



HAL
open science

Verification of real time properties in fiacre language

Nouha Abid

► **To cite this version:**

Nouha Abid. Verification of real time properties in fiacre language. Computation and Language [cs.CL]. INSA de Toulouse, 2012. English. NNT: . tel-00782554

HAL Id: tel-00782554

<https://theses.hal.science/tel-00782554>

Submitted on 30 Jan 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Université
de Toulouse

THÈSE

En vue de l'obtention du DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National des Sciences Appliquées de Toulouse (INSA Toulouse)

Discipline ou spécialité :

Sûreté logicielle et Calcul de haute performance

Présentée et soutenue par :

Nouha ABID

le : mardi 11 décembre 2012

Titre :

Verification of Real Time Properties in Fiacre Language

JURY

Dr. Yamine AIT AMEUR Professeur à l'ENSEEIH de Toulouse

Odile LAURENT Ingénieur AIRBUS

Ecole doctorale :

Mathématiques Informatique Télécommunications (MITT)

Unité de recherche :

LAAS- CNRS

Directeur(s) de Thèse :

Dr. Silvano DAL ZILIO Chargé de recherche CNRS

Dr. Didier LE BOTLAN Maître de conférences à l'INSA de Toulouse

Dr. François Vernadat Professeur à l'INSA de Toulouse

Rapporteurs :

Dr. Françoise Simonot-Lion Professeure à l'université de Lorraine

Dr. Olivier H. Roux Professeur à l'école centrale de Nantes

Verification of Real Time Properties in Fiacre Language

Nouha ABID

◇□ **Her story all over** ◇□

There will be time, there will be time,
to prepare a face to meet the faces that you meet,
there will be time to murder and create
and time for all the works and days of hands,
that lift and drop a question on your plate,
time for you and time for me
and time yet for a hundred indecisions
and for a hundred visions and revisions,
before the taking of a toast and tea.

– **T.S. Eliot**–

Acknowledgements

September 15th, 1991 was my first day at school and December 11th, 2012 is the date of my PhD defense. During these 21 years, I have met many persons who walked beside me and helped me along my way.

I have done my best in this work. However, it would not have been possible without the kind support and help of many individuals. I would like to thanks all of them.

First of all, I would like to thank my supervisor, Dr. Silvano Dal Zilio. Without his help, his guideness and his experience, this thesis will never have an end. During these 3 years, he was always available to answer my questions despite his commitments, to encourage me and to put me in the right path. I do not only consider him as my supervisor in work, but also as a friend. He helped me and gave me advices when I had difficult moments. It has been an honor to work with him.

I extend my thanks to Dr. Didier Le Botlan, whose pedagogy and knowledge in formal proofs make me love this field and have a critical point of view. He encourages me and supports me to make my first steps in this critical domain. Despite of his commitments, he was all the time available to discuss with me and to give me advices. I found in him the right balance between humain character and competence of work.

I would like to thank Dr. François Vernadat and Dr. Bernard Berthomieu. Their experience and knowledge were fundamental to accomplish this thesis and allowed me to achieve many of my goals. Both of them was for me an example to follow. Dr. Berthomieu has helped me in resolving many problems. I am impressed by his organisation in his work. Dr. Vernadat was for me a good example to follow. I am very impressed by his wisdom to treat problems.

I would like also to thank Dr. Françoise Simonot-Lion, Dr. Olivier H.Roux, Dr. Yamine Ait Ameur and Odile Laurent for having reviewed this work.

This thesis and its pages will be seen as an acknowledgement to the thousands of you who have helped me to make my life what is today.

Nahla my sister... I want just to say “THANK YOU” for all things you give me. I would not have considered never to enroll me into a Doctorate program before you encouraged me and helped me in choosing my way. You were and you are still my example for life. I’m so proud of you!

My parents Fatma & Mohamed, my brother Housseem... Thank you for the support you provided me through my entire life. Without your love and encouragements I would not have finished this thesis.

Cosi... Thank you for all the encouragements you give me. You were all the time helping me. We have shared many moments that I will never forget. You are a great person. Thank you for all!

I am indebted to many of my colleagues who supported me during these last three years. I will never forget our discussions about different subjects. Thank you for all things. These moments I spent with all of you were crucial to my personal and professional development. It was great to share experiences and knowledges with interesting people like you.

Last, I express my regards and gratitude to all of those who supported me in any aspect during the completion of this thesis.

Abstract

The formal verification of critical, reactive systems is a very complicated task, especially for non experts. In this work, we more particularly address the problem of *real time systems*, that is in the situation where the correctness of the system depends upon timing constraints, such as the “timeliness” of some interactions. Many solutions have been proposed to ease the specification and the verification of such systems. An interesting approach—that we follow in this thesis—is based on the definition of *specification patterns*, that is sets of general, reusable templates for commonly occurring classes of properties. However, patterns are rarely implemented, in the sense that the designers of specification languages rarely provide an effective verification method for checking a pattern on a system. The most common technique is to rely on a timed extension of a temporal logic to define the semantics of patterns and then to use a model-checker for this logic. However, this approach may be inadequate, in particular if patterns require the use of a logic associated to an undecidable model-checking problem or to an algorithm with a very high practical complexity.

We make several contributions. We propose a complete theoretical framework to specify and check real time properties on the formal model of a system. First, our framework provides a set of real time specification patterns (that may be viewed as a timed extension of Dwyer’s patterns). We provide a verification technique based on the use of observers that has been implemented in a tool for the Fiacre modelling language. Finally, we provide two methods to check the correctness of our verification approach; a “semantics”—theoretical— method as well as a “graphical”—practical— method.

[Keywords:] Verification; Requirement; Specification Patterns; Model Checking; Observers; Real Time Systems