The mission of the Institute for Computing and Information Sciences is to develop formal, mathematical theories, methods and tools that will support the specification, design, analysis and evaluation of computer-based systems. Research aims include improving the quality of software, with an emphasis on reliability, security, system architecture and alignment. Researchers at the Institute strive to develop a sound, well-understood theoretical basis for the methods underlying software development, which are not unlike the methods employed in the traditional engineering disciplines, such as those used in the design of bridges and buildings. Methods and tools are validated by tackling their applicability to problems encountered in other disciplines. Research is concentrated within five research groups, each with its own particular focus and aims.
Foundations (F)
To develop and study formal languages and logical theories involving algorithms, proofs, processes, computations, correctness and complexity, as well as developing and experimenting with computer tools that support these languages and logics.

Software technology (ST)
To develop theory, methods and tools for specification, programming (in particular functional and generic programming techniques), static analyses (especially type systems), and dynamic analyses (with a focus on specification and model-based testing) to support designers and developers in building and verifying reliable software.

Information and knowledge systems (IRIS)
To perform fundamental and applied research around the theme of knowledge-intensive systems, i.e. systems that can elicit, structure and process implicitly and explicitly represented knowledge of a problem or domain, drawing upon ideas, methods and techniques from information systems and artificial intelligence.

Security of systems (SoS)
To develop theories, formal methods and tools that contribute to the security of protocols and software (especially for Java), and contribute to ongoing developments and debates on socially relevant issues such as privacy, open source, electronic voting and biometric passports.

Informatics for technical applications (ITA)
To carry out fundamental research on formal methods and tools for the specification, design, analysis and testing of computer systems for technical applications (in particular embedded systems and protocols), and demonstrate and assess the effectiveness of using these methods and tools in industrial software development.

Collaboration
The Institute collaborates with the Distributed Systems and Semantics Group of the Aalborg University (Denmark), INRIA – Institute National de Recherche en Informatique et en Automatique, Verimag - Institute d’Informatique et Mathématiques Appliquées de Grenoble, France Telecom, Trusted Logic, SAP (France), University College Dublin (Ireland), University of Verona (Italy), AIST (Amagasaki, Japan), ASML, Embedded Systems Institute, Ministry of Internal Affairs, Surfnet, TNO, TNO-ITSEF, Chess-IT Haarlem, PricewaterhouseCoopers, Netherlands Cancer Institute.
Research results

The Foundations group has continued to formalize mathematics within the C-CoRN (Constructive Coq Repository at Nijmegen) project. The emphasis has shifted from a focus on real numbers to formalizing computability. Also the connection between formalized mathematics and computer-based mathematical documents has been studied further in the context of the EU Mowgli project, which ended in 2005. This has led to a proof of concept, focusing on a specific number from formalization projects. The group has also studied graphical proof representations, and foundational questions about the interaction between constructive mathematics and mathematical algorithms.

The Software technology group has developed a new generic programming technique with which interactive graphical user interfaces (editors) can be automatically generated. This enables the automatic generation of type-safe forms, even for higher order types. The technique is further refined and applied to automatically generating web pages. A start has been made with developing formal semantics for this technique. A fusion technique has been developed which avoids the need for generic programming for a very large class of applications.

The NWO project Profile-based retrieval of networked information resources (PRONIR) of the Information and knowledge systems group focused on the impact of economical models for the digital market on information disclosure strategies. Within the EU FET project Protocure II, formal methods and various verification tools were successfully applied to a medical guideline for managing diabetes mellitus type 2, indicating a number of shortcomings. In the context of the ProBayes and TimeBayes project, new techniques for the compact representation of probability tables in Bayesian networks – based on Boolean functions – were developed. There was successful collaboration with clinicians, demonstrating the usefulness of these techniques.

The Informatics for technical applications group studies the modeling and analysis of hybrid systems, i.e., systems that combine discrete and continuous components in computers that interact with the physical world. Hybrid systems are becoming more and more common, ranging from avionics...
and process control to automotive and consumer electronics. A thesis was defended on PHAver, a tool for verifying the safety properties of hybrid systems. Experiments show that PHAver computes faster and more accurately than other, comparable programs, such as the widely used HyTech package from the University of Berkeley. Together with MIT and the University of Verona, a monograph was completed on hybrid systems that will appear in January 2006. Coordinated by the institute, the European IST project AMETIST, which developed model checking techniques for the analysis of real-time systems, was successfully completed in 2005.

The Security of Systems group continued to be active in the area of electronic voting and is also involved in the plans to introduce a new biometric passport in the Netherlands. In the recently started EU IST project Mobius the group is analyzing the security of Java software on mobile phones, building on earlier success with verifying smartcard software. Work in the field of security protocols resulted in a proposal for electronic cash for peer-to-peer networks and initial steps towards a provable notion of anonymity. A paper on ‘proof support for general type classes’ was awarded the Best Student Paper Award at Trends in Functional Programming (TFP’04) by a unanimous vote.

**Societal impact**

Computer security is a key issue in society and the Security of Systems (SoS) group is actively engaged in public debates about issues in this domain. Investigations of the security of wireless networks in Nijmegen resulted for instance in an article in the regional newspaper De Gelderlander and a tightening of security in Nijmegen city hall. Prof. Jacobs received the annual I/O prize – awarded by the Dutch Informatics Platform – for raising media attention for ICT research with publicity about electronic voting. The group is closely involved in plans to introduce a new biometric passport in the Netherlands.

The Nijmegen branch of the Laboratory for Quality Software (LaQuSo), collaborates with the Eindhoven University of Technology (TU/e) on transferring state-of-the-art technology for software analysis from academia to industry through contract research. There have been projects with companies such as Nuon, Pricewaterhouse-Coopers, Compumatica and GX.

The CodeYard project started in 2005. This project, sponsored by IBM, NlNet, and Cap Gemini, is promoting active participation by students at secondary schools in the developing open source software.

A joint two-year Master’s programme in Computer Security – developed in collaboration with the University of Twente and TU/e – is due to start in September 2006.

ICIS collaborates with a number of universities in Africa, for example in Ghana and Uganda, the latter in a project sponsored by Nuffic. A similar project for collaboration with Mozambique has recently started.

With its Interactive Mathematics project, the Foundations group attempts to bridge the gap between formal mathematics (basically computer code) and the human readable mathematics in papers. This is part of a more general goal of disclosing digital information. It is also building up a library of formal mathematics to be used in verifying programs and systems.

Within projects in the Embedded Systems Institute (TANGRAM and BODERC) the Informatics for technical applications group collaborates directly with some of the main players in the Dutch embedded industry such as ASML, Philips and Océ on developing and testing methods for embedded systems. Model-based testing and verification techniques, whose development is the core research topic of the group, are routinely applied in a wide range of industrial applications in embedded systems, ranging from airplane landing manoeuvres to protocols for configuring local Internet network in the absence of DNS servers.

There is growing awareness in health care that, with rapid increases in biomedical knowledge, combined with strict budgetary constraints, the quality of health care and medical management cannot increase without extensive use of information technology. The Institute is leading two projects (TimeBayes and ProBayes), in collaboration with clinical partners that investigate the role and place of medical knowledge and online biomedical data in medical decision-making.

Apart from these programmes, the societal impact of the research mainly takes place through close collaboration with industry and other research institutes, sometimes in joint research projects with disciplines outside computing science.

**Future research**

Most of the Institute’s research is guided by projects that are externally funded by the European Commission, the national government and industry. Examples are four EU IST projects (Protocure II, Monet, Mowgli, Mobius), Prof. H. Barendregt’s Spinoza Prize, Prof. B. Jacobs’ Vici project, Dr. B. Spitters’ Veni project, and ten NWO projects, two ‘sentinel’ STW projects (Pinpas and Jason), Senter’s Boderc project (Beyond the Ordinary: Design of Embedded Real-time Control), Model-based integration and testing of complex high-tech products (TANGRAM), and PAW (Privacy in an Ambient World), as well as intense


PhD theses: 3
Scientific publications: 129
Professional publications: 30
research collaboration with ASML, OCE, ING bank, and LogicaCMG. Some of these projects are described below.

The Spinoza Prize will continue to support the development of tools and methods for formalized mathematics as well as case studies in that direction. A new four-year NWO FOCUS project – involving two post-docs and one associate professor – has received grant support. The aim of this project is to advance the use of proof assistants in mathematics and computer science, especially regarding reasoning over and computing with real numbers. A smaller NWO project with the aim of formalizing notions from complex analysis that are standard in the engineering sciences has received grant support.

Together with the TU/e, the Institute will operate the Laboratory for Quality Software (LaQuSo), which will perform research-related case studies submitted by third parties.

The new EU project ROBIN, due to start early 2006, will broaden the range of work on programme analysis in the SoS group, by investigating the security of operating system kernels.

Within the context of the NWO/DFG project VOSS and in collaboration with Prof. Lynch (MIT) and Prof. Segala (Verona), the work on semantic models for verifying distributed algorithms that involve probabilistic mechanisms (e.g. agreement algorithms and security protocols) will be continued.

So far, formally verifying clinical guidelines is only possible interactively, i.e. some of the proof rules need to be selected by the user. Within the Protocure II project it will be investigated whether model checking of formalized clinical guidelines allows for the automated study of relevant properties of such guidelines. In the ProBayes and TimeBayes project our aim is to refine and validate the medical Bayesian network models in collaboration with collaborating clinicians. Bayesian brain-computer interfacing (BCI), a new STW project, 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. Probability models are used to improve the performance of BCI systems.

Within the new European project AI4IA, artificial intelligence techniques will be developed and applied in close cooperation with testing facilities for rotating machine components at SKF, the world’s leading manufacturer of rolling bearings.

To strengthen the exchange of ideas between theoreticians and practitioners, IRIS will be involved in two working groups of the Netherlands Architecture Forum. This forum involves collaboration between industry and academics, focusing on enterprise architecture. We participate in a working group on the fundamental concepts of architecture, another on the role of business rules in architecting, and one on gathering and standardizing architectural knowledge.

The applicability of generic programming techniques to new applications such as Workflow Management Systems (with the TU/e), Information Systems (with the HAN in Arnhem/Nijmegen and the ESA in Noordwijk) and Embedded Systems (with Imtech in Belgium) will be further explored. The theory behind generic programming will be further refined in collaboration with the University of Utrecht (Prof. Jeuring).

Health care is currently undergoing rapid change, for instance with the introduction of electronic medical records. As part of the LaQuSo initiative, ICIS is using the NWO’s Hefboom scheme to form new relations with partners in health care. In 2006 the Pôle de Compétitivité consortium NUADU-NL will start a large project on Telemedecine, with a grant from the Dutch government. This new ITEA telemedicine project, under the direction of Philips Research, provides the institute with substantial funding, enabling it to move into this area, in collaboration with medical researchers from the UMC.