Priv-Doz Dr. Burkhart Wolff

bwolff@inf.ethz.ch
www.infsec.ethz.ch/people/wolffb
Haldeneggsteig 4
ETH-Zentrum, IFW C 46.1
CH-8092 Zürich
Telefon: +41 763231828

Mesdames et Messieurs,

ici je déclare formellement ma candidature à la qualification aux fonctions de professeur.

Burkhart Wolff

Ci-joint:

- CV
- Descriptif des activités d'enseignement, motivations
- Descriptif des thèmes de recherche et des résultats
- Descriptif des charges collectives assumées

Curriculum Vitae

12.11.1962	Né à Braunschweig, Niedersachsen, Allemagne.
1969	École élémentaire à Vienenburg, Niedersachsen.
1982	Baccalauréat. (Dégrée 1,8)
1982-83	Stage en France, cours de français à l'Alliance Française et un cours semestriel à la Sorbonne «Civilisation Française». (Dégrée: bien)
1983-90	Études de l'Informatique á l'Université Technique de Berlin. Diplôme (*Une Analyse de Sharing dans les Langues Applicatives*. Dégrée: très bien)
1991-1997	Doctorat dans la groupe de Prof. B. Krieg-Brückner à l'Université Bremen.
1997	Dissertation: «A Generic Calculus of Transformations». Supervisé par Prof. Bernd Krieg-Brückner et Prof. Tobias Nipkow. (Dégrée: Magna cum laude)
Oct. 1997	Assistant de recherche (Post-doc) dans la groupe de Prof. D. Basin à l'Université de Freiburg i. Brsg., Allemagne.
Sept. 2003	Conférence internationale on Theorem Proving in Higher-Order Logics (TPHOLs). Chair: D. Basin, B. Wolff
2004-2007	«Oberassistent» à la Eidgenössische Technische Hochschule (ETH), Zürich.
Julie 2005	Habilitation à l'Université Freiburg. Venia Legendi pour „Informatique“.
Sept. 2006	Conférence internationale de „Formal Aspects of Testing and Runtime-Verification“ (FATES/RV).Chair: B. Wolff, M. Munez, N. Klarlund, G. Rosu.

Avril 2007 – Sept. 2007: Rechercheur invité á Microsoft Research, Redmond, USA. (Sabattical de la ETH)

Dès Dec. 2007	«Privatdozent» dans la groupe d' architecture des ordinateurs (dirigé par Prof. Wolfgang Paul) à l'Université de Saarbrücken. (Projet Verisoft, Sous-projet: Verification du logiciel «Hyper-V», un environnement de virtualisation de Microsoft).

Descriptif des activités d'enseignement:

Vision générale:
Dans les dernières années, on peut constater un certain tendance de négliger des techniques des base, plus notamment dans la domaine de programmation et des méthodes formelles. Je considère l'adaptation de Java comme langage première dans les curriculums d'une grande partie des universités du monde responsable pour ce déclin, au moins en partie. *It's all about programming*, c'est le trend globale, qui a des résultats suivantes:

1) les exigences en mathématiques dans les curriculums de l'informatique se diminuent.
2) le développement des aptitude de programmation dans plusieurs langages est réduit en faveur des approaches des cahier de recettes (*cookbook approaches*) utilisant des bibliothèques de code et de *packages spéciales.*
3) La collections capacités acquissent pendant est insuffisant pour l'industrie du logiciels d'aujourd'hui, en particulier pour établir *safety* et *security* des systèmes critiques. Malheureusement, ça coïncide avec le tendance industrielle de *outsourcing*; Nous enseignent de plus en plus des professionnels qui sont facilement à remplacer.

Ces trends sont visible, par exemple, dans les *curriculum recommendations* de l'*Association for Computing Machinery* (ACM). Le curriculum 2005 ne mentionne des capacités mathématiques pas du tout, et mentionne seulement *une* cours dans la théorie des langages de programmation [1]. Grandes institutions de recherche en Europe (comme le ETH) suivent ce trend. En Allemagne, dans la volonté de s'adapter au standard de Bologne, une grande partie des universités a abolit le Diplôme classique et l'a remplacé par les curriculums Bachelor/Master plus courtes; normalement, les raccourcissement nécessaires sont appliques dans les domaines de théorie de base.

En même temps, dans la réalite du vie professionnelle en académia où en industrie, il y a de plus en plus des exigences de travailler en *team*, qui est très souvent une équipe globalisé. En résultat, l'entrâinement de l'anglais et des *soft skills* d'organiser des groupes sont de plus en plus importants.

Mon idéal de l'enseignement d'informatique est de trouver une bonne balance entre les fondations mathématiques d'un part et les applications d'autre part. Pour établir un bon lien entre les deux, il faut obtenir une dégrée d'expérience sur les deux domaines, qui est, de mon avis, un des problèmes principales dans l'enseignement notre discipline d'ingénieur. (En différence avec l'électrotechnique, qui a une structure ressemblante, c'est plutôt la mathématique discrète et la logique qui est important; étant donné que ces domaines de la mathématique „moderne“ sont pas tellement représentées dans les curriculums scolaires, ça représente des problèmes spécifiques pour l'enseignement de l'informatique universitaire).

Comment peut-on réaliser
Ich bin seit Langem an neuen computer-gestützten Lehrtechniken interessiert. Zusammen mit David Basin habe ich einen interaktiven Lehrkurs für das Gebiet “Theorembeweisen und seine Anwendungen in der Informatik” entwickelt (Hoare-Kalküle, verifizierte Verification Condition Generators, Programm-Entwicklung durch Verfeinerung, etc.). Das resultierende “interaktive Buch” besteht aus 1200 animierten Folien, die den Bereich von Logik-Grundlagen über automatische Deduktionstechniken bis hin zu Anwendungen abdecken. Der Kurs enthält auch 50 Übungen einschließlich Lösungen für einen modernen interaktiven Beweiser.
An der ETH Zürich und der Uni Freiburg bin ich zudem in vielfältige Lehrveranstaltungen

involviert gewesen (zumeist in englischer Sprache). Dies umfasst Lehrveranstaltungen aus den Gebieten Softwaretechnik, Semantik von Programmiersprachen, Programmieren in C, Theorembeweisen, Verfeinerung als auch Systematischer Test von Soft- und Hardware. Eine detaillierte Liste der Lehrveranstaltungen findet sich im Anhang.

Teaching at ETH Zürich

- Computer-supported Modelling and Reasoning WS 2006. „Prüfungsberechtigt“. (see http://www.infsec.ethz.ch/education/permanent/csmr).
- Computer-supported Modelling and Reasoning WS 2004 „Prüfungsberechtigt“. (see http://www.infsec.ethz.ch/education/permanent/csmr).
- Programmieren in C++ for Physics. (under Heino Gärtner). WS 2005.
- Diskrete Mathematik SS 2004 (under Prof. Ueli Maurer).

All these lectures and assistances have been regularly evaluated by the ETH (result: between good and very good).

Teaching at Freiburg

- Softwarearchitekturen (WS-00, lecture together with David Basin).
- Programmentwicklung durch Verfeinerung (SS-99; seminar together with Georg Struth).
- Softwaretechnik I (SS-98, SS-99, SS-00, SS-02; lecture together with David Basin).
- Softwaretechnik II (WS 99; lecture together with David Basin, Abdel Ayari, Stefan Friedrich).
- Testen von Soft- und Hardware (WS-98, seminar together with C.Scholl).

The lectures and assistances have been regularly evaluated by the Universität Freiburg (result: between good and very good.).

(Co-)Supervision of Phds

- Lukas Brügger (ETH Zürich, commencé Sept. 2007)
- Achim Brucker (ETH Zürich, finished Feb. 2007):
  An Interactive Proof Environment for Object-Oriented Specifications.
- Thomas Meyer (Universität Bremen, 2005):
  A Framework for Formal Representation and Transformational Optimization of Executable Specifications.

- Haykal Tej (Universität Bremen, 2003):
  CSP in Isabelle/HOL.

Title of Course	Year	Abstract	Created by me:	Level Students	Number Students
Software Engineering I	98,99, 00, 02	Standard Course in SE with some Formal Methods	30 %	5-7 sem.	100
Software Engineering II	W 99	Course on FM Tools in SE	25 %	6 sem.	40
Software Architectures	W 00	Seminary	50 %	5 sem.	20
Testing	W 98	Seminary	50 %	5 sem.	30
Computer-supported Modelling & Reasoning	... W 06	Logic Foundations and Theorem Proving	100%	5 sem.	10
Programming in C	W 05	Programming Course for Electical Engineers	5 %	1 sem.	200
Discrete Mathematics	W 04	Standard Course, Focus on Cryptography	5 %	3 sem.	150

[1] Joint Taskforce for Computing Curricula. “Computing Curricula 2005: The Overview Report.” ACM/AIS/ IEEE, 2005 <www.acm.org/education /curric_vols/CC2005-March06 Final.pdf>.

Descriptif des thèmes de recherche et des résultats:

Vision générale:
Mes intérêts dans la recherche se concentrent dans la domaine de la modélisation et validation dans certains procédés de construction du logiciel (en particulier dans «Model-driven engineering» (MDE)). Domaines de l'applications de ces techniques sont:

- des langages de programmation et de spécification
- la sécurité des systèmes
- les architectures des ordinateurs (plus récent).

Les techniques de validation sont basées sur la vérification formelle et des tests generés automatiquements de ces modèles. Dans la coté pratique, cela à résulté dans plusieurs logiciels --- basées sur des systèmes de preuve automatiques ou interactives --- supportant des procédé de construction de logiciel pendant le design et la validation.

Liste de mes projets (description thématique):

- En 2007, étais "invited researcher" dans la groupe FSE dirigé par Dr. Wolfram Schulte à Microsoft Research, Redmond, USA. Le projet de recherche poursuivi dans ce séjours était défini comme suivant: intégrer le système de preuve Isabelle/HOL dans le système de vérification de code, nommé *Boogie*, pour ajouter un moyen de preuve interactive pour des obligation de preuve résultant d'un programme en Spec# ou C annoter par des formules de la logique de premier ordre. Ce méthode peut être convenant si les systèmes de preuves automatiques (comme *simplify* ou *Z3*) n'arrive pas à trouver la preuve. Résultats du projet: 1) un système prototypique, nommé *HOL-Boogie*, qui peut être utiliser comme «back-end» interactive pour Boogie, 2) une vérification exemplaire d'un problème algorithmique (où les systèmes de preuve automatiques sont échoué) et 3) une modèle de mémoire pour le langage C avec une preuve formelle de son consistance.
  Le développement de HOL-Boogie va continuer dans le cadre du projet national VeriSoft (BMBF) dans une coopération avec l'université de München (Prof. Tobias Nipkow).

- De 2004-2007, j'ai dirigé le projet «Formal Testing Techniques» (Projet interne ETH 17301). Avec Achim Brucker, j'ai développé le système semi-automatique *HOL-TestGen* pour la génération des données de test à la base d'une spécification du système à tester. Le système, basée sur Isabelle/HOL, décompose la spécification dans une collection de formules (contraints) pour lesquelles des modèles satisfaisantes sont construites par une combinaison de techniques de résolution des contraints et une technique de test par des données randomisées. Le système génère automatiquement un logiciel («test driver») qui poursuit le test du logiciel spécifiée. Résultats: 1) Le système, 2) plusieurs études de cas substantielles, comme le test systématique d'une *Firewall*, et 3) une séries de publications présentées dans plusieurs publications dans des conférences internationales. En plus, *HOL-TestGen* a été présenté dans une «Tutorial» sur la conférence TestCom en 2007. Au présent, Lukas Brugger continue a développer HOL-TestGen, sous ma supervision: Une version future sera intégré dans le système HOL-OCL, ouvrant la possibilité de générer des données de test d'une spécification en UML.

- De 2002-2007, j'ai dirigé le projet «Modélisation et Vérification en UML/OCL» (HOL-OCL), conduit par Achim Brucker. (Ce projet était au début financée par la compagnie Interactive Objects, Freiburg, et plus tard le projet interne ETH 17305). La motivation était de formaliser la sémantique de la langage objet-orienté UML/OCL et de l'implémenter dans Isabelle/HOL dans une manière efficace. Sur le modèle sémantique, le premiers calculs était développer formellement (en Isabelle). Sur cette base, on a réalisé une groupe de procédures de décision sous forme des *tactics* pour cette langage. Le but finale de ce projet, c'est 1) développer support (??) semi-automatique pour des raffinements des modèles d'objets (jusqu'à ce que la génération de code est possible) et 2) de développer des données de test de ces modèles, en particulier pour valider des modèles pour «legacy» sous-systèmes. Le résultat de ce projet, c'est 1) l'implémentation et la documentation extensive sur www.brucker.ch/projects/holocl, 2) une méthode de générer automatiquement des modèles d'objets consistents, 3) une série d'exemples, et 4) une série de publications dans plusieurs conférences internationales et une dans une journal.

- Dans les années 2005-2006, j'ai dirigé le sous-projet «SecureUML in HOL-OCL», conduit par Jürgen Doser dans le cadre du EU-IP «TrustCoM» (http://www.eu-trustcom.com/, ETH 13581). Le but était d'augmenter l'environnement de preuve HOL-OCL par une environnement MDE avec *model repository*, un système de transformations de modèles, et des générateurs de code. Le résultat était, comme étude de cas, l'implémentation de SecureUML, un dialecte de UML qui permets d'annoter des classes et des objectes avec des contraints de sécurité, c'est à dire des droits d'accès de certains objets par des opérations du système. Par des transformations des modèles, ces annotations sont transformés dans des contraints supplémentaires qui règlent l'accès des objectes; des transformations finales résultent dans la génération du code. Les transformations dérivent aussi des obligations de preuves; si ces obligations sont prouvé dans HOL-OCL, la construction garantit que le système «gardé» aie la même fonctionnalité que la système originale pourvu que les droits de permissions soient suffisantes. Il y avait plusieurs publications dans des conférences internationales et une dans un journal.

- Dans les années 1999 – 2002, étais co-initiateur et co-dirigeant du projet «Formale Sicherheitsarchitekturen» (architectures formelles de sécurité). La motivation consiste de prouver --- par une raffinement formelle --- qu'une système avec une *security policy* intégré soit implémenté correctement par l'architecture de l'implémentation (c'est à dire, un système d'exploitation, par exemple) avec ses mécanismes de sécurité. Comme contribution pour ce projet, j'ai développé l'environnement de preuve HOL-Z qui permets de modéliser les deux systèmes dans la langage Z et de réaliser des preuve de raffinement entre les deux spécifications. Dans le cadre du projet, on a réalisé une étude de cas nommé *CVS-Server*, une système de versionnement configurée pour réaliser *role-based acces control*, qui était implémenté par le modèle d'accès réalisé par UNIX/POSIX. Récemment, j'ai conduit une autre étude de cas substantielle, poursuivant la même méthodologie, pour un système de signatures; cette étude était payé par HITACHI. Des résultats sont 1) le système HOL-Z (www.brucker.ch/projects/hol-z/), 2) des preuves formelles pour ces études de cas, et 3) une série de publications, parmi eux 3 articles de journaux.

Liste de mes projets (description organisatrice):

- SUML-HMS (payé par British-Telecom).
  Motivation: Génération des cas de test pour des spécifications en UML/OCL.
  Rôle: initiateur, superviseur du doctorat de Lukas Brügger (ETH). Budget 360000 CHF.
  Début Sept. 2007.

- EU IP: 'A Trust and Contract Management Framework for dynamic Virtual Organizations' (TrustCoM) (http://www.eu-trustcom.com/).
  Motivation: analyser la sécurité dans *web-based services utiliser* de réaliser des organisations virtuelles.
  Rôle: directeur locale du sous-projet à la ETH Zürich, *senior researcher*. Budget: 600000 CHF. 2003 – 2007.

- Projet: 'Secure Platform HDA' (payé par Hitachi):
  Modélisation et vérification d'un système de signature digitales.
  Rôle: *senior researcher*. Budget: 50000 CHF. 2004-2007.

- BMBF Verbundprojekt: 'MultiMedia-Instruktionen in Sicheren Systemen' (MMISS).
  Motivation: explorer des moyens d'enseignement par des systèmes de multimédia.
  Budget(total): 5700000 DM. Freiburg: 418.088 DM. Rôle: auteur du matériel d'enseignement. 2001-2004. Résultat: le livre interactive «Computer-supported modeling and reasoning», http://www.infsec.ethz.ch/education/permanent/csmr.

- EU-IST Working Group: 'Computer-Assisted Reasoning Based on Type Theory (TYPES)'.
  Motivation: collaboration européen de recherche sur des système de preuve d'ordre supérieure.
  Budget(total): 370000 EUR. Rôle: auteur, administrateur pour Freiburg. 1999 -2003.

- DFG Projekt: 'Formale Sicherheitsarchitekturen: Sicherheit durch formale Methoden in den Software-Entwurfsphasen.'
  Motivation: prouver --- par une raffinement formelle --- qu'une système avec une *security policy* intégré soit implémenté correctement par un autre proche du système d'exploitation. Budget (total) 480000 DM. Rôle: co-initiateur, co-superviseur of F. Rittinger (Phd). 2000-2002.

- Interactive Objects GmBH, Freiburg: 'Formal Methods for Distributed Object Systems' (CSFMDOS).
  Motivation: Développer un système de preuve pour UML/OCL.
  Budget: 150000€. Rôle: co-initiateur, et superviseur de A. Brucker. 2001-2003.

Descriptif des charges collectives assumées

A part de mes charges décrit dans le cadre de mes activités d'enseigement et a part des charges administratives prises dans le cadre de mes projets, voilà une liste des committées scientifiques dont j'ai appartenu:

- '21th. Intl. Conference on Theorem Proving in Higher-Order Logics'.(TPHOLs 2008)
- International Conference on Testing of Communicating Systems and Formal Approaches to Testing of Software (TestCom-Fates 2008).
- Test and Proof (TAP 2008).
- International Workshop Ocl4All, Dresden 2007.
- 19th IFIP International Conference on Testing Communication Systems and 7th International Workshop on Formal Approaches to Testing (TESTCOM-FATES07)
- '20th. Intl. Conference on Theorem Proving in Higher-Order Logics'.(TPHOLs 2007)
- Workshop OCL for Models in Multiple Application Domains, 2006.
- Conference Chair du '6th International Workshop on Formal Approaches to Testing and Runtime Testing' FATES/RV2006, 15/16Aug. 2006, Seattle, USA.
- '5th International Workshop on Formal Approaches to Testing' (FATES2005).
- SimSafe 2005.
- '18th. Intl. Conference on Theorem Proving in Higher-Order Logics'.(TPHOLs)
- '17th. Intl. Conference on Theorem Proving in Higher-Order Logics'.(TPHOLs)
- 'User Interfaces for Theorem Provers' (UITP 2005).
- Conference Chair de '16th. Intl. Conference on Theorem Proving in Higher-Order Logics' (TPHOLs 2003), Aug. 2003, Rome, Italy.
- Workshop 'User Interfaces for Theorem Provers' (UITP 2003).
- J'appartient au *steering committee* de la GI-Fachgruppe 'Formale Methoden und Software Engineering für Sichere Systeme'.

En plus, voici une liste des conférences où j'étais choisi comme rapporteur pour des publications:

- Formal Methods (FM 2008)
- Conference of Automated Deduction (CADE 2007).
- Formal Methods (FM 2005).
- 12th International Conference on Logic for Programming Artificial Intelligence and Reasoning (LPAR 05).
- Foundations of Software Science and Computation Structures (FOSSACS 05).
- 2nd IEEE International Conference on Software Engineering and Formal Methods (SEFM 04).
- Third International Conference on Quality Software (QSIC 2003).

- Frontieres in Combining Systems (FroCoS 1998, 2000).
- Theorem Proving in Higher-Order Logics (TPHOLs, since 1998).
- Formal Methods Europe (FME 2000, 2002, 2005).

Dans la dissertation de Rimvydas Rukas (Åbo Akademi University, Finlande, 2004): *Formal Development of Concurrent Components* j'étais chargée avec le rôle du rapporteur externe.