

Rapport d'activités

Nom d'usage : WOLFF Prénom : Burkhard Karl

Corps: PR U

Grade: C1 Ech 03

NUMEN: 25S0803686BTQ

Discipline / section : 27

Synthèse du parcours professionnel

Après avoir effectué une «Diplomarbeit» (équivalent DEA) à l'Université Technique de Berlin en 1991, j'ai obtenu un poste comme «wissenschaftlicher Mitarbeiter» dans l'équipe de Prof. Bernd Krieg-Brückner, BISS, à l'université de Brème. Ma thèse soutenue en 1997 concerne un calcul des systèmes d'écritures de seconde ordre. J'ai commencé à co-encadrer les thèses de mes trois premiers doctorants. De 1998 à 2004 j'étais «wissenschaftlicher Assistent» (équivalent MDC) à l'université de Freiburg où j'ai obtenu mon HDR en 2005 (Garant: D. Basin, J. Korvinck). De 2004 à 2008 j'étais «Oberassistent» à la ETH en Zürich (avec des séjours de 6-mois à Microsoft Research, Redmond et l'université du Saarland dans un projet de Vérification des systèmes d'exploitation). En 2008, j'étais nommé professeur 2ème classe à l'Université Paris-Sud. De 2010 à 2013 j'étais chef d'équipe ForTesSE au LRI (succédant Marie-Claude Gaudel) et de 2013-14 responsable de l'équipe VALS (résultant d'une fusion des équipes ForTesSE et Proval) et de 2014-2020 son co-responsable.

En 2014, j'ai obtenu ma dernière promotion sur PR 1 Classe.

Depuis 2010 à 2016 j'étais responsable de la licence, et, après une année en délégation à SystemX/NannoInnov, (2016/17) responsable RI à PolyTech de 2019-2023. De 2019 à 2022 j'étais chargé de Mission du projet EUGLOH auprès de la Faculté des Sciences. Depuis 2010 je suis membre de la CCUPS-27, et depuis 2020 son Vice-président élu et récemment son président élu.

Evolution des thématiques de recherche:

Thématiquement, j'ai pu ajouter à la tradition de techniques de test à base des modèles de l'équipe ForTesSE le savoir faire des techniques d'exécution symbolique, des systèmes de preuve interactives et automatiques, et la construction des outils sur la plateforme Isabelle. Ce travail a été effectué dans le cadre de deux chaires (une U-PSud, une Digiteo, 2009-12) qui avait pour but l'extension du système HOL-TestGen avec de nouvelles techniques de calculs parallélisés et de nouvelles interfaces de modélisation (PIDE).

HOL-TestGen a été appliqué dans le cadre du projet européen EUROMILS (2012-2015), en particulier dans la thèse de Yakoub Nemouchi. L'objectif du projet était la vérification et certification d'un MILS (Multiple Independent Levels of Security), un système d'exploitation de sécurité à haut niveau qui prend en compte la coexistence de composants non fiables et fiables. Pour la première fois, EURO-MILS a procédé à une évaluation complète de la sécurité d'un système MILS selon les Critères Communs à ses plus hauts niveaux d'assurance, y compris l'ingénierie de vérification formelle.

L'échec final du projet EURO-MILS concernant son objectif de certification m'a inspiré à une axe de recherche qui s'intéresse à des liens entre le formel et semi-formel dans des théories formelles, des documents de certification selon des standards comme CENELEC ou COMMON CRITERIA ou bien des documents techniques ou scientifiques en général. Cette ligne de recherche a abouti à un langage de spécification des ontologies en Isabelle/HOL, et un environnement de développement

des théories formelles validant la conformité a ces ontologies. La thèse de Nicolas Meric (en train de finition) à résulte dans le framework Isabelle/DOF et dans une langage ontologique impliquant héritage et polymorphisme avec des classes des types.

Les années 2012-15 marquaient le début d'une collaboration avec l'équipe autour de Jim Woodcock et Ana Cavalcanti, Université de York, concernant les sémantiques structurés dans les termes de la "Unified Theory of Programs" (UTP), ce qui résultait dans des théories formelles sur UTP et un langage de processus 'Circus', pour laquelle une théorie de test formel a été développé dans le cadre de la thèse de Abdou Felliachi (11-15, postdoc <16). Ces travaux sont actuellement poursuivi dans le cadre de la thèse (en cours) de Benoit Ballenghien(>22) pour une formalisation du calcul de processus HOL-CSP, une théorie plus riche et expressive sur des processus, leurs propriétés algébriques, leur techniques de preuve et des techniques de simulation et test. Le Leitmotif de cette axe de recherche est: "Jusque où peut-on pousser la théorie des algèbres de processus en abandonnant les contraintes de finitude des donnés et de structure dans des processus paramétrisés ?". Tous les travaux de preuve formel en Isabelle/HOL (HOL-CSP et ses extensions comptent entretemps 50000 LOC) ont été publiés dans l'Archive of Formal Proofs'.

Cette axe plutôt orienté "recherche fondamentale" a été complémenté par un axe de recherche appliqué en forte collaboration avec l'Institut de Recherche en Technologie (IRT) System X (un 'hub' pour des projets co-financé par des partenaires industriels et publics, notamment le ANR. Sa dépendance "NannoInnov" à Palaiseau est en particulier orienté vers la NanoTechnologie et des systèmes cyber-physiques). Le but est de modeler des concepts comme "scenario" and "driving strategies" connus dans la domaine des véhicules autonomes (AV) dans un framework basé sur HOL-CSP. Ce framework a été nommé HOL-CyberPhi et une publication sur le AFP est en préparation. Dans ce framework, on a pu modeler des 'acteurs' (les AV) comme des processus communicants et des 'driving strategies' comme des fonctions non-déterministes choisissant des accélérations qui sont effectués sur le véhicule. Dans ce framework, on a pu modéliser une stratégie de conduite RSS connue [3, 4], ce qui a permis d' établir par preuve formelle la sûreté de la stratégie ("no collision if everyone respects RSS"). Une telle preuve a pu établi la première fois de manière formelle [4,2].

En parallèle, j'ai également bâti une collaboration avec INRIA Saclay et INRIA Roquencourt ensemble via le projet ANR Paral-ITP (12-15/16), dont j'étais l'initiateur et coordinateur. Le but de cette collaboration était le développement et le transfert des techniques de parallélisation des noyaux des systèmes de preuve, qui sont maintenant partie de la distribution standard depuis Isabelle 2014. Une version dans le système Coq existe également. Bien évidemment, ces extensions sont réalisés de sorte que le degré de fiabilité nécessaire pour un système de preuve interactive de référence soit maintenu.

Evolution activités pédagogiques, et présentation synthétique:

J'ai crée les modules 'Génie Logiciel Avancé' (UFR L3) et 'Vérification et Validation' (PolyTech ET4) dans les années 2011-14. Ces modules intègrent dans un processus classique de génie logiciel (utilisant des techniques de modélisation semi-formelles en UML) des méthodes et outillages de plus en plus formelles, en passant par des annotations des class invariants, des techniques de génération de test boîte-noire et boîte blanche, et finalement les techniques de preuve des programmes. Le module est accompagné par des TPs couvrant test boîte noire, boîte blanche et preuves via le système gwhy.

Le module (en parallèle et en complément avec le cours 'Introduction a la logique' en L3) forme depuis son existence un des piliers dans la formation programmation et méthodes formelles à la fois dans les parcours info et miage en L3 et aussi en ET4 à PolyTech. La version pour PolyTech est

enseigné en anglais.

J'ai créé un module 'Introduction dans le test a partir des modèles' qui était enseigné entre 2010 - 2016 dans le master "Architectures et Réseaux". Le module était orienté vers la théorie des méthodes de test et combinait la théorie avec différentes applications dans le système HOL-TestGen, couvrant l'aspect modélisation et génération des tests et des test-harnesses pratiques. Des sa création, le cours était enseigné en anglais.

J'ai créé un module 'Introduction dans la preuve interactive' en 2018 qui est partie du master MPRI I (UFR) . Le module connecte au module dans le parcours "Lambda-Calcul" dans le MPRI, introduit à la présentation des calculs logiques en Isabelle/HOL, et démontre dans un ensemble pratiques des techniques de modélisation des structures inductives et des méthodes de preuve correspondantes en Isabelle/HOL. Dans une grande partie pratique (9 h TP), les différentes solutions sont présentés par "hands-on-proving". Des sa création, le cours est enseigné en anglais.

Mes cours sont placés essentiellement à la Faculté des Sciences (Orsay), composante de Paris-Sud resp. Paris-Saclay, dans le L2 (< 2015) et L3 (>2009, 120-140 étudiants), couvrant les deux l'informatique et le miage. Le cours "Verification et validation" dans la composante PolyTech de Paris-Saclay (>2009) ont une taille entre 30 et 40 étudiants. Les cours dans les masters "architecture et réseau" (< 2016) et "master parisien de recherche en informatique I", dont je suis le responsable depuis 2023, suivent autour de 15 étudiants.

(rubrique limitée à 9000 caractères, blancs non compris, soit 3 pages maximum)

Investissement pédagogique

1. Présentation synthétique de l'activité d'enseignement : *principaux enseignements en mettant l'accent sur les thématiques enseignées, les pratiques pédagogiques, les activités particulières : création d'un enseignement, transformation des enseignements.*

1. Programmation et Genie Logiciel (<2015). Un cours en L2 informatique/miage avec une introduction a la programmation Java et des bases dans la modélisation UML. 15h CM, 18h TD, 6-9h TP. ca 160 étudiants.
2. Une groupe "Histoire de l'informatique" dans le module "Histoire des Sciences" (=2015) offerts par le département langues. 1 gr TD 6*2 h. A fun project; helping out the language department.
3. Genie Logiciel Avancé (> 2014 dans le forme actuel ancré dans la maquette). UML avec des annotation logiques, class-invariants, pre-post-conditions in OCL et une variante de OCL en syntaxe logique, black-box-testing, white-box testing, introduction dans la logique Hoare. 15 CM, 18h TD, 6-9hTP. ca 130 étudiants miage, info, LDD.
4. Verification et Validation(>2011), Un cours en 4ème année informatique (ET4) dans la composante PolyTech de Paris-Saclay. UML avec des annotation logiques, class-invariants, pre-post-conditions in OCL et une variante de OCL en syntaxe logique, black-box-testing, white-box testing, introduction dans la logique Hoare. Enseigné en anglais. 12h CM,12h TD, 6h TP. 30-40 étudiants.
5. ca 15 accompagnements des stagiaires L3 dans les entreprises de la région.
6. 4 encadrements de stagiaires L3 et M1 au sein du laboratoire LMF.
7. ... and last but not least: encadrement de 8 doctorants et 4 postdocs.

Details annexe 3. Je rappelle que j'étais en delegation 100 % au SystemX entre sept. 2016 et aout 2017.

2. Responsabilités pédagogiques, en particulier direction, animation, montage de formations, notamment à l'international, fabrication et utilisation de ressources pédagogiques, soutien à l'insertion professionnelle, soutien à l'entrepreneuriat, etc.

1. (<2016) responsable du L3 et de la Licence Informatique et Miage. Responsable pendant AERES 2014-15.
2. (>2023) responsable du prestigieux master parisien de recherche en informatique (MPRI I, track UFR)
3. (2019 - 2023) responsable des RI de PolyTech (encadrement des stages sortant et entrant; suivi des conventions, ... Les stages en ET4 et ET5 sont obligatoires pour toutes les étudiants dans le parcours info ...)

3. Diffusion, rayonnement, activités internationales.

1. (2019-2021/22) Chargé de mission EUGLOH au niveau de la Fac des Sciences (European University Alliance for Global Health; voir <https://www.eugloh.eu/>). Information des départements sur l'évolution du projet, suivi des étudiants partantes, suivi de la construction des modules partagés. 40 h et 30 h décharge pour cette tâche.

Activité scientifique

1. Présentation synthétique des thématiques de recherche : *grands axes de recherche et apport dans le ou les domaines concernés*

1. Une axe générale est le développement des techniques de TEST FORMEL et des combinaisons avec la PREUVE FORMEL.
2. Une autre axe générale est le développement des sémantiques formelles pour des domain-specific languages (DSL)s dans les méthodes formelles.
3. Une autre axe générale est le développement du support technique pour la validation des liens entre le formel et l'informel dans des documents techniques, scientifiques, normatives, ... A ce fin, j'ai développé une langage de définition des ontologies intégré dans Isabelle/HOL et son système de generation des documents.
4. La dernière axe principale est l'extension de la plateforme Isabelle/HOL concernant les aspects parallélisation, interface, generation de code, generation des tests, et generation des documents (avec support ontologique).
5. J'ai un intérêt de longue date dans des substantielles études de cas, de préférence dans le contexte industriel, dans les domaines systèmes d'exploitation, safety et security, ferroviaire et automobile.

2. Publications et productions scientifiques : présentation, en quelques lignes, des 5 publications (ou brevets, logiciels, compte rendus, rapports) jugées les plus significatives (Liste complète en **annexe 7** sans transmission des documents)

1. Paolo Crisafulli, Safouan Taha, Burkhart Wolff: Modeling and analysing Cyber-Physical Systems in HOL-CSP. In: Robotics and Autonomous Systems. DOI: 10.1016/j.robot.2023.104549. Elsevier, Volume 170, Sept. 2023.

Nous présentons un nouveau framework basé sur Isabelle/HOL-CSP pour modéliser des systèmes cyber-physiques, notamment des véhicules autonomes. Cela comprend le temps réel, l'évolution physique, les « scènes » (états globaux) et les « scénarios » (traces) ainsi que l'interaction des « acteurs » (véhicules, piétons, feux de circulation) à l'intérieur de ce cadre. Pour plusieurs instances du framework, nous donnons des preuves formelles d'une propriété de sécurité particulière pour les voitures autonomes : si chaque voiture suit la même stratégie de conduite définie par ce que l'on appelle la sécurité sensible à la responsabilité (RSS)[XXX], aucune collision ne se produira. Les preuves donnent lieu à un certain nombre de variantes de RSS et d'optimisations ainsi qu'à un partitionnement de cas de tests abstraits et à une stratégie de test pour les tests d'intégration. Un rapport technique contient les preuves formelles: <https://inria.hal.science/hal-03429597v2>.

2. Achim D. Brucker, Frederic Tuong and Burkhart Wolff: Model Transformation as Conservative Theory-Transformation. In: Journal of Object Technology. DOI: 10.5381/jot.2020.19.3.a3. Volume 19, Issue 3, pages 1-16, September 2020.

Nous présentons une nouvelle technique pour la construction d'outils pour les langages spécifiques à un domaine (DSL) à l'intérieur de la plateforme Isabelle/HOL. Notre approche est basée sur la modélisation de la sémantique formelle du DSL en logique d'ordre supérieur (HOL), et de compiler des éléments syntaxiques des DSL via des compilateurs dans cette sémantique. En réutilisant des constructions de spécification "definition", "type-definition" et "record" de l'API d'Isabelle, on peut construire des outils comprenant IDE, document-generation, preuves interactives et automatiques, generation de code à l'intérieur de la plate-forme. Notre approche garantit la sécurité logique (conservativité) de l'extension du système et fournit ainsi un outil certifié. L'approche est démontrée dans ce papier pour des diagrammes de classe UML; mais des implantations d'autres langages comme TESL, CSP, Event-B et RoboChart (par une équipe à Univ. York) ont été réalisés suivant cet approche.

3. Achim D. , Idir Aït-Sadoune, Nicolas Méric, Burkhart Wolff: Using Deep Ontologies in Formal Software Engineering. ABZ 2023: 15-32. DOI 10.1007/978-3-031-33163-3_2, LNCS 14010, 2022. A journal version of this paper has been submitted to 'Science of Computer programming'.

Isabelle/DOF est un cadre d'ontologie au-dessus d'Isabelle Isabelle/DOF permet le développement formel d'ontologies ainsi que la vérification continue de la conformité des documents intégrés annotés par des données ontologiques. Un document intégré peut contenir du texte, du code, des définitions, des preuves et des constructions programmées par l'utilisateur prenant en charge un large éventail de méthodes formelles. Isabelle/DOF est conçu pour exploiter la traçabilité dans les documents intégrés en prenant en charge la navigation dans l'IDE d'Isabelle ainsi que le processus de génération de documents. Plutôt que d'introduire un propre langage de programmation pour les métadonnées, nous utilisons la logique d'ordre supérieur (HOL) pour les expressions, les contraintes de données, les invariants ontologiques et les requêtes via la génération de code et la réflexion. Nos exemples d'application couvrent des documents ciblant des certifications formelles telles que CENELEC, Common Criteria, etc. Le logiciel Isabelle/DOF est distribué par le page Zenodo: <https://zenodo.org/records/3370483#.YwjhnOxByWY>.

4. Hai Nguyen Van, Thibaut Balabonski, Frédéric Boulanger, Chantal Keller, Benoît Valiron, and Burkhart Wolff. On the semantics of polychronous polytimed specifications. *FORMATS 2020. LNCS 12288*, pages 23-40. Springer-Verlag 2020.

Ce texte est un point culminant d'une série des publications [21,11,34]. Nous étudions la sémantique d'un langage de spécification pour la coordination de systèmes concurrents, qui prend en charge le temps à différents niveaux : divers domaines temporels, polychronie et contraintes de temps mixtes métriques/logiques. Ce langage nommé TESL est définie par une sémantique dénotationnelle. Afin de pouvoir construire les délais possibles à des fins de vérification, nous définissons également une sémantique opérationnelle symbolique, qui est la référence pour une implémentation efficace d'un outil de test d'exécution de systèmes hétérogènes. Cette étude présente une nouvelle manière de relier ces deux sémantiques en tirant parti d'un principe de déroulement coinductif de ces chronologies. De plus, ces sémantiques et leurs équivalences ont été formalisées dans l'assistant de preuve Isabelle/HOL, accompagnées de preuves de correction, d'exhaustivité et d'avancement.

5. Safouan Taha, Burkhart Wolff, Lina Ye: Philosophers May Dine - Definitely! In: Integrated Formal Methods (IFM 2020). *LNCS 12546*, pages 419-439. Springer, 2020.

La théorie des 'communicating sequential processes' (CSP) développée par Hoare et Roscoe est encore aujourd'hui l'une des théories de référence pour la spécification des comportements concurrentes. HOL-CSP est une formalisation de la sémantique dénotationnelle de CSP en Isabelle/HOL qui est, vue que les événements peuvent être n'importe quel objet définissable en HOL, plus expressive que l'original. En particulier, ce modèle permet des alphabets infinis, et des processus paramétrable. Dans cet article, nous étendons cette théorie dans une large mesure en ajoutant des opérateurs architecturaux, des nouvelles concepts de raffinement, et de nouvelles techniques de preuve sur des architectures des processus de taille arbitraire. Comme exemple, on prouve que Dijkstra's dining philosophers sont sans blocage pour des anneaux de philosophes de taille arbitraire. Les théories sur CSPM, les Raffinement, et la sémantique opérationnelle de HOL-CSP sont publiées dans le Archive of Formal Proofs AFP.

Selon google scholar, j'ai un H-index de 29.

3. Encadrement doctoral et scientifique (*Liste complète en annexe 4*)

1. Abdou Felliachi (Phd 2012-15 100 %, Postdoc 2015-16; 100 %)
2. Yakoub Nemouchi (Phd 13-16, 100 %)
3. Frederic Tuong (Phd 2014-17, 100 %, postdoc 2018-19, 100 %)
4. Romain Aissat (Phd 2012-16, 100 %)
5. Hai Nguyen Van (Phd 2015-18, 50 %, avec F. Boulanger)
6. Nicolas Meric (Phd 2020 -2024 (mai), en cours, 80%, avec I. Ait-Sadoune)
7. Benoit Ballenghuin (Phd 2022, en cours, 70 %, avec C. Dubois)
8. Benedict Puyobro (Phd 2024. en cours, 100 %)

Additionnellement, je mentionne l'encadrement du postdoc Adrien Durier, 12 mois 2022-23. Entretemps, Adrien est MdC UFR et membre du LMF. Abdou Felliachi et Frederic Tuong ont prolongé leur travail de recherche avec un poste post-doc 6 mois resp. 12 mois.

1. Diffusion et rayonnement

1. Organisation des conférences :

- Co-PC-Chair International Conference on Unified Theories in Programming (UTP 12)
- Co-PC-Chair (International Conference on Testing Software and Systems ICTSS 11)
- Dagstuhl Seminary 13021 (2013): Symbolic Methods in Testing. (co-organizer with M. Veanes and T. Jérón)
- Co-PC-Chair Int. Conference on Test and Proof (TAP 11 and TAP 18)
- Co-organizer Journée MTV2 Mars 2023

2. Editorial Boards :

- Member of the Editorial Board of the Springer Journal "Formal Aspects of Computing (>2021)

3. Comités de programme:

- Unified Theory of Programming (UTP 12),
- Intl. Conference on Testing Software and Systems ICTSS 12-14, 18-20.
- Intl. Conference on Interactive Theorem Proving {12,13,14, 24},
- Test and Proof {TAP 09-20}, Steering committee (>18),
- Intl Conference on Theoretical Aspects of Computer Science (ICTAC 14)
- Formal Methods (FM 16)
- Intl Conference on Testing Software and Systems (ICTSS 16,18,19,20)
- Intl Conference on Object Constraint Logics (OCL 16,17)
- Theorem Proving Comp. of Educ. Softw. (CADE Workshop, 17,18)
- Symposium on Applied Computing (SAC 19,20,23)
- International Conference on Engineering of Complex Computer Systems (ICECC 23,24)

4. Invitations:

- Invited Talk au conference ABZ 1.6.2023: Using Deep Ontologies in Formal Software Engineering.
- Invited Talk @ Univ. Bremen Informatik Dept 22.6.22.: Using HOL-CSP for Autonomous Systems Modeling.
- Nov 15, 2021: Invited Talk by the Univ. Exeter: Modeling and Analysing Cyber-Physical Systems in HOL-CSP.
- 1. Sept. 2016 -31. Aug. 2017.: Delegation 100 % à SystemX, Palaiseau
- Oct 27, 2017: Invited Talk at the Departments Colloquium Virginia Tech, Blacksburg, USA: Towards Verified and Certifiable Subsystems.
- July 19, 2017: Invited Tutorial at the 11th International Conference on Tests & Proofs: Combining Verification and Testing.
- Feb 17, 2017: Invited Talk at the Departments Colloquium at University of Sheffield, GB: Monadic Program-based Tests - An Exercise in Test and Proof

- July 2015: Invited Talk at the Departments Colloquim University of York: Can Testing Be Liberated from the Automata Style ?

5.Expert en theses hors établissement:

- Mathieu Carlier (14, doc, Univ. Evry)
- Andrew Boyton (14, doc, Univ. New South Wales, Sidney, Australia)
- Alberto Calvi (15,doc, Univ. di Verona)
- Robert Sachtleben (22, doc, Univ. Bremen)
- Meryem AFENDI (22, doc, Univ Paris-Ext Creteil)

6. President HDR:

- Natalia Kushik (22, Telecom SudParis)
- Nikolay Kosmatov (20,CEA List)

7.Autres:

- J'ai une collaboration de longue terme avec le IRT SystemX, Palaiseau, avec un certain rayonnement dans les partenaires industrielles comme Alstom, EDF, Stellantis, Peugeot, ... Voir contrats de recherche.

1.Responsabilités scientifiques

- Responsable d'Equipe VALS (2010-2014) et Co-Resp. (2014-2020)
- Organisation du Seminaire de Recherche du Laboratoire de Methodes Formelles (LMF, >2021)
- Animation of the "Test-Club" and the "Isabelle-Club" (meetings irregulier des groupes de travail, >2018, dans l'equipe VALS et au LMF).

1.Contrats de Recherche

- >2023: Site leader comme partenaire le projet CVH @ Systeme X (budget 210000 €)
- 2019-21: Soutraintance d'un WP dans le projet 3SA @ Systeme X (budget 75000 €)
- 2016-17: Participation dans le projet OVH @ Systeme X sous forme d'une delegation pour 12 mois (budget 140000 €)
- Initiateur et Responsable du Projet ANR ParallTP 2011 - 14/15: (coordinateur, budget local LRI 390000 €; partenaires INRIA Rocquencourt, INRIA Saclay)
- 2013 - 16: Participation Project IRT SystemX (budget local LRI 215000 €)
- 2012 - 15: Local project leader EU IP EURO-MILS (budget LRI 311000 €)

Responsabilités collectives et d'intérêt général

2. Responsabilités administratives

- (>2010) Membre de la “Commission Consultative de Paris-Saclay” (ou ses prédécesseurs à Paris-Sud). Ce commission decide sur les suivis de carrières, composition des comités de selection, primes etc. des enseignant chercheurs de la section 27. Depuis 2020 vice-président élu, depuis 2023 président de la commission.
- (2019-2021/22) Chargé de mission EUGLOH au niveau de la Fac des Sciences (European University Alliance for Global Health; voir <https://www.eugloh.eu/>). Information des départements sur l'évolution du projet, suivi des étudiants partantes, suivi de la construction des modules partagés. 40 h et 30 h décharge pour cette tâche.

4. Responsabilités et mandats (internationaux, nationaux)

- (>2019) membre suppléant de la CNU, finalement 2023 membre. Participation en tant que tel dans l'évaluation RIPEC 2023 Marseille.
- (>2023) Candidature spontané dans le CNU après le mandat. Je suis donc dans la “réserve” de la CNU.

ANNEXES

3. Tableau des enseignements

| Titre du cours | Année | Rôle: | Niveau étudiant | Nombres d'étudiant |
|---|-----------|---|-------------------|--------------------|
| MPRI I (IPA) Introduction aux assistants de preuves interactives | 2020-24 | Créateur à 100 %, 9h CM, 9 h TP. | M1, 8 sem. | 10-20 |
| L3-GLA Genie Logiciel Avancé | 2011-24 | Créateur à 100 %, 18h CM, 2 * 18h TD (+ encadrement 2 TD), + 1 TP 9h (+ encadrement 3 TP) | 5 sem. | 120-130 |
| Verification et Validation (PolyTech) | 2012 - 24 | Créateur à 100 %, 14h CM, 2 * 14h TD, 2 * 6h TP noté; en anglais. | 8 sem. | 30 - 40 |
| L3: Projet Genie Logiciel | 2009-24 | Créateur à 100 %, 6 h cours, 36h TP | 6 sem. | 15-30 |
| L2-POnGL Programmation Java + Introduction Genie Logiciel | 2011 - 15 | Créateur à 100%, 27h C 18h, TD (+ encadrement 2 TD) 15TP | 4 sem. | 120 - 160 |
| Master Recherche 2: Test des Systemes en Informatique | 2009 - 16 | Créateur à 100 , 21/24h C | M2, 9 sem. | 5 à 10 |
| Elements sur Test dans le Tronc commun du M2R NSI | 2011-15 | Créateur à 100 %, 4.5h C, 3h TD | 9-10 sem. | 10 à 15 |
| L1: info121; Introduction dans l'informatique | 2013-14 | Créateur 0 %, 27h TD | 2 sem. | 20 |
| Master 2 Pro: Projet Genie Logiciel | 2009 | Remplaçant, 24h C | M2 Pro, 9-10 sem. | 25 |
| L3: Génie Logiciel | 2009-11 | Créateur à 50 %, 20h C, 18h TD | 6 sem. | 60 - 80 |

4. Liste classée des publications (celles-ci ne doivent pas être jointes)

Resume des publications depuis 2014, cf. liste des publications dans l'annexe:

- 1.Revues top tiers; Com. de relecture: [1][7][32][33]
- 2.Conf Core A+, A; Com. de relecture: [2][3][12][21][23][36]
- 3.Conf Core B+, B; Com. de relecture: [9][11][14][16][18][19][24][28][35]
- 4.Mechanically checked theories in the Archive of Formal Proofs (AFP): [5][6][20][26][30][37][38]
- 5.Other major software artefacts: [13]

5. Liste complete des direction et codirection de thèses

- 1.Haykal Tej (Phd 1994-98, co-encadrement 50% avec B. Krieg-Brueckner)
2. Thomas Meyer (Phd 1994-00, co-encadrement 50% avec B. Krieg-Brueckner)

3. Kolyang Kolyang (Phd 1994-98, co-encadrement 50% avec B. Krieg-Brueckner);
NOW: Prof à Garoua, Cameron)
4. Achim Brucker (Phd 2002-05, co-encadrement 50% avec D. Basin,
NOW: Prof and head of computer security Univ Exeter.)
5. Matthias Daum, (Universität Saarbrücken, co-encadrement 50% avec W. Paul, fin 2011;
NOW: Researcher at NICTA, Sidney, Australia).
6. Lukas Brügger (Phd 2006-09, co-encadrement 50% avec D. Basin)
7. Mathias Krieger (Phd 2010-2014)
8. Abdou Felliachi (Phd 2012-15 100 %, Postdoc 2015-16; 100 %;
NOW Positions a RATP et Stellantis)
9. Romain Aissat (LRI, 2012-16,
NOW: FM companies region parisienne)
10. Yakoub Nemouchi (Phd 13-16, 100 %,
LATER Postdocs U Virginia, NOW post at US patent office.)
11. Frederic Tuong (Phd 2014-17, 100 %, postdoc 2018-19, 100 %.:
LATER postdocs U Singapore, NOW permanent researcher at U Vancouver.)
12. Hai Nguyen Van (Phd 2015-18, 50 % avec F. Boulanger;
NOW FM companies region parisienne.)

TOUTES les theses étaient soutenues.

Thèses en cours

13. Nicolas Meric (Phd 2000(nov) - 2024 (mai)) [2][13]; une version journal de [2] a été soumise à SCP.
14. Benoit Ballenghuin (2022, en cours, 50 % avec C. Dubois)
15. Benedict Puyobro (2023, en cours)

6. Contrats, projets et collaborations

- 2023-... : : Participation dans le SystemX projet 3SA (partenaire, 70kEUR)
- 2020-22: Participation dans le SystemX projet OVH (subcontracting, 70kEUR)
- 2016-17: Participation dans le SystemX projet PST (delegation)
- 2013 - 16: Project SystemX (budget local LRI 215000 €; These F.Tuong)
- 2012 - 15: EU IP EURO-MILS (budget local LRI 311000 €)
- 2011 - 14/15: ANR Paral-ITP (coordinateur, budget local LRI 390000 €;
partenaires INRIA Rocquencourt, INRIA Saclay)

7. Liste (presque) complete des publications:

| | |
|------|---|
| [1] | Paolo Crisafulli, Safouan Taha, and Burkhart Wolff. Modeling and analysing cyber-physical systems in hol-csp. <i>Robotics and Autonomous Systems</i> , 170:104549, 2023. |
| [2] | Achim D. Brucker, Idir Aït-Sadoune, Nicolas Méric, and Burkhart Wolff. Using deep ontologies in formal software engineering. In Uwe Glässer, José Creissac Campos, Dominique Méry, and Philippe A. Palanque, editors, <i>Rigorous State-Based Methods - 9th International Conference, ABZ 2023</i> , LNCS 14010, pages 15-32. Springer, 2023. |
| [3] | Yamine Ait-Ameur and Ferhat Khendek, editors. <i>Automated Reasoning for Physical Quantities, Units, and Measurements in Isabelle/HOL</i> . Proceedings of the ICECCS, IEEE, 2023. |
| [4] | Paolo Crisafulli, Safouan Taha, and Burkhart Wolff. Modelling and Proving Safety in Autonomous Cars Scenarios in HOL-CSP. Research report, University Paris-Saclay ; IRT SystemX, Palaiseau, October 2021. |
| [5] | Simon Foster and Burkhart Wolff. A sound type system for physical quantities, units, and measurements. <i>Arch. Formal Proofs</i> , 2020, 2020. |
| [6] | Safouan Taha, Burkhart Wolff, and Lina Ye. The HOL-CSP refinement toolkit. <i>Arch. Formal Proofs</i> , 2020, 2020. |
| [7] | Achim D. Brucker, Frédéric Tuong, and Burkhart Wolff. Model transformation as conservative theory-transformation. <i>J. Object Technol.</i> , 19(3):3:1-16, 2020. |
| [8] | Hai Nguyen Van, Frédéric Boulanger, and Burkhart Wolff. Timed discrete-event simulation of aviation scenarios. <i>Simul. Notes Eur.</i> , 30(2):51-60, 2020. [bib DOI http] |
| [9] | Safouan Taha, Burkhart Wolff, and Lina Ye. Philosophers may dine - definitively! In Brijesh Dongol and Elena Troubitsyna, editors, <i>Integrated Formal Methods - 16th International Conference, IFM 2020</i> , LNCS 12546, pages 419-439. Springer, 2020. |
| [10] | Safouan Taha, Lina Ye, and Burkhart Wolff. Philosophers may Dine - Definitively! In Carlo A. Furia, editor, <i>Integrated Formal Methods (iFM)</i> , number 12546 in Lecture Notes in Computer Science. Springer-Verlag, Heidelberg, 2020. |
| [11] | Hai Nguyen Van, Frédéric Boulanger, and Burkhart Wolff. TESL: A Model with Metric Time for Modeling and Simulation. In Emilio Muñoz-Velasco, Ana Ozaki, and Martin Theobald, editors, <i>27th International Symposium on Temporal Representation and Reasoning (TIME 2020)</i> , LIPIcs volume 178, pages 15:1-15:15, 2020. |
| [12] | Hai Nguyen Van, Thibaut Balabonski, Frédéric Boulanger, Chantal Keller, Benoît Valiron, and Burkhart Wolff. On the semantics of polychronous polytimed specifications. <i>FORMATS 2020</i> . LNCS 12288, pages 23-40. Springer-Verlag 2020. |
| [13] | Achim D. Brucker and Burkhart Wolff. Isabelle/DOF, Version 1.1, ZENODO, August 2019. https://zenodo.org/records/3370483#.YwjhnOxByWY . |
| [14] | Achim D. Brucker and Burkhart Wolff. Using Ontologies in Formal Developments Targeting Certification. In Wolfgang Ahrendt and Silvia Lizeth Tapia Tarifa, editors, <i>Integrated Formal Methods (iFM)</i> , LNCS 11918. Springer-Verlag, Heidelberg, 2019. |
| [15] | Frédéric Tuong and Burkhart Wolff. Deeply Integrating C11 Code Support into Isabelle/PIDE. In <i>International Workshop on Formal Integrated Development Environments (F-IDE)</i> , EPTCS 314. Open Publishing Association, Heidelberg, 2019. |
| [16] | Achim D. Brucker and Burkhart Wolff. Isabelle/DOF: Design and Implementation. In <i>International Conference on Software Engineering and Formal Methods (SEFM)</i> , LNCS 11724, Springer-Verlag, Heidelberg, 2019. |

| | |
|------|--|
| [17] | Joshua A Bockenek, Peter Lammich, Yakoub Nemouchi, and Burkhart Wolff. Using Isabelle/UTP for the Verification of Siorting Algorithms: A Case Study. In <i>Isabelle Workshop part of FLOC'18</i> , July 2018. Isabelle Workshop 2018, Colocated with Interactive Theorem Proving. As part of FLOC 2018, Oxford, GB. |
| [18] | Achim D. Brucker, Idir Ait-Sadoune, Paolo Crisafulli, and Burkhart Wolff. Using the isabelle ontology framework: Linking the formal with the informal. In <i>Conference on Intelligent Computer Mathematics (CICM)</i> , LNCS 11006. Springer-Verlag, Heidelberg, 2018. |
| [19] | S. Bezzecchi, P. Crisafulli, C. Pichot, and B. Wolff. Making agile development processes fit for v-style certification procedures. In <i>ERTS'18</i> , ERTS Conference Proceedings, 2018. |
| [20] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. Formal network models and their application to firewall policies. <i>Archive of Formal Proofs</i> , 2017, 2017. [|
| [21] | Hai Nguyen Van, Thibaut Balabonski, Frédéric Boulanger, Chantal Keller, Benoît Valiron, and Burkhart Wolff. A symbolic operational semantics for TESL - with an application to heterogeneous system testing. <i>FORMATS 2017, LNTCS 10419</i> , pages 318-334, 2017. |
| [22] | Achim D. Brucker, Lukas Brügger, Abderrahmane Feliachi, Chantal Keller, Matthias P. Krieger, Delphine Longuet, Yakoub Nemouchi, Frédéric Tuong, and Burkhart Wolff. HOL-TestGen 1.8.0 user guide. Technical Report 1586, Laboratoire en Recherche en Informatique (LRI), Université Paris-Sud 11, France, April 2016. |
| [23] | R. Aissat, F. Voisin, and B. Wolff. Infeasible paths elimination by symbolic execution techniques: Proof of correctness and preservation of paths. In <i>ITP'16</i> , volume 9762 of <i>Lecture Notes in Computer Science</i> , 2016. |
| [24] | Achim D. Brucker and Burkhart Wolff. Monadic sequence testing and explicit test-refinements. In <i>Tests and Proofs - 10th International Conference, TAP 2016</i> , LNCS 7942, 2016. |
| [25] | Achim D. Brucker, Jordi Cabot, Gwendal Daniel, Martin Gogolla, Adolfo Sánchez-Barbudo Herrera, Frank Hilken, Frédéric Tuong, Edward D. Willink, and Burkhart Wolff. Recent developments in OCL and textual modelling. In <i>Proceedings of the 16th International Workshop on OCL and Textual Modelling co-located with 19th International Conference on Model Driven Engineering Languages and Systems (MODELS 2016)</i> , Saint-Malo, France, pages 157-165, 2016. |
| [26] | Romain Aïssat, Frédéric Voisin, and Burkhart Wolff. Infeasible paths elimination by symbolic execution techniques: Proof of correctness and preservation of paths. <i>Archive of Formal Proofs</i> , 2016, 2016. |
| [27] | R. Aissat, M.-C. Gaudel, F. Voisin, and B. Wolff. Pruning infeasible paths via graph transformations and symbolic execution: a method and a tool. Technical Report 1588, L.R.I., Univ. Paris-Sud, 2016. |
| [28] | Romain Aïssat, Marie-Claude Gaudel, Frédéric Voisin, and Burkhart Wolff. A method for pruning infeasible paths via graph transformations and symbolic execution. In <i>2016 IEEE International Conference on Software Quality, Reliability and Security, QRS 2016, Vienna, Austria, August 1-3, 2016</i> , pages 144-151, 2016. |
| [29] | Achim D. Brucker, Frédéric Tuong, and Burkhart Wolff. Featherweight OCL: A Proposal for a Machine-Checked Formal Semantics for OCL 2.5. Technical Report 1582, LRI, Univ Paris Sud, CNRS, Centrale Supélec, Université Paris-Saclay, France, September 2015. |
| [30] | Frédéric Tuong and Burkhart Wolff. A Meta-Model for the Isabelle API. <i>Archive of Formal Proofs</i> , 2015. |

| | |
|------|--|
| [31] | Yakoub Nemouchi, Abderrahmane Feliachi, Burkhart Wolff, and Cyril Proch. <i>Used Formal Methods</i> , chapter Using Isabelle/HOL in Certification Processes: A System Description and Mandatory Recommendations. The EURO-MILS Project, 2015. available from the Project site: http://www.euromils.eu/downloads/Deliverables/Y2/2015-EM-UsedFormalMethods-WhitePaper-October2015.pdf . |
| [32] | Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff. Symbolic test-generation in HOL-TestGen/Cirta: A case study. <i>Int. J. Software Informatics</i> , 9(2):177-203, 2015. |
| [33] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. Formal firewall conformance testing: An application of test and proof techniques. <i>Softw. Test., Verif. Reliab.</i> , 25(1):34-71, 2015. |
| [34] | Hai Nguyen Van, Thibaut Balabonski, Frédéric Boulanger, Safouan Taha, Benoît Valiron, Burkhart Wolff, and Lina Ye. Towards a formal semantics of the TESL specification language. <i>GEMOC+MPM@MoDELS 2015. Proceedings</i> , pages 14-19, 2015. |
| [35] | Achim D. Brucker, Oto Havle, Yakoub Nemouchi, and Burkhart Wolff. Testing the IPC protocol for a real-time operating system. In Arie Gurfinkel and Sanjit A. Seshia, editors, <i>Working Conference on Verified Software: Theories, Tools, and Experiments. LNCS 9593</i> . Springer-Verlag, Heidelberg, 2015. |
| [36] | Freek Verbeek, Oto Havle, Julien Schmaltz, Sergey Tverdyshev, Holger Blasum, Bruno Langenstein, Werner Stephan, Burkhart Wolff, and Yakoub Nemouchi. Formal API specification of the PikeOS separation kernel. In <i>NASA Formal Methods - 7th International Symposium, NFM 2015, Proceedings</i> , pages 375-389, 2015. |
| [37] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. The Unified Policy Framework (UPF). <i>Archive of Formal Proofs</i> , November 2014. http://afp.sf.net/entries/UPF.shtml , Formal proof development. |
| [38] | Freek Verbeek, Sergey Tverdyshev, Oto Havle, Holger Blasum, Bruno Langenstein, Werner Stephan, Yakoub Nemouchi, Abderrahmane Feliachi, Burkhart Wolff, and Julien Schmaltz. Formal specification of a generic separation kernel. <i>Archive of Formal Proofs</i> , July 2014. http://afp.sf.net/entries/CISC-Kernel.shtml , |
| [39] | Delphine Longuet, Frédéric Tuong, and Burkhart Wolff. Towards a Tool for Featherweight OCL: A Case Study On Semantic Reflection. In <i>Proceedings of the 14th International Workshop on OCL and Textual Modelling (co-located MODELS 2014)</i> , pages 43-52, 2014. |
| [40] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. The unified policy framework (UPF). <i>Archive of Formal Proofs</i> , 2014, 2014. |
| [41] | Achim D. Brucker, Tony Clark, Carolina Dania, Geri Georg, Martin Gogolla, Frédéric Jouault, Ernest Teniente, and Burkhart Wolff. Panel discussion: Proposals for improving OCL. In <i>Proceedings of the 14th International Workshop on OCL and Textual Modelling co-located with 17th International Conference on Model Driven Engineering Languages and Systems (MODELS 2014), Valencia, Spain, September 30, 2014.</i> , pages 83-99, 2014. [bib pdf] |
| [42] | Achim D. Brucker, Frédéric Tuong, and Burkhart Wolff. Featherweight ocl: A proposal for a machine-checked formal semantics for OCL 2.5. <i>Archive of Formal Proofs</i> , January 2014. http://afp.sf.net/entries/Featherweight_OCL.shtml , Formal proof development. |
| [43] | Thierry Jéron, Margus Veanes, and Burkhart Wolff. Symbolic Methods in Testing (Dagstuhl Seminar 13021). <i>Dagstuhl Reports</i> , 3(1):1-29, 2013. |
| [44] | Abderrahmane Feliachi, Marie-Claude Gaudel, Makarius Wenzel, and Burkhart Wolff. The circus testing theory revisited in isabelle/hol. In <i>International Conference on Formal Engineering Methods(ICFEM)</i> , LNCS 8144, Springer-Verlag, Heidelberg, 2013. |

| | |
|------|--|
| [45] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. HOL-TestGen/FW: An environment for specification-based firewall conformance testing. In <i>International Colloquium on Theoretical Aspects of Computing (ICTAC)</i> , LNCS 8049. Springer-Verlag, Heidelberg, 2013. |
| [46] | Bruno Barras, Lourdes Del Carmen González-Huesca, Hugo Herbelin, Yann Régis-Gianas, Enrico Tassi, Makarius Wenzel, and Burkhart Wolff. Pervasive parallelism in highly-trustable interactive theorem proving systems. In <i>MKM/Calculemus/DML</i> , LNCS 7961, pages 359-363. Springer, 2013. |
| [47] | Bruno Barras, Lourdes Del Carmen González-Huesca, Hugo Herbelin, Yann Régis-Gianas, Enrico Tassi, Makarius Wenzel, and Burkhart Wolff. Pervasive parallelism in highly-trustable interactive theorem proving systems. <i>CoRR</i> , abs/1305.7360, 2013. |
| [48] | Achim D. Brucker, Abderrahmane Feliachi, Yakoub Nemouchi, and Burkhart Wolff. Test program generation for a microprocessor - a case-study. In <i>Proceedings of the 6th Intl. Conf. on Test and Proof (TAP '13)</i> , LNCS 7942, Springer, 2013. |
| [49] | Burkhart Wolff, Marie-Claude Gaudel, and Abderrahmane Feliachi, editors. <i>Unifying Theories of Programming, 4th International Symposium, UTP 2012, Revised Selected Papers</i> , LNCS 7681. Springer, 2013. |
| [50] | Achim D. Brucker, Delphine Longuet, Frédéric Tuong, and Burkhart Wolff. On the Semantics of Object-Oriented Data Structures and Path Expressions. In <i>OCL@MoDELS</i> , volume 1092 of <i>CEUR Workshop Proceedings</i> , pages 23-32. CEUR-WS.org, 2013. |
| [51] | Achim D. Brucker, Dan Chiorean, Tony Clark, Birgit Demuth, Martin Gogolla, Dimitri Plotnikov, Bernhard Rumpe, Edward D. Willink, and Burkhart Wolff. Report on the Aachen OCL meeting. In <i>OCL@MoDELS</i> , volume 1092 of <i>CEUR Workshop Proceedings</i> , pages 103-111, 2013. |
| [52] | Achim D. Brucker and Burkhart Wolff. On Theorem Prover-based Testing. <i>Formal Asp. Comput. (FAOC)</i> , 25(5):683-721, 2013. |
| [53] | Achim D. Brucker and Burkhart Wolff. On theorem prover-based testing. <i>Formal Asp. Comput.</i> , 25(5):683-721, 2013. |
| [54] | Achim D. Brucker, Delphine Longuet, Frédéric Tuong, and Burkhart Wolff. On the semantics of object-oriented data structures and path expressions (extended version). Technical Report 1565, Laboratoire en Recherche en Informatique (LRI), Université Paris-Sud 11, France, 2013. |
| [55] | Abderrahmane Feliachi, Burkhart Wolff, and Marie-Claude Gaudel. Isabelle/circus. <i>Archive of Formal Proofs</i> , June 2012. http://afp.sourceforge.net/entries/Circus.shtml , Formal proof development. |
| [56] | Achim D. Brucker, Lukas Brügger, Matthias P. Krieger, and Burkhart Wolff. HOL-TestGen 1.7.0 user guide. Technical Report 1551, Laboratoire en Recherche en Informatique (LRI), Université Paris-Sud 11, France, April 2012. |
| [57] | Achim D. Brucker and Burkhart Wolff. Featherweight ocl: a study for the consistent semantics of ocl 2.3 in hol. In <i>Proceedings of the 12th Workshop on OCL and Textual Modelling</i> , OCL '12, pages 19-24, New York, NY, USA, 2012. ACM. |
| [58] | Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff. Isabelle/Circus: A process specification and verification environment. In <i>VSTTE</i> , LNCS 7152, pages 243-260, 2012. |
| [59] | Abderrahmane Feliachi. Representing Circus Operational Semantics in Isabelle/HOL. Technical Report 1544, LRI, http://www.lri.fr/Rapports-internes , Université Paris-Sud XI, August 2011. |
| [60] | Jordi Cabot, Robert Clarisó, Martin Gogolla, and Burkhart Wolff. Preface (OCL 2011 proceedings). <i>ECEASST</i> , 44, 2011. |

| | |
|------|---|
| [61] | Burkhart Wolff and Fatiha Zaidi, editors. <i>Testing Software and Systems - 23rd IFIP WG 6.1 International Conference, ICTSS 2011</i> . LNCS 7019. Springer, 2011. |
| [62] | Martin Gogolla and Burkhart Wolff, editors. <i>Tests and Proofs - 5th International Conference, TAP 2011, Zurich, Switzerland, June 30 - July 1, 2011. Proceedings</i> , LNCS 6706. Springer, 2011. |
| [63] | Achim D. Brucker, Lukas Brügger, Paul Kearney, and Burkhart Wolff. An approach to modular and testable security models of real-world health-care applications. Proceedings of the ACM Symposium on Access control models and technologies, pages 133-142. ACM, 2011. SACMAT 2011. |
| [64] | Achim D. Brucker, Lukas Brügger, Matthias P. Krieger, and Burkhart Wolff. HOL-TestGen 1.5.0 user guide. Technical Report 670, ETH Zurich, April 2010. |
| [65] | Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff. Unifying Theories in Isabelle/HOL. In <i>Unifying Theories of Programming (UTP2010)</i> , number 6445 in Lecture Notes in Computer Science. Springer-Verlag, Heidelberg, 2010. |
| [66] | Achim D. Brucker, Matthias P. Krieger, Delphine Longuet, and Burkhart Wolff. A Specification-based Test Case Generation Method for UML/OCL. In <i>Proceedings of the Workshop on OCL and Textual Modelling (OCL 2010)</i> , 2010. LNCS 6627. |
| [67] | Matthias P. Krieger, Alexander Knapp, and Burkhart Wolff. Automatic and Efficient Simulation of Operation Contracts. In Eelco Visser, Jaakko Jarvi, and Giorgios Economopoulos, editors, <i>Ninth International Conference on Generative Programming and Component Engineering (GPCE'10)</i> . IEEE Computer Society, 2010. |
| [68] | Achim D. Brucker, Lukas Brügger, Paul Kearney, and Burkhart Wolff. Verified Firewall Policy Transformations for Test Case Generation. <i>Software Testing, Verification, and Validation, 2010 International Conference on</i> , 0:345-354, 2010. |
| [69] | Burkhart Wolff. Top-down vs. Bottom-up: Formale Methoden im wissenschaftlichen Wettbewerb. Ein essayistischer Survey über den Stand der Kunst. Technical report, DFKI Technischer Bericht, 2009. Erschienen in der Festschrift zum 60. Geburtstag von Bernd Krieg-Brückner. |
| [70] | Sascha Böhme, Michal Moskal, Wolfram Schulte, and Burkhart Wolff. HOL-Boogie - An Interactive Prover-Backend for the Verified C Compiler. <i>Journal of Automated Reasoning (JAR)</i> , 44(1-2):111-144, 2009. |
| [71] | Achim D. Brucker and Burkhart Wolff. Semantics, Calculi, and Analysis for Object-Oriented Specifications. <i>Acta Informatica</i> , 46(4):255-284, 2009. |
| [72] | Matthias Daum, Jan Dörrenbächer, and Burkhart Wolff. Proving Fairness and Implementation Correctness of a Microkernel Scheduler. <i>Journal of Automated Reasoning (JAR)</i> , 42(2-4):349-388, 2009. G. Klein, R. Huuck and B. Schlich: Special Issue on Operating System Verification (2008). |
| [73] | Achim D. Brucker and Burkhart Wolff. HOL-TestGen: An Interactive Test-case Generation Framework. In Marsha Chechik and Martin Wirsing, editors, <i>Fundamental Approaches to Software Engineering (FASE09)</i> , LNCS 5503, pages 417-420. Springer-Verlag, Heidelberg, 2009. |
| [74] | Achim D. Brucker, Matthias P. Krieger, and Burkhart Wolff. Extending OCL with null-references. In S. Ghosh, editor, <i>MODELS 2009 Workshops</i> , LNCS 6002, pages 261-275. Springer Verlag, Heidelberg, 2009. Best-Paper Award at the OCL 2009 Workshop. |
| [75] | Matthias Daum, Jan Dörrenbächer, Mareike Schmidt, and Burkhart Wolff. A verification approach for system-level concurrent programs. In <i>Verified Software: Theories, Tools, Experiments</i> , LNCS 5295, pages 161-176. Springer Berlin / Heidelberg, 2008. |
| [76] | Achim D. Brucker and Burkhart Wolff. Extensible universes for object-oriented data models. In Jan Vitek, editor, <i>Proceedings of the European Conference of Object-Oriented Programming (ECOOP 2008)</i> , LNCS 5142, pages 438-462. Springer-Verlag, 2008. |

| | |
|------|--|
| [77] | Sascha Böhme, Rustan Leino, and Burkhart Wolff. HOL-Boogie - An Interactive Prover for the Boogie Program Verifier. <i>21th International Conference on Theorem proving in Higher-Order Logics (TPHOLs 2008)</i> , LNCS 5170. Springer-Verlag, 2008. |
| [78] | Achim D. Brucker and Burkhart Wolff. An Extensible Encoding of Object-oriented Data Models in HOL with an Application to IMP++. <i>Journal of Automated Reasoning (JAR)</i> , Selected Papers of the AVOCS-VERIFY Workshop 2006(3-4):219-249, 2008. |
| [79] | Achim D. Brucker and Burkhart Wolff. A Formal Proof Environment for UML/OCL. In <i>Proceedings of Formal Aspects of Software Engineering (FASE 2008)</i> , LNCS 4961, pages 97-101. Springer Berlin / Heidelberg, 2008. |
| [80] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. Model-based firewall conformance testing. In Kenji Suzuki and Teruo Higashino, editors, <i>Testcom/FATES 2008</i> , LNCS 5047, pages 103-118. Springer-Verlag, Tokyo, Japan, 2008. |
| [81] | Achim D. Brucker, Lukas Brügger, and Burkhart Wolff. Verifying test-hypotheses - an experiment in test and proof. In Bernd Finkbeiner, Yuri Gurevich, and Alexander K. Petrenko, editors, <i>Model-based Testing (MBT) 2008</i> , ENTCS 202, pages 15-28, 2008. Elsevier Science Publishers. |
| [82] | David Basin, Hironobu Kuruma, Shin Nakajima, and Burkhart Wolff. The Z Specification Language and the Proof Environment Isabelle/HOL-Z. <i>Computer Software - Journal of the Japanese Society for Software Science and Technology</i> , 24(2):21-26, April 2007. In Japanese. |
| [83] | David Basin, Hironobu Kuruma, Kunihiko Miyazaki, Kazuo Takaragi, and Burkhart Wolff. Verifying a signature architecture: a comparative case study. <i>Formal Aspects of Computing</i> , 19(1):63-91, March 2007. |
| [84] | Achim D. Brucker, Jürgen Doser, and Burkhart Wolff. An MDA framework supporting OCL. <i>Electronic Communications of the EASST</i> , 5, 2007. |
| [85] | Achim D. Brucker, Jürgen Doser, and Burkhart Wolff. Semantic issues of OCL: Past, present, and future. <i>Electronic Communications of the EASST</i> , 5, 2007. |
| [86] | Achim D. Brucker and Burkhart Wolff. Test-sequence generation with HOL-TestGen - with an application to firewall testing. In Bertrand Meyer and Yuri Gurevich, editors, <i>TAP 2007: Tests And Proofs</i> , LNCS 4454, pages 149-168. Springer-Verlag, 2007. |
| [87] | Makarius Wenzel and Burkhart Wolff. Building formal method tools in the isabelle/isar framework. In Klaus Schneider and Jens Brandt, editors, <i>TPHOLs 2007</i> , LNCS 4732, pages 351-366. Springer-Verlag, 2007. |
| [88] | Achim D. Brucker and Burkhart Wolff. A package for extensible object-oriented data models with an application to imp++. In Abhik Roychoudhury and Zijiang Yang, editors, <i>International Workshop on Software Verification and Validation (SVV 2006)</i> , Computing Research Repository (CoRR). Seattle, USA, August 2006. |
| [89] | Achim D. Brucker and Burkhart Wolff. The HOL-OCL Book. Technical Report 525, ETH Zürich, 2006. |
| [90] | Achim D. Brucker, Jürgen Doser, and Burkhart Wolff. An MDA framework supporting OCL. In <i>6th OCL Workshop at the UML/MoDELS Conference</i> , 2006. |
| [91] | Achim D. Brucker, Jürgen Doser, and Burkhart Wolff. A model transformation semantics and analysis methodology for SecureUML. In Oscar Nierstrasz, Jon Whittle, David Harel, and Gianna Reggio, editors, <i>MoDELS 2006: Model Driven Engineering Languages and Systems</i> , LNCS 4199, pages 306-320. Springer-Verlag, Genova, 2006. An extended version of this paper is available as ETH Technical Report, no. 524. |
| [92] | Achim D. Brucker, Jürgen Doser, and Burkhart Wolff. Semantic issues of OCL: Past, present, and future. In <i>6th OCL Workshop at the UML/MoDELS Conference</i> , 2006. |

| | |
|-------|---|
| [93] | Manuel Núñez García, Klaus Havelund, Grigore Rosu, and Burkhart Wolff, editors. <i>Proceedings of the International Workshop on Formal Aspects of Testing and Runtime Verification (FATES/RV)</i> , Seattle, USA. LNCS 4262, Springer Verlag, 2006. |
| [94] | David Aspinall, Christoph Lüth, and Burkhart Wolff. Assisted Proof Document Authoring. In <i>Fourth International Conference on Mathematical Knowledge Management (MKM 05)</i> , LNCS 3863. Springer Verlag, 2005. |
| [95] | David Basin, Hironobu Kuruma, Kazuo Takaragi, and Burkhart Wolff. Specifying and Verifying Hysteresis Signature System with HOL-Z. Technical Report 471, Computer Security Group, ETH Zürich, 2005. |
| [96] | David Basin, Hironobu Kuruma, Kazuo Takaragi, and Burkhart Wolff. Verification of a Signature Architecture with HOL-Z. In <i>Formal Methods 2005</i> , LNCS 3582, pages 269-285. Springer Verlag, 2005. |
| [97] | Achim D. Brucker and Burkhart Wolff. HOL-TestGen 1.0.0 user guide. Technical Report 482, Computer Security Group, ETH Zürich, April 2005. |
| [98] | Achim D. Brucker and Burkhart Wolff. Interactive Testing using HOL-TestGen. In Wolfgang Grieskamp and Carsten Weise, editors, <i>Formal Approaches to Testing of Software (FATES 05)</i> , LNCS 3997, pages 87-102. Springer-Verlag, 2005. |
| [99] | Achim D. Brucker and Burkhart Wolff. Symbolic test case generation for primitive recursive functions. In Jens Grabowski and Brian Nielsen, editors, <i>Formal Approaches to Testing of Software (FATES 04)</i> , LNCS 3395, pages 16-32. Springer-Verlag, 2005. |
| [100] | Achim D. Brucker and Burkhart Wolff. A verification approach for applied system security. <i>International Journal on Software Tools for Technology Transfer (STTT)</i> , 7(3):233-247, 2005. |
| [101] | Thomas Meyer and Burkhart Wolff. Tactic-based optimized compilation of functional programs. In Jean-Christophe Filliatre, Christine Paulin, and Benjamin Werner, editors, <i>Types for Proofs and Programs (TYPES 2004)</i> , LNCS 3839, pages 202-215. Springer Verlag, 8 2005. |
| [102] | Burkhart Wolff. Correct tools for formal methods in software engineering, Habilitationsschrift. Ludwig-Maximilian Universität Freiburg, 2005. |
| [103] | Achim D. Brucker and Burkhart Wolff. Symbolic test case generation for primitive recursive functions. Technical Report 449, Computer Security Group, ETH Zürich, jun 2004. |
| [104] | Nicole Rauch and Burkhart Wolff. Formalizing java's two's-complement integral type in isabelle/hol. Technical Report 458, ETH Zürich, 11 2004. |
| [105] | Achim D. Brucker, Frank Rittinger, and Burkhart Wolff. HOL-Z 2.0: A Proof Environment for Z-Specifications. <i>Journal of Universal Computer Science</i> , 9(2):152-172, February 2003. |
| [106] | David Basin and Burkhart Wolff, editors. <i>Theorem Proving in Higher Order Logics, 16th International Conference (TPHOLs 2003)</i> , LNCS 2758. Springer-Verlag, Sep 2003. |
| [107] | Achim D. Brucker and Burkhart Wolff. Using theory morphisms for implementing formal methods tools. In Herman Geuvers and Freek Wiedijk, editors, <i>Types 2002, Proceedings of the workshop Types for Proof and Programs</i> , LNCS 2646. Springer-Verlag, 2003. |
| [108] | Achim D. Brucker and Burkhart Wolff. A case study of a formalized security architecture. In Thomas Arts and Wan Fokkink, editors, <i>Eighth International Workshop on Formal Methods for Industrial Critical Systems (FMICS'03)</i> , volume 80. Elsevier Science Publishers, 2003. |
| [109] | Nicole Rauch and Burkhart Wolff. Formalizing java's two's-complement integral type in isabelle/hol. In <i>Electronic Notes in Theoretical Computer Science</i> , volume 80. Elsevier Science Publishers, 2003. |

| | |
|-------|---|
| [110] | Achim D. Brucker, Frank Rittinger, and Burkhart Wolff. The CVS-server case study: A formalized security architecture. In Dominik Haneberg, Gerhard Schellhorn, and Wolfgang Reif, editors, <i>FM-TOOLS 2002</i> , number 2002-11 in Technical Report, pages 47-52. Augsburg, July 2002. |
| [111] | Achim D. Brucker, Stefan Friedrich, Frank Rittinger, and Burkhart Wolff. HOL-Z 2.0: A proof environment for z-specifications. In Dominik Haneberg, Gerhard Schellhorn, and Wolfgang Reif, editors, <i>FMTOOLS 2002</i> , number 2002-11 in Technical Report, pages 33-38. Augsburg, July 2002. |
| [112] | Achim D. Brucker, Frank Rittinger, and Burkhart Wolff. A CVS-Server security architecture - concepts and formal analysis. Technical Report 182, Albert-Ludwigs-Universität Freiburg, 2002. |
| [113] | Achim D. Brucker and Burkhart Wolff. HOL-OCL: Experiences, consequences and design choices. In Jean-Marc Jézéquel, Heinrich Hussmann, and Stephen Cook, editors, <i>UML 2002: Model Engineering, Concepts and Tools</i> , LNCS 2460. Springer-Verlag, 2002. |
| [114] | Achim D. Brucker and Burkhart Wolff. A proposal for a formal OCL semantics in Isabelle/HOL. In <i>Theorem Proving in Higher Order Logics (TPHOLS)</i> , LNCS 2410, pages 99-114. Springer-Verlag, 2002. |
| [115] | Burkhart Wolff, Oliver Berthold, Sebastian Clauß, Hannes Federrath, Stefan Köpsell, and Andreas Pfitzmann. Towards a formal analysis of a mix network. Technical Report 171, Albert-Ludwigs-Universität Freiburg, 2002. |
| [116] | Achim D. Brucker and Burkhart Wolff. Testing distributed component based systems using UML/OCL. In K. Bauknecht, W. Brauer, and Th. Mück, editors, <i>Informatik 2001</i> , volume 1 of <i>Tagungsband der GI/ÖCG Jahrestagung</i> , pages 608-614, Wien, November 2001. Österreichische Computer Gesellschaft. |
| [117] | Achim D. Brucker and Burkhart Wolff. Checking OCL Constraints in Distributed Systems Using J2EE/EJB. Technical Report 157, Albert-Ludwigs-Universität Freiburg, July 2001. |
| [118] | Christoph Lüth and Burkhart Wolff. sml_tk: Functional programming for guis - reference manual. Technical Report 158, Albert-Ludwigs-Universität Freiburg, July 2001. |
| [119] | Burkhart Wolff. Verifying explicit substitution calculi in binding structures with effect binding. In Pierre Lescanne, editor, <i>Workshop on Explicit Substitution Theory and Applications (WESTAPP'01)</i> , volume 210 of <i>Logic Group Preprint Series</i> , pages 58 - 71. Department of Philosophy - Utrecht University, May 2001. |
| [120] | T. Meyer and Burkhart Wolff. Correct code-generation in a generic framework. In M. Aargaard, J. Harrison, and T. Schubert, editors, <i>TPHOLS 2000: Supplemental Proceedings</i> , OGI Technical Report CSE 00-009, pages 213-230. Oregon Graduate Institute, Portland, USA, July 2000. |
| [121] | David Basin, Luca Viganò, and Burkhart Wolff. Berichte aus den Instituten: Lehrstuhl für Softwaretechnik und Softwareproduktionsumgebung, Freiburg. <i>PIK (Praxis der Informationsverarbeitung und Kommunikation)</i> , 23(4):248-249, 2000. |
| [122] | Christoph Lüth and Burkhart Wolff. More about TAS and IsaWin: Tools for formal program development. In T. Maibaum, editor, <i>Fundamental Approaches to Software Engineering FASE 2000. Joint European Conferences on Theory and Practice of Software ETAPS 2000</i> , LNCS 1783, pages 367- 370. Springer Verlag, 2000. |
| [123] | Christoph Lüth and Burkhart Wolff. TAS - a generic window inference system. In J. Harrison and M. Aagaard, editors, <i>Theorem Proving in Higher Order Logics(TPHOLS)</i> , LNCS 1869, pages 405-422. Springer Verlag, 2000. |
| [124] | Christoph Lüth and Burkhart Wolff. Functional design and implementation of graphical user interfaces for theorem provers. <i>Journal of Functional Programming</i> , 9(2):167- 189, 1999. |

| | |
|-------|---|
| [125] | Christoph Lüth, Einar W. Karlsen, Kolyang, Stefan Westmeier, and Burkhart Wolff. HOL-Z in the UniForM-Workbench - a case study in tool integration for z. In J. Bowen, editor, <i>11. International Conference of Z Users ZUM'98</i> , LNCS 1493, pages 116-134. Springer Verlag, 1998. |
| [126] | C. Lüth, E. W. Karlsen, Kolyang, S. Westmeier, and B. Wolff. Tool integration in the uniform workbench. In Berghammer and Hoffmann, editors, <i>Workshop on Tool Support for System Specification, Development, and Verification</i> , 1998. |
| [127] | Haykal Tej, Christoph Lüth, and Burkhart Wolff. Generic transformational program development. Unpublished Paper., 1998. |
| [128] | Kolyang, C. Lüth, T. Meier, and B. Wolff. Tas and isawin: Generic interfaces for transformational program development and theorem proving. In M. Dauchet M. Bidoit, editor, <i>TAPSOFT 97: Theory and Practice of Software Development</i> , LNCS 1214, pages 855-858. Springer Verlag, 1997. |
| [129] | Kolyang, C. Lüth, T. Meier, and B. Wolff. Generic interfaces for transformation systems and interactive theorem provers. In B. Buth K. Berghammer, J. Peleska, editor, <i>Proceedings of the "International Workshop for Tool Support in Verification and Validation"</i> , BISS Monographs. Shaker Verlag, 1997. |
| [130] | H. Tej and B. Wolff. A corrected failure-divergence model for CSP in Isabelle/HOL. In J. Fitzgerald, C.B. Jones, and P. Lucas, editors, <i>Proceedings of the FME 97</i> , LNCS 1313, pages 318-337. Springer Verlag, 1997. |
| [131] | B. Wolff. <i>A Generic Calculus of Transformations</i> . PhD thesis, Universität Bremen, Aachen, 1997. |
| [132] | Kolyang, C. Lüth, T. Meier, and B. Wolff. Generating graphical user-interfaces in a functional setting. In N. Merriam, editor, <i>Proceedings of the User Interfaces for Theorem Provers (UITP 96)</i> , Technical Report. University of York, 1996. |
| [133] | Kolyang, T. Santen, and B. Wolff. Correct and user-friendly implementation of transformation systems. In M.-C. Gaudel and J. Woodcock, editors, <i>FME 96 - Industrial Benefits and Advances in Formal Methods</i> , LNCS 1051, pages 629-648. Springer Verlag, 1996. |
| [134] | Kolyang, T. Santen, and B. Wolff. A structure preserving encoding of z in Isabelle/HOL. In J. von Wright, J. Grundy, and J. Harrison, editors, <i>Theorem Proving in Higher Order Logics - 9th International Conference</i> , LNCS 1125, pages 283-298. Springer Verlag, 1996. |
| [135] | C. Lüth, S. Westmeier, and B. Wolff. sml_tk: Functional programming for graphical user interfaces. Technical Report 8/96, Universität Bremen, 1996. |
| [136] | B. Krieg-Brückner, J. Liu, H. Shi, and B. Wolff. Towards correct, efficient and re-usable transformational developments. In M. Broy and S. Jähnichen, editors, <i>KORSO - Methods, Languages, and Tools for the Construction of Correct Software</i> , LNCS 1009, pages 270-284. Springer Verlag, 1995. |
| [137] | Kolyang and B. Wolff. Development by refinement revisited: Lessons learnt from an example. In G. Snelting, editor, <i>Beiträge der GI-Fachtagung "Softwaretechnik 95"</i> , Braunschweig, Mitteilungen der Fachgruppen 'Software Engineering' und 'Requirements-Engineering', Band 15, Heft 3, ISSN 0720-8928, pages 57-66. GI, 1995. |