


## PROCÈS-VERBAL DE SOUTENANCE DE THÈSE

Nom et Prénom CHEVALIER Marc  
 Spécialité Informatique  
 Titre de la thèse Analyse de la sécurité de systèmes critiques embarqués à forte composante logicielle, par interprétation abstraite  
 Ecole doctorale Sciences Mathématiques de Paris Centre  
 Date de soutenance 27 novembre 2020  
 Soutenance  PUBLIQUE  À HUIS-CLOS

Président du jury \* : ...Patrick Cousot..... (à compléter).

Le jury prononce:

- l'admission du candidat au titre de docteur de l'Université PSL, thèse préparée à l'École normale supérieure  
 l'ajournement du candidat

Civilité, Nom, Prénom	Qualité	Titre	Etablissement de rattachement	Visio conférence	Signature
M. Jérôme FERET	Directeur de these	CR	Ecole normale supérieure	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
Mme Isabella MASTROENI	Rapporteur	Associate professor	Università degli Studi di Verona	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
M. David PICHARDIE	Rapporteur	Professeur	ENS Rennes	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
M. Patrick COUSOT	Examineur	Professor	New York University	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
M. Peter MÜLLER	Examineur	Professor	ETH Zürich	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
M. Marc POUZET	Examineur	Professeur	ENS	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
Mme Sukyoung RYU	Examineur	Associate professor	KAIST	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	
Mme Mihaela SIGHIREANU	Examineur	Maître de conférences	Université de Paris	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	

\* Article 18 de l'arrêté du 25 mai 2016 fixant le cadre national de la formation et les modalités conduisant à la délivrance du diplôme national de doctorat : **"Les membres du jury désignent parmi eux un président. Le président doit être un professeur ou assimilé ou un enseignant de rang équivalent."**



## DOCTORAT de l'Université PSL

### RAPPORT DE SOUTENANCE

Nom et prénom du doctorant : CHEVALIER Marc

Date de la soutenance : 27 novembre 2020

**Président du Jury** : ..Patrick COUSOT.....

The subject of the thesis, that is, the static analysis of C code including assembler instructions is an extremely hard challenge, a very difficult problem that was not previously considered, even less confronted with the reality of an existing operating system, and had to be solved in the context of an existing analyzer (Astrée).

The manuscript includes all the necessary technical and scientific background on machine architecture, operating system, static analysis by abstract interpretation, and the analyzer Astrée, exposed in a detailed, fluid, and cristal clear style. This information is not easy to extract from the literature and the synthetic presentation is definitely very useful for a large community. This makes the thesis readable by a wide spectrum of researchers with architecture, operating system, or static analysis background. It is both a precise, abstract, detailed, and high-level description of the state of the art. It provides a clear and complete exposition of the context of the work.

One of the main contributions is certainly the formal semantics of the C language, at a level of abstraction that is more refined than usual, in order to cope with the necessary interaction with the computer at a low level, the formal semantics of the assembly language of Intel X86 family of processors (refining the informal and incomplete official documentation), and the mixing/combination of these two semantics formalizing the interaction between the two languages and the machine architecture. Understanding and clearly formalizing the mixed semantics is an achievement of its own, going a lot beyond the state of the art. Moreover, this mixed semantics provides the formal basis from which the static analyzer is designed.

The second of the main contributions of the thesis, is the description of the abstraction of this mixed semantics, including arithmetic and logic statements, the abstraction of the stack, of control statements, up to the details of handling jumps in the assembly code, systems registers, dynamic code, the fixpoint computation induced by the assembly code in addition to the usual structural induction, and so on. This has been implemented, at a professional level of quality. Numerous examples are provided. The complex implementation decisions are discussed in detail. The static analyzer has been checked by an industrial partner on the concrete and realistic example of an industrial embedded operating system. This is in contrast with studies in verification of compilers or micro-kernels, where the program and its verification are designed simultaneously, often with enough restrictions to facilitate the proof. Here the code is given, and must be handled as is, without any possible compromise. This makes a lot of difference with standard academic research and prototypes!

The third of the main contributions of the thesis, is a number of abstract domains and tools of general use, beyond the specific application to the analysis of operating systems. This includes, for example, the base-offset pointer domain, the slice domain for bitwise operations, the Amical disassembler, and so forth.








The fourth of the main contributions of the thesis, is the reduced product with ghost variables. The reduced product aims at combining information on the program execution collected by different abstract domains, each one specialized for a specific kind of information. It is convincingly explained why the hierarchical approximation of the reduced product in Astrée has limitations when considering abstract domains handling ghost/auxiliary/intermediate variables. Such variables are used to name a function of the data manipulated by the program and to analyze its abstract value. Whereas changes to values of variables are clear (although sometimes indirectly through pointers), the changes to ghost variables are always indirect through the changes to the information they encode. This makes it difficult to use classical abstract domains understanding only explicit modifications through assignments and tests as well as for the communication of information from one abstract domain to another. The thesis introduces a new concept (reduced product with ghost variables) to solve these problems. It is a completely new approach to the design of static analyzers by the combination of abstractions, of general use, and with a broad scope. It is a somewhat unexpected outcome of the work, a new original way of designing static analyzers.

In conclusion, the manuscript is a bit long but really good, interesting, comprehensive, accessible, and convincing, very well written, structured, and illustrated, providing intuitions through examples, discussing the motivations and design choices, useful to different communities, solving a difficult problem with an implementation working in an industrial context and providing new concepts and tools to design static analyzers.

The defense was a tour de force, managing to explain clearly and summarizing the main contributions of the thesis in 45mn. It was an enjoyable presentation, at the right level of abstraction, providing meaningful information about an impressive work, and a good summary of the main results.

The answer to the numerous questions showed strong knowledge and maturity in the domains of machine architecture, operating systems, abstract interpretation, static analysis, and their implementations. The answers were very honest, on the strengths and inevitable limitations of the work, always going directly to the main points with great precision.

In conclusion, the jury was unanimous to laud the high-quality and innovative work, its presentation in the defense, and decided to congratulate the candidate for his contributions, and their brilliant written and oral presentations.

Prénom et Nom	Signature	Prénom et Nom	Signature
Jérôme FERET		Isabella MASTROENI	
David PICHARDIE		Patrick COUSOT	
Peter MÜLLER		Marc POUZET	
Sukyong RYU		Mihaela SIGHIREANU	