Modelling and Formal Verification in Action

The INGEQUIP Project Team

INGEQUIP
The INGEQUIP Project

Modelling and Formal Verification in Action

INGEQUIP project team

Eric Jenn ed.

2017
Ref. LIV-S009-Book-235-V0

Editor: Eric Jenn, IRT Saint Exupéry, seconded from Thales Avionics

Main contributors
- Philippe Cuenot, IRT Saint Exupéry, seconded from Continental
- Arnaud Dieumegard, IRT Saint Exupéry
- Pierre Gauffilet, IRT Saint Exupéry, seconded from Airbus
- Ning Ge, IRT Saint Exupéry, seconded from Systerel
- Eric Jenn, IRT Saint Exupéry, seconded from Thales Avionics
- Emilie Rouland, IRT Saint Exupéry, seconded from Actia
- Faiez Zaliia, IRT Saint Exupéry

Other contributors
- Yamine Aït Ameur, IRIT
- Bruno d’Ausbourg, ONERA
- Bernard Berthomieu, LAAS-CNRS
- Mark Burton, GreenSocs
- Guy Bois, SpaceCoDesign
- Pierre-Alain Bourdil, IRT Saint Exupéry
- Nicolas Broueilh, ASTC Design Partners
- Silvano Dal Zilio, LAAS-CNRS
- Pierre Disssaux, Elidiss-Technologies
- Patrick Farail, IRT Saint Exupéry, seconded from Airbus
- Clément Foucher, LAAS-CNRS
- Eric Faure, IRT ASTC Design Partners
- Hubert Guérard, SpaceCoDesign
- Jérôme Hugues, ISAE-SUPAERO
- Frédéric Konrad, IRT Saint Exupéry, seconded from Greensocs
- Jérôme Lachaize, IRT Saint Exupéry, seconded from Airbus Defence and Space
- Didier Le Botlan, LAAS-CNRS
- Vincent Lecrubier, ONERA
Fellipe Monteiro, IRT Saint Exupéry, seconded from Space-CoDesign
Alexandre Nketsa, LAAS CNRS
Bassem Ouni, IRT Saint Exupéry
Marc Pantel, IRIT
Fadhel Sassi, IRT Saint Exupéry
François Vernadat, LAAS-CNRS

We also thank the many trainees that have spent some time with us at IRT. In particular: Paul Boniol, Kevin Duplantier, Saul Pavon Berceril, Guillaume Ripoll, Jorge Enrique Gutierrez Zuluaga, and all the students from ENSEEIHT and ISAE.

Many thanks to Marie-Pierre (H) Le Tallec for her support during the final edition and printing process.

The work presented in this book has been obtained in the frame of the INGEQUIP project conducted at the French Institute of Technology IRT Saint Exupéry. We wish to acknowledge the industrial and academic members of IRT Saint Exupery who brought their support to this project both in terms of financial backing and know-how: Acxia, Airbus, Airbus Defence and Space, ASTC Design Partners, Continental, Ellidiss, GreenSocs, IRIT, ISAE, LAAS-CNRS, ONERA, SAFRAN Electronics and Defense, Systerel, and Thales Avionics.

We would like also to thank the French Commissariat Général à l’Investissements (CGI) and the Agence Nationale de la Recherche (ANR) for their financial support in the frame of the Programme d'Investissement d'Avenir (PIA).

This document and the information it contains is the property of IRT Saint Exupéry. It may not be used, reproduced or transmitted to a third party without prior written approval.
A few words from the INGEQUIP project facilitator

This project was very special for me, for the IRT Saint Exupéry and for its members: it was the first project which has been reached within this new organisation. It looks like collaborative projects such as ANR or FUI ones, but partners don’t work exactly on the same way: the work has been done in a common house hosted by the IRT Saint Exupéry in Toulouse, all people work together under the banner of the IRT Saint Exupéry some come from industries, from research laboratories and other with an IRT contract.

I honestly think that some benefits of IRT way of life was met during the project. All partners have to gain to work together and to merge skills and budgets. This a real motivation to attempt this gain and to facilitate technologies transfer from research to industries but also from technology providers to industries. Foster employment and skill of people are also a major goal we have to follow.

We didn’t deliver these results without high level and motivated people so I would like to thanks a lot all the team here, each one brings something valuable to our common study: people from industries with very wide experiences, technologies providers with strong professional support, academics with high scientific level, newcomers with promising intellectual and works capacity.

I would like also thanks our industrial members who follow our work during all these months, the French government for its financial support and all the IRT Saint Exupéry management staff and transversal services for their unconditional support and their valuable assistance.

Special and sincere thanks for their motivation and their investment in the group to Emilie, Ning, Eric, Arnaud, Bassem, Faïez, Pierre-Alain, Pierre, Jérôme, Philippe and Fadhel. It was not only a technical adventure but also an actual human experience. I hope this project was benefits for your professional and your personal life.

Long life to the IRT Saint Exupéry and its way of life

Patrick Farail Head of INGEQUIP project
# TABLE OF CONTENTS

**PART 1**  THE INGEQUIP PROJECT .......................................................... 1  
**INTRODUCTION** .................................................................................. 2  
  1  PROJECT OVERVIEW ........................................................................... 3  
    1.1  OBJECTIVES AND EXPECTED RESULTS .................................. 3  
    1.2  THE ORGANISATION .............................................................. 7  
    1.3  THE WORK PACKAGES .......................................................... 8  
  2  THE GENERAL ORGANISATION OF THIS BOOK ............................... 9  
**PART 2**  THE TWIRTEE SYSTEM .......................................................... 11  
**INTRODUCTION** ................................................................................ 12  
  1  THE MISSION AND THE SYSTEM .................................................. 15  
    1.1  THE MISSION ............................................................................ 15  
    1.2  THE GLOBAL SYSTEM .......................................................... 16  
    1.3  THE ROBOT ............................................................................. 18  
    1.4  THE SUPERVISION STATION .................................................. 23  
  2  ARCHITECTURAL OVERVIEW ......................................................... 26  
  3  A CLOSER LOOK AT SOME COMPONENTS .................................... 50  
    3.1  THE ROBOT WARNING SYSTEM (RWS) .................................. 50  
    3.2  THE IMAGE-BASED POSITION MONITORING (IBPM) ............ 54  
**PART 3**  MODELLING AND VIRTUAL PROTOTYPING ......................... 61  
**INTRODUCTION** ................................................................................ 62  
  1  MODELLING .................................................................................... 67  
    1.1  PROCESS OVERVIEW ............................................................ 67  

v
1.2 SYSTEM MODELLING WITH CAPELLA.............................................. 70
1.3 HARDWARE AND SOFTWARE MODELLING ................................. 92
1.4 MODEL TRANSFORMATIONS ..................................................... 102
1.5 EARLY VALIDATION USING ARCHITECTURAL MODELS............... 126
1.6 DESIGN SPACE EXPLORATION: THE IMAGE BASED MONITORING CASE 155
1.7 LANGUAGES AND TOOLS .......................................................... 171

2 VIRTUAL PROTOTYPING..................................................................... 183
  2.1 OVERVIEW .................................................................................. 183
  2.2 A CLOSER LOOK AT A VIRTUAL PLATFORM ................................. 184
  2.3 THE TRAMPOLINE CASE............................................................ 191
  2.4 THE MOTOR CONTROL CASE.................................................... 198
  2.5 THE MOTOR POWER SUPPLY CASE ......................................... 210
  2.6 THE CLOCK SYNCHRONIZATION CASE ..................................... 219
  2.7 THE REMOTE GUIDANCE CASE ............................................... 227
  2.8 THE SIMULATION PLATFORM .................................................. 233
  2.9 LANGUAGES AND TOOLS .......................................................... 240

3 TOOL EXTENSIONS: MULTITHREADING QBOX ............................ 249
  3.1 OBJECTIVES AND RATIONALES ................................................ 249
  3.2 DESCRIPTION OF WORK.............................................................. 250

PART 4 FORMAL VERIFICATION .............................................................. 259

INTRODUCTION .................................................................................... 260

1 FORMAL METHODS IN ACTION ....................................................... 262
  1.1 FORMAL VERIFICATION OF MAP CONFIGURATION DATA .......... 264
  1.2 FORMAL DEVELOPMENT OF THE AUTOMATIC ROBOT PROTECTION FUNCTION ............................................................................................................ 272
  1.3 CODE GENERATION FOR THE AUTOMATIC ROBOT PROTECTION .......... 292
  1.4 FORMAL VERIFICATION OF THE SYNCHRONOUS AUTOMATIC ROBOT PROTECTION ............................................................................................................. 306
  1.5 FORMAL VERIFICATION OF THE SYNCHRONOUS REDUNDANCY MANAGEMENT ..................................................................................................................... 325
1.6  FORMAL VERIFICATION OF THE AVOIDANCE MANOEUVRE .......... 335
1.7  FORMAL VERIFICATION OF THE CLOCK SYNCHRONIZATION FUNCTION 344
1.8  FORMAL DEVELOPMENT OF HMIs: THE ROBOT WARNING SYSTEM ... 362
1.9  OTHER TOPICS .......................................................... 390

2  INTEGRATION OF FORMAL METHODS IN INDUSTRIAL DEVELOPMENT PROCESSES ......................................................... 406
  2.1  SAFETY AND CONFIDENCE ARGUMENT .................................. 407
  2.2  INTEGRATION OF VERIFICATION TOOLS USING ETB ................. 421

3  LANGUAGES AND TOOLS ..................................................... 433
  3.1  LANGUAGES ........................................................................ 433
  3.2  TOOLS ................................................................................. 440

4  TOOL EXTENSIONS ................................................................. 446
  4.1  S3 FLOATING POINT EXTENSION ............................................. 446
  4.2  THE LIDL TO LUSTRE TRANSLATOR ................................... 451
  4.3  THE FIACRE IDE AND SIMULATOR ....................................... 457

PART 5  CONCLUSIONS, AND FUTURE WORKS .......................... 477
  1  ABOUT MODELLING AND VIRTUAL PROTOTYPING ................. 478
  2  ABOUT FORMAL VERIFICATION ............................................. 482
  3  SOME FINAL CONCLUDING WORDS ...................................... 489

APPENDIX A  EVENT-B MODEL OF THE TRAFFIC LIGHT CONTROL 515
APPENDIX B  EVENT-B TO HLL TRANSLATION RULES .................. 519
APPENDIX C  THE CLOCK SYNCHRONIZATION PROTOCOL ............. 523
Part 1
The INGEQUIP project

Eric Jenn

“All of that, I repeat is true – but four hundred ten pages of unvarying M C V's cannot belong to any language, however dialectical or primitive it may be. Some have suggested that each letter influences the next, and that the value of MCV on page 71, line 3, is not the value of the same series on another line of another page [...]”

Jorge Luis Borges, The Babel Library

In this first part, we briefly present the main technical objectives and the organisation of the INGEQUIP project.
Introduction

From September 2014 to December 2016, the INGEQUIP project was conducted at the Institut de Recherche Technologique Saint Exupéry in Toulouse thanks to the contribution of six industrial companies, five technology providers, and four academic institutions. The common objective was to propose and exploit innovative technologies for the design, the verification, and the validation of aeronautical, automotive, and space equipments.

During this period, a team composed of engineers, post-doctoral researchers, and trainees, selected, analysed, experimented, and evaluated various virtual prototyping environments, modelling formalisms, and formal verification methods and tools.

This book presents some of the results of this work. It gives an overview of the methods and tools studied during the project. It shows how they have been applied on small – but representative – examples, and illustrates how they could be implemented on actual industrial projects.

This book is aimed at contributing to the diffusion of those methods and tools to a wider audience, especially in the industrial domain.
1 Project overview

1.1 Objectives and expected results

Context and objectives

If complying with all functional and non-functional requirements is the prime objective of the development of any automotive, aircraft, or a satellite equipment¹, the designer is also facing several “transverse” challenges:

- Manage the functional and the architectural complexity of the equipment
- Reduce the time-to-market
- Reduce the non-recurrent and recurrent costs of the equipment
- Comply with the regulation constraints.

Faced to these challenges, the engineer can rely on a plethoric set of methods and tools to model, analyse, simulate, and implement a design.

Unfortunately, a set of methods and tools does not necessarily make a viable – i.e., usable and useful – industrial process. To make it viable, those methods and tools must comply with some very general constraints:

- They must interoperate with each other and with the legacy elements of the toolchain
- They must scale up
- They must be accepted by the user.

INGEQUIP addresses those challenges and constraints in the restricted field of hardware and software co-design and formal verification.

¹ By equipment, we mean a software application hosted on some hardware platform such as a Line Replaceable Module (LRM) or a Line Replaceable Unit (LRU) in the aeronautic domain, an Electronic Control Unit (ECU) in the automotive domain, or an “Electronic Unit” in the spatial domain.
Modelling: objectives and expected results

Modelling is the core of most engineering activity.

Simulation models, provide the capability to execute, evaluate, and then optimize a design. Formal verification models provide the capability to demonstrate (in the mathematical sense) the satisfaction of some property on a design.

In INGEQUIP, activities concerning modelling have been focused on two complementary aspects:

- The development of models to support the creation of virtual prototypes and the realisation of formal verification activities (see below)
- The development of model transformations to ensure a continuous and automated development process.

This book presents some of the results of the modelling activities performed on the project demonstrator, at system-level using the Capella modelling notation and tool, and at SW/HW levels using AADL (see §1.2 and §1.3, Part 3). The demonstrator, a small wheeled robot, is presented in details in Part 2.

Model transformations from Capella to AADL, and from AADL to the input language of the virtual platforms are covered in Part 3, §1.4.

Virtual prototyping: objectives and expected results

Virtual prototyping is an approach in which part of system under design (a core, a System-On-Chip, a board with its application software, or a complete system) is replaced by a composition of simulated and non-simulated parts in order to support or facilitate some verification and validation activities. In the context of INGEQUIP, focus is placed on the so-called “virtual platforms”.

A virtual platform is a simulator of a hardware execution platform. It is usually built on top of an Instruction Set Simulator (ISS) of a processor that is implemented in SystemC or in any other general purpose language. Simulated components are modelled at abstraction levels that de-
pend on the targeted precision and accuracy, and on the acceptable sim-
ulation times. Some models may be very fast but very abstract with re-
spect to time (e.g., Qemu models2) or may be much slower but more ac-
curate (e.g., so-called “cycle-accurate” models derived from low-level
hardware description models such as Freescale’s ADL and uADL [1], [2]).

Several COTS3 tools, commercial or open source provide the capability to
build and execute such virtual prototypes. Among them, ASTC’s VLAB,
GreenSocs’ QBox, and Space Codesign’s Space Studio have been selected
to form the core of INGEQUIP’s co-
design toolset. Those tools being pretty mature from a technical viewpoint, the project has been essen-
tially focused on (i) the evaluation of those technologies on typical use
cases, and (ii) their integration in a Model-Based Engineering process.
These aspects are addressed in Part 3 of this book.

Formal verification: objectives and expected results

Formal verification is a generic term covering a very large and heteroge-
neous set of verification methods that have in common several funda-
mental characteristics:

- They all use notations that have “precise, unambiguous, mathemat-
ically defined syntax and semantics” [3, Sec. FM.6.2.1]
- They are based on some sound reasoning procedure ensuring that it
  “never asserts that a property is true when it may not be true” [3, Sec. FM.6.2.1]

These methods rely on a strong mathematical background which may be
more or less “hidden” to the end-user. Some techniques, such as abstract
interpretation, hide most of the mathematical complexity to the end-us-
ers, while some other requires a certain level of understanding and inter-
action between the tool and the user. Nevertheless, all the techniques
rely on some kind of formal specification of the expected properties and/or some formal description of the system to be verified.

---

2 See www.qemu-project.org.
3 Components Off-The-Shelf.
Once the properties and the system are described formally, the verification process may be more or less automated. In INGEQUIP, focus has been placed on *model-checking*, for the verification of behavioural (including temporal) properties, implementation correctness, and on *formal proof* for the formal verification of the correct refinement of models. In both cases, we have privileged highly automated verification techniques relying on efficient model checking techniques or proof engines. Even though several successful applications of formal verification methods have been reported, their usage in industrial projects is still somewhat confidential, and focused on specific properties, type of software applications, etc. In INGEQUIP, no major breakthrough was expected on the methods themselves, but rather on their usage in actual setups. Technically, the objective was not to extend the verification capabilities of the techniques, but rather to (i) evaluate the capability of the selected formal verification techniques to verify some non-trivial design examples, (ii) evaluate the capability of the engineers to apply those methods on the same examples, and (iii) to improve the usability of those tools, by providing guidance or appropriate tool extensions. Results of formal verification activities are covered in depth in Part 4 of the current book.

Besides improving the usability or the capability of the formal verification methods and tools, another important question is the confidence into the process that combines these methods. Indeed, formal verification means are often dedicated to some specific aspect or property of a system. So, the verification of a system usually involves many different techniques and tools, each of them with its own “usage domain”. Additionally, verifying a single property may sometimes require several models (applying different abstraction), in order to reduce the complexity of the verification problem. Even though all verification activities are based on a sound and rigorous mathematical background, the multiplication of models and abstractions raise the problem of the confidence on the overall verification process. INGEQUIP has addressed this issue in the context of *Safety Cases*. This is addressed in Part 4, §2.1 and §2.2.