

FELADATKIÍRÁS

A feladatkiírást a tanszéki adminisztrációban lehet átvenni, és a leadott munkába eredeti, tanszéki pecséttel ellátott és a tanszékvezető által aláírt lapot kell belefűzni (ezen oldal *helyett*, ez az oldal csak útmutatás). Az elektronikusan feltöltött dolgozatban már nem kell beleszerkeszteni ezt a feladatkiírást.



Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Méréstechnika és Információs Rendszerek Tanszék

Állapottérkép verifikációs MagicDraw plugin továbbfejlesztése

DIPLOMATERV

Készítette
Gáti László Dávid

Konzulens
Tóthné Farkas Rebeka

2020. május 30.

Tartalomjegyzék

Kivonat	i
Abstract	ii
1. Bevezetés	1
2. Háttérismeretek	3
2.1. Kapcsolódó munkák	3
2.2. SysML	3
2.2.1. Állapotgépek, állapottérképek	4
2.2.2. Funkcionális architektúra modellek	5
2.3. MagicDraw	6
2.4. Modelltranszformációk	6
2.5. Felhasznált technológiák	7
2.5.1. Eclipse Modeling Framework	7
2.5.2. Xtext	8
2.5.3. Gamma Statechart Composition Framework	8
2.5.4.	10
2.6. MagicDraw állapotterkép verifikációs plugin	10
2.6.1. MagicDraw - Gamma transzformáció	10
2.6.2. Verifikáció menete	10
2.6.3. Örfeltételek, akciók	11
3. Plugin továbbfejlesztése	13
3.1. Fejlesztés céljai	13
3.1.1. Funkcionális dekompozíció transzformálása	13
3.1.2. Eredmények megjelenítése	13
3.1.3. Követelmények definiálása	14
3.2. MagicDraw profil	14
3.2.1. Kompozit szemantika	15
3.2.2. Check modell	15
3.2.3. Back-annotation modell	16
3.3. Kompozíciók transzformációja	18
3.3.1. Struktúra megfeleltetése	18
3.3.2. Kommunikáció megfeleltetése	19
3.4. CTL nyelvtan	20
3.5. Back-annotation transzformációja	20
3.6. Szimuláció	20
3.7. Példa	20
4. Értékelés	21

HALLGATÓI NYILATKOZAT

Alulírott *Gáti László Dávid*, szigorló hallgató kijelentem, hogy ezt a diplomatervet meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2020. május 30.

Gáti László Dávid
hallgató

Kivonat

TODO:

Abstract

TODO:

1. fejezet

Bevezetés

A IT technológiák térnyerésével egyre több és komplexebb rendszer készül, melyeknek sokszor valós időben kell működni. Mivel ilyen rendszerek jellemzően valamilyen biztonság kritikus környezetben működnek, elengedhetetlené válik ezek gondos megtervezése és átfogó vizsgálata különösen a helyes működés tekintetében.

A tervezés és ellenőrzés költséges, időigényes folyamat, ezért szükség van olyan eszközökre amelyek megkönnyítik vagy akár teljesen automatizálnak egyes folyamatokat. A tervezés során általában valamilyen modellvezért technikát alkalmaznak, melynek közép-pontjában a modellek állnak. A tervezés során elkészített tervek nagyon sok értékes információt tartalmaznak, melyeket újra fel tudunk használni és származtatni ezekből kódot, dokumentációt, vagy akár más modelleket, ezáltal időt és erőforrásokat megtakarítva. Ráadásul mivel ezeket automatikusan gépek végzik, minimalizálódnak az emberi hibák például a programkódban, ahhoz képest mintha ezeket kézzel végeznénk el.

Terveinket már érdemes a tervezés korai fázisaiban ellenőrizni, hiszen az itt vétett hibák akár kritikusak lehetnek a későbbiekben. Az ellenőrzésekhez szintén fel tudjuk használni a modelljeinket és szimulálni tudjuk a rendszert, vagy képesek vagyunk magát a modellt is vizsgálni formális módszerek segítségével.

A MagicDraw egy mára de-facto ipari standarddá vált szoftver, és rendszer architektúra modellező eszköz ami fejlett grafikus interfészt nyújt a felhasználók számára. Modelleket elsősorban egy általános célú modellezési nyelvvel UML-el lehet készíteni, azonban UML profilok segítségével akár saját szakterület specifikus nyelvek használatára is lehetőségünk nyílik. Ilyen formában a MagicDraw lehetővé teszi modellek létrehozását SysML nyelven is amihez a profilt maga biztosítja. A dolgozat a továbbiakban SysML modellekkel foglalkozik.

Ugyan a MagicDraw számos fontos és hasznos funkcióval rendelkezik, még mindig megvan az igény újabbakra főleg Verifikáció/Validáció tekintetében. A MagicDrawToGamma nevű MagicDrawhoz készült plugin SysML állapotterképek formális verifikálásához nyújt megoldást, melyhez a Gamma Statechart Composition Frameworköt és az UPPAAL nevű eszközöket használja fel.

Az eszköz ugyan *Proof of Concept* jelleggel már képes a verifikációt elvégezni, azonban, hogy akár szélesebb körben is használható eszközzé válhasson még sok tekintetben fejlesztésre szorul. Jelen dolgozat célja bemutatni azokat a fejlesztéseket amiket a mesterképzés során végeztem az eszközön és visszatekintve kiértékelni azokat a mérnöki megoldásokat melyeket a fejlesztés során hoztam.

A dolgozat felépítése a következő: a második fejezetben ismertetem azokat az ismereteket amelyek a dolgozat során felvetülő problémák illetve az ezekre adott megoldások megértéséhez szükségesek. A harmadik fejezetben ismertetem a projekt céljait és az ezekhez vezető utat, alkalmazott megoldásokat, illetve bemutatom a beépülő modul működését.

A negyedik fejezetben pedig értékelem az alkalmazott megoldások hatékonyságát és az elkészített plugint.

2. fejezet

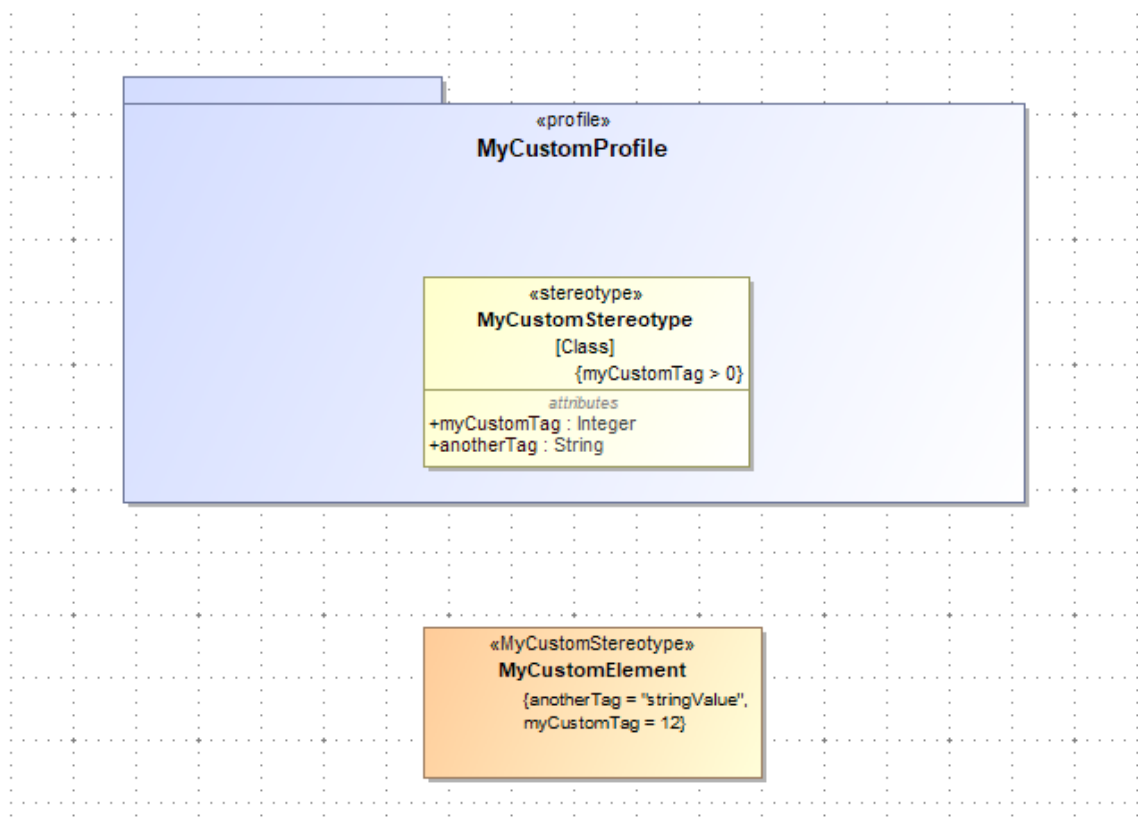
Háttérismeretek

2.1. Kapcsolódó munkák

2.2. SysML

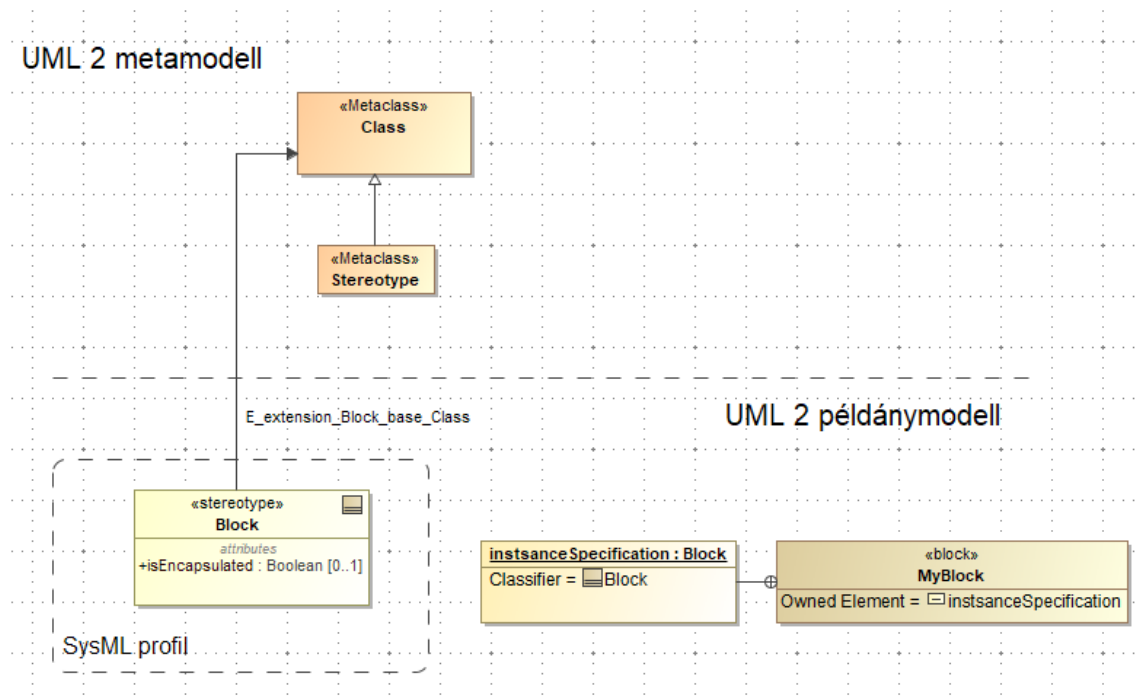
A System Modeling Language (SysML) egy általános célú architektúra modellező nyelv, melyet elsősorban rendszermérnökök használnak. A nyelvvel különböző komplex rendszereket tudunk leírni többféle megközelítésből mint magas szintű funkcionális modellek mind pedig az alacsonyabb akár fizikai modellekig.

A SysML-t mint ahogyan az UML-t is az Object Management Group (OMG) fejleszt, sőt az UML 2-nek egy dialógusa a nyelv, úgynevezett UML profil segítségével van definiálva. Az UML profil a nyelv specializálásának egy módja sztereotípiák (Stereotype), megkötések (Constraint) és címkézett értékek (Tagged Value) segítségével (2.1. ábra).



2.1. ábra. UML nyelv specializálása sztereotípiákkal

Egy nyelv lehetséges elemeit és kapcsolatait leíró struktúrát metamodellnek hívjuk, a tényleges elemekből és ezek kapcsolatából álló modellt pedig példánymodellnek. SysML esetében az UML profil az amit metamodellnek tudunk tekinteni, igaz a metaszintek eléggé összemósódnak és nem elegendő csak a profilt ismerni, hanem az UML metamodellt is ismerni kell. Például egy SysML Block valójában egy sztereotipizált UML Class. Ez azt jelenti, hogy van egy UML példány specifikáció (Instance Specification) aminek az osztája (Classifier) egy Block sztereotípiája és ez hozzá van rendelve az UML-s osztály példányunkhoz a modellünkben. Az UML-s osztály példány a sztereotípiája és a példány specifikáció tehát hagyományos értelemben azonos metaszinten helyezkednek el (2.2. ábra).



2.2. ábra. Meta szintek és Block sztereotípiája alkalmazása

SysML segítségével sokféle modellt lehet készíteni a teljesség igénye nélkül: Követelmény modellek, viselkedés modellek, struktúra modellek, allokáció modellek, mindezek közül azonban kettőre koncentrálok a dolgozat elkészítése közben, mégpedig a viselkedés modellek egy részére az állapotgépekre és a funkcionális architektúrára amely funkcionális architektúra egy de-komponált állapotgépet ír le.

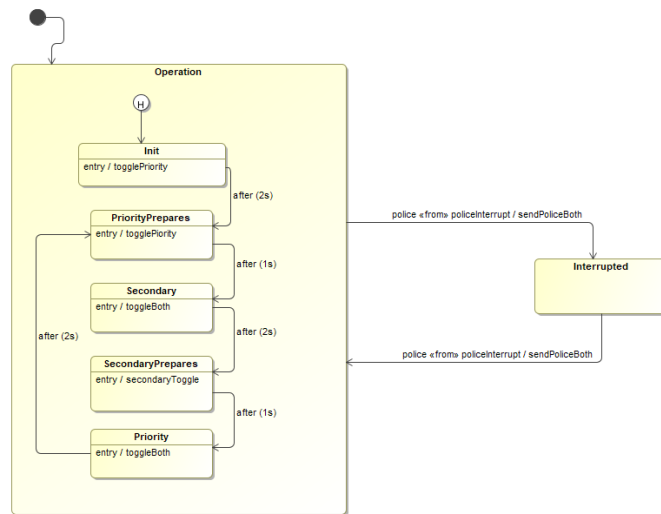
2.2.1. Állapotgépek, állapottérképek

Állapotgépek (State Machine) alatt olyan modelleket értünk amik a rendszert véges számú jól elkülönülő állapotát írják le, illetve az ezek közötti átmeneteket. Az állapotgépeket SysML-ben állapottérkép diagramokon (Statechart Diagram) tudunk definiálni. Szintaktikáját tekintve oválisok amik állapotokat jelentenek illetve az ezeket összekötő nyilak, melyek az állapotok közötti lehetséges váltások. A nyilak általában címkézettek. A címke három részből állhat: esemény (trigger), őrfeltétel (guard), akció (action).

esemény [őrfeltétel] / akció

Állapotváltás egy esemény bekövetkezésekor lehetséges. Amennyiben van őrfeltétel annak igaznak kell lennie. Az állapotváltás bekövetkezését szokás tüzelésnek is nevezni. Ha egy állapotátmenet tüzel és van akció az átmenethez rendelve ez végrehajtódik. Akció nem

csak állapotátmenetek, hanem állapotok be és kilépésénél is végrehajthatók, illetve létezik olyan akció is ami folyamatosan fut amíg a rendszer adott állapotban van.



2.3. ábra. Állapottérkép SysML-ben

Az állapotoknak van egy típusa melyet pszeudo állapotoknak nevezünk. Ezek nem tényleges állapotai a rendszernek olyan értelemben, hogy a rendszer soha nem tartózkodhat ezekben mindig azonnal át kell lépniük belőle egy tényleges állapotba, viszont fontos szemantikai jelentéssel bírnak. A kezdő állapot mely fekete körként jelenik meg egy régió belépési pontjai. Az állapotok mindig régiókban helyezkednek el, ezek tulajdonképpen állapotoknak egy olyan halmaza, amely halmazon belül mindig csak egy állapot lehet aktív, régiókból viszont lehet több is párhuzamosan. Így egy rendszernek lehet egyszerre több aktív állapota is régióként viszont csak egy (a fork-joinra a dolgozat nem tér ki).

Pszeudo állapotok még a *History Statek* is. Ezek segítségével meg lehet jegyezni, hogy egy összetett állapot mely belső állapota volt aktív, így az állapotba visszalépve nem a belső régió kezdő állapota hanem az utolsó aktív állapot lesz újra aktív. *History Statek*nek két változata van *Deep* és *Shallow*. Előbbi egymásba ágyazott esetén minden régióba az utolsó aktív állapotba lép át, míg utóbbi csak a saját régiójának utolsó aktív állapotába. Jelölésük kör benne "H"-val vagy "H*".

2.2.2. Funkcionális architektúra modellek

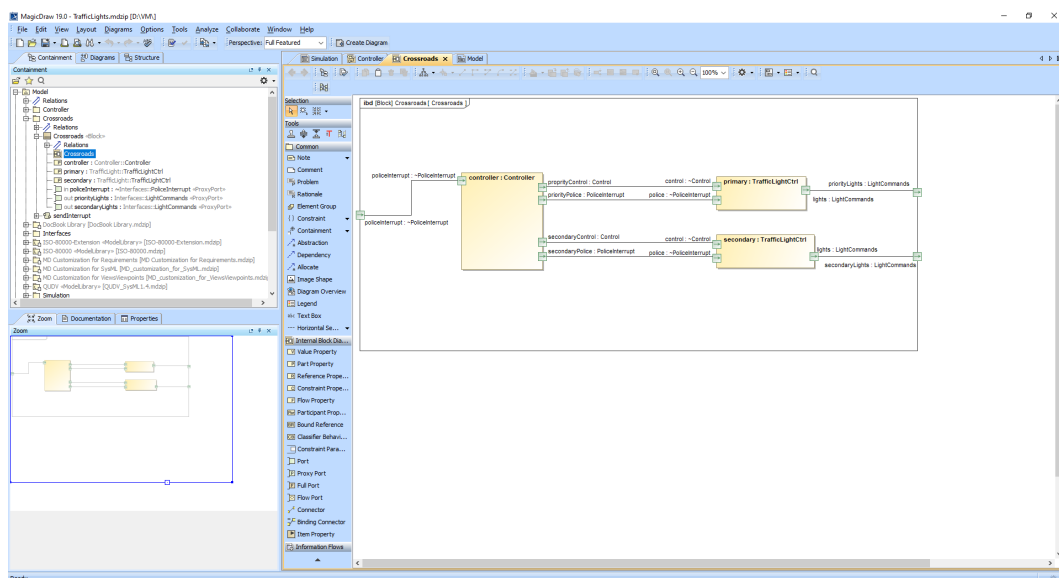
Egy rendszer funkcionális architektúráján olyan modelleket értünk melyek ennek logikai felépítését írják le azaz, hogy milyen funkciói vannak a rendszernek, ezek hogyan kapcsolódnak egymáshoz. Jelen esetben ezeket a modelleket a rendszer állapotgépezetnek a dekomponálására használjuk. Tehát van egy összetett rendszerünk melyeket funkcionális egységekre tudunk bontani úgy, hogy minden funkcionális egység állapot alapú viselkedések egy összessége. A komponensek képesek egymással kommunikálni és egymás viselkedését ezáltal befolyásolni.

A rendszert két szempont szerint tudjuk modellezni: komponens definíciók és ezek kompozíciója illetve ezek kapcsolatai szerint. Előbbiek blokkok formájában jelennek meg és SysMLben Blokk definíciós (Block Definition) vagy BDD diagramokon jelennek meg. Azt, hogy a blokkon belüli részek (Part) hogyan kapcsolódnak egymáshoz Internal Block Diagramok (IBD) tartalmazzák. A részek közötti kapcsolatot konnektorok írják le. Ezek jellemzően portokon keresztül kötik össze a részeket. A portok tekinthetők egy adott blokk interfészének is.

A dolgozat elkészítésénél kétféle blokkot különböztetek meg. Azokat melyek állapotgépeket definiálnak és nem bonthatók részekre ezeket állapot blokkoknak nevezem. Illetve olyan blokkokat melyen részekre bonthatók, de nem definiálhatnak saját állapotgépet, ezeket pedig kompozit blokkoknak.

2.3. MagicDraw

A MagicDraw egy modellező eszköz melyet a NoMagic fejlesztett elsősorban UML modellek készítésére. Ahhoz, hogy SysML-ben is tudjunk modelleket készíteni egy beépülő modulra van szükségünk (kivéve ha Cameo System Modellert használunk ami a SysML pluginnal integrálva szállít). A MagicDraw az iparban egy egyre inkább elterjedt eszköz. Szigorúan követi az UML és SysML szabványt. Az modellezőeszköz gazdag funkcionálitással rendelkezik mint fejlett felhasználói interfész (2.4. ábra), validációs motor - ami képes akár futásidőben a felhasználók által készített szabályok futtatására is, sablon alapú kódgenerátor és még sok egyéb. Ezen felül a funkcionalitás beépülő modulok segítségével bővíthető.



2.4. ábra. MagicDraw felhasználói felülete

MagicDrawhoz lehetőségünk van saját plugin fejlesztésére is, amik lehetővé teszik számunkra, új funkcionalitás integrálását az eszközben illetve modellek manipulálását is. A feladatot is egy ilyen plugin fejlesztésével oldottam meg.

2.4. Modelltranszformációk

Az ipari standardok mellett sok speciális modellezési nyelv is létezik, amelyek megannyi céllal és eszközkészlettel jöttek létre. Ezek között vannak magas absztrakciójú általánosabb nyelvek és alacsony szintűek is amik egy része olyan formalizmusokra épül amik felett bizonyos problémákra matematikai eszközökkel tudunk megoldást keresni.

A modellvezéreltség egyik alapötlete, hogy különböző modellekből származtatni tudunk más modelleket feltéve, hogy elegendő információ áll rendelkezésünkre a konverzió elvégzéséhez. Ezt a fajta származtatási folyamatot modelltranszformációnak nevezzük. A modelltranszformációk használata lehetővé teszi, hogy ne csak azokat a technológiákat

használjuk modellünk feldolgozására melyek speciálisan az adott modellezési nyelvhez készültek hanem a modelleket megpróbáljuk átalakítani - lehetőleg a szemantikai tartalom megőrzésével és automatizáltan - egy olyan modellezési nyelvre amelyhez már létezik az általunk használni kívánt funkcionalitást támogató technológia.

Ezen felül dokumentumokat is tudunk származtatni a modellekből a kódgenerálás tulajdonképpen ennek egy speciális esete. Az sem ritka, hogy a származtatások több lépésen és modellen keresztül történnek. A kód generálásnál maradvá a generált kód is egy modell amit általában egy fordítónak valamilyen futtatható állománnyá kell alakítani.

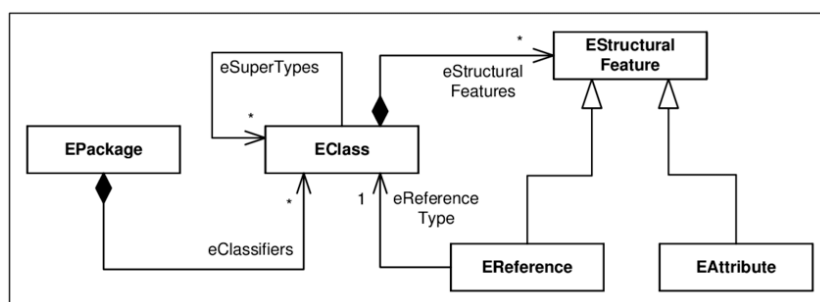
Fontos megjegyezni, hogy előfordulhatnak olyan esetek is amikor a modell transzformáció komplexitása és elkészítésének költsége, ha egyáltalán lehetséges ilyen készíteni, nagyobb mintha speciálisan az adott nyelvhez készítenénk egy speciális eszközt ami megvalósítja az állvart funkcionalitást.

2.5. Felhasznált technológiák

2.5.1. Eclipse Modeling Framework

Az Eclipse Modeling Framework (EMF) Eclipse pluginok egy halmaza amellyel jellemzően adatmodelleket tudunk készíteni illetve ezekből kódot vagy valamilyen dokumentumot generálni. Az EMF kétféle modell között tesz különbséget. Az egyik típus a metamodellek, a modell struktúrája azaz a felhasználó által definiált elemek és lehetséges kapcsolataik, megkötések. Illetve a példánymodellek, azok a modellek amik a metamodel által leírt elemekből állnak és ennek megfelelő kapcsolatokat tartalmaznak ezek között. Az EMF-nek van egy meta-metamodelje ami a felhasználók által létrehozott metamodellek metamodelleként szolgál (2.5. ábra) ezen felül API-t biztosít modellek manipulálásához és a modell elemekkel kapcsolatos események kezeléséhez.

Az EMF legjellemzőbb használati esete az, hogy valamilyen szabványos általában XMI formában metamodelleket hozunk létre, majd ennek megfelelő Java implementációs osztályokat generálunk. Ez a generált kód akár kézzel ki is bővíthető. Alkalmazásunkban a példánymodelleket ezeken az osztályokon keresztül tudjuk létrehozni és manipulálni. A framework lehetővé teszi ezeknek a szabványos formában történő kisorosítását is.



2.5. ábra. Az EMF metamodelje

A MagicDraw modelljei is realizálják az EMF-es interfészeket azonban saját implementációt használnak. Ez lehetővé teszi, hogy MagicDraw modelleket EMF-es API-n keresztül manipuláljuk. Ez sokszor hasznos lehet, azonban sok esetben érdemesebb a MagicDraw beépített segéd osztályaira támaszkodni. Ennek oka, hogy a MagicDraw projektek képesek elosztott környezetben is működni, ami miatt lehetnek olyan esetek, hogy a felhasználónak nincs írás hozzáférése egyes elemekhez. A MagicDraw API ilyenkor Exception dobásával képes jelezni ha az írás nem sikerült.

2.5.2. Xtext

Az Xtext egy keretrendszer amivel programozási nyelveket és egyéb szakterület specifikus nyelveket lehet készíteni, melyek szöveges formában manifesztálódnak. Ezeket valamilyen már meglévő modellezési nyelv egy konkrét szintaxisaként érdemes készíteni. Ez azt jelenti, hogy egy szövegesen megadott leírás elemeket és ezek kapcsolatait írja egy metamodellnek megfelelően.

Az Xtext nyelvtanok készítéséhez egy erős nyelvtan leíró nyelvet kínál. Az ezzel leírt nyelvtanhoz pedig teljes infrastruktúrát generál mint: parser, linker, típus ellenőrző, fordító. Ezen felül Eclipse környezetben a szerkesztéshez kapunk szintaxis kiemelést, content assistot (2.6. ábra).

MagicDraw-ban is ki tudjuk használni az Xtextben rejlő lehetőségeket és akár saját kiértékelő motort is tudunk írni, az általunk létrehozott nyelvtanokhoz. Sajnos a MagicDraw beépített szerkesztőjében elesünk olyan hasznos felhasználói funkcióktól mint a content assist vagy a szintaxis kiemelés. Erre megoldást jelenthet az Xtext language szervert támogatásának a kihasználása a dolgozat azonban ennek a vizsgálatára nem tér ki.

```
target "mysdl.mysmt"

//A[]
property @init or @myState and i < 10 is an invariant
//E<>
property @myState is reachable
//E[]
property i < 10 is sustainable
//A<>
property i == 3 is inevitable
// -->
property state i == 4 leads to state i == 5
```

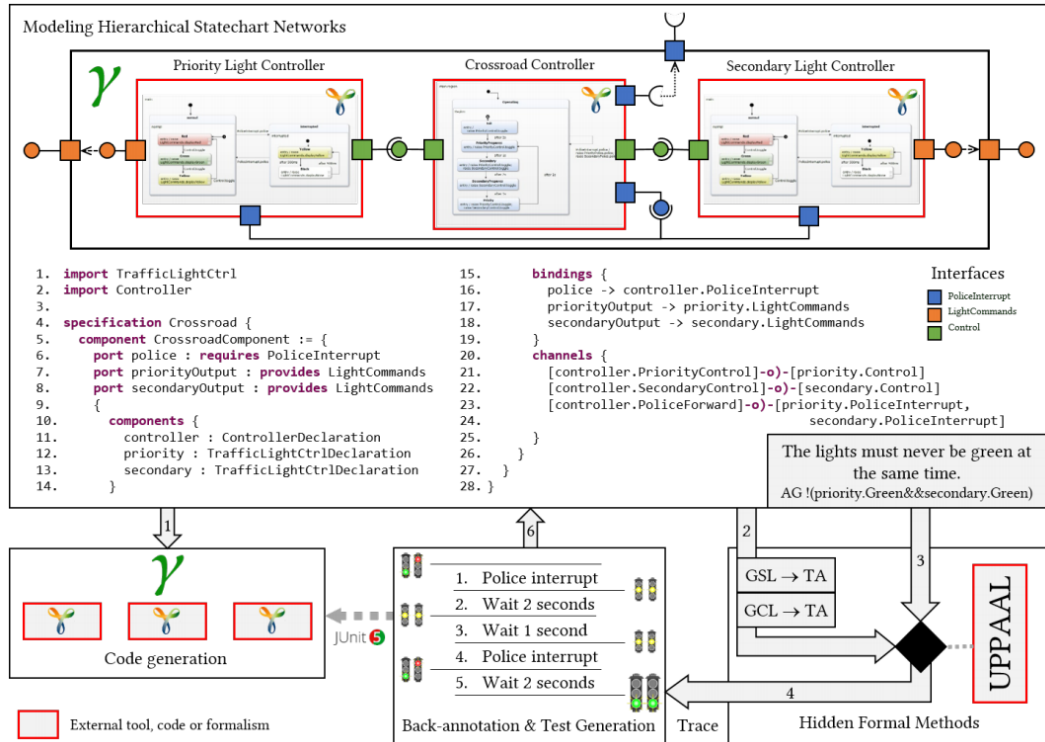
2.6. ábra. Példa: saját Xtext nyelvtan Eclipseben, szintaxis kiemeléssel

2.5.3. Gamma Statechart Composition Framework

A Gamma Statechart Composition Framework (továbbiakban Gamma) egy állapottérkép modellező keretrendszer Eclipse felett ami integrálja a YAKINDU-t, de ezen felül saját nyelveket definiál nem csak állapottérkép leíráshoz, hanem ezek kompozíciójának modellezéséhez is. Gammával a felhasználónak lehetősége van modellek formális verifikációját elvégezni, az eredményből pedig teszt kódot generálni, futtatható kód mellett.

A verifikáció eredményeként előálló időzítéseket és lépéseket visszavezeti a modellbe. Ezt Back-annotationnek nevezzük. Ezekhez szintén definiált egy nyelv, mely lehetővé teszi ezek dokumentálását.

A dolgozat elkészítése során nagy mértékben támaszkodtam a Gamma nyújtotta lehetőségekre. Ezt a Gamma mint egy köztes nyelv használatával érem el úgy, hogy modell transzformációk segítségével megvalósítok SysML-Gamma leképezést. A Gamma a formális verifikáció elvégzéséhez az UPPAAL nevű eszközt használja. Ez időzített automatákon tudja elvégezni a formális verifikációt (2.7. ábra). Ezeket a Gamma szintén modell transzformációk segítségével állítja elő, összekapcsolva a mérnöki modelleket matematikai modellekkel.



2.7. ábra. A Gamma Statechart Composition Framework¹

A Gamma nagy erőssége, hogy állapotgép kompozíciókat is lehet modellezni benne. A komponenseket végrehajtás szempontjából háromféle szemantika van megkülönböztetve.

Szinkron komponensek melyek egy lépésen belül fogadnak eseményeket ezekre lépnek és elküldik az eseményeket, ezek viszont a következő iterációban fognak fogadásra kerülni a hozzájuk kapcsolódó komponensekben.

Kaskád komponensek (Cascade Component) ezek hasonlóan működnek, mint a szinkron komponensek, viszont ebben az esetben a kiküldött üzenetek ugyan abban az iterációban kerülnek fogadásra. Ebből kifolyólag az üzenet áramlásnak aciklikusnak kell lennie, hiszen a feldolgozást végtelen ciklusba kerülne.

Aszinkron komponensek Az események feldolgozása aszinkron módon, üzenet sorok kiolvasásával történik. Állapottérkép definíciók alából szinkron szemantikával bírnak, így ahhoz hogy asszinkron szemantikával ruházzuk fel őket be kell csomagolni őket egy *Wrapperbe*. Ez definiálja számukra az üzenet sort is.

2.5.4. VIATRA²

A VIATRA egy keretrendszer mely lehetővé teszi eseményvezért modell transzformációk fejlesztését. Ehhez egy inkrementális modell lekérdezéseket leíró nyelvre a VIATRA Query Language-re (2.8. ábra) támaszkodik. A létrehozott transzformációkat egy reaktív Query Engine futtatja és tartja karban.

```
pattern StateMachines(stateMachine: StateMachine, name: java String){
    StateMachine.name(stateMachine, name);
}

pattern ParametersInStateMachine(stateMachine: StateMachine, parameter: Parameter){
    StateMachine.ownedParameter(stateMachine, parameter);
}

pattern RegionsInRegion(container: Region, region: Region){
    Region.subvertex(container, vertex);
    State.region(vertex, region);
}
```

2.8. ábra. Példa: VIATRA Query Language

A VIATRA használata jelentősen megkönnyíti a modellekkel való munkát, bár én első sorban a modell lekérdezés részére támaszkodtam a dolgozat elkészítése alatt. MagicDraw-ban egy pluginon keresztül van lehetőség VIATRA használatára melyet V4MD-nek hívnak. A plugin egy Query Engine-t biztosít számunkra per projekt. Ezen keresztül tudunk lekérdezéseket és transzformációkat regisztrálni. A V4MD leveszi a vállunkról a terhet az Engine életciklus menedzsmentjét illetően, azonban hátránya, hogy nagyon nagy modelleket komplex lekérdezések esetén a memóriagigénye elég jelentősre duzzadhat a háttérben, cserébe viszont az inkrementális működésnek köszönhetően a lekérdezések már csak a VIATRA által karbantartott táblázatokból való kiolvasás ezért költségül elhanyagolható.

2.6. MagicDraw állapotterkép verifikációs plugin

Ebben az alfejezetben bemutatom azt a SysML állapotterkép verifikációs eszközt, mely korábbi egyetemi munkám eredményeként képes volt MagicDraw modellek ellenőrzésére.

2.6.1. MagicDraw - Gamma transzformáció

A MagicDraw beépülő modul fő célja SysML állapotterképek formális verifikációja. A Gamma képes állapotgépek ellenőrzésére ezek viszont a Gamma saját nyelvén kellene, hogy legyenek definiálva. Modell transzformációk segítségével azonban lehetőségünk nyílik Gamma modellek származtatására SysML modellekből és ezáltal ellenőrizni őket.

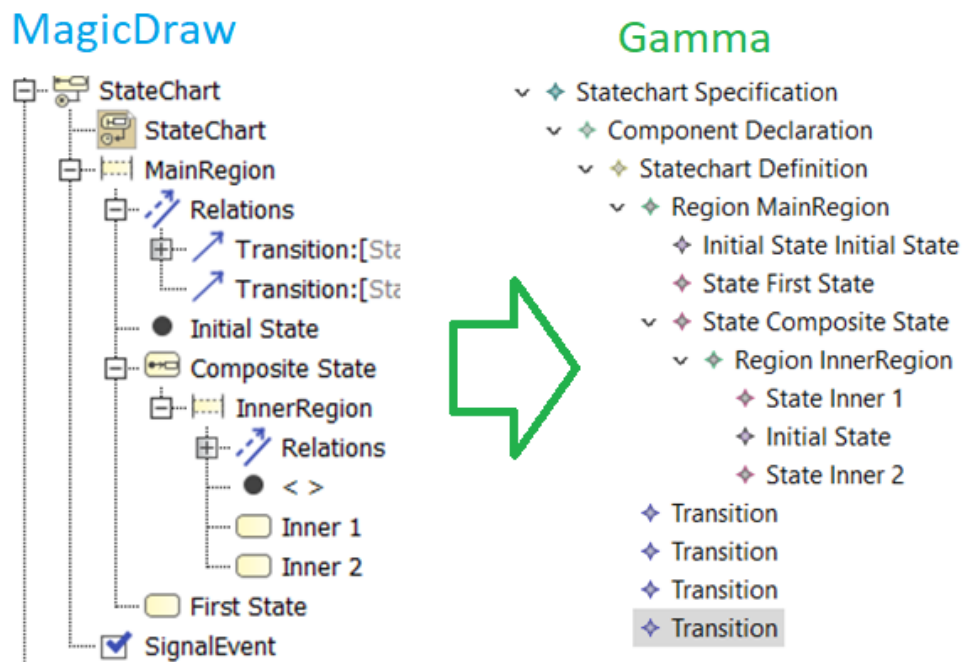
Ez a származtatás vagy modell transzformáció képezi az ötlet alapját (2.9. ábra). A kihívás pedig az két nyelv közötti szemantikai különbségek feloldása illetve az elemek megfelelő egymáshoz rendelésének megtervezése és végrehajtása.

2.6.2. Verifikáció menete

A verifikáció elvégzése a MagicDraw beépülő modul szemszögéből négy lépésből áll:

¹Forrás: <https://inf.mit.bme.hu/sites/default/files/publications/icse18.pdf>

²<https://www.eclipse.org/viatra/>



2.9. ábra. Példa: egy modell transzformációra MagicDrawról Gammára

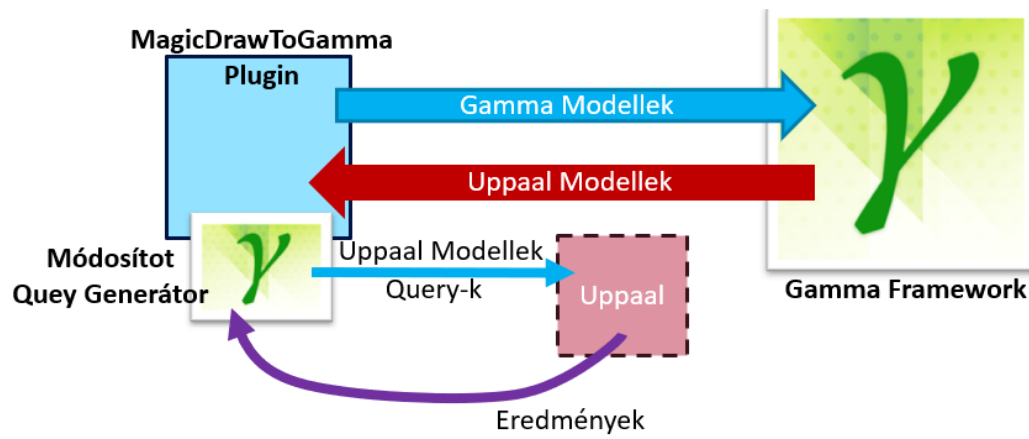
- MagicDraw modellek Gammává transzformálása
- Gamma modellek UPPAALmodellé transzformálása (ezt a Gamma keretrendszer végzi el)
- tulajdonságok ellenőrzése UPPAAL segítségével
- Eredmény megjelenítése

Ezt a folyamatot 2.10. ábra szemlélteti. A Gamma által elvégzett lépéseket a zöld "Gammák" jelölik a modellben. Az ábrán a verifikációt a "Módosított Query Generátor" kezdeményezi, mely szintén a "Gamma" jelölést kapta. Ennek oka, hogy a beépülő modul ezen verziójában az ellenőrizendő tulajdonságok megadása még nem volt kiforrott ezért egy a Gamma keretrendszerből átemelt megoldás segítségével lehetett ezeket megadni és a verifikációt kezdeményezni.

2.6.3. Örfeltételek, akciók

SysML nem definiál akció nyelvet örfeltételek és akciók végrehajtásához. Míg akciókat tudunk modellezni bármilyen viselkedést leíró modell segítségével, addig az örfeltételeket jellemzően valamilyen szöveges nyelvtannal szokás megadni.

Ahhoz, hogy a modell ellenőrzést végre lehessen hajtani ezeknek a Gamma számára érthető kifejezéseknek kell lenniük. A pluginnak ez a verziójában ezért minden örfeltélt és akciót a Gamma által biztosított nyelvtan segítségével kellett megírni. Ez abból a szempontból nem szerencsés, hogy ez nem egy olyan elterjedt nyelv, mint például a javascript amit a MagicDraw felkínál, továbbá nem áll még rendelkezésre olyan interpreter a MagicDraw-ban ami lehetővé tenné ezek futtatását ami elengedhetetlen többek között a modellek szimulációjához.



2.10. ábra. Verifikáció menete a pluginban

3. fejezet

Plugin továbbfejlesztése

Ebben a fejezetben ismertetem azokat a fejlesztéseket amelyeket a mesterképzés során az eszközön végeztem.

3.1. Fejlesztés céljai

A fejlesztés során hozott alkalmazott megoldások áttekintése előtt érdemes végigmenni a fejlesztés kitűzött céljain és átgondolni ezek létjogosultságát.

3.1.1. Funkcionális dekompozíció transzformálása

Egy rendszert állapotait és állapotváltásait le lehetne modellezni egy mindent tartalmazó állapotgéppel, párhuzamos régiókkal és egyéb modellezési megoldásokkal. Ahogy a modell mérete nő a funkcionalitást érdemes feldarabolni és részenként modellezni. Ez nem csak az áttekinthetőséget segíti, de megkönnyíti a modellen való csapatmunkát is a mérnökök számára hiszen a szétbontott részeket külön, egymástól független lehet modellezni, majd ezeket összekapcsolni.

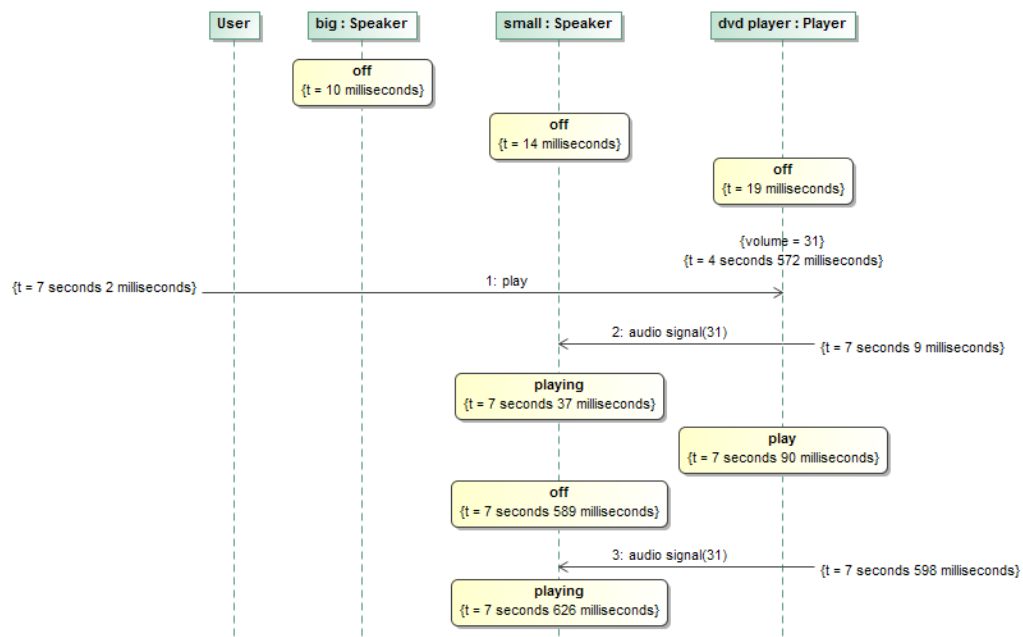
Szerencsére a Gamma erre a problémára is megoldást kínál, támogatja az állapot dekompozíció modellezését és formális verifikációját.

3.1.2. Eredmények megjelenítése

Fontos kérdés, hogy a formális verifikáció eredményét milyen formában kívánjuk megjeleníteni a mérnökök számára. A plugin eddigi verziója csak arra a kérdésre tudott választ adni, hogy teljesülnek-e a modellel szemben támasztott megkötések vagy sem.

Az UPPAAL és a Gamma is képes sokkal részletesebb választ adni. Ezt a Gamma Back-annotation formájában teszi azaz a verifikációban előállt időzítések és lépéseket visszavezeti az eredeti modellbe. Ehhez a Gamma egy elég jól értelmezhető nyelvtant definiál, azonban a SysML-t jellemzően rendszermérnökök használják akik inkább a diagramokat mint a szöveges leírásokat preferálják általában.

A Back-annotationt úgy is lehet interpretálni mint lépések egy sorozatát, amelyek szinkron esetben egymást jól meghatározható sorrendben követik. Ezt leginkább szekvencia diagramokon lehet ábrázolni. Ezen felül ami miatt még a szekvencia diagram tűnik a legkézenfekvőbb megjelenítési megoldásnak az a MagicDraw, illetve a Cameo Simulation toolkit. Ez ugyanis képes szimulációt rögzíteni szekvencia diagramok formájában (3.1. ábra)) és ezeket újra lejátszani. A cél tehát olyan szekvencia diagramok előállítása úgy mint-hogyha a szimulátort használva találtuk volna meg a hibautakat, így ezekről nem csak egy jól áttekinthető megoldást kapunk szekvenciák formájában, hanem ezek szimulálhatók is lesznek Cameo Toolkit segítségével.



3.1. ábra. Rögzített szimuláció szekvencia diagramon¹

3.1.3. Követelmények definiálása

A formális verifikáció elvégzéséhez a modelleken felül meg kell tudnia a felhasználónak azokat a kérdéseket melyekre választ szeretne kapni a modell ellenőrzése során. Ezek jelen esetben a "Kerülhet-e a rendszer adott állapotba" illetve "Adott állapotból el tud-e jutni egy másikba" típusúak jellemzően. A beépülő modul a kérdés vagy megkötések megfogalmazásához egy saját nyelvet kínál, amely azt érhetőséget célozza.

3.2. MagicDraw profil

A SysML nyelv nagyon általános, ezért célszerű specializálni, új elemeket bevezetni, vagy kiegészíteni a már meglévőket. Ennek eléréséhez készítettem egy UML profilt. Ez három részből áll.

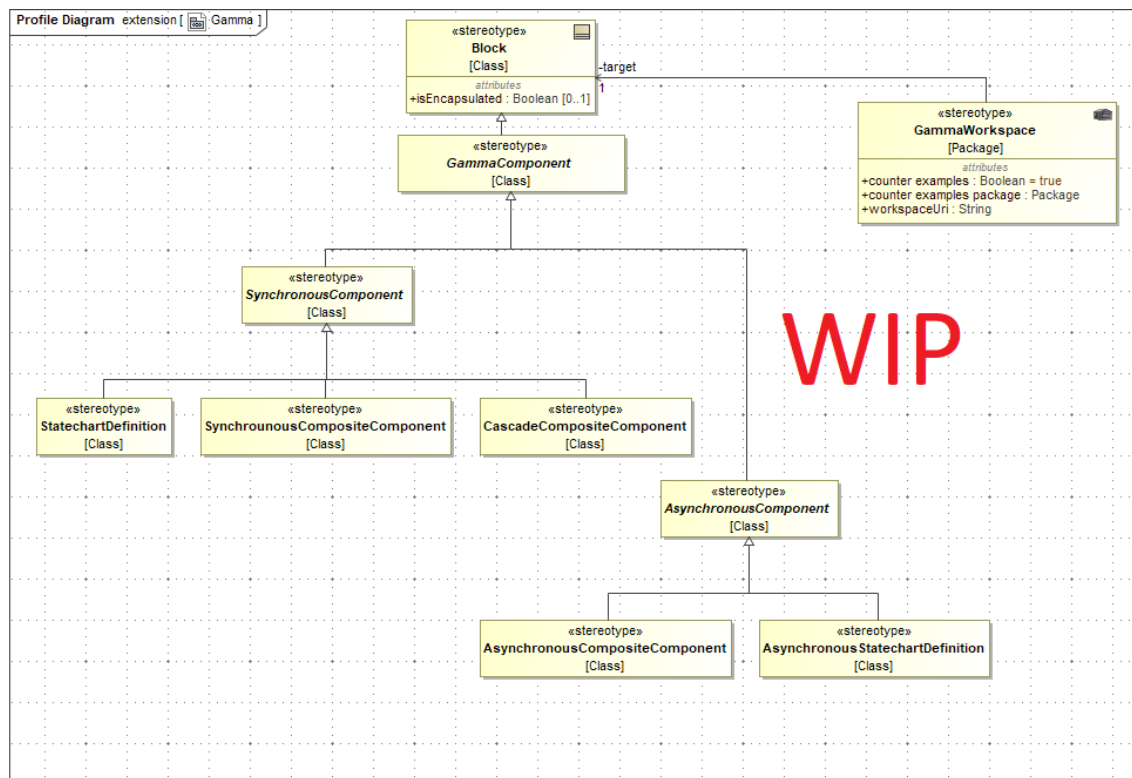
- Kompozit szemantika
- Check modell
- Back-annotation modell

Az UML profil érdekessége, hogy tartalmazásokat csak megkötés szintjén customizationön keresztül tudunk megadni. UML profil diagramon csak öröklést és attribútumokat tudunk definiálni elemeinknek.

¹Forrás: <https://docs.nomagic.com/display/CSTD184/Recording+simulation+as+a+Sequence+diagram>

3.2.1. Kompozit szemantika

A Gamma háromféle komponens végrehajtási szemantikát biztosít a felhasználók számára. Ugyan ezt implicit módon is meg lehet határozni, például a kommunikáció típusából, mégis fontos lehet ezek egyértelmű jelölése. Ezért az UML profil (3.2. ábra) a SysML nyelvet kiegészíti néhány sztereotípiával melyek segítségével explicit jelölhetők, hogy milyen szemantikát szeretne a felhasználó érteni Blokkjain.



3.2. ábra. Szinkron, asszinkron szemantikát támogató UML profil

3.2.2. Check modell

Ahhoz, hogy a formális verifikáció végrehajtható legyen ki kell választani, hogy milyen modelleket szeretnénk ellenőrizni és ezeken milyen követelményeket. Ezeknek a megadására sokféle megoldás például egy varázsló jellegű menü is elképzelhető. Én azonban ezeket az információkat magában a modellben tárolom el egyéb az technológiák és az infrastruktúra sajátosságaiból adódó információkkal együtt.

Az elképzelés szerint a felhasználó *Workspace*eket hoz létre. Ezek hivatkoznak a felhasználó számítógépén egy könyvtárra melyet az infrastruktúra sajátosságából adódó háttértárra kimentendő modelleket tárolására használok. Ezen felül ezen keresztül kell behivatkozni az ellenőrizendő modellt a projektből.

A modell transzformációk során *Trace*k keletkeznek. Ezek alapján lehet visszakeresni, hogy mely a MagicDraw - Gamma transzformáció során milyen leképzések történtek.

A követelményeket *GammaProperty* segítségével lehet megadni a plugin által definiált nyelvtan segítségével. Az ezek ellenőrzéséből származó Back-annotaion modellek is a *Workspace*ben helyezkednek el. A modell elemei a következők:

- **GammaWorkspace**

Transzformációk és ellenőrzések kezelésére szolgáló MagicDraw projektben tárolt

modell.

Attribútumok:

Target: InstanceSpecification[1]: transzformálandó modell

WorkspaceUri: String: egy elérési út a felhasználó egy könyvtárához

Counter examples: Boolean: Back-annotation engedélyezése

- **GammaCheck**

*GammaProperty*k konténere

- **GammaProperty**

Egy a modellel szemben támasztott követelmény a saját nyelven

Attribútumok:

body: String[1]: saját nyelven írt kifejezés

- **GammaWorkspaceFile**

Hivatkozás egy Gamma modellre a háttértáron. A modell elem neve a fájl elérési útja.

- **MD2G_Trace**

Egy megfeleltetés a MagicDraw és Gamma modellek között. A MagicDraw elemre egy Trace él mutat, a Gammabeli modell elem pedig EMF hivatkozás formájában kerül tárolásra.

Attribútumok:

URIFragment: String[1]: hivatkozás EMF-es modell elemekre

3.2.3. Back-annotation modell

A back-annotation modell feladata visszacsatolni az eredeti modellbe a valamilyen külső, jellemzően szimulátorból származó időzítési adatokat. A Gamma is készít egy ilyen modellt. A megoldás amit kidolgoztam Gamma modell egy MagicDraw specifikus változatának létrehozásából és egy Gamma-MagicDraw transzformáció megtervezéséből és megvalósításából állt. Az UML profil egy szakterület specifikus nyelvet definiál. Elemei pedig a következők:

- **ExecutionTrace**

Egy kompozit komponens végrehajtása. *Steppeket* azaz lépéseket tartalmaz, illetve a végrehajtás végén állhat egy lépésekből álló ciklus.

Attribútumok:

component: InstanceSpecification[1]: kompozit komponens példánya a modellben

steps: Step[1..*]: lépések

cycle: Cycle[0..1]: lépésekből álló ciklus amire a végrehajtás futhat

- **Step**

A végrehajtás egy lépése. Két részből áll egy *Act* részből, ami a végrehajtott műveleteket írja le és egy *Assert* részből, ami a lépésben elért állapotot írja le.

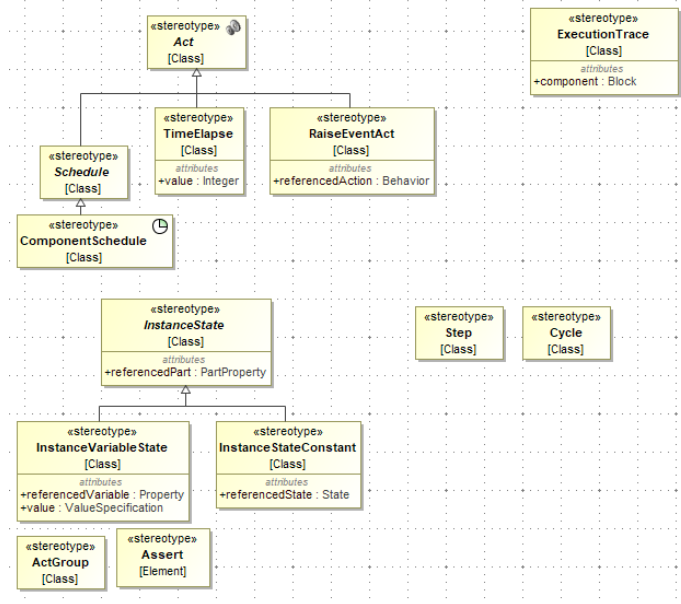
Attribútumok:

actGroup: ActGroup[0..1]: műveletek konténere

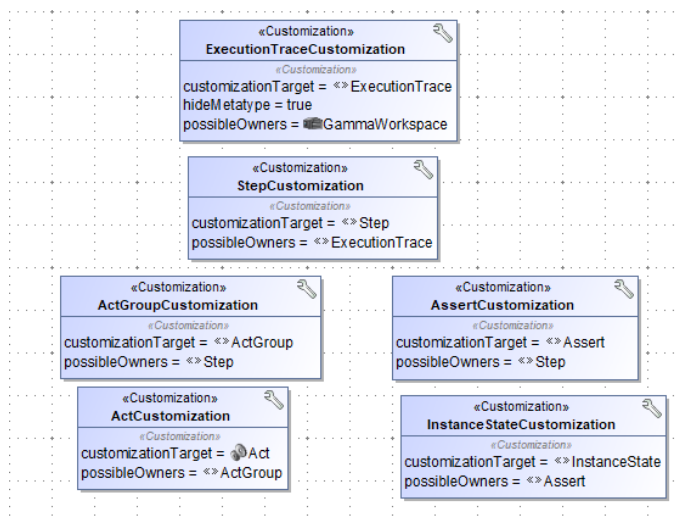
assert: Assert[1]: lépés során beálló állapotok

- **ActGroup**
Actok konténere a *Steppen* belül. Csak áttekinthetőségre szolgál.
Attribútumok:
acts: Act[0..*]: műveletek konténere
- **Act**
Absztrakt sztereotípi. Egy végrehajtott művelet.
- **ComponentSchedule**
Komponensen egy kör végrehajtása (üzenetek kiolvasása az üzenetsorokból, állapotok léptetése)
- **TimeElapse**
Végrehajtás várakoztatása bizonyos ideig.
Attribútumok:
value: Integer: várakozás ideje milliszekundumban
- **RaiseEventAct**
Egy esemény elküldése a komponens példánynak.
Attribútumok:
referencedAction: Behavior: eseményt küldő viselkedés.
- **InstanceState**
Absztrakt. Az egyes példányok, partok állapotainak leírása.
Attribútumok:
referencedPart: PartProperty: hivatkozott komponens példány
- **InstanceVariableState**
Egy változónak egy állapota.
Attribútumok:
referencedVariable: Property: hivatkozott változó
value: ValueSpecification: hivatkozott változó értéke
- **InstanceStateConstant**
Az állapot gép egy állapota.
Attribútumok:
referencedState: State: hivatkozott állapot konstans

A 3.3. ábra az UML profilt, a 3.4. ábra pedig ennek a customizationjét mutatja.



3.3. ábra. Back-annotation UML profilja



3.4. ábra. Back-annotation customization modellje

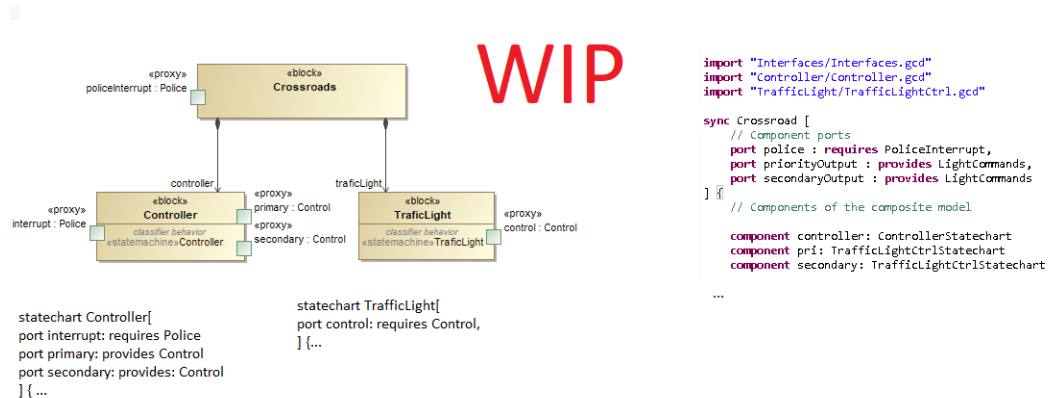
3.3. Kompozíciók transzformációja

Egy nagy komplex rendszert célszerű nem egyben, hanem részekre bontva modellezni majd a részek egymáshoz illesztéséből, komponálásából képezni a teljes rendszert. Állapottérképek dekomponálását azaz részekre bontását a Gamma is támogatja. A kihívás a SysML és a Gamma közötti megfeleltetések megválasztása oly módon, hogy a szemantika ne sérüljön. A megfeleltetés két szemponttól kell vizsgálni, egyszer az elemek tartalmazási hierarchiái szerint, egyszer pedig a köztük modellezett kommunikáció szerint.

3.3.1. Struktúra megfeleltetése

A Gammában nyelvi szinten elkülönül az állapottérkép (StatechartDefinition) és a kompozit komponens (Composite Component) fogalma. Állapottérképek a modell hierarchia gráfjában a levelekben helyezkednek el. SysML esetében a minden Bloknak lehet visel-

kedése, jelen esetben állapottérképe. A megfeleltetés elvégzéséhez megkötést fogalmaztam meg mely kétféle blokkot enged meg. A viselkedéssel rendelkező blokkokat és azokat amelyek nem tartalmazhatnak viselkedést csak Part Propertyket. Tehát állapottérképek ebben a modellben is csak levelekben lehetnek.



3.5. ábra. Struktúra megfeleltetése

Az érdekes kérdés lehet, hogy ha egy magasabb szintű blokknak mégis lehetne viselkedése, azt szemantikailag hogyan kezelhetnénk. Elképzelhető olyan értelmezés, hogy ez a magas szintű állapottérkép a dekomponált részek együttes viselkedését írja le. Ez lehetőséget adna arra, hogy a magasabb és az alacsonyabb szintű viselkedés halmazt összehasonlítsuk működés szempontjából és ha nincsenek szinkronban akkor tervezési hibaként fogjuk fel. Így a magasabb hierarchia szintek tulajdonképpen validálnák az alacsonyabb szinteket. Ennek a lehetőségnek a komolyabb kifejtése azonban nem célja a dolgozatnak.

3.3.2. Kommunikáció megfeleltetése

A Gammában a komponensek kommunikációja kimondottan az eseményvezérelt állapot alapú rendszerek sajátosságain alapul, azonban SysML-ben a kommunikáció leírása sokkal általánosabb és többféle módon is megadható. Éppen ezért a feladat elvégzése során az események és az interfészek modellezésére megkötéseket kellett megfogalmazni. Az egyik ilyen megkötés szerint a portokban interfész blokkokat kell tipizálniuk és szinkron szemantika esetében operációkat definiálni, asszinkron esetben pedig szignálokkal tipizált *Flow Property* formájában fel kell tüntetni milyen szignálok fogadására képes a blokk.

Az eseményeknek mindig specifikálniuk kell, hogy melyik porton várják az operáció hívását vagy szignál érkezését. Ez igaz az akciókra az ő esetükben azt kell specifikálni, hogy milyen porton keresztül történjen a küldés.

Portok közül csak a *Proxy* portok támogatottak. Proxy portok iránya származtatott a *Flow property* irányokból amik keresztül mehetnek rajta. Az irány az *isConjugated* flag igazra állításával változtatható. Az alap szemantika szerint minden port az interfész blokkját kínálja (provide), conjugate hatására pedig várja (require). Operációk minden esetben in irányúak.

3.4. CTL nyelvtan

3.5. Back-annotation transzformációja

A Back-annotation egy általában szimulátor által biztosított időzítési adatok visszacsatolása az eredeti modellbe. Ahhoz, hogy MagicDrawban is el tudjuk tárolni ezeket az adatokat létre kellett hoznom egy UML profilt ami a Back-annotation modell metamodelljeként fog szolgálni.

A transzformáció iránya itt megfordul nem MagicDraw modellekből állítok elő Gamma modelleket hanem épp fordítva Gammából alakítok MagicDraw-ra.

3.6. Szimuláció

3.7. Példa

4. fejezet

Értékelés

Ebben a fejezetben értékelem a megoldást és megvizsgálom az alternatív lehetőségeket, illetve összevetem ezekkel az alkalmazott megoldást.

5. fejezet

Összefoglalás