DONATAS MAŽEIKA

MODELIAIS GRĮSTOS SISTEMŲ INŽINERIJOS METODAS SAUGIŲ SISTEMŲ KŪRIMUI

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI, INFORMATIKOS INŽINERIJA (T 007)

Kaunas
2021

KAUNO TECHNOLOGIJOS UNIVERSITETAS
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

DONATAS MAŽEIKA

MODELIAIS GRĮSTOS SISTEMŲ INŽINERIJOS METODAS SAUGIŲ SISTEMŲ KŪRIMUI

Daktaro disertacijos santrauka
Technologijos mokslai, Informatikos inžinerija (T 007)

2021, Kaunas

Disertacija rengta 2015–2020 metais Kauno technologijos universitete, Informatikos fakultete, Informacijos sistemų katedroje. Mokslinius tyrimus rėmė Valstybinis studijų fondas.

Moksliniai vadovai:
Prof. dr. Lina NEMURAITĖ (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – T 007, 2015 m. – 2016 m.).
Prof. dr. Rimantas BUTLERIS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – T 007, 2016 m. – 2020 m.).

Redagavo: Asta Merkevičienė (kultūros ir mokslo sklaidos ir tyrimų centras „Pradmuo").

Informatikos inžinerijos mokslo krypties taryba:
Prof. dr. Tomas BLAŽAUSKAS (Kauno technologijos universitetas, informatikos inžinerija – T 007) – **pirmininkas**;
Prof. habil. dr. Gintautas DZEMYDA (Vilniaus universitetas, informatikos inžinerija – T 007);
doc. dr. Nikolaj GORANIN (Vilniaus Gedimino universitetas, informatikos inžinerija – T 007);
Prof. dr. Raimundas MATULEVIČIUS (Tartu universitetas, Estija, informatikos inžinerija – T 007);
Prof. dr. Jevgenijus TOLDINAS (Kauno technologijos universitetas, informatikos inžinerija – T 007).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties tarybos posėdyje, kuris įvyks 2021 m. liepos 1 d. 14:00 val. Kauno technologijos universiteto disertacijų gynimo salėje.

Adresas: K. Donelaičio g. 73-403, 44249 Kaunas, Lietuva.
Tel. (370) 37 300 042; faks. (370) 37 324 144; el. paštas doktorantura@ktu.lt.

Disertacijos santrauka išsiųsta 2021 m. birželio 1 d.
Su disertacija galima susipažinti internetinėje svetainėje http://ktu.edu ir Kauno technologijos universiteto bibliotekoje (K. Donelaičio g. 20, 44239 Kaunas).

1 ĮVADAS

1.1 Motyvacija

Šiuolaikinės sistemos iš tokių pramonės šakų, kaip gynyba ir kosmoso tyrinėjimas, automobilių ir medicinos prietaisų gamyba, tapo ypač sudėtingos ir tradicinių inžinerijos metodų nepakanka jas sėkmingai kurti. Sistemų kompleksiškumas išaugo dėl daugelio veiksnių:

- Beveik visos sudėtingos sistemos yra kibernetinės-fizinės sistemos ir jų veikimas priklauso nuo to, kaip sklandžiai yra integruoti kompiuteriniai algoritmai (programinė įranga) į įvairius fizinius komponentus [1].
- Išaugęs klientų poreikis sistemoms su sudėtingomis funkcijomis ir galimybėmis, padidėjusi rinkos ar karinė konkurencija [2].
- Sistemos yra sudarytos iš didelio kiekio komponentų, kurie komunikuoja tinkle, ir įprastai šie komponentai yra fiziškai ir funkciškai nevienalyčiai [3].

Sistemų kompleksiškumo iššūkį sprendžia tarpdisciplininė technologijų šaka – sistemų inžinerija (angl. *Systems Engineering* – SE), leidžianti valdyti, abstrahuoti ir integruoti skirtingų inžinerinių komandų darbo rezultatus. SE tikslas – užtikrinti sudėtingos sistemos sėkmingą sukūrimą sutelkiant dėmesį į klientų ir kitų suinteresuotų šalių poreikių surinkimą, aprašant sistemos reikalavimus, funkcionalumą ir dizainą ankstyvojoje sistemos kūrimo fazėje, lygiagrečiai atliekant sistemos ar komponentų integraciją, validaciją ir verifikaciją [4]. Modeliais grįsta sistemų inžinerija (angl. *Model-Based Systems Engineering* – MBSE) perkelia visas SE veiklas bei reikiamus artefaktus iš dokumentų į modelį CASE įrankyje, taip spręsdama esminius sistemų inžinerijos iššūkius, tokius kaip: atsekamumo galimybės ir pokyčių įtakos analizė; žinių kaupimas ir pakartotinis panaudojimas; komunikacijos gerinimas (vienas modelis naudojamas skirtingų komandų); kokybės gerinimas panaudojant automatizuotus tikrinimo įrankius; sudėtingumo valdymas; eksperimentavimas; dokumentacijos parengimas ir kt. [5, 6, 7].

Egzistuoja nemažai populiarių ir praktikoje naudojamų MBSE metodikų, kurios įgalina projektuoti sudėtingas sistemas, tačiau tik viena iš analizuotų metodikų ribotai siūlo įtraukti saugumo analizę ankstyvajame sistemos kūrimo etape. Antra vertus, yra keletas metodų ir priemonių, leidžiančių atlikti saugumo analizę pradiniame sistemų kūrimo etape (pvz.: *Misuse Cases, Abuse Cases, Secure-Tropos,* CHASSIS), tačiau jie yra atskirti nuo sistemų inžinerijos [8, 9].

Daug tyrėjų savo studijose [10, 11, 12, 13] aprašo didėjantį poreikį identifikuoti saugumo spragas ir jas minimizuoti sistemų inžinerijos metu. Pavyzdžiui, Nguyen ir kt. teigia, kad saugumo uždaviniai (tokie kaip konfidencialumas, integralumas ir prieinamumas) turėtų būti svarstomi kuo anksčiau, kartu su verslo logikos aprašymu, taip užtikrinant, kad sistemų

saugumas būtų prioritetinis klausimas. Tam MBSE yra tinkama, nes ji leidžia projektuoti ir testuoti sistemą įvairiose abstrakcijos lygiuose, o modeliavimo kalba (pvz.: UML ar *SysML*) gali būti pritaikoma konkrečiai dalykiniai sričiai [11]. Nors šiuo metu MBSE yra daugiausiai diegiama sistemų inžinierių, tačiau saugumo inžinieriai taip pat galėtų prisidėti prie šios veiklos, jei tam būtų paskirtas procesas ar karkasas [12].

Autoriai teigia, kad didžiausia MBSE vertė yra gaunama, kai sistemos validacija ir verifikacija atliekama ankstyvuose sistemos projektavimo etapuose [14, 15]. Kuo anksčiau aptinkami sistemos trūkumai ar klaidos, tuo jie gali būti greičiau pašalinami mažesniais kaštais, kartu išvengiant keitimo vėlesniuose etapuose ir mažinant riziką dėl projekto sąmatos padidėjimo ir atlikimo termino [15]. Tie patys principai galioja ir saugumo srityje – kuo anksčiau įvertinamos saugumo rizikos, tuo mažiau kainuoja įdiegti riziką mažinančias priemones [16].

1.2 Tyrimo sritis ir objektas

Šio tyrimo objektas yra modeliu grįstos sistemų inžinerijos metodas, skirtas saugioms sistemoms sukurti, formalizuotas UML kalba.

Tyrimo sritis:

- sistemų inžinerija (SE) ir modeliu grįsta sistemų inžinerija (MBSE);
- saugumo reikalavimų inžinerija;
- modeliavimo metodai ir būdai, skirti atlikti saugumo analizę;
- saugumo rizikos valdymas;
- standartai ir metodai, skirti sukurti dalykinės srities kalbą ir formalizuoti MBSE saugumo metodą.

1.3 Sprendžiama problema ir keliami klausimai

Vienas iš svarbiausių iššūkių, kurį organizacijos bando išspręsti kurdamos naują sistemą, – kaip sukurti saugią sistemą. Tradiciškai sistema laikoma saugia, jei garantuojami konfidencialumo, vientisumo ir prieinamumo principai.

Tyrimas turi atsakyti į šiuos klausimus:

1. Ar MBSE yra tinkama aplinka, norint apibrėžti ir valdyti saugumo reikalavimus ir atlikti saugumo analizę sudėtingoms kibernetinėms-fizinėms ir programinės įrangos sistemoms ankstyvajame sistemos kūrimo etape?
2. Ar UML profiliai ir MOF standartas yra tinkamos ir pakankamos priemonės, norint formalizuoti dalykinės srities kalbą ir MBSE saugumo metodą?
3. Kaip saugumo reikalavimų apibrėžimo ir saugumo analizės veiklos turi būti įtrauktos į MBSE procesą, kad būtų užtikrinamas projektuojamos sistemos saugumas ir išnaudojami MBSE privalumai?

4. Kokie su saugumu susiję konceptai turi būti įtraukti į sistemų modeliavimo kalbą, kad būtų galima modeliuoti saugumo aspektą ankstyvuoju sistemos kūrimo etapu?
5. Kokių dalykinės srities plėtinių (pvz.: stereotipų, diagramų, patikrinimo taisyklių) reikia saugos analizei atlikti?
6. Kokie MBSE įrankiai (pvz.: eksperimentavimas, pokyčio analizė, modelio tikrinimas) gali būti panaudoti su siūlomu saugumo metodu?
7. Ar siūlomas MBSE saugumo metodas leidžia visapusiškai, nepertekliškai, teisingai ir nuosekliai projektuoti sistemų saugumo aspektą CASE įrankyje tiek kibernetinėms-fizinėms, tiek programinės įrangos sistemoms?

1.4 Tikslas ir uždaviniai

Tyrimo tikslas – sukurti priemones, leidžiančias spręsti saugios sistemos projektavimo iššūkius ankstyvojoje sistemos kūrimo fazėje modeliais grįstoje sistemų inžinerijoje.

Siekiant nustatyto tyrimo tikslo, būtina išspręsti žemiau pateiktus darbo uždavinius:

1. Atlikti naujausių tyrimų disertacijos tema apžvalgą, kuri apimtų:
   1.1. sistemų inžineriją ir modeliu grįstą sistemų inžineriją;
   1.2. saugumo reikalavimų inžineriją;
   1.3. modeliavimo metodus, skirtus atlikti saugumo analizę;
   1.4. saugumo rizikos valdymą;
   1.5. standartus ir metodus, skirtus sukurti dalykinės srities kalbą ir formalizuoti MBSE saugumo metodą.
2. Teoriškai pagrįsti ir realizuoti naują MBSE metodą, leidžiantį identifikuoti saugumo spragas ir sumažinti jų riziką ankstyvajame sistemos kūrimo etape.
3. Atlikti eksperimentus, leidžiančius įvertinti pasiūlyto MBSE saugumo metodo tinkamumą ir praktinį pritaikomumą.

1.5 Tyrimo metodika

Disertacija paremta tradicinio mokslinio tyrimo metodika (ang. *design science research*) [17]. Pirmiausia informacijos analizės, palyginimo ir klasifikacijos metodai buvo naudoti tiriant SE, MBSE, saugumo reikalavimų inžinerijos, saugumo veiklų ir saugumo rizikos valdymo temas.

Po mokslinės literatūros analizės etapo buvo atlikta galimybių studija (bandomasis tyrimas), kuri leido pasitvirtinti metodo reikalingumą, praktinį pritaikomumą ir suinteresuotų šalių poreikius.

Toliau buvo pasirinktas klasikinis modeliavimo kalbos kūrimo metodas, kuris teigia, kad modeliavimo kalbos sukūrimui iš pradžių reikia nustatyti pagrindinės dalykinės srities sąvokas ir ryšius tarp jų, o tada sukurti tai atitinkančią

kalbą [18].

Pasiūlyto metodo eksperimentinis įvertinimas buvo atliktas keliomis iteracijomis. Pirmoje iteracijoje atliktas kokybinis įvertinimas, apklausiant ekspertus iš MBSE ir inžinerijos šakų, akademijos atstovus. Tada įvykdytas kiekybinis metodo įvertinimas, kuriame du realaus pasaulio modeliai (hibridinio automobilio ir skrydžio statusų sistema) buvo eksperimentiškai tikrinami pagal šiuos kriterijus: metodo visapusišką, nepertekliškumą, teisingumą ir nuoseklumą.

1.6 Ginamieji teiginiai

1. MBSE yra tinkama metodologija, norint apibrėžti ir valdyti saugumo reikalavimus ir atlikti saugumo analizę sudėtingoms kibernetinėms-fizinėms ir programinės įrangos sistemoms ankstyvajame sistemos kūrimo etape.
2. Modeliavimo kalba UML 2.5 ir MOF standartas yra tinkamos ir pakankamos priemonės, norint formalizuoti dalykinės srities kalbą ir MBSE saugumo metodą.
3. MBSE aplinkoje naudojami automatizuoti įrankiai (tokie kaip eksperimentavimas, pokyčio analizė, modelio validacija ir verifikacija, žinių kaupimas ir modelio perpanaudojimas) gali būti pritaikyti ir saugumo srityje su pasiūlytu MBSE saugumo metodu.
4. Visi artefaktai, kurie yra reikalingi saugumo reikalavimams apibrėžti ir saugumo analizei vykdyti (pvz.: palyginus su reikalavimais ISMS pagal ISO / IEC 27001:2013 standartą), gali būti teisingai, nepertekliškai ir nuosekliai sukurti siūlomu saugumo metodu MBSE modelyje.

1.7 Asmeninis indėlis ir naujumas

Šio tyrimo mokslinis naujumas ir asmeninis indėlis yra pateiktas žemiau:

1. Sukurtas dalykinės srities modelis, kuriame sujungti saugumo konceptai ir technikos iš saugumo reikalavimų inžinerijos ir kitų su saugumo analize susijusių mokslo šakų. Šis saugumo srities konceptų modelis leidžia saugumo ir sistemų inžinieriams geriau suprasti ir palyginti įvairius saugumo terminus ir metodus, kurie gali būti naudojami ankstyvajame sistemos projektavimo etape.
2. Pasiūlytas naujas MBSE metodas saugioms sistemoms kurti, leidžiantis specifikuoti ir analizuoti saugumo rizikas ankstyvajame sistemos projektavimo etape. Jis apima visas saugumo fazes: pradedant rizikų vertinimo konfigūracija ir saugumo reikalavimais, tęsiant saugomų objektų aprašymu ir jų susiejimu su sistemos struktūra, tuomet rizikų ir grėsmių analize ir užbaigiant saugumo tikslų iškėlimu ir kontrolinių priemonių nustatymu. Modeliais grįstų technikų ir standartų naudojimas užtikrina, kad saugumo ir sistemos artefaktai yra suderinti

ankstyvajame sistemos projektavimo etape, o MBSE teikiamų naudų spektras išplėstas į saugumo sritį.

3. Autoriaus pasiūlytas MBSE saugumo metodas yra vienas pirmųjų tokio tipo metodų disertacijos paskelbimo metu.

1.8 Praktinė reikšmė

Pagrindinė praktinė šio tyrimo reikšmė yra žingsnis link sistemų ir saugumo inžinerijos disciplinų susiejimo per MBSE aplinką. Pasiekti praktiniai rezultatai:

- Sukurtas MBSE saugumo metodas, leidžiantis projektuoti saugias sistemas CASE įrankyje.
- Pasiūlytas *MBSEsec* UML saugumo profilis ir metodo plėtinių paketas buvo sukurti su įrankiu *MagicDraw 19.0* ir gali būti įdiegti kaip įskiepiai į bet kurį suderinamą CASE įrankį. Metodo reikalavimai vienareikšmiškai aprašyti pagal IETF RFC2119 rekomendacijas ir gali būti atkurti bet kuriame UML kalbą palaikančiame CASE įrankyje.
- Saugumo metodas pateikia gaires, kaip jį praktiškai pritaikyti projektuojant sistemas ir kaip panaudoti MBSE įrankius, tokius kaip modelio validaciją ir verifikaciją, pokyčių analizę, atsekamumą.
- Siūlomas *MBSEsec* metodas yra suderintas su saugumo standartu ISO / IEC 27001, kurį naudoja daugelis inžinerinių organizacijų.
- Disertacijoje pateiktos dvi metodo pritaikomumo demonstracijos – hibridinio automobilio saugumo analizė galios blokui ir skrydžių statusų sistemos modernizavimo projektas.

1.9 Rezultatų aprobavimas

Mokslinių tyrimų disertacijos tema rezultatai buvo pristatyti trijose tarptautinėse konferencijose, vykusiose Norvegijoje, Australijoje ir Vengrijoje, ir viename tarptautiniame seminare Lietuvoje. Svarbiausi disertacijos rezultatai paskelbti dviejuose straipsniuose, išspausdintuose recenzuojamuose mokslo leidiniuose, turinčiuose cituojamumo rodiklį duomenų bazėje *Clarivate Analytics Web of Science* (CA WoS). Detalus publikacijų sąrašas pateiktas 7 skyriuje „Autoriaus publikacijų disertacijos tema sąrašas“.

1.10 Disertacijos struktūra

Disertaciją sudaro keturi pagrindiniai skyriai: pirmame analizuojami ir aprašomi darbai ir publikacijos, susiję su SE, MBSE, saugumo reikalavimų inžinerijos ir saugumo rizikos valdymo temomis; antrame skyriuje pateikiama galimybių studija, trečiame aprašomos priemonės, skirtos kalbos ir metodo formalizavimui, ir pristatomas *MBSEsec* metodas, o ketvirtame skyriuje pateikiami eksperimentiniai metodo įvertinimai. Be minėtų skyrių, disertacijoje pateikiamas įvadas ir išvados.

2 MOKSLINĖS LITERATŪROS ANALIZĖ

Mokslinės literatūros analizė apima keletą sričių: SE, MBSE, saugumo reikalavimų inžineriją, modeliavimo metodus saugumo analizei ir saugumo rizikos valdymą.

2.1 Sistemų inžinerija ir modeliais grįsta sistemų inžinerija

Sistemų inžinerija, kaip daugiadisciplinė šaka, palengvinanti sudėtingų sistemų kūrimą ir leidžianti valdyti projekto kaštus, terminus ir kitus resursus, pradėjo vystytis XX amžiaus 9-ajame dešimtmetyje [4, 19]. Iš pradžių SE buvo paremta inžinerinių dokumentų, tokių kaip sistemos specifikacijos, funkcinių schemų, reikalavimų dokumentacijos, sąsajos kontrolės dokumentų, architektūros aprašo ir kt., kūrimu. Paprastai šiuos artefaktus kurdavo ne vienas sistemų inžinierius, o dokumentai būdavo skirtingų formatų (tekstas, schemos, skaičiuoklės) ir išsaugoti kaip atskiros rinkmenos. Dėl to dokumentais grindžiama SE susiduria su dokumentų rinkinio vientisumo palaikymo, informacijos pernaudojimo, pokyčių atlikimo ir kitais iššūkiais, kuriuos bando spręsti modeliais grindžiama sistemų inžinerija [20].

Modeliais grįstoje sistemų inžinerijoje modelis tampa centrine SE figūra, kuri įgalina turėti vieną tiesos šaltinį (ang. *one source of truth*), sistemą matyti skirtingomis perspektyvomis (diagramomis, lentelėmis, matricomis), susieti kuriamus elementus, atlikti pokyčių įtakos analizę, mažinti kompleksiškumą modeliuojant skirtingos abstrakcijos lygius ir kt. [4]. Siekiant sėkmingai pritaikyti MBSE yra būtini trys dalykai: standartizuota sistemų modeliavimo kalba, metodika ir CASE įrankis [21].

Šioje disertacijoje detaliau nagrinėjamos lyderiaujančios MBSE metodikos, atrinktos pasitelkiant INCOSE oficialų MBSE metodikų sąrašą [22] ir išsamų MBSE tyrimą, atliktą *Estefan* [23]. Taip pat į disertaciją įtraukta *MagicGrid* metodika, kuri yra MBSE metodikų ir karkasų sintezė bei buvo sėkmingai pritaikyta praktikoje [24]. Analizuotos metodikos: *Object-Oriented Systems Engineering Methodology* (OOSEM), *IBM Harmony SE, Weilkiens Systems Modelling Process* (SYSMOD), *NASA JPL State Analysis, Vitech MBSE Methodology, MagicGrid.* MBSE metodikų palyginimas pateiktas 1 lentelėje.

1 lentelė. MBSE metodikų palyginimas

	OOSEM	**IBM *Harmony* SE**	**SYSMOD**	**JPL *State Analysis***	***Vitech* MBSE**	***MagicGrid***
Siūlo veiklas ankstyvajame sistemos kūrimo etape	Taip	Taip	Taip	Taip	Taip	Taip
Siūlo papildomas veiklas (ne	Sistemos architektū-	Integracija su progra-	Variantų modeliavimas;	Sistemos būsenos	Ne	Dabartinė versija nesiūlo

	OOSEM	IBM *Harmony* SE	SYSMOD	JPL *State Analysis*	*Vitech* MBSE	*MagicGrid*
SE)	ros vertinimas ir optimizavimas	minės įrangos modeliu	Funkcinė architektūra	numatymas; Atlikimo vertinimas; Įterptosios programinės įrangos architektūra		
Palaikoma modeliavimo kalba	UML ir *SysML*	*SysML*	*SysML*	SQL; papildomai *SysML*	*System Definition Language* (SDL)	*SysML*
Palaikomas iteratyvus procesas	Taip	Taip	Taip	Taip	Ne	Ne
Galima atlikti sistemos validaciją ir verifikaciją	Taip	Taip	Dabartinėje versijoje nesiūlo	Taip	Taip	Taip
Galima atlikti saugumo analizę	Ne	Taip	Ne	Ne	Ne	Ne
Paremta standartu / procesu	Taip, ISO/IEC 15288	Taip, *Rational Unified Process* (RUP)	Ne	Taip, *State Analysis* procesas	Ne	Ne

2.2 Saugumo reikalavimų inžinerija

Saugumo reikalavimų inžinerija apima tradicines reikalavimų inžinerijos veiklas, tokias kaip reikalavimų surinkimas, specifikacija ir analizė. Saugumo reikalavimai turėtų būti suprantami kaip detalizuoti saugumo tikslai, o saugumo tikslai įprastai yra skirstomi į tris kategorijas: konfidencialumas, vientisumas ir prieinamumas [25, 26]. Standartas ISO/IEC 13335-1:2004 konfidencialumą apibrėžia kaip sistemos charakteristiką, kuri užtikrina, kad informacija nėra prieinama ar atskleidžiama autorizuotos prieigos neturintiems vartotojams, subjektams ar išorinėms sistemoms. Vientisumo charakteristika teigia, kad sistema turi būti apsaugota nuo nesankcionuoto informacijos pakeitimo ar iškraipymo. Prieinamumas turi užtikrinti, kad sistema bet kuriuo metu yra prieinama autorizuotiems naudotojams [27].

Svarbu paminėti, kad saugumas (ang. *security*) ir sauga (ang. *safety*) yra skirtingos disciplinos. Nors saugumo ir saugos disciplinos turi panašumų (pvz.: abiejų tikslas yra apsaugoti sistemą, įdiegiant prevencines kontrolės priemones), tačiau egzistuoja ir esminiai skirtumai [28, 29]:

- Rizikos kilmė – saugumo disciplina analizuoja išorines grėsmes (pvz.: užpuolikas įsilaužia į orlaivio keleivių sistemą ir įrašo kenkėjišką programinę įrangą), o sauga analizuoja galimus vidinius pavojus (pvz., kas nutiks, jei orlaivio važiuoklė neišsiskleis nusileidimo metu).
- Pasekmių pobūdis – nesuvaldyta saugumo rizika gali pakenkti tiek pačiai sistemai, tiek jos naudotojams / aplinkai. Saugos rizikos pasekmės yra susijusios tik su sistemos naudotojais / aplinka.

Šioje disertacijoje analizuojami tik saugumo būdai ir metodikos (išskyrus CHASSIS metodiką, kuri apima tiek saugumą, tiek saugą).

2.3 Modeliavimo metodai, skirti atlikti saugumo analizę

Pagrindiniai modeliavimo metodai saugumo analizei atlikti buvo atrinkti pasitelkiant Fabian ir kt. saugumo reikalavimų inžinerijos palyginimo konceptualų karkasą [25] bei Kriaa ir kt. atliktą išsamų tyrimą šia tematika [29]. Analizei buvo atrinkti šie modeliavimo metodai, kurie galėtų būti naudojami ankstyvajame sistemos projektavimo etape ir integruoti į MBSE procesą: *Unified Architecture Framework* (UAF), CHASSIS, *SysML Sec, UML Sec,* CORAS. Formalūs saugumo metodai arba pusiau formalūs metodai, kurie grindžiami kitokia nei UML / *SysML* grafine forma (pvz., *Petri* tinklai, *Bayesian belief network*), nebuvo įtraukti į tyrimą, nes fundamentaliai skirtinga diagramų notacija sukeltų papildomų keblumų, o formalūs metodai įprastai įgyvendinami vėlesniame sistemos kūrimo etape.

Saugumo modeliavimo metodų analizė leido išskirti pagrindinius saugumo terminus, jų aprašymus ir sinonimus. Ši apibendrinta informacija pateikiama 2 lentelėje.

2 lentelė. Saugumo konceptai sulygiuoti pagal saugumo modeliavimo metodus

	UAF	**CHASSIS**	**SysML Sec**	**UML Sec**	**CORAS**	**Apibrėžimas**	**Sinonimai**
Vertybė	+	+	+	-	+	Sistemos ar aplinkos elementai, kuriuos norime apsaugoti nuo neigiamų padarinių [30].	Programinės įrangos vertybė, Sistemos vertybė, Duomenų vertybė

	UAF	CHASSIS	SysML Sec	UML Sec	CORAS	Apibrėžimas	Sinonimai
Saugumo apribojimas	+	+	+	+	+	Taisyklė, apibrėžianti saugumo tikslus, reglamentus ir gaires [31].	Saugumo reikalavimas, Saugumo tikslas
Saugumo kontrolė	+	-	+	-	+	Apsaugos arba atsakomosios priemonės, skirtos sistemai ar organizacijai apsaugoti turimų vertybių konfidencialumą, vientisumą ir prieinamumą [31].	Saugumo veikla, Apsaugos priemonė
Saugumo ypatybė	+	-	+	+	+	Vertybės charakteristika, apibūdinanti jos saugumo poreikius [31].	Informacijos užtikrinimo ypatybė
Rizika	+	+	+	-	+	Įvykio įtakos saugomoms vertybėms apibūdinimas [31].	-
Rizikos poveikis	+	+	+	-	-	Galimas poveikis sistemai dėl konkrečios priežasties (pvz.: prieinamumo, vientisumo ar konfidencialumo pažeidimo) [31].	Žala, Padariniai
Tikimybė	+	-	-	-	+	Rizikos atsitikimo tikimybė [31].	
Pažeidžiamumas	+	+	-	+	+	Vidinis sistemos trūkumas ar defektas, kuris leidžia įsilaužėliams pakenkti sistemai [30].	Sistemos silpnoji vieta
Užpuolikas	-	+	+	+	+	Asmuo ar sistema, vykdanti užpuolimą, siekiant pakeisti sistemos funkcionalumą ar našumą arba pasiekti konfidencialią informaciją [30].	Įsilaužėlis
Grėsmė	+	+	+	+	+	Galimas išpuolis, nukreiptas prieš sistemą ir galintis pakenkti saugomoms vertybėms [8].	Ataka

Be to, analizuojant saugumo modeliavimo metodus, buvo identifikuotos pagrindinės saugumo technikos, jų įgyvendinimas *SysML* kalboje ir paskirtis. Ši apibendrinta informacija pateikta 3 lentelėje.

3 lentelė. Saugumo technikos

	UAF	CHASSIS	SysML Sec	UML Sec	CORAS	Įgyvendinimas *SysML* kalboje	Paskirtis
Saugumo reikalavimų apibrėžimas	+	+	+	+	+	*SysML* reikalavimų diagrama, *SysML* panaudos atvejų diagrama	Specifikuoti funkcinius ir nefunkcinius saugumo reikalavimus
Saugumo procesai	+	-	-	-	-	*SysML* veiklos diagrama	Nustatyti saugumo kontrolę
Vertybių struktūra	+	-	-	-	+	*SysML* blokų apibrėžimo diagrama (BDD), *SysML* vidinė bloko diagrama (IBD)	Aprašyti sistemos vertybes ir jų alokacijas
Saugumo rizikos apibrėžimas	+	+	-	-	+	*SysML* blokų apibrėžimo diagrama (*BDD*)	Identifikuoti ir apibendrinti rizikas, jų poveikį, tikimybę ir kt.
Netinkamo naudojimo atvejai (*Misuse Cases*)	-	+	-	-	-	*SysML* panaudos atvejų diagrama	Identifikuoti grėsmes ir užpuolikus
Netinkamo naudojimo atvejų sekos	-	+	-	-	-	*SysML* sekų diagrama	Apibrėžti atakos seką įsilaužimo metu
HAZOP	-	+	-	-	+	Lentelė	Apibendrinti su rizikos ir saugumo reikalavimais susijusius duomenis
Atakos scenarijus	-	+	+	+	+	*SysML* veiklos diagrama, *SysML* parametrų diagrama	Identifikuoti ir aprašyti atakos žingsnius ir algoritmus
***Dolev–Yao* atakos modelis**	-	-	-	+	-	*SysML* blokų apibrėžimo diagrama, SysML būsenos mašinos diagrama	Formaliai apibrėžti galimus užpuoliko veiksmus

2.4 Saugumo rizikos valdymas

Ankstesniuose skyriuose pristatyti saugumo modeliavimo metodai ir saugumo reikalavimų inžinerija buvo orientuoti į saugios sistemos kūrimą, tačiau saugumo rizikos valdymas apima platesnę sritį, skirtą kibernetinio saugumo rizikai valdyti organizaciniame kontekste. Saugumo rizikos valdymą galima apibrėžti kaip taisyklių, procedūrų ir praktikų visumą, skirtą identifikuoti, analizuoti, vertinti, stebėti, komunikuoti ir minimizuoti saugumo rizikas [32].

Šiame tyrime pasirinktas saugumo standartas ISO/IEC 27001:2013, padedantis užtikrinti, kad sistemos rizika būtų sistemingai valdoma siūlomu MBSE saugumo metodu.

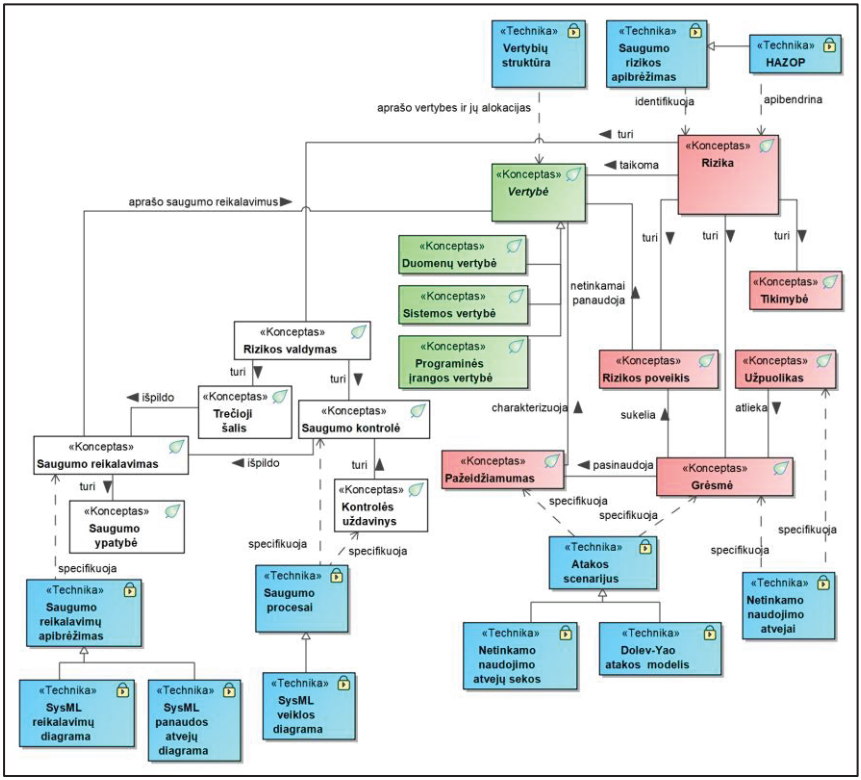
3 GALIMYBIŲ STUDIJA

Bandomajame tyrime (galimybių studijoje) buvo apklausti sistemų ir saugumo inžinerijai iš 10 skirtingų organizacijų, kurios kuria kompleksines sistemas. Tyrimas leido pasitvirtinti MBSE saugumo metodo reikalingumą, praktinį pritaikomumą ir suinteresuotų šalių poreikius. Buvo tiriama, kiek plačiai yra naudojami ir susiejami sistemų inžinerijos modeliai / dokumentai su saugumo artefaktais, kokie saugumo atributai yra svarbiausi saugumo inžinieriams, kokie validavimo ir verifikavimo metodai naudojami, kokio tipo ir dydžio modelius kuria respondentai, ar siūlomo metodo pateikiami konceptai, technikos, taisyklės yra aktualios bei padės išspręsti esamas problemas ir kt. Šio tyrimo rezultatai paskelbti žurnale *Security and Communication Networks* [37].

4 MODELIAIS GRĮSTOS SISTEMŲ INŽINERIJOS METODAS SAUGIOMS SISTEMOMS KURTI

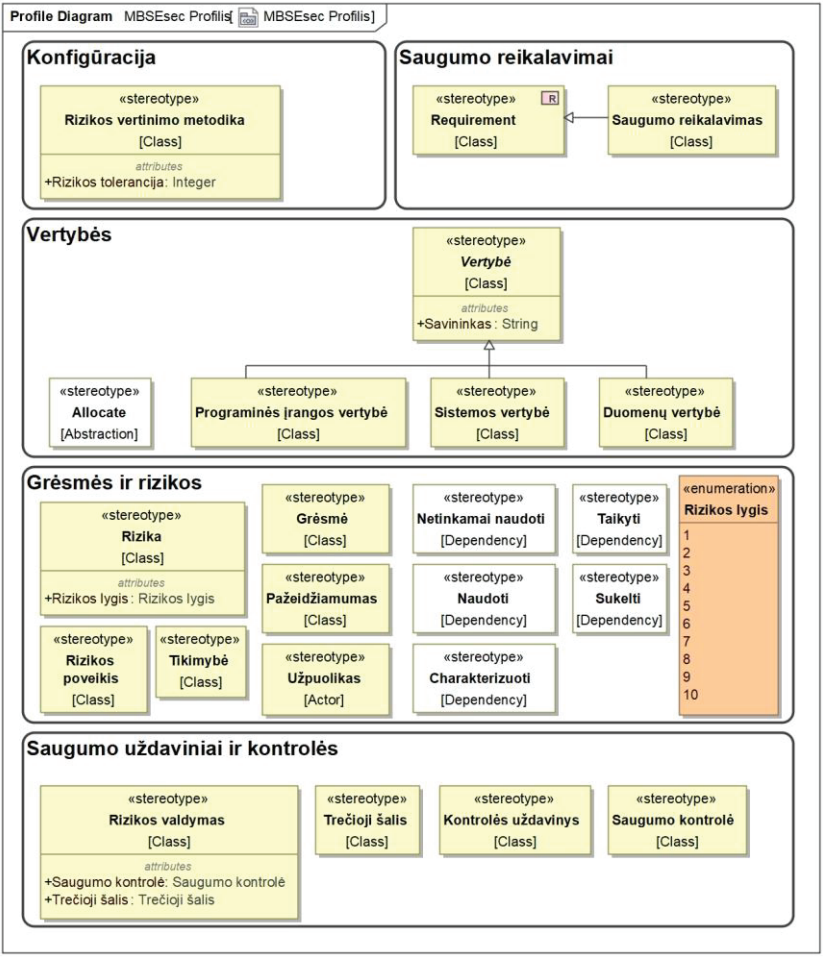
Siūlomo MBSE saugumo metodo formalizavimui pasirinktas standartas OMG MOF ir modeliavimo kalba UML 2.5, turinti integruotą metamodelio praplėtimo mechanizmą – UML profilius, taip pat į konkrečią dalykinę sritį orientuotos modeliavimo kalbos karkasas (angl. *domain specific modeling language* – DSML) [33, 34, 35]. Saugumo profilis ir susiję plėtiniai (diagramos, verifikacijos taisyklės, pavyzdiniai projektai ir kt.) sukurti su įrankiu *MagicDraw 19.0* ir gali būti įdiegti kaip įskiepiai į bet kurį suderinamą CASE įrankį. Be to, metodo reikalavimai vienareikšmiškai aprašyti pagal IETF RFC2119 rekomendacijas ir gali būti atkurti bet kuriame UML kalbą palaikančiame CASE įrankyje [36].

Pirmasis žingsnis kuriant MBSE saugumo metodą yra sudaryti dalykinės srities konceptų modelį, kuriami sujungti analizės metu identifikuoti saugumo konceptai ir technikos. Tai yra klasikinis naujos modeliavimo kalbos kūrimo metodas, kuris teigia, kad kalbos sudarymui iš pradžių reikia nustatyti pagrindinės dalykinės srities sąvokas ir ryšius tarp jų, o tada sukurti tai atitinkančią kalbą [18]. Siūlomas saugumo srities konceptų modelis yra atvaizduotas 1 paveiksle.



1 pav. Saugumo srities konceptų modelis

Kitas žingsnis – pagal saugumo srities konceptų modelį sudaryti UML profilį. 2 paveiksle pateiktas siūlomas MBSE saugumo profilis. UML profilio diagramoje išskirtos 5 kategorijos, kuriose atvaizduoti reikiami saugumo stereotipai. Siūlomas MBSE saugumo profilis yra suderintas su saugumo standartu ISO / IEC 27001:2013.

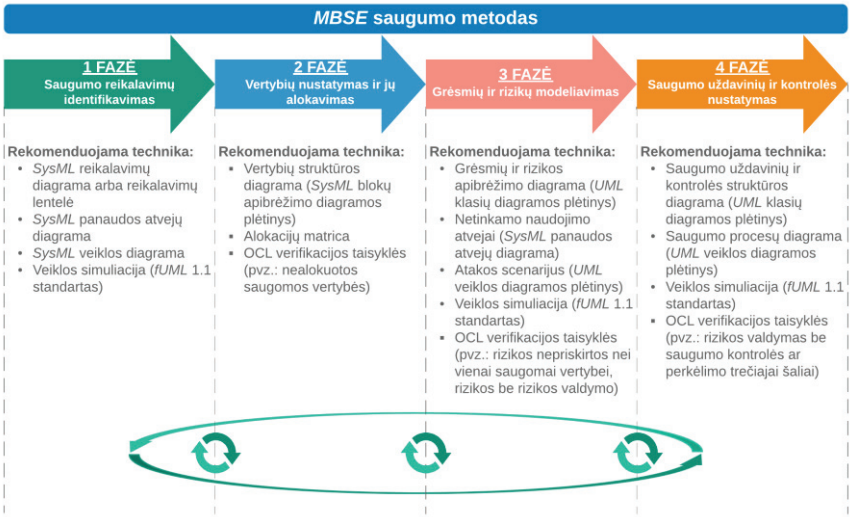


2 pav. MBSE saugumo profilis

UML profilis yra minimali priemonė sistemos saugumo analizei. Išsamiam siūlomo metodo išpildymui disertacijoje yra pateikiama:

- informacija, kokios naujos ir esamos *SysML* diagramos ir technikos turėtų būti įtrauktos į saugumo analizę. Be to, kokie elementai ir stereotipai turi būti pateikiami tose diagramose;
- gairės, aprašančios kiekvienos saugumo fazės esminius žingsnius;
- atsekamumo taisyklės;
- modelio kiekybinės analizės taisyklės;
- rekomenduojama modelio struktūra;
- pavyzdiniai projektai.

3 paveiksle pateikta apibendrinta MBSE metodo diagrama su saugumo fazėmis ir rekomenduojamomis technikomis.



3 pav. MBSE saugumo metodo fazės ir rekomenduojamos technikos

MBSE saugumo metodas turi 4 pagrindines fazes ir vieną pasiruošimo / būtinųjų sąlygų fazę:

- **Būtinosios sąlygos**. Prieš pradedant saugumo reikalavimų identifikavimą ir kitas saugumo analizės fazes, rizikos vertinimo metodika turi būti užfiksuota „Rizikos vertinimo metodikos“ stereotipe. Taip pat turi būti nustatytas skaitinis rizikos tolerancijos kriterijus, kuris vėliau bus naudojamas modelio verifikacijai.
- **1 fazė – Saugumo reikalavimų identifikavimas**. Šioje fazėje su saugumu susiję funkciniai ir nefunkciniai reikalavimai turi būti užfiksuoti „Saugumo reikalavimų“ stereotipuose, *SysML* reikalavimų diagramoje arba lentelėje. Tolesnis saugumo reikalavimų tikslinimas papildomai gali būti atliekamas naudojant *SysML* panaudos atvejų ir veiklos diagramas.
- **2 fazė – Vertybių nustatymas ir alokavimas**. Antrasis etapas skirtas apibrėžti saugomus objektus (stereotipai „Sistemos vertybė“, „Duomenų vertybė“, „Programinės įrangos vertybė“) ir alokuoti juos sistemos dalims iš loginės sistemos struktūros (naudojant *SysML* alokacijos ryšį). Ši informacija turėtų būti sumodeliuota Vertybių struktūros diagramoje ir (arba) alokacijų matricoje.
- **3 fazė – Grėsmių ir rizikų modeliavimas.** Ši fazė susideda iš dviejų dalių: elgsenos ir struktūrinės dalies. Elgsenos dalyje turėtų būti specifikuojama Netinkamo naudojimo atvejų diagrama ir

modeliuojama Atakos scenarijaus diagrama. Struktūrinėje dalyje turėtų būti apibendrinta visa su rizika susijusi informacija. Tam tikslui turi būti naudojama Grėsmių ir rizikos apibrėžimo diagrama, kurioje atvaizduojami ir sujungiami šie stereotipai: Rizika, Rizikos valdymas, Rizikos poveikis, Tikimybė, Grėsmė, Pažeidžiamumas.

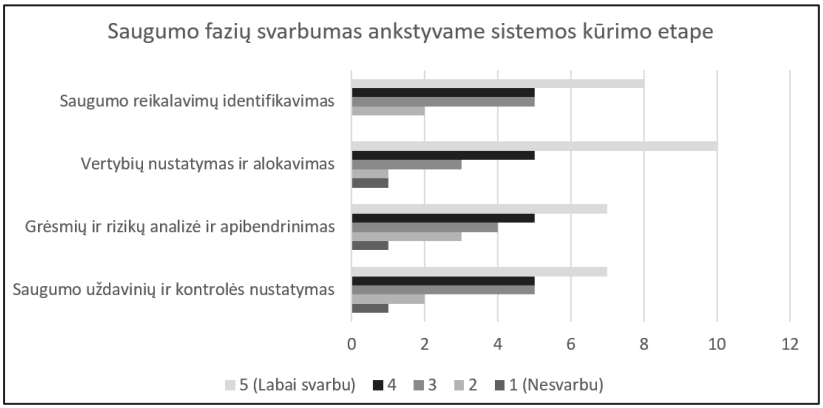
- **4 fazė – Saugumo uždavinių ir kontrolės nustatymas**. Paskutinis etapas yra skirtas apibrėžti saugumo kontrolės uždavinius ir saugumo kontrolę. Saugumo uždavinių ir kontrolės struktūros diagrama leidžia apibrėžti šiuos stereotipus: Saugumo kontrolė, Kontrolės uždavinys, Rizikos valdymas, Trečioji šalis. Saugumo procesų diagrama (UML veiklos diagramos plėtinys) leidžia aprašyti ir simuliuoti saugumo kontrolės algoritmą. Norint teisingai paleisti algoritmo simuliaciją – saugumo procesų diagrama turėtų būti modeliuojama laikantis *fUML1.1.* standarto reikalavimų.

Tyrime pateikiamos ir pagrindinės saugumo modelio tikrinimo taisyklės, kurios leidžia atsakyti į tokius klausimus:

1. Ar yra *Rizikų*, kurios neturi priskirto *Rizikos valdymo* elemento ir kurių *Rizikos lygis* yra didesnis nei *Rizikos tolerancijos* kriterijus *Rizikos vertinimo metodikoje*?
2. Ar yra *Rizikos valdymo* elementų, kurie neturi priskirtos *Saugumo kontrolės* ar *Trečiosios šalies*?
3. Ar yra *Rizikų*, kurios nėra priskirtos jokiai *Vertybei*?
4. Ar yra loginių sistemos blokų, kurie nėra alokuoti *Vertybėms*?

5 EKSPERIMENTINIS ĮVERTINIMAS

Pasiūlyto MBSE saugumo metodo eksperimentinis įvertinimas buvo atliktas keliomis iteracijomis. Pirmoje iteracijoje atliktas kokybinis pasiūlyto MBSE metodo tyrimas, kurio metu apklausta 20 ekspertų. 16 ekspertų atstovavo inžinerinėms šių sektorių organizacijoms: transporto, gynybos ir kosmoso tyrinėjimo, laivų, medicinos įrangos gamintojų, programinės įrangos kūrėjų. 4 ekspertai buvo iš akademinės bendruomenės. Apibendrinant šio tyrimo rezultatus galima teigti, kad du trečdaliai ekspertų sutiko, kad visos MBSE metodo siūlomos saugumo fazės yra labai svarbios arba svarbios ankstyvajame sistemos kūrimo etape (4 paveiksle pateikiami detalūs rezultatai). Ekspertai taip pat įvardijo, kokios MBSE priemonės labiausiai padėtų atlikti saugumo analizę (t. y. modelio simuliacija, galimybė atvaizduoti informaciją skirtingomis perspektyvomis, vienas tiesos šaltinis) ir kokios papildomos saugumo technikos galėtų būti įtrauktos į metodą ateityje (t. y. CVSS įverčiai, informacijos apsikeitimo analizė ir kt.). Be to, respondentai įvertino reikiamą mokymų trukmę, norint pradėti naudotis siūlomu MBSE saugumo metodu – 61 % teigė, kad tai galėtų užtrukti nuo 2 iki 5 dienų.



4 pav. Saugumo fazių svarbumas ankstyvajame sistemos kūrimo etape

Antrajame eksperimentinio įvertinimo etape suprojektuoti du detalūs modeliai *MagicDraw CASE* įrankyje, reprezentuojantys saugumo aspektą kibernetinei-fizinei sistemai ir programinės įrangos sistemai. Šie modeliai buvo eksperimentiškai tikrinami pagal šiuos kriterijus:

- Visapusiškumas – ar visi artefaktai, kurie yra reikalingi saugumo reikalavimams apibrėžti ir saugumo analizei vykdyti (pvz., palyginus su reikalavimais ISMS pagal standartą ISO / IEC 27001:2013), gali būti sukurti su siūlomu saugumo metodu MBSE modelyje.
- Nepertekliškumas – kiek siūlomo metodo diagramų / elementų / ryšių buvo panaudota abiem modeliams (t. y. ar visi siūlomo metodo artefaktai gali būti prasmingai panaudoti ir nėra pertekliniai).
- Teisingumas – ar reprezentatyvius modelius galima sumodeliuoti su siūlomu MBSE metodu nepažeidžiant UML kalbos taisyklių.
- Nuoseklumas – ar užtikrinamas modelio nuoseklumas tarp skirtingo saugumo fazių ir sistemos modelio / saugumo aspektų.

Kibernetinei-fizinei sistemai buvo pasirinktas hibridinio automobilio projektas iš *OMG SysML* specifikacijos. Šiuolaikiniai automobiliai turi daug sąsajų, per kurias įsilaužėliai gali bandyti vykdyti atakas (pvz.: OBD-II, USB, *Bluetooth*, belaidžio rakto sistema ir kt.), o tų atakų pasekmės gali būti labai rimtos. Hibridinio automobilio modelyje saugumo aspektas pagal siūlomą *MBSEsec* metodą buvo sumodeliuotas galios valdymo blokui. Šis saugumo modelis kartu su *MBSEsec* metodu buvo pristatyti straipsnyje, išspausdintame mokslo žurnale *Applied Sciences-Basel* [38].

Antrasis modelis pristatė kritinės programinės įrangos modernizavimo projektą skrydžio statusų sistemai. Skrydžio statusų sistema renka duomenis iš įvairių šaltinių (pvz.: avialinijų, ADS-B stotelių, eismo srautų valdymo sistemų), juos apdoroja, verifikuoja ir perduoda klientams. Bet koks šios sistemos darbo sutrukdymas (vientisumo, prieinamumo, konfidencialumo) gali sukelti didelius

nuostolius aviacijos industrijos įmonėms, pvz.: Paryžiaus Šarlio de Golio tarptautinio oro uosto sustabdymas valandai gali kainuoti daugiau kaip 1 mln. eurų Prancūzijos BVP [39]. Skrydžio statusų sistemos tyrimo rezultatai buvo pristatyti konferencijoje *IEEE 15th International Conference on System of Systems Engineering* [37].

Abiejų modelių – hibridinio automobilio ir skrydžio statusų sistemos – rezultatai parodė, kad visi artefaktai, kurie yra reikalingi saugumo reikalavimams apibrėžti ir saugumo analizei vykdyti, gali būti nepertekliškai, teisingai ir nuosekliai suprojektuoti MBSE modelyje su pasiūlytu saugumo metodu. Taip pat šis tyrimas patvirtino, kad siūlomas metodas yra universalus ir tinka tiek programinės įrangos sistemoms, tiek kibernetinėms-fizinėms sistemoms.

6 IŠVADOS

Šios disertacijos metu atliktas tyrimas atskleidė, kaip saugumo reikalavimų inžinerija ir saugumo analizės veiklos galėtų būti integruotos į MBSE, vykdomą ankstyvajame sistemos kūrimo etape. Pagrindinis tyrimo tikslas buvo sudaryti sąlygas sistemų ir saugos inžinieriams projektuoti saugias sistemas su pasiūlytu MBSE metodu. Atsakymai į tyrimo uždavinius ir pasiekti rezultatai yra pateikti žemiau:

1. Naujausia mokslinių darbų analizė parodė, kad MBSE yra tinkama aplinka sujungti saugumo reikalavimų inžineriją ir saugumo analizės veiklas į sistemų inžinerijos procesą. Saugumo aspektas yra labai svarbus kuriant sudėtingą sistemą, tačiau pagrindinės MBSE metodikos nesiūlo saugumo analizės (arba siūlo labai ribotas galimybes). Bandomasis tyrimas, kurio metu apklausta 10 inžinerinių organizacijų, buvo atliktas prieš kuriant MBSE saugumo metodą ir leido pasitvirtinti metodo reikalingumą, praktinį pritaikomumą ir suinteresuotų šalių poreikius.
2. Saugumo srities kalbos ir siūlomo MBSE metodo pagrindas buvo dalykinės srities konceptų modelis, kuriame sujungti analizės metu identifikuoti saugumo konceptai ir technikos.
4. Pasiūlytą MBSE saugumo metodą sudaro UML profilis su saugumo stereotipais; DSML saugumo paketas su naujomis saugumo diagramomis, verifikacijos taisyklėmis ir pavyzdiniais projektais. UML profilis ir DSML saugumo paketas buvo sukurti įrankiu *MagicDraw 19.0* ir gali būti įdiegti kaip įskiepiai į bet kurį suderinamą CASE įrankį. Metodo reikalavimai vienareikšmiškai aprašyti pagal IETF RFC2119 rekomendacijas ir gali būti atkurti bet kuriame UML kalbą palaikančiame CASE įrankyje. Pasiūlytas metodas yra vienas pirmųjų tokio tipo metodų tyrimo paskelbimo metu.
3. Kokybinis metodo įvertinimas – ekspertų apklausa – parodė, kad yra poreikis sujungti saugumo reikalavimų inžinerijos ir saugumo analizės

veiklas kartu su sistemos dizaino kūrimu MBSE modelyje naudojant CASE modeliavimo įrankį. Ekspertai patvirtino, kad visos saugumo fazės, pasiūlytos MBSE saugumo metode (Saugumo reikalavimų identifikavimas, Vertybių nustatymas ir alokavimas, Grėsmių ir rizikų modeliavimas, Saugumo uždavinių ir kontrolės nustatymas), yra svarbios norint sumodeliuoti ir sukurti saugią kompleksinę sistemą. Tyrimas parodė, kokios papildomos saugumo technikos galėtų būtų įtrauktos į naują metodo versiją (t. y. CVSS įverčiai, informacijos apsikeitimo analizė ir kt.).

4. Kiekybinio eksperimento etape buvo suprojektuoti ir įvertinti du detalūs modeliai, demonstruojantys metodo pritaikomumą realaus pasaulio objektams (hibridinio automobilio ir skrydžio statusų sistemos). Tyrimas parodė, kad siūlomas MBSE saugumo metodas leidžia visapusiškai, teisingai, nepertekliškai ir nuosekliai projektuoti saugumo aspektą tiek kibernetinėms-fizinėms, tiek programinės įrangos sistemoms.

7 LITERATŪROS SĄRAŠAS

1. NSF-National Science Foundation, “Cyber-physical systems (CPS),” 2017. [Online]. Available: https://www.nsf.gov/pubs/2017/nsf17529/nsf17529.pdf.
2. INCOSE, “The challenge of complex systems,” [Online]. Available: http://www.incose-coa.org/the-challenge-of-complex-syst.
3. J. Guckenheimer and J. M. Ottino, “Foundations for Complex Systems Research in the Physical Sciences and Engineering,” NSF Workshop, 2008.
4. INCOSE, Systems Engineering Handbook: A Guide for System Life Cycle Processing and Activities, 4th edition, Hoboken, NJ, USA: John Wiley & Sons, 2015.
5. R. S. Kalawsky, J. O'Brien, S. Chong, C. Wong, H. Jia, H. Pan and P. R. Moore, “Bridging the gaps in a model-based system engineering workflow by encompassing hardware-in-the-loop simulation,” *IEEE Systems Journal,* vol. 7, no. 4, p. 593–605, 2013.
6. J. Holt, S. Perry, M. Brownsword, D. Cancila, S. Hallerstede and F. O. Hansen, “Model-based requirements engineering for system of systems,” in *roceedings of the 2012 7th International Conference on System of Systems Engineering (SoSE)*, Genova, Italy, July 2012.
7. INCOSE UK, “What Is Model Based Systems Engineering (V2),” 2015. [Online]. Available: http://www.incoseonline.org.uk/Program_Files/Publications/zGuides_9.aspx?CatID=Publications.
8. É. Dubois, P. Heymans, N. Mayer and R. Matulevičius, “A Systematic Approach to Define the Domain of Information System Security Risk Management,” in *Intentional Perspectives on Information Systems Engineering*, Berlin, Springer, 2010, pp. 289-306.
9. C. Raspotnig, P. Karpati and A. L. Opdahl, “Combined Assessment of Software Safety and Security Requirements: An Industrial Evaluation of the CHASSIS Method,” *Journal of Cases on Information Technology (JCIT),* vol. 20, no. 1, pp. 46-69, 2018.
10. G. Styles and R. S. Kalawsky, “Research Top Challenges for MBSE in Industry 4.0 and IoT – Workshop Report,” 2015.
11. P. H. Nguyen, S. Ali and T. Yue, “Model-based security engineering for cyber-physical systems: a systematic mapping study,” *Information and Software Technology,* vol. 83, pp. 116-135, 2017.
12. B. L. Papke, “Enabling design of agile security in the IOT with MBSE,” in *Proceedings of the 2017 12th System of Systems Engineering Conference*

(SoSE), Waikoloa, HI, USA, 2017.

13. J. Jürjens and P. Shabalin, "Tools for secure systems development with UML," *International Journal on Software Tools for Technology Transfer,* vol. 9, pp. 527-544, 2007.
14. A. M. Madni and S. Purohit, "Economic Analysis of Model-Based Systems Engineering," *Systems ,* vol. 7, no. 1, pp. 1-12, 2019.
15. E. Carroll, "Systematic Literature Review: How Is Model-Based Systems Engineering Justified?," 2016. [Online]. Available: http://www.omgwiki.org/MBSE/lib/exe/fetch.php?media=mbse:incose_mbse_iw_2017:sand2016-11485_pe_uur_161109_howismodel-basedsystemsengineeringjustified_.pdf.
16. NIST, "Security Considerations in the System Development Life Cycle," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf.
17. A. R. Hevner, S. T. March, J. Park and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly,* vol. 28, no. 1, pp. 75-105, 2004.
18. T. W. Olle, H. G. Sol and I. G. MacDonald, Information Systems Methodologies: A Framework for Understanding, Boston, MA, USA: Addison-Wesley, 1991.
19. Sebok, "Systems Engineering: Historic and Future Challenges," 2019. [Online]. Available: https://www.sebokwiki.org/wiki/Systems_Engineering:_Historic_and_Future_Challenges.
20. L. E. Hart, "Introduction To Model-Based System Engineering (MBSE) and SysML," [Online]. Available: https://www.incose.org/docs/default-source/delaware-valley/mbse-overview-incose-30-july-2015.pdf.
21. A. Morkevicius, A. Aleksandraviciene, D. Mazeika, L. Bisikirskiene and Z. Strolia, "MBSE Grid: A Simplified SysML-Based Approach for Modeling Complex Systems," in *INCOSE International Symposium*, Adelaide, Australia, 2017.
22. INCOSE, "MBSE Wiki: Mehtodology and Metrics," 2020. [Online]. Available: http://www.omgwiki.org/MBSE/doku.php?id=mbse:methodology.
23. J. A. Estefan, "INCOSE Survey of MBSE Methodologies," INCOSE TD 2007-003-02, Seattle, WA, USA, 2008.
24. D. Mazeika, A. Morkevicius and A. Aleksandraviciene, "MBSE driven approach for defining problem domain," in *System of Systems Engineering*

(SoSE), Kongsberg, Norway, 2016.

25. B. Fabian, S. Gurses, M. Heisel, T. Santen and H. Schmidt, "A comparison of security requirements engineering methods," *Requirements Engineering,* vol. 15, no. 1, p. 7–40, 2010.
26. P. Salini and S. Kanman, "Survey and analysis on security requirements engineering," *Computers & Electrical Engineering,* vol. 38, no. 6, p. 1785–1797, 2012.
27. ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security: Part 1, International Organization for Standardization, 2007.
28. E. Albrechtsen, "Safety vs Security," 2003. [Online]. Available: http://www.iot.ntnu.no/users/albrecht/rapporter/notat%20safety%20v%20security.pdf.
29. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety,* vol. 139, pp. 156-178, 2015.
30. C. Raspotnig, V. Katta, P. Karpati and A. L. Opdahl, "Enhancing CHASSIS: A Method for Combining Safety and Security," in *International Conference on Availability, Reliability and Security*, Regensburg, Germany, 2013.
31. Object Management Group, "About the Unified Architecture Framework Specification Version 1.0," 2017. [Online]. Available: http://www.omg.org/spec/UAF/1.0/Beta2/.
32. D. Watson and A. Jones, "Risk Management," in *Digital Forensics Processing and Procedures*, 2013, pp. 109-176.
33. D. Mažeika and R. Butleris, "Identifying Security Issues with MBSE while Rebuilding Legacy Software Systems," in *IEEE 15th International Conference on System of Systems Engineering (SoSE)*, Budapest, Hungary, 2020.
34. D. Šilingas, R. Vitiutinas, A. Armonas and L. Nemuraitė, "Domain-specific modeling environment based on UML profiles," in *Information technologies*, Kaunas, Lithuania, 2009.
35. Object Management Group, "About the Meta Object Facility specification version 2.5.1," 2016. [Online]. Available: https://www.omg.org/spec/MOF;jsessionid=FE501A2F1AABFF3587B96AA1DE7F4EFF.
36. UML diagrams, "UML, Meta Meta Models and Profiles," 2020. [Online]. Available: https://www.uml-diagrams.org/uml-meta-models.html.
37. S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," 1997. [Online]. Available: https://tools.ietf.org/html/rfc2119.

38. D. Mažeika and R. Butleris, “MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems,” *Applied Sciences,* vol. 10, no. 7, pp. 1-18, 2020.
39. SESAR, “Addressing airport cyber-security. Final report,” 2016. [Online]. Available: https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf.
40. INCOSE, “SE vision 2025,” 2014. [Online]. Available: https://www.incose.org/AboutSE/sevision.
41. D. Mazeika and R. Butleris, “Integrating security requirements engineering into MBSE: Profile and guidelines,” *Security and Communication Networks,* p. 1–12, 2020.

8 AUTORIAUS PUBLIKACIJŲ DISERTACIJOS TEMA SĄRAŠAS

Straipsniai recenzuojamuose mokslo leidiniuose, turinčiuose cituojamumo rodiklį *Clarivate Analytics Web of Science* (*CA WoS*) duomenų bazėje:

1. **Mažeika, D.**; Butleris, R. Integrating security requirements engineering into MBSE: profile and guidelines // Security and Communication Networks. London: Wiley–Hindawi. ISSN 1939-0114. eISSN 1939-0122. 2020, vol. 2020, art. no. 5137625, p. 1-12. DOI: 10.1155/2020/5137625.
2. **Mažeika, D.**; Butleris, Rimantas. MBSEsec: Model-based systems engineering method for creating secure systems // Applied Sciences. Basel: MDPI AG. ISSN 2076-3417. 2020, vol. 10, iss. 7, art. no. 2574, p. 1-18. DOI: 10.3390/app10072574.

Straipsniai, išspausdinti tarptautinių konferencijų medžiagoje:

1. **Mažeika, D.**; Morkevičius, A.; Aleksandravičienė, A. MBSE driven approach for defining problem domain // 2016 11th System of Systems Engineering Conference (SoSE), IEEE, June 12-16, 2016, Kongsberg, Norway. Piscataway, NJ : IEEE, 2016. ISBN 9781467387279. p. 1-6. DOI: 10.1109/SYSOSE.2016.7542911.
2. Morkevičius, A.; Aleksandravičienė, A.; **Mažeika, D.**; Bisikirskienė, L.; Strolia, Ž. MBSE grid: a simplified SysMLbased approach for modeling complex systems // INCOSE international symposium: 27th annual INCOSE international symposium (IS 2017), Adelaide, Australia, July 15-20, 2017. San Francisco, CA : Wiley. ISSN 2334-5837. 2017, vol. 27, iss. 1, p. 136-150. DOI: 10.1002/j.2334-5837.2017.00350.x.
3. **Mažeika, D.**; Butleris, R. Model-based systems engineering approach for creating secure complex systems // 9th International workshop on

data analysis methods for software systems, DAMSS : Druskininkai, Lithuania, November 30 - December 2, 2017 / Lithuanian Computer Society, Vilnius University, Institute of Data Science and Digital Technologies, Lithuanian Academy of Sciences. Vilnius: Vilnius University, 2017. ISBN 9789986680642. p. 32. DOI: 10.15388/DAMSS.2017.

4. **Mažeika, D.**; Butleris, Rimantas. Identifying security issues with MBSE while rebuilding legacy software systems // SOSE 2020: IEEE 15th international conference of system of systems engineering, Budapest, Hungary, June 2-4, 2020: proceedings. Piscataway, NJ : IEEE, 2020. ISBN 9781728180519. eISBN 9781728180502. p. 1-4. DOI: 10.1109/SoSE50414.2020.9130491.

9 INFORMACIJA APIE AUTORIŲ

Išsilavinimas:

2015–2020	Informatikos inžinerijos doktorantūros studijos Kauno technologijos universitete
2016	Išklausytas studijų modulis Vienos universitete (Naujos kartos veiklos architektūros modeliavimas)
2010–2012	Įgytas verslo informacijos sistemų magistro laipsnis Vilniaus universitete
2006–2010	Įgytas verslo informatikos bakalauro laipsnis Vilniaus universitete

Darbo patirtis:

2019–dabar	Produkto vystymo vadovas UAB „OAG Aviation Worldwide“
2017–2019	Lektorius Kauno technologijos universitete
2014–2019	Sistemų analitikas / sprendimų architektas UAB „No Magic Europe“
2012–2014	Vyriausias sistemų analitikas UAB „ATEA Lietuva“
2010–2012	Programuotojas UAB „OptimusCRM“

10 ABSTRACT

10.1 Motivation[1]

Modern systems among industries such as automotive, medical devices, aerospace and defence are becoming extremely complex; therefore, traditional engineering methods are not enough for their successful realization. The systems have become more complex due to many factors, to name a few:

- Increased spectrum of technologies: complex systems have become cyber-physical systems (CPS) and now depend upon the seamless integration of computational algorithms and various physical components [1];
- Increased customer demands for more sophisticated systems and market or military competition [2];
- Systems consist of many components interacting in a network structure and usually these components are physically and functionally heterogeneous [3].

The discipline of systems engineering (SE) was initiated and developed to manage and unite work results of multidisciplinary engineering teams. The goal of SE is a successful realization of systems with the focus on gathering customer needs and defining required functionality early in the development cycle as well as documenting requirements, then proceeding with design synthesis and system validation [4]. Nowadays, organizations that cannot cope with systems complexity have switched (or are switching) from a document-based approach to a model-based approach in the SE activities. International Council on Systems Engineering (INCOSE) emphasizes MBSE importance, and they envision that MBSE will become a synonym of SE by 2025 [40]. The advantages of using models instead of documents in SE include the following [5, 6, 7]:

- Increased systems engineering efficiency by:
    - reusing existing projects or common components to support design and technology evolution;
    - enabling impact analysis of requirements changes;
    - improving communication across a multidisciplinary team;
    - enabling auto-generation of documentation.
- Reduced risk by early and iterative requirements validation and design verification;
- Managed complexity.

There are a few methods that guide users on how to get all the MBSE benefits when creating a system design model; sadly, almost all the analysed methods do not include the security analysis at the early stage of system design. Conversely, there are several tools and approaches that allow performing security

[1] The material in the “Motivation” section was presented by Mažeika et al. in [38, 41]

analysis at the initial phase of systems creation (e.g., Misuse Cases, Abuse Cases, Secure-Tropos, CHASSIS); however, they are disjointed from the systems engineering [8, 9].

Many researchers in their studies [10, 11, 12, 13] agree that there is a need to identify and tackle security risks during the systems engineering lifecycle. Nguyen et al. state that security objectives (such as confidentiality, integrity and availability) should be considered together with the business logic very early, which is crucial in engineering secure systems. Thus, MBSE could be a key helper because of the opportunity to manipulate models on a higher abstraction level, possibility to tailor generic modelling language (e.g., UML and SysML) with the security-related concepts and performing reasoning with external analysis tools [11]. Nowadays, the MBSE activity mostly focuses on the design phase, which is usually done by the systems engineers. When developing complex systems, the security analysis is often conducted in parallel with the design phase. Papke argues that security engineers and systems engineers should work together, and a joint design process or framework is needed in order to define security aspects in a common model [12].

The authors recognize that the biggest value of MBSE activities is gained when system validation and verification are performed at the early phase of system design, especially in terms of change of cost [14, 15]. In such case, the defects could be fixed with less impact and the rework prevented in the later phases, thus mitigating uncertainties to cost and schedule [15]. The same principles apply in the security field: the risk identification and mitigation are the most effective and maximize the return on investment if it is integrated into the design process and utilized in the early stages [16].

10.2 Object and scope of research

The research object of this work is the MBSE method for creating secure complex systems formalized with the UML language.

The scope of the research encompasses the following fields:

- Systems Engineering (SE) and Model-Based Systems Engineering (MBSE),
- Security Requirements Engineering,
- Modelling approaches and techniques for security analysis,
- Security Risk Management,
- Standards and methods for creating domain specific language and formalizing the MBSE security method.

10.3 Problem statement and research questions

One of the most important challenges that organizations are trying to solve while creating a new system is how to develop a secure system. Traditionally, the system is treated as a secure system if the principles of Confidentiality, Integrity

and Availability are guaranteed.

Nowadays, the system security engineering field includes a variety of methods and techniques for tackling security risks; however, they are disjointed from each other as well as from SE. As MBSE serves as an umbrella for connecting various disciplines, this disparity between security and SE becomes more evident. The problem of this dissertation focuses on the lack of MBSE methods for tackling security issues at the early stage of system creation.

This dissertation should give answers to the following research questions:

1. Is MBSE a suitable application for defining and managing security requirements and conducting security analysis for complex cyber-physical and software systems at the early stage of system creation?
2. Are the UML Profiles and MOF standard the right techniques and standards for creating and formalizing the domain-specific language and MBSE security method?
3. How can security requirement engineering and security analysis activities be included in the MBSE process to design a secure system and leverage MBSE advantages?
4. What are the security concepts that should be introduced in systems modelling language in order to support security aspects during the early stages of system development?
5. What domain specific extensions (e.g., stereotypes, diagrams, verification rules) are needed for security analysis?
6. Can the automated MBSE tools, including but not limited to simulation, verification and validation, change impact analysis, single source of truth, be successfully applied in the security field by using the proposed method?
7. Does the proposed MBSE security method allow completely, concisely, correctly and consistently model security aspects of both cyber-physical and software systems in the CASE tool?

10.4 Aim and objectives

The main aim of this research is to find an effective way to solve the secure system creation challenge at the early stage of system development by taking advantage of Model-Based Systems Engineering.

Research tasks:

1. To analyse research literature, methods, applications and tools related to:
    - 1.1. Systems Engineering (SE) and Model-Based Systems Engineering (MBSE),
    - 1.2. Security Requirements Engineering,
    - 1.3. Modelling approaches and techniques for security analysis,
    - 1.4. Security Risk Management,

1.5. Standards and methods for creating domain specific language and formalizing the MBSE security method.

2. To develop a formalized MBSE method for creating secure complex systems.
3. To perform an experiment for evaluating the suitability of the created method and evaluate the research results.

10.5 Research methodology

The research methodology followed in this thesis is based on a traditional design science research pattern [17]. The starting point was the evaluation of the state-of-the-art of the existing literature in SE, MBSE, security requirements engineering and security risk management fields. This initial evaluation of the state-of-the-art literature analysis aimed to identify the limitations and potential needs in SE, MBSE and security areas, align concepts and techniques and select the core elements for the domain specific language and the MBSE security method.

Next, the feasibility survey was conducted in order to validate the business needs before creating the MBSE security method.

The next chapter of "MBSE method for creating secure systems" started by presenting the standards and tools that are needed to define domain-specific language and formalize the MBSE security method (i.e., UML 2.5 Profiling capability, MOF standard, DSML definition framework). Next, a classical modelling language design approach where the key concepts of the domain should be determined at first and then a new language could be created to support it was used [18]. The security concepts that were identified in the literature analysis part were mapped and represented in the domain model; then, UML profile was prepared according to the domain model. The requirements of MBSE security method implementation (which as well serves as guidelines) were defined in textual form by following IETF RFC2119 recommendations.

The evaluation part consisted of several iterations. Firstly, the qualitative evaluation of the proposed MBSE security method was done by surveying experts from the MBSE, engineering and academic fields. Then, two case studies were modelled using the suggested MBSE security method in which the viability for cyber-physical and software systems were presented. Finally, these case studies were experimentally tested against four criteria: completeness, correctness, conciseness and consistency.

10.6 Defended statements

The statements that were defended by the research are as follows:

1. MBSE is a suitable application for defining and managing security requirements and conducting security analysis for complex cyber-physical and software systems at the early stage of system creation.

2. The UML 2.5 Profiling capability and MOF standard are the right techniques for creating and formalizing the domain-specific language and MBSE security method.
3. The automated MBSE tools, including but not limited to simulation, verification and validation, change impact analysis, single source of truth, can be successfully applied in the security field by using the proposed method.
4. All the artefacts that are mandatory for defining security-related documentation (i.e., comparing with the ISO/IEC 27001:2013 standard) can be correctly, concisely and consistently modelled in a model-based environment with a suggested MBSE method for both cyber-physical and software systems.

10.7 Major contributions and novelty

The scientific novelty and major contributions of this thesis are listed below:

1. The thesis introduces the security domain model that maps concepts and techniques from the modelling approaches for security analysis and security requirement engineering. The mapping and the security domain model help security and system engineers to understand and compare wide range security terms and techniques that could be used at the early stage of system design.
2. It introduces a novel MBSE method for creating secure systems. It allows specifying and analysing security aspect together with the system model for complex systems. The suggested MBSE method covers the full spectra of security phases, starting with security requirements, continuing on assets, model threats and risks and finishing with control objectives and controls. The use of model-based techniques ensures that the security and system artefacts are aligned at the early phase of system design, and MBSE benefits are extended to security engineer discipline.
3. The author's suggested security method is one of the first methods in the MBSE field at the time of publication.

10.8 Practical significance

The key practical significance of this research is the step towards linking systems engineering and security engineering disciplines via model-based environment. The expected practical results of the research:

- The MBSE method for creating secure systems is prepared and can be used for designing any complex system with an MBSE CASE tool.
- The MBSEsec profile and DSML definition package was prepared with the MagicDraw 19.0 CASE tool and can be installed as a plugin in any compatible tool. Moreover, the requirements of the MBSE method

implementation unambiguously define how this method can be recreated with any tool.
- The MBSEsec method provides guidelines on how to use and take leverage of the MBSE benefits (e.g., model verification and simulation, change impact analysis, traceability).
- The proposed MBSEsec method is aligned with the ISO/IEC 27001:2013 security standard which is used by many engineering organizations.
- The thesis presents two case studies for automotive and software system domains.
- The practical significance was validated in two surveys: feasibility and qualitative expert evaluation.

10.9 Scientific approval

Two articles presenting dissertation results were published in peer-reviewed scientific journals that are indexed in the Clarivate Analytics Web of Science (CA WoS) database. Moreover, the results of this research were presented in three international conferences in Norway, Australia and Hungary and in one international workshop in Lithuania. The corresponding publications were published in the conference proceedings. A detailed list of publications is provided in Chapter 7 “List of publications of Donatas Mažeika on the theme of dissertation”.

10.10 Structure of the Dissertation

The dissertation consists of an introduction of the thesis, four main chapters, general conclusions, references, a list of the author’s publications and appendixes. Moreover, the terms and abbreviations, lists of figures and tables are presented at the beginning of this work. The total scope of the thesis is 99 pages; it includes 48 figures and 12 tables.

UDK 004.056(043.3)

SL344. 2021-05-04, 2 leidyb. apsk. l. Tiražas 50 egz. Užsakymas 118.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas