Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Measurement and Information Systems

Formal modeling and verification of process models in component-based reactive systems

Scientific Students' Association Report

Author:

Ármin Zavada

Advisor:

dr. Vince Molnár
Bence Graics

Contents

Kivonat

A biztonságkritikus rendszerek komplexitása folyamatosan növekedett az elmúlt években. A komplexitás csökkentése érdekében a modellalapú paradigma vált a meghatározó módszerré ilyen rendszerek tervezéshez. Modellalapú rendszertervezés során a komponensek viselkedését általában állapotalapú, vagy folyamatorientált modellek segítségével írjuk le. Az előbbi formalizmusa azt írja le, hogy a komponens milyen állapotokban lehet, míg az utóbbié azt, hogy milyen lépéseket hajthat végre, valamint milyen sorrendben. Gyakran ezen modellek valamilyen kombinálása a legjobb módja egy komplex komponens viselkedésének leírásához.

Formális szemantikával rendelkező modellezési nyelvek lehetővé teszik a leírt viselkedés (kimerítő) verifikációját. Formális verifikáció használatával már a fejlesztés korai fázisaiban felfedezhetőek a hibák: a módszer ellenőrzi, hogy a rendszer egy adott (hibás) állapota elérhető-e, és amennyiben elérhető, ad hozzá egy elérési útvonalat. A formális verifikációs eszközök emiatt gyakran csak alacsony szintű, állapotalapú modelleken működnek, melyek messze vannak az emberek által könnyen érthető nyelvektől. Ezért, hogy magas szintű viselkedési modelleket tudjunk verifikálni, implementálnunk kell egy olyan modell transzformációt, mely megtartja a folyamat- és állapotalapú modellek szemantikáját azok kombinációja után is.

Ebben a dolgozatban megvizsgálom a folyamatalapú modellek szemantikáját, valamint a kapcsolatukat egyéb hagyományos állapotalapú modellekkel. Emellett megoldásokat vetek fel a potenciális konfliktusokra a kombinált alacsonyszintű modellben. Munkám során a Gamma állapotgép kompozíciós keretrendszerre építek, mellyel komponensalapú reaktív rendszereket modellezhetünk és verifikálhatunk. Mivel a Gamma még nem támogatja az aktivitásokat, bevezetek egy új aktivitás nyelvet, melyhez a SysMLv2 szolgál inspirációként. Ezzel együtt implementálom hozzá a szükséges transzformációkat a Gamma alacsony szintű analízis formalizmusára. Végezetül pedig kiértékelem a koncepcionális és gyakorlati eredményeket esettanulmányokon és méréseken keresztül, valamint felvetek lehetséges fejlesztéseket és alkalmazásokat.

Abstract

The complexity of safety-critical systems has been increasing rapidly in recent years. To mitigate said complexity, the model-based paradigm has become the decisive way to design such systems. In model-based systems engineering, we usually define the behaviour of system components using state-based or process-oriented models. The former formalism describes what states the component can be in, while the latter describes what steps it can perform and in what order. Oftentimes, the best way to model the behaviour of a complex component is to combine these models in some way.

Modelling languages with formal semantics enable the (exhaustive) verification of the described behaviour. Formal verification may be used to detect errors early during development by checking if a given (erroneous) state of the system can be reached, and if so, providing a way to reach it. Formal verification tools often require low-level state-based mathematical models, which are far from human-understandable languages. Thus, to enable the verification of high-level behavioural models, a model transformation must be implemented that preserves the semantics of both process-oriented and state-based models, even when combined.

In this report, I analyse the semantics of process-oriented models, as well as its relation to traditional state-based models, and propose solutions for the possible conflicts in a combined low-level model. In my work, I build on the Gamma Statechart Composition Framework, which is a tool for modelling and verifying component-based reactive systems based on statecharts. Since Gamma does not support activities yet, I introduce a new activity language inspired by SysMLv2, and implement the necessary transformations to Gamma's low-level analysis formalism. Finally, I evaluate the conceptual and practical results through case studies and measurements then propose potential improvements and applications.

Chapter 1

Introduction

The complexity of safety-critical systems has been increasing rapidly in recent years. To mitigate said complexity, the model-based paradigm has become the decisive way to design such systems. In model-based systems engineering, we usually define the behaviour of system components using state-based or process-oriented models. The former formalism describes what states the component can be in, while the latter describes what steps it can perform and in what order. Oftentimes, the best way to model the behaviour of a complex component is to combine these models in some way.

Modelling languages with formal semantics enable the (exhaustive) verification of the described behaviour. Formal verification may be used to detect errors early during development by checking if a given (erroneous) state of the system can be reached, and if so, providing a way to reach it. Formal verification tools often require low-level state-based mathematical models, which are far from human-understandable languages. Thus, to enable the verification of high-level behavioural models, a model transformation must be implemented that preserves the semantics of both process-oriented and state-based models, even when combined.

Gamma Statechart Composition Framework is a tool for bridging the gap between the two models. It is a tool for modelling and verifying component-based reactive systems based on statecharts. Since Gamma does not support activities yet, I introduce a new activity language inspired by SysMLv2, and implement the necessary transformations to Gamma's low-level analysis formalism.

ezt még át kéne írni

kicsit beszélni a létező implementációkró

Chapter 2

Background

In this chapter I address the foundations of this work. In **??** I introduce the theoretical bases of behaviour modeling, which is used widely in systems engineering, and their implementation in an existing language - SysML. After this I talk about Formal Verification in Section 2.2, which is a mathematically rigorous method for finding specific configurations of modelled systems. Lastly, I introduce the Gamma Composite Statechart Framework, which is a tool for stating and verifying composite models using statechart behaviours.

2.1 Model-based Systems Engineering

The INCOSE SE Vision 2020[1] defines Model-based systems engineering (MBSE) as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases. MBSE is part of a long-term trend toward model-centric approaches adopted by other engineering disciplines, including mechanical, electrical and software. In particular, MBSE is expected to replace the document-centric approach that has been practiced by systems engineers in the past and to influence the future practice of systems engineering by being fully integrated into the definition of systems engineering processes."

Applying MBSE is expected to provide significant benefits over the document centric approach by enhancing productivity and quality, reducing risk, and providing improved communications among the system development team.[2]

In MBSE, one of the most important concepts is the term "model" itself. In the literature it has many different definitions:

1. A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.[5]
2. A representation of one or more concepts that may be realized in the physical world.[7]
3. A simplified representation of a system at some particular point in time or space intended to promote understanding of the real system.[4]
4. An abstraction of a system, aimed at understanding, communicating, explaining, or designing aspects of interest of that system.[6]

5. A selective representation of some system whose form and content are chosen based on a specific set of concerns. The model is related to the system by an explicit or implicit mapping.[9]

As one can see, choosing a definition is very much dependent upon how we wish to use our "model"; in this work I will use the number 1 definition.

2.1.1 Systems Modeling Language

Systems Modeling Language (OMG SysML)[8] is a general-purpose modeling language that supports the specification, design, analysis, and verification of systems that may include harware and equipment, software, data, personnel, procedures, and facilities. SysML is a graphical modeling language with a semantic foundation for representing requirements, behaviour, structure, and properties of the system and its components.[7]

This work focuses only on the *behavioural* modeling tools SysML provides. In the following section, I present two of the most used concepts.

2.1.1.1 State Machine

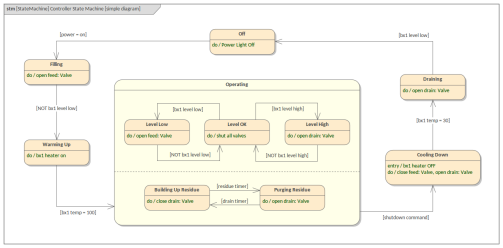

Figure 2.1: A SysML State Machine.

2.1.1.2 Activity

2.1.1.3 Differences and Combination

State Machines are a popular [1, 2] language to capture the behaviour of reactive systems[11] that react to external stimuli depending on their internal state. Stat Machines provide an expressive formalism to represent complex *state-based* behaviour by introducing hierarchical state refinement, memory (variables and history state) and complex transitions (e.g., fork and join transitions).

As contrast, Activities model the behaviour of distributed systems with many interconnecting components, all running in parallel; said components may have dependencies on each other (one calculates a value the other needs), or have a limited resources (a factory only has one worker).

SysML provides a functionality to combine different behaviours, using the *call behaviour* pattern. By using a call behaviour action inside a State Machine, we are able to combine the behaviour of the two. This is the basis of composite behaviour models, and the motivation of this work.

2.2 Formal Verification

In order to raise the reliability of system analysis, a system analysis technique is required that can have the precision of paper-and-pencil based mathematical proofs, and thus does not rely upon computer-arithmetic, and utilizes the computers for bookkeeping, to be able to handle complex systems without having to worry about human-errors. Formal verification methods, which are primarily based on theoretical computer science fundamentals like logic calculi, automata theory and strongly type systems, fulfil these requirements. The main principle behind formal analysis of a system is to construct a computer based mathematical model of the given system and formally verify, within a computer, that this model meets rigorous specifications of intended behaviour. Due to the mathematical nature of the analysis, 100% accuracy can be guaranteed.[12]

2.2.1 Model Checking

Model Checking is a formal verification method to verify properties of finite systems, i.e., to decide whether a given formal model M satisfies a given requirement γ or not. The name comes from formal logic, where a logical formula may have zero or more models, which define the interpretation of the symbols used in the formula and the base set such that the formula is true. In this sense, the question is whether the formal model is indeed a model of the formal requirement: $M \models \gamma$?

Model Checker algorithms (see Figure 2.2), such as UPPAAL[1][3] or Theta[2][16] use SAT solvers to answer this question; and can even return a *proof* (i.e., a part of the model) that M indeed does satisfy said requirement[3].

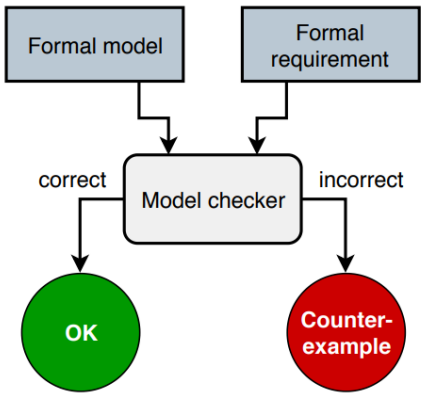

Figure 2.2: An illustration of model checking.

2.2.2 Petri Net

Petri nets are a widely used formalism to model concurrent, asynchronous systems [15]. The formal definition of a Petri net (including inhibitor arcs) is as follows (see Figure 2.3 for an illustration of the notations).

[1]https://uppaal.org/
[2]https://inf.mit.bme.hu/en/theta
[3]These proofs usually come in the form of an execution trace

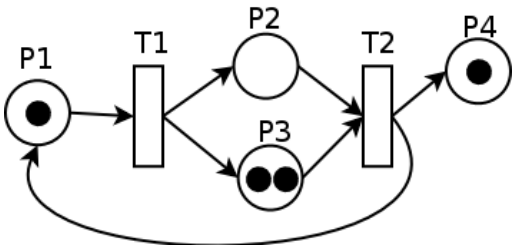

Figure 2.3: An example Petri net with 2 transitions and 4 places.

Definition 1 (Petri net). A Petri net is a tuple $PN = (P, T, W, M_0)$

- P is the set of *places* (defining state variables);
- T is the set of *transitions* (defining behaviour), such that $P \bigcap T = \emptyset$;
- $W \subseteq W^+ \bigcup W^-$ is a set of two types of arcs, where $W^+ : T \times P \to \mathbb{N}$ and $W^- : P \times T \to \mathbb{N}$ are the set of input arcs and output arcs, respectively ($\mathbb{N}$ is the set of all natural numbers);
- $M_0 : P \to \mathbb{N}$ is the *initial marking*, i.e., the number of *tokens* on each place. ▪

The state of a Petri net is defined by the current marking $M : P \to \mathbb{N}$. The behaviour of the systems is described as follows. A transition t is enabled if $\forall p \in P : M(p) \in W(p, t)$. Any enabled transition t may fire non-deterministically, creating the new marking M' of the Petri as follows: $\forall p \in P : M'(p) = M(p) - W^-(p, t) + W^+(t, p)$.

In words: W describes the *weight* of each flow from a transition to a place, or from a place to a transition. Firing a transition t in a marking M consumes $W^-(p_i, t)$ tokens from each of its input places p_i, and produces $W(t, p_o)$ tokens in each of its output places p_o. One such transition t is *enabled* (it may *fire*) in M if there are enough tokens in its input places for the consumptions to be possible, i.e., if and only if $\forall p : M(p) \geq W(s, t)$.

2.2.3 Activities as Petri Nets

As I have mentioned in the beginning of this Section, formal verification requires models to be specified using *mathematical* precision. In the paper called "Verifying SysML activity diagrams using formal transformation to Petri nets"[13] by Edward Huang, Leon F. McGinnis and Steven W. Mitchell they propose a way to *partially* map SysML activity diagrams to Petri nets. In the following, I will summarise their work.

Constrained Sub-set of SysML

Since SysML Activity Diagrams do not have exact execution semantics[14], the PN mapping can only be done for a limited subset of the modeling elements: actions, initial nodes, final nodes, join nodes, fork nodes, merge nodes, decision nodes, pins and object/control flows, which have precise execution semantics as defined in the Foundational Subset for Executable UML Models.[10]

The other constraints are:

1. The value of tokens is not considered.

Node type	Inputs	Outputs	Petri net
Action	0	>= 1	
Action	>= 0	0	
Action	>= 0	>= 1	
Fork	1	>= 1	
Join	>= 1	1	

Table 2.1: LAS nodes mapping.

Node type	Inputs	Outputs	Petri net
Activity final node	>= 1	0	
Merge node	>= 1	1	
Decision node	1	>= 1	
Pin	>= 0	>= 0	

Table 2.2: IR nodes mapping.

2. Control flows with multiple tokens at a time are not considered.
3. Optional object/control flows are not considered, i.e., multiplicity lower bounds are strictly positive.

As a result of these constraints, the exact semantics of activities cannot be described using only Petri nets. This fact will be addressed in Chapter 4.

Mapping Rules

The paper groups the given elements into two sets: "load-and-send" (LAS) and "immediate-repeat" (IR)

LAS nodes are fired when all their inputs have tokens equal to or more than the weight function (in PN) or the multiplicity lower bounds (in activity diagrams). When an LAS node fires,the number of tokens (equal to the weight function or the multiplicity lower bound) associated with an input arcs/pin is consumed and the number of tokens (equal to the weight function or the multiplicity lower bound) associated with an output arc/pin is added. Examples of LAS nodes in PN are transitions. Table 2.1 shows the mapping rules for LAS nodes.

In contrast, as soon as an IR node receives a token from any input, it immediately adds a token to its output nodes. Places in PN are an example of IR nodes. Table 2.2 shows the mapping rules for IR nodes.

2.3 The Gamma Statechart Composition Framework

The Gamma Statechart Composition Framework is a tool created to support platform-independent modeling and heterogeneous development of [system] components. For my purposes, it provides an interface to *design* composite systems and transform them to a verifiable model (XSTS).

részletesebben, komponensek felírása, mert később még bele fogunk nyúlni

2.3.1 Statechart

2.3.2 Activity

2.4 Extended Symbolic Transition System

The high-level nature of engineering models means they are easy-to-use for engineers, but leads to difficulties during the formal verification process. In case of statecharts for example, orthogonal regions, hierarchical state-refinement or broadcast communication are all high-level constructs that make the modeling workflow more intuitive and enable the modeling of significantly more complex systems. They are however difficult to process using formal methods that are defined on low-level mathematical formalism and verified using SMT solvers. In this section, I introduce the XSTS language, which is a low-level modeling formalism designed to bridge the aforementioned gap between engineering models and formal methods.

2.4.1 Formal definition

Definition 2 (Extended symbolic transition system). An *Extended symbolic transition system* is a tuple $XSTS = (D, V, V_C, IV, Tr, In, En)$, where:

- $D = D_{v1}, D_{v2}, \ldots, D_{vn}$ is a set of value domains;
- $V = v_1, v_2, \ldots, v_n$ is a set of variables with domains $D_{v1}, D_{v2}, \ldots, D_{vn}$;
- $V_C \subseteq V$ is a set of variables marked as *control variables*;
- $IV \in D_{v1} \times D_{v2} \times \cdots \times D_{vn}$ is the *initial value function* used to describe the initial state. The initial value function IV assigns an initial value $IV(v) \in D_v$ to variables $v \in V$ of their domain D_v;
- $Tr \subseteq Ops$ is a set of operations, representing the *internal transition relation*; it describes the internal behaviour of the system;
- $In \subseteq Ops$ is a set of operations, representing the *initialisation transition relation*; it is used to describe more complex initialisation, and is executed once and only once, at the very beginning;
- $En \subseteq Ops$ is a set of operations, representing the *environmental transition relation*; it is used to model the system's interactions with its environment. ▪

In any state of the system a single operation is executed, which is selected from the sets introduced above. The set from where the operation can be selected depends on the current state. In the initial state - (which is described by the initialization vector IV) - only operations from the In set can be executed. Operations from the In set can only fire in the initial state and nowhere else. After that, En and Tr can be fired in an alternating manner.

Operations $op \in Ops$ describe the transitions between states of the system, where Ops is the set of all possible transitions. All operations are atomic in the sense that they are either executed in their entirety or none at all.

2.4.2 Language constructs

In the following section, I will introduce the language constructs and their semantics of XSTS language.

2.4.2.1 Types

XSTS contains two default variable types, logical variables (*boolean*) and mathematical integers (*integer*). Types defined this way make up the domains $D_{v1}, D_{v2}, \ldots, D_{vn}$ introduced in Extended symbolic transition system 2.4.1. XSTS also allows the user to define *custom types*, similarly to enum types in common programming languages.

A custom type can be declared the following way:

```
type <name> : { <literal_1>, . . . , <literal_n> }
```

Where $D_{name} = \{literal_1, \ldots, literal_n\}$.

2.4.2.2 Variables

Variables can be declared the following way, where `<value>` denotes the value that will be assigned to the variable in the initialization vector:

```
var <name> : <type> = <value>
```

Where v_{name} will be in domain D_{type}.

If the user wishes to declare a variable without an initial value, this is possible as well:

```
var <name> : <type>
```

A variable can be tagged as a control variable with the keyword `ctrl`:

```
ctrl var <name> : <type>
```

In which case the variable v will also be added to V_C (the set of control variables).

2.4.2.3 Basic operations

Operations make up the set *Ops* introduced in Extended symbolic transition system 2.4.1. These operations, and their compositions define the behaviour of the XSTS model.

Assume An assumption operation can only be executed, if and only if its *expression* evaluates to *true*. This fact means, that if a composite operation contains a *falsy* assumption, the whole composite operation will not fire.

A simple assumption operation can be stated like the following:

```
assume <expr>
```

Assignment Assignments have the following syntax, where `<varname>` is the name of a variable and `<expr>` is an expression of the same type:

```
<varname> := <expr>
```

An assignment operation overwrites the variables value upon execution.

Havoc Havocs give the XSTS models randomness, by randomly *assigning* a value.

The syntax of havocs is the following, where `<varname>` is the name of a variable:

```
havoc <varname>
```

2.4.2.4 Composite operations

Composite operations give way to building up more complicated transition trees, by providing nesting the already introduced simple operations.

Choice Non-deterministic choices work by randomly executing one and only one of its composed operations.

Non-deterministic choices have the following syntax, where `<operation>` are arbitrary basic or composite operations:

```
choice { <operation> } or { <operation> }
```

Sequence Sequences execute all composed operations one-by-one from top to bottom.

Sequences have the following syntax:

```
<operation>
<operation>
<operation>
```

2.4.2.5 Transitions

Each transition is a single operation (basic or composite). We distinguish between three sets of transitions, *Tran*, *Init* and *Env* - associating to the three different operation sets introduced in Extended symbolic transition system 2.4.1. Transitions are described with the following syntax, where `<transition-set>` is either `tran`, `env` or `init`:

```
<transition-set> {
    <operation>
} or {
    <operation>
} or
...
or {
    <operation>
}
```

2.4.2.6 Simple example

Below is a simple example given in the textual representation of the XSTS DSL. The XSTS has two variables, x and y, both with the inital value 0. The init transition sets both variables' values to 1. After this, the environment repeatedly increments the value of y, to which the systems reacts by either incrementing x, or leaving the value of x unchanged.

```
var x: integer = 0
var y: integer = 0
tran {
    x:=x+1
} or {
    x:=x
}
init {
    x:=1
    y:=1
}
env {
    y:=y+1
}
```

Chapter 3

Gamma Activity Language

The Gamma Activity Language aims at providing a medium in which one can describe Activities like in SysML, but also be semantically consistent.

The aim of the language is to sit in the middle of the SysML and XSTS semantics – provide a *bridge* in between the two . To achieve that, first, it needs to be **semantically correct** – at least according to our *activity semantics* – to lift the burden of filtering out incorrect models. Secondly, it needs to be easily transformed to XSTS and from SysML.

The latter can be done by having a metamodel close to SysML, and the former by minimising the complexity of the language. Needless to say, this is not an easy thing to do, and requires an incremental design process.

3.1 Language Design

sysml és sysml2-höz képesti különbségek, a subset amit bevállalunk, és miért csak ezeket (do behaviour pontosítása, felesleges elemek kihagyása, stb)

3.2 Formal modelling

formal modeling howto, why needed, etc

semantic part, formal model, enforcing well formedness, etc

3.2.1 Root Structure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Activity Declaration Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Definition Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

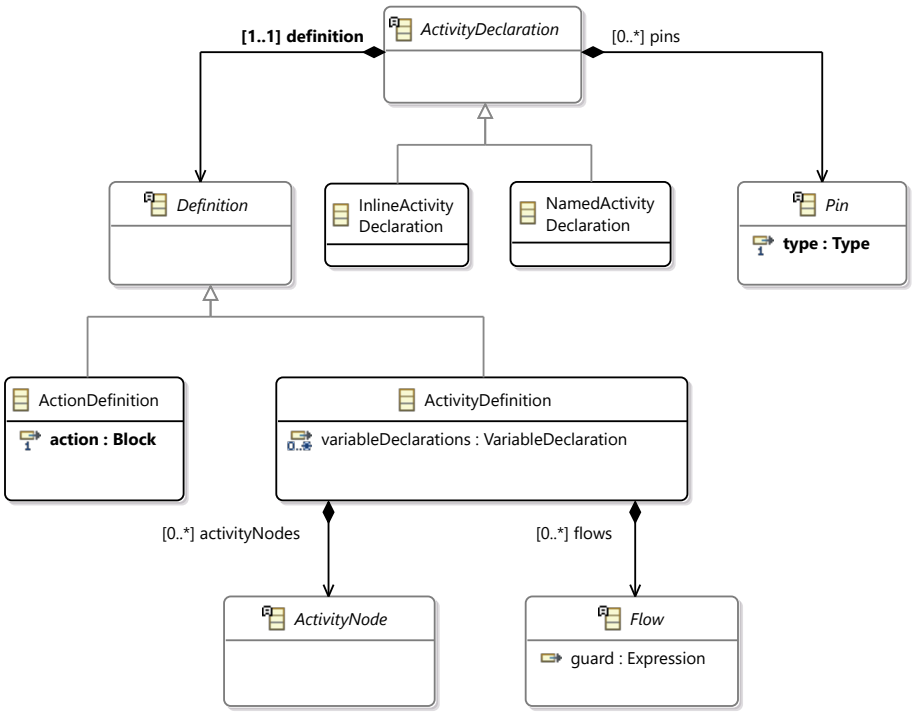

Figure 3.1: The root structure of the language

3.2.2 Activity Nodes

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Pseudo Activity Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Initial Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Final Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Data Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Fork Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Join Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Decision Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Merge Node Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

3.2.3 Composing Activities

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

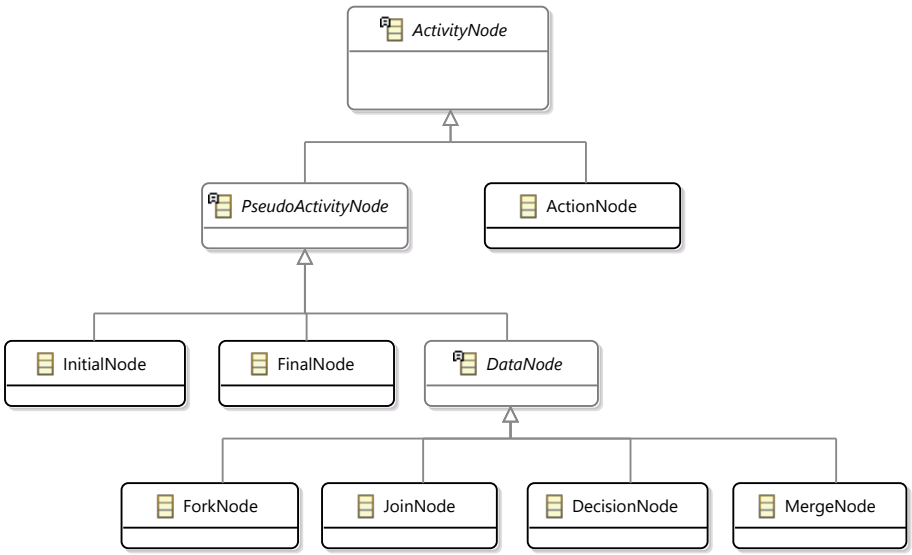

Figure 3.2: The Activity Node structure

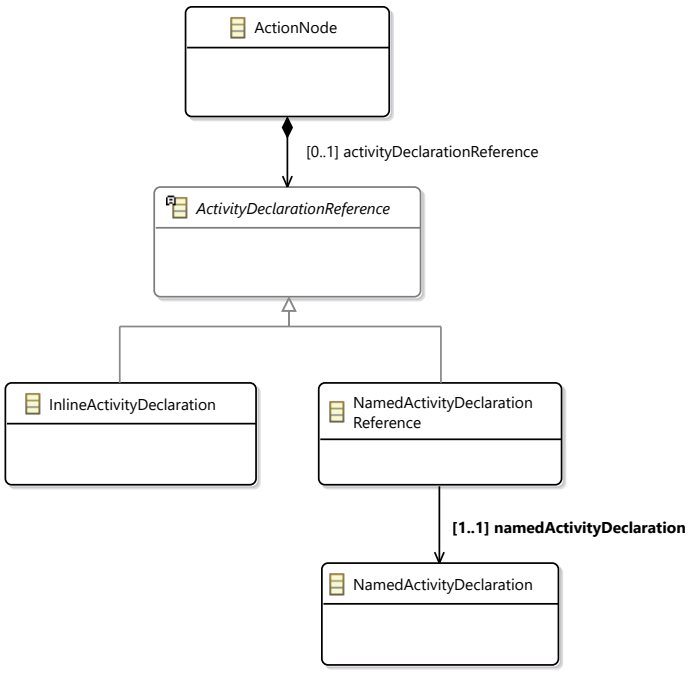

Figure 3.3: The

3.2.4 Flows

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Control Flow Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Data Flow Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

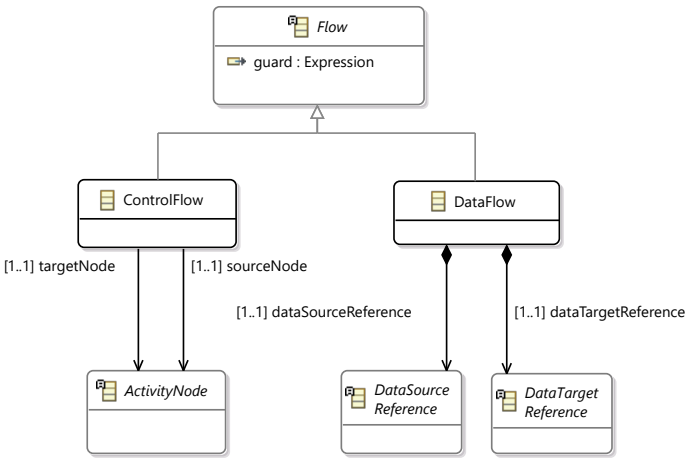

Figure 3.4: The Flows structure

3.2.5 Pins

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Input Pin Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

Output Pin Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

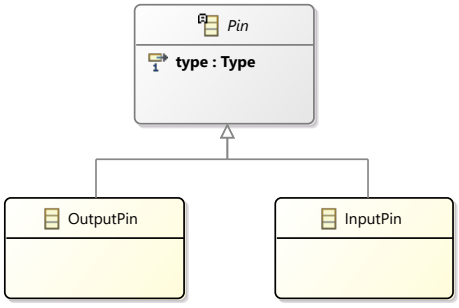

Figure 3.5: The Pins structure

3.2.6 Data Source-Target Reference

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

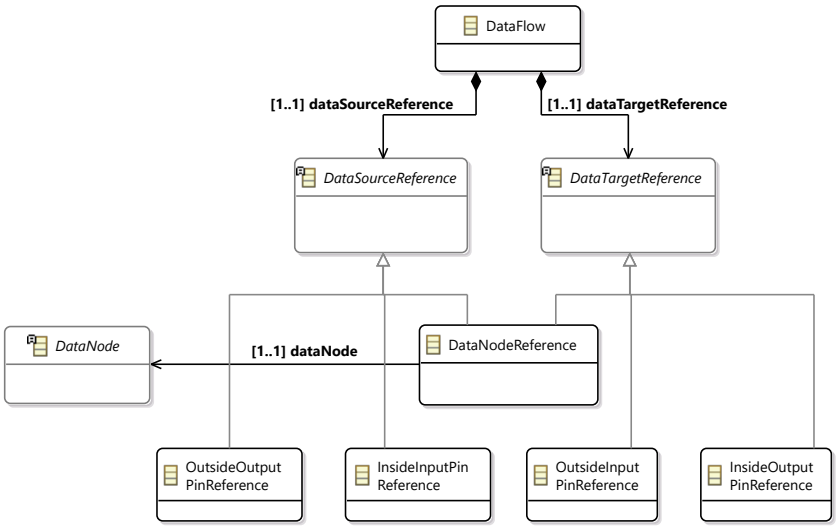

Figure 3.6: The Data node reference structure

3.2.7 Pin Reference

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vehicula turpis eget enim maximus, vel rutrum dui ullamcorper. Nulla enim ex, dapibus non aliquam vitae, molestie quis magna. Maecenas mattis turpis non ex feugiat, vitae pulvinar nisl vulputate.

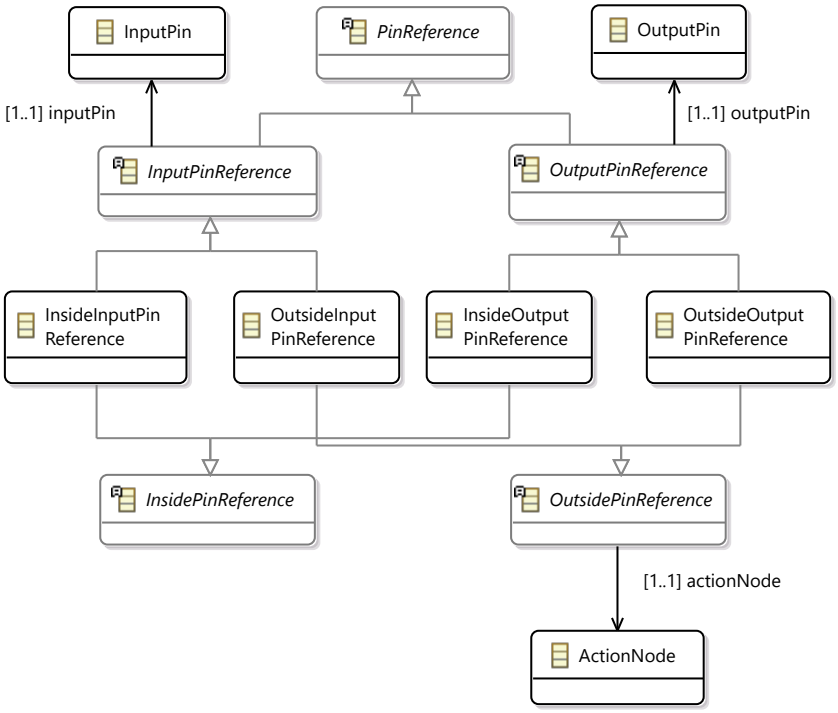

Figure 3.7: The Data node reference structure

3.3 Domain-specific Language

ide még jöhet később xtext kód

In order to make it easier to test both the XSTS and SysML transformations, I created an **Xtext** domain-specific language. Easy readability and writing was not one of the main priorities, because the end goal is to have a higher-level systems modelling language as a source. As a result, many many constructs are inherently repetitive to write.

3.3.1 Language elements

The following section gives high level introduction into the syntax of the Gamma Activity DSL.

Inherited from Gamma

Some of the used constructs were reused from the other languages of the Gamma framework in order to provide tighter integration.

Lehet ez is rossz helyen van.. Végülis visszamehet a background részre

Pins

Pins can be declared the following way, where `<direction>` can be either `in` or `out`, and `type` a valid Gamma Expression type.

```
<direction> <name> : <type>
```

For example:

```
in examplePin : integer
```

where the direction is `in`, the name is `examplePin` and the type is `integer`.

Nodes

Nodes can be declared by stating the `type` of the node and then it's name. The type determines the underlying meta element. See figure **??**

The available node types:

```
initial InitialNode
decision DecisionNode
merge MergeNode
fork ForkNode
join JoinNode
final FinalNode
action ActionNode
```

Flows

The behaviour of the Activity can be described by stating `data` or `control` flows between two nodes. Flows may have guards on them, which limits when the flow can fire. Activities may only be from the current activity definition's children. Pins can be accessed using the `.` accessor operator, the activity on the left hand side, and the pin's name on the right. The enclosing activity's name is `self`.

Flows can be declared the following way, where `<kind>` is the kind of flow, `<source>` and `<target>` is the source/target node or pin, and `<guard>` is a Gamma Expression returning boolean:

```
<kind> flow from <source> to <target> [<guard>]

control flow from activity1 to activity2
control flow from activity1 to activity2 [x == 10]
data flow from activity1.pin1 to activity2.pin2
data flow from self.pin to activity3.pin2
```

Declarations

Activity declarations state the *name* of the activity, as well as its *pins* 3.3.1.

```
activity Example (
  ..pins..
) {
  ..body..
}
```

You can also declare activities inline by using the `:` operator:

```
activity Example {
  action InlineActivityExample : activity
}
```

Definitions

Activities also have definitions, which give them bodies. The body language can be either `activity` or `action` depending on the language metadata set. Using the `action` language let's you use any Gamma Action expression, including timeout resetting, raising events through component ports, or simple arithmetic operations.

An example activity defined by an action body:

```
activity Example (
  in x : integer,
  out y : integer
) [language=action] {
  self.y := self.x * 2;
}
```

Inline activities may also have pins and be defined using action language:

```
activity Example {
  action InlineActivityExample : activity (
    in input : integer,
    out output : integer
  ) [language=action] {
    self.output := self.input;
  }
```

```
}
```

3.3.2 Integration into Gamma

3.4 Examples

3.4.1 Adder Example

The following is a basic example of an adder activity. It 'reads' two numbers, adds them, and then 'logs' the result.

diagram, opaque action

Ehelyett egyébként lehetne a running example, amit még az egész elején definiálunk

```
package hu.mit.bme.example

activity Adder(
  in x : integer,
  in y : integer,
  out o : integer
) [language=action]  {
  self.o := self.x + self.y;
}

activity Example {
  initial Initial

  action ReadSelf1 : activity (
    out x : integer
  )
  action ReadSelf2 : activity (
    out x : integer
  )
  action Add : Adder
  action Log : activity (
    in x : integer
  )

  final Final

  control flow from Initial to ReadSelf1
  control flow from Initial to ReadSelf2
  control flow from Initial to Add
  data flow from ReadSelf1.x to Add.x
  data flow from ReadSelf2.x to Add.y
  data flow from Add.o to Log.x
  control flow from Log to Final
}
```

Chapter 4

Activity Model Verification

4.1 Activities as State-based Models

activity vagy proces-model?

ahogy fentebb írtam, tokenek haladnak, és tranzíciók vannak.

A process-orionted model előnye itt a hátrányunk; mivel sok process mehet teljesen függetlenül egymástól, ezért nagyon nehéz szépen leírni őket

tegyük fel, hogy a node-ok és csatlakozók token-tartalma egy állapot; vagy van benne, vagy nincs. ehhez még hozzátesszük azt, hogy a node éppen fut, kész, vagy nem csinál semmit.

ezek alapján le tudunk írni bármilyen process-oriontált modelt állapot alapú modellben, feltételezve, hogy bármikor bármelyik tranzíció tüzelhet.

itt leírom az activity különböző node-jait, és azoknak a különböző szabályait (merge, choice, stb)

majd leírom a különböző csatlakozók segítségével is

4.2 Activities Alongside Statecharts

fentebb leírtam, hogyan lehet leképezni proces modelleket, de így csak magukban futhatnak. Itt most leírom, hogy milyen nehézségeket okozhat, amikor egymás mellett futtatjuk őket:

do activity:

amikor a state aktív, futhat az aktivity, de ez pár problémával jön: párhuzamossági és szinkornizációs problémák

action:

egy activity értékét ki kell lapítani, hogy a tranzíció tüzelése után azonnal értelmezhető legyen (nem felezhetjük el az adott tranzíciót, mert akkor érvénytelen állapotaink lesznek)

unblock:

még nagy kérdés, hogy milyen szinten bontsuk fel a lépéseket, mennyire legyenek atomikusak, mik futhatnak egymás mellett, stb

alap elképzelésben akár egy activity akár egy állapotgép definiálhat egy komponsens viselkedését, de jelenleg ezt is egyszerűsített módon implementáltuk; az activity az állapotgép része lehet

megoldás a kérdésekre:

megoldásként a legegyszerűbb módszert választottuk, mert első sorban az a kérdés, hogy ez a módszer egyáltalán alkalmazható-e; a másik mindenképpen bonyolítja az implementációt és a létrejövő modellt is

Chapter 5

Implementation

TODO: rövid leírása az implementációnak; kb milyen méretű a változtatás. nem szeretném hosszúra, annyira nem érdekes, viszont jó lenne valahogy mutatni, hogy nem volt azért triviális.

Chapter 6

Evaluation

Chapter 7

Conclusion

Acknowledgements

Ez nem kötelező, akár törölhető is. Ha a szerző szükségét érzi, itt lehet köszönetet nyilvánítani azoknak, akik hozzájárultak munkájukkal ahhoz, hogy a hallgató a szakdolgozatban vagy diplomamunkában leírt feladatokat sikeresen elvégezze. A konzulensnek való köszönetnyilvánítás sem kötelező, a konzulensnek hivatalosan is dolga, hogy a hallgatót konzultálja.

Bibliography

[1] Technical operations international council on systems engineering incose. incose systems engineering vision 2020. technical report. URL https://sebokwiki.org/wiki/INCOSE_Systems_Engineering_Vision_2020.

[2] Mbse wiki. URL https://www.omgwiki.org/MBSE/doku.php?id=start.

[3] David A. Larsen K. G. Håkansson J. Pettersson P. Yi W. Hendriks M. Behrmann, G. Uppaal 4.0. 2006.

[4] G Bellinger. Modeling & simulation: An introduction. 2004. URL http://www.systems-thinking.org/modsim/modsim.htm.

[5] DoD. Dod modeling and simulation (m&s) glossary. *DoD Manual 5000.59-M. Arlington, VA, USA: US Department of Defense*, 1998. URL https://apps.dtic.mil/sti/pdfs/ADA349800.pdf.

[6] D. Dori. Object-process methodology: A holistic system paradigm. *New York, NY, USA: Springer.*, 2002.

[7] A. Moore R. Steiner Friedenthal, S. and M. Kaufman. A practical guide to sysml: The systems modeling language, 3rd edition. *MK/OMG Press.,*, 2014.

[8] Object Management Group. Omg system modeling language. URL https://www.omg.org/spec/SysML/.

[9] Object Management Group. Mda foundation model. omg document number ormsc/2010-09-06. 2010.

[10] Object Management Group. Semantics of a foundational subset for executable uml models. 2018. URL https://www.omg.org/spec/FUML/1.4/.

[11] David Harel. Statecharts: a visual formalism for complex systems. *Science of Computer Programming*, 8(3):231–274, 1987. ISSN 0167-6423. DOI: https://doi.org/10.1016/0167-6423(87)90035-9. URL https://www.sciencedirect.com/science/article/pii/0167642387900359.

[12] Osman Hasan and Sofiène Tahar. Encyclopedia of information science and technology, third edition. pages 7162–7170., 2015. DOI: https://doi:10.4018/978-1-4666-5888-2.ch705.

[13] Edward Huang, Leon F. McGinnis, and Steven W. Mitchell. Verifying sysml activity diagrams using formal transformation to petri nets. *Systems Engineering*, 23(1):118–135, 2020. DOI: https://doi.org/10.1002/sys.21524. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sys.21524.

[14] Balcer MJ. Mellor SJ. Executable uml: A foundation for model- drivenarchitecture. *The Addison-Wesley Object TechnologySeries: Addison-Wesley Professional*, 2002.

[15] T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989. DOI: 10.1109/5.24143.

[16] Hajdu A. Vörös A. Micskei Z. Majzik I. Tóth, T. Theta: a framework for abstraction refinement-based model checking. *Stewart, D., Weissenbacher, G. (eds.), Proceedings of the 17th Conference on Formal Methods in Computer-Aided Design.*

Appendix

A.1 XSTS Language Constructs

A.2 Gamma Activity Language