UBFC
UNIVERSITÉ
BOURGOGNE FRANCHE-COMTÉ

UFC
UNIVERSITÉ
DE FRANCHE-COMTÉ

THÈSE DE DOCTORAT DE L'ÉTABLISSEMENT UNIVERSITÉ BOURGOGNE FRANCHE-COMTÉ

PRÉPARÉE À L'UNIVERSITÉ DE FRANCHE-COMTÉ

École doctorale n°37

Sciences Pour l'Ingénieur et Microtechniques

Doctorat d'Informatique

par

KARIM BOUDAOUD

Combinaison de l'exigence et de la propriété psl dans SysMl pour la vérification

Sous-titre

Thèse présentée et soutenue à Besançon, le 14 Mars 2018

Composition du Jury :

HULK INCROYABLE	Professeur à l'Université de Gotham City	Président

N° | X | X | X |

école doctorale **sciences pour l'ingénieur et microtechniques**

Titre : Combinaison de l'exigence et de la propriété psl dans SysMl pour la vérification

Mots-clés : Sysml, PSL , Vérification Formelle , Exigence Formelle

Résumé :

Notre approche consiste à avancer l'étape de vérification le plus tôt possible dans le cycle de développement des systèmes hétérogène. Notre but est de proposer une méthode pour étendre le diagramme des exigences dans SysMl avec des propriétés basées sur le langage PSL comme étant une logique expressive non ambiguë, Ces propriétés peuvent à la fois être utilisées pour la vérification statique ou dynamique. Nous avons choisi l'environnement de développement Papyrus sous (Eclipse) comme outil pour manipuler le langage SysMl afin de construire un profil qui nous permettra plus tard d'effectuer la traduction des propriétés puis leurs vérification. La traduction se fera grâce au plug-in Acceleo qu'on ajoute à Eclipse pour extraire les propriétés PSL depuis l'instance de notre modèle utilisant la notion de template.

Université Bourgogne Franche-Comté
32, avenue de l'Observatoire
25000 Besanon, France

REMERCIEMENTS

SOMMAIRE

I Contexte et Problématiques 1

1 Introduction 3

1.1 Contexte . . . 3
1.2 Objectifs de la thèse . . . 3
1.3 L'état de l'art . . . 3
1.4 Introduction général . . . 3

2 État de l'art 5

2.1 Langages de modélisation . . . 5
2.1.1 UML . . . 5
2.1.1.1 Diagrammes dynamiques et de comportement d'UML . . . 5
2.1.2 SYSML . . . 5
2.1.3 Automates . . . 5
2.1.4 Autres . . . 5
2.2 Ingénierie deriger par les modèles . . . 5
2.2.1 Défintions . . . 5
2.2.2 m2m . . . 5
2.2.3 m2t . . . 5
2.3 vérification et validation . . . 5
2.3.1 test et simulation . . . 5
2.3.2 méthodes formelles . . . 5
2.3.2.1 model cheking . . . 5
2.3.2.2 theorm proving . . . 5

3 vers une vérification formelle des modèles SYSML 7

4 Sysml2ta : 9

4.0.1 de Sysml vers UPPAAL . . . 9
4.0.2 Algorithmes développer . . . 9
4.0.3 Étude de cas . . . 9

5 Conclusion **11**

I

CONTEXTE ET PROBLÉMATIQUES

1

INTRODUCTION

1.1/ CONTEXTE

Ce sujet est situé dans un contexte de recherche et développement pour la modélisation et la vérification de systèmes hétérogènes (par exemple des systèmes répartis sur des plateformes diverses ou des logiciels embarqués sur divers matériels). La composition souple de divers composants est une voie pour modéliser et construire de tels systèmes. Cependant afin de les analyser et garantir leur correction vis à vis des exigences, il faut formaliser les propriétés locales ou globales et les vérifier.

1.2/ OBJECTIFS DE LA THÈSE

Les objectifs de cette thèses sont :

- Proposer un profile SysML permettant de mieux décrire les exigences afin de les intégrer dans le processus de vérification. Ce profile inclura essentiellement la description formelle des exigences.
- Exploiter les exigences étendues de ce profile pour vérifier localement chaque composant s'il satisfait bien ses propriétés (souvent comportementales). On peut se baser sur l'un des diagramme comportementaux de SysML (par exemple, diagramme de séquence ou état transition, etc.). Des outils de *model checking* peuvent être utilisés pour vérifier de telles propriétés.

1.3/ L'ÉTAT DE L'ART

1.4/ INTRODUCTION GÉNÉRAL

Les systèmes critiques temps réel deviennent de plus en plus complexes et exigent un niveau de sûreté et de fiabilité très élevé. Cela nécessite l'utilisation des méthodes de spécification et de vérification dans la phase de conception pendant le cycle de développement de ces systèmes afin de réduire la notion d'erreur avant même de commencer l'implémentation ce qui permet le développement d'un système fiable, de réduire les couts et de gagner du temps. La conception est une phase importante dans l'ingénierie des systèmes, elle détermine l'architecture du système sur plusieurs niveaux

pour la satisfaction des exigences prises en charge par un langage de modélisation (SysML), ce dernier est défini comme une extension de Métamodèle (UML). SysMl a ajouté un diagramme d'exigence parmi les nouveaux diagrammes par rapport a UML compte tenu de l'importance de l'exigence pour un système fiable. Ce diagramme permet d'exprimer les spécifications de façon semi-formelle. Pour cela notre but prioritaire au début est d'établir un ensemble de propriétés écrites comme assertions en utilisant (PSL) comme langage formel pour permettre le développement d'une propriété formelle (une Propriété PSL) qui doit être vérifiée par un modèle de vérification (Model checker).

2

ÉTAT DE L'ART

2.1/ LANGAGES DE MODÉLISATION

2.1.1/ UML

2.1.1.1/ DIAGRAMMES DYNAMIQUES ET DE COMPORTEMENT D'UML

2.1.2/ SYSML

2.1.3/ AUTOMATES

2.1.4/ AUTRES

2.2/ INGÉNIERIE DERIGER PAR LES MODÈLES

2.2.1/ DÉFINTIONS

2.2.2/ M2M

2.2.3/ M2T

2.3/ VÉRIFICATION ET VALIDATION

2.3.1/ TEST ET SIMULATION

2.3.2/ MÉTHODES FORMELLES

langage formelle .....

2.3.2.1/ MODEL CHEKING

2.3.2.2/ THEORM PROVING

3

VERS UNE VÉRIFICATION FORMELLE DES MODÈLES SYSML

4

SYSML2TA :

4.0.1/ DE SYSML VERS UPPAAL

4.0.2/ ALGORITHMES DÉVELOPPER

4.0.3/ ÉTUDE DE CAS

5

CONCLUSION

Document réalisé avec LaTeX et :
le style LaTeX pour Thèse de Doctorat créé par S. Galland — http://www.multiagent.fr/ThesisStyle
la collection de paquets `tex-upmethodology` — http://www.arakhne.org/tex-upmethodology/