AN ESTONIAN RESEARCH EXCELLENCE CENTRE IN COMPUTER SCIENCE

TARMO UUSTALU
Tarmo Uustalu (born 1969) is a senior researcher of the Institute of Cybernetics at TUT and professor of the Tallinn University of Technology. He holds a MSc from the Tallinn University of Technology (1992) and PhLic and PhD degrees from Kungliga Tekniska Högskolan, Stockholm (1995 and 1998) and has a postdoctoral researcher experience from Universidade do Minho, Braga. His main research areas are logical methods in computer science, programming language theory, functional programming, formal methods of analysis and construction of programs.

In recent years, many governments around the world have begun to concentrate excellent scientific research into "centres of excellence" (CoEs). The idea is to join the strongest research groups together, so as take maximum advantage of their total competence in the most economical constellation of human potential and material resources.

In 2001, a similar initiative was launched in Estonia too, by the Ministry of Education and Research and its Council of Scientific Competence. In 2001 and 2002, the ministry organized two competitions for the title of a national centre of excellence in research. As a result, ten institutions and consortia were awarded this status until year 2006 (now prolonged until 2007), when the list will be reviewed. The list of these centres covers a number of disciplines of scientific enquiry, ranging from physics through life sciences to humanities.

In this article, I want to write about the Estonian Centre for Dependable Computing, CDC, which obtained the title of a national centre of excellence as a result of the 2002 competition. CDC is a computer science research centre and, as such, it is the only one of the ten centres in Estonia, specializing the priority area of information technologies. And I'd maintain that it is also among the strongest and most successful centres. More specifically, the research conducted at CDC is concerned with the correctness and security of computer hardware and software.

WHO ARE THE CENTRE?

CDC is a network, so it is not based on one single organization. Rather, it is an umbrella for research groups in a number of organizations.

Officially, CDC was formed to compete for the CoE title, but in reality, it is not that new, since it only formalized a long-standing informal collaboration between a number of people and organizations.

CDC unites researchers from the following research institutes and university departments:

- Institute of Cybernetics (IoC) at Tallinn University of Technology,
- the Departments of Computer Science, Computer Engineering and Computer Control of Tallinn University of Technology (TUT),
- the Department of Computer Science of University of Tartu (UT),
- Tartu University Institute of Technology (TUIT),
- Cybernetica AS.

These organizations act together in a consortium led by the Institute of Cybernetics. IoC is a semi-autonomous research institute of TUT conducting research in various areas of applied mathematics, including computer science, a former Estonian Academy of Sciences research institute. The centre is led by a research council, consisting of Prof-s Jaan Penjam, Ahto Buldas, Raimund Ubar and Tarmo Uustalu. The centre also has an international scientific advisory board. The members of this body are Prof Emeritus Reino Kurki-Suonio (Tampere University of Technology), Prof Kim Larsen (Aalborg University), Prof José Oliveira (University of Minho, Braga), Prof Reinhard Wilhelm (University of Saarland, Saarbrücken). The project is led by Jaan Penjam.

CDC engages both some of the most highly reputed Estonian computer scientists with an extensive research experience from a long career - such as the members of the Estonian Academy of Sciences Leo Mõtus, Enn Tõugu and Raimund Ubar - as well as number of their considerably younger colleagues - Ahto Buldas, Gert Jervan, Peeter Laud, Helger Lipmaa, Jaan Raik, Tarmo Uustalu, Eero Vainikko, Varmo Vene, Jaak Vilo. It is significant that nearly all of these younger people have all at one point studied for a PhD or held a postdoc position abroad and are now back in their home country. They are publishing in renowned international venues and are leading specialists in their fields, despite the circumstances that have not always been the friendliest. (I am not foremostly thinking of access to funding here, but much more of the policies of the state and the university leaderships, which have not always been clear or strong or strategic.)

RESEARCH AREAS AND ACTIVITIES

In broad terms, all of CDC's research is aimed at technologies for making software and hardware more correct and more secure.

By the narrower research agendas pursued, CDC is structured into four research teams:

- mathematical foundations and programming languages (leader Tarmo Uustalu),
- formal methods in systems development (leader Jaan Penjam),
- information security and cryptology (leader Ahto Buldas),
- design and test of digital systems (leader Raimund Ubar).

The research in mathematical foundations and programming languages is conducted at IoC and the Department of Computer Science of UT. The research areas of the team are categorical semantics of functional languages, program logics and type systems for describing program analyses, semantics-based manipulation of programs, language-based security.

The formal methods team has members from IoC, the Departments of Computer Science and Computer Control of TUT and the Tartu University Institute of Technology. The research topics are software composition and visual programming, automated theorem proving with applications to hardware verification and the Semantic Web, model checking of hybrid systems, models of interactive computation and scientific computing. Tanel Tammet's theorem-proving program Gandalf is one of the strongest in the world and has repeatedly won first prizes in several categories of the annual world competition of such programs.

The centres research in information security and cryptology takes place at Cybernetica AS and the Department of Computer Science of UT. This team studies methods for public key distribution and certificate validation, security and auditability of queries to public databases and security of time-stamping schemes. This team has participated in a number of government projects such as the national id-card, e-elections etc.

The research team of digital design and test is based on TUT's Department of Computer Engineering. This team studies fault modelling, test generation, diagnosis of design errors and faults. Special attention is paid to new paradigms such as systems-on-chip, software-hardware codesign, testability, built-in self-test.

GRADUATE EDUCATION

One of the missions of CDC is to advance the IT graduate education provided at TUT and UT. By concentrating the best Estonian competence in computer science and engineering, CDC is more than well-suited for this task.

CDC advances graduate education through providing supervision to degree candidates and equipping them with a research environment, but also via special events. There are three such series of events: the international winter and summer schools EWSCS and ESSCaSS and the national computer science theory days.

The international EWSCS winter schools in computer science are held in Estonia annually from as early as 1996. All these schools, except for the first one, have been organized by IoC. The schools have a theory bias and cover both algorithmics, complexity and models of computation as well as logic, semantics and programming theory. Each school consists of 4-5 intensive courses from internationally renowned scientists. The audience (approx 50 students) is half Estonian, half international and consists mainly of graduate students. The EWSCS are widely known in the worldwide theoretical computer science community and have a very positive image.

The more practical ESSCaSS summer schools in computer and systems science are a younger sister of the EWSCS series. By their format, they are similar to the EWSCS schools, but the topics are selected from software engineering, artificial intelligence etc.

Once a Tallinn schoolgirl, Edith Elkind has become a Princeton doctor who now works at Warwick and studies the connections between algorithmics, game theory and economic theory

Adam Eppendahl thinks knot theory is relevant for databases. The researcher with a PhD from Queen Mary in London worked at IoC for a year and is now in Malaysia.

The theory days, started in autumn 2002, are a highly popular informal forum for where the Estonian computer science theorists learn about each others' work. These are held biannually.

During the existence of CDC, eight PhD degrees have been defended in the centre: Marina Brik (2002), Artur Jutman, Hellis Tamm (2004), Gert Jervan, Raul Savimaa, Jelena Fomina (2005), Kristo Heero, Härmel Nestra (2006). These numbers are smaller than we would like, but it must be taken into account that, given the current extreme shortage of IT engineers in Estonia, it is very difficult for the universities to compete with the IT industry for students. The universities cannot offer competitive salaries and working conditions and, as a result, the number of full-time PhD students is small and part-time PhD students hardly ever finish.

INTERNATIONAL PROJECTS

One of the strong emphases in the activities of CDC is internationalization of Estonian IT research. Apart from ad hoc individual contacts between scientists, the main way to achieve this is to increase participation in international projects. For CDC, the single most important international funding body thus far has been the European Commission through its 5th and 6th Framework Programmes (FP). CDC has met significant success in seeking participation in the Information Society Technologies Programmes of FP5 and FP6.

From Nov. 2005 to Sept. 2005, IoC, the Departments of Computer Engineering and Computer Science of TUT, the Department of Computer Science of UT and Cybernetica implemented the FP5 IST project eVikings II, whose objective was to

establish in Estonia a virtual centre of IST research excellence. IoC was a coordinating partner and, in addition to the partners of CDC, a number of Estonian organizations (such as the Archimedes Foundation) and some foreign universities (Helsinki University of Technology, École Polytechnique Féderale de Lausanne) took part. It is fair to say that this project was a support measure for CDC, financed by the European Commission. But, in fact, the scope of eVikings II was wider than that of CDC. In addition to software and information security technologies and digital systems, it also covered human language technology and touched upon IT innovation, technology foresight etc.

During the period from Jan. 2003 to June 2006, IoC together with more than 20 European research centres participated in a FP6 IST thematic network dedicated to applied semantics, codenamed APPSEM II. The objective of this mobility project was to coordinate the European research efforts in programming language theory. In APPSEM II, IoC had an important role to play - IoC organized one of the three major annual workshops of the project.

The FP6 IST coordination action TYPES, which also has IoC among its consortium partners, is similar by its mission, activities and organization to APPSEM II. The TYPES project lasts from Sept. 2004 to Aug. 2008 and coordinates research in type theory, its applications to mathematics and software technology, advancing type-theoretic languages and systems and applying this technology to domains such as certified code, formalized mathematics and mathematical education.

From Sept. 2005 to Aug. 2009, IoC is a partner in the FP6 IST integrated project MOBIUS (Mobility, Ubiquity and Security for Small Devices). This is a large-scale research project and sets out to develop a new platform of trust and security for the next generation global computers, based on the proof-carrying code (PCC) paradigm. The idea of PCC is that it is the responsibility of the producer of a piece to prove that it is safe. The producer must accompany the code with a proof of safety, a certificate that the consumer can check mechanically. The challenges of MOBIUS are to extend the method of PCC to global computers and scale it from basic safety policies to stronger safety criteria, up until functional correctness. The technical tools employed are novel logics and type systems.

The Department of Computer Science of TUT participated in the FP5 IST thematic network EURON (European Robotics Network, Dec. 2000-April 2004) and is one of the consortium partners in its follow-up project EURON II (May 2004-April 2008), a network of excellence in FP6 IST. The mission of these projects is to strengthen EUs competitiveness in robotics in comparison with USA and Japan.

The Department of Computer Engineering of TUT has a long-standing experience in teaching the design of SoCs and participated in the FP5 IST accompanying measure REASON (Research and Training Action for System-on-Chip Design, Jan. 2002-30 June 2005). REASON aimed synchronizing the research of Central and Eastern European microelectronics centres with that conducted at the EU institutions. Right now, the same department is involved in a FP6 IST specific targeted research project VERTIGO (Verification and Validation of Embedded System Design Workbench, June 2006-Nov. 2008).

At TUT, the tuition of computer science is coordinated by Prof Jüri Vain.

Sven Laur is a PhD student in cryptology both at the University of Tartu and Helsinki University of Technology.

Cybernetica AS participated in two FP5 IST projects: the accompanying measures project OpenEvidence (An Open Source Technology for Data Certification in Value-Added Services, April 2002-Sept. 2003) and the thematic network RESET (Roadmaps for European Research on Smartcard Technologies, Sept. 2002-May 2003). The OpenEvidence project was carried out by three firms and studied technologies for securing long-term authenticity of documents with digital signatures, time stamping and standardization of document formats. The RESET project tried to predict the future of the smartcard technology.

From Sept. 2005 to Aug. 2009 Cybernetica AS is implementing the FP6 IST project AEOLUS (Algorithmic Principles for Building Efficient Overlay Computers). This project studies the algorithmics of constructing overlay computers. They are also active in the FP6 IST specific targeted research project BALTICTIME (Reinforcing eGovernment Services in Baltic States through Legal and Accountable Digital Time Stamp, Jan. 2006-Dec. 2008).

SCIENTIFIC EVENTS IN ESTONIA

In addition to the internationalization of its core research activities, CDC has also paid considerable attention to increasing its international visibility. To this end, CDC has invited foreign researchers to Estonia to give seminar talks and teach courses, to do research in Estonia. BUt CDC has also attracted high-level scientific events to the country. I'll now give a brief overview of the events that CDC has organized. Given the young age of CDC, their number is vert high.

In Oct. 2002, IoC brought to Tallinn the 14th edition of the Nordic Workshops of Programming Theory, NWPT, the programming theory forum of the Nordic countries and Estonia. NWPT had been held in Tallinn also once before, in 1997.

In April 2004, IoC organized in Tallinn the 2nd annual meeting of the APPSEM II thematic network, APPSEM 2004, together with a workshop on normalization by evaluation, NBE 2004. Beside research papers, the programme of APPSEM 2004 featured a special session about industrial applications of semantics, with invited talks by industry representatives.

In Aug. 2004, an influential summer school in functional programming took place in Tartu, organized by the Department of Computer Science of the University of Tartu. This event, the 5th International Summer School on Advanced Functional Programming, AFP 2004, was very well attended by young functional programmers from many research centres from both Europe and elsewhere.

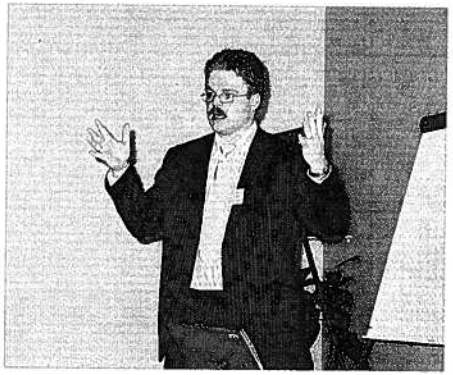
The summer of 2005 was an extraordinary summer of conferences for CDC. Never before have so many so prestigious computer science events taken place in Estonia during such a short period.

The hot summer of conferences began in May, with a major microelectronics event of a European scale. Organized by the Computer Engineering Department of TUT, the 10th IEEE European Test Symposium, ETS 2005, and the affiliated IEEE European Board Test Workshop, EBTW 2005, were held in Tallinn. IEEE (the Institute of Electrical and Electronics Engineers) is the international professional society of electrical and electronics engineers.

In July, the 20th International Conference on Automated Deduction, CADE-20 was hosted in Tallinn by the Department of Computer Science of TUT. CADE is an annual meeting of researchers in automated theorem proving that includes a world competition of theorem-proving programs. In September, a meeting in database research, the 9th East-European Conference on Advances in Databases and Information Systems, ADBIS 2005, gathered in Tallinn hosted by IoC.

And then, in September-October, three functional programming and software technology conferences took place in Tallinn consequtively as one joint event. These were the 6th International Symposium on Trends in Functional Programming, TFP 2005, the 10th ACM SIGPLAN International Conference on Functional Programming, ICFP 2005, and the 4th International Conference on Generative Programming and Component Engineering, GPCE 2005. ACM (the Association for Computing Machinery) is the world's oldest and largest society of computer professionals. ICFP is one of the three biggest conferences of ACM's Special Interest Group on Programming Languages, SIGPLAN. In Tallinn, the ICFP conference was accompanied by eight satellite workshops and a programming contest, spanning over a whole week. In connection with TFP/ICFP/GPCE, the Estonian capital was visited by almost 350 programming language researchers from all over the world. This was undoubtedly the largest computer science conference ever held here and probably also one of the largest scientific conferences overall that Estonia has seen. The scientific programme contained nearly 200 presentations. The full texts of those were published in 14 volumes, seven of them by Springer-Verlag and the ACM Press.

The joint conference in Tallinn was followed by a meeting at Kalvi of Working Group 2.8, the functional programming working group, of IFIP (the International Federation of Information Processing, another international professional society in



One of the frequent visitors of the centre is Dr Margus Veanes, our attaché to the research labs of Microsoft at Redmond.

Andreas Bogk and Hannes Mehnert, the winners of the ICFP 2005 programming contest.

computing). The meetings of IFIP's working groups differ from ordinary scientific conferences. They are closed working meetings and only members and observers of the group can attend.

The more regional 9th (Fenno-Ugric) Symposium on Programming Languages and Software Tools, SPLST 2005, and the 10th Nordic Workshop on Secure IT Systems, NordSec 2005, were held in Tartu in August, organized by the Tartu University Institute of Technology and Cybernetica AS. Of those two, SPLST took place in Estonia already for the third time.

This 2006 saw some exciting international conferences too. In July, the IoC team took 80 mathematical software technologists to Kuressaare on the island of Saaremaa for the 8th International Conference on Mathematics of Program Construction, MPC 2006, and the 11th International Conference on Algebraic Methodology and Software Technology, AMAST 2006. In Tallinn, an East-European-Japanese knowledge-based software technology conference, JCKBSE 2006, was hosted by IoC in August.

RESEARCHERS FROM ABROAD

As the Estonian universities do not yet produce enough PhDs even for their own needs, CDC has actively sought to repatriate Estonian IT-scientists working abroad and to bring to Estonia foreign postdoctoral researchers. From Oct. 2004 to June 2005, IoC hosted Dr Adam Eppendahl from Queen Mary, University London, a semanticist and robotics engineer, who is now working in Kuala Lumpur. From Sept. 2005 to Aug. 2006, the MOBIUS team at IoC benefitted from the contributions of Dr Olha Shkaravska, who came from Ludwig-Maximilians-Universität München and has by now moved on to Nijmegen.

From May 2005 to Aug. 2006, Dr Helger Lipmaa from the Helsinki University of Technology conducted cryptology research at Cybernetica and the Department of Computer Science of UT. In Sept. 2005, Dr Hellis Tamm from the University of Helsinki joined the ranks of IoC to continue her research in automata theory. In June 2005, the Department of Computer Engineering of TUT recruited Dr Gert Jervan, an Estonian computer engineer who obtained his PhD degree at Linköping.

Given that the Estonian computer science will not be self-sustainable during at least a decade, the need to repatriate researchers of Estonian origin and to attract to Estonia foreign researchers will persist.

PLANS FOR THE FUTURE

The five years of operation of the centre have been an undisputable major success. Several of the goals, especially in relation to internationalization, that felt highly risky and perhaps overambitious, have materialized in much larger dimensions than originally conceived. This shows that the computer science research activity of Estonia is vital, visible and worth of advancing.

Crucial for future successes is linking the centre to institutional graduate education. In order for the initiatives of the centre to last, we need a steady inflow of young researchers.

ESTONIA

MEMBER STATE OF NATO AND THE EU

INTERNATIONAL BUSINESS HANDBOOK
2007 – 2008

ESTONIA
MEMBER
STATE
OF NATO
AND
THE EU

INTERNATIONAL
BUSINESS
HANDBOOK

ISSN 1736-0706

www.estonianyearbook.ee

ADDRESS
P. O. BOX 3530
10507 TALLINN
ESTONIA

E-MAIL
euroinfo@neti.ee

COPYEDITING
Tricia Cornell
Kristopher Rikken
Kullo Vende

PUBLISHER
EUROINFORMER
P.O. BOX 3530
10507 TALLINN
ESTONIA

00620

This handbook is distributed in countries with which Estonia has diplomatic and business relations and is published by the non-profit organization Euroinformer in cooperation with the institutions representated in these pages.

ACKNOWLEDGEMENTS

More than 500 people contributed valuable subject matter, information and advice to the creation of this handbook. This is a partial list of those who were so gracious in their help.

Ülari Alamets
Jaan-Olle Andersoo
Andrus Ansip
Jüri Arrak
Urmas Arumäe
Jüri Arusoo
José Manuel Barroso
Tanel Bulitko
Tricia Cornell
Annikki Eigo
Jüri Engelbrecht
Anneli Entson
Ene Ergma
Paul Goble
Kadi Herkül
Tetiana Horupovych
Aita Ilja
Magnus Ilmjärv
Anne Ilves
Kärt Ilves
Toomas Hendrik Ilves
Aivar Jarne
Ain Kaljurand
Piret Kallas
Argo Kangro
Allan Kasesalu
Mari-Ann Kelam
Tunne Kelam
Ilmar Kirt
Birute Klaas
Alari Kopli
Ants Käärma
Ago Künnap
Eeva Laanemäe
Ants Laaneots
Ants Laansalu
Mart Laar
Peeter Langovits
Edmund Lanier
Marju Lauristin
Eva Lehtla
Virge Leil
Rein Loik
Kersti Luha
Lauri Luht
Meelis Maripuu
Jüri Martin
Marko Mumm
Viive Metsis
Raul Mälk
Kai Naber
Ants Noot
Mati Ormisson
Siiri Oviir
Marge Paas
Urmas Paet
Tiia Palmaru
Mai Parras
Juhan Parts
Mari Pedak
Erik Peinar
Raimo Poom
Ene Priimets
Mari Rahumägi
Priit Raudkivi
Mart Redl
Merike Riipinen
Kristopher Rikken
Andry Ruumet
Helle Ruusing
Ebba Rääts
Aarne Saar
Mart Saarma
Ain Saarna
Toomas Savi
Jüri Shehovtsov Kaido Simmermann
Uno Silberg
Tiit Sinissaar
Kalle Solba
Enn Soosaar
Peeter Tali
Asko Talu
Andres Tarand
Enn Tarto
Martin Tauer
Raivo Terve
Harri Tildo
Urmas Tsirkel
Gert Uiboaed
Raivo Uukkivi
Tarmo Uustalu
Tarvo Vaasa
Galina Variamova
Anne Veiliste
Trivimi Veiliste
Kullo Vende
Arvo Veskimets
Ago Vilo
Tiit Vähi