

# VU Research Portal

## Bringing Model Checking Closer To Practical Software Engineering

Remenska, D.

2016

### **document version**

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

### **citation for published version (APA)**

Remenska, D. (2016). *Bringing Model Checking Closer To Practical Software Engineering*. [PhD-Thesis - Research and graduation internal, Vrije Universiteit Amsterdam].

### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

### **E-mail address:**

[vuresearchportal.ub@vu.nl](mailto:vuresearchportal.ub@vu.nl)

# Contents

Acknowledgements	iii
Contents	vii
List of Figures	xi
List of Tables	xiii
List of Abbreviations	xv
1 Introduction	1
1.1 Context and Research Objectives	3
1.2 Main Contributions	5
1.3 Dissertation outline	6
2 DIRAC: A Community Grid Solution	9
2.1 Introduction	9
2.2 Workload Management System	13
2.3 Storage Management System	16
3 Formal Modeling and Analysis of Distributed Systems	19
3.1 Introduction	19
3.2 Labeled Transition Systems	19
3.3 The mCRL2 Formalism	22
3.4 From DIRAC to mCRL2	25
3.4.1 Control-Flow Abstractions	27
3.4.2 Data Abstractions	29
3.5 Analysis and Issues	32
3.5.1 Simulation and debugging	33

3.5.2	Visualization	34
3.5.3	Model checking	36
3.6	Discussion and Evaluation of the Approach	41
3.7	Related Work	43
3.8	Conclusions	45
4	Model-Transformation Methodology	47
4.1	Introduction	47
4.2	Modeling Interactions in UML	50
4.2.1	Sequence Diagrams	50
4.2.2	Activity Diagrams	54
4.3	Transformation Methodology	55
4.3.1	The Object-Process Problem	55
4.3.2	Design Choices in the Semantics of Sequence Diagrams	57
4.3.3	Mapping UML to mCRL2	59
4.4	Case Study: DIRAC's Executor Framework	68
4.5	Discussion and Evaluation of the Approach	71
4.6	Conclusions	72
5	Assisting Non-Experts in Property Specification	73
5.1	Introduction	73
5.2	Background: Property Specification Patterns	75
5.3	Related Work	77
5.4	PASS: An Implementation and Extension of PSP	80
5.4.1	$\mu$ -calculus and the PSP system	80
5.4.2	Pattern Extensions for $\mu$ -calculus	84
5.4.3	Sequence Diagrams for Visual Property Specification	88
5.4.4	Transforming a $\mu$ -calculus Formula Into a Monitor Process	89
5.4.5	A Walk-Through Example	92
5.4.6	PASS Integration in the Eclipse Platform	93
5.5	PASS by Example: Revisiting DIRAC	94
5.5.1	PASS: The Property ASSistant	95
5.5.2	PASSWebStart: The Alternative	99
5.5.3	The DIRAC ProcessPool	100
5.6	Property Specifications with $\mu$ -calculus: A Survey of Published Works	104
5.6.1	Is the PSP Classification Useful?	104
5.6.2	Is Manual Formalization of Properties Error-Prone?	106
5.7	Conclusions	113

6	Conclusions	115
6.1	Thesis summary . . . . .	116
6.2	Limitations and Future Directions . . . . .	118
	Samenvatting	121
A	Appendix	125
A.1	Definitions . . . . .	125
A.2	Proof of the Monitor Construction Correctness . . . . .	131
	References	139