

Systems Thinking and Systems Engineering

Volume 2

# A Discipline of Mathematical Systems Modelling

Volume 1  
A Journey Through the Systems Landscape  
Harold "Bud" Lawson

Volume 2  
A Discipline of Mathematical Systems Modelling  
Matthew Collinson, Brian Monahan, and David Pym

Systems Thinking and Systems Engineering Series Editors  
Harold "Bud" Lawson  
Jon P. Wade

[bud@lawson.se](mailto:bud@lawson.se)  
[jon.wade@stevens.edu](mailto:jon.wade@stevens.edu)

# A Discipline of Mathematical Systems Modelling

Matthew Collinson,  
Brian Monahan,  
and  
David Pym

© Hewlett-Packard Development Company, L.P. and College Publications, 2012. All rights reserved.

ISBN 978-1-904987-50-5

College Publications

Scientific Director: Dov Gabbay

Managing Director: Jane Spurr

Department of Computer Science

King's College London, Strand, London WC2R 2LS, UK

<http://www.collegepublications.co.uk>

Printed by Printondemand-worldwide, UK

---

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording or otherwise without prior permission, in writing, from the publisher.

# Preface

The mathematization of the sciences, of engineering, and of economics has been an outstandingly successful intellectual enterprise, enabling the modern world. As the operations of the world become more and more dependent on highly interconnected, massively complex, networked systems of computational devices, the need to develop a mathematical understanding of their properties and behaviours is increasingly pressing.

Our approach, described in this monograph, is to combine the compositionality of formal specification — using techniques from algebra, computation theory, logic, and probability theory — with the control of level of abstraction afforded by the classical mathematical modelling method.

The first chapter provides a complete high-level view of the approach to systems modelling that is developed in the monograph. It provides both conceptual and philosophical background and introductions to the technical development. The remaining chapters develop the mathematical and computational aspects of our approach. Each chapter develops a specific mathematical or computational component, clearly integrated into the overall development. Examples, including ones based on industrial and commercial applications, are provided throughout. An implementation of a simulation engine (Core Gnosis) for executing models is available for download from HP Labs: see the College Publications website, [www.collegepublications.co.uk](http://www.collegepublications.co.uk), for more information.

This book is about the conceptual and mathematical foundations of a modelling approach, with indications of how it can, and has been, deployed in practice. We defer to another occasion an account of the pragmatics of the deployment.

Dr. Matthew Collinson is a Lecturer in Computing Science, University of Aberdeen.

Dr. Brian Monahan is a researcher in the Cloud and Security Lab, HP Labs, Bristol.

Prof. David Pym is 6th Century Chair in Logic, and SICSA Professor of Computing Science, University of Aberdeen.

# Contents

<b>1</b>	<b>Mathematical Systems Modelling</b>	<b>1</b>
1.1	Introduction . . . . .	2
1.1.1	Some Issues for Mathematical Modelling . . . . .	3
1.1.2	A Guide to the Remaining Sections . . . . .	5
1.2	Modelling Systems . . . . .	5
1.3	A Semantic Basis . . . . .	10
1.3.1	Processes . . . . .	11
1.3.2	Resources . . . . .	12
1.3.3	Processes and Resources . . . . .	14
1.3.4	Location . . . . .	15
1.3.5	Environment . . . . .	19
1.4	Exploring Models: Introducing Core Gnosis . . . . .	20
1.4.1	Introducing Core Gnosis . . . . .	20
1.4.2	Adding Located Resource: Secure Boats . . . . .	23
1.5	Discrete Process Simulation . . . . .	29
1.5.1	Experimental Methodology . . . . .	31
1.5.2	Comparing Modelling Approaches . . . . .	32
1.6	Reasoning about Models . . . . .	32
1.6.1	Possible Worlds Semantics, Resource Semantics, and Bunched Logic . . . . .	32
1.6.2	Process Logic . . . . .	34
1.6.3	Adding Location . . . . .	36
1.6.4	Model Checking . . . . .	37
1.6.5	A Note on Information . . . . .	38
1.7	The Economic Context of Systems Models . . . . .	38
1.7.1	Systems Security Economics . . . . .	39
1.8	Discussion: Systems Models, Utility, and Security . . . . .	40
1.8.1	Systems Models and Utility . . . . .	40
1.8.2	Integrating System Models and Economic Models . . . . .	42
1.9	Validation in an Industrial Context . . . . .	43
1.10	Obtaining Core Gnosis . . . . .	45
1.11	Obtaining the Model-checker . . . . .	45

<b>2</b>	<b>A Calculus of Resources and Processes</b>	<b>47</b>
2.1	Introduction . . . . .	48
2.2	The Process Calculus . . . . .	48
2.3	Examples . . . . .	53
2.3.1	Mutual Exclusion . . . . .	53
2.3.2	Resource Transfer with Exclusion . . . . .	54
2.3.3	Handshaking . . . . .	56
2.3.4	Privacy . . . . .	57
2.3.5	Asynchronous Resource Transfer without Exclusion . . . . .	57
2.4	Structural Properties . . . . .	58
2.5	Bisimulation . . . . .	59
2.6	Specifying Modifications . . . . .	65
2.7	Conclusion . . . . .	67
<b>3</b>	<b>A Modal Logic of Resources and Processes</b>	<b>69</b>
3.1	Introduction . . . . .	70
3.2	Bunched Implications . . . . .	71
3.3	A Modal Logic . . . . .	74
3.4	Semantics . . . . .	77
3.5	Essential Metatheory . . . . .	79
3.6	Characterization of the Logical Equivalence . . . . .	81
3.7	Quantification . . . . .	83
3.8	Examples . . . . .	86
3.8.1	Mutual Exclusion . . . . .	86
3.8.2	Resource Transfer . . . . .	86
3.8.3	Handshaking . . . . .	87
3.8.4	Privacy . . . . .	88
3.8.5	Asynchronous Resource Transfer without Exclusion . . . . .	88
3.9	An Application to Computer Security . . . . .	89
3.9.1	Introduction . . . . .	89
3.9.2	Extending the Calculus and the Logic . . . . .	91
3.9.3	Summarizing the Metatheory . . . . .	92
3.9.4	Examples . . . . .	93
3.10	Conclusion . . . . .	105
<b>4</b>	<b>The (Stochastic) Environment</b>	<b>107</b>
4.1	Introduction . . . . .	108
4.2	The Stochastic Method . . . . .	108
4.2.1	Process Dynamics and Statistics . . . . .	109
4.2.2	Stochastic Models Expressed Using Core Gnosis . . . . .	109
4.3	Use of Distributions in Core Gnosis . . . . .	110
4.3.1	Sampling a Variable . . . . .	110
4.3.2	Timing Distributions . . . . .	111
4.4	Available Distributions . . . . .	111
4.4.1	The Discrete Uniform Distribution . . . . .	112
4.4.2	Point Distribution . . . . .	112
4.4.3	The Bernoulli Distribution . . . . .	112

4.4.4	The Binomial Distribution . . . . .	112
4.4.5	The Poisson Distribution . . . . .	113
4.4.6	The Continuous Uniform Distribution . . . . .	114
4.4.7	The Negative Exponential Distribution . . . . .	114
4.4.8	The Normal (or Gaussian) Distribution . . . . .	116
4.4.9	The Weibull Distribution . . . . .	117
4.5	Sampling and Random Number Generation . . . . .	118
4.6	Persistent and Transient Effects . . . . .	119
4.7	Analysis and Interpretation of Results . . . . .	122
4.8	Conclusion . . . . .	124
<b>5</b>	<b>Adding Location to the Calculus</b>	<b>125</b>
5.1	Introduction . . . . .	126
5.2	A General Theory of Location, Resource and Process . . . . .	126
5.2.1	The Supporting Structures . . . . .	127
5.2.2	The Process Calculus . . . . .	131
5.2.3	Simulation . . . . .	133
5.3	Properties of the General Theory . . . . .	134
5.3.1	Transition Properties . . . . .	134
5.3.2	Simulation Results . . . . .	134
5.4	The Basic Location Model and the Special Theory . . . . .	135
5.5	Examples of Located Resources . . . . .	138
5.6	Secure Boats: A Paradigmatic Example . . . . .	139
5.7	Conjectured Security Examples with Location . . . . .	144
5.8	Conclusion . . . . .	145
<b>6</b>	<b>Adding Location to the Logic</b>	<b>147</b>
6.1	Introduction . . . . .	148
6.2	A Logical Language . . . . .	148
6.3	Semantics: Interpretation in <b>OLSCR</b> P . . . . .	149
6.4	Metatheory . . . . .	151
6.5	Examples . . . . .	151
6.6	Access Control Revisited . . . . .	154
6.7	Conclusion . . . . .	156
<b>7</b>	<b>Core Gnosis and Its Semantics</b>	<b>157</b>
7.1	Introduction . . . . .	158
7.2	Core Gnosis . . . . .	160
7.2.1	The Core Gnosis Tool . . . . .	160
7.2.2	Basic Features of Core Gnosis Models . . . . .	160
7.2.3	More Boats World — in Core Gnosis . . . . .	171
7.2.4	Comparison of Boats World models in <b>LSCR</b> P and Core Gnosis . . . . .	177
7.2.5	Implementation of Core Gnosis . . . . .	178
7.3	The Operational Semantics of Core Gnosis . . . . .	179
7.3.1	Methodological Remarks . . . . .	179
7.3.2	Notation . . . . .	179
7.3.3	Names, Times, and Building Blocks . . . . .	180



7.3.4	Environments and Expressions . . . . .	181
7.3.5	Processes and Entities . . . . .	184
7.3.6	The Scheduling Queues . . . . .	185
7.3.7	Model States . . . . .	187
7.3.8	Environmental Definitions . . . . .	188
7.3.9	Temporal Change . . . . .	189
7.3.10	Location Operations . . . . .	189
7.3.11	Resource Operations . . . . .	190
7.3.12	Compound Control Statements . . . . .	193
7.3.13	Output . . . . .	197
7.3.14	Birth and Death . . . . .	197
7.3.15	The Initial Schedule, the Main Process, and the Close . . . . .	198
7.4	Interpreting Core Gnosis Processes in <b>LSCR</b> P . . . . .	199
7.4.1	Motivation and Approach . . . . .	199
7.4.2	Restricted Core Gnosis Models . . . . .	201
7.4.3	The Interpretation . . . . .	203
7.4.4	Example of the <b>LSCR</b> P-interpretation . . . . .	205
7.4.5	Evaluation of Methodology . . . . .	207
7.5	Conclusion . . . . .	208
7.6	Obtaining Core Gnosis . . . . .	209
<b>8</b>	<b>Model Checking the Modal Logic</b>	<b>211</b>
8.1	Introduction . . . . .	212
8.2	Automated Evolution and Analysis . . . . .	212
8.3	A Recursive <b>LSCR</b> P . . . . .	214
8.4	The Interpreter . . . . .	223
8.5	The Checker . . . . .	227
8.5.1	The General Set-up . . . . .	227
8.5.2	Implementation of the Logical Language . . . . .	229
8.5.3	Environments and Valuations . . . . .	230
8.5.4	Checking Formulae . . . . .	232
8.6	Reasoning about Simulations . . . . .	235
8.7	Translating and Reasoning about Models . . . . .	237
8.8	Conclusion . . . . .	241
8.9	Obtaining the Model Checker . . . . .	241
<b>A</b>	<b>Core Gnosis: Formal Syntax and Other Details</b>	<b>255</b>
A.1	Grammar . . . . .	256
A.2	Lexeme Classes (Regular Expressions) . . . . .	264
A.3	Output Files . . . . .	264
A.4	Random Variates . . . . .	264
A.5	Trace Statement . . . . .	265
A.6	Dump Statement . . . . .	266
A.7	Outputs Statement . . . . .	266
A.8	Pragma Statements . . . . .	266
A.9	Line and Block Comments . . . . .	268
A.10	Reserved Words . . . . .	268

*CONTENTS*

xv

A.11 Symbols . . . . .	269
A.12 Core Gnosis Software License Terms . . . . .	270