

# Application BASTRI

## Fiches Equipes

### VERIDIS (SR0524TR)

Modeling and Verification of Distributed Algorithms and Systems  
VERIDIS (SR0426IR) □ VERIDIS

**Statut:** Décision signée

**Responsable :** Stephan Merz

**Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" :** A2.1.1. Sémantique des langages de programmation , A2.1.4. Programmation fonctionnelle , A2.1.7. Programmation distribuée , A2.1.11. Langages de preuve , A2.2. Compilation , A2.4. Méthodes formelles pour vérification, sûreté, certification , A2.4.1. Analyse , A2.4.2. Model-checking , A2.4.3. Preuves , A2.5. Génie logiciel , A4.5. Méthodes formelles pour la sécurité , A7.2. Logique , A8.4. Calcul formel, calcul algébrique

**Mots-clés de "B - Autres sciences et domaines d'application - 2023" :** B6.1. Industrie du logiciel , B6.1.1. Génie logiciel , B6.3.2. Protocoles , B6.6. Systèmes embarqués

**Domaine :** Algorithmique, programmation, logiciels et architectures  
**Thème :** Preuves et vérification

**Période :** 01/07/2012 -> 31/12/2024

**Dates d'évaluation :** 17/03/2015 , 20/03/2019 ,

**Etablissement(s) de rattachement :** CNRS, U. DE LORRAINE, MPII  
**Laboratoire(s) partenaire(s) :** LORIA (UMR7503)

**CRI :** Centre Inria de l'Université de Lorraine  
**Localisation :** Centre Inria de l'Université de Lorraine  
**Code structure Inria :** 051091-1

**Numéro RNSR :** 201020692C  
**N° de structure Inria:** SR0524TR

### Présentation

L'équipe projet **VeriDis** est commune au centre de recherche Inria Nancy-Grand Est, le Max-Planck Institut für Informatik, le CNRS et l'Université de Lorraine. Ses membres à Nancy et à Saarbrücken sont des experts en méthodes formelles et en vérification. Les missions du projet sont doubles: d'une part nous contribuons à des progrès en matière des techniques de vérification (fondées sur la preuve automatique et interactive mais aussi sur la vérification algorithmique) et de leur intégration. Notre domaine privilégié d'application est celui des algorithmes et systèmes parallèles et répartis. D'autre part nous travaillons sur les méthodes précises de conception intégrant les techniques formelles de vérification dans les processus de spécification, conception et validation de ces systèmes. Notre but est d'assister les concepteurs à mener des projets de développement prouvé d'algorithmes et de systèmes avec la découverte automatique de preuves de propriétés intéressantes, ainsi que d'erreurs. Les techniques de déduction automatique et interactive ont fait des progrès spectaculaires pendant la décennie passée, et ces techniques ont déjà eu un impact considérable. Par exemple, elles ont été utilisées avec succès dans la vérification et analyse de programmes séquentiels, souvent conjointement avec des techniques d'analyse statique et de model checking. Dans un monde idéal, les systèmes et leurs propriétés sont décrits dans des langage expressifs de haut niveau, les erreurs dans les spécifications sont découvertes automatiquement et enfin, une vérification complète et automatique est également effectuée. Bien évidemment ceci n'est pas possible en général, dû à la complexité inhérente à ce problème. Néanmoins nous avons observé des progrès importants dans des techniques de preuves automatiques et interactives, auxquelles nous avons aussi contribué. Par exemple, beaucoup de progrès a été fait concernant l'intégration de théories importantes comme l'arithmétique dans des techniques de preuve symboliques. Ces progrès suggèrent qu'un degré beaucoup plus élevé d'automatisation est possible dans la vérification de systèmes, par rapport à ce que fournissent les outils actuels. Les démonstrateurs automatiques de théorèmes ne sont pas une panacée pour la vérification de systèmes mais leur utilisation doit être fondée sur une méthodologie saine de modélisation et de vérification de systèmes. Nous avons une expertise considérable dans le développement et dans l'application de méthodes formelles dans le domaine des algorithmes et systèmes parallèles et distribués. Le concept du *refinement* est central dans notre démarche. Il est

### Contact

- **Responsable :** Stephan Merz
- **Tél :** 03.54.95.84.78
- **Secrétariat Tél :** 03.83.59.30.52

### En savoir plus

- Site de l'équipe
- Site sur [inria.fr](http://inria.fr)
- Site du responsable
- Derniers Rapports d'Activité : 2015 , 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023

### Documents sur la structure

- Intranet
- Privés

### Décisions

- **8843** (02/08/2012) : création
- **11317** (14/12/2015) : prolongation
- **14025** (16/12/2019) : prolongation
- **16659** (11/12/2023) : prolongation
- **16998** (26/04/2024) : prolongation

### Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157

important de garantir que ces méthodes viennent en soutien effectif à la conception d'algorithmes et de systèmes répartis.

## Axes de recherche

langages et formalismes pour la modélisation de systèmes répartis, techniques et outils pour la preuve automatique de théorèmes, procédures de décision, solveurs SAT et SMT, preuve interactive, vérification algorithmique par model checking, plate-formes intégrées de vérification

## Logiciels

- **veriT** SMT Solver
- **TLAPS** : TLA+ Proof System
- **Spass** : An Automated Theorem Prover for First-Order Logic with Equality
- **Spass-SATT** : solver for ground linear arithmetic
- **Redlog** : Reduce Logic System

## Relations industrielles et internationales

- Projets européens : ERC **Matryoshka** (2016-2022)
- Participation dans des projets nationaux : ANR-NRF **ProMiS**, ANR **BisoUS**, ANR **BLaSST**, ANR **Discont**, ANR **ICSPA**
- Partenariats internationaux : LMU Munich (Allemagne), TU Dresden (Allemagne), TU Wien (Autriche), JAIST Kanazawa (Japon)