

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Meelis Lutsar 180443IAIB

**NUTIKA KUUELAMU ELUTAGAMISSÜSTEEMI
TÖÖKINDLUSE PROTOTÜÜPIMINE**

Bakalaureusetöö

Juhendaja: Jüri Vain
PhD

Tallinn 2025

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: Meelis Lutsar

01.06.2025

Annotatsioon

Töö eesmärgiks on koostada Uppaal Stratego abil mudelipere, mis kirjeldaks formaalselt IGLUNA kuuelamu ohutuse ja töökindluse mehhanismid ning võimaldaks neid simulatsioonipõhiselt analüüsida ja verifitseerida nende korrektsus mudelkontrolli meetodiga.

Autor on töös kirjeldanud ohutuskriitiliste süsteemide alused, võimalikud hädaolukorrad ja nende lahendamine ning kuuelamu süsteemi arhitektuur, mis oleks aluseks antud töös kavandatud superviisorsüsteemi väljatöötamisele. Töös koostatud mudelid võimaldavad veenduda, et tekkinud hädaolukorrad on loogiliselt lahenduvad enne lahendusmehhanismide reaalsel programmeerimist.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 32 leheküljel, 6 peatükki, 11 joonist, 0 tabelit.

Abstract

Prototyping the Reliability of the Life Support System in a Smart Lunar Habitat

The aim of the thesis is to create a family of models using Uppaal Stratego that would formally describe the safety and reliability mechanisms of the IGLUNA lunar home and would allow them to be analyzed on a simulation basis and verified for correctness using the model checking method.

In the thesis, the author has described the foundations of safety-critical systems, possible emergencies and their resolution, and the lunar home system architecture, which would be the basis for developing the supervisor system proposed in this thesis. The models created in the thesis allow us to verify that the emergencies that arise are logically solvable before the actual programming of the resolution mechanisms.

The thesis is written in Estonian and is 32 pages long, including 6 chapters, 11 figures and 0 tables.

Lühendite ja mõistete sõnastik

Andur	seade, mis muundab mõõdetava füüsilise suuruse signaalliks, mida on parem mõõta [1].
Juhtimiskontuur	tarkvara jälgib sensorite ja muu vajaliku abil protsessi ja vajadusel reguleerib selle tööd, et saavutada/säilitada soovitud eesmärk või eesmärgid [2]. (<i>Control loop</i>)
ESA	Euroopa Kosmoseagentuur. Euroopa kosmoseuuringutega tegelev asutus, mille liikmeteks on 23 Euroopa riiki (<i>European Space Agency</i>)
Kosmiline kiirgus	kosmiline kiirgus on energeetilised subatomaarsed osakesed, mis saabuvad väljastpoolt Maa atmosfääri [3].
Mööduv viga	ajutine tõrge süsteemis, mis ei ole põhjustatud püsivast riistvararikkest. Need on tavaliselt lühiajalised ja lahenevad sageli iseenesest ilma välise sekkumiseta [4]. (<i>Transient fault</i>)
NASA	Riiklik Aeronautika- ja Kosmoseadministratsioon. Ameerika Ühendriikide riigiasutus, mis vastutab teaduse ja tehnoloogia eest, mis on seotud lennunduse ja kosmosega [5]. (<i>National Aeronautics and Space Agency</i>)
Tõrge	seadme vms. töövõime osaline või täielik kadu, kõrvalekalle tavapärasest talitlusest [6].
Verifitseerimine	protsess, mille käigus kontrollitakse, kas miski vastab seatud nõuetele või spetsifikatsioonidele [7].
Viga	eksimus reegli, normi, standardi, fakti vms. vastu, kõrvalekaldumine õigest sooritusest [8].

Sisukord

1	Sissejuhatus	9
1.1	Probleemist ja motivatsioonist	9
1.2	Ülesande püstitus	9
2	Töö teoreetilised alused ja kasutatavad tehnoloogiad	11
2.1	Kuuelamu rajamise plaane	11
2.2	Ohutuskriitilised süsteemid ja nende töökindluse alused	11
2.3	Uppaali ajaga automaadid	13
2.4	Uppaal Stratego	13
3	Kuuelamu tõrgete, ohusituatsioonide ja nende kompensatsioonimehhanismide taksonoomia	15
3.1	Sissejuhatus	15
3.2	Päikesepursked	15
3.3	Andurite ekslikud näidud	17
3.4	Elektrilühised	20
3.5	Tulekahju	20
3.6	Elektritootmise vähenemine	22
3.7	Ebanormaalne atmosfääri koostis	23
3.8	Ebanormaalne õhurõhk	25
3.9	Süsteemi tarkvara viga	27
4	Tõrgete kompensatsioonimeetmete kavandamine	29
4.1	Ohutuse ja töökindluse tagamise üldprintsüübid	29
4.2	Ohutussüsteemi arhitektuur	30
4.2.1	Süsteemi üldine kirjeldus	30
4.2.2	Süsteemi konfiguratsioon	30
4.2.3	Otsustusprotsess	31
4.2.4	Kuuelamu süsteemist laekuvate andmete usaldusväärsuse tagamine	32
4.2.5	Atmosfääri monitoorimine	33
4.2.6	Tulekahju monitoorimine	34
4.2.7	Andurite edastatud näitude monitoorimine	34
4.2.8	Mitmele samaaegse ohusituatsioonile reageerimine	35
5	Mudelipõhine verifitseerimine	36
5.1	Tõrgete kompenseerimise mehhanismide korrektsusomadused	36

5.2	Kombineeruvate tõrgete kompenseerimise korrektsuse verifitseerimine . .	37
5.3	Edasised arendused	38
6	Kokkuvõte	40
	Kasutatud kirjandus	41
	Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaa-	
	davaks tegemiseks	44

Jooniste loetelu

Joonis 1.	Päikesepurske lahendamise mudeli süsteemi automaat.	16
Joonis 2.	Päikesepurske lahendamise mudeli keskkonna automaat.	16
Joonis 3.	Anduri ekslike näitude lahendamise mudeli süsteemi automaat. . . .	18
Joonis 4.	Anduri ekslike näitude lahendamise mudeli keskkonna automaat. . .	19
Joonis 5.	Tulekahju lahendamise mudeli süsteemi automaat.	21
Joonis 6.	Tulekahju lahendamise mudeli keskkonna automaat.	22
Joonis 7.	Ebanormaalse atmosfääri koostise lahendamise mudeli süsteemi automaat.	24
Joonis 8.	Ebanormaalse atmosfääri koostise lahendamise mudeli keskkonna automaat.	24
Joonis 9.	Ebanormaalse õhurõhu lahendamise mudeli süsteemi automaat. . .	26
Joonis 10.	Ebanormaalse õhurõhu lahendamise mudeli keskkonna automaat. .	27
Joonis 11.	Anduri eksliku näidu (ülemine kontuur) ja päikesepurske lahenda- mise süsteemi (keskmine kontuur) kokkusulatatud automaadid (alumine kontuur).	38

1. Sissejuhatus

1.1 Probleemist ja motivatsioonist

IGLUNA on Šveitsi organisatsiooni Space Innovation interdistsiplinaarne platvorm, kus üliõpilased üle maailma kavandavad ja teevad koostööd uuenduslike projektidega kosmosuuringute tulevikuks ja elu parandamiseks Maal [9]. Septembris 2019 algas IGLUNA 2020, mille eesmärgiks oli demonstreerida kosmoseelupaiga tehnoloogiaid, mis säilitavad elu ekstreemses keskkonnas, ja kasutada uudseid tehnoloogiaid kaugjuhtimisrežiimi kaudu [10]. IGLUNA 2020 projekt on lõppenud, kuid teema jätkub teistes rahvusvahelistes projektides. Kuna kosmosevaldkonna organisatsioonidel ja erafirmadel on plaane Kuule ja Marsile baase rajada ning aastakümneid on olnud erinevaid plaane ja unistusi muuta inimkond mitmeplaneediliseks liigiks, on töö eesmärk endiselt relevantne.

Töö eesmärgiks on lähtudes ülaltoodud rahvusvahelistes projektides pakutud kontseptuaallahendustest koostada kuuelamu töökindlusomadusi kirjeldavad mudelid. Mudelite koostamisel võtsin aluseks eelduse, et süsteem peaks olema võimalikult veakindel ehk kõik torked peaksid olema lahendatavad või nende mõju leevendatav. Probleemid on jaotatud kolme klassi, mille alusel saab torked klassifitseerida ja prioritseerida. Töö raames koostas vastavalt torkete liikidele nende kompenseerimismehhanismide kirjeldavad mudelid ning näitasin kuidas neid komponeerida, kui erinevad torked esinevad samaaegselt. Mudelite kasutamine süsteemi kavandamise faasis võimaldab uurida ja kontrollida lahenduste toimimist enne nende reaalset programmeerimist, mis säästab arendusressurssi ning aega. Käesolevas töös loodud torkete lahendamist kirjeldavate mudelite spetsiifika seisneb selles, et mudelid on aluseks süsteemile, mis peab juhtima maavälistes tingimustes toimivat elukeskkonda.

1.2 Ülesande püstitus

Antud lõputöö eesmärgiks on koostada mudelite pere projektis „Igluna“ väljatöötatud kuuelamu ohutuse ja töökindluse mehhanismide formaalseks kirjeldamiseks, simulatsiooni põhiseks analüüsiks ja korrektsuse verifitseerimiseks mudelkontrolli meetodiga. Töös loodavad mudelid peavad kirjeldama kuidas süsteem saab erinevaid ohusituatsioone lahendada juhtudel kui need esinevad ükshaaval, kui ka kombineerudes samaaegselt. Mudelid on aluseks modelleerimiskeskonnale Uppaal Stratego abil ohuolukorra lahendamiseks sobiva torkete kompenseerimise strateegia sünteesil. Kirjeldatud lähenemine võimaldab uurida ja

kontrollida lahenduse toimimist enne selle reaalselt programmeerimist, hoida kokku aega ja ressursse ning verifitseerida kas disainitud kompenseerimisprotseduurid suudavad tagada kuuelamus ka tõrgete korral nõutava elukvaliteedi.

Lõputöö autori ülesanneteks on kirjeldada mudelite abil juhtimisstrateegiad üksikute ohuolukordade lahendamiseks ning integreerida kriitilisemate ohuolukordade mudelid, mille abil saab luua ja lahendada erinevaid ohuolukordi kombineerivaid stsenaariume. Mudeli korrektsuse saab verifitseerida Uppaal Strategoga, näidates, et mudel on loogiliselt korrektne ning võimaldab verifitseerida, et ohuolukordadele leitakse etteantud kitsenduste tingimustes nõutav lahendusstrateegia.

2. Töö teoreetilised alused ja kasutatavad tehnoloogiad

2.1 Kuuelamu rajamise plaane

Ainsad senini Kuule rajatud ajutised elupaigad on olnud Apollo kuumoodulid [11]. Need olid planeeritud viima kaks astronauti Kuu pinnale, võimaldama neil Kuu pinnal elada ja ümbrust uurida ning viia nad seejärel tagasi Kuu orbiidile [12].

NASA ehk Riiklik Aeronautika- ja Kosmoseadministratsioon plaanib Artemise programmi raames lisaks muudele eesmärkidele rajada pikaajalise kohaloleku. Hiina, Venemaa, India, Kanada, Jaapan ja Euroopa Liit on väljendanud huvi NASAga Kuu peal koostööd teha või siis konkureerida [13]. NASA plaanib inimesed Kuule maandada 2027. aastal ning kuuelamu rajamist alustada mitte varem kui 2033. aastal [14]. Hiina plaanib inimesed Kuule maandada 2030. aastal ning rajada Kuule alalise baasi 2035. aastaks. Hiina Kuu-plaanides osaleb Hiina riigimeedia sõnul tosin riiki ning umbes 40 välisorganisatsiooni [15]. Eelneva kirjelduse põhjal võib järeldada, et erinevatel riikidel ja organisatsioonidel on suurem huvi rajada Kuule kuuelamu.

Üks projektidest, mis inspireeris ka käesoleva lõputöö teema valikut oli IGLUNA. IGLUNA 2020 oli Space Innovationi projekt, milles 15 tiimi kümnest Euroopa ülikoolist arendasid erinevaid tehnoloogia demonstraatoreid kosmoseelamu jaoks, mis suudaks säilitada elu äärmuslikes tingimustes ning kasutaks uusi tehnoloogiaid. Projekt kattis erinevaid teemasid elamu kontseptsioonist ja ehitamisest kuni elualalhoiusüsteemide, side ja inimeste heaoluni. Kuigi projekt lõppes ametlikult juulis 2020, jätkavad mitmed tiimid arendustööd praeguse ajani [16] ja ka käesolevas töös leiavad edasiarendust just kuuelamu töökindluse ja ohutuse tagamisega seotud teemad.

2.2 Ohutuskriitilised süsteemid ja nende töökindluse alused

Töökindlus on ohutuskriitiliste süsteemide töös kasvava olulisusega nõue, kus süsteem peab tagama oma teenuste kvaliteedi sõltumata rikestest, rünnakutest, konfiguratsiooni muutmistest jne. Töökindluse saavutamine süsteemis on keeruline, sest see võib minna vastuollu mõne teise süsteemile esitatud nõudega, näiteks turvalisusega või jõudlusega [17].

Tõrkekindlus on süsteemi võime tagada sobiv funktsionaalsus ka tõrgete korral, mis

mõjutavad süsteemi. Ohutuskriitilistes süsteemides, nagu elektri- ja sidevõrgud, transpordivahendid ja tootmistaristud on oluline, et süsteem jätkaks tööd ka ebasoodsas keskkonnas [18]. *Tõrge* tähendab seadme töövõime osalist või täielikku kadu, kõrvalekallet tavapärasest talitlusest [6]. *Viga* tähendab eksimust näiteks reegli või normi vastu, kõrvalekallet õigest sooritusest [8]. Eesti keeles kasutatakse neid sageli mittesüstemaatiliselt, kuid antud töös on need selgelt defineeritud terminid ja erineva tähendusega. Tõrge võib süsteemis tekkida näiteks mõne detailiga nagu andur, mis on katki läinud. Samas võib tõrge tekkida ka välise mõjuri tulemusel. Kuuelamut või mõnda selle osa võib tabada kosmiline kiirgus või päikesepurse, mille tulemusel mõni süsteemi osa lakkab töötamast. Viga on näiteks valesti kirjutatud tarkvara, mis toimib vastavalt programmeeritule kuid seda tehes saavutab planeeritust erineva eesmärgi. Tõrkekindlus on elualalhoiusüsteemis väga oluline, sest süsteem peab tõrke või vea tekkimisel suutma funktsioneerimist jätkata, et tagada kuuelamu ohutus seal viibivatele astronautidele.

Tõrkekindlus vigadele, mis kuuelamu ohutust mõjutavad, on jaotatud kolme klassi, mille aluseks olen võtnud Anish Arora ja Sandeep S. Kulkarni kirjutatud teadusartiklis "*Component Based Design of Multitolerant Systems*" välja pakutud klassid [19]. Nende klasside põhjal saab hinnata vigade tõsidust ehk millise prioriteediga peaksid astronautid ja missioonijuhtimiskeskus nende kõrvaldamisega tegelema ning mida peaks kuuelamu arvutisüsteem nende kõrvaldamiseks tegema.

Klassid on järgmised:

- Tolerantne maskeerimisele – vea tekkimisel viga isoleeritakse ning isoleerimine ei mõjuta süsteemi tööd. Süsteem tuvastab kõrvalekalde õigest sooritusest ning see tuleb kõrvaldada, kuid see ei nõua viivitamatut sekkumist, sest süsteem on võimeline funktsioneerimist jätkama ka antud vea olemasolul. Tolerantne maskeerimine on näiteks andurite edastatud ekslikud näidud, mille korral tuvastab süsteem vigase anduri ja ei kasuta selle näite kuni vea kõrvaldamiseni.
- Ebatolerantne maskeerimisele – vea tekkimisel viga ei isoleerita ning see mõjutab süsteemi tööd. Viga võib, aga ei pruugi olla viivitamatut sekkumist nõudev. Sellised vead vajavad siiski astronautide ja missiooni juhtimiskeskuse sekkumist, sest süsteemi normaalne töö taastub alles siis, kui viga on kõrvaldatud. Antud klassi kuuluvad näiteks elektritootluse vähenemine, mis suure tõenäosusega segab astronautide tegevust ja päikeseloided, mis on otseselt ohtlikud kuuelamule ja selle elanikele.
- Tolerantne veakindlusele – vea tekkimisel viga ei isoleerita ja see mõjutab süsteemi tööd. Erinevalt eelnevast klassist, kus ainus lahendus on vea otsene kõrvaldamine, kompenseerib süsteem vea, kasutades selleks ettenähtud lahendust. Oluline on eristada, et siinkohal ei taasta süsteem eelnevat seisutaset vaid tagab töö jätkumise või-

malikkuse hoolimata teenuse kvaliteedi langusest. Sellesse klassi kuulub näiteks väiksem õhuleke, sest süsteem kompenseerib selle lekkiva ruumi eraldamisega, kuid ei paranda leket ennast.

2.3 Uppaali ajaga automaadid

Uppaali ajaga automaat koosneb olekutest (*location*) ja olekute vahelistest siiretest (*edge*). Olek saab olla kas *normal*, *committed* või *urgent*. *Normal* olekul võib aga ei pea olema ajaline kitsendus. Ajalise kitsenduse täitumisel täidetakse üks väljuvatest siiretest, mille täitmistingimus (*guard*) on tõene. *Committed* olekus aeg ei progresseeru ning viivitus ei ole lubatud. *Committed* olekust peab automaadi täitmine liikuma hetkeliselt järgmisse olekusse. *Urgent* olekus aeg samuti ei progresseeru, kuid *normal* olekute vaheldumine on lubatud [20]. Siirde täitmisel omistatakse siirdel olevatele muutujatele uued väärtused ja nullitakse vajadusel mudeli kell(ad). Siiretel saab määrata ka sünkroniseerimistingimusi, kasutades kanaleid, milles sünkroniseerimise suund on määratud sümbolitega „!“ (väljuv) ja „?“ (sisenev), ning siiretele saab omistada kaalusid, et kirjeldada siirde valimise tõenäosust [21]. Siirded võivad olla juhitavad (pidev nool) ning mittejuhitavad (katkendlik joon). Kasutusel võivad olla globaalsed muutujad, aga ka lokaalsed muutujad, mille tüüp võib olla *clock* (kell), *channel* (kanal), *bool* (tõeväärtus), *integer* (täisarv) või massiiv [22].

2.4 Uppaal Stratego

Kuuelamu Otsustussüsteemi demonstraatori realiseerin, kasutades otsustusmootorina Uppaal Strategot. Eelduseks on see, et kuuelamu elutähtsaid funktsioone juhtiv superviisor-süsteem edastab andmed Strategole, mis modelleerib elamu seisundit ja tagastab kõige tõenäolisema stsenaariumi, mida süsteem saab omakorda kasutada planeerimisel ning eriti ajakriitiliste otsuste tegemisel.

Kõik selles töös kirjeldatud mudelid on verifitseerimise keerukuse vähendamiseks disainitud ühtse struktuuriga. Mudelid koosnevad kahest automaadist, millest üks kirjeldab ohutuse tagamise süsteemi (edaspidi „süsteem“) ja teine selle keskkonda (tõrgete tekkimise mehhanismi). Süsteemi mudel kirjeldab, kuidas juhtimissüsteem peaks reageerima tekkinud olukorrale ning eesmärgiks on tõestada, et modelleeritud tingimustel süsteem jõuab seisundisse „*Compensated*“, mis tähendab, et olukord on lahendatud. Keskkonna mudel kirjeldab võimalikke tõrgete ja ohuolukordade tekkimist ja tingimusi, milles need tekivad. Keskkonna mudelit on võimalik parameetriliselt seadistada muutes tingimused keerulisemaks või lihtsamaks.

Uppaal Stratego on tööriist, mida kasutatakse reaalajasüsteemide modelleerimiseks ja verifitseerimiseks. See sobib kasutamiseks süsteemides, mille modelleerimisel saab kasutada ajaga automaate ja nende paralleelkompositsiooni. Informatsiooni liikumine süsteemis on modelleeritud kasutades kahte mudeli konstruktsiooni - kanaleid ja automaatide vahel jagatavaid andmestruktuure - globaalmuutujaid [23].

Uppaal Stratego integreerib kahte teist Uppaali perekonna tööriista, Uppaal SMC ja Uppaal Tiga. Strategol on klassi objektid, mida saab luua, võrrelda, optimeerida ja kasutades etteantud strateegia raames seatud piiranguid. Stratego kasutamisel näiteks ajalehe lugemise ajastamisel, kus iga lugeja loeb lehte erinevalt ning erineva ajakuluga, loob Stratego lugejate jaoks optimaalse strateegia, mitte ei koosta staatilist planeerijat [24].

Stratego võimaldab modelleerida reaalajasüsteeme ajaga automaatide võrguna, neid verifitseerida, optimeerida käitumist, võrrelda strateegiaid ning mõõta nende efektiivsust kasufunktsiooni suhtes. Stratego võimaldab koostatud strateegiaid uurida enne nende lõplikku realiseerimist [25].

Uppaali perekonda kuuluvad tööriistad koosnevad kolmest osast: kirjeldavast keelest, simulaatorist ja mudeli kontrollijast. Kirjeldav keel on mittedeterministlik käsukeel, mis kirjeldab süsteemi käitumist automaatide võrguna, millel on muutujad kellade ja andmete jaoks.

Simulaator on verifitseerimistööriist, mis võimaldab uurida arendamise varastes staadiumites süsteemi käitumist konkreetsete stsenaariumide läbimängimise teel. Mudeli kontrollija saab süsteemi olekuruumi läbides kontrollida süsteemi ohutuse ja saavutatavuse omadusi ehk analüüsida, kas süsteemis seatud piirangutega on võimalik jõuda ettenähtud seisundisse. Mudeli kontrollija võib automaatselt luua ka diagnostika jälje, mis selgitab miks antud süsteemi osa vastab või ei vasta kirjeldatud omadustele [26].

Uppaali tööriistade peret arendavad Uppsala Ülikool Rootsi Kuningriigis ja Aalborgi Ülikool Taani Kuningriigis [27].

3. Kuuelamu tõrgete, ohusituatsioonide ja nende kompensatsioonimehhanismide taksonoomia

3.1 Sissejuhatus

Antud peatükk käsitleb mõningaid tüüpilisi ohusituatsioone, mis võivad kuuelamus tekkida ja selle tööd mõjutada. Peatükis on välja toodud olukordi, mis võivad tekkida süsteemi tõrke tagajärjel, erakorralisi ohusituatsioone, mis tekkivad ootamatult ja võivad kiiresti muutuda eluohtlikuks, ning ka olukordi, kus jaama töö on häiritud elamu süsteemist sõltumatu põhjusel. Ohusituatsioone esitatakse süstemaatiliselt taksonoomiana, kus iga olukorra puhul sisaldab kirjeldus järgmisi punkte: ohuolukorra olemus, selle tuvastus, mõju elukeskkonnale ja inimestele, ohuolukorra klass, elamupoolne korrigeerimine, meeskonna teavitus ja käitumisjuhised. Enamikule olukordadele on lisatud ka olukorra lahendamise mudelid ja nende kirjeldused. Mõnel olukorral ei ole mudelit lisatud, kuid need on konstrueeritavad samade mallide põhjal.

3.2 Päikesepursked

Olemus: päikesepurse on plahvatus Päikese pinnal, mis tekib, kui Päikese magnetväljadesse salvestatud energia järsult vabaneb. Sellised magnetväljad asuvad tavaliselt päikesepilekkide juures[28].

Tuvastus: ESA ehk Euroopa Kosmoseagentuuri vastavasisuline hoiatus. Sellise hoiatussüsteemi kasutamisel pole vaja arendada ja ehitada Kuule eraldi süsteemi, mis päikesepurskeid tuvastaks, sest vastava hoiatuse annab ESA *Space Weather Office* [29].

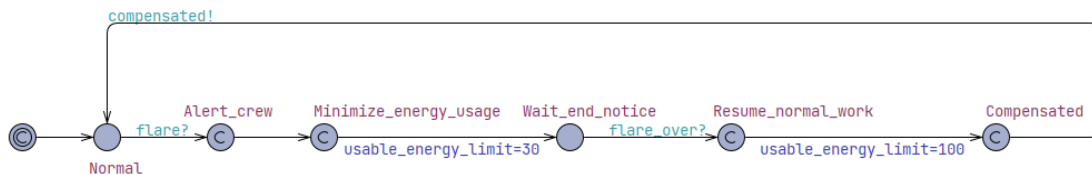
Mõju: Kuul asuvat elamut ning selle astronautidest elanikke ohustavad röntgenkiirgus, gammakiirgus ja muu radiatsioon [30].

Klass: ebatolerantne maskeerimisele

Elamupoolne korrigeerimine: süsteem ei saa olukorda korrigeerida, sest see on kuuelamust sõltumatu sündmus. Süsteem saab lülitada välja mittekriitilised süsteemid ning minimeerida energiatarbimist kuni oht on möödas. Süsteem loeb olukorra lõppenuks, kui on saanud Maalt vastava korralduse.

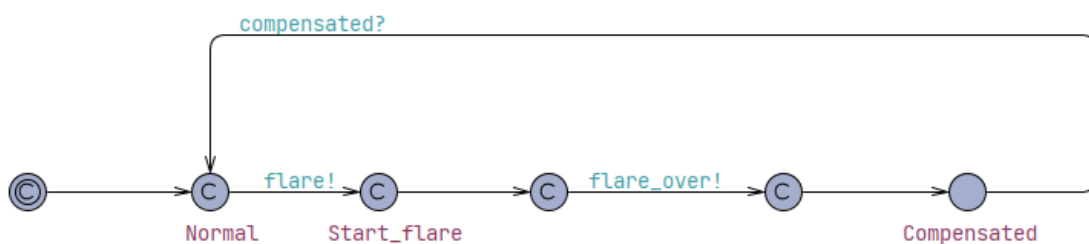
Meeskonna teavitus ja käitumisjuhised: kuuelamule saadetakse sidesüsteemi kaudu hoiatus, milles on oodatava purske kirjeldus ja ennustatav toimumisaeg. Meeskond varjub purske ajaks spetsiaalselt selleks ettenähtud sektsiooni, mis kaitseb meeskonnaliikmeid ohtlike kiirguste eest. Purske ajal katkeb tõenäoliselt raadioside Maaga ning astronautid saavad ainult oodata. Olukord lõpeb siis, kui side Maaga taastub ning missioonijuhtimiskeskus saadab astronautidele kinnituse, et oht on möödas.

Ohusituatsiooni lahendamise mudel:



Joonis 1. Päikesepurske lahendamise mudeli süsteemi automaat.

Päikesepurse on süsteemi jaoks võrdlemisi unikaalne juhtum, sest süsteem ei saa olukorda korrigeerida ning see kajastub ka mudelis. Diagrammil läheb süsteem algolekust normaalolekusse (“Normal”) ning on seejärel ootel. Päikesepurske tekkides annab süsteem meeskonnale häire, mis saabub kanali *flare* kaudu. Energiakasutus minimeeritakse ning süsteem saab kasutada kuni 30% tavapärasest energiakogusest. Seejärel jäädakse ooteseisundis ootama olukorra lõpu teadet. Pärast teate laekumist, taastab süsteem normaalse töö, loeb ohuolukorra lõppenuks (“Compensated”) ning naaseb normaalolekusse, teavitades keskkonnamudelit ohuolukorra lahendamisest, kasutades kanalit *compensated*.



Joonis 2. Päikesepurske lahendamise mudeli keskkonna automaat.

Valikute vähesus kajastub ka keskkonnamudelis, kus on ainult üks võimalus edasi liikuda. Normaalseisundist („Normal”) antakse kanali *flare* kaudu süsteemile häire. Diagrammil on näha ka mitmed vaheolekud, mis on vajalikud süsteemi ja keskkonna automaatide sünkroniseerimiseks. Sünkroniseerimine on antud mudelis oluline, sest ühe automaadi olek sõltub teise automaadi olekust. Viimase vaheoleku järel liigutakse seisundisse „Compensated”, mille ajal saadetakse süsteemile teade olukorra lõpust, kasutades kanalit *flare_over*.

Süsteemilt kinnituse laekumisel kanali *compensated* kaudu, liigub ka keskkonna automaat tagasi normaalolekusse.

3.3 Andurite ekslikud näidud

Olemus: andurid võivad ajutise rikke (*transient fault*) või mõne muu mõjutuse korral anda ebaõigeid näitusid, mis mõjutavad süsteemi tööd

Tuvastus: süsteem peab näite omavahel ning lubatud piirmäärade suhtes ristvõrdlema. Juhul kui süsteem tuvastab tõrke, peab see vastavalt vajadusele tõrke korrigeerima. Andur võib vale näidu edastada ajutise tõrke tõttu, näiteks kosmilise kiirguse sähvatuse mõjul. Sellisel juhul on tegemist ajutise rikkega, mis ei kujuta ohtu, ning süsteem ignoreerib viga. Samas võib vale näit tekkida ka anduri alalise rikke tõttu. Sellisel juhul tuleb antud andur isoleerida, et takistada süsteemi valede andmete alusel otsuseid tegemast. Süsteem peab alati olema teadlik anduritest, mida ei saa enam usaldada, et ristvõrdlemisel ei kasutataks valesid näite.

Ennetav reageerimine: anduri ennetav hooldus ning varasem väljavahetamine. Hooldused ja vahetused ei välista anduri tõrkeid, kuid vähendavad oluliselt nende esinemise tõenäosust.

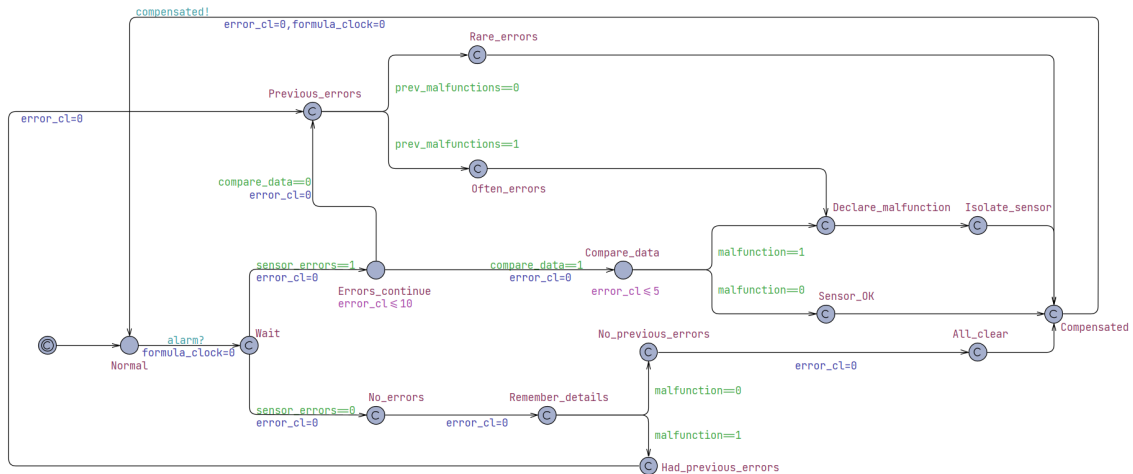
Mõju: süsteem võib ebaõigete andmete alusel võtta vastu valesid otsuseid, mis võivad segada süsteemi teiste osade tööd ja halvimal juhul ohustada elamut ning astronautide elu ja tervist.

Klass: tolerantne maskeerimine

Elamupoolne korrigeerimine: juhul kui anduri seisundi jälgimisel selgub, et andur edastab suure tõenäosusega ebaõigeid näite, isoleeritakse see süsteemist.

Meeskonna teavituse ja käitumisjuhise: Ebausaldusväärne andur ei eelda tingimata meeskonna kohest reageerimist. Meeskond saab anduri kohta teavituse ja peab hooldustööde raames vastavalt vealogis antud infole anduri välja vahetama.

Ohusituatsiooni lahendamise mudel:

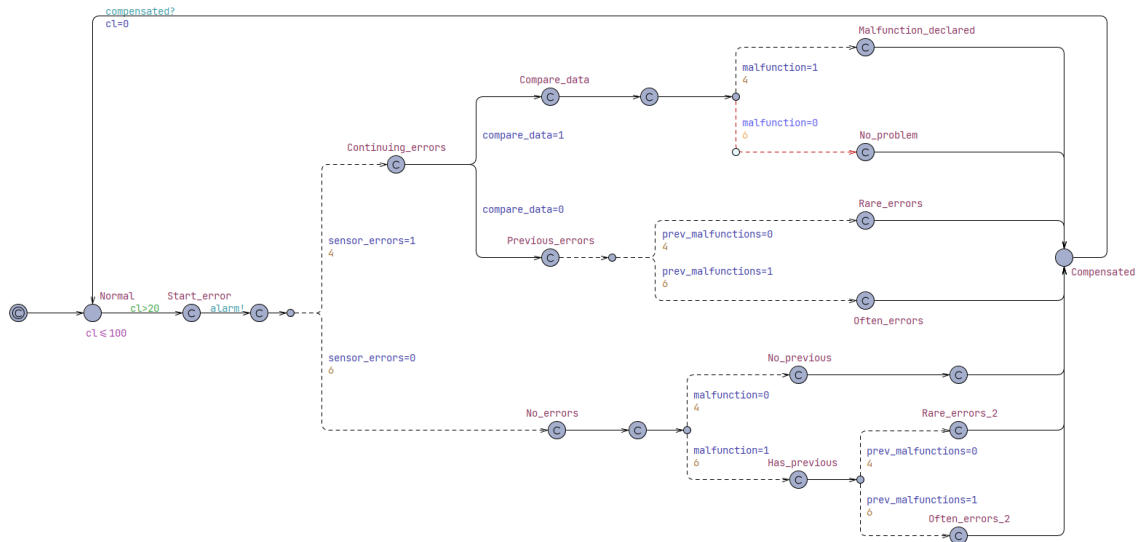


Joonis 3. Anduri ekslike näitade lahendamise mudeli süsteemi automaat.

Andurite ekslikud näidud on süsteemi jaoks keeruline probleem. Mudeli käivitumisel on edasiseks tegevuseks kaks võimalust.

Ekslike näitade jätkumisel (“*Errors_continue*”) näitavad Boole’i muutujad *prev_malfunctions=0* ja *prev_malfunctions=1* esmalt, kas anduril on varasem veaajalugu või mitte. Juhul kui ei ole, võrreldakse teiste antud ruumi andurite andmeid ning andmete põhjal kuulutatakse sensor korras olevaks (“*Sensor_OK*”) või rikkis olevaks (“*Declare_malfunction*”). Rikkis oleva sensori korral see isoleeritakse ning ohuolukord loetakse lõppenuks ehk jõutakse seisundisse “*Compensated*”. Varasema veaajaloo korral otsustatakse anduri seisund veaajaloo põhjal. Juhul kui ekslikke näite on edastatud harva, on andur terve ning muul juhul loetakse see vigaseks.

Juhul kui tuvastatakse ekslik näit, aga mitte pidev ekslikke näitude edastamine, minnakse teist teed (“*No_errors*”). Vea andmed salvestatakse ning juhul kui varasemaid vigu ei ole, loetakse olukord lõppenuks. Varasema veaajaloo korral otsustatakse anduri seisund veaajaloo põhjal.



Joonis 4. Anduri ekslike näitude lahendamise mudeli keskkonna automaat.

Keskkonna automaat jaguneb kaheks suuremaks haruks, mis omakorda jagunevad väiksemateks harudeks. Kõigil lahknemistel otsustab valiku juhuse (eeldame, et keskkond käitub mittedeterministlikult), mis mõjutab ka lõplikku süsteemi otsust anduri seisundi osas.

Ülemine suurharu sätestab süsteemile olukorra, kus ekslike näitude edastamine jätkub (*sensor_errors=1*). Selle valiku tõenäosus on veidi väiksem alumise haru valiku tõenäosusest. Järgmisena otsustatakse olekus “*Continuing_errors*”, kas andmete võrdlemine on vajalik või mitte (*compare_data* võrdub 1 või 0). Juhul kui valitakse, et andmeid peab võrdlema, valitakse kas andur on katki või mitte ning siinkohal kaldub edasine tõenäosus anduri korrasoleku kasuks. Pärast seda liigutakse asukohta “*Compensated*” ning jäädakse ootama süsteemi teadet olukorra lahendumise kohta.

Juhul kui olekus “*Continuing_errors*” otsustatakse, andmete võrdlemisest loobuda, valitakse seejärel kas anduril on veaajalugu või mitte ning liigutakse olekusse “*Compensated*”, sest keskkonnaautomaat on selleks ajaks genereerinud süsteemile kõik andmed, mida see vajab olukorra tuvastamiseks ja lahendamiseks.

Alumine haru on oluliselt lihtsam kui ülemine haru ning mudelis on selle valik tõenäolisem. Seisundist “*No_errors*”, liigutakse vaheolekusse, kus valitakse, kas anduril on varasemalt tõrkeid olnud (“*Often_errors*”) või mitte (“*Rare_errors*”). Juhul kui valitakse, et anduril on olnud varasemaid tõrkeid, valitakse kas need tõrked on haruldased või mitte ning seejärel liigutakse olekusse “*Compensated*”. Varasemate tõrgete puudumise valimisel liigutakse kohe olekusse “*Compensated*”.

3.4 Elektrilühised

Olemus: Isolatsioonimaterjalide kahjustumine mehhaanilise või termilise vigastuse mõjul, mille põhjuseks võib olla näiteks elektromagnetkiirguse sähvatus või tarbimisvoolu ülekoormus.

Tuvastus: lühise puhul peaksid esmajärjekorras rakenduma elektrikaitsmed, kuid kuna lühis võib tekitada tulekahju, siis tuleb elektrisüsteemi monitoorida. See on vajalik, et takistada lühist elektriseadmeid kahjustamast ja tulekahjut tekitamast.

Mõju: lühised võivad tekitada tulekahju ja/või kahjustada elektriseadmeid

Klass: ebatolerantne maskeerimisele

Elamupoolne korrigeerimine: elamu korrigeerib lühiseid, lülitades lühisesse sattunud elektrisüsteemi välja, ja saadab hoiatuse. Sõltuvalt süsteemist võib lühis jaama tööd oluliselt häirida.

Meeskonna teavitust ja käitumisjuhiseid: astronautid peavad kindlaks tegema lühise põhjuse ning selle kõrvaldama enne kui jaama normaalne töö saab jätkuda.

3.5 Tulekahju

Olemus: tulekahju on kontrolli alt väljunud, kahju põhjustav põlemine [31].

Tuvastus: Suitsu-, vingugaasi- ja temperatuuriandurite signaalid

Süsteem monitoorib ruumide temperatuure ja jälgib, et ruumides poleks suitsu või vingugaasi. Eesmärk on tulekahju tuvastada võimalikult algusjärgus, et piirata selle mõju kuuelamule ning meeskonnaliikmetele. Süsteem peab käivitama tulekahjualarmi, kui tuvastab ruumis suitsu, vingugaasi või ebatavaliselt kõrge temperatuuri.

Ennetav reageerimine: mittepõlevate materjalide kasutamine piirab põlengu intensiivsust ja ulatust.

Mõju: tulekahju suletud ruumis on äärmiselt ohtlik, kuna see kasutab kiiresti ära kogu hapniku ning temperatuur ja põlemisgaasid on astronautidele väga ohtlikud.

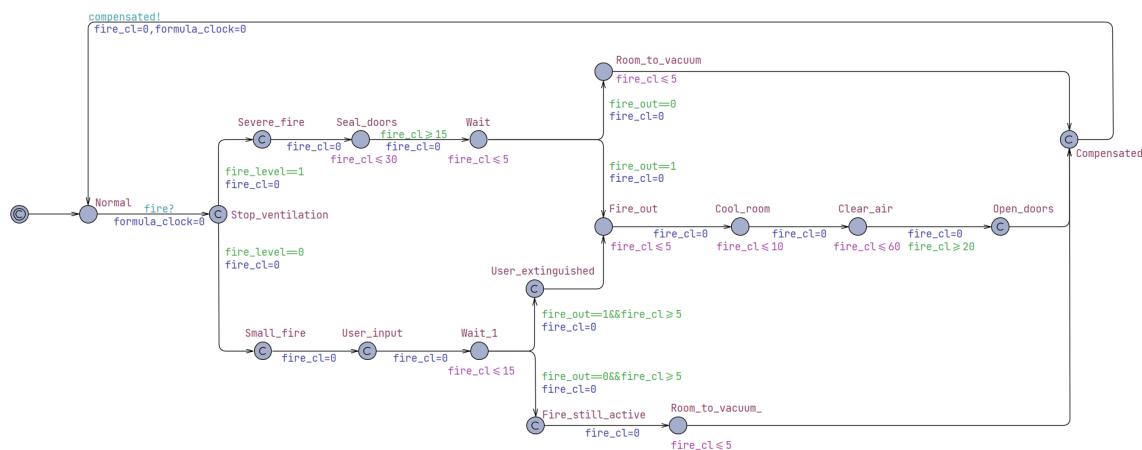
Klass: ebatolerantne maskeerimisele

Elamupoolne korrigeerimine: elamu võimaldab astronautidel sekkuda ning põlengu iseseisvalt kustutada. Suuremate põlengute puhul isoleerib süsteem automaatselt vaheuste abil ruumi, kus põleng asub, ja üritab seda aktiivselt summutada, lastes tulekahjul ära kasutada kogu ruumis oleva hapniku.

Tulekahju kustumise järel jahutab elamu kahjutulest haaratud ruumid ning puhastab õhu mürgistest gaasidest. Pärast seda kui on kindel, et tulekahju uuesti ei sütti, avatakse suletud uksed ja elamu normaalne töö saab jätkuda.

Meeskonna teavitus ja käitumisjuhised: meeskonnaliikmed saavad hädaolukorrast teada tulekahjualarmi ajal. Alarmi korral peavad meeskonnaliikmed esmalt liikuma kogunemispaika ning uurima, mis on juhtunud ja kust häire pärineb. Seejärel tuleb olukorrale vastavalt kas tulekahju kustutada või evakueeruda.

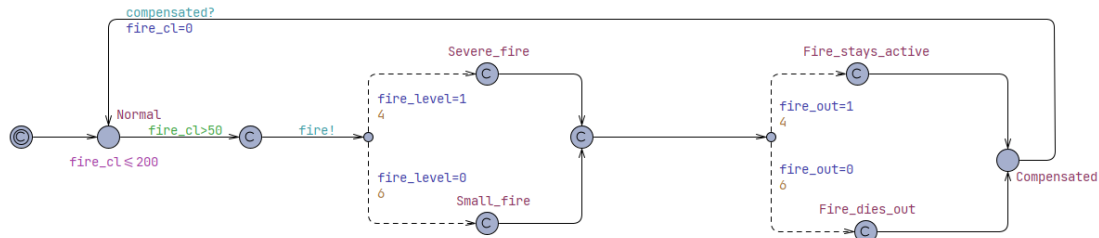
Ohusituatsiooni lahendamise mudel:



Joonis 5. Tulekahju lahendamise mudeli süsteemi automaat.

Süsteemi jaoks on tulekahju väga ajakriitiline ohuolukord. Eristatakse kahte stsenaariumi. Ülemine haru kirjeldab ohuolukorda, mille korral on tegemist suurema tulekahjuga („Severe_fire“). Süsteem sulgeb peale astronautide evakueerumist ruumide uksed („Seal_doors“) ning jääb ootele („Wait“). Tulekahju kustumisel („Fire_out“), alustatakse ruumi jahutamist („Cool_room“) ja õhu puhastamist („Clean_air“) ning seejärel avatakse uksed („Open_doors“) ja olukord loetakse lõppenuks („Compensated“). Juhul kui tulekahju ei kustu ise, viiakse ruum pärast ootel olekut („Wait“) vaakumisse („Room_to_vacuum“) ning loetakse olukord lõppenuks („Compensated“).

Alumine haru kirjeldab käitumist väiksema tulekahju korral, kus antakse astronautidele aega tulekahju iseseisvalt kustutada. Tulekahju kustutamisel (“*User_extinguished*”) korral alustatakse sarnaselt ülemise haruga, ruumi jahutamist ja muud selle juurde kuuluvat. Tulekahju kustutamise ebaõnnestumisel võtab süsteem kustutamise üle ja viib põleva ruumi vajadusel vaakumisse.



Joonis 6. Tulekahju lahendamise mudeli keskkonna automaat.

Keskkonna automaat kirjeldab täpsemalt kahte tulekahju stsenaariumi. Normaalolekust antakse kanali *fire* kaudu tulekahjuhäire. Seejärel valitakse kas tegemist on suurema tulekahjuga või väiksema tulekahjuga (*fire_level* on vastavalt 1 või 0). Väiksemal tulekahjul („*Small_fire*“) eelis, sest väiksema algusjärgus tulekahju tõenäosus on suurem kui laialdase leviku ja mõjuga tulekahjul („*Severe_fire*“), sest ohutussüsteemi arhitektuur eeldab iga ruumi jälgimist mitmete anduritega. Tulekahju tüübi määramise järel valib keskkonna automaat kas tulekahju jätkub („*Fire_stays_active*“) või see kustub/kustutatakse („*Fire_dies_out*“). Tulekahju kustumise või jätkumise otsustab Boole'i muutujad *fire_out*, mis on vastavalt 1 või 0 ning eelis on tulekahju lõppemisel, sest kuna eelis on väiksema tulekahju tekkel, võib eeldada et tekkiv tulekahju on väike ja kustutatav. Viimaks liigutakse olekusse „*Compensated*“ ja tagasi algolekusse kui on saadud süsteemilt kinnitus kanali *compensated* kaudu.

3.6 Elektritootmise vähenemine

Olemus: elekter on kuuelamule elutähtis, sest ilma selleta ei tööta ükski kuuelamu süsteem. Kui saadaolev elekter ei kata tarbimist, peab elamu elektrit millegi arvelt kokku hoidma, mis võib astronaute mõjutada.

Tuvastus: süsteem saab pidevalt andmeid kui palju võimsust on parasjagu saadaval ning kui suur on vajalik tarbimine.

Ennetav reageerimine: kuuelamu elektritarbimist võrreldakse pidevalt elektritootmisega. Kui tuvastatakse, et tarbimine hakkab lähenema tootmisele, alustatakse ennetavalt tarbimise

piiramist vähemtähtsatest, madalama prioriteediga seadmetest. Tarbimist saab piirata vähendades süsteemide tööd tühjas toas ning lubades suure tarbimisega seadmetel, näiteks küttel ja toitu hoiustaval külmutuskapil, töötada intervallidega. Ennetav reageerimine ei mõjutaks kõrge prioriteediga seadmeid, näiteks elamut juhtivat arvutit, mis peab töötama pidevalt.

Mõju: elektritootmise vähenemine tähendab, et astronautid peavad elama tavapärasest energiasäästlikumalt, mis võib nende tegevusi segada.

Klass: ebatolerantne maskeerimisele

Elamupoolne korrigeerimine: Juhul kui tuvastatakse, et elektrit on saadaval vähem kui on tarvis, hakkab elamu elektritarbimist piirama, et tarbimine ei ületaks tootmist.

Meeskonna teavitus ja käitumisjuhised: kuuelamu saadab sellekohase teate ning seejärel alustab tarbimiskohtade prioriteetide alusel tarbimise vähendamist.

3.7 Ebanormaalne atmosfääri koostis

Klass: tolerantne veakindlusele

Olemus: kuuelamu elanikud hingavad õhku, mille koostist ning erinevate gaaside omavahelist tasakaalu tuleb pidevalt jälgida. Süsteem peab olema võimeline tuvastama kui elamu atmosfääris on inimesele kahjuliku gaasi kontsentratsioon liiga kõrge või kui gaaside tasakaal on paigast läinud. Kahjuliku gaasi kõrge kontsentratsioon võib tekkida, kui näiteks süsihappegaasi sisaldus õhus tõuseb umbes ühelt protsendilt kolmele ning gaaside tasakaal võib paigast minna, kui hapniku tase tõuseb näiteks 24 protsendini.

Tuvastus: kuuelamu peab eluruumide õhku pidevalt analüüsima ning tuvastama sealt kahjulikud gaasid.

Ennetav reageerimine: kuuelamu hakkab õhku filtreerima ja kahjulikke gaase keemiliselt siduma, kui tuvastab mõne gaasi taseme tõusu.

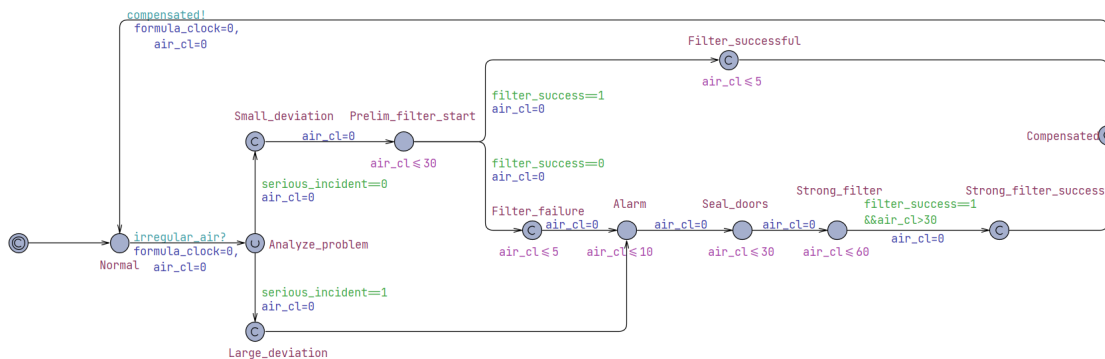
Mõju: ettenähtud parameetritest kõrvale kaldunud atmosfääri koostis tähendab, et astronautide hingatav õhk võib muutuda ohtlikuks nende tervisele ja/või elule. Tavapärane jaama töö on sel ajal häiritud.

Elamupoolne korrigeerimine: pärast häire põhjustanud gaasi kindlaks tegemist, peab

kuuelamu olukorra parandama elamu õhku filtreerides ja töödeldes, et kahjulike gaaside kontsentratsiooni vähendada või mõnda gaasi õhku lisama, et taastada tavapärane seisukord.

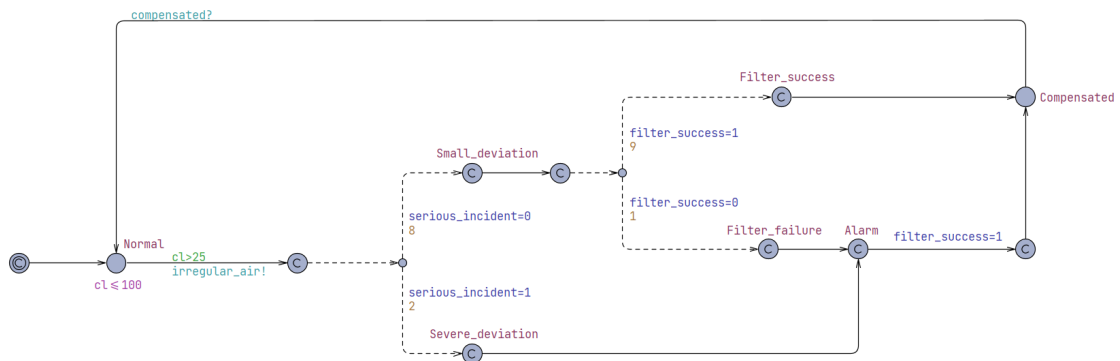
Meeskonna teavitus ja käitumisjuhised: astronautid peavad, samal ajal kui kuuelamu olukorda korrigeerida üritab, võtma kasutusele hapnikumaskid ja muu kaitsevarustuse või isoleerima ennast kahjulikke gaase sisaldavatest ruumidest.

Ohusituatsiooni lahendamise mudel:



Joonis 7. Ebanormaalse atmosfääri koostise lahendamise mudeli süsteemi automaat.

Normist kõrvalekaldunud atmosfääri koostis on süsteemi jaoks ajakriitiline probleem. Eristatakse kahte stsenaariumi. Esimene on väike kõrvalekalle, mille korral käivitatakse ennetav filtreerimine („*Prelim_filter_start*“) ning kui see õnnestub („*Filter_successful*“) loetakse olukord lõppenuks („*Compensated*“). Ennetava filtreerimise ebaõnnestumisel käivitatakse alarm ja suletakse uksed („*Seal_doors*“). Seejärel võetakse kasutusele tugev filtreerimine („*Strong_filter*“) ning selle õnnestumisel („*Strong_filter_success*“) loetakse olukord lõppenuks.



Joonis 8. Ebanormaalse atmosfääri koostise lahendamise mudeli keskkonna automaat.

Keskkonna automaat kirjeldab kaks ebanormaalse atmosfääri koostise stsenaariumi. Normaalsest antakse kanali *irregular_air* kaudu häire. Seejärel valitakse kas tegemist on väikese või suure kõrvalekaldega (*serious_incident* vastavalt 0 või 1). Väiksemal kõrvalekaldel on eelis, sest võib eeldada et inimeste kohalolu ja masinate töö mõjutab pidevalt õhus olevate gaaside tasakaalu. Väiksema kõrvalekalde korral valitakse kas filtreerimine õnnestus või mitte (*filter_success* vastavalt 1 või 0). Viimaks liigutakse olekusse „*Compensated*“.

3.8 Ebanormaalne õhurõhk

Klass: tolerantne veakindlusele

Olemus: inimese keha on harjunud kindla õhurõhuga ning liiga kõrge või madal õhurõhk mõjub inimesele kahjulikult ning võib hakata mõjutama astronauti võimet otsuseid vastu võtta. Astronautide elu ja tervise kaitseks peab süsteem pidevalt õhurõhku jälgima ning käivitama alarmi kui tuvastab normist kõrvalekalde.

Tuvastus: kuuelamu peab atmosfääri õhurõhku pidevalt mõõtma ning tuvastama normist erineva rõhu

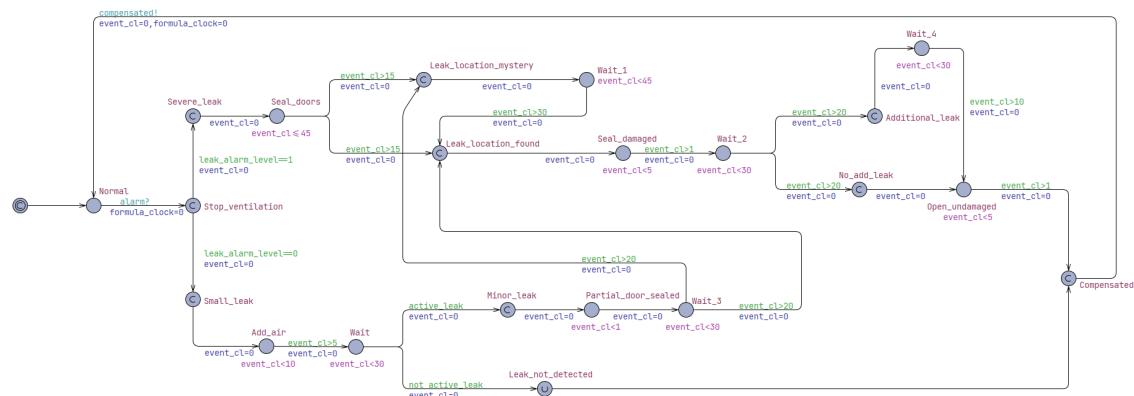
Ennetav reageerimine: tõsise lekke korral on ennetav reageerimine keeruline. Väiksema lekke korral saab elamu asuda tuvastama lekke asukohta. Kõrgema õhurõhu puhul on reageerimine analoogne. Suure muutuse korral on ennetavalt reageerida keeruline, kuid väiksema tõusu korral saab kindlale piirile lähenedes asuda rõhku langetama, et vähendada häire tekkimise tõenäosust.

Mõju: liiga kõrge või madal õhurõhk võib muutuda ohtlikuks meeskonnaliikmete tervisele ja/või elule. Tavapärane jaama töö on sel ajal häiritud.

Elamupoolne korrigeerimine: kuuelamu proovib lekke/ülerõhu põhjuse kõrvaldada, muutes tsirkulatsioonipumpade võimust või lisades atmosfääri õhku, et tõsta rõhk ettenähtud tasemele. Probleemi jätkudes peab süsteem eeldama, et elamus on tekkinud leke, sulgema ruumide vaheuksed ning tuvastama, kus on leke ning kas see on suur või väike.

Meeskonna teavitust ja käitumisjuhiseid: astronautid peavad, samal ajal kui elamu olukorda korrigeerida üritab, võtma kasutusele hapnikumaskid ja muu kaitsevarustuse.

Ohusituatsiooni lahendamise mudel:

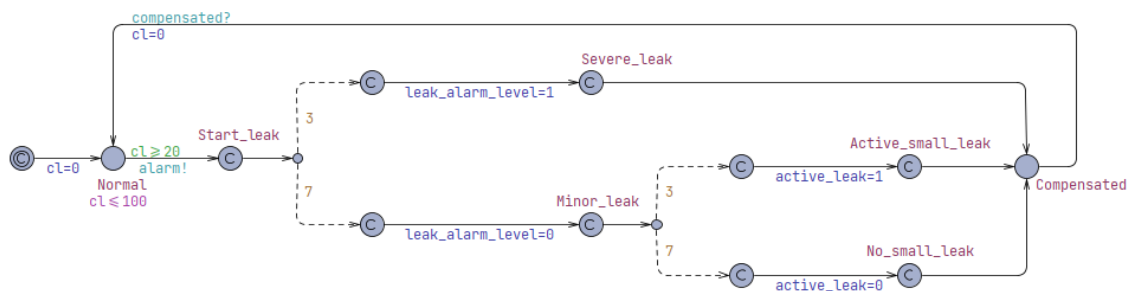


Joonis 9. Ebanormaalse õhurõhu lahendamise mudeli süsteemi automaat.

Süsteemi jaoks on see muutliku kriitilisusega olukord. Vähese muutuse korral („*Small_leak*“) lisatakse õhku („*Add_air*“) ning liigutakse ooteolekusse („*Wait*“). Juhul kui edasisi kõrvalekaldeid ei tuvastata („*Leak_not_detected*“), loetakse olukord lõppenuks („*Compensated*“). Väikese lekke tuvastamise korral („*Minor_leak*“), suletakse elamus osaliselt ukSED („*Partial_door_sealed*“) ning jäädakse ooteolekusse („*Wait_3*“). Osalise uste sulgemise järel lekkekoha leidmata jäämisel suletakse kõik ukSED. Juhul kui lekkekoht on endiselt teadmata, pikendatakse ooteolekut („*Wait_1*“) kuni lekkekoht leitakse („*Leak_location_found*“). Esimesest ooteolekust („*Wait_3*“) on võimalik minna ka kohe lekkega tegelemisele.

Suurema muutuse korral eraldatakse esmalt kõik ruumid, mis võimaldab ruume eraldi jälgida ning lekkekoht kiiresti üles leida.

Lekke leidmisel eraldatakse kahjustatud kuuelamu osa („*Seal_damaged*“) ning jäädakse veelkord ootele („*Wait_2*“), et veenduda lisalekete puudumises. Lisalekete puudumisel („*No_add_leak*“) avatakse korras ruumid („*Open_undamaged*“) ja loetakse olukord lõppenuks. Muul juhul esmalt oodatakse („*Wait_4*“), et tuvastada milliste ruumidega on probleeme ning seejärel avatakse kahjustamata ruumid ja loetakse olukord lõpetatuks.



Joonis 10. Ebanormaalse õhurõhu lahendamise mudeli keskkonna automaat.

Keskkonna automaat kirjeldab kahte ebanormaalse õhurõhu stsenaariumi. Normaalolekust antakse kanali *alarm* kaudu häire. Seejärel valitakse, kas tegemist on suurema või väiksema rõhuprobleemiga (*leak_alarm_level* on vastavalt 1 või 0). Väiksemal õhulekkel on eelis, sest kuna kuuelamu süsteemide tööd jälgitakse pidevalt, võib eeldada et muutused õhurõhus tuvastatakse varakult ning skafandrita astronauti majutava kuuelamu moodulid on põhjalikult ehitatud ja testitud. Tõsise rõhuprobleemi valimise korral liigutakse olekusse „*Compensated*“, sest edasist olukorra lahendamist selle otsused ei mõjuta. Süsteemi automaat ei lahenda olukorda täielikult, sest lekke füüsilise kõrvaldamise asemel tuvastatakse lekke asukoht ning isoleeritakse kahjustunud moodul(id) ülejäänud elamust. Väikese lekke valimise järel otsustab keskkonna automaat, kas süsteem peab tegelema ka lisalekke lahendamisega (*active_leak* vastavalt 1 või 0). Eelis on lisalekke puudumise valikul, sest mitu leket erinevates ruumides pole kuigi tõenäoline stsenaarium. Viimaks liigutakse olekusse „*Compensated*“ ja tagasi algolekusse kui süsteemilt saabub kinnitus kanali „*compensated*“ kaudu.

3.9 Süsteemi tarkvara viga

Klass: tolerantne veakindlusele

Olemus: vea tekkimine, mida süsteem ei suuda iseseisvalt lahendada. Selline viga võib olla näiteks mäluleke või programmeerimisel ja testimisel avastamata jäänud tarkvara viga.

Tuvastus: Süsteemil on ettenähtud kindel ajavahemik, mil ta peab jõudma otsuseni, mis on tehtud kogutud andmete põhjal. Juhul kui ta etteantud ajavahemiku jooksul ning korduvalt proovides otsusele ei jõua, eeldatakse, et kusagil on tekkinud viga.

Ennetav reageerimine: süsteemi töö monitoorimine vigade avastamiseks ja mõju piiramiseks. Mitme paralleelselt töötava mooduli kasutamine, mis kasutavad sama tarkvara kuid on programmeeritud ja testitud erinevate arendustiimide poolt.

Mõju: süsteemi tõrge võib olulisel määral mõjutada astronautide tööd, sest juhul kui elutagamissüsteemi töökindlus pole tagatud, võivad tõrked süsteemis põhjustada kaskaadefekti, mis omakorda võivad muutuda astronautidele ohtlikuks.

Elamupoolne korrigeerimine: tõrke tekkimisel proovib süsteem seda kõrvaldada restardiga eeldades ajutist viga (*transient fault*). Juhul kui restartimine ei aita ning tõrge püsib või tekib uuesti, annab süsteem kasutajale sellekohase teate.

Meeskonna teavitus ja käitumisjuhised: Juhul kui süsteem ei suuda tõrget restardiga kõrvaldada, lülitatakse ümber varurežiimile ning saadetakse meeskonnale teade. Seejärel saavad astronautid koos missioonijuhtimiskeskusega rikut uurima asuda.

4. Tõrgete kompensatsioonimeetmete kavandamine

4.1 Ohutuse ja töökindluse tagamise üldprintsüübid

Süsteem peab kuuelamu monitooringu andmete põhjal operatiivselt otsustama, kas kuuelamu seisund on normaalne või on tekkinud ohtlik olukord. Usaldusväärsete otsustuste tegemiseks võib monitooringu andmete kogumisega kaasneda siiski teatud ajaline viide. Sõltuvalt veaklassist on käitumine olukorras, kus andmete põhjal otsuse tegemine viibib, erinev. Juhul kui otsus puudutab atmosfääriga seotud andmeid ning otsuse tegemise ajakulu on ettenähtust suurem, üritab see esmalt ise otsuste langetada ja olukorda hallata enda restartimisega või kasutades reservsüsteeme. Juhul kui kindel arv restarte ja muud meetmed olukorda ei lahenda, teavitab süsteem kompenseerimismeetmete ebaõnnestumise osas meeskonda. See lähenemine tagab, et astronautid on süsteemi seisundist pidevalt informeeritud ning veateadete abil on inimesel võimalik õigeaegselt avastada kui süsteemil on tekkinud tõsisem tõrge, mida süsteem ise ei suuda või ei saa diagnoosida. Valisin sellise lähenemise, sest jaanuaris 2004 tekkis NASA marsikulgur Spiritil kriitiline olukord, kui see lõpetas infovahetuse Maaga. Inseneridel õnnestus kindlaks teha, et Spiriti normaalne töö on häiritud ning selle operatsioonisüsteem teeb järjestikuseid restarte. Kuna viga tekkis uuesti igal restardil, jäi kulgur ennast lõputult restartima, mis ajapikku hakkas kulgurit ohustama kuniks kulguri riistvara veakaitse rakendus ning võimaldas inseneridel kontrolli kulguri üle taastada [32]. Veast teavitamise kohustus esialgsete abimeetmete ammendumisel võimaldab analoogse vea kuuelamu süsteemidest kiiremini avastada ning ebasobiva kompensatsioonimehhanismi töö katkestada.

Kriitiliste süsteemide puhul peab kokkujooksmine ja andmete põhjal tehtavate otsuste viibimine olema minimaalne ning igasugune liigne ajakulutamine välistatud. Juhul kui otsustamine venib, peab süsteem käituma ennetavalt ja eeldama halvimat stsenaariumi, et vältida olukorda, kus otsustamatus ohustab astronaute. Samas on sellisel lähenemisel oluline olukordi pidevalt analüüsida ning tuvastatud probleeme jooksvalt prioritseerida. See on oluline vältimaks olukorda, kus halvima stsenaariumi eeldamine ning lahendamine ohustab astronaute või muudab lahenduse kasutamisega olukorra kriitilisemaks.

Oluline on ka varurežiimi kasutamine olukorras, kus süsteemis endas on tekkinud viga. Kuna süsteemi ei saa paranduse ajaks niisama välja lülitada, peab sel olema ka tagavara-süsteem, mida kasutada juhul, kui põhissüsteem vajab hooldust või parandust.

4.2 Ohutussüsteemi arhitektuur

4.2.1 Süsteemi üldine kirjeldus

Elutagamissüsteemi töökindlust tagav süsteem on oma põhimõttelt superviisorsüsteem. Superviisor sekkub, kui see peaks olema vajalik lokaalseid juhtimiskontuure seadistada. Muul ajal jälgib superviisor alama taseme kontrollereid, kuid ei osale aktiivselt nendes juhtimiskontuurides. Superviisor teeb otsused kontrolleritest saadud sisendandmete põhjal, mis on enne superviisorisse saabumist puhastatud signaalimürast ja muudest segavatest mõjuritest. Superviisoris eraldi andmete puhastamist ei toimu.

Kuuelamu juhtimiskontrollerid on töökindluse huvides nõrgalt seotud. See tähendab, et arhitektuuri erinevad tasemed jagavad informatsiooni, kuid on üksteisest selgelt eraldatud. See on vajalik, et takistada süsteemis tekkinud tõrgete levimist superviisorisse ning vastupidi.

Süsteemi ja olukordade lahenduste puhul on arvestatud, et kuuelamu on sisemiselt esmalt isoleeritav sektsioonidesse ehk probleemne osa elamust on isoleeritav ehk vaheustega eraldatav, et vältida probleemi laienemist kogu elamusse. Teine variant oleks olnud kasutada elamus näiteks turvapaiga ehk safe haveni kontseptsiooni, mida on kirjeldanud Robert Howard [33]. See tähendab, et juhul kui tekib olukord, mille tõttu pole elamu võimeline elutegevust toetama, liiguvad astronautid turvapaika, kus neil on võimalik viibida abi saamiseni. Turvapaik võimaldab meeskonnal märkimisväärselt tõenäolisemalt ellu jääda ning missiooniga jätkata [33]. Otsustasin mudelite planeerimisel lähtuda võimalusest, et astronautid saavad elamu osi esialgu isoleerida, sest minu hinnangul vaheuste ja turvapaiga kasutamine saavad üksteist täiendada. Vaheuksed võimaldavad turvapaika suundumist edasi lükata, aga samas tähendab turvapaiga olemasolu, et vajadusel saab hoopiski astronaut end isoleerida ja anda sellega elamule võimalus lahendada olukorda agressiivsemalt.

4.2.2 Süsteemi konfiguratsioon

Süsteem kasutab andmete kogumiseks erinevaid andureid ning analüüsib seejärel saadud infot. Superviisor saab alama taseme kontrolleritelt andmed ning selle eesmärgiks on sekkuda, kui see tuvastab ebatavalisi näite või ohuolukorra. Reageerimisajad on erinevad ja sõltuvad peamiselt tekkinud olukorra tõsidusest. Näiteks tulekahju on olulisem kui elektritootmise vähenemine. Mitme häire puhul otsustab süsteem milline neist on olulisem ehk eluohtlikum ja prioritseerib kompenseerimisprotseduurid vastavalt sellele juhul, kui

neile ei ole võimalik samaaegselt reageerida.

Superviisorsüsteem teostab kontrolli ettenähtud sagedusega, see tähendab, et monitooringu näite võrreldakse ajalises perspektiivis, mitte ei piirduta näiteks ainult nende logimisega. Superviisorsüsteem jaguneb käitumuslikult kaheks, passiivseks ja aktiivseks jälgimiseks. Passiivset jälgimist kasutatakse näiteks andurite järelevalvel. Andurite näite võrreldakse, et tuvastada võimalikke anomaaliaid, kuid kui nendest midagi ebatavalist ei leita, ei tee superviisorsüsteem midagi. Juhul kui ühe anduri näit on teistest erinev, muutub jälgimine aktiivseks. Võimaliku probleemi ennetamiseks kontrollitakse antud ruumi andurite näite sagedamini, et tuvastada, kas ekslik näit on juhuslik või mitte. Aktiivselt jälgitakse pidevalt näiteks atmosfääriga seonduvaid näite. Temperatuuri, atmosfääri koostise ja õhurõhu näite võrreldakse sageli, sest nendega seotud olukorrad võivad sageli kriitiliseks muutuda.

Superviisorsüsteemi teostatavas järelevalves on oluline ka ennetav käitumine. See pole projekteeritud ainult arvestusega, et tekkinud ohuolukord lahenduks, vaid sõltuvalt olukorrast on määratud ka piirid, millele lähenedes üritatakse olukorda parandada enne kui see muutub piisavalt tõsiseks, et anda häire ja kuulutada see ohuolukorraks.

4.2.3 Otsustusprotsess

Kirjeldan süsteemi otsustusprotsessi ja jälgimise erinevusi temperatuuri näitel. Superviisorsüsteem saab ruumi temperatuuri andmed, mis koosnevad kahe komakohani ümardatud temperatuurinäitudest ja andurite infost, mis need võtsid. Näiteks “22,41; 23,02; 22,60” ja “puhkeruum 1, puhkeruum 2, puhkeruum 3”. Superviisorsüsteem võrdleb näite omavahel ja ettenähtud normide suhtes ja tuvastab, et näidud on omavahel sarnased ehk ükski näit ei erine tunduvalt teistest ja ettenähtud piirnormide suhtes pole eksitud. Kui kõik on korras, tagastab superviisorsüsteem otsuse, et puhkeruumi temperatuuriga on kõik korras.

Samas võib juhtuda, et superviisorsüsteem saab sama ruumi kohta näiteks andmed “22,34; 28,90; 22,56” ja “puhkeruum 1, puhkeruum 2, puhkeruum 3”. Puhkeruumi 2. temperatuurandur on nüüd tuvastanud ettenähtust kõrgema temperatuuri ja on vastuolus ülejäänud anduritega. Kuna kaks andurit kolmest on mõõtnud toatemperatuuriks umbes 22 kraadi, otsustab superviisorsüsteem, et toa temperatuuriga on kõik korras aga jätab meelde, et üks anduritest andis eksliku näidu ning teeb sellele restardi. Probleemi jätkumisel peab superviisorsüsteem kuulutama selle anduri tulemused ebatäpseks ning kasutuskõlbmatuks. Seega andurit ei kuulutata vigaseks kohe vaid süsteem teostab esialgu passiivset jälgimist ning kui probleemi olemasolu on kinnitatud ehk on kindlaid tõendeid, et ekslikke andmeid ei edastata juhuslikult, vaid pidevalt, alustab süsteem aktiivset jälgimist, et tuvastada, kas tegemist on juhuslikkuse või reeglga. Superviisorsüsteemis on oluline eristada ka

vigade ajavahemikku, sest näiteks üks viga kahe minuti jooksul pole põhjus häiret anda, kuid viis viga tunni jooksul peaks olema piisav põhjus kahtlustada anduri riket. Juhul kui andur jätkab teatud aja vältel ebatavaliste näitude edastamist, superviisorsüsteem sekkub ja informeerib süsteemi, et anduri edastatud näite ei saa usaldada.

Atmosfääri puhul saab otsustusprotsessis kasutada ka erinevate andmete ristvõrdlemist. See tähendab, et kui eeltoodud temperatuurianduri ebatavalisele näidule lisandub näiteks atmosfääri koostise muutus, võib see tähendada algstaadiumis tulekahju. Sarnases piirkonnas asuvate andurite näitude muutumisel ebatavaliseks, peab süsteem usaldama vähemuse andmeid. Kuigi säilib võimalus, et mitu andurit on korraga ekslikke näite edastanud, on häire sellisel juhul pigem õigustatud.

Otsustusprotsessis on võimalik ka olukord, kus superviisorsüsteem ei jõua otsusele, kas ohuolukord eksisteerib või puudub. Sellisel juhul katkestab superviisorsüsteem iseseisva otsustamise ning palub abi inimkasutajalt. Inimkasutaja saab superviisorsüsteemilt info, mis olukorra olemasolu kahtlustatakse ning seejärel kontrollib, kas antud ohuolukord eksisteerib. Inimkasutajalt saadud andmete abil tehakse otsus ja seejärel jätkub tavapärane protsess, kus superviisor lahendab tekkinud ohuolukorra või uurib välja, miks sai süsteem ekslikud andmed, mille alusel järeldati, et ohuolukord eksisteeris kui seda reaalsuses polnud.

4.2.4 Kuuelamu süsteemist laekuvate andmete usaldusväärsuse tagamine

Vigade vältimiseks otsustusprotsessis, peab superviisorsüsteemil olema ka andmed süsteemi konfiguratsioonist ja selle moodulite seisundist. Näiteks, mitu andurit mingis ruumis on ja mis tüüpi need on. Näiteks kui kolme anduriga ruumis kuulutatakse ühe anduri edastatav teave ebausaldusväärseks, peab süsteem edaspidi kontrollima ainult kahe anduri korrasolekut. Samas peab vigase anduri asendamise järel süsteem asuma taas kontrollima kolme anduri edastatavat teavet ning korrasolekut.

Superviisorsüsteemis on oluline ka andmete kogumise järelevalve. Süsteem peab teadma millistelt anduritelt ta informatsiooni saab ning jälgima, et ühendus nendega ei kaoks. See on tagatav heartbeat-süsteemiga ehk teatud ajavahemiku tagant peab süsteem kontrollima, et kõik töös olevad komponendid töötavad, on usaldusväärsed ja omavad ühendust ülejäänud süsteemiga. See tähendab, et lisaks andurite edastatavale teabe analüüsimisele, peab süsteem kontrollima andurite endi olemasolu ehk veenduma, et kui ühes ruumis on näiteks kolm atmosfääri koostist ja rõhku kontrollivat andurit, siis need kolm andurit

töötavad ja edastavad andmeid. See aitab vältida olukorda, kus superviisorsüsteem saab andmed, kuid mõni andur ei edasta enam üldse teavet ja seega langetatakse otsus puudulike andmetega. Oluline aspekt on ka rõhukaoga toimetulek, sest ruum(id) küll eraldatakse, kuid andmete edastus jätkub. Ruumi füüsilise vaheustega eraldamise järel võiks süsteem edastada analüüsi ja olukorraga kursis olekuks andmeid, kuid see ei tohi enam nende andmete põhjal enam uut sama taseme häiret anda.

4.2.5 Atmosfääri monitoorimine

Süsteem monitoorib kuuelamu atmosfääri temperatuuri, rõhu, suitsu, vingugaasi ja õhukvaliteedi sensoritega, mille arv sõltub ruumi suuruselt. Suuremates ning meeskonna poolt tihedamini kasutatavates ruumides peab andureid olema rohkem, kuna sellistes ruumides viibib rohkem astronaute ja õhukvaliteet muutub tihedamini ja suuremal määral kui näiteks WC-s, mille puhul võib eeldada, et kasutusintensiivsus on pigem madal.

Konfiguratsioonide kirjeldamisel olen aluseks võtnud Rahvusvahelises kosmosejaamas kasutusel olevad vahemikud [34]. Sensorite hälvete kirjeldused on hinnangulised ehk need tuleb algsedistada vastavalt rakendustingimustele.

Konfiguratsioonis kirjeldatud lubatud vahemik on suurus, mida süsteem peaks hoidma ning millest väljumisel on tegemist sekkumist vajava olukorraga. Lubatud hälve on sensori mõõtteksimus, mis on aktsepteeritav.

Temperatuuri mõõtmise konfiguratsioon

- Sensoreid: 1-3 (sõltuvalt ruumist)
- Kasutatav skaala: Celsius
- Lubatud vahemik: 17 kuni 28 kraadi
- Lubatud hälve: 0,5 kraadi

Juhul kui suhteline õhuniiskus on 60% nagu Rahvusvahelises Kosmosejaamas, tekib inimesele ohtlik olukord kui õhutemperatuur on 38 °C, sest pärast selle temperatuuri ületamist ei suuda inimese keha ennast jahutada [35] [36]. Seega antud olukorras tuleks alarm käivitada kui õhutemperatuur on 30 °C ning ennetav käitumine käivitada kui temperatuur on üle 28 °C.

Rõhu monitoorimine

- Sensoreid: 1-3 (sõltuvalt ruumist)
- Kasutatav mõõtühik: kPa

- Lubatud vahemik: 97,9 kuni 102,7 kPa (0,96 kuni 1,01 atmosfääri)
- Lubatud hälve: 0,5 kPa

Õhukvaliteedi monitoorimine

- Sensoreid: 1-3 (sõltuvalt ruumist)
- Kasutatav mõõtetühik: protsent
- Lubatud hälve: 0,5%

Õhukvaliteedi andurid peavad analüüsima atmosfääri koostist ning tuvastama õhust gaasid, mis on astronautidele eluohtlikud. Mõõtmine toimub protsentides ja arvestatakse gaasi suhet teiste suhtes. Normaalne atmosfäärikoostis on 21% hapnikku ja 78% lämmastikku. Maksimaalne lubatud hapnikusisaldus on 24%. Süsihappegaasi tohib õhus olla maksimaalselt 0,7% [34].

4.2.6 Tulekahju monitoorimine

Süsteem tuvastab tulekahju, monitoorides süsinikdioksiidi ehk süsihappegaasi ja süsinikmonoksiidi ehk vingugaasi sisaldust elamu atmosfääris. Süsinikmonoksiidi avastamine viitab võimalikule ebatäielikule põlemisele, samas kui süsinikdioksiidi sisalduse tõus viitab võimalikule põlengule. Mõlemal juhul peab käivituma tulekahjualarm. Lisaks atmosfääri monitoorimisele ennetatakse tulekahjusid ka temperatuuriandurite abil, sest juhul kui ruumis tuvastatakse ebatavaliselt kõrge temperatuur, on süsteemi jaoks endiselt tegemist tulekahjuga. See on vajalik, et vältida elamus tagasitõmbe teket, kus tulekahju kasutab ära kogu hapniku ja leegid kustuvad, kuid kõrge temperatuur säilib. Juhul kui astronaut suundub sellises olukorras ruumi kahjustusi üle vaatama, lisab ta hermeetilise ukse avamisega ruumi kiiresti uuesti hapnikku ning toimub põlengu uuesti süttimine, millele järgneb plahvatus [37].

4.2.7 Andurite edastatud näitude monitoorimine

Andurid edastavad süsteemile pidevalt näite, mille põhjal langetab süsteem otsuseid. Samas on pidevalt olemas ka oht, et andur läheb rikki ning mitte ei lõpeta mõõtmistulemuste edastamist, vaid hakkab edastama ebaõigeid tulemusi. Vigaseid andureid saab välja selgitada, võrreldes omavahel andurite tulemusi ja vajadusel ka eelnevaid tulemusi.

Kolme ja enama sama anduriga ruumid

Andurite mõõdetud tulemusi võrreldakse omavahel ja kui üks andur saab teistest erineva tulemuse, usaldatakse kahe anduri tulemusi ning kolmanda oma mitte.

Kahe ja vähema sama anduriga ruumid

Juhul kui ruumis on kaks andurit, võrreldakse omavahel nende tulemusi ning ka varasemaid tulemusi. Ühe anduriga mõõtmise korral, võrreldakse saadud tulemust eelmiste tulemustega, et tuvastada, kas andur on registreerinud eelmiste tulemustega võrreldes märkimisväärselt erineva näidu.

4.2.8 Mitmele samaaegse ohusituatsioonile reageerimine

Ohutussüsteemi arhitektuuri kavandamisel peab arvestama võimalusega, et mitu ohuolukorda võib ja saab tekkida samaaegselt või üksteise järel. Sellisel juhul peab süsteem olukorrad prioritseerima ning valima kumma olukorraga tegeletakse varem. Näiteks võib kuuelamus lühikese ajavahemiku jooksul tekkida tulekahju ning õhuleke. Süsteem otsustab antud näites tegeleda esmalt tulekahjuga ning pärast tulekahju kustutamist asub see tegelema võimaliku õhulekke tuvastamise ja lahendamisega. Süsteem ei ignoreeri tekkinud ohuolukordi ning kõik olukorrad tuvastatakse ja lahendatakse. Süsteem peab ohuolukordade lahendamisel lähtuma ka kompenseerimismehhanismi ressursivajadusest. Näiteks elektrivarustus on kriitiline ressurss ja selle kasutamisel peab jälgima, et ei tekiks energiapuudust mõnes teises elutähtsas alamsüsteemis. Näiteks piiratud koguse elektri korral võib piirata tarbimist olukorra lahendamiseks, kuid ei tohi lubada tekkida olukorral, kus näiteks õhupuhasti või mõni muu oluline seade jääb vooluta.

5. Mudelipõhine verifitseerimine

Töös loodud kriitiliste olukordade lahendamise mudelid on verifitseeritud, et veenduda nende korrektse toimimises. Verifitseeritud mudelid kindlustavad, et ohutuskriitilise süsteemi töökindlus on enne detailprojekteerimise ja ehitamise algust kontrollitud.

Mudelid on verifitseeritud kasutades Stratego verifitseerijat (verifier) ning jooksutades ohutustingimusi verifitseerivaid päringuid. Verifitseerimine toimub mudelipõhiselt ning päringute eesmärgiks on veenduda, et mudel tuleb tõrkega toime ning erinevad ohuolukorrad ei mõjuta teineteist. Järgnevalt käsitlen olulisemaid päringu tüüpe, mida saab kasutada kõikide tõrkeklasside kompensatsiooni mehhanismide verifitseerimisel.

5.1 Tõrgete kompenseerimise mehhanismide korrektsusomadused

Tõrgete esinemist ja nendele reageerimise korrektsust verifitseeritakse töös mudelkontrolli päringutega. Järgnevalt on toodud olulisemad mudelite korrektsusomadusi tõestavad päringud.

A[] not deadlock

Päringu eesmärk on kontrollida, et mudelis ei ole tupikut (deadlock). Juhul kui päringutingimus on täidetud, on kindel, et keskkonna ja süsteemi mudelites ei teki olukorda, kus üks või mitu automaati ei jõua disainivea tõttu lõppolekusse.

A<> S.Compensated

Päring kontrollib, kas süsteemi mudelis jõutakse algolekust alati soovitud lõppolekusse "*Compensated*", mis on kõigil mudelitel tõrke või avariiolekorra kompenseerimise protseduuri lõppolek. Päring dubleerib mõnevõrra eelmises punktis kirjeldatud päringut, kuid see võimaldab ilma aega arvestamata kontrollida, kas mudel on etteantud tingimustel algusest lõpuni läbitav.

A<> S.Compensated && formula_clock <= 200

Päring kontrollib, kas süsteemi mudelis jõutakse algolekust alati olekusse "*Compensated*" ettenähtud aja jooksul. Päring koosneb kahest osast, A<> S.Compensated, mis on kirjeldatud eelmises punktis, ja formula_clock <= 200, mis seab piirangu süsteemi reaktsiooniajale.

Formula_clock on mudeli kell, mis mõõdab mudelis häiretingimuse tekkimisest lõplahenduseni jõudmiseks kulunud aega. Mudelites on ajapiiranguks seatud näiteks 200 ajaühikut, kuid üldjuhul sõltub see konkreetsest tõrke tüübist ja selle kompenseerimismehhanismist.

A[] S.Wait_2 not imply S.event_cl <= 45

Päring kontrollib, kas süsteem jõuab olekusse Wait_2 hiljemalt 45 ajaühiku jooksul. See tingimus tagab, et süsteem reageerib olukorrale ettenähtud ajaga või kiiremini.

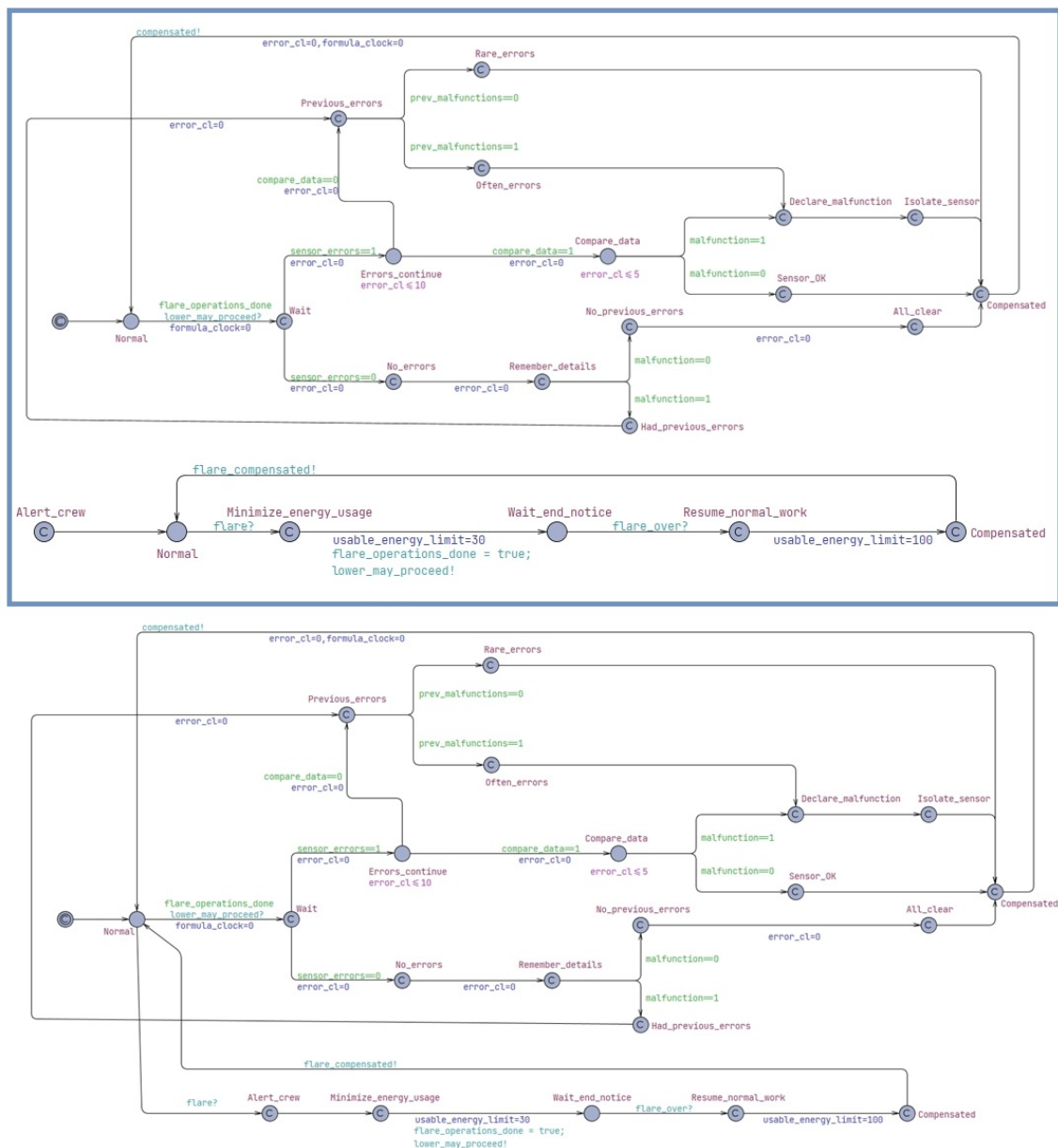
5.2 Kombineeruvate tõrgete kompenseerimise korrektsuse verifitseerimine

Senitoodud mudelid kirjeldavad süsteemi tööd tõrkeklasside kompenseerimisel, kui tõrked tekivad ühekaupa. Praktikas on üsna tavaline, et tõrked esinevad samaaegselt. Et süsteem suudaks ka niisugusi olukordi kompenseerida, tuleb nii keskkonna kui süsteemi tõrkepõhiseid mudeleid omavahel siduda paralleel-kompositsiooni. Kuivõrd nii süsteemi kui keskkonna mudelid omavad standardset struktuuri on nende omavaheline sidumine võimalik kas paralleelkompositsiooni või nn kokkusulutamise (*merging*) teel.

Paralleelkompositsioon tähendab, et üksiktõrke tekkimist kirjeldavad mudelid on paralleelkompositsioonis süsteemi tõrkekompenseerimise mudelitega.

Kokkusulutamisel seotakse omavahel nii üksikud tõrkemudelid kui ka nende kompenseerimise mudelid. Näiteks seotakse omavahel süsteemi mudelid sulatades kokku automaatide olekud „*normal*“ (vt joonis 11). See tähendab, et süsteem saab korraga reageerida ainult ühte tüüpi tõrkele.

Praktikas võivad eri tüüpi tõrked tekkida samaaegselt ja süsteem peab neile paralleelselt reageerima. Järelikult tuleb nii tõrkeid kui ka kompenseerimismehhanisme modelleerida koos, kasutades paralleelkompositsiooni. Teiselt poolt kasvab paralleelkompositsiooni korral mudeli korrektsuse kontrolli keerukus eksponentsiaalselt sõltuvalt paralleelsete automaatide arvust ja nende keerukusest (olekute ja siirete arvust). Praktiliseks lahenduseks oleks verifitseerida korrektsusomadusi tõrkegruppide kaupa tõestamaks, et korrektsusomadused kehtivad gruppide piires sõltumata tõrgete omavahelisest kombineerumisest. Sel juhul määrab mudeli kontrolli keerukuse grupi suurus ja suurim arv tõrkeid, mis võivad eelduste kohaselt samaaegselt esineda.



Joonis 11. Anduri eksliku näidu (ülemine kontuur) ja päikesepurske lahendamise süsteemi (keskmise kontuur) kokkusulatatud automaadid (alumise kontuur).

5.3 Edasised arendused

Antud töö eeldab reaalse tarkvara arendamisel *model-based development* (MBD) ehk mudelipõhise arendusprotsessi kasutamist. Mudelipõhine arendusprotsess on tarkvaraarenduse meetod, mille puhul kasutatakse mudeleid keerukate süsteemide kavandamiseks ja simuleerimiseks. Mudelipõhine arendusprotsess eeldab, et loodud mudelid kajastavad täpselt tegelikku süsteemi ning nende täpsus on ülioluline, et simulatsioonid ja süsteemi toimivuse prognoosid oleksid usaldusväärsed [38].

Töös koostatud mudel kirjeldab tarkvara algoritmilist osa abstraktsel tasemel ja annab sisuliselt programmi spetsifikatsiooni ja töövoogu struktuuri programmeerijale. Mudeli siiretel olevad muutujad tuleb täpsustada vastavaks reaalsele tingimustele. Samas on mudel juba ette kirjeldanud, kuidas protsessid reaalselt täidetakse. Pärast koodi kirjutamist saab mudelipõhise testimisega kontrollida, kas tarkvara käitub vastavalt mudelis kirjeldatule.

Edasist lahendamist vajab mitme samaaegselt toimuva olukorra mudelite koostamine ning verifitseerimine. Olukorrad tuleks grupeerida näiteks vastavalt klassidele ning kasutades antud töö alapeatükis 5.2 kirjeldatud kokkusulatamist (*merging*) või paralleelkompositsiooni. Samaaegselt toimuvate olukordade mudeldamine võimaldab uurida ja kontrollida, et ka mitme samaaegse olukorra tekkimisel on lõpptulemuseks olukorra lahendumine. Gruppide verifitseerimise järel võiks koostada suure mitut ohuolukorra gruppi sisaldava mudeli olukordade juhtumipõhiseks analüüsiks. Juhul kui mudelikontrolli abil on omavahel sõltuvate gruppide korrektsus verifitseeritud, siis sellest järeldeb ka käitumuslikult sõltumatute gruppide kompositsiooni korrektsus, milles need sõltuvad grupid esinevad.

6. Kokkuvõte

Antud töös on kirjeldatud kuuelamu „IGLUNA“ projektiga seotud ohuolukordi ning mudeldatud nende kompenseerimise mehhanisme, kasutades mudelkontrolli keskkonda Uppaal Stratego. Töö eesmärgiks oli koostada mudelipere, mis kirjeldaks mõned esineda võivad ohuolukorrad ning eeldab, et hiljem koostatakse *model-based development* arendusprotsessi alusel neist toimiv tarkvara.

Iga tõrke klassi jaoks on loodud eraldi mudel, kuid need mudelid on konfigureeritud sarnaselt. Iga mudel sisaldab keskkonna automaati, mis modelleerib ohuolukorra tekkimist ning süsteemi automaati, mis kirjeldab kuidas süsteem reageerib tekkinud ohuolukorrale. Tänu unifitseeritud mudelite kujule saab kõigi mudelite korral rakendada ühesugust verifitseerimispäringute komplekti. Need lihtsustavad nii uute mudelite konstrueerimist kui ka verifitseerimistingimuste formuleerimist üksik tõrkemudelite korral. Kõik mudelid on verifitseeritud töös toodud verifitseerimispäringute vastu.

Tänu ühtsele struktuurile on tulevikus võimalik need situatsioonidele vastavad üksikmudelid hõlpsasti omavahel liita hübriidseid olukordi kirjeldavateks mudeliteks ning verifitseerida süsteemi käitumist tõrkeolukordade kombineerumise tingimustes. Samaaegselt toimuvate olukordade mudeldamine võimaldab uurida ja kontrollida, et ka mitme samaaegse olukorra tekkimisel on lõpptulemuseks olukorra lahendumine.

Kasutatud kirjandus

- [1] *Andur*. <https://et.wikipedia.org/wiki/Andur>. Kasutatud 6. mai 2025.
- [2] *Control loop*. <https://www.techtarget.com/whatis/definition/control-loop>. Kasutatud 25. aprill 2025. TechTarget.
- [3] *What Are Cosmic Rays?* <http://www.telescopearray.org/index.php/about/what-are-cosmic-rays>. Kasutatud 13. aprill 2020.
- [4] *What is a Transient Fault?* <https://www.ituonline.com/tech-definitions/what-is-a-transient-fault/>. Kasutatud 14. aprill 2025. ITU.
- [5] NASA Science Editorial Team. *What is NASA?* <https://science.nasa.gov/learning-resources/for-kids-and-students/what-is-nasa/>. Kasutatud 25. aprill 2025.
- [6] *Tõrge*. <https://arhiiv.eki.ee/dict/ekss/index.cgi?Q=tõrge>. Kasutatud 29. juuni 2020. 2009.
- [7] Indeed Editorial Team. *Indeed.com*. <https://uk.indeed.com/career-advice/career-development/verification-vs-validation>. Kasutatud 1. juuni 2025.
- [8] *Viga*. <https://arhiiv.eki.ee/dict/ekss/index.cgi?Q=viga>. Kasutatud 30. juuni 2020. 2009.
- [9] *IGLUNA ABOUT*. <https://space-innovation.ch/activities/igluna/>. Kasutatud 24. märts 2025. Space Innovation.
- [10] *IGLUNA 2020*. <https://space-innovation.ch/activities/igluna/previouseditions/>. Kasutatud 24. märts 2025. Space Innovation.
- [11] *Lunar habitation*. https://en.wikipedia.org/wiki/Lunar_habitation. Kasutatud 30. märts 2025.
- [12] NASA Office of the Chief Health & Medical Officer (OCHMO). *Apollo Lunar Lander Module Design: Medical & Human Performance Perspective*. NASA, 2023.
- [13] R. Mueller. "Lunar Base Construction Planning". Teoses: köide 1. ASCE Earth and Space Conference. Denver, 2022.
- [14] J. Taveau. *NASA Plans to Assign Missions for Two Future Artemis Cargo Landers*. <https://www.nasa.gov/news-release/nasa-plans-to-assign-missions-for-two-future-artemis-cargo-landers>. Kasutatud 3. märts 2025. 2024.
- [15] L. Ehret ja L. Lin. *China tests building Moon base with lunar soil bricks*. <https://phys.org/news/2024-11-china-moon-base-lunar-soil.html>. Kasutatud 3. märts 2025. Phys.org, 2024.

- [16] *IGLUNA Previous editions*. <https://space-innovation.ch/activities/igluna/previouseditions/>. Kasutatud 24. märts 2025. Space Innovation.
- [17] S. Kulkarni ja A. Arora. “Component Based Design of Multitolerant Systems”. *IEEE Transactions on Software Engineering* (jaanuar 1998), lk. 1.
- [18] S. Kulkarni. “Component based design of fault-tolerance”. Doktoritöö. The Ohio State University, 2010, lk. 1.
- [19] A. Arora ja S. Kulkarni. *Component Based Design of Multitolerant Systems*. Jaanuar 1998.
- [20] G. Behrmann, A. David ja K. G. Larsen. *A Tutorial on Uppaal 4.0*. Aalborg, 2006.
- [21] *Edges*. <https://docs.uppaal.org/language-reference/system-description/templates/edges/>. Kasutatud 8. mai 2025.
- [22] *Declarations*. <https://docs.uppaal.org/language-reference/system-description/declarations/>. Kasutatud 8. mai 2025.
- [23] *UPPAAL Help*. <https://docs.uppaal.org/>. Kasutatud 23. märts 2025.
- [24] A. David, P. Gjøøl Jensen, K. Guldstrand Larsen, M. Mikučionis ja J. Haahr Taankvist. *Uppaal Stratego*. Aalborg, 2015.
- [25] *Uppaal Stratego*. <https://people.cs.aau.dk/~marius/stratego/intro.html>. Kasutatud 31. märts 2021. 2015.
- [26] *UPPAAL*. <https://www.it.uu.se/research/group/darts/uppaal/about.shtml>. Kasutatud 16. mai 2021. 2019.
- [27] *UPPAAL*. <https://www.it.uu.se/research/group/darts/uppaal/about.shtml#team>. Kasutatud 31. märts 2021. 2019.
- [28] *What are solar flares?* https://www.esa.int/Science_Exploration/Space_Science/What_are_solar_flares. Kasutatud 23. märts 2025.
- [29] *Space Weather Office*. https://www.esa.int/Space_Safety/Space_weather/Space_Weather_Office. Kasutatud 23. märts 2025.
- [30] *Space radiation: the Apollo crews were extremely lucky*. <https://theconversation.com/space-radiation-the-apollo-crews-were-extremely-lucky-120339>. Kasutatud 23. märts 2025. 2017.
- [31] *Sõnaveeb*. <https://sonaveeb.ee/search/unif/dlall/dsall/tulekahju/1/est>. Kasutatud 14. aprill 2025.
- [32] G. Reeves ja T. Neilson. *The Mars Rover Spirit FLASH Anomaly*. Pasadena: Jet Propulsion Laboratory (JPL), 2004.
- [33] R. Howard. *A Safe Haven Concept for the Common Habitat in Moon, Mars, and Transit Environments*. Houston: NASA Johnson Space Center, 2021.

- [34] M. Sabbatini, N. Sentse, G. De Chiara, D. Ducros ja K. Oldenburg. “ESA User Guide to Low Gravity Platforms”. Teoses: European Space Agency, 2014. Ptk 7.4 Internal environment, lk. 33.
- [35] A. Suh, S. Ditelberg, J. J. Szeto, D. Kumar, J. Ong, R. Gibson, T. H. Mader, E. Waisberg ja A. G. Lee. *Safety protocols, precautions, and countermeasures aboard the International Space Station to prevent ocular injury*. 2024.
- [36] L. Kenney, D. Vecellio, R. Cottle ja T. Wolf. *HowStuffWorks*. <https://science.howstuffworks.com/life/biology-fields/how-hot-is-too-hot-outside.htm>. Kasutatud 6. mai 2025.
- [37] I. Šarin ja M. Soontalu. “Suitsu ja põlemisgaaside eemaldamine tulekahjudel”. Teoses: Tallinn: Sisekaitseakadeemia, 2015. Ptk Tagasitõmme, lk. 22.
- [38] Tomasz Zietek. *Spyrosoft.com*. <https://spyro-soft.com/blog/industry-4-0/model-based-software-development>. Kasutatud 1. juuni 2025.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks¹

Mina, Meelis Lutsar

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose “Nutika kuuelamu elutagamissüsteemi töökindluse prototüüpimine”, mille juhendaja on Jüri Vain
 - 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.

01.06.2025

¹Lihtlitsents 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 loomingu tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtjaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.