:M kui M:1 hargnemised, nende väljendamiseks ei vajata BPMN lüüside (gateways) taolisi juhtkonstruktsioone. FRAM mudeli väliste liidestena talitlevad nö taustafunktsioonid (*background functions*), millel vastavalt puudub kas sisend I või väljund O (vrdl UML liidestega, [55]).

FRAM alusprintsiibid

FRAM-meetodi keskseks mõisteks on süsteemi funktsionaalne resonants, mis moodustub kirjeldusele mittealluvast variatiivsusest inimkäitumise eri etappidel ning mis saab olla nii positiivse kui negatiivse iseloomuga. FRAM meetodi paradigma tugineb neljale alusprintsiibile.

I – **samaväärsusprintsiip** (*principle of equivalence*). Selle printsiibi kohaselt õnnestumine ja ebaedu süsteemis on samaväärsed. Keerulises ja tihedalt seostatud süsteemis võib tekkida olulisi mittelineaarsusi ning pole põhimõttelist didaktilist vahet, kumb tulemus (funktsionaalse resonantsi tõttu) saabub.

II – **ligikaudsete lähenduste printsiip** (*approximate adjustment*). Selle printsiibi kohaselt pole inimkomponenti sisaldavates süsteemides põhimõtteliselt võimalik "konstruktsiooni" täpselt modelleerida. Töökorraldus, juhiste kvaliteet ning tööd segavad faktorid jäävad alati alamääratletuteks, sest nüansside hulk on täpseks modelleerimiseks liiga suur. Õnneks on inimene intelligentne olevus ning suudab need

ebatäpsused oma korrektiivse tegutsemisega reaalajas kompenseerida. Kahjuks pole säärane olukorraga automaatse kohandumise protsess enam täpselt modelleeritav.

III – **emergentsusprintsiip** (*emergent outcome*). See printsiip tugineb kahele eelmisele printsiibile, nimelt satub inimkomponendi unikaalsuse tõttu süsteemi alati teatav variatiivsus, kusjuures pole ette teada, kas variatiivsuse kuhjumine keerukas süsteemis viib õnnestumise või ebaeduni. Ebaedul pole ühtainukest juurpõhjust, mille saaks lõpliku ajakuluga välja juurida. Nii oodatu kui ootamatu moodustub mitme põhjuse variatiivsusest või tekkida lubatud sündmuste liitumisest, kusjuures iga üksiku põhjuse variatiivsus võib täiesti jääda lubatu piiridesse.

IV – **funktsionaalresonants** (*functional resonance*) võtab neljanda printsiibina kokku kõik eelmised. Pole teada, milline on iga üksiku elemendi variatiivsus või kuidas variatiivsused omavahel kombineeruvad. Võimalik, et süsteemil on "resonants", mida variatiivsus asub kõigutama. Võib tuua analoogia harmooniliste siinusvõnkumiste liitumisega – see võib juhtuda nii päri- kui vastandfaasis. Millal liituvad kahe viiuli ülemtoonid nii, et salvestava A/D muunduri ulatusest enam ei piisa?!

FRAM kui meetod

FRAM kui meetod koosneb neljast järgust.

I – tuvasta ning kirjelda süsteemi olulised funktsioonid ning määratle iga funktsiooni kuus aspekti. Funktsioonide kogum moodustab FRAM mudeli.

II – määratle mudelis iga funktsiooni potentsiaalne variatiivsus, samuti ühe või enama konkretiseeritud isendmudeli variatiivsus.

III – tuvasta mudelis funktsionaalse resonantsi ilmingud - need moodustuvad üksikute funktsioonide variatiivsusest ja funktsioonide omavahelisest sidestatusest. Tuvastamist saab sooritada nii potentsiaalse variatiivsuse põhjal (üldmudel) kui tegeliku variatiivsuse alusel (konkreetne isendmudel).

IV – anna soovitusi, kuidas avastatud variatiivsust seirata ja ohjata, vastavalt kas soovimatut emergentsi põhjustava variatiivsusese summutamise teel või soovitud emergentsi põhjustava variatiivsuse tugevdamise teel.

Võimalikud probleemid FRAM metoodikaga

FRAM metoodika kasutamisel tuleb arvesse võtta järgmisi teadaolevaid riske:

- meetodi uudsus, kasutamiskogemust napib;
- väärtuste sisseviimine (järk 2) ja isendmudelite konstrueerimine on ajamahukas;
- neljas järk – mudel käsitsi analüüsimine – võib osutuda väga ajamahukaks.

Eesti kultuuriruumis tuleb lisaks arvesse võtta, et FRAM mudeli üht põhinõuet – et iga funktsiooni (piktogrammi) nimi oleks väljendatud infinitiivvormis verbina (või verbifraasina), pole soome-ugri keelte puhul keele iseärasuse tõttu võimalik rakendada. Nimelt, soome-ugri keeltes on infinitiive mitu. Eesti keele ametlikus grammatikas eristatakse ma- ja -da tegevusnime[1], soome keeleõpetuses on infinitiive viis. Seega tekib keeruline küsimus, kumba kahest infinitiivist kasutada.

Eesti arvutiasjanduses on hästi juurdunud kokkulepe, et graafilise liidese menüüpunkte (save! open! exit!) tõlkides käsitletakse neid ainsuse teise isiku käskiva kõneviisina (salvesta! ava! välju!). Ilmselt on otstarbekas kasutada sama konventsiooni ka FRAM funktsioonide nimetamisel. Saaduste (*deliverables*) nimetamine probleeme ei põhjusta, saab probleemivabalt kasutada nimisõna või nimisõnafraasi.

Veel üheks arusaamatuste allikaks võib osutuda proto-indo-euroopa päriolu sõna „funktsioon”[2] – eesti semantikas puudub sellele üksainuke universaalne selgitus. See on kas „parasjagu käimasolev tegevus”, funktsionaalsus (võime või omadus), või kest millegi peitmiseks (funktsioon vs protseduur programmeerimises). Nii näiteks allikas [56] esitab ingliskeelsele sõnale *function* üksteist semantilist tähendust. Ka eesti keel ei anna funktsiooni ega funktsionaalsuse olemust edasi kuigi hästi.

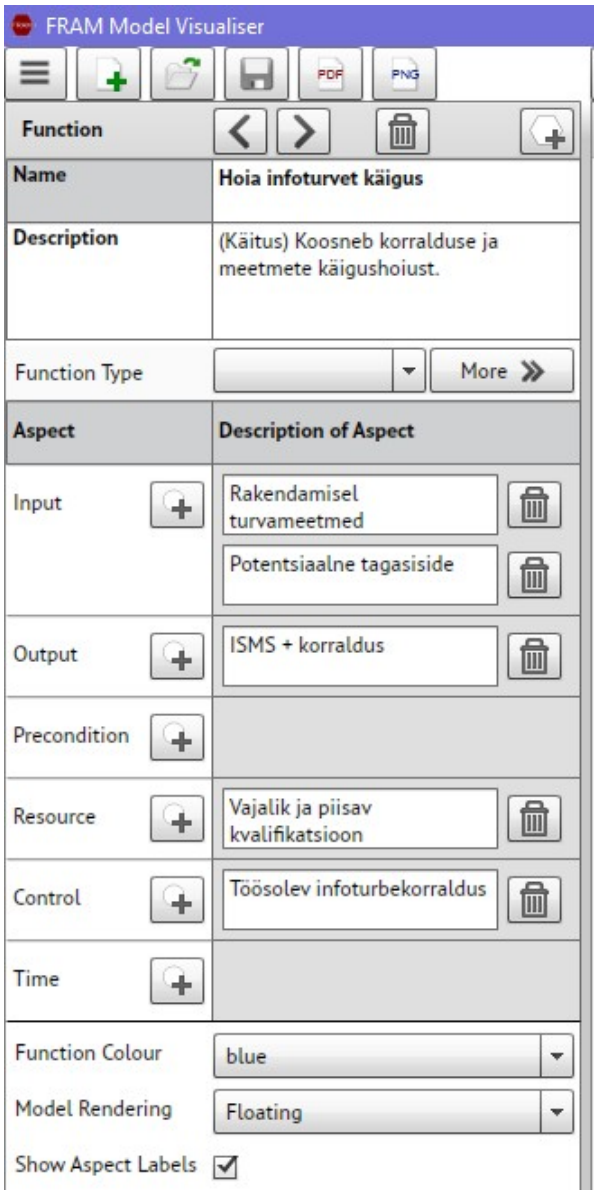
1 Alternatiivse käsitluse kohaselt on eesti keeles isegi kuus infinitiivi: joos**ta**, jooks**ma**, jooks**mas**, jooks**mast**, jooks**maks**, jooks**mata**

2 Vt https://en.wiktionary.org/wiki/function

FRAM meetodi kasutamist piirab praktikas asjaolu, et isendmudelite sügavam analüüs ja mugavusvõimalused (grupeerimine, mudeliosade import/eksport) on saadaval üksnes toetava tarkvara FMV [57] Pro versioonis hinnaga 345 EUR.

Tarkvara: Functional Model Visualizer

Functional Model Visualize [57] on üldkasutatav tarkvara, mis võimaldab koostada FRAM notatsioonis mudeleid, neid valideerida ning pakkuda tuge järgneval analüüsil. Tarkvara on vabalt allalaaditav [58] . L2_Joonis 3 esitab ekraanitõmmise ühe konkreetse funktsiooni sisustamisest tarkvara FMV abil.



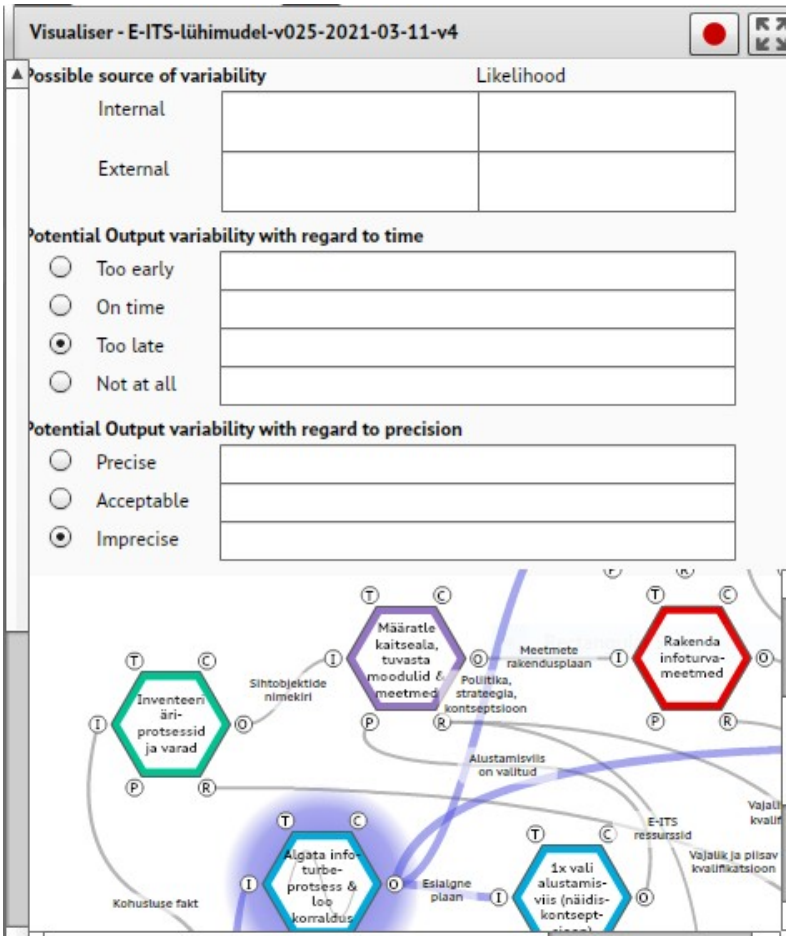
L2_Joonis 3. FMV tarkvara kasutamine konkreetse funktsiooni kirjeldamisel

FRAM mudeli parametriseerimine

L2_Joonis 4 kujutab FMV tarkvara võimalusi mudeli isendistamisel. Saab sisestada variatiivsuse jämedaid hinnanguid, ning kasutada neid järgneval analüüsil (viimast võimaldab kahjuks küll vaid tasuline versioon tarkvarast).

Tarkvara: Functional Model Interpreter

Functional Model Interpreter (FMI) [47] on ette nähtud eelnevalt FMV abil koostatud mudeli valideerimiseks. Tarkvara saab vabalt alla laadida [59] . FMV tasulisse versiooni on FMI funktsionaalsus juba integreeritud ning eraldi validaatorit ei vajata.



L2_Joonis 4. FMV tarkvara kasutamine – võimalused mudeli parametriseerimiseks

Lisa 3 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Anto Veldre:

1 Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Eesti infoturbestandardi protsessimudeli evalveerimine", mille juhendaja on Kristjan Karmo;

1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2 üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2 Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.

3 Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

17.05.2021

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.