Report for the Research Assessment Computer Science
2003–2008

iCIS

August 21, 2009
# Contents

List of abbreviations 6  
Preface 7  

**Part A** 8  

A Institute for Computing and Information Sciences 11  
A.0 Documentation regarding the level of the institute 11  
A.1 Mission statement 11  
A.2 Leadership 11  
  A.2.1 Organization and managerial style of iCIS 11  
  A.2.2 Rearrangement into sections 12  
  A.2.3 Chairs and principal investigators 13  
  A.2.4 Reflection on the organizational changes 14  
A.3 Strategy and Policy 15  
  A.3.1 Research vision 15  
  A.3.2 Mission 15  
  A.3.3 Strategy 16  
A.4 Researchers and Other Personnel 21  
  A.4.1 Strategic alliances 23  
A.5 Resources, Funding and Facilities 24  
  A.5.1 Direct funding and research funds 24  
  A.5.2 Facilities 24  
A.6 Processes in Research, Internal and External Collaboration 25  
  A.6.1 Research environment 25  
  A.6.2 Teaching and research 26  
  A.6.3 Internal collaboration 26  
  A.6.4 External collaboration 27  
A.7 Academic Reputation 27  
A.8 Internal Evaluation 28  
A.9 External Validation 28  
  A.9.1 Previous external evaluation 28  
  A.9.2 Contributions to society 28  
A.10 Overview of the Results 29  
A.11 Analysis, Perspectives and Expectations 30  
  A.11.1 Strengths 30  
  A.11.2 Weaknesses 31  
  A.11.3 Opportunities 31  
  A.11.4 Threats 32  
  A.11.5 Analysis 32  
  A.11.6 Adjusted goals 33
A.11.7 Adjusted strategy .................................................. 33

Part B ................................. 39

B.1 Digital Security ................................................. 41
   B.1.1 Leadership ....................................................... 41
   B.1.2 Strategy and Policy ............................................. 42
      B.1.2.1 Software security and correctness .......................... 43
      B.1.2.2 Identity-centric security, privacy & search .................. 45
      B.1.2.3 Valorisation and outreach .................................. 46
   B.1.3 Processes in Research, Internal and External Collaboration .... 47
   B.1.4 Academic Reputation .......................................... 49
   B.1.5 Internal Evaluation ........................................... 50
   B.1.6 External Validation ........................................... 50
   B.1.7 Researchers and Other Personnel ................................ 50
   B.1.8 Resources, Funding and Facilities ................................ 52
      B.1.8.1 Resources and funding ....................................... 52
      B.1.8.2 Facilities ...................................................... 52
   B.1.9 Overview of the Results .......................................... 53
   B.1.10 Analysis, Perspectives and Expectations ......................... 53
   B.1.11 Publications ................................................... 57

B.2 Intelligent Systems ............................................. 81
   B.2.1 Leadership ....................................................... 81
   B.2.2 Strategy and Policy ............................................. 82
      B.2.2.1 Proof Assistants Group ..................................... 83
      B.2.2.2 Mind-Brain-Mindfulness Group .............................. 87
      B.2.2.3 Machine Learning Group ...................................... 89
   B.2.3 Processes in Research, Internal and External Collaboration .... 92
   B.2.4 Academic Reputation .......................................... 94
   B.2.5 Internal Evaluation ........................................... 96
   B.2.6 External Validation ........................................... 96
   B.2.7 Researchers and Other Personnel ................................ 97
   B.2.8 Resources, Funding and Facilities ................................ 99
      B.2.8.1 Resources and funding ....................................... 99
      B.2.8.2 Facilities ...................................................... 99
   B.2.9 Overview of the Results .......................................... 99
   B.2.10 Analysis, Perspectives and Expectations ......................... 100
   B.2.11 Publications ................................................... 104

B.3 Model-Based System Development ................................ 123
   B.3.1 Leadership ....................................................... 123
   B.3.2 Strategy and Policy ............................................. 124
      B.3.2.1 History and Context .......................................... 124
      B.3.2.2 Research Focus .............................................. 125
      B.3.2.3 Characteristics ............................................... 126
      B.3.2.4 Basic Techniques ............................................. 126
         T.1 Computer-aided verification and analysis ...................... 127
         T.2 Probabilistic graphical models .................................. 129
         T.3 Model-based application generation ........................... 130
         T.4 Conceptual modeling ............................................. 131
   B.3.2.5 Application Areas ............................................. 132
   A.1 Embedded and distributed systems .................................. 132
## List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AiA</td>
<td>AiA Software Nijmegen</td>
</tr>
<tr>
<td>BCI</td>
<td>Brain-Computer Interfacing</td>
</tr>
<tr>
<td>CWI</td>
<td>Centrum voor Wiskunde en Informatica (Center for Mathematics and Computer Science), Amsterdam</td>
</tr>
<tr>
<td>CYCRIS</td>
<td>Centre for Cybercrime Studies</td>
</tr>
<tr>
<td>CSF</td>
<td>Cerebrospinal fluid</td>
</tr>
<tr>
<td>DS</td>
<td>Section Digital Security of iCIS</td>
</tr>
<tr>
<td>EURYI</td>
<td>European Young Investigator Awards</td>
</tr>
<tr>
<td>ESI</td>
<td>Embedded Systems Institute (Eindhoven)</td>
</tr>
<tr>
<td>EE</td>
<td>Enterprise Engineering</td>
</tr>
<tr>
<td>FES</td>
<td>Fonds Economische Structuurversterking</td>
</tr>
<tr>
<td>FNWI</td>
<td>Faculty of Science of the Radboud University</td>
</tr>
<tr>
<td>Fnds</td>
<td>Former department Foundations, now part of IS</td>
</tr>
<tr>
<td>FMICS</td>
<td>Formal Methods for Industrial Critical Systems</td>
</tr>
<tr>
<td>IWWR</td>
<td>Institute for Water and Wetland Research, a research institute of FNWI</td>
</tr>
<tr>
<td>IFL</td>
<td>Information Foraging Lab</td>
</tr>
<tr>
<td>ISIS</td>
<td>Institute for Science, Innovation and Society, a research institute of FNWI</td>
</tr>
<tr>
<td>IRUN</td>
<td>International Research Universities Network</td>
</tr>
<tr>
<td>IPA</td>
<td>Institute for Programming research and Algorithmics, a Dutch research school</td>
</tr>
<tr>
<td>iCIS</td>
<td>Institute for Computing and Information Sciences</td>
</tr>
<tr>
<td>IS</td>
<td>Section Intelligent Systems of iCIS</td>
</tr>
<tr>
<td>IRIS</td>
<td>Former department of Information and Knowledge Systems, split up between DS, IS and MBSD</td>
</tr>
<tr>
<td>ITA</td>
<td>Former department Informatics for Technical Applications, now part of MBSD</td>
</tr>
<tr>
<td>IMAPP</td>
<td>Institute for Mathematics, Astrophysics and Particle Physics, a research institute of FNWI</td>
</tr>
<tr>
<td>LaQuSo</td>
<td>Laboratory for Quality of Software, a cooperation with the Technical University Eindhoven</td>
</tr>
<tr>
<td>MBSD</td>
<td>Section Model-Based System Development of iCIS</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>NCMLS</td>
<td>Nijmegen Centre for Molecular Life Sciences, a research institute of the RU, a collaboration of RUMC and FNWI</td>
</tr>
<tr>
<td>Nuffic</td>
<td>Netherlands Organization for International Cooperation in Higher Education</td>
</tr>
<tr>
<td>NWO</td>
<td>Netherlands Organization for Scientific Research</td>
</tr>
<tr>
<td>NAF</td>
<td>Netherlands Architecture Forum</td>
</tr>
<tr>
<td>OCW/EZ</td>
<td>Department of Education, Culture and Science and of Economic Affairs</td>
</tr>
<tr>
<td>OBP</td>
<td>Opleidings- en Begeleidingsplan (Training and Guidance Plan)</td>
</tr>
<tr>
<td>PI</td>
<td>Principal Investigator</td>
</tr>
<tr>
<td>PC</td>
<td>Program Committee</td>
</tr>
<tr>
<td>RPP</td>
<td>Rappe Promotie Premie, a financial premium of 1360 € for students who finish their PhD within the allotted four years</td>
</tr>
<tr>
<td>RU</td>
<td>Radboud University Nijmegen</td>
</tr>
<tr>
<td>RUMC</td>
<td>Radboud University Medical Centre</td>
</tr>
<tr>
<td>STW</td>
<td>Stichting van de Technische Wetenschappen (Technology Foundation)</td>
</tr>
<tr>
<td>SoS</td>
<td>Former department Security of Systems, now part of DS</td>
</tr>
<tr>
<td>ST</td>
<td>Former department Software Technology, now part of MBSD</td>
</tr>
<tr>
<td>SIKS</td>
<td>Dutch research School for Information and Knowledge Systems</td>
</tr>
<tr>
<td>SNN</td>
<td>Stichting Neurale Netwerken</td>
</tr>
<tr>
<td>TILT</td>
<td>Tilburg Institute for Law, Technology, and Society</td>
</tr>
<tr>
<td>ZonMw</td>
<td>Netherlands organization for health research and development, part of NWO</td>
</tr>
</tbody>
</table>
Preface

The institute for Computing and Information Sciences (iCIS) is one of the 22 research institutes of the Radboud University Nijmegen and belongs to the Faculty of Science (FNWI). iCIS was officially founded in 2005, as a natural continuation of the sub-faculty Computer Science when the Radboud University introduced its organization based on research institutes. In the last couple of years, iCIS optimized its internal organization: it went from 5 departments to 3 sections, organized around the institute’s main research programmes and with principal investigators steering the research. The present division into these 3 research programmes — Digital Security, Intelligent Systems, and Model-Based System Development — effective since January 2008, has been taken as the basis for this research assessment. The department of Biophysics, which temporarily belonged to iCIS in 2006 and 2007 before it joined the newly formed Donders Centre for Neuroscience, is not part of this assessment.

Within the review period researchers of iCIS have been very active, and visibly so. Impact reached extraordinary heights in 2008, when members of the section Digital Security discovered serious vulnerabilities in the Mifare Classic RFID chip, which is used in hundred of millions of cards worldwide for public transport and building access. This discovery led to questionings in Dutch parliament, official letters of the Minister of the Interior, news items in for instance the New York Times and on the BBC, and court rulings on the value of academic freedom over commercial profit. The high quality of iCIS’ research is further exemplified by the various prestigious prizes and personal grants awarded to iCIS members, both just before and during the review period: the Spinoza prize (“Dutch Nobel prize”) for Henk Barendregt (2002), the Pionier grant for Bart Jacobs (2002), and the VICI grant for Tom Heskes (2006).

The structure of this self-evaluation based on the three research programmes reflects iCIS’ ambition to play an internationally leading scientific role in each of these fields.

Tom Heskes (research director since 2009)
Bart Jacobs (research director 2004-2008)
Bernadette Smelik (managing director)

Nijmegen, August 20, 2009
Part A
Chapter A

Institute for Computing and Information Sciences

A.0 Documentation regarding the level of the institute

Name of the institute: Institute for Computing and Information Sciences (iCIS)
Date of establishment: 1 January 2005
Institutional affiliations: Faculty of Science
Radboud University Nijmegen
The Netherlands

A.1 Mission statement

The mission of the Institute for Computing and Information Sciences (iCIS) is to improve analysis and development of computer-based systems, through mathematically founded theories, methods and tools. iCIS’ main research focus is the quality of software, with an emphasis on reliability, security, architecture and system alignment. The applicability of the institute’s methods and tools is validated by tackling these problems, as encountered in society, industry, and other scientific disciplines.

Research is concentrated within three recognizable research programmes—Digital Security, Intelligent Systems and Model-Based System Development—each with its own research focus and aims. These programmes fit well into the Dutch national ICT research agenda (NOAG-ICT 2005-2010 Met vaste hand). In each of these research areas, it is iCIS’ ambition to play a leading international role.

Alongside its research ambitions, iCIS aims to deliver PhD students capable of working at the appropriate level of abstraction that allows them to keep an overview over developments, independently of accidental details and hypes of the moment, with the skills to extend knowledge boundaries, and an analytical and critical mind-set.

A.2 Leadership

A.2.1 Organization and managerial style of iCIS

Director of Research: prof.dr. T.M. Heskes
Deputy Director: prof.dr. B.P.F. Jacobs
Managing Director: dr. B. Smelik
CHAPTER A. INSTITUTE FOR COMPUTING AND INFORMATION SCIENCES

Since January 2008, the institute is divided into three sections, Digital Security (DS), Intelligent Systems (IS), and Model-Based System Development (MBSD). The section leaders are responsible for the daily management of the sections. The director of the institute determines the overall policy and strategy of the institute, and is responsible for the management of the institute, assisted by the deputy director and the managing director. They meet once a week, together with representatives from the personnel and finance departments, to discuss operational matters of the institute. On a monthly basis, there are management board meetings of the section leaders and their deputies, representatives from the affiliated teaching institute and organization, the research directorate, and the LaQuSo\(^1\) director. The management board meetings provide steering and feedback to the director. The director has monthly meetings with the dean to discuss institutional issues. Additionally, there are monthly meetings of the faculty board with all research directors of the Faculty of Science.

The managerial style of iCIS aims at a balance between stimulating creativity in the quest for new developments and goal-directed cooperation: a controlled chaos in a melting-pot for scientific work. The research programme is a reflection of this balance in terms of short term research goals and long term vision. Short term research goals involve a mixture of “valorization push” via knowledge transfer to industry and government, and of “inspiration pull” for guidance and relevance.

### A.2.2 Rearrangement into sections

iCIS’ staff members held several meetings and retreats in 2006-2007 to discuss the mission and strategy of the institute. It was concluded that, in order to realize its ambitions, iCIS needed a stronger research focus with a larger critical mass per research programme, a better visibility of the main research and research leaders, and a more flexible organization to stimulate and prosper high-quality research. Consequently, iCIS changed its organization quite drastically: it went from 5 departments led by chair holders each focused on their own specialism, to 3 sections, organized around the institute’s main research programmes and with principal investigators steering the research. The chosen research programmes reflect the strength of the institutes’ researchers and cover key scientific challenges in computer science (see Section A.3.3 as well as the self-evaluations of the individual sections). The new organization has been taken as the basis for this self-evaluation and assessment.

Table A.1: Organization of iCIS before January 1, 2008.

<table>
<thead>
<tr>
<th>Department (acronym)</th>
<th>Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of Systems (SoS)</td>
<td>prof. B. Jacobs</td>
</tr>
<tr>
<td>Information and Knowledge Systems (IRIS)</td>
<td>prof. T. van der Weide</td>
</tr>
<tr>
<td>Foundations (Fnds)</td>
<td>prof. H. Barendregt</td>
</tr>
<tr>
<td>Informatics for Technical Applications (ITA)</td>
<td>prof. F. Vaandrager</td>
</tr>
<tr>
<td>Software Technology (ST)</td>
<td>prof. R. Plasmeijer</td>
</tr>
</tbody>
</table>

Table A.1 displays the organization before January 1, 2008 in departments with chair holders. The current organization, in terms of sections and section leaders, effective as of January 1, 2008, is given in Table A.2. The roles of chairs and principal investigators is explained in more detail in the next section.

Table A.2 also specifies the chairs within each section. Most researchers followed the chair that they belonged to prior to the rearrangement of the institute, with the notable exception of IRIS, which was subdivided between all three new sections: researchers working under the direct supervision of prof. E. Proper and dr. P. Lucas moved to MBSD, of prof. T. Heskes to IS, and of prof. T. van der Weide to DS.

---

\(^1\)Laboratory for Quality of Software; explained in more detail below.
Table A.2: Organization of iCIS as of January 1, 2008.

<table>
<thead>
<tr>
<th>Section (acronym; section leader)</th>
<th>Chairs</th>
<th>Principal Investigators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Security (DS; dr. E. Poll)</td>
<td>prof. B. Jacobs</td>
<td>prof. B. Jacobs</td>
</tr>
<tr>
<td></td>
<td>prof. T. van der Weide</td>
<td>dr. E. Poll (aspiring)</td>
</tr>
<tr>
<td></td>
<td>prof. M. van Eekelen (aspiring)</td>
<td>prof. M. van Eekelen (aspiring)</td>
</tr>
<tr>
<td>Intelligent Systems (IS; dr. E. Marchiori)</td>
<td>prof. H. Barendregt</td>
<td>prof. H. Barendregt (honorary)</td>
</tr>
<tr>
<td></td>
<td>prof. H. Geuvers</td>
<td>prof. H. Geuvers</td>
</tr>
<tr>
<td></td>
<td>prof. T. Heskes</td>
<td>prof. T. Heskes</td>
</tr>
<tr>
<td>Model-Based System Development (MBSD; dr. P. Lucas)</td>
<td>prof. F. Vaandrager</td>
<td>prof. F. Vaandrager</td>
</tr>
<tr>
<td></td>
<td>prof. R. Plasmeijer</td>
<td>dr. P. Lucas</td>
</tr>
</tbody>
</table>

The rearrangement took place under the guidance of the previous institute’s director, prof. B. Jacobs, and with input from the personnel department on personnel and legal matters. It also involved a rearrangement of the supporting staff, which now roughly amounts to one management assistant and one scientific programmer per section. Despite its impact, the whole operation went very smoothly and received full support from all staff members involved.

A.2.3 Chairs and principal investigators

Chairs (leerstoelen) form the basic organizational units of the university. Every staff member formally belongs to a chair. The chair holder is responsible for research and teaching in his/her area and safeguard the institute’s long-term research programmes. The hierarchy within the Faculty of Science, that iCIS belongs to, is visualized in Figure A.1. It describes the situation before January 2008, and is still the official underlying legal structure, for instance in case of a conflict.

![Figure A.1: The hierarchical structure within the Faculty of Science.](image-url)

Since a substantial part of the institute’s internal and external funding depends on research performance, it is an institute-wide interest to give those members that perform outstandingly the position and resources to excel. These members are not necessarily the chair holders and it was therefore generally accepted and agreed upon that iCIS required a more flexible system to optimize
on high-quality research output. This led to the functional organization sketched in Figure A.2. In the current organization (since mid 2007), chairs are embedded within the sections, delegating administrative responsibilities to the section leaders (who need not be professors) and (possibly) research steering to principal investigators (PIs). These PIs played a leading role in the formation and definition of the new research programmes. They meet from time to time with the research director to discuss strategic issues. Currently, these meetings do not have a formal status.

![Functional chart of delegations within iCIS](image)

Figure A.2: The functional chart of delegations within iCIS.

PIs are successful researchers within one of the iCIS research programmes who meet severe quality standards (in terms of numbers of publications and supervised PhDs, acquired external funding, and research status and impact). Every three years an external committee, which includes the vice-dean of research of the faculty, re-evaluates the PIs. This introduces a reasonable level of dynamics into the organization, based on research performance. PI-ship involves a reduced teaching and administration load (30% instead of nominally 40%, and 10% instead of 20%, respectively) and an extended research task 60%—which includes research management. PI-ship provides status, but also responsibilities for the success of the research programmes. The research of PIs has high priority for the institute and receives special attention and support. Staff members are encouraged to join the research activities of a PI, but are not forced to do so.

### A.2.4 Reflection on the organizational changes

Sofar, the rearrangement into three new sections turned out to be successful, certainly from an organizational perspective and increasingly from a scientific point of view. The more flexible way of dividing responsibilities, between PIs, chairs, and section leaders has been an improvement over the old approach. It avoids the concentration of all these duties in (consequently overburdened) chairs. The additional flexibility has been successfully exploited to make the most of our collective capabilities. By pooling management assistants and scientific programmers, iCIS is ahead of an upcoming rearrangement planned by the faculty.

In the process since the start of the new sections and towards this self-evaluation, the research programme within each section was further shaped and new links between the different subthemes were explored. Collaborations between some subthemes are more obvious and more easily effectuated than those between others. This can be both because these subthemes are scientifically further apart and because there are no researchers directly available to build the bridge. iCIS’s policy is not to force interaction when this has no added-value, but to stimulate researchers to interact and explore possibilities that could strengthen the quality and focus of iCIS’ research. Further integration is stimulated by creating new positions on the overlap between different subthemes. A concrete example is the internal funding of a PhD position on the overlap between the model-based reasoning subtheme led by dr. P. Lucas and the conceptual modeling subtheme of prof. E. Proper. Another example is the appointment of prof. W. Kraaij, whose research interests link the work on information retrieval and on security and privacy.

The PI-system works as intended, although with a few shortcomings. PIs do have a special
status, both internally and externally, which further highlights the strengths of the institute. Furthermore, the system gives talented, young researchers the possibility to set up and strengthen their own research line, for which they have full responsibility and receive all credits. However, the projected reduction in teaching and administrative load for PIs has not been achieved: most PIs, in particular the research and teaching directors, still have considerable administrative duties. In the current situation, the PIs are nicely spread over the different research programmes, but this is not guaranteed in subsequent application rounds. Last but not least, some staff members are not part of a PI-group, which implies that their research for the institute as a whole has lower priority. Some deliberately choose to focus more on teaching, others try to improve the quality and impact of their research such as to become an (aspiring) PI in the next application round. In short, the advantages appear to outweigh the disadvantages, but some of the details, in particular the subdivision between research, teaching and administrative duties, may have to be made more realistic.

### A.3 Strategy and Policy

The outline of this section is as follows. First, in Section A.3.1 iCIS’ vision on research is described to motivate its mission with respect to research. Section A.3.2 gives a more detailed account of iCIS’ mission as formulated in Section A.1 with respect to research, the training of PhD students as well as valorization and outreach, and ends with a specification of iCIS’ ambition level. Section A.3.3 finally discusses iCIS’ strategy and policies corresponding to these four aspects of its mission.

#### A.3.1 Research vision

Pure academic research is focused on going beyond knowledge boundaries and developing new paradigms. It has a high cultural and societal value, even though actual applications may appear only after many years. Neglecting pure research does not have an immediate negative impact, but it definitely is detrimental in the long run, for a modern knowledge-driven society.

The fast pace of development of computer related technology works as a permanent trigger that comes in hypes and often requires budgets that are beyond the means of a (medium size) university. Consequently, in (more applied) subareas of the quickly developing ICT-field, companies have become leading, for instance in information technology (Google), operating systems (Windows, Linux), programming languages (SUN), databases (Oracle) and communication (with many large international service providers). Nonetheless, many of these companies originate from and still rely on academic research, for instance for new and efficient algorithms, protocols, and data structures.

Exploring the possibilities and limitations of new technological developments forms an applied research activity in itself. Such investigations are still relevant within an academic setting, not only to obtain research inspiration and focus from the newest technology, but also to generate external revenues: modern scientific research is increasingly supposed to generate its own budgets.

#### A.3.2 Mission

**Research**

Given the above, iCIS’ highest priority is to perform pure computer science (informatica) and information science (informatiekunde) research. At the heart of computer science at iCIS are the mathematically oriented research activities centered on formal modeling and analysis. Since actual software is usually too complicated and large (in terms of number of lines of code) to comprehend, abstractions are needed, in the form of models. Ideally, such models are formulated before programming starts. Such a model is usually a mathematical artifact (e.g. a certain automaton) that can be analyzed, often with dedicated computer programs (tools) such as simulators, model checkers or theorem provers. In such a way one can establish suitable properties of the model, and thus of the software that will be built on top. Formal modeling and analysis therefore play
an important role within each of the research programmes and form the common language and glue between them.

iCIS not only aims to study technical aspects of software systems, but also their embedding in the environments in which they have to operate. It is a highly non-trivial matter how to incorporate such environmental issues into a formal model, that can be used as basis for software development and maintenance. Understanding these environmental factors often requires knowledge of specific application domains or of social interaction patterns. iCIS wishes to incorporate the analysis and formalization of such non-technical issues in its activities as a preparatory activity for the analysis and construction of software (models).

iCIS wants to have firm roots within the broad “general university” environment offered by the Radboud University. This explains the focus on formal modeling and analysis and distinguishes iCIS from computer science departments at technical universities, which typically have a more applied focus. Furthermore, iCIS aims to contribute to the progress of science in other disciplines, such as neuroscience, biology, law, and medicine, scientific areas in which the Radboud University is particularly strong.

**Training of PhD students**

It is part of iCIS’ explicit mission to deliver PhD students capable of working at the appropriate level of abstraction that allows them to keep an overview over developments, independently of accidental details and hypes of the moment, with the skills to extend knowledge boundaries, and an analytical and critical mind set. After four years, they should be independent, well-connected scientists that know how to organize their own careers, whether inside or outside science.

**Valorization and outreach**

iCIS wishes to make concrete contributions to society, through valorization (e.g., in the form of exploration or evaluation activities as independent consultancy in industry) as well as outreach (e.g., through active participation in public debates and activities to enhance IT-knowledge in developing countries). iCIS’ valorization activities are not a goal in itself, but are a natural consequence of its scientific activities, contribute to its open culture, reinforce themselves by raising new questions beyond the specific practical study, and add to continuity of iCIS’ research.

**Ambition level**

iCIS wishes to be a research institute competing at the international top level. It wants to be prominent in its research themes, demonstrated by its scientific, industrial and governmental, and societal impact. Key indicators for impact are well-recognized contributions to the international scientific community, cooperation in national and international research programmes, valorization (both cultural and economical), contributions to societal debates (e.g. on the use and impact of ICT), popular publications, expert opinions in the press, company founding (spin-offs), contributions to open source and open standards, and developing country support.

**A.3.3 Strategy**

**Research**

The research programmes—*Digital Security, Intelligent Systems* and *Model-Based System Development*—reflect the strength of the institutes’ researchers, building upon the expertise in theoretical computer science that Nijmegen is famous for. Moreover, they cover key scientific challenges in computer science. Each programme has a direct link to one of the themes in the national research agenda ICT (NOAG-ict) *Met vaste hand: Digital Security to Digitale Veiligheid, Model-Based System Development to Methoden voor bouwen en ontwerpen, and Intelligent Systems to Intelligente Systemen*. The deliberate focus on these three programmes guarantees enough diversity to cover a substantial part of computer science (which is relevant for teaching), while at the same time
each research programme has sufficient critical mass to indeed play a leading role. Furthermore, the different research programmes give ample opportunity to realize iCIS’ ambitions to make contributions to society (e.g., the heavy involvement of members of Digital Security in discussions on the use of ICT) and other scientific disciplines (e.g., the application of artificial intelligence techniques for the analysis of neuroimaging and biological data).

iCIS aims to study not only the technical aspects of software systems, the main arena of computer science, but also their interaction with the computing environment, often referred to as information science. Information science research is embedded within the (now) three research programmes within the institute. iCIS has fewer members with a specialized research background and focus on information science than originally planned. One reason is that it appeared to be very difficult to attract new qualified staff members with such a background and focus. Also, because the Information Science curriculum was drawn closer to the Computer Science curriculum, the need for specialized expertise from a teaching perspective became less prominent. In the current situation, there is insufficient critical mass and leadership for a separate research line on information science within the institute and measures have been taken to move the existing line of research closer to other lines of research, in particular within Model-Based System Development. Information science research in general, alongside more technically oriented computer science research, will remain one of iCIS’ objectives. The research within Digital Security, combining both technical and societal aspects of digital security, is an excellent example thereof and is further strengthened with the appointment of prof. W. Kraaij. iCIS will search for one or two additional extra-ordinary professors who can cover information science research related to ongoing computer science research, for example in the direction of data mining.

iCIS stimulates collaboration with research groups from other institutes within and outside the Faculty of Science. Digital Security (DS) cooperates with colleagues in the law department, especially in the area of cybercrime. Intelligent Systems (IS) maintains close connections with research in neuroscience and (cognitive) artificial intelligence, via several joint research projects. Model-Based System Development (MBSD) cooperates with management sciences on modeling of organizations and with the Radboud University Medical Center on decision support systems and data analysis. Both IS and MBSD are involved in a new initiative for systems biology. Furthermore, there are close ties to mathematical researchers within IMAPP, through the supervision of joint master and PhD students and joint research grants. The increased activity has not only paid off through several publications in high-quality interdisciplinary journals, but also by providing inspiration for new computer science research. iCIS will therefore certainly continue along this line.

iCIS made a deliberate decision to focus on the three research programmes and foresees no reason to deviate from this path in the next few years. Even in the longer term, iCIS’ new organization is expected to be rather robust, although (even) less internal (baseline) funding will put pressure on the scientific quality. Within the next review period, two chair holders will retire: prof. H. Barendregt (Foundations of Mathematics and Computer Science, Intelligent Systems) in 2012 and prof. T. van der Weide (Information Retrieval and Information Systems, Digital Security) in 2015. Prof. H. Barendregt’s research line on formalizing mathematics will continue under the guidance of prof. H. Geuvers. His research on mind-brain-mindfulness, which is an excellent example of iCIS’ ambition to contribute to other scientific disciplines, will be more difficult to prolong within iCIS, but then again is not within iCIS’ core research. With prof. van der Weide’s retirement, a bit further away, iCIS will have to reconsider the interpretation of his chair in information retrieval and information systems and might move it more into the direction of protecting privacy and combatting cybercrime. Since 2008 this line of research is being explored at the level of an extraordinary chair (prof. W. Kraaij).

Summarizing, iCIS stands firm on its deliberate choice for the three research programmes, with sufficient coverage to perform its teaching duties, enough focus and critical mass for leading research, and ample connections to other scientific disciplines. Information science research is spread across different programmes, alongside technology-oriented computer science research. No major changes are foreseen in the next couple of years.
Training of PhD students

All starting PhD students have to agree together with their promotor and direct supervisor on a Training and Guidance Plan. This plan also involves training and education and describes the courses the candidate will follow for the next four years. Many general courses are offered by the Radboud University, such as ‘Presentation skills’, ‘Academic Writing’, ‘Advanced English Conversation’, ‘Management for PhD students’, ‘Didactics in Practice’, ‘Reflection on scientific conduct’, and so on. Specialized courses can be either master courses the students did not yet follow during their previous studies (possibly in different scientific disciplines) as well as courses and workshops offered by the national research schools (SIKS, IPA). Each PhD student is either a member of SIKS or of IPA. The Training and Guidance Plan is used as a guideline: some deviations, most notably with respect to the courses being followed, are certainly allowed. Overall, PhD students appreciate the breadth and quality of the courses offered, in particular those that can be put in direct practice (e.g., ‘Presentation skills’ and ‘Academic Writing’). One PhD student even went as far as obtaining the full teaching qualification (Basiskwalificatie Onderwijs) for assistant or associate professors.

PhD students are encouraged to visit an international summer school on their research topic in the early stages of their PhD studies, as well as to visit international workshops and conferences, both to learn and to build their own scientific network. Many students spend a small part of their PhD abroad, at another university. PhD students regularly present their research and research plans within group meetings, where they are trained to clearly formulate their ideas and the wider consequences of their study. All PhD students are encouraged to have a (small) organizational task, such as the organization of group or institute’s seminars or maintenance of the group’s web site.

The Training and Guidance Plan encompasses a yearly assessment interview in which the past year is evaluated and the planning for the coming year is made. PhD students initially have a position for 18 months, after which an assessment is made which results in a go/no-go decision. After a positive outcome, the contract of the PhD student is prolonged to 4 years. It is an explicit policy of iCIS to stop problematic PhD trajectories early on, in order to prevent waste of time and effort and disappointment later on. This applied to 3 PhD students during the review period. Two PhD trajectories only were stopped on initiative of the PhD students themselves.

Table A.3: Standard PhD-Candidates (SEP Table 2.1 and 2.2)

<table>
<thead>
<tr>
<th>Starting year</th>
<th>Total</th>
<th>4 years</th>
<th>5 years</th>
<th>6 years</th>
<th>7 years</th>
<th>not yet finished</th>
<th>discontinued</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>5</td>
<td>40%</td>
<td>20%</td>
<td>0%</td>
<td>20%</td>
<td>0%</td>
<td>20%</td>
</tr>
<tr>
<td>2001</td>
<td>1</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>2002</td>
<td>9</td>
<td>70%</td>
<td>0%</td>
<td>0%</td>
<td>10%</td>
<td>0%</td>
<td>20%</td>
</tr>
<tr>
<td>2003</td>
<td>9</td>
<td>44%</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>22%</td>
<td>11%</td>
</tr>
<tr>
<td>2004</td>
<td>3</td>
<td>100%</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>28</td>
<td>57%</td>
<td>14.5%</td>
<td>0%</td>
<td>7%</td>
<td>7%</td>
<td>14.5%</td>
</tr>
</tbody>
</table>

Graduation results per year are shown in Table A.3. Students who finish their PhD within the allotted four years receive a financial premium of 1360 €, the so-called ‘RPP’ (Rappe Promotie Premie). As can also be seen in Tables A.16 through A.19 at the end of Part A, where all PhD candidates are listed, this premium has been awarded to almost 80% of the graduated students.

One staff member of iCIS, currently dr. S. Hoppenbrouwers, acts as a confidential advisor for PhD students. This coordinator’s task is to support, and protect the interests of PhD students in a general sense (not concerning the contents of the PhD work) and to give advice on PhD matters to individual PhD students, their supervisors, or to the iCIS director. On a regular basis (minimally once a year), the PhD coordinator meets with each PhD student to confidentially discuss conditions of work, supervision, progress, and potential or actual problems. Supervisors ask the coordinator for input in the preparation of an assessment interview. In case of serious problems,
the coordinator first consults the director of iCIS. In all these matters, the PhD coordinator maintains an independent position and adheres to full confidentiality.

iCIS is also dedicated to the training of PhD students from developing countries, e.g., through various Nuffic programs (see Section A.3.3).

Some PhD students did their master study at the Radboud University and basically continued the research they started for their master project. Most students are acquired through internet advertisements and the individual staff members’ network. About half of the PhD students are from abroad. Considering the low percentage of early drop-outs and high percentage of graduations within 4 years (see Tables A.3 through A.18), acquisition can be considered successful.

Table A.4: Career destination after end of contract (SEP Table 3)

<table>
<thead>
<tr>
<th>Category</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenured academic staff in the Netherlands</td>
<td>2</td>
</tr>
<tr>
<td>Tenured academic staff abroad</td>
<td>1</td>
</tr>
<tr>
<td>Non-tenured academic staff in the Netherlands</td>
<td>9</td>
</tr>
<tr>
<td>Non-tenured academic staff abroad</td>
<td>6</td>
</tr>
<tr>
<td>Trade and Industry</td>
<td>8</td>
</tr>
<tr>
<td>Government</td>
<td>1</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>0</td>
</tr>
<tr>
<td>Unemployed</td>
<td>0</td>
</tr>
</tbody>
</table>

Table A.4 lists the career destinations of the PhD students who finished their PhD studies (i.e., excluding the PhD students whose contract has not been prolonged to 4 years). It can be seen that about two-third, at least for their first contract after their PhD, stays within academics, and about one-third goes to industry or government.

Summarizing, iCIS’ policies with respect to the training and guidance of PhD students are well thought-out with various built-in checks (yearly assessments, confidential advisor) and worked well in the past.

Valorization and outreach

To meet its ambitions with respect to valorization, iCIS organized most of its contract research activities in a separate unit, called LaQuSo. LaQuSo stands for ‘Laboratory for Quality Software’. It is a cooperation with the Technical University of Eindhoven aimed at transferring scientific software analysis techniques to a commercial setting, via contract research. LaQuSo Nijmegen has its own scientific director (who is a member of the management board), managing director, and support staff. For specific commercial projects, individual members of staff may temporarily be placed under the responsibility of the LaQuSo director. Contract research through LaQuSo has been quite successful in recent years, generating varying yearly revenues of 50-100 k€. Projects are related to research in various ways: demonstrating applicability (e.g., using the GAST model based test generation tool to validate the security of the Dutch national passport), exploring future research areas (e.g., security assessment of smart power meters and of road-pricing which led to several research proposals), or performing formal method industrial case studies that push the state-of-the-art a bit further (e.g., the Aia case study which led both to a research publication in FMICS [D273] and to a new academically published certification model [D277].

There are various incentives for doing valorization research: getting inspiration for new scientific research and making a contribution to society, but also generating some additional revenues for one’s research group. Such revenues are typically used to build up a little reserve to allow for extra research related activities. However, most of the revenues generated by iCIS’ members
through contract research in recent years were used to compensate for financial losses elsewhere within the Faculty of Science. Institutes and research groups could not build up reserves (and use these to hire new personnel) nor could they hire personnel up front based on a sensible estimate of future (valorization) revenues. This caused a significant reduction in the motivation for acquiring new valorization projects. The faculty board has promised to change its policies in this regard, such as to stimulate rather than discourage valorization activities.

iCIS' links with government and industry have been and will continue to be strengthened through strategic appointments for extra-ordinary professors (see Section A.4.1 on strategic alliances) as well as through part-time positions for staff members who also work at research institute (ESI, TNO). This has been very fruitful in terms of publications as well as joint research projects. Besides, iCIS staff members supervise several external, industrial PhD students. Efforts will continue to accommodate external PhD students, but the institute has no explicit strategy to attract them.

Several iCIS members are very active in societal debates related to the use of ICT in society. Especially within digital security there are many hot topics—such as electronic voting, smart and RFID cards, and privacy—where scientists contribute with their expertise. In particular the dismantling of the Mifare Classic RFID chip, used in the OV-chipkaart, received an enormous amount of media coverage in 2008.

Staff members, often in cooperation with students, have been involved in various activities to improve on the one hand IT-knowledge in developing countries, and on the other hand to obtain insight in the specific problems developing countries are faced with if they want to apply information technology in their society. There are strong ties to universities in Uganda and Ghana, not only for teaching but also for research. In the context of a joint Nuffic project with the universities of Eindhoven and Groningen, several students from Uganda started their PhD studies in Nijmegen under the guidance of iCIS staff members. Three students already received their PhD degree and now have a leading position at a university in their home country. To raise the students’ research to a level that is actually worth a PhD requires quite some efforts from their supervisors. Nevertheless, iCIS is determined to actively and continuously pursue and support these activities.

In short, iCIS successfully uses LaQuSo as an outlet for valorization and builds bridges with industry through extra-ordinary professorships and external PhDs. An important incentive for doing contract research, generating additional revenues, has been under pressure because of current faculty policies. Other contributions to society, e.g., through involvement in societal debates and support to developing countries, are flourishing.

**Ambition level**

As described above, iCIS has recently been rearranged to a well-organized institute with three sections to be better equipped to meet its ambitions to become internationally leading in each of the corresponding research areas. Research within iCIS is predominantly steered by principal investigators, who have their own responsibility. PIs are evaluated every 3 years on indicators such as scientific output, number of PhDs supervised, fund raising, and societal impact. This system is expected to lead to an additional incentive to PI and PI-groups to produce high-quality research. Success of the PI-groups thereby guarantees the success of iCIS as a whole. The PI-criteria also play a role in the evaluation of candidates for new staff positions.

The PI-system is also flexible, in that it provides a means to give responsibility and credit to (young) successful assistant/associate professors. Groups of researchers or individual researchers that do not (yet) belong to a PI-group should feel an incentive to increase the level and impact of their research or reshape their research agenda such that it does fit within one of the PI-groups. By explicating the indicators for excellent research and by creating the surroundings and incentives to meet those, iCIS’ target is to achieve that all staff members are part of a PI-group within the next three to five years.

Within iCIS there is an increasing ambition to publish in high-impact and leading disciplinary journals, although this has not yet been fully taken up by all its staff members. In evaluations
and assessments of individuals, quality of the publication venue, and not just quantity, is increasingly taken into account. Young scientists are stimulated and supported to write their own research proposals, for example in the VENI-VDI-VICI program of NWO, but also in the NWO open competition and STW technology program. This has been very successful, resulting in a VICI for Tom Heskes (then assistant professor), VENIs for Bas Spitters and Milad Niqui (postdocs), STW/Sentinels project PINPAS JC and EU projects Mobius and Robin for Erik Poll (then postdoc) and NWO open competition grants for Julien Schmaltz and Peter van Rossum (then postdocs).

A.4 Researchers and Other Personnel

Table A.5 displays the number of fte’s available for research for the whole institute, Table A.6 does the same per section.

| Table A.5: Research staff at institutional level (SEP Table 1) |
|---|---|---|---|---|---|---|
| 2003 | 2004 | 2005 | 2006 | 2007 | 2008 |
| Tenured staff | 8.32 | 8.72 | 9.01 | 9.24 | 8.89 | 9.39 |
| PhD candidates | 15.01 | 19.22 | 17.52 | 16.48 | 16.29 | 19.17 |
| Total research staff | 35.62 | 37.9 | 35.98 | 38.94 | 38.26 | 41.55 |

| Table A.6: Research staff at programme level (SEP Table 1) |
|---|---|---|---|---|---|---|
| Total tenured staff | 1.90 | 2.20 | 2.13 | 2.10 | 2.16 | 2.50 |
| Total non tenured staff | 5.16 | 3.32 | 3.38 | 7.13 | 5.71 | 4.96 |
| Total PhD candidates | 4.11 | 5.87 | 4.97 | 5.07 | 6.12 | 4.42 |
| Total research staff | 11.17 | 11.39 | 10.48 | 14.3 | 13.99 | 11.88 |

<table>
<thead>
<tr>
<th>Intelligent Systems</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total tenured staff</td>
<td>2.20</td>
<td>2.50</td>
<td>2.80</td>
<td>3.17</td>
<td>3.03</td>
<td>3.39</td>
</tr>
<tr>
<td>Total non tenured staff</td>
<td>2.99</td>
<td>3.43</td>
<td>3.32</td>
<td>3.53</td>
<td>4.63</td>
<td>5.58</td>
</tr>
<tr>
<td>Total PhD candidates</td>
<td>2.78</td>
<td>2.57</td>
<td>3.79</td>
<td>5.62</td>
<td>6.34</td>
<td>8.90</td>
</tr>
<tr>
<td>Total research staff</td>
<td>7.97</td>
<td>8.50</td>
<td>9.91</td>
<td>12.32</td>
<td>14.0</td>
<td>17.87</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model-Based System Development</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total tenured staff</td>
<td>4.22</td>
<td>4.02</td>
<td>4.08</td>
<td>3.97</td>
<td>3.70</td>
<td>3.50</td>
</tr>
<tr>
<td>Total non tenured staff</td>
<td>4.14</td>
<td>3.21</td>
<td>2.75</td>
<td>2.56</td>
<td>2.74</td>
<td>2.45</td>
</tr>
<tr>
<td>Total PhD candidates</td>
<td>8.12</td>
<td>10.78</td>
<td>8.76</td>
<td>5.79</td>
<td>3.83</td>
<td>5.85</td>
</tr>
<tr>
<td>Total research staff</td>
<td>16.48</td>
<td>18.01</td>
<td>15.59</td>
<td>12.32</td>
<td>10.27</td>
<td>11.80</td>
</tr>
</tbody>
</table>
It can be seen that the available research staff slowly increased throughout the review period, mostly because of an increase in non-tenured staff and PhD candidates as a result of the successful acquisition of research funds (see Section A.5).

Table A.7: Supporting staff at institutional level (SEP Table 1)

<table>
<thead>
<tr>
<th>Year</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>fte</td>
<td>9.9</td>
<td>10.3</td>
<td>9.7</td>
<td>9.7</td>
<td>8.8</td>
<td>8.0</td>
</tr>
</tbody>
</table>

Supporting staff, summarized in Table A.7, roughly amounts to one management assistant and one scientific programmer per section plus a managing director and assistant for iCIS’ research bureau. It should be noted that, whereas the numbers in Table A.5 correspond purely to research equivalents, the numbers in Table A.7 for the supporting staff are full fte’s. As can be seen from Table A.8, the number of fte’s supporting staff (scientific programmers, management assistants, managing director) divided by the number of fte’s total staff shows a continuous decline throughout over the years and is well below 15%.

Table A.8: Supporting staff as percentage of total staff

<table>
<thead>
<tr>
<th>Year</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratio supporting over total staff</td>
<td>14.7%</td>
<td>14.6%</td>
<td>14.5%</td>
<td>13.7%</td>
<td>13.2%</td>
<td>11.8%</td>
</tr>
</tbody>
</table>

All iCIS permanent staff members and most postdoctoral and PhD students are involved in teaching. Generally permanent staff members are expected to devote 40% of their time to teaching, 20% to managerial tasks, and 40% to research. In practice, these percentages fluctuate between individuals, with some staff members devoting much more time to teaching than 40%. Postdocs and PhD students are expected to spend 10% of their time to teaching. Teaching load per staff member is increasing, both because of a decline in permanent staff and the recent extended involvement in the study Artificial Intelligence (Kunstmatige Intelligentie), which is now shared between the Faculty of Science and the Faculty of Social Sciences. Too high teaching load for the remaining staff members may lead to a negative effect on the quality of research.

Senior researchers, at the level of assistant and associate professors, are offered and stimulated to follow a university-wide course on Academic Leadership, which was started a couple of years ago. The course includes several workshops (e.g., on communication skills, financial management, supervision of PhDs, personnel and legal affairs, and so on), guidance by a personal coach, and group intervision sessions. Six of iCIS members already followed this course. A similar crash course is offered to young professors. The courses are not only meant for education, but also to get in touch and learn from fellow researchers from other faculties and scientific disciplines.

A serious concern is the lack of perspectives and career tracks for excellent postdoctoral researchers, not only within iCIS, but in general within the Dutch university system. Even those who perform exceptionally well, e.g., by raising their own grants, iCIS could not offer any perspective beyond their temporary contracts up to maximally 6 years: the number of available permanent positions at the level of assistant/associate professors is too limited. This situation slightly changed with new faculty regulations that do allow for permanent positions of talented researchers, strictly conditioned upon the availability of specific external funding. iCIS aims to make use of these regulations, but only for excellent postdocs who clearly have the ambition and qualities to pursue an academic career and are capable to generate (a substantial part of) their own funding. iCIS does not want to delude postdocs with false hopes and encourages them to also make use of the university’s facilities to prepare them for a career outside academia (workshops, coaching).

iCIS’ policies regarding PhD students are outlined in Section A.3.3.
A.4. RESEARCHERS AND OTHER PERSONNEL

A.4.1 Strategic alliances

In addition to the regular staff at iCIS, a number of strategic appointments for extra-ordinary professors have been made to stimulate certain areas of research (see Table A.9). Such opportunities are all the more interesting given the limited internal means. iCIS has started another procedure to recruit an additional extra-ordinary professor from CWI in theoretical computer science.

<table>
<thead>
<tr>
<th>Period</th>
<th>Section</th>
<th>Other Institute</th>
<th>FTE at iCIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Klop, J.W.</td>
<td>2002-2008</td>
<td>IS</td>
<td>CWI</td>
</tr>
<tr>
<td>Vliet, M. van</td>
<td>2003-present</td>
<td>MBSD</td>
<td>CapGemini/Deloitte</td>
</tr>
<tr>
<td>Rijsenbrij, D.</td>
<td>2004-2007</td>
<td>DS</td>
<td>CapGemini</td>
</tr>
<tr>
<td>Verheul, E.</td>
<td>2005-present</td>
<td>DS</td>
<td>PricewaterhouseCoopers</td>
</tr>
<tr>
<td>Zantema, H.</td>
<td>2007-present</td>
<td>IS</td>
<td>TU Eindhoven</td>
</tr>
<tr>
<td>Proper, E.</td>
<td>2008-present</td>
<td>MBSD</td>
<td>CapGemini</td>
</tr>
<tr>
<td>Kraaij, W.</td>
<td>2008-present</td>
<td>DS</td>
<td>TNO</td>
</tr>
</tbody>
</table>

The initiative for the appointments is jointly taken by group leaders (previously department heads, now section leaders) and the director of iCIS, and follow the standard procedure of the University Board. All candidates for whom the procedure is started should have an excellent track record, and should complement the regular staff in scientific and educational matters. The extra-ordinary professors are hosted by and affiliated to one of iCIS’ sections. The performance of the extra-ordinary professor is annually assessed and after 3 years a formal decision for prolongation of the appointment is made by the University Board on advice from the director of iCIS.

<table>
<thead>
<tr>
<th>Period</th>
<th>Section</th>
<th>Other Institute</th>
<th>FTE at iCIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hooman, J.</td>
<td>2003-2009</td>
<td>MBSD</td>
<td>ESI</td>
</tr>
<tr>
<td>Tretmans, J.</td>
<td>2006-present</td>
<td>MBSD</td>
<td>ESI</td>
</tr>
<tr>
<td>Hoepman, J.H.</td>
<td>2006-2008</td>
<td>DS</td>
<td>TNO</td>
</tr>
<tr>
<td>Oostdijk, M.</td>
<td>2007-2008</td>
<td>DS</td>
<td>Riscure</td>
</tr>
<tr>
<td>Hoepman, J.H.</td>
<td>2008-present</td>
<td>DS</td>
<td>TNO</td>
</tr>
</tbody>
</table>

Specific strategic alliances with industry are effectuated by several iCIS staff members who have a part-time position at iCIS and a part-time position at an industrial research institutes such as TNO and ESI (see Table A.10). Some iCIS professors have part-time positions at other universities or academic institutes (Table A.11).

<table>
<thead>
<tr>
<th>Period</th>
<th>Section</th>
<th>Other Institute</th>
<th>FTE Elsewhere</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobs, B.</td>
<td>2005-2008</td>
<td>DS</td>
<td>TU Eindhoven</td>
</tr>
<tr>
<td>Geuvers, H.</td>
<td>2007-present</td>
<td>IS</td>
<td>TU Eindhoven</td>
</tr>
<tr>
<td>Barendsen, E.</td>
<td>2008-present</td>
<td>MBSD</td>
<td>ILS (RU)</td>
</tr>
<tr>
<td>Eekelen, M.</td>
<td>2009-present</td>
<td>DS</td>
<td>Open University</td>
</tr>
</tbody>
</table>
A.5 Resources, Funding and Facilities

A.5.1 Direct funding and research funds

Baseline funding (*eerste geldstroom*) is limited and is, because of the unstable financial position of the Faculty of Science, likely to decrease in the future. External research funds are necessary to maintain critical mass within each of the research programmes. iCIS therefore aims at a healthy balance between internal (baseline) funding and external funding (research funds and contracts, *tweede en derde geldstroom*) within each of the programmes. iCIS stimulates its researchers to write national and international grant proposals. Fund raising is one of the important criteria in the evaluation of PIs and individual researchers. PIs and section leaders are involved in the writing of new grants and make sure that these fit into the research programmes. The university provides excellent support, in terms of workshops, feedback on proposals, and practice interviews, for those who want to apply for personal grants (*e.g.*, *Vernieuwingsimpuls* and EURYI). Although within the institute there are no official guidelines, the habit is that concept grant proposals are evaluated and commented on by one or more senior researchers before they are submitted. The main external resources for funding are the Netherlands Organization for Scientific Research (NWO), the Foundation for Applied Research (STW), the European Union, and contract research for industries.

Table A.12: Funding at institutional level (SEP Table 2)

<table>
<thead>
<tr>
<th>in percentages</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Direct Funding</td>
<td>69.5</td>
<td>63.9</td>
<td>58.3</td>
<td>51.8</td>
<td>50.2</td>
<td>47.3</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>18.5</td>
<td>24.3</td>
<td>30.8</td>
<td>37.0</td>
<td>41.2</td>
<td>45.0</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>12.0</td>
<td>11.8</td>
<td>10.9</td>
<td>11.2</td>
<td>8.6</td>
<td>7.7</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>in k€</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Funding</td>
<td>2,756</td>
<td>2,816</td>
<td>2,953</td>
<td>3,525</td>
<td>3,125</td>
<td>3,388</td>
</tr>
<tr>
<td>Research Funding</td>
<td>734</td>
<td>1,071</td>
<td>1,560</td>
<td>1,454</td>
<td>1,520</td>
<td>1,607</td>
</tr>
<tr>
<td>Contracts</td>
<td>476</td>
<td>520</td>
<td>552</td>
<td>439</td>
<td>317</td>
<td>274</td>
</tr>
<tr>
<td>Total</td>
<td>3,966</td>
<td>4,407</td>
<td>5,065</td>
<td>5,418</td>
<td>4,962</td>
<td>5,369</td>
</tr>
</tbody>
</table>

Table A.12 clearly shows that iCIS as a whole has been increasingly successful in raising external research funds. While the increase in direct funding more or less amounts to inflation corrections, external research funds and contracts in 2008 make up more than 50% of iCIS’ funding, to be compared to 30% in 2003. As can be seen from Table A.13, the ratio between direct funding and external funding (research funds plus contracts) varies quite a lot between sections and over the years. Similar fluctuations occur within sections. Because of the low average success rate of grant proposals (*e.g.*, for the NWO *Vrije competitie* currently around 10%), success has become somewhat unpredictable. This makes it yet impossible to tell whether the existing differences are structural. The short-term strategy is therefore to re-allocate direct funding to counterbalance the (lack of) external funding. In the longer term the imbalance may have more serious consequences and could lead to the reconsideration of (sub)themes.

A.5.2 Facilities

In 2006, iCIS moved to the brand new Huygens Building, the home of the Faculty of Science. This move brought all groups closer to each other, all rooms and facilities being on one level. In the immediate surroundings we have a special room with equipment for video conferencing.
A.6. Processes in Research, Internal and External Collaboration

Table A.13: Funding at programme level in percentages (SEP Table 2)

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: Direct Funding</td>
<td>53.1</td>
<td>58.2</td>
<td>47.9</td>
<td>38.5</td>
<td>40.4</td>
<td>45.2</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>36.7</td>
<td>39.6</td>
<td>40.2</td>
<td>43.4</td>
<td>44.5</td>
<td>43.4</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>10.2</td>
<td>2.2</td>
<td>11.9</td>
<td>18.1</td>
<td>15.1</td>
<td>11.4</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Intelligent Systems</strong></td>
<td>2003</td>
<td>2004</td>
<td>2005</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
</tr>
<tr>
<td>1: Direct Funding</td>
<td>83.2</td>
<td>63.7</td>
<td>55.9</td>
<td>44.3</td>
<td>37.4</td>
<td>32.5</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>15.1</td>
<td>24.8</td>
<td>43.5</td>
<td>49.3</td>
<td>57.3</td>
<td>63.5</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>1.7</td>
<td>11.5</td>
<td>0.6</td>
<td>6.4</td>
<td>3.3</td>
<td>4.0</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Model-Based System Development</strong></td>
<td>2003</td>
<td>2004</td>
<td>2005</td>
<td>2006</td>
<td>2007</td>
<td>2008</td>
</tr>
<tr>
<td>1: Direct Funding</td>
<td>72.2</td>
<td>65.3</td>
<td>64.6</td>
<td>67.9</td>
<td>70.7</td>
<td>62.4</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>9.6</td>
<td>16.4</td>
<td>18.8</td>
<td>22.3</td>
<td>24.5</td>
<td>29.3</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>18.2</td>
<td>18.3</td>
<td>16.6</td>
<td>9.8</td>
<td>4.8</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Early 2009 large spaces have been compartmentalized into smaller rooms for PhD students and researchers to give them more quiet places to work in.

A.6 Processes in Research, Internal and External Collaboration

A.6.1 Research environment

The shared aim of all iCIS members is to perform high-quality research. iCIS tries to achieve its ambitions by creating a stimulating environment for its members in a structured context intended to obtain a goal-directed flow. A basic understanding is that scientific inventions require an open stimulating environment, but cannot be planned ahead. However, they can be steered in a certain direction, for instance via targeted funding or via human resource management. In the new PI-system, principal investigators play an important role. They create an enthusiastic atmosphere of collaboration, both within their group and between groups. PIs are expected to have a broad vision on the group’s future research lines and possible internal and external collaborations, for example, through joint grant proposals. Furthermore, they generate new research ideas and have charisma. The most common indicators—publications, citations, and external funding—are monitored on a regular basis, for instance via regular external peer reviews, via yearly appraisal and assessment interviews (jaargesprekken) or via (irregular) internal reviews of various activities. They can be an indication to reconsider concrete or even strategic decisions.

Since the rearrangement in terms of sections, each research programme is located in its own wing/corridor within the new Huygens building, which greatly stimulates social and scientific interaction between its members. All sections organize one or two weekly colloquia with internal and external speakers. All seminars are announced (by email and on a video system) and open to all members of the institute. Besides the section seminars, there are iCIS colloquia, typically organized on a monthly basis, by distinguished speakers on topics of interest to the general iCIS.
A.6.2 Teaching and research

iCIS aims at coherence between research and educational activities, as an important mechanism to transfer knowledge to fields of application and to educate new researchers in a swiftly evolving scientific discipline. Nevertheless, although student numbers are slowly increasing, relatively few computer and information science students are deeply interested in science for its own sake, which in practice means that it is often difficult to link master research projects to ongoing, state-of-the-art research which requires a strong mathematical background. Furthermore, most graduating students choose to pursue a career in industry, which severely limits the flow of "own" graduate students to PhD positions within iCIS. Besides the existing Kerkhoffs master on Security, a joint venture between the universities of Eindhoven, Twente and Nijmegen, a new initiative for a joint research master with mathematics, called Mathematical Foundations of Computer Science, has been started in an attempt to attract more mathematically oriented students, also from abroad. Furthermore, starting from fall 2009, the master curriculum of Artificial Intelligence will be a joint venture of the Faculty of Science and the Faculty of Social Sciences, further enhancing the involvement and visibility of iCIS' researchers.

All PhD students are part of one of the national research schools (for Nijmegen either IPA or SIKS) and are stimulated to join the courses and workshop offered (see Section A.3.3). iCIS staff members play an active role in these research schools, e.g., by organizing workshops and seminars. Prof. T. van der Weide is member of the SIKS Board of Governors, prof. R. Plasmeijer of the IPA Board.

A.6.3 Internal collaboration

Achieving more and better internal collaboration to obtain a larger critical mass and stronger research focus was one of the objectives of the recent rearrangement. As discussed in more detail in Section A.2.4, iCIS’ policy is to stimulate such collaborations, but not at any price and not where it makes no sense. Within Model-Based System Development, where four different subthemes meet, integration appears to be most essential to obtain critical mass. And indeed, as should be evident from the section’s self-evaluation, quite some links are being explored. Within Digital Security, a merger between the chairs on security of systems and information retrieval and information systems, privacy aspects in information retrieval as well as cybercrime form natural joint research topics in which both subgroups have expressed interests. The subgroups within Intelligent Systems —the former Foundations department and the machine learning group— are arguably furthest apart, with some possibilities to start joint projects, ranging from obvious (both are part of the Braingain consortium and work on the analysis and interpretation of EEG/MEG signals) to rather speculative (machine learning for proof assistants).

Obviously, there are also ample opportunities for joint high-quality research between sections, exploiting the expertise within the different research programmes. Common themes, essentially covered in the research programmes of all sections, are mathematical foundations of computer science and the use of model checkers. More specific opportunities to be further investigated include machine learning methods for outlier detection (IS and DS) and artificial intelligence for biomedicine (MBSD and IS). As already discussed in Section A.3.3, many collaborations exist with other research groups at the Radboud University, both within and outside the Faculty of Science. New collaborations that could be further explored within the Faculty of Science include metagenomics/ecogenomics with biology, computational science with astrophysics, and quantum logic with mathematics.
A.6.4 External collaboration

The (many) collaborations with national and international researchers outside the Radboud University are described in detail in part B with the self-evaluation of the individual sections. Many of these take place in the context of or started as nationally or internationally (mainly European) funded research projects, such as Ametist, Verificard, Protocure, Mowgli, and AH4IA.

The Radboud University initiated IRUN (International Research Universities Network), a network of 9 broad-based European research universities. The aim of IRUN is to further improve the quality of research and teaching at the universities involved. Within the Network, the exchange of researchers, lecturers and students is encouraged and facilitated. Until now, IRUN has mainly focused on (the mobility of) students. The Radboud University also has special ties (a covenant) with the Catholic University of Leuven. iCIS intends to pay special attention to potential collaborations with (the computer science departments of) these universities, for pragmatic reasons (additional funding opportunities) and in solidarity with the partners.

To sum up this whole section, iCIS cherishes an open research and social atmosphere, stimulating and encouraging interaction between its members and with others outside the institute. Efforts are underway to further improve the coherence between research and education.

A.7 Academic Reputation

iCIS is a medium-sized research institute with a clear focus on a few selected areas within computer science with particular emphasis on formal modeling and analysis. Within these areas, iCIS has built up a strong international reputation.

iCIS’ ambition to play an internationally leading role is, for instance, well recognized by Dutch and European funding agencies and reflected in the ability to attract substantial amount of funding from (inter)national competitive programs. Several iCIS members received prestigious prizes or personal grants, such as the Spinoza prize (“Dutch Nobel prize”) for Henk Barendregt (2002), the Pionier grant for Bart Jacobs (2002) in the area of program security and correctness, and the VICI grant for Tom Heskes (2006) in the area of artificial intelligence. Furthermore, iCIS members have led several larger European projects, such as Verificard and Ametist.

iCIS members frequently publish in the top journals and conferences in their areas\(^4\) such as Journal of the ACM, Artificial Intelligence, Bioinformatics, Information & Computation, Machine Learning, TACAS, CONCUR, NIPS, UAI, FM, ICALP, RTSS. Our researchers serve on the editorial board of leading journals such as Information & Computation, Theoretical Computer Science, Logical Methods in Computer Science, Neurocomputing (editor-in-chief), Foundations and Trends in Machine Learning, International Journal of Computational Intelligence Systems, BioData Mining, and Artificial Evolution and Applications. iCIS members served on more than 100 program committees during the review period.

For their papers, iCIS researchers received best paper awards at conferences such as ICALP, ETAPS, FMICS, BNAIC, NLDB and TFP. In July 2009, iCIS had 11 scientists in the list of 10.000 most cited authors in computer science of http://libra.mrsa.cn. In particular the work of Jacobs, Vaandrager, Barendregt, and Klop is highly cited. For example, their H-indices according to Google Scholar (numbers gathered on July 16, 2009) are 31, 31, 26 and 37, respectively. Scholar mentions more than 3600 citations to Barendregt’s book on the lambda calculus and more than 1000 citations to his article on lambda calculi with types. From the iCIS papers that appeared in the period 2003-2008, in particular the overview of JML tools and applications by Burdy et al., and the article of Lynch et al. on hybrid i/o automata have a particularly high citation impact (445 and 331 citations in Google Scholar).

The dismantling of the Mifare Classic chipcard by members of Digital Security in 2008 not only led to world-wide media coverage, with for instance time in BBC World’s “Click” program with about 300 million viewers across the world, but also to an article in Science Magazine.

Barendregt and Klop are members of the Dutch Royal Academy of Sciences. In 2008, Plasmeijer was granted the title of Doctor and Professor Honoris Causa at the Eötvös Loránd University. Since 2006, Vaandrager represents the area of Computer Science within the Board of the Physical Sciences division of the Netherlands Organisation for Scientific Research (NWO). Jacobs is member of the daily board of Sentinels, a joint national research programme in computer security funded by NWO, STW, and the department of Economic Affairs.

A.8 Internal Evaluation

The director of iCIS is responsible for the human resource management of the institute in close collaboration with the board of the Faculty of Science. Together, they perform all duties related to personnel, recruitment, education, training, mobility, outplacement, and legal guidance. All personnel are actively encouraged to discuss their career track and make a long term planning with respect to training and personal development. Most if not all education is paid by (the sections of) iCIS. Employees are individually expected to contribute significantly to the extension and development of the international success and visibility of the institute.

Ways to improve the output, acquisition, and time management are yearly discussed by the immediate supervisor in an official assessment and appraisal interview (jaargesprek). Customized forms have been developed and are widely used within the institute. The yearly assessment interviews are highly valued by everyone involved and contribute significantly to improve the high standards of individual performance in research and education to the overall ambition of iCIS. In a small number of cases, the evaluation resulted in substantial actions, such as a reduction in time allotted to research (often by request of the employee), the transfer of personnel to another supervisor or research group, or even to the termination of the contract.

Once every three years, researchers can apply for a role as (aspiring) principal investigator. The applications are evaluated by a committee including the vice-dean research of the faculty. In addition to individual evaluations, also the institute as a whole is evaluated by the faculty and university on the basis of its yearly research report, which is discussed during the yearly assessment and appraisal of the director by the dean.

A.9 External Validation

A.9.1 Previous external evaluation

iCIS, then called the Nijmegen Institute for Computer and Information Science and consisting of 4 departments, was last evaluated externally during the QANU evaluation that took place in 2003 (report from May 2004) over the period 1996-2002. Overall, the departments were rated ‘good’ to ‘very good’ (mainly) and ‘excellent’, with the exception of ST (Software Technology), which received scores between ‘satisfactory’ and ‘good’.

The recommendations of committee were taken very seriously. As already projected in the self-evaluation of the 2003 assessment, part of the department ITA (Informatics for Technical Applications) split off and formed the new department SoS (Security of Systems). Furthermore, some members of the department ST moved to the new department SoS. Further developments and insights led to the recent rearrangement from 5 departments to 3 sections.

A.9.2 Contributions to society

iCIS’ contributions to society, an integral part of its mission, are manifold. Valorization of research mainly takes place through LaQuSo (see Section A.3.3). To name a few highlights, projects have been performed on model-based testing of the Scottish election software (finding small errors in both the software and the specification), applying formal methods in certifying a document production system (improving and certifying a component which otherwise would have been fully rewritten [D161,D215,D273] and several security assessments varying from secure metering systems such
A.10. OVERVIEW OF THE RESULTS

as smart power meters and road pricing [D271,D286] to passports and e-voting [D96,D140,D284] (uncovering several vulnerabilities in each assessment).

iCIS' research members, in particular those from Digital Security, play a prominent role in public discussions and governance on the use of ICT in society. Prof. B. Jacobs was a member of the national voting process committee (Adviescommissie inrichting verkiezingsproces) that was appointed to redesign voting in the Netherlands. The dismantling of the Mifare Classic Chip by members of Digital Security urged Minister Ter Horst of the Interior (Binnenlandse zaken) to write a letter to the parliament (Tweede Kamer) to warn society for the implications and security risks. Also, the attempt of NXP (the manufacturer of the Mifare Classic) to prevent publication of a scientific article exposing the flaws of the chip and the subsequent ruling of the judge in favor of publication, started a broad public debate on academic freedom.

Much of iCIS' research has direct implications for society. Examples thereof are research on the analysis and interpretation of breast cancer images for early diagnosis, development of psychotherapy through a better understanding of mindfulness, and bioinformatics research to understand gene regulation of the malaria parasite that should lead to new vaccines.

As described in Section A.3.3, iCIS is devoted to improve research and education on ICT in developing countries. Several PhD students from Uganda already received their PhD at the Radboud University and more will follow. In the context of a collaboration with the Catholic University College of Ghana, iCIS' members regularly visit Ghana to teach computer and information science courses.

A.10 Overview of the Results

The results, in terms of numbers of publications in different categories, are given in Table A.14 for the whole institute and Table A.15 for the individual sections. Because of the recent rearrangement in sections, the results per section should be treated with much care: quite some publications are reported in more than one section, most notably because two authors that used to belong to the same department, ended up in different sections after the rearrangement. This in particular applies to the sections Model-Based System Development and Digital Security, who share 50 academic publications (mainly of prof. Van der Weide and prof. Van Eekelen). The overlap between Model-Based System Development and Intelligent Systems amounts to 10 academic publications, and between Digital Security and Intelligent Systems to 4 academic publications.

| Table A.14: Aggregated results of the institute (SEP Table 3) |
|-----------------------------|--------|--------|--------|--------|--------|--------|--------|
| 1. Academic publications    | 2003   | 2004   | 2005   | 2006   | 2007   | 2008   | Total  |
| a. in refereed journals    | 2      | 18     | 31     | 27     | 36     | 31     | 145    |
| b. in refereed proceedings | 60     | 70     | 77     | 100    | 99     | 90     | 496    |
| c. book chapters           | 1      | 3      | 5      | 8      | 10     | 10     | 37     |
| Total academic publications | 63     | 91     | 113    | 135    | 145    | 131    | 678    |
| 2. Monographs              | 7      | 2      | 5      | 2      | 12     | 12     | 40     |
| 3. PhD theses              | 1      | 3      | 2      | 8      | 3      | 8      | 25     |
| 4. Professional publications and products | 15 | 37 | 35 | 33 | 52 | 21 | 193 |
| Total publications         | 86     | 133    | 155    | 178    | 212    | 172    |

Further care is needed when one tries to relate the output in terms of number of academic publications to the research fte in Table A.6. The section Intelligent Systems grew rapidly over the last couple of years, which only with some delay can be expected to yield a similar increase in number of academic publications. The section Model-Based System Development shrunk in terms of research fte, but did manage to keep a high level of productivity, with a relatively large
percentage of conference papers and book chapters. The input (in terms of research fte’s) and output (in terms of publications) of the section Digital Security is most stable over the years.

Table A.15: Results: outcome numbers at programme level (SEP Table 6)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td>21</td>
<td>22</td>
<td>29</td>
<td>41</td>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>c. book chapters</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Total academic publications</td>
<td>22</td>
<td>25</td>
<td>37</td>
<td>49</td>
<td>44</td>
<td>43</td>
</tr>
<tr>
<td>2. Monographs</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3. PhD theses</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td>2</td>
<td>13</td>
<td>9</td>
<td>6</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>Total publications</td>
<td>25</td>
<td>40</td>
<td>47</td>
<td>58</td>
<td>63</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intelligent Systems</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td>0</td>
<td>5</td>
<td>14</td>
<td>11</td>
<td>15</td>
<td>14</td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td>6</td>
<td>15</td>
<td>13</td>
<td>19</td>
<td>28</td>
<td>23</td>
</tr>
<tr>
<td>c. book chapters</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Total academic publications</td>
<td>6</td>
<td>21</td>
<td>28</td>
<td>33</td>
<td>43</td>
<td>41</td>
</tr>
<tr>
<td>2. Monographs</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>3. PhD theses</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Total publications</td>
<td>11</td>
<td>26</td>
<td>29</td>
<td>40</td>
<td>57</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model-Based System Development</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td>4</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>18</td>
<td>11</td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td>35</td>
<td>40</td>
<td>52</td>
<td>48</td>
<td>45</td>
<td>38</td>
</tr>
<tr>
<td>c. book chapters</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>Total academic publications</td>
<td>40</td>
<td>53</td>
<td>69</td>
<td>63</td>
<td>70</td>
<td>58</td>
</tr>
<tr>
<td>2. Monographs</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>3. PhD theses</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td>11</td>
<td>27</td>
<td>31</td>
<td>24</td>
<td>33</td>
<td>10</td>
</tr>
<tr>
<td>Total publications</td>
<td>55</td>
<td>81</td>
<td>106</td>
<td>93</td>
<td>108</td>
<td>79</td>
</tr>
</tbody>
</table>

A.11 Analysis, Perspectives and Expectations

A.11.1 Strengths

- Within the focus areas that have been selected, iCIS’ researchers are internationally leading.
- The organization into three research programmes guarantees focus and critical mass.
A.11. ANALYSIS, PERSPECTIVES AND EXPECTATIONS

- The new PI system leads to the incentives and flexibility required for excellent research.
- iCIS’ researchers play a prominent role in public discussions and governance on the use of ICT in society.
- iCIS has strong ties to other scientific disciplines (neuroscience, biology, medicine, law, mathematics, engineering).
- Through LaQuSO, iCIS has a perfect outlet for contract research and valorization.
- iCIS has many contacts with government agencies and industry.
- iCIS has an excellent record in the training of PhD students, including those from developing countries.
- iCIS is successful in attracting external funding.
- iCIS has short and direct lines in management, with relatively little bureaucracy and a focus on its primary tasks: research and teaching.

A.11.2 Weaknesses

- The original plan, to increase the research time available to principal investigators, appears to be difficult to realize: most of them still have a substantial teaching and administrative load.
- Information science research has insufficient critical mass for a separate research line, partly because of the difficulty to attract high-quality researchers.
- Coherence between research and teaching is suboptimal in the mathematically oriented research topics, mainly because few computer and information science students are attracted to this type of research.
- iCIS no longer has structural, internally funded PhD positions, which seriously hampers opportunities for “blue sky” research.
- iCIS offers too few internal career tracks for young scientists.
- Whereas overall in the institute the ratio between direct and external funding is considered very good, there are considerable fluctuations between and within sections.
- Not all staff members (yet) have a habit of publishing in high-impact and leading disciplinary journals.
- The strong visibility of the Digital Security group in societal debates overshadows in the media the scientific role and achievements (e.g., iCIS security researchers are in the media often referred to as “hackers”).

A.11.3 Opportunities

- The integration of subthemes within sections as well as collaborations between sections can be furthered strengthened.
- Collaboration within the Faculty of Science, most notably with biology on metagenomics, astrophysics on data mining, and mathematics on quantum logic, can further increase.
- Participation in national research programs (FES, masterplan ICT) leads to new sources for external funding.
• The increasing general awareness of the societal relevance of, and dependence on, ICT and the need for fundamental ICT research to manage the complexity and security of ICT systems in practice opens up new possibilities for research funding and contract research\(^5\).

• The initiative of OCW/EZ to send knowledge workers from industry and consultancy on secondment to universities can help to further strengthen iCIS’ links to industry and valorization.

A.11.4 Threats

• A limited inflow of students as well as the financial status of the Faculty of Science as a whole may lead to further budget cuts.

• Faculty policies may further reduce incentives for entrepreneurship of staff members and their dedication to work on contract research and valorization.

• Relatively low acceptance rates for computer science research as a whole in the NWO Vrije competitie and Vernieuwingimpuls makes it increasingly difficult to attract funding, in particular for fundamental research without a direct link to applications.

• Diminishing interest of industry to (partially) fund computer and information science research may lead to less contract research as well as increasing difficulty to obtain matching for, e.g., STW proposals.

A.11.5 Analysis

During the review period, iCIS has become a thematically focused institute with a flexible PI-based internal organization aimed at scientific quality output. The current organization is designed to maintain and further strengthen iCIS’ leading position in selected research areas, even under financially turbulent conditions.

The PI-system does have a potential risk: it not only strengthens the PIs, but then indirectly also weakens (at least in standing) non-PIs. For its success, it is essential that PIs cover a large part of iCIS’ research areas and are reasonably spread over the three sections. The idea to relieve PIs to some extent from managerial and teaching obligations is under constant pressure and, also in light of increasing teaching duties of iCIS personnel as a whole, tends to become unrealistic.

With declining direct funding, iCIS’ vitality strongly depends on its success to raise external funding. The exceptionally low overall acceptance rates in some of the most relevant competitions (NWO, EU) are a serious concern. Where some (sub)groups have been very successful in recent years, others have been less fortunate.

Structural internally funded PhD positions are no longer available, which further limits possibilities to start new lines of research. An alternative would be to build a financial reserve, e.g., from additional income through contract research, and use this to finance new positions. Alas, faculty policies did not allow for this: all financial reserves at section and institute level were pruned away.

Despite iCIS’ attempts during the previous review period, a separate research line for information science with sufficient critical mass has not been achieved. Information science research is increasingly positioned alongside more technically oriented computer science research, which appears to be the best option given the current circumstances (limited budget, difficulty to attract high-quality researchers).

\(^5\)For instance, the National Advisory Centre for the Critical Infrastructure (NAVI) has recently started a national research programme to improve the way we protect our critical digital (and physical) infrastructure. See, see [https://www.navi-online.nl/English](https://www.navi-online.nl/English).
A.11.6 Adjusted goals

As will be clear from the above, iCIS adjusted its goals considerably during this review period: a clearer focus on a selective number of research themes and more emphasis on high-quality scientific research.

There are at this stage no reasons to make a major adjustment to our mission. The three different research programmes provide a reasonable coverage of computer science, information science, and artificial intelligence, which is required to fulfill iCIS’ teaching obligations in the corresponding curricula and to attract enough students. Focus and critical mass is needed to be able to compete with other Dutch universities and meet the quality standard imposed by the Radboud University, which in its Strategic Plan 2009-2013 (p. 10) states that “research programmes should achieve [at least] a ‘very good’ evaluation and that all programmes should continue to be evaluated as among the top 25% of Dutch universities”.

Adaptations within the research programmes are foreseen some years down the road, with the retirement of prof. H. Barendregt and (later) prof. T. van der Weide. Prof. Barendregt’s research line on theoretical foundations of computer science is covered by prof. Geuvers, who then may consider (even) closer collaboration with prof. Gehrke from mathematics at IMAPP to maintain sufficient critical mass. Prof. van der Weide’s research line on information retrieval will likely be drawn closer to digital security, which has already been started with the appointment of prof. W. Kraaij as extraordinary professor.

A.11.7 Adjusted strategy

iCIS will apply the following strategy to tackle the above-mentioned weaknesses and counter the threats.

The PI-system, now running only for 2 years, will be thoroughly evaluated before the next application round (mid 2010). This may lead to some changes, in particular with respect to the division between research/teaching/administrative duties and in the definition of the PI-criteria, putting more emphasis on quality of publications. Staff members will be encouraged, more strongly than before, to either become an aspiring PI themselves or to become a member of existing PI-groups.

The existing line of research on information science research is drawn closer to other lines of research within Model-Based System Development. iCIS will attempt to attract additional extraordinary professors on the interface between computer science and society to further strengthen information science research.

Several initiatives are taken to improve the coherence between research and education, most notably a new master in Mathematical Foundations of Computer Science and stronger involvement in the master program Artificial Intelligence. iCIS’ members continue to invest in PR activities to attract new students.

Staff members will need to tap new sources for funding. iCIS will (have to) rely more and more on the faculty and the university for guidance and assistance with applications. Such support for funding applications to NWO is good, but has to become better for other resources (EU, Senter Novem, ZonMw). The Faculty of Science recently started a new policy to support researchers with applications to the EU FP7 programme. iCIS will continue to invest in collaborations with industrial partners and researchers from other scientific disciplines, not only to increase funding possibilities, but also to do high-quality research and get new inspiration for computer science research.

iCIS intends to make use of new regulations and create permanent positions for excellent postdocs under strict (funding) conditions, but only when it is considered beneficial for these postdocs in the longer term.

Quality and not just quantity of research output will play a more prominent role in evaluations, e.g., for PI-ship. Publications in high-impact journals can also be achieved through collaborations with other scientific disciplines.
To balance the decline in baseline funding, iCIS has to (further) increase integration within sections and to strengthen their focus. Indirect funding is increasingly important, not only to maintain critical mass, but also to generate additional revenues that can be used to compensate for the lack of directly funded PhD positions. iCIS has to tap for other funding resources. iCIS encourages the entrepreneurship of its leading researchers and relies on the Faculty of Science to do the same as soon as possible.

In summary, it is strongly felt that, given the quality of its staff members and with the recent rearrangements, iCIS is well-prepared to meet its ambitions and to play an internationally leading role in the three chosen research programmes.
Table A.16: PhD candidates within Digital Security

<table>
<thead>
<tr>
<th>name</th>
<th>project</th>
<th>year started</th>
<th>graduated (comments)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berg, J. van den</td>
<td>Reasoning about Java programs in PVS using JML</td>
<td>2002</td>
<td>2-7-2009</td>
</tr>
<tr>
<td>Breunisse, C.</td>
<td>On JML: topics in tool-assisted verification of Java programs</td>
<td>2001</td>
<td>24-4-2006</td>
</tr>
<tr>
<td>Alsters, M.</td>
<td>Fundamentals of adaptive personalisation</td>
<td>2002</td>
<td>discontinued within 3 months</td>
</tr>
<tr>
<td>Vrieze, P. de</td>
<td>Language based security for Java and JML</td>
<td>2002</td>
<td>13-12-2006 (RPP)</td>
</tr>
<tr>
<td>Warnier, M.</td>
<td>Formal and computational cryptography</td>
<td>2003</td>
<td>9-5-2008</td>
</tr>
<tr>
<td>Garcia, F.</td>
<td>La volonté machinale</td>
<td>2003</td>
<td>21-1-2008 (RPP)</td>
</tr>
<tr>
<td>Pieters, W.</td>
<td>Tracing anonymity with coalgebras</td>
<td>2004</td>
<td>10-3-2008 (cum laude; RPP)</td>
</tr>
<tr>
<td>Hasuo, I.</td>
<td>Categorical quantum logic</td>
<td>2004</td>
<td>end of 2009 (RPP)</td>
</tr>
<tr>
<td>Heunen, C.</td>
<td>Developing the &quot;secure network of objects&quot; paradigm</td>
<td>2004</td>
<td>discontinued after 1st contract</td>
</tr>
<tr>
<td>Nguyen, T.</td>
<td>Security and cryptographic protocols</td>
<td>2005</td>
<td>n/a</td>
</tr>
<tr>
<td>Chmielewski, L.</td>
<td>Analysis of anonymity</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Andres, M.</td>
<td>Generating correct software</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Lensink, L.</td>
<td>Amortized heap space usage analysis</td>
<td>2006</td>
<td>discontinued after 1 year (preferred working in industry)</td>
</tr>
<tr>
<td>Kesteren, R. van</td>
<td>Code-model conformance</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Tamalet, A.</td>
<td>Analysis of anonymity</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Koning Gans, G. de</td>
<td>Secure software surgery</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Madlener, K</td>
<td>Verification and web applications</td>
<td>2009</td>
<td>n/a</td>
</tr>
<tr>
<td>Sessink, J.</td>
<td>The effectiveness of ICT in knowledge management activities</td>
<td>2009</td>
<td>n/a</td>
</tr>
<tr>
<td>Omona, W.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table A.17: PhD candidates within Intelligent Systems

<table>
<thead>
<tr>
<th>name</th>
<th>project</th>
<th>year started</th>
<th>graduated (comments)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Niqui, M.</td>
<td>Formalising exact arithmetic: representations, algorithms and proofs</td>
<td>2000</td>
<td>27-9-2004 (RPP)</td>
</tr>
<tr>
<td>Stein, J.</td>
<td>Formalising linear algebra</td>
<td>2000</td>
<td>finished without thesis</td>
</tr>
<tr>
<td>Calle, M.</td>
<td>Integrative physiology and communication in the amphibian brain</td>
<td>2002</td>
<td>2-11-2006</td>
</tr>
<tr>
<td>Loeb, I.</td>
<td>Natural deduction: sharing by presentation</td>
<td>2003</td>
<td>20-6-2007 (RPP)</td>
</tr>
<tr>
<td>Jurgeleinaite, R.</td>
<td>Symmetric causal independence models</td>
<td>2003</td>
<td>19-1-2009</td>
</tr>
<tr>
<td>Mamane, L.</td>
<td>Interactive mathematical documents</td>
<td>2003</td>
<td>n/a (part-time)</td>
</tr>
<tr>
<td>Kaliszky, C.</td>
<td>Formalizing elementary analysis rigorously</td>
<td>2005</td>
<td>3-9-2009 (RPP)</td>
</tr>
<tr>
<td>O’Connor, R.</td>
<td>Formalization of logic and analysis in type theory</td>
<td>2005</td>
<td>5-10-2009 (RPP)</td>
</tr>
<tr>
<td>Cseke, B.</td>
<td>Artificial intelligence for industrial applications</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Hurk, P. van den</td>
<td>The effect of mindfulness meditation on the brain</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Birlutiu, A.</td>
<td>Personalization through Bayesian preference elicitation</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Claassen, T.</td>
<td>Learning causal models from multiple datasets</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Whitmash, S.</td>
<td>Neural state and trait effects of meditation</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Bahramisharif, A.</td>
<td>Transfer learning for brain-computer interfacing</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Gori, F.</td>
<td>Machine learning for metagenomic data analysis</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Jancura, P.</td>
<td>Knowledge discovery through protein-protein interaction networks</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Choi, Y.</td>
<td>Mindfulness and well-being</td>
<td>2009</td>
<td>n/a</td>
</tr>
</tbody>
</table>
### Table A.18: PhD candidates within Model-Based System Development

<table>
<thead>
<tr>
<th>name</th>
<th>project</th>
<th>year started</th>
<th>graduated (comments)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mol, M. de</td>
<td>Reasoning about functional programs</td>
<td>1998</td>
<td>4-3-2009</td>
</tr>
<tr>
<td>Groot, A. de</td>
<td>Practical automaton proofs in PVS</td>
<td>2000</td>
<td>6-3-2008</td>
</tr>
<tr>
<td>Alimarine, A.</td>
<td>Generic functional programming</td>
<td>2000</td>
<td>14-9-2005</td>
</tr>
<tr>
<td>Hoppenbrouwers, S.</td>
<td>Freezing language; conceptualisation processes across ICT-supported organisations</td>
<td>2000</td>
<td>10-12-2003</td>
</tr>
<tr>
<td>Cheung, L.</td>
<td>Reconciling nondeterministic and probabilistic choices</td>
<td>2002</td>
<td>18-9-2006 (<em>cum laude</em>; RPP)</td>
</tr>
<tr>
<td>Fregonese, S.</td>
<td>Verification of real-time embedded systems</td>
<td>2002</td>
<td>discontinued (moved abroad)</td>
</tr>
<tr>
<td>Gebremichael, B.</td>
<td>Expressivity of timed automata models</td>
<td>2002</td>
<td>11-12-2006 (RPP)</td>
</tr>
<tr>
<td>Gilis, B. van</td>
<td>Aptness on the web</td>
<td>2002</td>
<td>8-12-2006 (RPP)</td>
</tr>
<tr>
<td>Hendriks, M.</td>
<td>Model checking timed automata: techniques and applications</td>
<td>2002</td>
<td>4-4-2006 (RPP)</td>
</tr>
<tr>
<td>Arhel, D. van</td>
<td>Autonomous middleware</td>
<td>2003</td>
<td>discontinued after 1st contract</td>
</tr>
<tr>
<td>Frantzen, L.</td>
<td>Symbolic extensions of the IOCO theory</td>
<td>2003</td>
<td></td>
</tr>
<tr>
<td>Gerven, M. van</td>
<td>Bayesian networks for clinical support</td>
<td>2003</td>
<td>5-9-2007 (RPP)</td>
</tr>
<tr>
<td>Weelden, A. van</td>
<td>Putting types to good use</td>
<td>2003</td>
<td>17-10-2007 (RPP)</td>
</tr>
<tr>
<td>Flesch, I.</td>
<td>On the use of independence relations in Bayesian networks</td>
<td>2004</td>
<td>27-11-2008 (RPP)</td>
</tr>
<tr>
<td>Hommersom, A.</td>
<td>On the application of formal methods to clinical guidelines</td>
<td>2004</td>
<td>18-4-2008 (RPP)</td>
</tr>
<tr>
<td>Berendsen, J.</td>
<td>Incremental analysis of fault-tolerant real-time algorithms</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Igna, G.</td>
<td>Design of adaptive data paths in printers</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Heisdarian Dehkordi, F.</td>
<td>Abstraction refinement for timed systems</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Heijden, M. van den</td>
<td>Development of a Bayesian network model</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Noort, T. van</td>
<td>Demand driven workflow systems</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Verbeek, F.</td>
<td>Formal verification of deadlock avoidance mechanisms</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Lijnse, B.</td>
<td>Dynamic workflows for planning</td>
<td>2009</td>
<td>n/a</td>
</tr>
<tr>
<td>Wilmont, I.</td>
<td>Using games for collaborative modelling</td>
<td>2009</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### Table A.19: Contract students from abroad (Portugal, Pakistan, Uganda)

<table>
<thead>
<tr>
<th>name</th>
<th>project</th>
<th>year started</th>
<th>graduated (comments)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cruz-Filipe, L.</td>
<td>Constructive real analysis: a type-theoretical formalization and applications</td>
<td>2001</td>
<td>15-6-2004 (RPP)</td>
</tr>
<tr>
<td>Kanagwa, B.</td>
<td>Design, discovery and construction of service-oriented systems</td>
<td>2007</td>
<td>21-4-2009</td>
</tr>
<tr>
<td>Nabukenya, J.</td>
<td>Improving the quality of organisational policy making</td>
<td>2007</td>
<td>3-3-2009 (RPP)</td>
</tr>
<tr>
<td>Abbas, S.</td>
<td>Bayesian perception</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Nakakawa, A.</td>
<td>Collaborative evaluation of enterprise architecture design alternatives</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Ngobye, M.</td>
<td>Specification and verification of software agents</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Ssebuggwawo, D.</td>
<td>A pragmatic and semiotic approach to business process modelling</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>Tulinayo, F.</td>
<td>Integration system dynamics with conceptual and process modelling</td>
<td>2008</td>
<td>n/a</td>
</tr>
<tr>
<td>name</td>
<td>project</td>
<td>year started</td>
<td>graduated (comments)</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Frehse, G.</td>
<td>Compositional verification of hybrid systems using simulation relations</td>
<td>2000</td>
<td>10-10-2005</td>
</tr>
<tr>
<td>Farkas, J.</td>
<td>A semiotically oriented cognitive model of knowledge</td>
<td>2005</td>
<td>23-4-2008</td>
</tr>
<tr>
<td>Overbeek, S.</td>
<td>Foundations and applications of intelligent knowledge exchange</td>
<td>2005</td>
<td>24-4-2009</td>
</tr>
<tr>
<td>Breemen, A. van</td>
<td>Peirce’s theory of interpretants and the possibility of (self)control</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Paauwe, M.</td>
<td>Architecture principles</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Wagter, R.</td>
<td>General enterprise architecture</td>
<td>2006</td>
<td>n/a</td>
</tr>
<tr>
<td>Willems, T.</td>
<td>Qualification of financial architecture</td>
<td>2007</td>
<td>n/a</td>
</tr>
<tr>
<td>Onderdelinden, E.</td>
<td>Appreciation of IT in mergers and acquisitions</td>
<td>2008</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Part B
Chapter B.1

Digital Security

Title of the Research Programme: Digital Security (DS)

Research Area and Mission: As information technology pervades every corner of society, protection of information is becoming ever more important. Our mission is to contribute to a better understanding of security and privacy issues, and to develop theories and formal methods to analyse and improve security in the digital world. As part of our mission we take an active role in public debate on socially relevant issues involving computer security, such as privacy, transparency, and on the wider issue of open source and open standards.

In the section’s research, a coarse distinction can be made between two sub-themes, namely (i) software security & correctness and (ii) identity-centric security & privacy. The latter line of research was in the start-up phase during the reporting period, the former was established from the beginning. In the area of software security & correctness, research focuses on the formal specification and verification of (security-critical) software. In the area of identity-centric security & privacy, research is carried out on the semantics, analysis, and design of security protocols, on privacy and anonymity, and more concrete topics such as electronic voting and particular applications of smartcards and RFID tags. Also, as information search technology is increasingly relevant for esp. privacy, the iCIS research on data mining and search technology is now part of the Digital Security section.

Keywords: computer security, software verification and specification, smartcards, RFID, electronic voting, identity management, information retrieval, data mining

Programme Leaders: prof.dr. B.P.F. Jacobs and dr.ir. E. Poll (since autumn 2005)

Starting Date of the Programme: 2002

Affiliations outside iCIS: DS participates in the Dutch graduate schools IPA (Institute for Programming research and Algorithmics) and SIKS (Information and Knowledge Systems), the latter being more relevant for search-related research.

B.1.1 Leadership

The current section Digital Security (DS) was founded in 2008 (see part A), and groups together researchers interested in the topic of digital security in a broad context. The predecessor Security of Systems (SoS) group was founded by prof. Jacobs in 2002. In light of his administrative duties as head of iCIS, dr. Poll took over as interim group leader in 2005. In practice, some responsibilities are shared between them. The group involves one PI (Jacobs) and two aspiring PIs (Poll and van Eekelen).

With several long term lines of research within the group, we actively look for and exploit opportunities for more focused, short term projects – often more practical work on case studies – as a way of fostering collaborating between people with different interests and expertise.
Besides possible funding from traditional sources (NWO, STW, EU), opportunities for contract research projects are also actively pursued. Here the section has taken the lead in establishing the cooperation with the TU Eindhoven in the form of the LaQuSo research lab for contract research.

Group members are given the freedom to spend some of their time to freely pursue their wider research interests and pet interests, also on topics unrelated to digital security, as long as this produces quality research with ample output in the form of publications and/or projects.

Weekly lunch meetings are held to discuss ongoing organisational and scientific issues. Here people take turns to give informal talks about work in progress, open problems, or interesting challenges. It also provides an opportunity for PhD students to present and hear about work from others other than their direct supervisor.

Responsible disclosure of security problems is taken seriously, like in the Mifare Classic case. At the same time we are extremely reluctant to enter into Non-Disclosure Agreements, in order to avoid restrictions in publications and public debates.

B.1.2 Strategy and Policy

History and context

The (predecessor) group of ‘Digital Security’ was founded in 2002, as the ‘Security of Systems’ group, following an NWO Pionier grant awarded to prof. Jacobs for the project PROSECCO (Program Security and Correctness). The group was split off from the chair “Informatics for Technical Applications”, with a clear aim to broaden and re-focus its area of research towards computer security. Prior to 2003 the group, informally known as the LOOP group, mainly worked on Java program verification. At the start in 2008 the group was expanded with members from the former IRIS group working on information systems and information retrieval, and re-baptised ‘Digital Security’.

Strategy

In the area of software security and correctness, the group was already well-established as a leading international group working on formal verification for Java at the start of the current assessment period, with a special focus on the Java Card, the Java dialect for programming smartcards.

Here the aim has been to strive for impact at an international level: through the active collaboration on the specification language JML, European projects (VERIFICARD, MOBIUS, ROBIN, CHARTER, and the ESF-COST network on Verification of Object-Oriented Software). To broaden the scope in application areas, we have explored new application areas apart from Java Card, for instance J2ME mobile phone applications in MOBIUS, operating system hypervisors in ROBIN, and Java real-time applications in CHARTER. To broaden the scope in techniques, we started new, more exploratory, lines of research on software surgery (combining program verification and model checking) and resource consumption analysis (for which we found an interesting application area in Java real-time applications in CHARTER).

At a national level, an aim has been to further harness our expertise in collaboration with industry, for instance through the STW/Sentinels projects PINPAS (on Java Card smartcards, in collaboration with Brightsight and ST Microelectronics) and JASON (on Java for embedded platforms and Service-Oriented Architecture, in collaboration with Chess IT).

The strategy to broaden the scope of the group into the field of security has been very pragmatic, namely

- attracting (scarce) experienced senior personnel with a security background, namely dr. Hoepman, prof. Verheul and, more recently, prof. Kraaij, (both professors by special appointment);
building on existing expertise to investigate broader computer security issues (for example, expertise on Java and Java Card led to research on smartcards in general and on security protocols);

invest in new areas that were regarded as highly relevant given our mission, such as e-voting;

actively pursuing the possibilities of contract research, as a way to establish links with the more practical side of computer security and privacy, and with socially relevant issues.

Often the measures above have fed into each other.

As relative newcomers to the field of security – from an international perspective – we have taking the initiative to collaborate with the (few) security researchers at other universities in the Netherlands. Here we also joined forces in the Kerckhoffs Institute (www.kerckhoffs-institute.org), a collaboration with the security groups at the University of Twente (UT) and TU Eindhoven Technology (TU/e) to offer a joint Master track specialising in computer security.

We also took steps to establish links outside the immediate field of computer science: within the Radboud University Nijmegen with the Institute for Science, Innovation and Society (ISIS) on e-voting, with the law faculty at the Radboud University, on ICT/penal law, and with the language faculty within the Information Foraging Lab (IFL, see below) on natural language processing. Outside our university (and outside our immediate field), there are close links with the Institute for Law, Technology, and Society (TILT) at the University of Tilburg, on privacy and cyber crime.

Clearly information systems and information retrieval technology are highly relevant to the issue of privacy. For this reason staff working in these areas (prof. van der Weide and prof.em. Koster) joined the Digital Research group following the department reorganisation in 2008. A new professor by special appointment, prof. W. Kraaij, was joined in the autumn of 2008 to further boost research in this area, which led to the formation of a new sub-group in the Information Foraging Lab (IFL).

B.1.2.1 Software security and correctness

An important line of research in the group is the formal specification and verification of software, in particular Java programs. Long-term goal here is the formal verification of security-critical software.

Specification and verification of Java programs

Research on Java program specification and verification has been carried out in the EU project VERIFICARD (which we coordinated), a successor EU project MOBIUS, the NWO projects CARDSPEC and SAMASC, and an ESF Cost Network on ‘Verification of Object-Oriented Software’. We developed a formal semantics for sequential Java [D46, D13, D27], a semantics and logic for the Java specification language JML [D27, D4] and associated verification tool support [D162, D164]. Initially, case studies were mainly Java Card smartcard programs [D28, D40], including a commercial smartcard application [D67] that was successfully verified. Since then, work on Java verification has continued to progress to look at ambitious case studies, for example e-voting software [D199]. More recently work on case studies has focused on Java software for mobile phones, where we for instance verified an implementation of SSH [D203].

In MOBIUS we have begun to tackle the challenge of verifying multi-threaded Java code, with support for a notion immutability for Java objects [D189] and an approach to specify and verify multi-threaded Java code (e.g. [D253]).

Research on Java Card programs has evolved into research on the trickier aspects of smartcard technology, for instance the reaction to power failures [D41] and the platform level security the Java Card runtime environment [D265].

An important success in the worldwide work on Java verification has been the formal specification language JML for Java. We have played a major role in the development of JML and taken the lead in using JML as specification language in case studies. From our initial collaboration
CHAPTER B.1. DIGITAL SECURITY

Figure B.1.1: Overview of the Software Surgery Methodology

with prof. Leavens (Univ. of Central Florida), JML has grown into the de-facto standard formal specification language for Java ([www.jmlspecs.org](http://www.jmlspecs.org)) used at dozens of research institutes around the world (and in many development projects). We have given the tutorials on JML at leading international conferences (ETAPS, ECOOP, FME) and co-authored the JML reference manual [D229]. The 2005 JML overview article for which we took the initiative [D68] currently has well over 400 citations in Google Scholar.

In addition to the research on post-hoc verification, we also investigate ways to simplify the construction of secure Java software, through the development of the JASON middleware framework to handle security aspects (authentication, access control, secure communication, etc.). The JASON architecture, originally aimed at smartcards, now targets Java-programmable embedded devices [D183] and more generally Service-Oriented Architecture [D245].

**Verification of C programs**

The verification approach we pioneered for Java, using a shallow embedding of the semantics in a theorem prover, has also been pursued for the verification of C++ code in the EU project ROBIN, with the aim to verify properties of an operating system security kernel (hypervisor) [D205].

**Resource consumption & software surgery**

Work on the analysis of resource consumption started in the NWO project Amortized Heap Space Usage Analysis (AHA), where for a small functional language type systems have been developed to analyze output-on-input size dependencies for function definitions. The focus is on checking and inference of polynomial complexity including non-monotonic polynomials ([D209, D204, D272, D243, D296, D287, D295]). The results of this work will be transferred to imperative object-oriented languages, focusing on Real-Time Java (in the EU-Artemis CHARTER project that was awarded in December 2008).

The ‘software surgery’ research explores the verification of safety-critical software using a combination of model checking and theorem proving, exploiting the respective advantages of these techniques, see Figure B.1.2.1. This approach can ultimately yield highly reliable code, automatically extracted from fully verified formal models. Currently, the research on this topic is exploratory: various phases of the methodology have been performed on real-life case studies ([D179, D262, D273, D274, D241]), also in collaboration with NASA Langley Research Center. The most recent case study ([D274, D298]), (verifying a re-entrant lock implementation from a professional software library) won the best paper award at the 13th International Workshop on Formal Methods for Industrial Critical Systems (FMICS) in 2008. In the near future, we expect to verify for the Dutch Rijkswaterstaat a key part of the software of the Dutch Maeslant Storm Surge Barrier (‘the worlds largest autonomous robot’).

**Coalgebras**

More in the background, the Digital Security group is involved in more theoretical research, in particular in the area of coalgebras. These mathematical structures form an abstract foundation for state based systems and for operational semantics of programs. A general and abstract theory
of traces of computations has been developed [D280], which has been applied as a semantics of
security protocol and in a theory of anonymity [D191, D176], as already mentioned above.

Another more theoretical project is a joint PhD project with the mathematics department
(prof. K. Landsman), working on interpreting quantum protocols within the categorical setting of
topos theory (intuitionistic type theory and logic) [D237, D257].

B.1.2.2 Identity-centric security, privacy & search

Outside the field of software, our research into computer security centres around ‘identity-centric
security’, by which we mean security issues where the end-user – and the information protection
concerns of the end user, notably privacy – are very much at the centre. This includes research
on policies and protocols for identity management, the mechanisms such as smartcards and RFID
tags that can be used for this, the security protocols and applied cryptography involved, and the
impact of all this privacy and anonymity on the end-user.

Security protocols

Our interest in on security protocols grew from the work on smartcards software (which typically
has to securely implement some security protocol) and was already a field of research of dr.
Hoepman, who joined the group in 2002.

Our research on security protocols includes research on the design of protocols, research on the
formal analysis of protocols, and more foundational research on the semantics and logic of security
protocols and notions such as anonymity to enable such analyses. Privacy is an underlying theme
that runs through all this work.

Research on protocol design has produced a range of protocols, for instance for accountability in
decentralised systems [D130], digital cash that can be used in P2P or grid systems [D84], ephemeral
pairing on anonymous networks [D89], and road pricing [D292]. Work on the design on security
protocols was partly carried out in the IOP GenCom project PAW (Privacy in an Ambient World)
and continues in the recently started Sentinels project PEARL (Privacy Enhancing Architecture
for RFID Labels).

In the field of protocol analysis, research on cryptographic primitives investigated the relation
between the symbolic and the computational approach to prove the security of cryptographic pro-
tocols [D83, D135]. In the NWO project NN (Analysis of Anonymity) model-checking techniques
have been developed to verify anonymity properties of protocols [D244]. More theoretical work
on coalgebras within the group (also discussed above) has been applied to provide semantics and
logics for security protocols\(^1\) [D291] and to develop a formal theory of anonymity (e.g. [D191]).

E-voting

E-voting is a more concrete topic where several of our research interests – security protocols, the
societal aspects of security, and security of software – meet.

A PhD project carried out in collaboration with the Institute for Science, Innovation and
Society (ISIS, dr. Consoli), and the Faculty of Philosophy (dr. Becker) investigated the societal
and philosophical questions raised by e-voting [D281].

On the more practical side, several systems for (remote) electronic voting were investigated.
For the KOA (Kiezen op Afstand) experiment for internet voting in the European elections by
expats carried out by the Dutch government we performed a blackbox security test of the voting
website and developed Java vote counting software, parts of which were formally specified, tested,
and verified [D42, D199]. We also performed a security analysis of the RIES voting system used
for Waterschapsverkiezingen and expat voting in European elections [D96, D284]. This RIES
system allows counting by independent parties, which was actually done by our group in both
deployments (yielding exactly the same outcome as the official one).

Smartcards and RFID

Smartcards and RFID are another topic where several of our research interests and areas of expertise meet. (As smartcards are increasingly contactless, the precise border between smartcards and RFID tags is increasingly vague.) Apart from the research on smartcard software and RFID protocols already discussed above, on the more practical side we have investigated concrete smartcard and RFID applications, in particular electronic passports and Mifare Classic RFID cards.

The new electronic passport incorporates a contactless smartcard. We investigated security and privacy issues of the e-passport [D140, D267] and developed an open source Java Card implementation of the passport (http://jmrtd.org), as an interesting Java Card case study and an – albeit unofficial – open source reference implementation of the international specifications by the UN for the wider research community.

Work on Mifare Classic RFID cards grew from curiosity in how the personnel pass of our university – and the associated paid parking system – works. These cards turned out to use Mifare Classic, the leading industry standard for RFID technology. Hundreds of millions of such cards are deployed, e.g. as public transport or building access cards. Our research into the technology of Mifare Classic culminated into the reverse engineering and breaking of the proprietary cryptographic CRYPTO1 algorithm used in these cards. Within the reporting period this work resulted in two scientific publications, at ESORICS [D250] and CARDIS [D247], and was described in Science ². It also drew worldwide attention in the security community and the media. For the work on Mifare Classic we developed infrastructure (both hardware and software) for the security analysis of RFID systems, including a hardware emulator produced by the faculty’s Technical Centre.

A more practical project developing an RFID application, as opposed to analysing an existing one, is the OV-CHIP 2.0 project, funded by NLNet Labs, which investigates the feasibility of a privacy friendly public transport card using zero-knowledge proofs.

Information retrieval/data mining/IFL

After the formation of the DS group the Information Foraging Lab (IFL) has been set up as an inter-faculty research team focusing on the development of models and techniques supporting modern knowledge workers. IFL is a collaboration between researchers from the Institute of Computing and Information Sciences (iCIS) from the Faculty of Science and the Language and Speech Unit of the Arts and Language Faculty, both at Radboud University Nijmegen.

Information foraging refers to the iterative process of finding and processing relevant information by systematically deploying various information sources such as search engines, multimedia portals and community sites. Examples of information processing are aggregation, summarization, classification, curation and contextual interpretation.

The IFL is a blend of researchers in information retrieval, natural language processing (NLP) and speech technology. The current research foci are: web: topology, dynamics, query log analysis; trend analysis; question answering; user modeling: activity modeling, profiling; social networks; semantic and contextual search; speaker diarization and speaker identification; deep NLP for patent retrieval. Some initial results are related to community detection on the Internet ([D192] and [D289]), analyzing click data ([D290], [D297]), sentiment mining ([D294]), and video ([D293]).

B.1.2.3 Valorisation and outreach

We take an active role in the public debate on issues such as e-voting, smart cards (in banking, transport, or health), privacy and open source. We have published about these issues in the scientific literature (e.g. in the Communications of the ACM [D177]) and in professional journals (Automatiseringsgids, Informatiebeveiliging, Computable), and written over a dozen opinion articles in national newspapers (Trouw, NRC, Volkskrant, Reformatorisch Dagblad). Our Code-

Yard project (www.codeyard.net) involves students at secondary schools in open source software projects.

We see contract research not only as an important opportunity to disseminate knowledge and expertise outside the academic community, but also as an inspiration for scientific research, and a way to establish links with the more practical side of computer security. Our success with contract research led to the collaboration with the TU Eindhoven in LaQuSo, the Laboratory for Quality Software, which started in 2006. The DS group is very active within this LaQuSo context.

B.1.3 Processes in Research, Internal and External Collaboration

Research

Given the size of the group and the range of research topics, the group is organised in a decentral manner, with several sub-groups headed by senior staff working of more specific topic, often organised by externally funded project.

Weekly informal lunch-colloquia are held as a way to stimulate interaction and discussion within the group. In addition to the sub-groups, which focus on a broader topic over a longer period of time, shorter term collaborations, in the form of projects on very specific topics, are actively encouraged. These collaborations typically involve members of various sub-groups – ideally, they are case studies that bring together several lines of research – and provide a useful way to foster collaboration within the whole group. For example, investigation of the KOA system for electronic voting brought together interests in e-voting and Java program verification within the group; a LaQuSo project to test vote-counting software for the Scottish elections brought together our interests in e-voting and testing expertise from the MBSD group. Such projects also offer an opportunity for new PhD students to discover a thesis topic that really excites them, and more generally interact with others besides their direct supervisor.

This attention to collaborations does not mean that people are prevented from pursuing their own interests and fascinations, as long as this explores promising directions and produces quality results.

For PhD students there is a standard process in the faculty in the form of a Training and Guidance Plan (Opleidings- en begeleidingsplan, OBP). All PhD students join the research school IPA, or, if they are more active in the area of information search technology, SIKS.

Apart from the annual meetings of individual staff members with their direct supervisor (jaargesprekken), the iCIS-wide evaluation of application of PIs provides an additional mechanism to evaluate the quality of research.

Internal Collaboration

Within iCIS there are collaborations with MBSD (for instance in the area of model checking and functional programming and through LaQuSo projects) and with IS (in the area of theorem proving, coalgebras and coinduction, and more generally, category theory).

Outside iCIS, but within the Radboud University, there are collaborations with the Mathematics department (IMAPP, prof. Landsman, prof. Gehrke). As part of these collaborations, there has been a joint PhD student (defence expected in 2009) and a joint NWO proposal which been awarded in 2008.

As computer security is a broad topic with a reach beyond computer science, we have been looking for possible with groups outside iCIS and the field of computer science, at the Radboud university and beyond. A collaboration with ISIS (Institute for Science, Innovation and Society) at the Radboud University has led to a PhD thesis on the topic of e-voting, with a co-promotor from the Faculty of Philosophy. In the Centre for Cybercrime studies (CYCRIS) we collaborate with the Faculty of Law of the Radboud University (prof. Buruma, mr. van der Staak) and the University of Tilburg (prof. Koops, dr. Leenes, dr. Schellekens).
External Collaboration

On a national level, we have collaborations with several other universities (TU/e, TUD, UT) and several companies (Chess IT, Brightsight, ST Microelectronics, Philips, TNO ICT, Riscure) which have led to national projects funded through NWO, STW/Sentinels, and SenterNovem (namely the projects PAW, JASON, PINPAS JC, PEARL, SAMASC).

On a national level we have also taken a leading role in establishing Safe-NL (www.safe-nl.org), a platform for computer security researchers from academia, industry and government, which organises bi-annual workshops to bring together people from these different areas.

Contacts with industry are also maintained through participation in professional organisations such as the Q-society (society for ICT Quality Professionals), the working group ‘Kwaliteit’ of the Platform voor Productsoftware, OWASP Netherlands, and the annual VVSS symposium organised by LaQuSo.

To accomplish our mission of having a positive impact on the Dutch ICT landscape when it comes to security and privacy, contacts outside academia are essential. We have taken advantage opportunities to become involved in society-relevant issues involving ICT security and privacy, sometimes in the form of contract research through LaQuSo. For instance, close contacts now exist with several ministeries: internal affairs (passports, voting, access cards), transport (ov-chip, road pricing, e-driving license), health (electronic patient records).

On an international level, we participate in several European projects and networks:


- EU IST Thematic Network RESET (Roadmap for European Research on Smartcard Technologies).

- EU IST project MOBIUS (Mobility, Ubiquity and Security - Enabling proof-carrying code for Java on mobile devices): INRIA, Chalmers University of Technology, Imperial College, Univ. of Edinburgh, University College Dublin, TU Zurich, Trusted Labs, TLS, France Telecom/Orange R&D, Tallinn Institute of Cybernetics, Ludwig-Maximilians-University Munich, IMDEA Software, TU Darmstadt, Warsaw University.

- EU project ROBIN (Open Robust Infrastructures): ST Microelectronics France, TU Dresden, Secunet GMBH.

- EU Marie Curie Internal Fellowship SOJOURN (for dr. Schubert of Warsaw University).

- ESF COST Action IC0701: Formal Verification of Object-Oriented Software: 15 participating countries.

A longer running international collaboration is in the JML project (www.jmlspecs.org) where we collaborate with academic institutes worldwide on a common specification language for Java.

In two large Nuffic-funded projects, iCIS collaborates with RU Groningen and TU Eindhoven on developing the training and research capacity at public universities in Uganda in the field of ICT. The first of these focused largely on teaching, with the training of Master and PhD students, while the second focused exclusively on research, by setting up 4 research groups and training 12 PhD students. The DS group is very active in this area, not only in overall coordination, but also in actual supervision of the PhD students. Many of the students from Uganda show great interest in security issues.

These projects and other collaborations have led to joint publications with, among others: dr. D’Argenio (Univ. of Cordoba), prof. B. Baryamureeba (Makerere Univ.), dr. Barthe (IMDEA, Spain) dr. Butterfield (Trinity Colledge Dublin) prof. Chalin (Concordia Univ. Montreal), dr. Cok (Kodak Eastman, USA), dr. Cregut (France Telecom), prof. Ernst (MIT), prof. J. Fairhurst (Univ. Pretoria), prof. N. Fuhr (Univ. Duisburg-Essen), dr. Galbraith (Royal Holloway), dr. Galindo (Malaga Univ.), dr. Huisman (INRIA, France) dr. Kiniry (UCD Dublin), prof. Kutten (Technion,
Haifa), prof. Lahmas (Univ. Glasgow), prof. Leavens (Univ. of Florida), dr. Leino (Microsoft Research, USA), dr. Marché (INRIA, France) prof. Müller (ETH Zurich), prof. R. du Plessis (Univ. Pretoria), dr. Rushby (SRI, USA), dr. Schubert (Warsaw University), dr. Spoto (Univ. of Verona), dr. Sokolova (Salzburg University), prof. van Rijsbergen (Univ. Glasgow), dr. Tsigas (Chalmers, Sweden), dr. Unustula (Tallinn Univ.).

**B.1.4 Academic Reputation**

Prof. Jacobs is editor of Theoretical Computer Science and was during the reporting period member of the Advisory Committee Computer Science of NWO. He has given many invited talks for professional organisations and the general public. Prof. Jacobs is member of the daily board of Sentinels, a joint national research programme in computer security funded by NWO, STW, and the department of Economic Affairs. He and prof. Verheul also serve on the Programme Committee of Sentinels.

Dr. Poll chairs the steering committee of Formal Methods for Java-like Programs (FTfJP) and has been guest editor for the journal Concurrency and Computation. He was keynote speaker at the Grand Challenge Workshop on Software Verification at ETAPS’2005, has given tutorials at FME, ECOOP, and ETAPS.

Both prof. Jacobs and dr. Poll have been invited to give tutorials the international FOSAD summer school (Foundations of Security Analysis and Design), on electronic voting and Java program security, respectively.

Dr. Hoepman chairs IFIP Working Group 11.2 (Small System Security) and is member of the Permanent Stakeholders Group of the European Network and Information Security Agency (ENISA). He has given a tutorial at the FIDIS/IFIP Internet Security & Privacy Summer School in Brno, Czech Republic.

Prof. van Eekelen chairs the steering committee of Trends in Functional Programming and recently obtained a part-time position as full professor at the Open University. He has been invited to give a tutorial at the international Central European Functional Programming (CEFP) summer school.

Awards for research include the Best Theory Paper Award at the joint ETAPS conferences in 2007, the Best Software Science Paper Award at the 13th International Workshop on Formal Methods for Industrial Critical Systems (FMICS 2008), the Best Student Paper Award at the international symposium on Trends in Functional Programming (TFP 2004) and the Best Paper Award at NLDB 2004.

Important grants awarded during the current reporting period include

- EU project CHARTER in the Artemis programme,
- EU project ROBIN in the Preparatory Action for Security Research (PASR),
- EU project MOBIUS in FP6,
- COST Network ‘Formal Verification of Object-Oriented Software’ funded by ESF (European Science Foundation),
- NWO projects in the NWO Open Competition: AHA (Amortized Heap Space Usage Analysis), NN (Analysis of Anonymity), and Mathematically and computationally relevant dualities (joint project with prof. Gehrke of IMAPP (mathematics))
- STW/Sentinels projects JASON, PINPAS, PEARL,
- European Open Source Service Standard project (EOS3), funded by EU Interregio Programme (Rhein-Waal),
- Ov-Chip 2.0, funded by Stichting NLNet,
• TM4IP, funded by the company Matrixware.

Programme committees of international events that group members have served or are serving on include ESORICS, ESOP, FOSSACS, TPHOL, TERMGRAPH, ICALP, PASTE, CALCO, CARDIS, CMCS, IFL, TFP, SSS, VVSS, FMOODS, VOTE-ID, DISC, and ICDCS.

B.1.5 Internal Evaluation

Internal evaluation takes place through the usual procedures of iCIS: individual annual meeting (jaargesprekken), for PhD students with an additional evaluation after one year, and the principal investigator (PI) system. Currently prof. Jacobs has PI status, and prof. van Eekelen and dr. Poll are aspiring PIs.

B.1.6 External Validation

The Digital Security group has been highly visible outside the scientific community.

A PhD project on e-voting was well underway when the discussion on voting machines erupted in the Netherlands in 2005, and prof. Jacobs was member of the national voting process committee (Adviescommissie inrichting verkiezingsproces) and chairman of the Expert Group Nieuwe Stemtechnologie in het Stemlokaal (New Voting Technology) set up by the Ministry of Internal Affairs.

Our investigation of the technology of the ov-chipkaart, Mifare Classic, gave rise to a big debate about the Dutch RFID card for public transport, the ‘ov-chipkaart’. Members of the group had meetings at cabinet level and have given evidence in parliamentary hearings on several occasions, which even led to a motion of no confidence against the responsible secretary of state. Our research into electronic passports also led to discussions in parliament. The whole ov-chipkaart episode has certainly changed the mindset and attention paid to security in the Netherlands, esp. in government circles, and – in the field of RFID – even worldwide.

On both occasions above the group won the national I/O Media Award, awarded by NWO for the best achievement in bringing ICT research to the attention of the general public: in 2005 for the attention to voting machines, and in 2008 for the work on Mifare Classic and the ov-chipkaart.

Prof. van der Weide was asked to organize an international workshop on Gender Issues in ICT in Makerere University Uganda.

Another way in which we have had an impact outside the scientific community is through contract research, since 2006 under the flag of LaQuSo. We have done research project for many organisations in the private and public sector, for instance a security analysis of smart electricity meters for Nuon, analysis of software for GX and Aia software, and testing the counting software used for the Scottish elections (in a joint project with MBSD). Many projects have been carried out for various branches of the Dutch government: developing vote counting software for Dutch experiments with internet voting; investigating the security of the electronic passport, of the new government access card (Rijkspas), of the RIES internet voting system used for Waterschapsverkiezingen (joint project with TU Eindhoven), of access control to electronic health records (Electronisch Patiendentossier), of road pricing (kilometerheffing), and developing a proof-of-concept implementation of the new electronic driving license.

B.1.7 Researchers and Other Personnel

Group members are given the freedom to make the most of their talents, even if that means breaking the mould of established job descriptions. For example, one of our scientific programmers has started working towards a PhD, another has a part-time teaching appointment, and a bright former Master student (who won the national student of the year award for his Master thesis) has a part-time appointment as researcher.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenured staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full professors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jacobs, Bart</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
</tr>
<tr>
<td>Weide, Theo van der</td>
<td>0.40</td>
<td>0.40</td>
<td>0.30</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>Associate professors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eekeelen, Marko van</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.50</td>
<td>0.60</td>
<td>0.08</td>
</tr>
<tr>
<td>Hoepman, Jaap-Henk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meijer, Hans</td>
<td>0.40</td>
<td>0.40</td>
<td>0.03</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poll, Erik</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.60</td>
</tr>
<tr>
<td>Assistant professors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oostdijk, Martijn</td>
<td>0.13</td>
<td>0.40</td>
<td>0.40</td>
<td>0.13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poll, Erik</td>
<td>0.17</td>
<td>0.40</td>
<td>0.40</td>
<td>0.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rossum, Peter van</td>
<td>0.13</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
</tr>
<tr>
<td>Smetsers, Sjaak</td>
<td>0.40</td>
<td>0.40</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
</tr>
<tr>
<td>Total tenured staff</td>
<td>1.90</td>
<td>2.20</td>
<td>2.13</td>
<td>2.10</td>
<td>2.16</td>
<td>2.50</td>
</tr>
<tr>
<td>Non tenured staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arampatzis, Avgi</td>
<td>0.25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breunesses, Cees-Bart</td>
<td>0.42</td>
<td>0.63</td>
<td>0.10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consoli, Luca</td>
<td>0.18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Galindo Chacon, David</td>
<td>0.11</td>
<td>0.90</td>
<td>0.79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Garcia, Flavio</td>
<td>0.34</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grootjen, Franc</td>
<td>0.37</td>
<td>0.40</td>
<td>0.03</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hoepman, Jaap-Henk</td>
<td>0.32</td>
<td>0.32</td>
<td>0.28</td>
<td>0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Haack, Christian</td>
<td>0.23</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
</tr>
<tr>
<td>Hubbers, Engelbert</td>
<td>0.90</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hughes, Jesse</td>
<td>0.62</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kiniry, Joe</td>
<td>0.90</td>
<td>0.67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kraaij, Wessel</td>
<td>0.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mostowski, Wojciech</td>
<td>0.30</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
</tr>
<tr>
<td>Oostdijk, Martijn</td>
<td>0.90</td>
<td>0.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poll, Erik</td>
<td>0.90</td>
<td>0.47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rossum, Peter van</td>
<td>0.87</td>
<td>0.90</td>
<td>0.63</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schubert, Alekx</td>
<td>0.15</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skharavskla, Olha</td>
<td>0.33</td>
<td>0.80</td>
<td>0.80</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sokolova, Ana</td>
<td>0.11</td>
<td>0.45</td>
<td>0.07</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teepe, Wouter</td>
<td>0.75</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tews, Hendrik</td>
<td>0.82</td>
<td>0.90</td>
<td>0.30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verheul, Eric</td>
<td>0.05</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total non tenured staff</td>
<td>5.16</td>
<td>3.32</td>
<td>3.38</td>
<td>7.13</td>
<td>5.71</td>
<td>4.96</td>
</tr>
<tr>
<td>PhD candidates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Andres, Miguel</td>
<td>0.09</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bosman, Sander</td>
<td>0.77</td>
<td>0.73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breunesses, Cees-Bart</td>
<td>0.90</td>
<td>0.90</td>
<td>0.15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chmielewski, Lukasz</td>
<td>0.15</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
</tr>
<tr>
<td>Garcia, Flavio</td>
<td>0.34</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.56</td>
<td>0.90</td>
</tr>
<tr>
<td>Hasuo, Ichiro</td>
<td>0.64</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.26</td>
<td></td>
</tr>
<tr>
<td>Beunen, Chris</td>
<td>0.17</td>
<td>0.45</td>
<td>0.45</td>
<td>0.45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kesteren, Ron van</td>
<td>0.30</td>
<td>0.37</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Koning Gans, Gerhard de</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lensink, Leonard</td>
<td>0.08</td>
<td>0.54</td>
<td>0.54</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Madsen, Ken</td>
<td>0.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pieters, Wolter</td>
<td>0.30</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.60</td>
<td>0.90</td>
</tr>
<tr>
<td>Tamalet, Alejandro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warnier, Martijn</td>
<td>0.90</td>
<td>0.90</td>
<td>0.08</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verdult, Roel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.21</td>
</tr>
<tr>
<td>Vrieze, Paul de</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total PhD candidates</td>
<td>4.11</td>
<td>5.87</td>
<td>4.97</td>
<td>5.07</td>
<td>6.12</td>
<td>4.42</td>
</tr>
<tr>
<td>Total research staff</td>
<td>11.17</td>
<td>11.39</td>
<td>10.48</td>
<td>14.30</td>
<td>13.99</td>
<td>11.88</td>
</tr>
</tbody>
</table>
All PhD students participate in the research schools IPA and SIKS and attend at least one international summer school. Many also pay longer research visits to other university or research institutes abroad (including SRI and NASA Langley in the US, the University of Cordoba in Argentina, the University of Nottingham in the UK, and NTT Corporation Research Centre in Japan).

We try to let PhD students make the most of their possibly wider talents. For example, the PhD thesis of W. Pieters, a PhD student with a double Master degree in both Philosophy and Computer Science, involved a co-promotor from the department of philosophy, and we currently have a joint PhD student, C. Heunen, with the mathematics department.

We are pleased that several former PhD students have taken up interesting jobs in the security field both in the private sector (Riscure, Brightsight) and in government (Min. of Internal Affairs), which is thanks – at least in part – to our many collaboration outside academia.

Our international network and visibility abroad provides an important means to attract quality PhD students and postdocs from abroad, from as far afield as the USA, Japan, Argentina, Sweden and Poland. Having a good reputation as an exciting research group has been important to attract and keep good personnel.

The university offers training programs for teaching qualification and for management and academic leadership, which many group members have participated in. For a number of group members we have arranged an ad-hoc opportunity for a media training programme. Dr. Poll has benefited from a faculty level programme (‘Versterking Marktwerking’) to employ more experienced researchers from the overhead on external projects.

Prof. Jacobs has had a secondment at the TU Eindhoven for one day a week for the period 2005-2008, and dr. Hoepman also works for TNO ICT. Since January 1 2009, dr. van Eckelen is appointed to the Software Technology Chair at the Open Universiteit Nederland for 0.3 fte. The group currently has two professors by special appointment (bijzonder hoogleraren): prof. Verheul from PriceWaterhouseCoopers and prof. Kraaij from TNO ICT. This contributes to our mission to keep in touch with the broader field of security research, incl. the more practical aspects.

### B.1.8 Resources, Funding and Facilities

#### B.1.8.1 Resources and funding

Table B.1.2 specifies the ratio between direct and indirect funding over the years, showing a gradual shift towards more indirect funding.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Direct Funding</td>
<td>53.1</td>
<td>58.2</td>
<td>47.9</td>
<td>38.5</td>
<td>40.4</td>
<td>45.2</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>36.7</td>
<td>39.6</td>
<td>40.2</td>
<td>43.4</td>
<td>44.5</td>
<td>43.4</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>10.2</td>
<td>2.2</td>
<td>11.9</td>
<td>18.1</td>
<td>15.1</td>
<td>11.4</td>
</tr>
<tr>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

#### B.1.8.2 Facilities

The group has an extensive collection of smartcard- and RFID-related software and hardware, including cards, card readers, emulators and eavesdropping devices for contact and contactless cards, and NFC-capable mobile phones. Some of this equipment has been developed in-house by the Technical Centre of the faculty.

LaQuSo profits have recently been used to invest in the purchase of two Sun X4440 workstations with 128 Gbyte memory each, to be used for model checking.
B.1.9 Overview of the Results

Key publications (with motivations):

   (This is the publication about the reverse engineering of the Mifare Classic chip card, causing such a stir.)

   (Best Theory Paper Award at joint ETAPS conferences.)

   (Good representative of the Java verification work in PVS.)

   (Foundational paper in resource consumption, including soundness and decidability of a size-aware type system, forming a basis for much subsequent work.)

   (Illustration of the theory underlying security/anonymity work.)

---

Table B.1.3: Programme results: outcome numbers (SEP Table 6)

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. book chapters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total academic publications</td>
<td>22</td>
<td>25</td>
<td>37</td>
<td>49</td>
<td>44</td>
<td>43</td>
</tr>
<tr>
<td>2. Monographs</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3. PhD theses</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td>2</td>
<td>13</td>
<td>9</td>
<td>6</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>Total publications</td>
<td>25</td>
<td>40</td>
<td>47</td>
<td>58</td>
<td>63</td>
<td>53</td>
</tr>
</tbody>
</table>

B.1.10 Analysis, Perspectives and Expectations

Strengths

- The group’s research spans a broad range from theoretical to very applied. It combines theory with implementation and analysis and also with social context. This has allowed for both solid scientific results and practical impact, and offers group members (and students working on Master thesis projects) much variety, and much freedom to make the best of their particular interests and talents.
• The group has a high visibility and a real impact outside the scientific community. It has contributed to the awareness that security (with privacy implicit) issues can make or break large ICT-projects, and it contributes to novel solutions. “Computer security at Nijmegen” has a significant brand value outside the university, certainly in the Netherlands.

• The group has attracted a lot of commercial contract research, establishing many links with organisations in the public and private sector.

• In the field of software security the group is involved in many successful international collaborations.

Weaknesses

• A counterpoint to the first strength above is that the broad range of topics is hard to support with the available staff. The group “spreads itself thin”, at times.

• Not all the more practical security work leads to high-quality research or publications.

• In comparison to the strong national position, the group has a relatively low profile in the international academic security community (program committees of conferences and editorial boards of journals).

Opportunities

• Security remains an important and relevant topic for the foreseeable future.

• There are many opportunities for LaQuSo contract research, especially given the group’s reputation.

• There are many opportunities for inter-disciplinary research in the field of security.

• Expertise in the group on the topics of security and of information systems and information retrieval (within IFL) makes for an interesting combination with much potential.

Threats

• The broad range in (practical) research topics in the group brings the risk of fragmentation.

• There is some tension between fundamental and applied research, and striking the right balance requires care. There is the danger in getting carried away in very exciting (but potentially very time-consuming) practical work that is scientifically less interesting. Similarly, extreme media interest as witnessed in the past year can also be a distraction from scientific research.

• Some of the expertise in the group is with non-permanent staff (postdocs and PhD students), and can disappear quickly as people take up jobs elsewhere.

• More generally, a majority of permanent staff do not have an original background in security.

• Due to financial uncertainty in research funding, using the proceeds of contract research to pay for our own personnel (e.g. for contract extensions of temporary staff) is not automatic.

• As the NWO Pioneer grant comes to an end, the flexibility in employing funds that this has offered will end.
Analysis

In the past 6 years, the Digital Security group can claim to have been highly successful in broadening its scope and focus towards computer security: in the field of computer security the group has produced quality research (demonstrated by publications in top security conferences and journals, e.g. ESORICS and Journal of Computer Security) and the group can boast a high visibility and impact, also outside the scientific community. In the analysis of the Mifare Classic chipcard the group has realised a rare combination of strong academic work and mega-impact. The story behind it has led to a proud group portrait in Science (see footnote 2 on page 46), the top scientific journal, in which computer scientists are exceptions, unfortunately.

Contract research has had a healthy interaction with scientific research, e.g. building on and deepening existing scientific expertise or leading to new directions for scientific research explored in new STW projects.

Given that our expertise is actively sought by numerous government bodies tackling issues that involve security and privacy, we can certainly claim that our mission to have an active role outside academia has been successful, and that our strategy for this has worked.

Adjusted goals

For the security research our goal is to have more extensive scientific collaborations with disciplines outside the field of computer science, in particular the collaboration with the law faculties started in the Centre for CyberCrime Studies, CYCRIS, especially in collaboration with the more ‘search-oriented’ members of the DS group.

In the area of software correctness, we aim to continue to work towards making formal specification and verification a reality for real-life programs. In the area of security, the promotion of privacy has gradually become a more important part of our mission, and we see it as our aim to ensure that controversial projects like the ov-chipcard will not set the standard for either security or for privacy.

Adjusted strategy

Given the large reliance of external funding, part of the direction will be steered by funding opportunities, and making the most of NWO and EU sources to fund for more fundamental research and STW and commercial contract research to fund more applied research. Given the group’s Java expertise, Safety Critical Java is a promising application area here. Building on the strong reputation that the group has acquired, we wish to be more pro-active in setting the research agenda for security, certainly on a national level. We will continue to strive to have smaller, more focused projects as a way of tying different strands of research together, and reducing the risk of fragmentation.

The group will appoint a new assistant professor in the course of 2009. This person has a strong security background in RFID, smartcard hardware security, and applied cryptography. This will further consolidate the group’s expertise in one of its core research topics, and more generally improve the security expertise among the permanent staff.

The recent foundation of the ‘Information Foraging Lab’ is a step to combine research efforts in the area of information services, information retrieval security-oriented data mining and communication.

To promote privacy research, we will investigate privacy-friendly alternatives and ‘identity-poor’ solutions and develop prototypes of such systems.

Provable security as an interesting topic at the crossroads of cryptography and computer science (program semantics, theorem proving) where the group has a lot of relevant expertise, namely in formal methods, security protocols, and applied crypto.
Tackling the weaknesses

- As to the breadth of the group, we want to further consolidate the group’s research in computer security, and continue to strive for an interesting and exciting mix between fundamental and applied research. The appointment of a new assistant professor, already mentioned above, will also contribute to this.

- In line with this approach we wish to be more selective in the application-oriented security work, and strive for a stronger focus and link with scientific results.

- To improve our visibility in the international academic security community, we plan to host security workshops and conference. Concrete plans involve WITSP 2010 and ICTIR 2011. Also, we aim to develop some international collaborations in EU projects in the area of security, like we already have many in the area of software correctness.

Summary

The Digital Security group has grown in the reporting period from start-up phase to maturity. It has extended its original expertise in (Java) program specification and verification to broader security issues. In doing so it has had both scientific and societal impact.
B.1.11.  PUBLICATIONS

2003

Academic publications

Refereed journal publications


Articles in refereed proceedings


Monographs


Professional publications


2004

Academic publications

Refereed journal publications


Articles in refereed proceedings


Monographs

PhD theses


Professional publications


Academic publications

Refereed journal publications


Articles in refereed proceedings


B.1.11. PUBLICATIONS


CHAPTER B.1. DIGITAL SECURITY


Monographs


Professional publications


2006

Academic publications

Referred journal publications


**Articles in refereed proceedings**


B.1.11. PUBLICATIONS


PhD theses


Professional publications


CHAPTER B.1. DIGITAL SECURITY


2007

Academic publications

Refereed journal publications


Articles in refereed proceedings


B.1.11. PUBLICATIONS


B.1.11. PUBLICATIONS

Book chapters


Monographs


Professional publications


CHAPTER B.1. DIGITAL SECURITY


2008

Academic publications

Refereed journal publications


**Articles in refereed proceedings**


B.1.11. PUBLICATIONS  


Book chapters


Monographs


PhD theses


CHAPTER B.1. DIGITAL SECURITY

Professional publications


Other publications referenced in the text


Chapter B.2

Intelligent Systems

Title of the Research Programme: Intelligent Systems (IS)

Research Area and Mission: Our main challenge is to make computer systems more ‘intelligent’. We do this by both pursuing the connectionist and the symbolic approach. The connectionist approach follows the statistical view on knowledge; our specific expertise lies in Bayesian methods and machine learning with main applications in bioinformatics and neuroscience. The symbolic approach follows the (formal) logical view on knowledge; our specific expertise lies in type theory and proof assistants with applications in software verification and formalization of mathematics. A central notion from logic towards intelligence is ‘reflection’: the view on a system (including ourselves) from higher levels. This has applications in proof technology and in psychiatry.

Keywords: type theory, lambda calculus, term rewriting, reflection, proof assistants, formalizing mathematics, machine learning, bioinformatics


Starting Date of the Programme: 2008

Affiliations outside iCIS: IS participates in the Dutch graduate schools IPA (Institute for Programming research and Algorithmics) and SIKS (Information and Knowledge Systems)

B.2.1 Leadership

The research is organized in PI-groups around the three Principal Investigators: prof. H. Barendregt, prof. H. Geuvers, and prof. T. Heskes. While they operate autonomously in their selection of research topics, they also seek cooperation between the PI groups. Between the groups of Barendregt and Barendregt/Geuvers, there is—historically—a strong cooperation, although not on the topic of Brain research. Between the groups of Barendregt and Heskes, there is an initial cooperation on brain research and between the groups of Heskes and Geuvers/Barendregt, there are opportunities for the application of methods from machine learning for search techniques in proof assistants. In particular Geuvers has recently appointed a post-doc with expertise in applying machine learning techniques in the proof assistant Mizar.

The Intelligent Systems section has monthly staff meetings, where all current issues of the section and the institute are discussed. Each PhD student and post-doc meets with his/her supervisor at least once a week to discuss research progress. The Proof Assistants group has a regular seminar and a regular research lunch to discuss ongoing and future research. The Mindfulness research group has a biweekly meeting with all PhD and Master students and there are biweekly meetings of the PhD students with their direct supervisors. There is a monthly meeting with all researchers involved and the three directors Barendregt, Gielen and Speckens. The Machine Learning group has weekly meetings to discuss ongoing and future research.
B.2.2 Strategy and Context

History and Context

The section Intelligent Systems was formed in January 2008 and consists of three subgroups: the Proof Assistants group (headed by prof. H. Barendregt and prof. H. Geuvers) coming from the former Foundations department, the Mind-Brain-Mindfulness group (headed by prof. H. Barendregt) coming from the former Foundations department and the Machine Learning group (headed by prof. T. Heskes).

The Foundations department has existed from the start of the evaluation period, until January 2008, when it was absorbed into the section IS. The Foundations department was headed by prof. Barendregt. In August 2006, prof. Geuvers was appointed as a professor and joint research leader of the Foundations department. This has been formalized in the summer of 2007, when he was appointed as a Principal Investigator. Most researchers from the Machine Learning group were part of the IRIS department before 2008. Machine learning research was one of the research lines within IRIS, but did not have an official status.

The research on Mind-Brain-Mindfulness is not really part of computer science, although there are connections with it. Specifically, with the research in brain computing in the Machine Learning group and the research on logical reflection in the Proof Assistants group. The Mind-Brain-Mindfulness group has emerged from a personal research interest of Barendregt. It has been funded by the Spinoza award and from other external projects. As this research forms part of the Intelligent Systems section, we report it here, even though topic-wise it might fit better within biology or neurophysiology. It is expected that this Mind-Brain-Mindfulness research line will not be continued within iCIS after the retirement of Barendregt.

Strategy

In the section IS both intelligence of computer systems and of humans is being studied, with the aim to enhance performance by understanding both types of intelligence and to create fruitful interactions between the two. The research themes of the three subgroups cover different aspects of Intelligent Systems research.

Specifically, in the Proof Assistants group mathematical and symbolic reasoning constraints are precisely formalized and techniques are developed to support the user. The problems involved are often undecidable or algorithmically infeasible, so that these systems are often interactive. This means that humans provide the intuition for the abstractions (definitions of concepts) and reasoning (proofs), whereas the computer verifies whether the concepts are well-defined and the proofs logically sound.

In the Mind-Brain-Mindfulness group one is focussed on regulation of emotions (i.e. internal states) and modification of behavior, something that is difficult for humans, but easy for rule-based machine systems. For systems obtained by machine learning this modification is obtained by a training period of feedback. Mindfulness is a meta-cognitive state of mind (‘Reflection’), enabling the human to modify motives and thereby behavior.

Finally, in the Machine Learning group higher-level objectives are formulated and algorithms are derived to meet those objectives. Many of the problems that one encounters are intractable: exact solutions are infeasible and therefore focus is on efficient approximations. The methods that are developed are applied to solve problems in (cognitive) neuroscience and bioinformatics.

Since each subgroup has enough people to generate sufficient critical mass, it conducted its own research line independently of the other subgroups. At a high (section) level the strategy of the IS section is to continue these independent research lines in order to maintain the broad scope of the section’s research. Furthermore, we plan to stimulate occasional interactions between the groups by exploiting each other’s expertise.

At a low (group) level, the strategy followed by each of the three groups is based on interdisciplinary collaboration, in order to perform and integrate high quality fundamental research and real-life practical applications. Indeed, the research performed in all three groups is highly
interdisciplinary and very broad in scope. The methods derive from computer science, mathematics, and physics and are often inspired by cognitive science. The work involves applications in many different fields, most notably (bio)medicine (decision support systems, medical data analysis), mathematics (proof checking, repositories of formal mathematics) and computer science itself (verification of software), and also psychiatry (mindfulness training). There are close collaborations with, among others, the Donders Research Institute for Brain, Cognition and Behavior, IWWR Research Institute (Microbiology) and IMAPP Research Institute (Mathematics), Psychiatry and Social Psychology (see Figure B.2.1).

In the following three subsections the mission and strategy, topics, methods and applications of the three groups are explained in more detail.

**B.2.2.1 Proof Assistants Group**

**Mission and Strategy**

The research line of this group aims at advancing the use of Proof Assistants, both in computer science – as tools for specifying, modelling and verifying software and systems – and mathematics – as tools for developing and verifying proofs. To this end we do research into the following three topics.

- **Foundational topics**: Type Theory, Lambda Calculus, Term Rewriting and Exact Real Number Computation.
- **Engineering**: Proof Assistants and Interfaces.
- **Applications**: Modelling and Verification, and Formalization of Mathematics.

Our foundational research also serves as topics of theoretical interest on their own. The research group aims at being the national centre and internationally leading group for these topics. The part-time appointment of prof. J.W. Klop, prof. H. Zantema (starting in 2007) and prof. J. Rutten (starting in 2009) should be seen in the light of those ambitions.

Some concrete research topics that form a bridge between foundations and applications are exact real arithmetic, constructive mathematics and dependent typed programming. To advance the use of proof assistants, we furthermore perform formalization case studies and research into their proof style, input language and interfaces and into the integration of proof assistants.
Proof assistants serve as tools for the correctness of software and as tools for formalizing mathematics. For presentation clarity, we distinguish these two application areas, though they have a strong mutual influence on each other: one needs to formalize (basic) mathematics to be able to specify, state and prove properties of programs; in the other direction, (verified) programs are used as executable functions in formalized mathematics and for decision procedures to speed up proofs. There is also a direct influence of the foundational research on the application areas. The other way around, the application areas also pose engineering question regarding proof assistants and interfaces and also questions that can be cast on the foundational level or that require a revision of the theory.

In Computer Science we observe a strong increase of tool support for the specification and verification of systems and software. This is a consequence of the success of formal methods in formalizing (specific aspects of) computer systems and being able to implement tools that make these formal methods “work”. Proof Assistants are the most generic among the tools that provide computer support to model systems and verify their properties. This makes them suitable for many verification tasks, but, as they are not domain-specific, one may lose some efficiency. A big advantage is that, when doing verification using a Proof Assistant, one is actually exhibiting a proof, that has a very precise meaning (in the underlying logic of the Proof Assistant). A Proof Assistant that satisfies the “de Bruijn criterion” even creates “proof-objects” that can be checked independently (of the proof assistant they were created with). This leads to a very high level of confidence in the correctness of the verified result. In mathematics, the use of Proof Assistants is advancing only slowly: proving is seen as the specific domain of the human, and a proof that can not be human-understood (but only machine checked) is often not accepted as a proof by mathematicians. However, in some cases, like the proof of the Kepler conjecture or the 4-Colour Theorem, computer support seems to be indispensable. It is expected that in the future, mathematical proofs that are checked by a Proof Assistant will play a more and more important role in mathematics as well.

Foundational topics: Type Theory, Lambda Calculus, Term Rewriting and Exact Real Number Computation

Type Theory, Lambda Calculus and Term Rewriting are fundamental concepts behind computing and reasoning. We study them for their own right and for their applicability in proof assistants, formalizing mathematics and correctness of software. Exact Real Number Computation studies and develops methods for computing with (potentially) infinite precision real numbers.

The logic of exact arithmetic is constructive. For this and more technical reasons (refined expressivity, the availability of a realizability interpretation and the possibility of program extraction from proofs) we have an interest in using constructive methods. This can be seen as a continuation of Bishop’s [I243] visionary program to use constructive mathematics as a programming language for numerical analysis. As part of his Veni research project, Spitters has continued this program [I42, I62, I147, I61, I174, I73, I48, I43], studying and reproving various classical results from analysis and casting them in a computational form. Spitters also co-supervised the Ph.D. student O’Connor who has provided the first efficient verified implementation of exact real arithmetic (see under Correctness of Software). Surprisingly, these techniques and results were also crucial in applications in quantum theory [I224, I188], which forms a very interesting link with the mathematics department in the IMAPP institute of the Radboud University Nijmegen. Spitters, now working at Eindhoven is still a guest in the group for 2 days per week and we will continue this line of research.

In the reporting period, we have performed various theoretical studies into lambda calculus and term rewriting [I63, I168, I139, I57, I172, I141]. In term rewriting, a lot of attention has focused on criteria for normalization [I91, I110, I149, I226, I165, I142, I192, I193] and furthermore on the new emerging fields of infinitary terms [I140] and infinitary reduction [I58, I199]. The study of infinitary terms and infinitary rewriting is one of the focal points for the future; it is closely related to the study of co-inductive types and co-induction principles, which we have also carried out in the context of exact real arithmetic.
B.2.2. STRATEGY AND POLICY

Exact real arithmetic works with infinitary precision real numbers, to overcome the inherent unreliability problem with floating point arithmetic. (Our publication [I112] gives an overview of the field.) The aim is to write algorithms that compute with arbitrary close approximations of real numbers: given an input and a required output precision \( \varepsilon \), the algorithm asks for a precise enough approximation of the input (to be able to compute output with precision \( \varepsilon \)) and then computes the approximation of the output. So such an algorithm consists of two components: one that computes output approximations from input approximations and one that computes an input precision from the required output precision. In this setting, a real number is a potentially infinite piece of data, as it can produce arbitrarily precise approximations of its value. In the reporting period, we have performed theoretical research into exact real arithmetic, developing the proper co-recursion principles for defining these algorithms and the proper co-induction principles for reasoning over them [I72, I93, I34, I59, I170, I143, I115, I114]. Furthermore, we have formalized these algorithms in the proof assistant Coq. That is: we have defined them as executable programs and proven (correctness) properties about them. See the subsection Correctness of Software.

In Type Theory, we have studied various topics, ranging from purely theoretical to proof assistant inspired. Our experience with proof assistants has led us to study logics and type theories with “open proofs and open terms” [I218, I24]: in an interactive proof session, one basically deals with “proofs with holes” and refines these with the end goal of obtaining a closed finished proof. We have studied this on the level of the type theory, to provide a better understanding of this on the implementation level. Our combined knowledge of proof assistants and type theory has led to a study of the type theory of the Mizar proof assistant [I148]. Similarly inspired by questions from proof assistants and program correctness questions were our theoretical studies into co-inductive type theory, partly in cooperation with researchers from Estonia [I69]. A topic of purely theoretical interest has been the study of graph deduction [I111, I155, I79, I185] that has emerged from the study of various proof formats, like Fitch style [I21] and Gentzen style natural deduction. This has interesting connections with proof display in the "ProofWeb" user interface, see the subsection Engineering: Proof Assistants and Interfaces.

Finally, we have performed foundational studies in proof assistants and type theory [I76, I22] and in process theory [I85, I86]. A new seminal book on type theory by Barendregt, Dekkers et al. [I242], has been finished and has been accepted for publication by Cambridge University Press. We have organized a one day symposium “Reflections on Type Theory, Lambda Calculus, and the Mind”, to bring together researchers from these fields and to celebrate Henk Barendregt’s 60th birthday (on 17 December 2007). The proceedings of this symposium have appeared as [I151].

Engineering: Proof Assistants and Interfaces

Proof assistants can be seen as a first step towards a system for Computer Mathematics: a computer tool where one can combine the mathematical activities of defining, computing and proving in a reliable way. We have discussed and promoted this vision in various publications [I38, I121, I176]. There are various obstacles to the successful deployment of proof assistants. First, there is a great need for a well-documented coherent repository of formalized mathematics, constituting a real “library of formalized mathematics”. Also there is a great need for enhancing the proving process and the possibilities for cooperative work. We have been working on these topics in various ways, but these remain the main research themes for the near future. We have developed a “declarative” proof mode for Coq [I182], where the proofs are in a more standard mathematical style. (This is now part of the Coq system.) We have developed the notion of “Formal Proof Sketch” [I28], as a way of transforming an informal proof (on paper) to a formalized proof (in a proof assistant). This notion has become influential in the field. Other work on bridging the gap between the informal and formal proof language is [I1, I233]. We have also experimented – in an implementation combining the proof assistant Coq with the text editor TeXmacs – with a document centric approach to proving, where the writing of a mathematical document is integrated with a formalization [I80].

Towards cooperative formalization, we have developed a web-based prover interface called “ProofWeb” for various proof assistants (see http://proofweb.cs.ru.nl/) [I113]. This opens up the possibility for researchers to work jointly on a formalization (which resides on the server)
through a standard web interface. The system now supports various proof assistants and the future goal is to extend this to a “MathWiki” system for formalized mathematics [I131], supporting both the joint cooperative formalization work and the creation of high level informative pages about mathematical notions. In cooperation with representatives the main European proof assistants and experts in semantic web technology for mathematics, we have coordinated a proposal for a European IST-FET project to develop a MathWiki system. This proposal was well-received, but failed to get funded. A smaller project to develop such a MathWiki system will start in 2009, supported by the Dutch science foundation NWO (one post-doc and one junior researcher).

The “ProofWeb” system has originally been developed as part of the project (joint with the Free University of Amsterdam, supported by the Dutch Surf foundation) “Web Deduction”, creating a web-based system for teaching logic using a proof assistant [I138, I223]. This system has been successfully used in various courses and has thus proved very useful, as an educational tool for logic, but also as a user-friendly interface for teaching the proof assistant Coq. Towards education, we have also experimented with the extraction of course notes from a formalization, in the EU funded IST project MOWGLI (Mathematics On the Web, Get it by Logic and Interfaces, http://mowgli.cs.unibo.it/). The idea is to combine an existing set of web-based course notes (Algebra interactive!, an interactive course on algebra developed at the Technical University Eindhoven http://www.win.tue.nl/ida/) with formalized proofs, by rendering proof-objects of Coq as natural language proofs inside the document [I78]. This method turned out to be quite heavy and involved, with little gain in terms of a nice proof presentation, also because at the time, web tools weren’t that well-developed yet. However, the MOWGLI project has given us quite a lot of experience and insight in using web technology and it has also enabled us to further develop our repository of formalized mathematics in Coq (see under Formalizing Mathematics).

To expose our work on proof assistants and to further spur and encourage cooperation, we have (co-)organized several meetings, like the “Dutch Proof Tools Day” in 2004, the “Types for Mathematics / Libraries of Formal Mathematics” international workshop in 2004, the “Curry-Howard Implementation Techniques/ Connecting Humans and Type-checkers” (ChitChat) international workshop in 2006, all in Nijmegen and the “Proof Assistants and Types in Education” international workshop in 2007 in Paris (as part of RDP 2007, the Federated Conference on Rewriting, Deduction, and Programming). Another successful way of improving the cohesion and the interaction in the proof assistant community has been the LNCS volume “The seventeen provers of the world” [I100], consisting of formalizations of the same theorem in 17 different provers, collected and edited by Wiedijk from our group.

Applications

Modelling and Verification In computer science, we aim at applications of proof assistants for the specification, modelling and verification of software and systems. In general, for verification tasks, one tries to develop computer (tool) support that automates the verification as much as possible, but that’s not always possible and that’s where interactive proof assistants come in. A particularly interesting case is where the system involves continuous behavior or where the programs deal with real number computations. The problems encountered here are (almost) always undecidable, the state spaces uncountable and moreover, the usual algorithms (that work with floating point real numbers) have correctness problems because of making too coarse approximations. As the software (for example a program that acts as a controller in a continuous environment) is often safety critical, this is the ideal place for proof assistants, that allow to both model precisely the continuous environment and to write and verify the control programs. We see this as a crucial application area for proof assistants in computer science in the coming period.

We see exact real arithmetic as an important framework for modelling systems with continuous behavior and developing certified control algorithms for them. We have produced a certified library for exact real arithmetic in the proof assistant Coq [I25, I116]. On top of this, we have developed a tactic that can prove the inequality of two real number expressions automatically, by an iterated approximation of the value of the expressions, using the algorithms for the functions used in the expressions [I195]. This certified library can also be used as a “certified calculator”,
which provides as many digits of a real number as desired in a completely certified way [I225]
(see also http://proofweb.cs.ru.nl/calc.html). Another important use of this work is in the
certified numeric approximation of solutions for differential equations. We have organized in 2005
a very successful workshop “Constructive analysis, types and exact real numbers”, with refereed
proceedings [I153], and as part of that the “Many Digits Competition” to compare computer
packages for exact real arithmetic. The exact real arithmetic in Coq is part of C-CoRN [I18],
our Constructive Coq Repository of formalized mathematics. See also below under Formalising
Mathematics.

In applying our certified exact real number library to system verification, we are developing a
Coq tool set for the verification of hybrid systems [I194]. This work has lead to a first prototype
at the end of 2008, which we expect to work out into a complete tool in 2009. Hybrid systems
combine discrete (control) features with continuous behavior, which is often given via (the solution
of) a differential equation. Our verification of Hybrid systems avoids the use of floating point
arithmetic, as it uses the exact real arithmetic that we have formalized in Coq. Thus we can
provide completely certified safety proofs of Hybrid systems. This is a concrete research goal for
the coming years.

A different approach to the correctness of software is provided by programming in dependent
type theory, where the expressivity of the type system is used to provide a refined specification
of the program; then a term of this type is a correct program “by construction”. Together with
researchers from Gothenburg, we have developed various techniques for doing this, now known as
the “Bove-Capretta” method [I125, I180], which we have applied inside the Coq system, but the
method has also found its way to other platforms. Since the summer of 2007, J. McKinna, one of
the developers of the dependently typed programming language Epigram has joined our research
group, giving the research on programming in dependently typed languages a new impetus.

We have performed various case studies in system verification using proof assistants: [I128,
I210, I3].

Formalizing Mathematics Towards concrete formalization studies, apart from the already
mentioned developments on exact real arithmetic, we have further developed C-CoRN [I18, I33],
our Constructive Coq Repository at Nijmegen (http://c-corn.cs.ru.nl/), containing an alge-
bric hierarchy of structures up to the reals and the complex numbers and all kinds of basic results
in constructive analysis. Many functions over the reals and the complex numbers are also defined as
executable functions, using exact real arithmetic. This repository has been used e.g. by Zumkeller
in his formalization work in the Flyspeck project http://code.google.com/p/flyspeck/.

Our choice of formalizing constructive proofs has proven very useful in the application to exact
real arithmetic. We don’t have a philosophical bias towards constructivity, but it gives more
refined results (that are true classically as well) and provides decision procedures and computable
functions. As part of his Veni research project, B. Spitters has studied and reproved various
classical results from analysis and cast them in a computational form. This has again contributed
to the work on exact real arithmetic. Concrete formalizations as a result of this are the ones on
compact sets [I196] and transcendental numbers [I195].

We have also worked in the field of computer mathematics, where we have integrated HOL light
with computer algebra features, developing a certified computer algebra on top of a proof assistant
[I37, I191]. Other formalization case studies involve the formalization of higher order abstract
syntax (languages with binding) [I127], Craig’s interpolation theorem [I181], Arrows theorem [I240]
and Conway’s “surreal numbers” [I92]. Finally, a really major formalization has been the proof of
Gödel’s incompleteness theorem in Coq [I60].

B.2.2.2 Mind-Brain-Mindfulness Group

Mission and Strategy

Like all living beings humans are being conditioned. We follow objects of our desires and avoid
objects of repulsion. Usually forms of conditioning give survival advantage, but the simple example
of insects flying into a lamp shows that this is not always the case. An important realization is that mind-states (e.g., emotions) have an overwhelming effect on our behavior. The Mind-Brain-Mindfulness studies the possibilities for humans to recondition themselves. Not by a ‘newyear’s resolution’, but by systematic training. Assuming that human intelligence is Turing complete (Church-Turing thesis upside down!) it follows that it should be able to reflect upon itself and this makes it plausible that humans can decondition themselves from preprogrammed instincts. Mindfulness, which is nothing but meta-awareness, is an endeavor par excellence that enables one to do this.

Insight or mindfulness meditation is a 2500 year old technique to train the mind in concentration and attention. Philosophers like Husserl have reinvented mindfulness (‘epoche’, ‘einklamern’). It is a mental reflection mechanism, related to Gödel-numbering (in mathematical logic) or quoting (in computer languages like LISP). The last 30 years it has been applied to the intervention for mood disturbances like depression and anxieties on the one hand and physical ailments (psoriasis) on the other.

Concentration and attention are studied behaviorally and neurophysiologically in patients suffering from forced rumination (patients with periods of depression) and in healthy subjects (meditators). This will be done before and after mindfulness trainings by the Dept of Psychiatry and mindfulness meditation retreats by insight teachers, among whom Barendregt.

Aims

Mindfulness meditation has been invented as a medicine against existential fears (for dying or more generally for not being in control over a for us important situation). This does not cure these existential problems, they are being domesticated. This means that one changes the attitude towards them. Similarly depressed patients learns to accept the fact to be sometimes in a negative mood. This acceptance is an important step towards letting it occur less often. The theory (behind mindfulness meditation and therapy) is that usually existential situations are hidden by feelings, thoughts and actions. This is the so-called cover-up model in which mindfulness plays a purifying role.

It has been made plausible that mindfulness is a quite powerful tool, yet its functioning is poorly understood. The aims of the Mind-Brain-Mindfulness group are more ambitious. In order to describe these, some psychological background is necessary.

Humans have a feeling of ‘self’ or ‘agency’ that does exist as a process, but not as a stable ‘thing’. From the point of view of cognitive neuropsychology and even of computer science process theory this is quite understandable. If an unprepared person experiences loss of agency for the first time the result is often an existential fear, i.e., a fear not related to the input of seeing, hearing, etcetera, but related to the operating system of our mind. This existential fear is more common than usually acknowledged. Nevertheless, most people are able to create a feeling of agency, making it possible for them to live their life. The existential fear is caused by perceiving that this feeling of agency is a construction, even if it is a useful construction. Advanced meditators have experienced this lack of agency and have learned not to panic, but be in perfect balance with it. This may be compared to astronauts that do not need a pill against travel illness when they are weightless (which feels like falling down under acceleration).

The research questions of the Mind-Brain-Mindfulness group are as follows.
1. How does the feeling of agency come about?
2. How does it get lost?
3. How does mindfulness work to domesticate the existential fear?

On each of these questions we have working hypotheses that are based on personal experience and that are consistent with that of others [97, 65, 178]

H1. The feeling of agency is supported by a general suppression mechanism, meditated by the cerebrospinal fluid (CSF) [68, 67, 40, 41, 171, 101].

H2. Loss of agency is caused by dissociations and these by neural desynchronizations [preliminary result: [44]].
H3. Domesticating fear consists of creating new neural paths, meditated by mindfulness, that bypass the limbic system.

Methods

As to H1, there was encouraging experimental study of Calle concerning opioid containing cells neighbouring the ventricles. This motivated Veening and Barendregt to start a literature review on the role of the CSF and certain neuropeptides.

As to H2, the EEG of advanced meditators will be taken during a test that has been reported to indicate dissociation. The group Machine Learning will examine the collected data.

As to H3, the following operationalization of the mind-state mindfulness is proposed. According to the meditation tradition mindfulness co-occurs with increased attention, memory, flexibility and equanimity. These four mental concommitants have been studied well in experimental psychology. If these factors correlate they are proposed as the operationalization of mindfulness. The question whether mindfulness can be trained is being addressed by longitudinal studies before and after intensive retreats of insight meditation.

In the meditation tradition the falsifiable claim is made that mindfulness co-occurs with increased attention, memory, flexibility and equanimity. These psychological factors have validated tests. The investigation will be made whether the intensity of these four measurable factors correlate, so that they can be taken as an operationalization for mindfulness. The question whether mindfulness can be trained can be addressed by longitudinal studies of subjects before and after an intensive insight meditation retreat.

Application

In collaboration with the Department of Psychiatry the success of preventing relapse to depression is studied among participants of mindfulness trainings. Previous research showed that after three episodes of depression there is 90% chance to relapse; after the mindfulness training this drops to 45%. For those patients that still relapse, the developed mindfulness indicator will be tested as a predictor. This may lead to applications in the direction of increasing the patient population that will not relapse.

B.2.2.3 Machine Learning Group

Mission and strategy

The high-level ambition of the Machine Learning (ML) group is to work towards “bounded rational” machine learning: machine learning methods that properly take into account all information available (both data and prior knowledge) and then provide an optimal answer, given finite resources and computation time. The ML group aims to show that such algorithms (indeed) improve the state-of-the-art, both in theory and in practice. By applying machine learning methods to problems in other scientific domains, the ML group wishes to contribute to the progress in other scientific disciplines.

We continue to follow two approaches: top-down, through a Bayesian approach, and bottom-up, by designing clever heuristics. The Bayesian approach has—in theory—many desirable properties, such as consistency, coherence, and optimality, but in practice leads to computationally intractable problems. More heuristic approaches are designed to be tractable in the first place, but are more difficult to interpret in terms of objective measures of optimality. Having expertise on both sides, we strive to combine the best of both worlds: better heuristics to approximate the Bayesian computations and better understanding to add to the success of the bottom-up approaches.

We hook up with scientists from other disciplines to work together on the analysis of their data to extract new scientific knowledge. This does not only provide a test-bed for existing machine learning methods, but also provides inspiration for new ones. We made a deliberate choice to focus more and more on applications in (cognitive) neuroscience and genomics: two disciplines that are
strongly represented at the Radboud University and where we can really make a contribution to science and society.

Methods

An important research focus of the machine learning group is on Bayesian approximate methods.

Using Bayes’ rule, one can manipulate degrees of belief in different models in the light of new data in a consistent and coherent manner. In real world problem domains, applying Bayes’ rule exactly is usually impractical because it involves summing or integrating over too large a space of models. These computationally intractable sums or integrals can be avoided by using approximate Bayesian methods. The Machine Learning group plays a leading role in the development and understanding of new techniques for such approximate inference. This is, among others, evidenced by invitations to write chapters in handbooks [I32, I241] as well as to write a comment on a highly influential paper in the Journal of the Royal Statistical Society as a representative from the machine learning community [I231].

More specifically, we have been working on message passing algorithms such as loopy belief propagation and extensions thereof. The standard message passing algorithms often yield amazingly accurate results, but are not guaranteed to converge. Of the variants that do guarantee convergence, the algorithm we invented came out as the clear winner in an independent test [I221] and has been patented [I219]. Another drawback of loopy belief propagation is that it does not apply to probabilistic graphical models that contain both discrete and continuous variables, such as switching linear dynamical systems. We studied and further developed message passing algorithms for such cases and compared it with alternative (sampling) approaches [I109, I45, I50, I51, I77, I124, I184, I64, I96] (see also the PhD thesis of O. Zoeter [I222], realized under the guidance of T. Heskes). We will continue along these lines, specifically aiming for methods that are robust and give guaranteed performance.

Another research focus of the machine learning group orthogonal to Bayesian approximate inference concerns the development of efficient and effective (non-parametric) methods for data analysis. We adopt a bottom-up approach involving new knowledge representation frameworks for discovery interesting properties of the data. For example, we developed effective heuristic methods based on a new graph-based representation of a training set for improving accuracy and storage performance of the one nearest neighbor rule [I169, I235]. Recently, we introduced an elegant method based on discrete graph differential geometry for detecting and removing critical instances and outliers from a training set [I236]. We plan to adopt this approach in the development of non-parametric methods for transferring knowledge among tasks (multi-task learning).

Our research on machine learning methods is more theoretical than applied: it involves the design of knowledge representation frameworks, of evaluation and optimization criteria, convergence proofs, stability analysis, and so on. However, we care to show that our algorithms are useful in practice by applying them to a range of relevant real-world domains, by means of the following interdisciplinary projects conducted in close collaboration with domain experts.

Applications in Brain Research and Cognition

Brain-computer interfacing (BCI) allows people to communicate their intent to the outside world without having to rely on any aspect of conventional motor function. It can be used to create a new communication channel for the severely handicapped, or to augment existing means of control for healthy individuals. Most BCI systems are based on measuring electroencephalographic (EEG) activity from the scalp. With signal processing techniques, this activity is then on-line and continually analyzed to infer the user’s intention. From a machine learning perspective, a BCI system corresponds to an extremely challenging on-line classification problem: a time-series of typically very high-dimensional signals has to be continuously classified into several categories.

In collaboration with dr. Jensen’s group from the Donders Centre for Cognitive Neuroimaging, we successfully built and tested a BCI system based on magnetoencephalographic (MEG) activity [I187, I87, I134]. Where this system, as most other BCI systems, make use of a motor-imagery
B.2.2. STRATEGY AND POLICY

paradigm (changes in EEG/MEG activity can be measured not only when you actually perform movements, but also when you imagine making movements), we recently started studying another paradigm, based on covert attention (attentional focus at a particular location gives a localized response in visual cortex) [I239].

No matter which paradigm one uses, EEG and MEG signals contain many features and clever techniques are needed to find the relevant features and reduce the risk of overfitting. We proposed and studied the use of so-called L1/Lp regularization to learn which features are most relevant for BCI. An article from our group on this topic recently appeared in the leading journal on (techniques for) cognitive neuroimaging [I238].

Dr. Sarbo’s line of research on knowledge representation concerns the development of a cognitively based, semiotical model of information processing [I75, I94, I145]. This model has interesting applications in language parsing [I95], meaningful summarization [I146, I144, I197, I27] and ontology design [I26], as also demonstrated in the PhD thesis of J. Farkas [I209], defended in 2008. Indeed, in natural language processing, the model enables a linearly complex algorithm for parsing, and in meaningful text summarization (which is immensely complex) it provides the definition of a systematic approach. Furthermore, this model may also explain how the brain actually processes information. Neuroimaging experiments are being planned to validate predictions of the model, which would bring this line of research closer to the other interests of the Machine Learning group. Another area of overlap which is currently explored is the formation of semantic maps using machine learning techniques. His research on a generalization of informative processes provides a possible framework for model based feature selection.

In many cases, a decision maker is uncertain about the user’s preferences, but still wishes to recommend (or take) decisions on the user’s behalf. Furthermore, by asking additional questions, the decision maker wants to gain further knowledge about these preferences. This problem appears in many different settings and is often referred to as (adaptive) preference elicitation.

Preference elicitation is an interesting test-bed for machine learning research, because, different from “standard” classification and regression problems, it has many interesting characteristics that makes it a lot more challenging: like BCI, it is an on-line problem, with a human in the loop; the problem is not just to learn the correct model from passively generated data, but also to actively generate the most relevant data; there are often many users involved which gives us the possibility to transfer knowledge from one learner to another. A Bayesian approach, in particular Bayesian experimental design in combination with Bayesian hierarchical modelling, seems ideal to handle such problems.

In collaboration with the hearing aid company GN ReSound, the TU Eindhoven (Signal Processing Group) and the AMC Amsterdam (Audiology department), we develop preference elicitation algorithms for the personalization of hearings aids [I179, I179, I124, I54]. Using listening tests of the type “which of the two audio samples sounds best?” we elicit responses from the user and adapt our probabilistic models using (an appropriate approximation of) Bayes’ rule. Bayesian experimental design is implemented to select the next listening experiment. Within the hearing aid domain, most of the algorithms have now been build and the challenge will be to actually get them to work in practice in the next few years. In future work, we aim to address preference elicitation in the context of negotiations, which will raise further challenges: for instance, taking into account non-stationarity, inconsistencies, and different objectives for different parties involved.

Applications in Bioinformatics

The large scale production of biological data makes computational data analysis a required tool in the knowledge discovery process, boosting the collaboration among researchers from different disciplines, such as computer science and biology. Biological data are typically multidimensional and contain noise as well as technical and biological variability. Furthermore the underlying biological mechanisms to be analyzed are in general unknown and have a complex nature. Therefore models must be learned from the data. This makes bioinformatics an interesting and challenging application area for machine learning.

In collaboration with prof. Huynen from the Nijmegen Center for Molecular Life Sciences
(NCMLS), we are working on the design of novel graph-based machine learning methods for the comparative analysis of protein-protein interaction networks. Such interaction networks are naturally represented by means of (weighted) graphs. We combined biological knowledge and graph-based optimization techniques for discovering interesting knowledge from such networks, such as protein complexes conserved across species [I189, I190].

In collaboration with prof. Jetten from the Institute for Water and Wetland Research (the research institute on biology at our Science faculty), we are working on the development and application of novel machine learning methods for metagenomics. The rapidly emerging field of metagenomics seeks to examine the genomic content of communities of organisms to understand their roles and interactions in an ecosystem. We proposed knowledge-based clustering methods based on optimization for analyzing the taxonomic content of metagenome short reads [I229, I230]. Experiments on real-life benchmark datasets showed the effectiveness of these methods for reducing the size of a metagenome dataset while maintaining a high accuracy of organism content.

We plan to develop publicly available tools for this type of applications, as done in previous work, for instance [I177].

A new project funded by NWO in the 2008 round of the Computational Life Sciences program, called GeNeUSS (genetic networks underlying synaptic signaling) just started. The aim of this project is to develop dynamical models of neurotransmitter vesicle release. From a machine learning perspective, the challenge is to develop efficient techniques for structure learning in large dynamical models.

Another line of research concerns the application of machine learning techniques for the understanding of gene regulation in the malaria parasite, which may then lead to suggestions for new vaccines. Novel techniques for learning symmetric causal independence models [I215, I167, I90, I89] have been used to link structural information (sequences) to functional information (gene expression) [I136]. The results of this study have recently been published in the leading journal on bioinformatics [I232] and are part of the PhD thesis of R. Jurgelenaite, defended in January 2009. A project proposal to continue our initial efforts (see also [I186]) has been granted in the 2009 round of the Computational Life Sciences program.

B.2.3 Processes in Research, Internal and External Collaboration

Most junior and postdoctoral researchers in the Proof Assistants group come from abroad and we strongly encourage them to participate in and form their own international network. The group has cooperated (and continues to cooperate) with groups in the EU supported Types Coordination Action (2004–2008) and the EU supported FET project Mowgli (2002–2005). These are the main sites in Europe for research into type theory and proof assistants and include INRIA Sophia-Antipolis (Bertot, Théry), INRIA Paris-Rocquencourt (Herbelin, Coq team), Ecole Polytechnique (Dowek), Microsoft-INRIA Research Lab Paris (Gonthier, Werner), ENS Lyon (Hirschowitz), Chalmers University Sweden (Coquand, Bove), University of Białystok, Poland (Trybulec), University of Bologna (Asperti, Sacerdoti Coen), Technical University Munich (Nipkow, Wenzel), Ludwig Maximilian University Munich (Schwichtenberg), Tallin Estonia (Uustalu, Vene).

Furthermore, we cooperate with researchers from the US and Canada: John Harrison, Intel Research, Portland Oregon; Michael Beeson, University of San Jose, California; Zena Ariola, University of Oregon, Eugene; Rick Statman, Carnegie Mellon University Pittsburgh; Amy Felty, University of Ottawa; Jacques Carette, McMaster University, Hamilton, Ontario.

In the Netherlands we cooperate with the Technical University Eindhoven (since August 2006, Geuvers works 1 day per week as a professor at TUE and Zantema from TUE works 1 day per week in Nijmegen; furthermore we cooperate with Nederpelt and Geuvers has served as a copromotor and PhD supervisor of Jojgov) and the Free University of Amsterdam (Surf funded Web Deduction project with De Vrijer and Van Raamsdonk; infinitary rewriting with Endrullis), and furthermore in the Diamant cluster for mathematics.
In iCIS we cooperate with the Digital Security section on foundational themes: category theory, denotational semantics, and with the Model Based System Development section on verification and modelling of hybrid systems and on (dependently typed) functional programming languages. In the Faculty of Science, we cooperate with the Algebra and Logic group in IMAPP, on logic and denotational semantics. Furthermore, we have set up a joint master program “Mathematical Foundations of Computer Science” with the Algebra and Logic group.

The Mind-Brain-Mindfulness group is in close collaboration with the Departments of Biology (prof. E. Roubeos), Biophysics (prof. S. Gielen), Psychiatry (prof. A. Speckens), the Donders Centre for Cognitive Neuroimaging (dr. O. Jensen), Neuroanatomy (dr. J. Veening) and Psychology (dr. H. van Schie and dr. J. Karremans) is established in the form of common PhD and Master students and/or common publications. One such PhD student has defended her thesis (M. Calle), four are working on it. The project attracts international visitors (J. Kabat-Zinn, A. Lutz). A close collaboration is planned with H. Slagter, who returns from the university of Wisconsin at Madison to the University of Amsterdam.

For the study of mindfulness, its application to patients and its function in healthy meditators the interdisciplinary Han Fortmann Center for Mindfulness has been established. It enjoys subsidy for three years by the Radboud Stichting and for six years by the Smartmix project BrainGain.

In the Machine Learning group most junior and postdoctoral researchers work on projects that have both a theoretical and more applied, interdisciplinary component. The application is in collaboration with other researchers outside of our own group. Wherever possible, interaction is stimulated by spending one or two days a week at the (physical) location of the group we work with. Researchers learn to collaborate with researchers from various backgrounds, which we consider a great asset to their future career in- or outside academia.

Because of its ambition to contribute to other scientific disciplines, the Machine Learning group naturally entertains many collaborations with other research groups. Since frequent interaction is considered a prerequisite for success, most of these collaborations are local and national. Within the Radboud University, there are strong ties to several groups within the Donders Centre for Brain, Cognition and Behavior, to the Institute for Wetland and Water Research, and the Centre for Molecular and Biomolecular Informatics. Furthermore, a possibility of collaboration with the Digital Security section is going to be investigated on the research topic of machine learning methods for outlier detection, specifically intrusion detection, credit card fraud and more in general cybercrime.

In the Netherlands, the Machine Learning group works on signal processing for optimizing hearing aids with the TU Eindhoven, audiology with the Academic Medical Center Amsterdam, systems biology for presynaptic genes with the Center for Neurogenomics and Cognitive Research at the VU Amsterdam, and on malaria research with the Biomedical Primate Research Center in Rijswijk. There is a nice balance between the collaborations that started from our own initiative (e.g., brain-computer interfacing, metagenomics, and malaria) and those in which we were asked to partner (e.g., optimization of hearing aids, synaptic genes).

International collaborations of the Machine Learning group are more technology-oriented and exist with, among others, Pablo de Olavide University (Seville, Spain; dr. Divina), Universidad Autónoma de Madrid (prof. Suárez), Eötvös Loránd University (Budapest, Hungary; prof. Lőrincz), Northeastern University Boston (prof. Sternad), the Institute of High Performance Computing and Networking (ICAR-CNR, Catanzaro, Italy; dr. Pizzuti, ing. Folino), University of Cambridge (Computer Laboratory, UK; Pietro Lio’), the University of Reading (Informatics Research Centre, UK; prof. Kecheng Liu), the Dartmouth-Hitchcock Medical Center (Computational Genetics Laboratory, USA; dr. Moore), the Nanyang Technological University (School of Computer Engineering, Singapore; prof. Jagath Rajapakse), the Tuebingen University (Algorithms in Bioinformatics group, Germany; prof. Daniel Huson), and the Max Planck Society (Friedrich Miescher Laboratory, Tuebingen, Germany; dr. Gunnar Raetsch). Through several STW projects, the Smartmix BrainGain project, and a European Marie Curie project, the Machine Learning group has many links to industry. Prominent examples thereof are GN ReSound, a world-leading hearing aid company, and SKF, world’s leading bearing manufacturer.

There is a growing tendency to focus on journal publications covered by ISI. As a rule of thumb,
PhD students in the Machine Learning group are encouraged and supported to write at least 2 journal papers in high-impact, leading disciplinary journals as first authors during their four years of study, alongside 3 to 5 conference papers. W.r.t. these conference papers, we aim for the major conferences in our field (ICML, UAI, NIPS, ECML).

B.2.4 Academic Reputation

Proof Assistants Group

Prof. Barendregt, in 2003 recipient of the Spinoza award (the highest scientific award in the Netherlands), is internationally known for his work on lambda calculus and type theory. Presently he directs an interdisciplinary group studying the neurophysiological correlates of mind-states. He is an adjunct professor at Carnegie-Mellon University and a member of the Editorial Board of the electronic journal Logical Methods in Computer Science. He has been a co-organizer of the meeting International Conference on Mathematical Software (Castro-Urdiales, 1-3.09.2006) together with Wiedijk. Also he had co-organized Computability in Europe (Athens, 8-12.06.2008). From 2005-2009 Barendregt is member of the Board of Diamant Cluster for Mathematics. He is a member of the Academia Europaea (since 1992), Koninklijke Hollandsche Maatschappij der Wetenschappen (since 1995) and the Royal Dutch Academy of Sciences (KNAW, since 1997).

Prof. Geuvers is a world leading expert on type theory and proof assistants. He has been a member of the Steering Committee of the EU Coordination Action “Types” and Trustee of the MKM (Mathematical Knowledge Management) Interest Group. He has lead and is leading a number of NWO funded projects, notably the BRICKS (Basic Research in Informatics for Creating the Knowledge Society) project ARPA (Advancing the Real use of Proof Assistants) involving 500 MEuro. Geuvers has been very successful in obtaining funding from the NWO open competition (4 projects granted in the reporting period). He was the organization chair and PC member of the Logic Colloquium 2006, the annual logic meeting organized under auspices of the ASL, and chief editor of its proceedings as Lectures Notes on Logic in the LNL series (2009) and as a volume of the Annals of Pure and Applied Logic (2008). Prof. Geuvers has been organizer and PC member of various workshops and conferences. Since August 2007, prof. Geuvers works 1 day per week as a professor in the OAS group of the Faculty of Mathematics and Computer Science of the Technical University Eindhoven. He is a member of the BCI (committee for the evaluation of research proposals in Computer Science of NWO). He has been an invited speaker at various meetings, an invited lecturer at various research summer schools all over the world (France, Sweden, Italy, USA and Uruguay) and an external examiner of national and international PhD. defenses. He has been external co-promotor of four PhD students [I217, I218, I220, I226].

Prof. Klop is a world leading expert on term rewriting, lambda calculus and process theory. He is one of the most cited Dutch computer scientists, a member of the Royal Dutch Academy of Sciences (KNAW, since 2003), a CWI fellow (since 2005), member of the IFIP working group 1.6 on term rewriting, and a Doctor honoris causa at UEA, University of East-Anglia. He is one of the initiators, editors and main authors of the seminal overview book “Term Rewriting Systems” by the Terese author group (including also Zantema). Klop has given numerous invited talks, has been the project leader of numerous NWO projects and has been external examiner of 12 national and international PhD theses. Finally, Klop is an editor of Indagationes Mathematicae (since 2007), member of the board of NVTI (Dutch Association for Theoretical Computer Science, since 2002; and chairman of the board 2002-2004) and he has been a member of the board of the IPA research school (2002-2006).

Prof. Zantema is a world leading expert on term and string rewriting. His tool TORPA was the winner in the category string rewriting in the Termination Competition, reported at the International Workshop on Termination, in 2004 and in 2005. He was organizer of the international Termination Competition (together with Claude Marche, Paris) from 2005 to 2007. He is a member of the editorial board of the Journal of Logic and Algebraic Programming and a frequent member of the Program Committee of the annual conference on Rewriting Techniques and Applications
B.2.4. ACADEMIC REPUTATION

(RTA) and a member of the IFIP working group WG 1.6 Term Rewriting.

Dr. Wiedijk is a worldwide known specialist in proof assistants and formalization of mathematics. He has conceived and edited the book *The Seventeen Provers of the World*, (Springer LNAI 3600, 2006) and has written an invited paper *Formal proof - getting started*, in the Notices of the AMS (volume 55(11), 2008). Wiedijk has been a member of various PCs, editor of various proceedings and has given various invited talks.

The Ph.D. student O’Connor has been invited to present a research proposal (as one of the 10 out of 63 applicants) at the “Young Scholar’s Competition” at the “Horizons of Truth: Gödel Centenary 2006”. He presented a proposal called “New Horizons of Proof: Software Verification of Gödel’s Second Incompleteness Theorem”, which was well-received but did not end in the top three. The Ph.D. student Loeb was awarded the Frye Stipendium in 2005, an annual grant for the most promising female PhD. students at the Radboud Universiteit Nijmegen.

The Proof Assistants group attracted the following grants.

- BRICK NWO-Focus project ARPA on advancing the real use of proof assistants.
- NWO projects IMDoc on interactive mathematical documents creation and presentation; MathWiki; CoFDERA, on coalgebraic formal development of real arithmetic; OpenTerms on the use and meaning of open terms in interactive formal problem solving, in collaboration with TUE.
- Surf project Webeduction in collaboration with VUA.
- EU projects Mowgli (EU-IST-FET project) on “Mathematics On the Web, Get it by Logic and Interfaces”, in collaboration with University of Bologna, Saarbreken, INRIA, Trusted Logic, and Max Planck gesellschaft; Calculus (EU-IST-TMR) on systems for integrated computation and deduction, in collaboration with TUE.

Mind-Brain-Mindfulness Group

The academic reputation of prof. Barendregt is described in the previous sub-section. The directors of the Mind-Brain-Mindfulness related project have created the Han Fortmann Center for Mindfulness. It has the unique position of bringing together mindfulness meditation and mindfulness intervention in a (neuro-) scientific research environment. Visitors have been J. Kabat-Zinn, A. Lutz.

The Mind-Brain-Mindfulness attracted the following grants.

- NWO Spinoza awarded to prof. Henk Barendregt.
- Smartmix project Braingain on brain-computer interfaces (with many other Dutch partners).
- Bial project (Institute of Public Utility, Portugal).

Machine Learning Group

Prof. Heskes is editor-in-chief of Neurocomputing, one of the main journals on neural networks and among the ten largest journals in computer science. Since 2003, the start of his appointment as editor-in-chief, Neurocomputing’s volume increased by 50% and its impact factor doubled (now 1.234). He is further an editorial board member of “Foundations and Trends in Machine Learning” and the “Journal of Computational Intelligence Systems” and an area editor for the Handbook of Natural Computing (in press). During the review period, he acted as an opponent at 6 PhD defenses outside the Netherlands, gave invited talks at conferences, workshops, and institutes, was a programme committee member of about 40 conferences, and reviewed many national and international grant proposals. Prof. Heskes is an affiliated principal investigator at the Center for Neuroscience of the Donders Institute for Brain, Cognition, and Behavior.
Dr. Marchiori is specialist in heuristic (stochastic) optimization, machine learning and bioinformatics. She started working at the RU in the Machine Learning group in 2008. She has an H-index according to Google Scholar of 19 (on 16 June 2009). She is editorial board member of the two international journals ‘BioData Mining’ and ‘Journal of Artificial Evolution and Applications’. In 2008, she was technical co-chair of three international conferences in Machine Learning and Bioinformatics. She was the initiator in 2002 of the EvoNet working group on Evolutionary Computation, Machine Learning and Datamining in Bioinformatics (EvoBIO), upgraded from workshop to conference in 2007. At present, she is (co)chairman of the Steering Committee of EvoBIO. In 2008 she was programme committee member of 12 international conferences, reviewer of many international journals, and of international project proposals. She is at the moment project leader of two RU projects on bioinformatics in collaboration with prof. M. Huynen (NCMLS) and prof. M. Jetten (IWWRI), in which she is supervising two PhD’s. Moreover, she is co-promotor of one external PhD student.

Dr. Sarbo is recognized as a specialist in the field of computational semiotics. His research has been acknowledged by a best paper award in 2005 [I94]. Sarbo organized an international workshop (The Dynamics of Knowledge and Interpretation), in 2008. Invited by prof. Kecheng Liu, Sarbo had been on sabbatical at Reading University (Reading, UK) for two months, in 2009. This year he gave lectures on semiotic research at the Francois-Rabelais Polytechnical University (Tours, France), for a week. Sarbo was a PC member of ICCS for several years.

The Machine Learning group attracted the following grants.

- NWO VICI awarded to prof. T. Heskes.
- STW projects HearClip on personalizing hearing aids (collaboration with TU Eindhoven and AMC Amsterdam) and Bayesian Brain-Computer Interfacing (collaboration with FC Donders Centre for Cognitive Neuroimaging).
- NWO-CLS projects GENEUSS on synaptic signalling (collaboration with VU Amsterdam) and RUMPHI on malaria (collaboration with Biomedical Primate Research Center).
- Smartmix project Braingain on brain-computer interfaces (with many other Dutch partners).
- EU Marie Curie project AI4IA on industrial applications of artificial intelligence (collaboration with SKF Research and other European partners).

### B.2.5 Internal Evaluation

All members of the groups have annual assessments, where all activities (including research) are evaluated. PhD students have an additional assessment after one-and-half year, after which their contract is (possibly) extended to the full four years. At the monthly IS staff meetings the general issues and policies are discussed. At the biweekly research lunches of the Proof Assistants group, concrete research results and questions are presented in an informal atmosphere. Also the research strategy is discussed at these lunch meetings.

### B.2.6 External Validation

Results of research performed within the IS section have positive effects outside the scientific community, both in industry and society.

Applications of Proof Assistants to modelling and verification are used in industry. In particular, INRIA-Microsoft Research Labs in Paris and Intel in Portland Oregon use proof assistants for industrial size verification; various small companies – e.g. in France – have started to use Coq for software verification. Moreover, research on Proof Assistants attracts interest also from the media. An article entitled “Zegt de Computer” appeared recently (31-01-2009) in one of the major
national newspapers NRC, where Freek Wiedijk was interviewed on the topic on formalization of mathematics (see http://www.cs.ru.nl/IS/ISWebRep/NRC.pdf).

The effects of collaboration and dissemination of research on Mind-Brain-Mindfulness outside the scientific community are demonstrated by the many lectures held by Barendregt about this topic. For instance, the local Science Cafe devoted one evening to mindfulness studies (see http://www.sciencecafenijmegen.nl/?page=10februari2009). Moreover, Henk Barendregt and Karin Videc gave four public lectures on “The Mind on the Brain and the Brain on the Mind” at the Han Fortmann Center (see http://www.cs.ru.nl/~henk/HFL.html).

The Machine Learning group works on several problems in collaboration with and inspired by industry, in particular within the context of STW projects on the personalization of hearing aids and brain-computer interfaces, and the Marie Curie project AI4IA coordinated by the bearing company SKF. The MEG system build in collaboration with researchers from the Donders Centre for Cognitive Neuroimaging was covered by the national television science program Nieuwslicht (January 16, 2008). Both our efforts towards better methods for cognitive neuroimaging and our bioinformatics research on synaptic signalling (GENEUSS project) aim at a better understanding of how the brain functions in health and disease. Our bioinformatics research line on the malaria parasite is motivated by the need to develop better vaccines. The bioinformatics research line on protein networks is motivated by the need to improve knowledge on protein function in relation to disease onset and progression. The one on metagenomics is motivated by the need to develop microbial communities for remediation of environmental contamination.

B.2.7 Researchers and Other Personnel

As mentioned before, the section Intelligent Systems started in 2008 out of the former Foundations department and some members of the former IRIS department.

Proof Assistant Group

The Proof Assistant Group has operated as a separate research group ‘Foundations’ until January 2008, until August 2006 under the research leadership of prof. H. Barendregt and since then under the joint leadership of prof. H. Barendregt and prof. H. Geuvers. Since 2006, dr. F. Wiedijk has joined the group as an assistant professor, as a successor of dr. W. Dekkers, who has retired. During the whole period, dr. D. van Leijenhorst has also been associate professor in the group, but he has devoted most of his time to education and since 2008 he is absent due to illness. The other scientific staff in the group are non-permanent, funded from external sources. The group has profited a lot from external grants, among which the mentioned Spinoza award. At its largest the group consisted of about 20 scientists.

At present the group consists of – apart from the three permanent staff members mentioned above – 2 part-time professors (prof. J.W. Klop and prof. H. Zantema, both 0.2 fte), one non-permanent assistant professor (dr. J. McKinna, funded from the Dutch NWO Mathematics cluster Diamant), one post-doc (dr. A. Koprowski), two part-time scientific programmers and five PhD students.

Junior researchers and post-docs are acquired through internet advertisements and our personal scientific network. A strong logical/mathematical background is important.

Mind-Brain-Mindfulness Group

The related project is presently directed by: prof. dr. H. Barendregt (ICIS), prof. dr. S. Gielen (F.C. Donders Instituut, Biophysics), and prof. dr. A. Speckens (Psychiatry).

Senior researchers: dr. F. Giommi (clinical psychology); dr. J. Veening (neuro anatomy).

Table B.2.1: Research staff at programme level (SEP Table 4)

<table>
<thead>
<tr>
<th>Intelligent Systems</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tenured staff</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Full professors</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barendregt, Henk</td>
<td>0.80</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Geuvers, Herman</td>
<td>0.50</td>
<td>0.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heskes, Tom</td>
<td>0.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Associate professors</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geuvers, Herman</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heskes, Tom</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.47</td>
<td></td>
</tr>
<tr>
<td>Leijenhorst, Dick van</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
</tr>
<tr>
<td>Marchiori, Elena</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.39</td>
</tr>
<tr>
<td><strong>Assistant professors</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dekkers, Wil</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>Heskes, Tom</td>
<td>0.10</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.37</td>
<td>0.40</td>
</tr>
<tr>
<td>Sarbo, Janes</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>Wiedijk, Freek</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.37</td>
<td>0.40</td>
</tr>
<tr>
<td><strong>Total tenured staff</strong></td>
<td>2.20</td>
<td>2.50</td>
<td>2.80</td>
<td>3.17</td>
<td>3.03</td>
<td>3.39</td>
</tr>
<tr>
<td><strong>Non tenured staff</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capretta, Venanzio</td>
<td>0.30</td>
<td>0.90</td>
<td>0.82</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carlström, Jesper</td>
<td>0.25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corbineau, Pierre</td>
<td>0.23</td>
<td>0.90</td>
<td>0.90</td>
<td>0.67</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cruz-Filipe, Luis</td>
<td>0.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dijkstra, Tjeerd</td>
<td>0.02</td>
<td>0.20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gerven, Marcel van</td>
<td>0.75</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Giero, Mariusz</td>
<td>0.95</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Giommi, Fabio</td>
<td>0.27</td>
<td>0.25</td>
<td>0.30</td>
<td>0.30</td>
<td>0.30</td>
<td>0.27</td>
</tr>
<tr>
<td>Groot, Perry</td>
<td>0.15</td>
<td>0.90</td>
<td>0.67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hendriks, Dimitri</td>
<td>0.15</td>
<td>0.90</td>
<td>0.67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hurkens, Tonny</td>
<td>0.03</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
</tr>
<tr>
<td>Klop, Jan-Willem</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.20</td>
<td>0.08</td>
<td>0.04</td>
</tr>
<tr>
<td>McKinna, James</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.13</td>
<td>0.40</td>
</tr>
<tr>
<td>Niqui, Milad</td>
<td>0.20</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.45</td>
</tr>
<tr>
<td>Spitters, Bas</td>
<td>0.92</td>
<td>0.85</td>
<td>0.92</td>
<td>1.00</td>
<td>0.33</td>
<td></td>
</tr>
<tr>
<td>Wiedijk, Freek</td>
<td>0.77</td>
<td>0.82</td>
<td>0.37</td>
<td>0.03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zantema, Hans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.06</td>
<td>0.10</td>
</tr>
<tr>
<td><strong>Total non tenured staff</strong></td>
<td>2.99</td>
<td>3.43</td>
<td>3.32</td>
<td>3.53</td>
<td>4.63</td>
<td>5.58</td>
</tr>
<tr>
<td><strong>PhD candidates</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahramisharif, Ali</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.08</td>
</tr>
<tr>
<td>Bizlutiu, Adriana</td>
<td>0.51</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calle, Cinzia</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cheung, Ling</td>
<td>0.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claassen, Tom</td>
<td>0.17</td>
<td>0.77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cseke, Botond</td>
<td>0.75</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gori, Florencia</td>
<td>0.23</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hurk, Paul van den</td>
<td>0.23</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jancuro, Pavol</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jurgen, Rasa</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kalisz, Cezary</td>
<td>0.34</td>
<td>0.68</td>
<td>0.22</td>
<td>0.90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leob, Iris</td>
<td>0.82</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.08</td>
<td></td>
</tr>
<tr>
<td>Mamane, Lionel</td>
<td>0.19</td>
<td>0.90</td>
<td>0.45</td>
<td>0.45</td>
<td>0.90</td>
<td>0.53</td>
</tr>
<tr>
<td>Niqui, Milad</td>
<td>0.90</td>
<td>0.52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O’Connor, Russell</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td></td>
</tr>
<tr>
<td>Whitmarsh, Stephen</td>
<td>0.17</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total PhD candidates</strong></td>
<td>2.78</td>
<td>2.57</td>
<td>3.79</td>
<td>5.62</td>
<td>6.34</td>
<td>8.90</td>
</tr>
<tr>
<td><strong>Total research staff</strong></td>
<td>7.97</td>
<td>8.50</td>
<td>9.91</td>
<td>12.32</td>
<td>14.00</td>
<td>17.87</td>
</tr>
</tbody>
</table>
Machine Learning Group

The Machine Learning group operated more or less independently of other subgroups within IRIS during the period October 2004 - December 2007, basically consisting of one staff member (prof. T. Heskes, then assistant and later associate professor) and a couple of junior researchers. Successful acquisition of external funding led to a rapid growth, in particular during the last 2 years. A new senior position, in anticipation of the retirement of other staff members and until then financed externally, was created to strengthen and broaden the group’s expertise: dr. E. Marchiori joined the group in February 2008. With the rearrangement of iCIS in January 2008, dr. J. Sarbo moved from IRIS to the Machine Learning group, which was the most natural option considering his ongoing research. The group currently hosts 7 junior researchers, 3 postdoctoral researchers, one senior researcher (dr. T. Dijkstra, 0.2 fte), one assistant professor (dr. J. Sarbo), one associate professor (dr. E. Marchiori), and one full professor (prof. T. Heskes).

Junior researchers are typically acquired through internet advertisements and the researchers’ own network. A strong mathematical background is important, which may explain why we have quite some candidates from Eastern Europe.

B.2.8 Resources, Funding and Facilities

B.2.8.1 Resources and Funding

Table B.2.2 specifies the ratio between direct and indirect funding over the years, showing a huge shift, from over 80% direct funding in 2003 to just over 30% in 2008.

<table>
<thead>
<tr>
<th>Intelligent Systems</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Direct Funding</td>
<td>83.2</td>
<td>63.7</td>
<td>55.9</td>
<td>44.3</td>
<td>37.4</td>
<td>32.5</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>15.1</td>
<td>24.8</td>
<td>43.5</td>
<td>49.3</td>
<td>57.3</td>
<td>63.5</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>1.7</td>
<td>11.5</td>
<td>0.6</td>
<td>6.4</td>
<td>5.3</td>
<td>4.0</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

B.2.8.2 Facilities

The Mind-Brain-Mindfulness group has its own an EEG experimentation room. Both the Mind-Brain-Mindfulness and the Machine Learning group make, through their collaborations, use of the excellent facilities (EEG, MEG, occasionally fMRI) at the Donders Centre for Cognitive Neuroimaging.

In 2008, the section purchased two Sun X4150 servers, to be used for proof checking and verification, data analysis, and machine learning applications.

B.2.9 Overview of the Results

Key publications (with motivation).

  (Publication in a top artificial intelligence journal following-up on earlier patent [I219].)
(Introducing the philosophy of our work in proof assistants and computer mathematics.)


(Overview paper of exact real arithmetic and its connections with domain theory and constructive analysis.)


(Formalization of the proof of Gödel’s incompleteness theorem. A milestone in the formalization of mathematics.)


/Publication of a new data analysis method in a machine learning journal with high - 3.116 - impact factor.

Table B.2.3: Programme results: outcome numbers (SEP Table 6)

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. book chapters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total academic publications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Monographs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. PhD theses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total publications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B.2.10 Analysis, Perspectives and Expectations

Strengths

- The IS section has a very good national and international reputation, in particular for research in type theory, term rewriting, proof assistants, and machine learning. Its expertise in type theory, proof assistants, formalizing mathematics, and Bayesian machine learning is unique in the Netherlands.

- Research performed within IS is both theoretical and applied. The Proof Assistants group has a unique combination of expertise, covering the range from the underlying theories of proof assistants to their engineering aspects and applications in formalizing mathematics. The Machine Learning group performs fundamental research in Bayesian techniques and pattern recognition, and uses these results to tackle case studies in diverse application areas such as (cognitive) neuroscience and bioinformatics. The IS section is at the international forefront of the above mentioned research areas.
Acquisition of numerous external projects and funding, including the prestigious Spinoza award (the highest scientific prize in the Netherlands) by Barendregt and the VICI award by Heskes, allows for a good critical mass: researchers can learn not only from their supervisors but also from each other, and a sufficiently large critical mass allows us to invite interesting external researchers and speakers at the group seminars.

The IS section has many active collaborations with researchers from different disciplines, including biology, neuroimaging, audiology, signal processing, mathematics, psychology. This leads to high quality research and gives many opportunities for feedback and funding.

Weaknesses

- Each group conducts its own research line independently of the other groups.
- Coherence between research and teaching is suboptimal in the mathematically oriented research topics, mainly because few computer and information science students are attracted to this type of research.
- The application domains currently under consideration are quite wide-spread (including neuroimaging, audiology, acoustic emission, biology, mathematics, psychology). It is impossible for the group leaders to keep track of the literature in all these fields. For an important part, they have to rely on the researchers with whom they collaborate and on the junior researchers’ endeavor.
- Tool and software development requires substantial time and yields relatively few publications.
- Machine learning research in Nijmegen is spread across different institutes (Donders Centre for Cognition, SNN Department of Biophysics). Thisdiffusesthe external perception of the Machine Learning group. The same applies to the Mind-Brain-Mindfulness group.
- The number of Ph.D. students in the Proof Assistants group is quite low. (Two defending in 2009, one student remaining and one open position.)

Opportunities

- The multi-disciplinary research performed in the section allows to investigate new research fields and applications of computer science.
- The applications of proof assistants to modelling and verification have now transcended the level of toy examples (INRIA-Microsoft Research Labs in Paris and Intel in Portland Oregon use proof assistants for industrial size verification; various small companies – e.g. in France – have started to use Coq for software verification). This opens up the possibility of setting up larger joint cooperations and attracting funding from these companies.
- The formalization of mathematics has applications in the context of the semantic web: providing semantically rich mathematical information on the web through formalized mathematics. We have very recently (2009) started the (NWO funded) MathWiki project to develop technology for supporting this.
- The new master theme “Mathematical foundations of computer science”, a cooperation with the Algebra and Logic group of the Mathematics department, gives us a platform to attract good master students to our research and to enhance the cooperation with the mathematics department.
- Our involvement in the bachelor and, starting from 2009, master curriculum Artificial Intelligence, opens the possibility to interest and attract more students, who eventually might be interested in obtaining PhD positions.
There are ample opportunities to apply Intelligent Systems to many different domains, not only in science, but also in industry. We have not actively pursued contract research on industrial applications in the last couple of years, but could do so in the future, e.g., as a follow-up of the STW projects.

The different background of IS staff yields new research opportunities. Stronger links between the groups will boost interdisciplinary research.

Threats

- The permanent staff members of the IS section have a high organizational load: starting from January 2009, prof. H. Geuvers is the education director of iCIS, and prof. T. Heskes is the research director of iCIS. This may affect their scientific productivity and the one of their group members.

- The section members are responsible for a large part of the teaching of the courses in theoretical computer science and artificial intelligence.

- The number of PhD students in the Machine Learning group increased a lot over the last years, putting a high demand on supervision to continuously guarantee the high level of research output.

- The increased focus of the section on applications may affect the production of more speculative or foundational research.

Analysis

It should be clear from the above SWOT analysis that the IS section has been quite successful in attracting research funds (see Strengths). This has also allowed the funding of quite speculative and foundational research, notably by the Spinoza of Barendregt and the VICI of Heskes. In general there is more funding for more applied research, which means that we have to work hard to maintain the level of foundational research. Furthermore, the highly interdisciplinary character of the IS research themes requires continuous effort for keeping track of new achievements in both the application domain and methods, and for collaborating with domain experts. Finally, the high organizational and teaching load of this section, severely restricts the time available for research. On the other hand, the participation of the section in teaching of courses provides an opportunity for directly involving master students in research projects.

Adjusted goals

There is no immediate need for the IS section to adjust its goals. The Proof Assistants group continues to advance the use of proof assistants through foundational research, interfaces and applications in computer science and formalizing mathematics. The Machine Learning group continues to contribute to theoretical and applied research in this field.

Adjusted strategy

We will address the threats reported in the SWOT list by exploiting the mentioned opportunities. Specifically, we will apply for external grants, in particular in collaboration with industry, in order to fund new senior and postdoc personnel. This will decrease the teaching load of the senior staff and will increase and maintain the critical mass of the groups.

The reported weaknesses and threats will be tackled as follows.
Tackling the weaknesses

- The diversity of the research themes within the IS section implies that they cover a broad range of AI approaches. At the moment this is possible because each of the three groups has a sufficient number of researchers for generating critical mass. We plan to profit from this rich expertise in joint research activities, by means of a synergy of diverse approaches that will boost research on the frontier of AI. For instance, the Machine Learning and Mind-Brain-Mindfulness groups started a collaboration on recording different brain states in the hope that classification techniques may differentiate them.

- Several initiatives are taken to improve the coherence between research and education, most notably a new master in Mathematical Foundations of Computer Science and stronger involvement in the master program Artificial Intelligence. Section members continue to invest in PR activities to attract new students.

- The application domains currently under consideration are quite wide-spread (including neuroimaging, audiology, acoustic emission, biology, mathematics, psychology). In order to keep track of the literature in all these fields we work in close collaboration with domain experts. Moreover, we try to set up projects involving not only PhD students but also postdocs, the latter ones being more experienced hence offering a solid technological background on techniques related to these projects.

- The IS section is more and more focusing on tool and software development. Covering the entire research and development process requires substantial time and yields relatively few publications. We are addressing this potential weakness by involving also master students and scientific programmers in this process, in particular in the tool design and implementation phases. This will also allow the permanent staff to focus also on more speculative and foundational research (thus tackling also the threat above mentioned).

- Research in Nijmegen closely related to that of the IS section, specifically those of the Machine Learning and Mind-Brain-Mindfulness groups, is spread across different institutes (Donders Centre for Cognition, SNN Department of Biophysics). We are turning such potential weakness, caused by a possible diffuse perception of these groups, into strengths by working in close collaboration with the above mentioned institutes, in order to increase the visibility of Nijmegen research.

- In order to increase the number of Ph.D. students in the Proof Assistants group and to balance the decline in baseline funding, we will strive to acquire more projects involving PhD students positions, both at national and European level.

- To handle the growth of the Machine Learning group, in combination with the increased teaching and administrative duties, we give a more prominent role to experienced postdoctoral researchers: they assist in the supervision of PhD students as well as in the acquisition of new grants.

Summary

The IS section has grown rapidly from its start in 2008 into a cluster of three groups with clear and well structured research lines covering complementary themes in Intelligent Systems research. The interdisciplinary character of the research performed within this section has favored and stimulated achievements both in scientific as well as in societal relevant areas.
B.2.11 Publications

2003

Academic publications

Articles in refereed proceedings


Monographs


Professional publications


2004

Academic publications

Refereed journal publications


Articles in refereed proceedings


**Book chapters**


**PhD theses**


**Professional publications**


2005

Academic publications

Refereed journal publications


Articles in refereed proceedings


B.2.11. PUBLICATIONS


Book chapters


Professional publications


2006

Academic publications

Refereed journal publications


Articles in refereed proceedings


**Book chapters**


**Monographs**


**PhD theses**

Professional publications


2007

Academic publications

Refereed journal publications


Articles in refereed proceedings


B.2.11. PUBLICATIONS


Monographs


PhD theses


Professional publications


2008

Academic publications

Refereed journal publications


Articles in refereed proceedings


Book chapters

B.2.11. PUBLICATIONS


Monographs


PhD theses


Professional publications


Other publications referenced in the text


Chapter B.3

Model-Based System Development

Title of the Research Programme: Model-based System Development (MBSD)

Research Area and Mission: The topics driving the research carried out in the section on model-based system development are models and modeling. Models provide abstractions of systems, artificial or natural, that allow reasoning about properties of these systems, ignoring extraneous details while focusing on relevant ones. Explicit models have always played a key role in science and engineering. There is now a clear trend in computer and information science towards the systematic use of models as the primary artifacts throughout the engineering life cycle of computer-based systems. Requirements, behavior, functionality, construction and testing strategies of computer-based systems are all described in terms of models. Models are not only used to reason about a system, but also used to allow all stakeholders to participate in the development process and to communicate with each other, to generate implementations, and to facilitate reuse.

The mission of MBSD is to carry out fundamental research on the use of (mathematical) models in the development of computer systems in relationship to application areas, on the one hand, and basic techniques, on the other hand, as schematically depicted in Figure B.3.1. Our theories, methods and tools are empirically validated through the development of challenging applications from business, industry, government, and health care, thus aiming at bridging the gap between theory and practice.

Keywords: modeling, embedded and distributed systems, computer-aided verification and analysis, model-based application generation, model-based testing, medical decision-support systems


Starting Date of the Programme: 2008

Affiliations outside iCIS: MBSD participates in the Dutch graduate schools IPA (Institute for Programming research and Algorithmics) and SIKS (Information and Knowledge Systems)

B.3.1 Leadership

Almost from its inception, the MBSD section was seen by its members as being one group of researchers without a sharp subdivision into subgroups, with each section member having specialized expertise on part of model-based system development and responsibility to manage this expertise. As this yielded a flat organization structure, it was decided to adopt a management style in correspondence with that structure, i.e., flat, open, and informal, often called Nordic nowadays, where section members who are affected by decisions are invited to express their opinions and judgements, respecting their expertise in particular areas, and allowing them to influence the decisions. Traditionally, Dutch universities are organized hierarchically, where the professor is head of department and acts as ‘the boss’. At MBSD, we have adopted the Anglo-Saxon way.
university departments are organized, where responsibilities are shared.

A flat organization structure works well for maximizing parallelism of research, but is not optimal for driving the research, finding new research challenges, looking for cooperation with internal and external researchers and groups, and for finding ways to attract new funding for research. It is impossible for a single person, such as the head of the section, to cover the entire thematic spectrum of model-based system development, which is why much of the research innovation is driven by subtheme leaders: section members with significant research experience in a specialized field. They are the program leaders mentioned at the beginning of this chapter. The subtheme leaders meet on a regular basis, usually weekly on an ad-hoc basis, to discuss new opportunities and matters of research strategy, but by appointment if there is something important on the agenda. Anyone in the section has freedom to work on any of the subthemes.

Having a flat section structure, it took some effort to increase the synergy of the research in the section. The need for this was obvious as by combining expertise on different aspects of model-based system development, research can be done that would be impossible otherwise. From the beginning, steps were taken to increase the synergy by involving members with diverse backgrounds in research projects. A typical example is the involvement of section members with a different background in the OCTOPUS project, where section members use both methods for model-based analysis and probabilistic graphical models. In addition, increase in synergy was stimulated by regular meetings and a weekly section colloquium, where researchers of the section informed each other of their research.

Through part-time appointments of prof. Hooman, dr. Tretmans (both Embedded System Institute), prof. Proper (Capgemini), and prof. van Vliet (Deloitte), together with close interaction with professionals in the health-care sector, financial sector and government, it is ensured that our more academic research is driven by real-world demands and sought for innovation by the various fields of application.

B.3.2 Strategy and Policy

B.3.2.1 History and Context

The main motivation for creating MBSD was the insight that the vision of model-based system development is becoming an increasingly important driving force of the software and hardware
industry, whereas it already played a key role in the research of many groups within iCIS. The MBSD section was created at the beginning of 2008, as part of an effort to restructure the research within iCIS in somewhat larger units. In particular, there was existing research on:

- computer-aided verification and analysis techniques in the previously existing Departments of Informatics for Technical Applications (ITA) and Software Technology (ST),
- advanced functional programming and code generation techniques for model-driven application development in the previously existing ST department,
- model-based reasoning using probabilistic graphical models in the previously existing Department of Information and Knowledge Systems (IRIS), and
- conceptual modeling, focusing on the modeling process and the use of models as a means for communication between stakeholders, also in the IRIS department.

These model-based research topics have been merged in the MBSD section. The members of the MBSD section have thus expertise covering a broad range of topics concerning model-based system development, which is seen as a unique feature of the group with significant added value.

### B.3.2.2 Research Focus

Combining the expertise on model-based system development yielded the research landscape shown in Figure B.3.1. The diagram indicates that our research is grounded on expertise in specific basic techniques (lowest layer in the diagram), which roughly correspond to the subthemes that drive our research. Each subtheme is led by a subtheme leader: the subtheme of computer-aided verification and analysis (T.1) is led by prof. Vaandrager, the subtheme on model-based reasoning using probabilistic graphical models (T.2) is being led by dr. Lucas, the subtheme on model-based application generation (T.3) by prof. Plasmeijer, and, finally, prof. Proper leads the conceptual modeling subtheme (T.4).

MBSD is committed to apply the basic techniques (theories, methods, and tools) to challenging practical applications, and these are shown as the top layer of the diagram in Figure B.3.1. The middle layer indicates that both research on basic techniques and applications are directly linked to various aspects of the overall research theme of model-based system development. The middle layer expresses that once a model is available one can reason with it in order to diagnose problems, predict particular system behavior, and, thus, also to analyze the behavior. Dependent on the characteristics of the model, this can be done using different techniques, e.g., using model checking, probabilistic reasoning, a functional program, etc. Furthermore, models may also need transformation, based on changed requirements from a problem domain or used as a development method. Finally, models are constructed based on the requirements of a problem, stakeholders, etc., and implemented using model-based software generation methods or reasoning methods; validation of whether the model does what it should do is performed relative to the problem domain or system for which the model was built.

Members of MBSD are well known for their work in the following application areas:

- embedded and distributed systems (A.1) (e.g. [M78, M14, M9, M244, M268, M248, M469, M412, M79, M299, M84, M18, M142, M406, M195, M448, M287, M333, M250]),
- workflow management systems and enterprise engineering (A.2) (e.g. [M471, M475, M382, M428, M400, M481, M202, M334, M504, M292, M345, M499, M346]), and
- medical decision support (A.3) (e.g. [M61, M147, M344, M349, M348, M450, M340, M445, M442, M451]).

Companies and organizations typically are not interested in just one specific application of models. Once they have gone through the costly effort of constructing models for, say, verification, they also want to use them for application generation, testing, fault diagnosis, etc. By the integrated
use of our basic techniques during the whole model-based system development life cycle, we can handle practical applications more effectively.

The research landscape of MBSD is broad. MBSD’s future research strategy is to focus MBSD research especially on the following topics — which combine elements of the basic techniques, development activities, and applications of the diagram in Figure B.3.1 —, discussed in more detail below:

1. Computer-aided verification, analysis and testing of embedded systems and software;

2. Model-based application generation for building workflow management and other software systems;

3. Model-based methods for building medical decision-support systems.

B.3.2.3 Characteristics

Some characteristics of the research within our section are:

- The inspiration comes from practice, in the form of challenging problems, which subsequently forms the basis for fundamental research at an international level on basic techniques. Thus, the research approach is both society-driven and knowledge-driven.

- Software tools play an essential role within our research: formal methods are considered incomplete without tools such as compilers, theorem provers, test tools, model editors, model checkers, visualization engines and reasoning engines.

- The results of this scientific research contribute to the solution of the original industrial problems that formed its inspiration. Indeed, it is the section’s ambition to have an internationally acknowledged leading position both in developing new scientific theories and in applying them in (business, industry, public sector, health care) practice, following the practice-as-laboratory approach (cf. Figure B.3.2). Several of our PhD students and postdocs are supported by industry, government, and health care.

- Being able to cover a wide spectrum ranging from theory to practice is highly appreciated by us. Much of our research is carried out in a multidisciplinary context.

- External funding is seen as an important criterion for the quality and societal relevance of the research, and as an essential structuring factor.

- Pure curiosity-driven or fundamental research (in this context in areas such as methodology, automata theory, logic) is seen as an essential part of an academic attitude.

- Influence inside and outside academia is sought not only via publications in the scientific literature and joint projects, but also via contributions in non-scientific periodicals and in the press, contact with high school students, via participation in scientific steering committees (within funding bodies and program committees of conferences), and professional organizations such as the Netherlands Architecture Forum (NAF).

B.3.2.4 Basic Techniques

We will now elaborate on our research strategy concerning the four basic technologies (bottom row of Figure B.3.1) that are being used and further developed within our section.
T.1 Computer-aided verification and analysis

**Timed, hybrid and probabilistic automata.** Model checking is emerging as a practical tool for automated debugging of complex reactive systems such as embedded controllers and network protocols. In model checking, specifications about the system are expressed as (temporal) logic formulas, and efficient symbolic algorithms are used to traverse the model defined by the system and check if the specification holds or not.\(^1\) In our research on model checking, we consider systems that are described as networks of *timed automata* in the sense of Alur and Dill. Our group is one of the two or three leading groups worldwide in the area of applying timed automata model checking to industrial sized problems. In part due to our work, tools such as Uppaal are now routinely used for industrial case studies. We follow an iterative approach where fundamental research on theory and algorithms – challenged by real-life case-studies – is developed and implemented in methods and tools, which are evaluated again through case studies. This research cycle is very labor intensive and for that reason we have decided not to develop our own model checking tool. Instead, we closely collaborate with the team of prof. Larsen of Aalborg University to add new functionality to the Uppaal model checker. This collaboration is supported by the EU projects AMETIST (that we coordinated) and QUASIMODO. At the national level our research is supported by the projects HaaST, FRAAI, ARTS, and OCTOPUS.

We have proposed and implemented (together with the team of prof. Larsen) several extensions of Uppaal, such as distributed model checking (2000), guided model checking (2001) and parametric model checking (2002). More recently, we enhanced Uppaal with symmetry reduction [M81] and we developed an effective method for compositional abstraction [M411]. Our team coauthors the latest Uppaal 4.0 release in which this extension has been implemented [M252]. Uppaal is downloaded more than 700 times each month and has many users both in academia and industry. We pioneered the use of model checking in a freshman’s course on operating systems and in a master class for high school students [M444].

Hybrid systems are systems that exhibit a combination of discrete and continuous behavior. Typical hybrid systems include computer components, which operate in discrete program steps, and real-world components, whose behavior over time intervals evolves according to physical constraints. Such systems can be very complex, and very difficult to describe and analyze. In close collaboration with the group of prof. Nancy Lynch at MIT and prof. Roberto Segala from the University of Verona, we developed the *timed and hybrid I/O automata* frameworks [M2, M22, M304]. These basic mathematical frameworks support description and analysis of timed and hybrid computer based systems. The TIOA and HIOA frameworks are widely used, amongst others, to analyze automated transportation systems, intelligent vehicle highway systems, air traffic control systems, automotive control systems, consumer electronics applications, and wireless ad hoc networks. Our paper [M2] on the HIOA framework has 328 cites in Google Scholar (June 2009). We wrote a monograph on the TIOA framework [M304]. A toolset supporting the framework, which includes embeddings of TIOA into PVS and Uppaal, is being developed by VeroModo Inc. A different line of hybrid systems research was followed by our PhD student Goran Frehse in his thesis on the hybrid automata model checker PHAVer [M209]. Experiments show that PHAVer computes faster and more accurately than other, comparable programs, such as the widely used HyTech tool from the University of Berkeley.

Nondeterminism is a key feature in models for concurrent and reactive systems. It allows us to express that often we do not know (or do not care) which events will occur or in which order certain events will occur. Randomization is similar but nevertheless distinctly different from nondeterminism, and plays an essential role in many distributed algorithms. *Probabilistic automata*, proposed by Segala in his PhD thesis from ’95, constitute a general modeling framework for systems that exhibit both nondeterministic and probabilistic behavior, such as distributed algorithms and network protocols. We established a number of fundamental results in this area. In [M29], we presented a simple and intuitive testing scenario for image finite probabilistic automata. This work received the EATCS Best Paper Award. A journal version of this paper was published

\(^1\)In 2007, E.M. Clarke, E.A. Emerson and J. Sifakis were awarded the ACM Turing Award for their roles in developing model checking into a highly effective verification technology, widely adopted in industry.
in JACM [M335]. For her contribution to this paper, Stoelinga received the 2008 Professor De Winter prize. In a SIAMCOMP paper [M342], we established that the simulation preorder is the coarsest refinement of the trace distribution preorder that is compositional for probabilistic automata. This result was the starting point for the PhD research of Ling Cheung, who proposed various restricted notions of schedulers for which trace inclusion is compositional, with applications to distributed algorithms and security protocols [M259, M258, M257, M213, M413, M155, M242]. In 2006, Cheung was awarded a PhD degree cum laude [M305].

In 2007, Dr. Jansen joined our group, bringing in considerable expertise on probabilistic model checking, an area where we see many important challenges [M470, M370, M253, M396]. Our work on probabilistic systems takes place in the context of the NWO-DFG bilateral cooperation projects VOSS1, VOSS2, and ROCKS and the EU FP7 project QUASIMODO.

Model-based testing. Systematic testing is important for software quality, but it is also error-prone, expensive, and time-consuming. Model-based testing (MBT) is a new technology that can improve the effectiveness and efficiency of the testing process. With MBT a system under test (SUT) is tested against a formal description, or model, of the SUT’s behaviour. Such a model serves as a precise and complete basis for the algorithmic generation of test cases, for defining coverage metrics, and for proving the validity (soundness and exhaustiveness) of tests. MBT is complementary to model-checking (verification): whereas model-checking is conducted on the level of models by verifying properties of these models, MBT is used to check the behaviour of real, executing implementations against these models. MBT research within MBSD ranges from fundamental theory and algorithms for test generation, via test tools, to their application for testing of (software) systems. Covering this whole spectrum allows us to validate new ideas on (realistic) case studies, and to rapidly obtain feedback leading, in turn, to new research questions.

Based on different modelling paradigms two approaches to MBT are pursued: the state-based and function-based approach. For the state-based approach there is a rich and well-understood theory for testing of reactive systems. This so-called $ioco$-test theory for labelled transition systems [M485] was developed by MBSD members together with the University of Twente, and forms now the underlying theory for several MBT tools such as TORX, TGV, STG, TESTGEN, UPPAL-TRON, and AGEDIS. Research is directed towards extending this theory with quantitative aspects such as real-time [M483] and data variables with large or infinite domains. For the latter the challenge is to find finite representations of these infinite domains, and to lift the test generation algorithms to these representations. This was achieved using symbolic transition systems [M159, M266], and the corresponding test generation were implemented in the test generation tools JAMBITION and TORXAKIS.

For the function-based approach algorithms to generate tests from formal models have been developed and implemented in the test tool Gast [M23]. In Gast, models can be specified in several ways. One can use a MBT language to specify properties of functions and instances of data types in first order logic [M176], or rather define the model as an extended state machine [M89]. In Gast the models themselves can be subject to testing [M473] and partial exploration by the test-engineer [M474]. The developed algorithms for generating test cases can be used for programming by example [M277, M399]. Gast is based entirely on the state-of-art generic programming techniques that we have developed and incorporated in the functional language Clean. Gast has been successfully used to test libraries of higher order functions (e.g. parser combinators [M223, M276]). Real-world applications of model-based testing are discussed in Section A.1.

Proof assistants. When one wants to formally reason about a model with a proof assistant such as PVS, Isabelle or COQ, one has to translate the model description to an equivalent description in the language of the proof tool and one has to incorporate the formal semantics of the modeling language into the proof tool as well. Formal reasoning then has to take place in a completely different world, which makes such systems very hard to use for non-specialists. We have developed the proof assistant Sparkle (PhD thesis Maarten de Mol, defended in March 2009). With Sparkle, the software engineer can apply formal reasoning steps on the code itself, instead of some sort of abstraction. The system has been created entirely within the functional language Clean.
B.3.2. STRATEGY AND POLICY

We have contributed to the theory for reasoning about lazy functional programming languages (see [M458]), for reasoning about strictness in the context in lazy languages (see [M295], [M389]), and for dealing with type classes [M100] (best student paper award). Sparkle has been used for proving properties of our GEC and iData system on (see below) which the iTask workflow system is based.

Extensions to Sparkle have been made at the Eötvös Loránd University in Budapest to enable reasoning about state. At Trinity College in Dublin it has been used to reason about I/O. At both sites the work with Sparkle resulted in a PhD Thesis.

In summary, our research on computer-aided verification and analysis and on model-based testing has been very successful, and we have been able to achieve significant impact with this research. These topics will remain amongst the most important strands of research of the MBSD section in the coming years.

T.2 Probabilistic graphical models

Model-based reasoning is an area in artificial intelligence (AI) where there is an emphasis on symbolic, qualitative representation of models of systems and on reasoning with the models in order to solve problems. The European Network of Excellence on Model-based Systems and Qualitative Reasoning MONET (monet.aber.ac.uk), in which we were involved, had the aim of stimulating such research and to bridge the gap between academic research and fields of application [M246]. Dr. Lucas was a member of the executive board of MONET and was also co-leading its Biomedical Task Group. Typical examples of qualitative models are the causal models used in model-based diagnosis in AI, where a diagnosis of failure of a system can be determined by abductive reasoning, thus explaining a given set of observations using cause-effect relationships. Model-based reasoning methods also allow incorporating quantitative detail if necessary and when available. In our model-based reasoning research, we aim at merging qualitative knowledge with uncertainty, taking probabilistic graphical models as a start. Probabilistic graphical models, and in particular Bayesian networks, are powerful probabilistic representations that have become increasingly popular since the publication of Judea Pearl’s book “Probabilistic Reasoning in Intelligent Systems” [M520].

We often bring probabilistic graphical models in connection with other methods, e.g. from logic (see below), constraint satisfaction [M10], explanation [M442], and learning [M107]. The recognition of our research by the international community is reflected by the fact that dr. Lucas chaired the biennial European Workshop on Probabilistic Graphical Models in 2004 ([M109]), and co-edited a book on advances in probabilistic graphical models [M404].

Normally in our research, we adopt an approach where development of theory goes hand in hand with modeling and system development, in particular in the medical domain (See Section A.3). In the OCTOPUS project, which aims at the development of methods for printer adaptivity in a joint effort with the Embedded Systems Institute, Océ, and a number of other academic partners, a similar approach is being pursued, however in an industrial rather than in a medical setting.

Another research strand in probabilistic graphical models is the exploitation of simplified ways of specifying discrete probability tables in Bayesian networks. The motivation underlying this research derives from the fact that in many situations detailed numerical information about real-life processes is difficult, and sometimes impossible, to obtain, whereas it is much easier to acquire information about how variables influence each other qualitatively. In particular, we have done a considerable amount of research on the development of a theory of causal independence in which probability tables can be specified using Boolean functions. This research resulted in publications presented at ECAI-2004 [M88] and ECSQARU-2005 [M192], and extended journal papers on this work were published in the AI journal [M146], the International Journal of Approximate Reasoning [M449], and the Knowledge-based Systems journal [M145]. Furthermore, some work was done on the semantics of dynamic Bayesian networks and presented at ECSQARU-2007 [M360].

In some of the research we either draw inspiration from logical reasoning to develop probabilistic analogues, or merge the two languages in one way or other. A typical example is our work
on the concept of conflict-based diagnosis, that was inspired by existing work on consistency-based reasoning by Johan de Kleer at Xerox in Palo Alto [M517, M518], the dominant theory of model-based diagnosis for more than two decades, where logical consistency checking was replaced by a probabilistic match measure, called the conflict measure. This allowed us to develop a theory similar to consistency-based diagnosis, yet more flexible, which was presented at IJCAI-2007 [M361]. Finally, we started a new line of research on probabilistic logics in 2008 with the development of a logic inspired by earlier work of David Poole on probabilistic Horn logic and that generalizes chain graph. We received the best paper award at BNAIC’08 [M460] for this work and an extended version of the paper was presented at ECML/PKDD 2009. In the next few years we wish to continue this line of research; the main goal is to design probabilistic logics that are computational, useful in the context of applications, and in which logical and probabilistic reasoning go hand in hand.

T.3 Model-based application generation

The holy grail we are looking for is the ability to generate a complete working system fully automatically from a model, with the aim of reducing software development time and increasing system reliability. This is clearly very hard to accomplish in general, but for specific problem areas it should be possible. Ideally one wishes to specify a system at a level of abstraction that is easily understood by domain specialists. For this purpose it is probably best to use a domain specific language. To cope with the intricacies of an actual system, a lot of detailed technical information needs to be supplied. The underlying modeling language must, therefore, possess powerful abstraction mechanisms enabling to abstract from low level details. For this reason we believe it is better to embed the modeling language in an advanced general purpose programming language. This also makes it commonly much easier to extend the modeling language with new constructs.

Functional languages are well known for their high expressive power. Recently, they have received renewed attention, not only at universities (functional programming has become part of the new ACM curriculum), but also in industry: Microsoft Research at Cambridge, UK, develops both Haskell and F#. The latter now even has become an official commercially supported Microsoft language. Due to their mathematical basis, high expressive power, and sophisticated type systems, functional languages are well suited to model complex problem domains. A modeling language that is embedded in a functional language inherits the expressive power of the functional host language for free. For over two decades, Nijmegen has maintained a leading role in the development of efficient functional programming languages, which has resulted in the freely available, state-of-art, pure, lazy functional programming language Clean (clean.cs.ru.nl). We have developed tooling, in particular the systems Gast and Sparkle mentioned in Section T.1, for formal reasoning about Clean applications, and hence also of models defined in Clean.

To make functional languages better suited for being used as embedded modeling language, we have contributed to the innovations mentioned below. This work was partly sponsored by the STW project NWI177.4411 “A software development environment for intrinsically safe distributed systems”, a collaboration with Thales, ABN-AMRO, NLR, Philips Research Laboratories, Rijkswaterstaat and KLM. Industrial support came from Decis labs, InterNL-net and the Royal Dutch Navy.

Our research is leading in showing how generic (i.e. type driven) programming [M208] can be used for producing real systems or parts of real systems. We have used the technique successfully to generate tests for our test system Gast [M23]; to automate important parts of a compiler [M196]; to enable interfacing with legacy database systems [M476]; to generate efficient persistent storage and retrieval of arbitrary (recursive) data structures [M484]; to generate and handle interactive desktop GUI applications [M6, M68, M106, M67]; to generate and handle interactive web applications (iData library); to generate and handle multi-user web-enabled workflow systems (iTasks combinator library), and to generate functions for programming by example [M176], [M399].

We have developed a hybrid type system for Clean: statically typed values (data as well as functions) can be turned into dynamically typed values (“Dynamics”) and vice versa. This can be
done in a very flexible way by using type pattern variables which enable dynamic type unification of Dynamics. Dynamics are fundamental to many applications, such as type safe data and code exchange between independently developed applications, inside the iTask workflow system, and to build a type safe operating system (see PhD Thesis van Weelden [M408] and [M37] which received the Peter Landin award). Clean’s well-known uniqueness type system allows to handle side-effects in a pure functional language.

In collaboration with the Trinity College Dublin (PhD Thesis by de Vries (2008)) an improved uniqueness type system has been designed [M357, M394]. The typing rules have become easier while at the same time the new system can deal with type constructs such as Rank-n types and Generalized Algebraic Data Types (GADT’s). The system has been implemented in Microsoft’s experimental language Morrow by Daan Leijen at Microsoft Research.

The group has continued its work on compiler technology. The Clean compiler is well-known for the quality of the code that it generates. It scores very high in the international Computer Language Benchmark shootout in which 33 programming languages are being compared. When also the expressiveness of languages is taken into account, Clean even scores best. See:

http://shootout.alioth.debian.org/

We have also initiated a project to merge Clean and Haskell within one unified compiler. With this compiler, the sources of the two language communities can be integrated seamlessly.

Our research strategy in the review period has been to move from functional programming as the main research area, to using functional and generic programming as enabling technologies for the model-based generation of applications. This research transition has been successful and smoothly.

T.4 Conceptual modeling

Traditionally, the field of computer science has a strong focus on formal aspects of models and modeling techniques. As a result, there is a tendency to relate the quality of models exclusively to their formal properties. Members working on the “conceptual modeling” theme have a tradition in research on the formal aspects of modeling languages for information systems [M519, M169, M182, M183, M292, M402, M486], as well as the fundamental principles underlying their operations [M345, M343, M346, M351, M447]. Inspired by practical experiences [M504, M516, M72], however, including the personal experience of some of our members when working outside academia, we have gradually become aware that there is much more to the quality of a model than its formal properties, making it more of a relative notion depending on the needs at hand. Why is the model needed? Should it serve as a base for analysis, and for which audience? Even more, the situation in which actual modeling is to take place has a huge impact on how practical it is to achieve the quality ambitions [M184]. How much time and money is available to produce the model? Do we have access to the right informants and stakeholders? Since 2003 a number of results have been produced exploring several aspects of these intriguing questions that are at the base of successful and effective modelling, and therefore pivotal to the applicability of the results of the MBSD group [M21, M65, M184, M200, M200, M202, M201, M143, M144, M387, M172, M93, M499].

In relation to the above issues, a number of international researchers, mostly from the fields of Information Systems and Enterprise Engineering, has recently been pushing towards a shift in focus from language-oriented foundations of modeling to issues of operationalization of methods and techniques (leading to e.g. working conferences such as Practice of Enterprise Modelling (PoEM), and Practice-driven Research on Enterprise Transformation (NAF-Academy – PRET), and workshops such as Trends in Enterprise Architecture Research (TEAR), and Enterprise Modelling and Information Systems Architectures (EMISA). This requires a partial shift in research methodology, and creates opportunities for new interdisciplinary connections with established fields like operations research, human-computer interaction, intervention methodology, decision making, problem solving, and so on. The primary research paradigm for our research is design science. Design
science includes not just systems design, but also method design. In addition, we look at operational methods for enterprise modeling as interactive systems. The shift in focus discussed above requires us to explore research methods relatively new to the field. In this respect, we have been able to make contributions in developing new viewpoints on operational modeling and related research methods [M170, M468, M86, M168, M467, M285, M286]. This development is still in full swing, but has already led to the creation of a new international research community, with collaborations, events, and book series of its own (such as the enterprise engineering series of Springer). To be able to gather empirical data underpinning our theoretical work it is crucial to invest in a long term application domain. We have selected to focus our empirical efforts on the design and evolution of enterprises, referred to as Enterprise Engineering. Our involvement in these developments is evident from the new book series on Enterprise Engineering, published by Springer, of which prof. Proper is joint editor-in-chief.

In practice, models are not created by people in isolation, but rather in the context of groups of people [M482, M467, M371, M372]. The creation of models often involves a collaborative process in which different actors will play a role, where each actor will bring their own stakes, goals and abilities to the table. What happens when people create models? What cognitive and interactive processes are at play? How can a shared understanding, agreement and commitment be warranted? Here we also study how people model in reality, before adding interventions aimed to improve their effectiveness.

Our longer term strategy is to first capture the attention of advanced practitioners and then, through dialogue and empirical testing of theory-based methods and techniques, increase the academic depth of the field.

B.3.2.5 Application Areas

As mentioned earlier, MBSD’s fundamental research is carried out in connection with various areas of application (top row of Figure B.3.1) adopting the philosophy of the practice-as-laboratory approach, as schematically illustrated by Figure B.3.2.

A.1 Embedded and distributed systems

In order to validate the effectiveness of our basic technologies and to get inspiration for further research, we apply them to challenging industrial applications. Embedded systems constitute a natural application area for the technologies developed within our group, in particular for computer-aided verification and analysis. Crucial for our work in this area is the collaboration with the Embedded Systems Institute (ESI), a research organization founded in 2002 by the three Dutch technological universities and a number of companies. Recall that two members of our group, Hooman and Tretmans work four days per week as research fellow at ESI and one day per week at our institute. ESI acts as coordinator of research projects in embedded systems in which industry and universities collaborate following an industry-as-laboratory approach.

Our group participates (or has participated) in three of these projects (Boderc, Octopus and Tangram). Another rich source of case studies are some European projects (VHS, OMEGA, AMETIST, QUASIMODO) in which our group is (or has been) involved. Within these projects the industrial partners provided challenging problems for us to work on. Finally, we have informal contacts and ad-hoc research collaborations with a large number of companies, for instance through Master’s Thesis projects.

Co-simulation. Within the Boderc project, we extended an existing formal semantic framework for discrete event models to allow for consistent co-simulation of continuous time models from within this framework. The level of confidence in the design can now be raised in the very early stages of the system design life-cycle instead of postponing system-level design issues until the integration and test phase is reached. We demonstrate the extended semantic framework by co-simulation of VDM++ and bond-graph models for the embedded control of a printer paper path, and the level control of a water tank [M333, M391, M298, M392, M352]. Océ expressed great
satisfaction with the results of the Boderc project: it brought them both useful, specific results and promising general directions. For example, Orbons states that the “Happy flow” modeling approach from Boderc has enabled Océ to skip a complete physical machine-build iteration cycle, saving many man-years of effort”. Verhoef states that Chess has explicitly implemented the innovative processes from Boderc in their business model [M333].

**Performance evaluation of embedded architectures.** Another contribution to the Boderc project has been the development of techniques to model and evaluate the performance of embedded system architectures. In joint work with the group of prof. Lothar Thiele at ETH Zurich, a number of state-of-the-art performance evaluation methods and tools were put to test on a simple case study that has been inspired by industrial practice [M269, M250]. This was the first time that such a quantitative comparison was performed on a single case study at this scale. As the only tool, Uppaal was able to compute the exact best and worst case execution times, with as a price that Uppaal does not scale so well. Our work on comparing performance models was continued with a significantly larger scope involving more case studies and additional tools by subsequent work at ETH Zurich.

**Combining formal methods and UML.** To connect formal approaches to industrial practice, the combination of formal methods and UML has been studied in EU-IST project Omega (Correct Development of Real-Time Embedded systems in UML). A formal semantics of a UML kernel has been defined in PVS and the verification of UML models by means of PVS has been studied. A part of the MARS system (Medium Altitude Reconnaissance System) from the NLR (National Aerospace Laboratory) has been selected as a common real-time embedded application within the OMEGA project. This industrial case study has been used to illustrate interactive verification supported by the PVS theorem prover. In addition, a comparison has been made with other techniques applied that have been applied to the MARS case study, such as Live Sequence Charts, the UVE tool for model checking of functional properties, and the IFx tool for timed model checking [M70, M79, M177, M279, M446].

---

**Figure B.3.2: The practice-as-laboratory approach.**
Analysis and synthesis of controllers. We have applied timed/hybrid automata in a number of case studies on analysis and synthesis of controllers:

- Deadlock avoidance and throughput optimization for a wafer scanner from ASML (2004). Using the SMV model checker, we synthesized a deadlock avoidance policy for a new EUV wafer scanner from ASML, and using Uppaal we optimized the throughput of this machine [M244]. Our results are referred to in patent application ASML ref. P-1784.010.

- We defined a formal model of the real-time service allocation unit for a Car Periphery Supervision (CPS) system proposed by Robert Bosch GmbH, and verified some safety properties using Uppaal [M15, M77].

- We modeled and analyzed the behavior of a simple Lego car with caterpillar treads using the hybrid I/O automata framework [M14].

- Using the Cadence SMV model checker we synthesized a scheduler for the smart card personalization system, a case study that has been proposed by Cybernetix [M78]. The controller that we synthesized automatically was previously patented by Cybernetix.

Scheduling related problems. Scheduling and resource allocation problems occur in many different domains. Typically, in each of these domains problems are solved using different approaches and mathematical tools. The EU IST AMETIST project, that we coordinated, has provided the foundations for a unifying framework for time-dependent behavior and dynamic resource allocation that crosses the boundaries of application domains. AMETIST has shown that modeling approach that underlies the successful domain of formal verification and timed automata model checking, can be extended to resource allocation, scheduling and other time-related problems. We have successfully applied this approach in the design of the datapath of printers/copiers at Océ [M469] and for scheduling of lacquer production [M152, M151] (for this last case study, our model checking technology outperformed the tools of Axxom Software AG, a company that specializes in value chain management).

Model-based testing. Model-based testing was an important aspect of the project TANGRAM, which was a joint research and development effort of a couple of universities and companies, coordinated by the Embedded Systems Institute, in which ASML is the core industrial partner [M403, M406, M401].

GAST has been applied successfully in practice in situations ranging from computational modules of insurance companies and pension firms (together with the University of Groningen [M314]), election software (as part of a LaQuSo project), and a smart-card [M376]. Model-based testing was also applied to situations such as an electronic purse on a JavaCard [M195]. TorXakis (see above section on model-based testing, Section T.1) has been used successfully for testing of the new Dutch electronic passport. This work was commissioned by the Ministry of Internal Affairs and it was performed in close collaboration with the section DS of iCIS. We also applied model-based testing to web-applications constructed by the iData toolkit [M323]. Also this test setup appears to be a very effective way to spot non-conformance issues. In all tested systems new issues were found by model-based testing. In collaboration with CNR/ISTI Pisa JAMBITION was successfully used for testing of web services [M455].

Distributed algorithms and protocols. We have used (extensions of) model-checkers and interactive theorem provers for the verification of complex real-time and fault-tolerant distributed algorithms and protocols [M9, M268, M410, M421, M256, M384, M385, M456, M356, M341, M248, M161, M163, M261, M12, M507]. Case studies are provided by industrial partners in projects, organizations such as NLnetsLabs, or just taken from the literature. Our goal is to push forward the range of applicability of formal methods. As a tangible result of our analysis efforts, we discovered many errors and ambiguities in industrial communication protocols, and thus helped to improve the quality of these protocols (see e.g. [M268, M410, M421, M256]). Tool support is mainly obtained by the use of interactive theorem provers (such as PVS, Isabelle/HOL, Sparkle, and ACL2),
and model checkers (such as Uppaal, Murphi, NuSMV, Spin and PRISM). We take a pragmatic approach and use whichever tools that are most suited to do the analysis. Frequently, we benefit from using combinations of theorem provers and model checkers (see e.g. [M384, M341, M248]. Using state-of-the-art model checking and theorem proving technology, we regularly manage to analyze protocols which, just a few years before, would have been far too complex for formal analysis. Several case studies that we carried out have become standard benchmarks in the verification literature with more than 70 citations in Google Scholar.

A.2 Enterprises

**Enterprise engineering.** Enterprise Engineering (EE) is an emerging discipline which aims to deal with the challenges (agility, adaptability, etc.) and the opportunities (new markets, new technologies, etc.) faced by contemporary enterprises, including commercial, nonprofit and governmental institutions. The field is based on the paradigm that such enterprises are purposefully designed systems, and thus they can be redesigned in a systematic and controlled way. Enterprise engineering projects typically involve architecture, design, and implementation aspects. Indicative of the growing maturity of the young field of EE, Springer Verlag has recently initiated a book series dedicated to this theme. To us, the domain of EE is an interesting and fertile context in which to study and evaluate our fundamental research on conceptual modeling. Results include [M337, M219, M386, M292, M377, M28, M488].

The discipline of Enterprise Engineering combines relevant parts from the organizational sciences and the information systems sciences; the aim is to develop theories and methodologies for the analysis, design, and implementation of future enterprises. Two crucial concepts have emerged that are considered paramount for accomplishing this mission: **enterprise ontologies** and **enterprise architecture**. A precondition for incorporating these methodologies effectively in an enterprise is a well established practice of enterprise governance.

Practical relevance of our research may be our main reason for getting close to industry, but admittedly we also seek interaction with industry to create more leverage towards obtaining funding. Current enterprise engineering practice provides numerous challenges that are heartfelt in practice. By using these challenges to prioritize our research agenda, we are able to create an intimate and sustainable relationship with industry. The intimate relationship with industry serves as a base for funded projects: large ones (like ArchiMate), but also smaller projects such as individual PhD projects.

Key in building the relationship with industry are our adjunct professors, but also our participation in the Netherlands Architecture Forum (NAF), an organisation bringing together client organizations, consultancy firms and universities. Our group was one of the co-initiators of NAF, and has been one of the most active academic participants since it started.

We already mentioned the co-initiation of the Netherlands Architecture Forum, which is a key national (Dutch) instrument for enabling practical impact. Internationally, however, our biggest impact so far has been achieved by means of the ArchiMate Project [M21, M59, M206], which has also been an accelerator for our work on conceptual modeling. Many of the results of this project have found their way to industry. Most important is the ArchiMate language, which has now been accepted by The Open Group as their preferred language for architectural descriptions to be used in conjunction with their TOGAF architecture method. Currently, ArchiMate is in use by over 200 organisations ([www.archimate.org](http://www.archimate.org)).

Another aspect of enterprises is regulation of business behaviour and transformation processes. The work in the field of “business rules” aimed at restricting/regulating the operational behaviour of business processes. Within this field, our group has been able to leverage past theoretical results and transfer some of these insights into the practical domain, for example by contributions to the NAF working group on Business Rules, as well as advisory roles towards various industrial partners. With regards to the restricting/guiding operational behaviour through architecture, the theoretical insights from our group have found their way into numerous publications and presentations of NAF and many other academic and industrial audiences.

EE provides regulations which enable key decision makers to govern the transformation of
CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT

(Their) enterprise. The transfer of insights in this area have led to prof. Proper’s membership of the advisory board of Ordina’s GEA project [M434, M436, M435, M437, M438, M439, M440], as well as the part-time PhD project of Roel Wagter, a leading architect at Ordina. In addition, Mark Paauwe (Paauwe & Partners) is doing a part-time PhD project on a related topic. Furthermore, we provided extensive input on xAF (Extendable Architecture Framework) workgroup, which produced a NAF-sponsored book, and initiated and still chair the NAF Principles workgroup, now also working towards a book.

Workflow management systems. A category of challenging industrial applications is formed by Workflow Management Systems (WFMS). WFMSs are automated systems which coordinate tasks that have to be executed by human workers and computers. This project has been initiated by industrial WFMS users who are also aware of the expressive power of modern day functional programming languages, and Clean in particular. Our work on workflow systems is partly being financed by STW. We collaborate among others with the Technical University Eindhoven (prof. van der Aalst) and Pallas-Athena, a manufacturer of commercial WFMS, such as FLOWer. Furthermore we collaborate and are financed by the Royal Dutch Navy. The main goal of this project is to breed an innovative kind of WFMS, in which key properties of modern functional languages such as demand driven evaluation, strong typing, algebraic and recursive types, higher-order functions and tasks, and data centric behavior are integrated with workflow concepts. It is also an excellent example of model-based system development because we aim to generate a complete WFMS from its model.

There are many interesting problems to solve: workflow systems coordinate work of possibly many people that work together distributively, the tasks to do have to be presented in an understandable way and have to be handled interactively, one has to therefore create and maintain a distributed system, data being manipulated has to be stored persistently, but one also has to remember which tasks are being processed by whom, one has to interface with existing databases and applications, one has to take into account that organizations and the way people work is changing over time, and so on. Hence, to generate a full fledged workflow management system from a high level workflow specification is quite a challenge, but we believe it is doable. Many of the basic techniques that have been described in Section T.3 can be deployed, and it is likely that many new techniques will be produced as a result of this project. However, it will clearly take some years before we have solved all problems. Nevertheless, we have made significant contributions: we have studied the generation of Graphical User Interfaces from models intensively ([M6, M106, M67, M68] for desktop GUIs and [M283, M284, M327] for web GUIs). We have used our tools Gast and Sparkle to analyze these systems [M323, M511]. Based on this work, we have constructed a first version of demand driven workflow system, the iTask system [M382, M400] and extended it to a full fledged web enabled system [M481]. The iTask approach is different from traditional workflow approaches because workflows are dynamically constructed and may depend on the result of previous work. Recently, our data centric workflow approach is getting more and more attention in the workflow community internationally. Financed by the Dutch Navy we are investigating the applicability of the iTask system for complex logistic situations (such as international missions) and very dynamic situations (e.g. crisis management) [M496].

A.3 Medical decision support

Medicine and health care are challenging application areas for model-based system development. It is the main area of our model-based reasoning research, with a focus on the use of probabilistic graphical models and logics. There are two research strands. The first research strand focuses on clinical guidelines, and checking the quality of clinical guidelines using logical methods, in particular theorem proving and model checking techniques. This research has relationships with our research on workflow management and distributed algorithms and protocols mentioned above. Although clinical guidelines are used to support making clinical decisions, our primary research goal here is to scrutinize these guidelines using formal methods. The second research strand revolves around the development of models that can be used as part of clinical decision support
systems. Each of these research strands is described in more detail below.

**Quality checking of clinical guidelines.** Clinical guidelines are structured documents that are aimed at assisting medical practitioners and patients in making decisions about appropriate health care for specific clinical conditions. Clearly, it is unacceptable if clinical guidelines contain flaws, and detecting such flaws using computer-aided tools is thus appealing. In particular in the context of the European projects Protocure I and II much of our research on detecting flaws in clinical guidelines was done. The premise of both projects was that clinical guidelines can be looked on as program-like representations and that their development has some similarity to software development. There are good reasons for this insight, as a major part of a guideline consists of descriptions of actions that need to be executed conditionally, in parallel, sequentially or repeatedly, often under particular timing constraints. A variety of computer-based guideline representation languages, such as ProForma, Asbru and GLIF, have been shown to be able to capture essential aspects of such guideline knowledge.

Some special methods and techniques have been developed by us to be able to check the quality of a clinical guideline using formal methods, most of them based on temporal logics. The specific techniques varied from abductive reasoning using methods from logic programming and automated reasoning (e.g. [M445]), interactive formal verification, for which we used tools such as KIV (e.g. [M340]), and model checking, for which Cadence SMV was used (e.g. [M367]). In addition, we have done some work on special purpose temporal logics in order to be able to model task execution in accordance to the semantics of clinical guidelines [M465]. Furthermore, methods to represent and reason about clinical guidelines were developed, mostly with the Asbru representation language used as the target language. Two real clinical guidelines (treatment of breast cancer and diabetes mellitus) were verified as part of case studies, and a number of different errors were discovered. Note that this line of research explores the basic technology of computer-aided verification and analysis and is, in fact, a somewhat unusual application of this technology. The nature of the medical domain, however, also required the development of modeling methods that were special, such as for representing and reasoning with causal knowledge [M26]. One PhD thesis was completed successfully in this project [M509].

**Medical decision making.** This line of the research is concerned with model development for medical decision support systems using probabilistic graphical models, in particular Bayesian networks, as the main technology. Funded projects in which such research was undertaken in the review period and within the medical domain were TimeBayes, ProBayes (both funded by NWO/EW), and B-Screen (BRICKS/FOCUS).

In the TimeBayes project, various techniques in Bayesian networks were explored, in particular ways to deal with temporal evolution using temporal and dynamic Bayesian networks (e.g. [M260, M393]) and methods for the compact specification of probability tables (e.g. [M197]). The main clinical problem domain in which the developed methods were explored was the diagnosis of ventilator-associated pneumonia in ICU patients, and the selection of appropriate antibiotic treatment for this disease.

The ProBayes project focused on the development of prognostic probabilistic models, where in particular dynamic Bayesian networks have been explored as a method to obtain more detailed information about the evolution of the disease than obtained by standard statistical methods, such as Cox’s regression [M450, M348, M360]. The usefulness of causal independence modeling was also studied in the project [M349].

A strong point of our research is that we were able to establish a close collaboration with healthcare professionals, both clinical and in the area of guideline development (CBO, www.cbo.nl). As a consequence, we have also been successful in publishing research results in purely medical journals, a somewhat uncommon achievement of computer scientists (e.g. [M147, M344, M451, M452]). Dr. Lucas supervised four PhD students within the TimeBayes and ProBayes projects, whom during the review period completed their PhD theses [M53, M407, M515, M508].

B-Screen is a collaborative project with the Department of Radiology of the St Radboud Medical Center Nijmegen, in which we investigate ways to improve the interpretation of breast
images, so-called mammograms, using probabilistic methods. Current computer-aided analysis methods interpret each mammogram separately, the so-called single-view interpretation. However, the interpreting radiologists consider the images jointly, as they are related to each other in terms of, for example, density. Analyzing mammograms in a correlated manner is called multiview interpretation. Much of our research centers around exploiting probabilistic graphical models for such multiview interpretation of mammograms. We have successfully used causal independence models to merge information obtained from multiple mammograms of the same patient [M489, M490].

With the now widespread introduction of information technology in health care – a gradual, but inevitable process –, and in particular the deployment of electronic patient record systems in the care flow, it is expected that the line of research on medical decision support systems may have major impact. The expertise in this area which has accrued over the years, places us into the right position to contribute to these developments in the future.

B.3.2.6 Creation of Research Synergy

As the researchers of the MBSD section cover expertise in a broad range of topics in model-based system development, we are actively pursuing ways to combine this expertise in particular research. At the same time we use this research across subthemes to increase both the synergy in the section as well as the focus of our research, as mentioned at the end of Section B.3.2.2.

Examples of combined work are the following:

1. Dr. Lucas and prof. Vaandrager are jointly involved in the ESI project OCTOPUS. The OCTOPUS project addresses the issue of system adaptability in the setting of digital document printers from Océ, i.e. the ability of a system to adapt itself to fluctuations in the environment, the use of the product, etc. Within this project, the expertise of Lucas on model-based diagnosis and probabilistic graphical models is complemented by the expertise of Vaandrager on model checking and real-time systems.

2. Work on model-based analysis of software and protocols using semi-automatic verification methods and model checking by Vaandrager and others is strongly related to work on quality checking of clinical guidelines done using similar technology by Lucas.

3. Dr. Hoppenbrouwers and Lucas have started exploring the links between enterprise modeling and knowledge modeling as using in AI. In particular, they are addressing recent ideas from argumentation theory and games for knowledge elicitation from domain experts without skills in formal modeling. This has already led to a publication at the British AISB Convention 2009.

4. Joint work involving prof. Plasmeijer and dr. Lucas on exploring workflow management systems, in particular the iTask environment, in medical decision support has recently been initiated with the appointment of a joint PhD student (Bas Lijnse).

5. Prof. Plasmeijer and dr. Hoppenbrouwer collaborate on exploring ideas from the fields of conceptual modeling and model-based application generation, where the basic idea is that conceptual models act as specification for the automatic generation of software.

6. Prof. Proper and prof. Vaandrager are jointly involved in a project proposal on dynamic cooperative traffic and travel management. Here the expertise of Proper on architectures is complemented by the expertise of Vaandrager on embedded systems.

7. There are close links between the work on software testing by dr. Tretmans and dr. Koopman ([M23, M195]).

Research topics 1, 2, 6, and 7 are investigated within the focus on model-based verification, analysis and testing. Research topics 1, 2, 3, and 4 are part of the focus on model-based methods for
building (medical) decision-support systems. Finally, model-based application generation is investigated in topic 4, 5, and 7. Note the deliberate overlap, which means that a topic is approached using different basic techniques. For example, to build a decision-support system that is able to suggest particular actions in a particular order dependent on user input, it is our plan to use the iTask environment to generate the software.

B.3.3 Processes in Research, Internal and External Collaboration

Processes in Research

As mentioned at the beginning of this chapter, the research within MBSD is organized around four closely interacting subthemes. The PIs play an important role in initiating discussions within the section on whether or not the research direction is still appropriate, whether or not particular new initiatives should be explored, and in coordinating collaboration between subthemes. Maintaining links with the application areas is also organized around the subthemes. The computer-aided verification and analysis subtheme has the strongest links with industry, the probabilistic graphical models subtheme with health care, the model-based application generation subtheme with the public sector, and the conceptual modeling subtheme with business and the financial sector.

Section members are free to select any research topic within the MBSD program; however, collaboration with other members in the section, and for some topics also across sections, is encouraged.

Internal Collaboration

Within iCIS there are collaborations with the DS section in the area of functional programming and through LaQuSo projects. Quality of software and the use of formal verification methods and tools is an area where researchers from the DS and IS sections are also working on, although often from a somewhat different viewpoint. Through interaction with members of the other sections, we try to profit from expertise available in this area in iCIS.

External Collaboration

In the area of computer-aided verification and analysis, we collaborate with a large number of colleagues within national and international projects (see below). In addition, we have a close collaboration with, amongst others, MIT (prof. Lynch), the University of Verona (prof. Segala), CNR in Pisa (dr Bertolino), INPG Grenoble (Dominique Borrione and Amr Helmy and Laurence Pierre), and IRISA Rennes (Thierry Jéron, Vlad Rusu).

In the area of model-based application there is collaboration with the University of Dublin, Eötvös Loránd University (Budapest), University of Utrecht, University of Eindhoven, Defence Academy (Den Helder).

Several of the PhD students within the MBSD department originate from a collaboration between our University, The University of Groningen and Makerere University in Kampala, Uganda. Collaboration also exists with the Tilburg University on the field of modelling in an e-commerce context and enterprise architecture. Furthermore, the collaboration with the Telematica Instituut, which started during the ArchiMate project, is still continuing. In addition, several part-time PhD students are involved in our research. E.g. from Capgemini and e-Office.

Research in probabilistic graphical models and medical decision support is driven by contacts with clinical researchers from a number of academic hospitals (Nijmegen and Utrecht) and the Netherlands Cancer Institute. This involves different departments, such as radiology, obstetrics and gynecology, internal medicine, infectious diseases and oncology. Furthermore, we have a joint project with the Technical University of Madrid (prof.dr. C. Bielza) on probabilistic graphical models.
The details of external collaboration are in many cases dictated by the content of the actual project we are involved with:

- **ATOMYSTE (2002–2006):** Atom Splitting in Embedded Systems testing, STW PROGRESS project TES.5417, together with the University of Twente.

- **STRESS (2003–2008):** Systematic Testing of Realtime Embedded Software Systems, NWO 612.064.207, together with the University of Twente.

- **AMETIST (2002–2005):** University of Aalborg, University of Dortmund, University of Twente, Verimag, Weizmann Institute, LIF Marseille, Bosch, Cybernetix, Axxom, Terma.

- **Nuffic (2003–2010) training of Ugandese PhD students:** joint project with the Universities of Groningen and Eindhoven.

- **QUASIMODO (2008-2011):** Embedded Systems Institute, University of Twente, University of Aalborg, CNRS, Free University of Brussels, Terma, Chess, Hydac.

- **Protocure II (2003–2007; Improving Medical Protocols by Formal Methods) project.** This was an IST/Strep Open Domain EU project with researchers involved from Spain, Germany and Austria.


- **BODERC (2002-2007):** Océ, Intech, Chess, the Embedded System Institute, and the technical universities of Twente and Eindhoven.

- **TANGRAM (2003–2007):** funded by the Netherlands Ministry of Economic Affairs under the SenterNovem TS program; partners: Embedded Systems Institute, ASML, TNO, and the technical universities of Delft, Twente, and Eindhoven.

- **TAROT, Training And Research On Testing (2004–2008):** EU FP6 Marie Curie research training network.

- **OCTOPUS (2008–2012):** BRICKS project with partners from Océ, the Embedded System Institute, and the technical universities of Delft, Twente, and Eindhoven.

- **ArchiMate (2003–2006):** ArchiMate project consisted of a broad consortium from industry and academia. ArchiMate’s business partners were ABN AMRO, Stichting Pensioenfonds ABP, and the Dutch Tax and Customs Administration (Belastingdienst); in addition to members from our group, other academic partners were Telematica Instituut, Ordina, Centrum voor Wiskunde en Informatica (CWI), the Leiden Institute for Advanced Computer Science (LIACS).

- **HaaST (1999-2004):** Philips Research Laboratories and the University of Twente.

- **ProBayes (2003–2008):** an NWO/EW project involving clinical researchers from the Netherlands Cancer Institute (NKI) in Amsterdam.

- **TimeBayes (2003–2008):** NWO/TOKEN-2000 involving clinical researchers from the Department of Infectious Disease from Utrecht University Medical Center, and with computer scientists from the Institute for Information and Computing Science at Utrecht University.

- **B-Screen (2006–2009):** NWO FOCUS project in collaboration with the Department of Radiology of St Radboud University Medical Center, Nijmegen, and with Preventicon in Utrecht.

- **MONET European Network of Excellence on Model-based Systems and Qualitative Reasoning (IST-33540),** from 2002 to 2006 involved partners were from Wales, Scotland, Italy, France, and Germany.
B.3.4 Academic Reputation

Prof. Vaandrager is well known for his work on formal methods for real-time and distributed systems. Editor of the journals *Information and Computation* and *Logical Methods in Computer Science*. PC member of many top conferences in his field, e.g., ICALP, CAV, CONCUR, TACAS, EMSOFT, and FORMATS (PC co-chair 2009). Recipient of best paper award at ICALP’03. Reviewer of e.g. DFG Research Center AVACS and EU IST project COMBEST. Involved in many national and international research projects, in particular as coordinator of the EU IST project AMETIST. Represents the area of Computer Science within the Board of the Physical Sciences division of the Netherlands Organisation for Scientific Research (NWO).

Prof. Hooman is internationally known for his work on the application of theorem proving to distributed real-time and fault-tolerant systems. In the context of the EU project Omega, he coordinated the application and evaluation of formal methods from different European institutes to an industrial system modelled in UML. Research in several industry-as-lab projects on reliability and performance, resulted in publications on model-based awareness and co-simulation. He is a frequent reviewer of several international journals and funding institutions such as NWO, STW, ITEA, Austrian Science Fund (FWF), and the Australian Research Council. He was a member of the Artist Network of Excellence on Embedded Systems Design, Cluster Execution Platforms, and the NWO Veni committee concerning grants for young excellent researchers.

Dr. Tretmans is well-known for his fundamental and applied work on model-based testing. In addition, he has worked on the academic-industrial transfer of formal methods, verification, and (model-based) testing technology. Currently, he combines a part-time associate professorship at the Radboud University Nijmegen with an appointment as research fellow at the Embedded Systems Institute in Eindhoven. Dr. Tretmans is PC member of a couple of conferences and workshops in the area of (model-based) testing and software quality, such as IFIP TESTCOM/FATES (founder of FATES, steering committee, PC co-chair in 2007), IEEE Int. Symp. on Software Reliability Engineering ISSRE, ACM Symposium on Applied Computing, IEEE Int. Conf. on Software Testing, Verification and Validation ICST, Advances in Model Based Testing A-MOST, Workshop on Model-Based Testing MBT, and Software Quality Assurance SOQUA. Dr. Tretmans was involved in many national and international research projects (EU FP7, EU Marie Curie, NWO, STW, BSIK, directly with industry).

Dr. Lucas is well known for his work on model-based reasoning, Bayesian networks and medical decision support systems. International recognition of this research is evident from his membership of the executive board of the MONET European Network of Excellence (monet.aber.ac.uk, which ran until 2006), membership of the boards of AI in Medicine, which organises the biennial AI in Medicine conferences, and Probabilistic Graphical Models (PGM), which is responsible for the biennial PGM workshops. Dr. Lucas has organised many workshops in his area of expertise funded by ESF, NWO, the Lorentz Centre and ECCAI, and has been a PC member of conferences such as IJCAI, UAI, ECAI, ECML and ECSQARU. He is the representative for Europe in the British
AI conference organisation (through invitation). He is the only Dutch AI researcher whose work is extensively cited (4 pages) in the standard AI textbook by Russell and Norvig. Finally, dr. Lucas has been able to obtain a number of research grants in the review period and supervised five PhD students, who completed their thesis in the review period.

Prof. Plasmeijer has been granted the title of Doctor Honoris Causa and Professor Honoris Causa at the Eötvös Loránd University, he is member of IFIP working group 2.8 on functional languages, chairs the steering committee of the IFL (Implementation and Applications of Functional Languages). He has given invited lectures at functional language summer schools for many years. As a result he has become a member of the steering committee of CEFP (Central European summer schools on Functional Programming), and a member of the steering committee of AFP (Advanced Functional Programming). Plasmeijer is editor of the Journal of Functional and Logical Languages (JFLP). He is internationally well-known as chief designer of the functional language Clean. Plasmeijer has been a member of several program committees (e.g. CEFP, ICFP, IFL, TFP, APLAS, PPDP, ICCT, ACTIVE, TERMGRAPH). Plasmeijer is an adviser of the Technology Rating International, specialists in rating innovative technology ventures. He has been member of the advisory council of the Poly-technical University of Enschede.

Prof. Proper is well known for his leading work in enterprise engineering and enterprise architecture in Europe and the Netherlands. He has been chair and co-chair of EMMSAD since 2005 (Exploring Modeling Methods for System Analysis and Design); this workshop, which is officially supported by IFIP workgroup 8.1 (of which Proper and Dr. Hoppenbrouwers are members) is a key event among academics in the fields of conceptual modeling and method engineering. EMMSAD is structurally affiliated to the CAiSE conferences, which in Europe are a key event for Information Systems in its broadest sense. Rooted in the EMMSAD community, two further events have been set up recently, closely involving various TEE members. First, 2008 saw the first IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling (PoEM, Stockholm). Proper also initiated and chaired a more industry-oriented Working Conference, PRET 2009: “Practice-Driven Research on Enterprise Transformation”.

The new practice-oriented community in Enterprise Engineering now regularly publishes its proceedings under “Advances in Enterprise Engineering”, a sub-series of the Lecture Notes on Business Information Processing (Springer). To establish and further develop the discipline of Enterprise Engineering, Springer also established a new book series on Enterprise Engineering, of which Erik Proper is joint Editor-in-Chief. Books in this series are aimed at academic students and advanced professionals, while their content ranges from theoretical foundations to application experiences. Prof. Proper is on the Editorial Board of the International Journal of Information System Modeling and Design (IJISMD), a new journal by IGI Global (USA); Dr. Hoppenbrouwers is on the review board.

Dr. Hoppenbrouwers has become internationally known as a specialist in conceptual modeling, in particular in processes and procedures in systems modelling. He co-chaired a CAiSE workshop on Regulations Modeling and Deployment (ReMoD 2008), and chaired the 4th SIKS conference on Enterprise Information Systems (EIS 2009, Nijmegen). He also has been an invited speaker at some international events. He is on a number of international program committees and reviewing boards, including the PoEM working conferences. He has served as an adviser to industry on various occasions, and is co-translator to Dutch of standardization-oriented documents like the Business Rule Manifesto and RuleSpeak. He is or has been involved in NAF workgroups on Business Rules, Simulation and Gaming, and ArchiMate.

Prof. van Vliet is well known for his industrial role in the field of value chain optimisation. Furthermore, he is board member of the Nederland Distributieland (Netherlands Distribution Nation) organisation, and chair of the jury of Capgemini’s Open Source Award.

Dr. Achten and dr. Koopman are program chairs of the symposium trends in functional programming 2008, TFP08, and symposium chairs of TFP09. They are both member of the steering committee of TFP. Koopman, Plasmeijer and Swierstra (Utrecht University) are chairs of the Sixth International Summer School on Advanced Functional Programming. Koopman has been a member of several program committees, opponent in PhD defenses, an editor of the proceedings of VVSS 2008 (Verification and Validation of Software Systems), is member of the advisory board
and management team of LaQuSo, is invited to write a chapter in a book on testing, and is invited as speaker on AAIP. Achten has been member of several program committees.

### B.3.5 Internal Evaluation

Evaluation of research output of research personnel is done through annual assessments by the (senior) person who has been allocated as supervisor to the section member. This process allows identifying potential career paths; for example, researchers can be advised to work towards obtaining a personal grant (Veni, Vidi or Vici) from NWO. In addition, iCIS offers the temporary position of principal investigator to highly successful researchers, based on the outcome of a stringent evaluation procedure. The MBSD section includes two of iCIS’s principal investigators: prof. Vaandrager and dr. Lucas.

### B.3.6 External Validation

The MBSD section maintains close contacts with industry through the appointment of adjunct professors from industry (Prof. Proper from Capgemini and Prof. Van Vliet from Deloitte). In addition, some section members work parttime within an industrial environment (prof. Hooman and dr. Tretmans at the Embedded Systems Institute). Furthermore, a considerable portion of our research is driven by demands from industry. A typical example is the OCTOPUS project, where our involvement was based on perceived relevance of our research for industry (for OCTOPUS Océ).

Our involvement in research in clinical medicine and health care also indicates that we are able to bridge the gap between academic research in computer science and practical health-care applications. In recent projects, such as AERIAL, we aim at achieving an even higher level of impact to the practice of health care.

Finally, some members, in particular dr. Koopman, are actively involved in application-driven work within LaQuSo.

### B.3.7 Researchers and Other Personnel

Section members are allowed to work on all aspects of model-based system development, and some staff members has started working on different subthemes in the context of projects such as OCTOPUS and AERIAL. Doing research is not limited to staff members only: technical staff and adjunct professors are also involved in research to various degree. For example, the scientific programmers John van Groningen and Harco Kuppens are sometimes also involved in the production of scientific publications. Furthermore, our adjunct professors play a significant role in supervising PhD students. For example, prof. van Vliet supervised the Ugandese Nuffic PhD student John Ngubiri. Prof. Proper has been involved in the supervision of many other Ugandese Nuffic PhD students.

Training of the MBSD PhD students is done under the supervision of the research schools IPA and SIKS. Staff members are stimulated to take courses offered by the university to enhance opportunities for a career in research, teaching, or both. Senior staff members take special management courses. An overview of the research staff in the review period is shown in Table B.3.1. In addition to the staff members included in Table B.3.1, we have two staff members (dr. Wupper and prof. Barendsen) who are mainly involved in teaching and whose research is focused on teaching in computer science in general. As their research has no links to MBSD, they have not been included in the self assessment.
### Model Based System Development

#### Tenured staff

<table>
<thead>
<tr>
<th>Full professors</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plasmeijer, Rinus</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.50</td>
</tr>
<tr>
<td>Proper, Erik</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>Vaandrager, Frits</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Associate professors</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hooman, Jozef</td>
<td>0.30</td>
<td>0.10</td>
<td>0.10</td>
<td>0.10</td>
<td>0.10</td>
<td>0.10</td>
</tr>
<tr>
<td>Lucas, Peter</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.50</td>
<td>0.60</td>
</tr>
<tr>
<td>Tretmans, Jan</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.30</td>
<td>0.08</td>
<td>0.08</td>
</tr>
</tbody>
</table>

#### Associate professors

| Achten, Peter | 0.32 | 0.32 | 0.32 | 0.32 | 0.32 | 0.32 |
| Bommel, Patrick van | 0.40 | 0.40 | 0.40 | 0.40 | 0.40 | 0.40 |
| Hoppenbrouwers, Stijn | 0.06 | 0.36 | 0.40 | 0.40 | 0.40 | 0.40 |
| Koopman, Pieter | 0.40 | 0.40 | 0.40 | 0.40 | 0.40 | 0.40 |
| Schouten, Theo | 0.40 | 0.40 | 0.40 | 0.20 | 0.20 | 0.10 |
| Veldhuijzen van Zanten, Gert | 0.40 | 0.40 | 0.40 | 0.09 | 0.09 | 0.09 |

#### Total tenured staff

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total tenured staff</td>
<td>4.22</td>
<td>4.02</td>
<td>4.08</td>
<td>3.97</td>
<td>3.70</td>
<td>3.50</td>
</tr>
</tbody>
</table>

#### Non tenured staff

| de Carvalho Ferreira, Nivea | 0.13 | 0.4 |
| Chklaev, Dmitri | 0.90 | 0.55 |
| Evers, Sander | 0.64 |
| Gronov, Maxim | 0.84 |
| Groot, Perry | 0.25 | 0.90 | 0.90 | 0.75 |
| Hoppenbrouwers, Stijn | 0.20 | 0.68 | 0.45 |
| Jansen, David | 0.15 | 0.40 |
| Proper, Erik | 0.15 |
| Schmaltz, Julien | 0.84 | 0.90 |
| Vervoort, Martijn | 0.40 |
| Vliet, Mario van | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 |
| Willemse, Tim | 0.82 | 0.90 | 0.64 |
| Zhang, Miaomiao | 1.00 | 0.16 |
| Zwaag, Mark van der | 0.90 | 0.52 |

#### Total non tenured staff

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total non tenured staff</td>
<td>4.14</td>
<td>3.21</td>
<td>2.75</td>
<td>2.56</td>
<td>2.74</td>
<td>2.45</td>
</tr>
</tbody>
</table>

#### PhD candidates

| Alimarine, Artem | 0.90 | 0.60 |
| Arkel, Diederik van | 0.30 | 0.82 |
| Berendsen, Jasper | 0.75 | 0.90 | 0.90 |
| Cheung, Ling | 0.30 | 0.90 | 0.90 | 0.60 |
| Flesch, Ildiko | 0.75 | 0.90 | 0.90 | 0.90 | 0.30 |
| Frantzen, Lars | 0.60 | 0.90 | 0.82 | 0.49 | 0.78 |
| Gelremichael, Biniam | 0.90 | 0.90 | 0.90 | 0.18 |
| Gerven, Marcel van | 0.68 | 0.90 | 0.90 | 0.22 |
| Gils, Bas van | 0.84 | 0.32 | 0.81 | 0.37 |
| Groot, Adriaan de | 0.90 | 0.85 | 0.06 |
| Heidarian Dehakori, Faranak | 0.09 |
| Hendriks, Martijn | 0.84 | 0.87 | 0.90 | 0.52 |
| Hommersom, Arjen | 0.90 | 0.90 | 0.80 | 0.80 | 0.90 |
| Hoppenbrouwers, Stijn | 0.67 |
| Igna, Georgeta | 0.08 | 0.90 |
| Jurgelenaita, Rasa | 0.30 | 0.90 |
| Mol, Maarten de | 0.30 | 0.67 | 0.90 |
| Noort, Thomas van | 0.30 | 0.67 | 0.90 |
| Verbeek, Freek | 0.92 |
| Verheoef, Marcel | 0.25 |
| Weelden, Arjen van | 0.03 |

#### Total PhD candidates

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total PhD candidates</td>
<td>8.12</td>
<td>10.78</td>
<td>8.76</td>
<td>5.79</td>
<td>3.83</td>
<td>5.85</td>
</tr>
</tbody>
</table>

#### Total research staff

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total research staff</td>
<td>16.48</td>
<td>18.01</td>
<td>15.59</td>
<td>12.32</td>
<td>10.27</td>
<td>11.80</td>
</tr>
</tbody>
</table>
B.3.8 Resources, Funding and Facilities

Table B.3.2 gives an overview of the resources and funding of the MBSD research.

<table>
<thead>
<tr>
<th>Model-Based System Development</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Direct Funding</td>
<td>72.2</td>
<td>65.3</td>
<td>64.6</td>
<td>67.9</td>
<td>70.7</td>
<td>62.4</td>
</tr>
<tr>
<td>2: Research Funds</td>
<td>9.6</td>
<td>16.4</td>
<td>18.8</td>
<td>22.3</td>
<td>24.5</td>
<td>29.3</td>
</tr>
<tr>
<td>3: Contracts</td>
<td>18.2</td>
<td>18.3</td>
<td>16.6</td>
<td>9.8</td>
<td>4.8</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

B.3.9 Overview of the Results

Key publications


- L. Cheung, M. I. A. Stoelinga, and F. W. Vaandrager. A testing scenario for probabilistic processes. *Journal of the ACM*, 54(6), 2007. (Fundamental result published in top journal. Conference version received best paper award at ICALP. Stoelinga received the De Winter prize from the University of Twente for her contribution to this work.)


Table B.3.3: Programme results: outcome numbers (SEP Table 6)

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic publications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in refereed journals</td>
<td>4</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>18</td>
<td>11</td>
</tr>
<tr>
<td>b. in refereed proceedings</td>
<td>35</td>
<td>40</td>
<td>52</td>
<td>48</td>
<td>45</td>
<td>38</td>
</tr>
<tr>
<td>c. book chapters</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total academic publications</strong></td>
<td>40</td>
<td>53</td>
<td>69</td>
<td>63</td>
<td>70</td>
<td>58</td>
</tr>
<tr>
<td>2. Monographs</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>3. PhD theses</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4. Professional publications and products</td>
<td>11</td>
<td>27</td>
<td>31</td>
<td>24</td>
<td>33</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total publications</strong></td>
<td>55</td>
<td>81</td>
<td>106</td>
<td>93</td>
<td>108</td>
<td>79</td>
</tr>
</tbody>
</table>

B.3.10 Analysis, Perspectives and Expectations

Strengths

- There is a clear focus of MBSD research on modeling, model construction, analysis and exploitation.
- MBSD expertise covers a major part of the process of developing model-based systems ranging from conceptual modeling, via the deployment of formal methods, application generation, testing and experimentation, to verification and validation.
- Our research ranges from theory to the development of applications.
- Many MBSD projects are successful in bridging the gap between academic research and application areas within the industrial sector (AMETIST, BODERC, OCTOPUS, TANGRAM), health care (TimeBayes, ProBayes, B-Screen, AERIAL, Protocure), the public sector (ArchiMate, Controlling Dynamic Real Life Workflow Systems), and the financial sector (ArchiMate, business rules).
- MBSD research is well-funded by grants from national and European research agencies.
- MBSD research is internationally leading in the areas of computer-aided verification and analysis using timed automata, functional and generic programming, and medical decision-support systems.
- MBSD is very productive in publishing research results.
- MBSD research attracts many master students: two-third of the master’s thesis projects of iCIS are supervised by members from the MBSD section.

Weaknesses

- The MBSD section was the result of a merge of different groups, and although their research fields are linked to each other, the communities to which the various section members belong vary. This is viewed as a bottleneck to cooperation.
- Modern science assessment instruments such as citation analysis are placing an ever-increasing emphasis on journal papers as the main output of research. However, some of our research concerns the development of software tools with the purpose of demonstrating the viability of certain principles and concepts, which we as computer scientists think is important. Tool development imposes, on the one hand, high demands on human resources, yielding, on the other hand, limited output in terms of scientific publications.
• Some of our research focuses on the detailed modeling and analysis of hardware and software systems that are considered to be crucial by industry. Although this work is central to our research mission, it is very labor intensive and not highly rewarding in terms of the number of scientific publications.

• MBSD is a broad area and given the size of MBSD it is not possible to develop sufficient critical mass for achieving high scientific impact for all the topics considered relevant for MBSD research.

• The conceptual modeling and enterprise engineering subthemes are currently managed by an adjunct professor who works only part-time.

Opportunities

• The ideas underlying model-based system development are now also increasingly adopted by various application fields, beginning with the highly innovative companies. This yields new opportunities for collaborative research.

• As the subthemes of MBSD research fit nicely to each other, this allows pursuing project that would not have been possible otherwise. Setting up collaborative research and increasing the amount of synergy in the section is an active policy that is supported by all MBSD members, which will allow us to target new sources for funding.

• With the development of F# and involvement in the Haskell community, Microsoft Research has now also entered the areas of functional and generic programming. Some of the ideas originating from research within MBSD have been adopted by Microsoft Research, creating an opportunity to profit by increasing our visibility.

• The model-based approach to system development offers an attractive paradigm for communication with disciplines outside computer science. We believe that this may yield new opportunities for multidisciplinary research, and we have started to explore such opportunities in the context of workflow management, biomedicine, embedded systems, and business rules.

Threats

• The deplorable financial state of the faculty has turned an originally financially prosperous situation for MBSD into one with no financial means for flexible staff management and growth. The effects of this are further enhanced by the fact that it is difficult to attract external funding for fundamental computer science research. Most of the funding now comes from project that are funded by the EU or Dutch government and that have strong links with industry or are multidisciplinary in nature. In addition, the amount of national funding available for main stream computer science research is not in par with the requests for funding, which has dramatically increased over the past two years.

• The economic downturn has reduced the number of new opportunities for research funding that comes directly from the computer science related industries.

• MBSD includes a number of excellent postdoc researchers who contribute substantially in terms of research output. Without the availability of (new) vacancies for permanent staff members their expertise will be lost and this may negatively affect the competitiveness of MBSD research in the near future.
Analysis
The weaknesses listed above are subsequently addressed one by one:

- Although the MBSD section was created from groups coming from different departments, members of the new section support the policy of creating synergy between the different research subthemes. Here it may have helped that the MBSD members have fully embraced model-based methods as an appropriate unifying concept of our research. Thus, MBSD members share a common vision and mission. It has been an active policy from the start of the creation of MBSD to look upon the section as being one group, specialized in different, but closely related, subthemes. First steps in enhancing synergy have been set by actively pursuing collaborative research between the subthemes through the appointment of PhD students that cross the boundaries between the subthemes and my mutual involvement of people in projects.

- The emphasis of some of the MBSD research on tool development is increasingly underappreciated by government and university policy makers by an increasing emphasis on journal publication as the sole means for achieving research impact. This trend may have a very negative effect on future investments in research concerned with experimental validation. One result of this trend has been that a decreasing portion of MBSD research is concerned with tool development; in many cases use is made of existing tools, that are subsequently extended to our needs. The fact that we are productive as a section in terms of number of publications is partly a consequence of this switch from tool development to work on publications. However, some level of tool development remains a necessary prerequisite for doing successful research in MBSD.

- Some of our section members develop elaborate hardware and software models that are considered of great relevance by industry. These members have been faced with the negative consequences of such work in terms of underappreciation of their quality as researcher, when it was only measured in terms of number of (journal) publications. This, unfortunately, has happened a number of times when they applied for a personal grant with NWO. So far, we have not been able to resolve this issue, also as we consider the development of elaborate industrial size models as being crucial for MBSD research.

- To increase visibility and scientific impact of MBSD research it was necessary to enhance the focus of our research, and such has already been happening during the past few years. The research on functional programming and the development of the functional programming language Clean, which has been a focus of research for many years in Nijmegen, has yielded a mature product, as is also acknowledged by the programming language community at large. This research has, therefore, changed its orientation towards model-based application development, in particular workflow-management systems, using functional and generic programming as an enabling technology. This change in research focus has already given rise to the attraction of new external funding for research.

  Similarly, the development of proof assistants is currently not a focus of research of MBSD, and although this research has had international impact, it is currently seen as another enabling technology for model-based system development, rather than as a research focus.

- By embedding the conceptual modeling and enterprise engineering research into the context of other subthemes covered by MBSD we intend to reduce the risk that this subtheme is drifting apart from the lines of research set out for MBSD. So far, this policy has been successful and has been further strengthened by the appointment of a PhD student working on the intersection between conceptual modeling and enterprise engineering, on the one hand, and model-based reasoning, on the other hand.

The threats mentioned above are all related to limited financial means from resources that have been exploited for many years successfully to set up new research. As a consequence, we have adjusted our strategy for obtaining research funding, as is discussed below.
Adjusted goals

Members of MBSD feel comfortable with the model-based systems development theme. Although people work on several subthemes, the policy to break down boundaries between the original groups has been successful. In the near future more emphasis will be placed on profiting from the complementary expertise available within the section, in particular in attracting funding for research.

As mentioned above, research in functional programming has been redirected towards the challenging new area of model-based application development, with an emphasis on workflow-management systems. Work on the development of proof assistants for Clean will be discontinued.

Adjusted strategies

By increasing the synergy within MBSD, we hope to achieve more scientific impact in the areas in which we are currently most successful: model-based verification, analysis and testing, model-based application development, and model-based decision support. In these areas we will likely be able to realize MBSD’s mission of doing fundamental research on the use of (mathematical) models in the development of computer systems in relationship to application areas from industry, government, and health care, in particular by empirically validating methods and techniques through the development of challenging applications. Here there is also a clear role for our section members that work part-time in industry.

While traditionally we have obtained most of our research funding from computer-science programs of NWO (Netherlands Science Foundation)/EW (Exact Sciences) and the IST programs of the EU, the combination of lack of funding from the faculty and the low success rates of NWO/EW and IST proposals have motivated us to look for sources of funding outside computer science, such as from health care and government. Lately, we have been successful in attracting funding for research in clinical guidelines and clinical computer-aided decision making from the Medical Research Council (ZonMW/NWO), and likewise in the area of workflow management from the Dutch Navy. Similarly, we are trying to establish connections with biologists and clinicians to explore ways to set up research in systems biology.

Summary

The MBSD section has evolved in the reporting period from four independent groups to one group of which all members have embraced the common mission and vision of model-based system development, realizing the considerable benefits obtained by the unique feature of the section that it is able to cover a large portion of MBSD research. The synergy between subthemes has seen a significant increase since the start in 2008 and our research has been flourishing.
B.3.11 Publications

2003

Academic publications

Refereed journal publications


Articles in refereed proceedings


B.3.11. PUBLICATIONS


B.3.11. PUBLICATIONS


Book chapters


Monographs


PhD theses


Professional publications


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


2004

Academic publications

Refereed journal publications


Articles in refereed proceedings


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


B.3.11. PUBLICATIONS


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


Book chapters


Monographs


Professional publications


2005

Academic publications

Referred journal publications


**Articles in refereed proceedings**


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


B.3.11. PUBLICATIONS


Book chapters

CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


Monographs


PhD theses


Professional publications


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


2006

Academic publications

Refereed journal publications


**Articles in refereed proceedings**


B.3.11. PUBLICATIONS


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


B.3.11. PUBLICATIONS


Book chapters


Monographs

PhD theses


Professional publications


B.3.11. PUBLICATIONS


2007

Academic publications

Refereed journal publications


Articles in refereed proceedings


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


Book chapters


Monographs


PhD theses


Professional publications


B.3.11. PUBLICATIONS


2008

Academic publications

Refereed journal publications


B.3.11. PUBLICATIONS


**Articles in refereed proceedings**


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT


Book chapters


B.3.11. PUBLICATIONS

Monographs


PhD theses


CHAPTER B.3. MODEL-BASED SYSTEM DEVELOPMENT

Professional publications


Other publications referenced in the text


Self-evaluation 2003-2008

Institute for Computing and Information Sciences

Radboud University Nijmegen
Faculty of Science
PO Box 9010
6500 GL Nijmegen
The Netherlands

www.ru.nl/icis/