# Avis de Soutenance

## Monsieur Virgile ROBLES

## Informatique

Soutiendra publiquement ses travaux de thèse intitulés

*Spécifier et vérifier des exigences de haut niveau sur des programmes importants : application à la sécurité des programmes C*

dirigés par Madame Pascale LE GALL

Soutenance prévue le ***mardi 21 janvier 2022*** à 14h00
Lieu : CEA List – Nano-INNOV, 2 Bd Thomas Gobert, 91120 PALAISEAU
Salle : Amphithéâtre 33/34 (RDC)
Visio : https://app.livestorm.co/cea_list/soutenance-de-these-virgile-robles

**Composition du jury proposé**

| | | |
|---|---|---|
| Mme Pascale LE GALL | Université Paris-Saclay | Directrice de thèse |
| M. Alain GIORGIETTI | Université de Franche-Comté | Rapporteur |
| M. Frédéric LOULERGUE | Université d'Orléans | Rapporteur |
| M. Claude MARCHÉ | Université Paris-Saclay | Examinateur |
| M. Mathieu JAUME | Sorbonne Université | Examinateur |
| M. Virgile PREVOSTO | Université Paris-Saclay | Encadrant de thèse |
| M. Nikolai KOSMATOV | Thales Research & Technology | Encadrant de thèse |

M. Louis RILLING DGA Invité

**Mots-clés :** Méthodes formelles, Vérification déductive, Frama-C, Language de spécification

**Résumé :**

La spécification et la vérification d'exigences haut niveau (comme des propriétés de sécurité, telles que l'intégrité des données ou la confidentialité) reste un défi pour l'industrie, alors queles cahiers des charges en sont remplis. Cette thèseprésente un cadre formel pour les exprimer appelélesmeta-propriétés, décrites pour un langage deprogrammation abstrait, et centrées sur les propriétés liées aux manipulations de la mémoire etles invariants globaux. Ce cadre formel est appliquéau langage C avecHILARE, une extension d'ACSL,qui permet la spécification d'exigences haut niveausur des programmes C de grande taille avec facilité.Des techniques de vérification pour HILARE,basées sur la génération d'assertions locales et laréutilisation des analyseurs de Frama-C existants,sont présentées et implantées dans le greffonMetAcslpour Frama-C. Une méthodologie pour l'évaluation des propriétés de grands programmes estdétaillée, articulant les méta-propriétés, les techniques de vérification et les particularités du C.Cette méthodologie est illustrée par un cas d'étudecomplexe : le bootloader de Wookey, un périphérique de stockage chiffré. Enfin, nous explorons uneautre manière de vérifier une exigence de haut niveau en la déduisant à partir d'autres, via un système formel prouvé en Why3 et intégré dans MetAcsl.

**Abstract :**

Specification and verification of high-level requirements (such as security properties like data integrity or confidentiality) remains an important challenge for the industrial practice, despite being a major part of functional specifications. This thesis presents a formal framework for their expression called meta-properties, supported by a description on an abstract programming language, focusing on properties related to memory and global invariants. This framework is then applied to the C programming language, introducing the HILARE extension to ACSL, to allow easy specification of these requirements on large C programs. Verification techniques for HILARE, based on local assertion generation and reuse of the existing Frama-C analyzers, are presented and implemented into the MetAcsl plugin for Frama-C. A complete methodology for assessing large programs is laid out, articulating meta-properties, verification techniques and quirks specific to the C programming language. This methodology is illustrated to a complex case study involving the bootloader of WooKey, a secure USB

storage device. Finally, we explore another way to verify a high-level requirement deducing it from others, through a formal system proven in Why3 and integrated in MetAcsl.