Number 75, October 2008

ERCIM NEWS

European Research Consortium
for Informatics and Mathematics
www.ercim.org

Special:

Safety-Critical Software

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of 10,500 copies. The printed version of ERCIM News has a production cost of €8 per copy. Subscription is currently available free of charge.

ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
Tel: +33 4 9238 5010, E-mail: contact@ercim.org
Director: Jérôme Chailloux
ISSN 0926-4981

Contributions
Contributions must be submitted to the local editor of your country

Advertising
For current advertising rates and conditions, see
http://ercim-news.ercim.org/ or contact office@ercim.org

ERCIM News online edition
The online edition is published at http://ercim-news.ercim.org/

Subscription
Subscribe to ERCIM News by:
sending email to en-subscriptions@ercim.org
or by filling out the form at the ERCIM News website:
http://ercim-news.ercim.org/

Cover photo:
An A380 flies over Hong Kong. © Airbus S.A.S.

Next issue:
January 2009, Special theme: Sensor Web.

Beware of the Computer: the Invasion of Embedded Systems

Gérard Berry,
Chief Scientist, Esterel Technologies;
Member of the ERCIM Advisory Board;
Member Académie des sciences,
Académie des technologies, and Academia Europaea.

Embedded systems are becoming ubiquitous. Most existing computers do not have a screen, a keyboard or a mouse. Instead, they are hidden in innumerable kinds of objects: automobiles, trains, aeroplanes, tractors and cranes, domestic appliances, medical devices, robots, telephones, cameras, TVs, music players, smartcards etc. Because of the flexibility and efficiency of information processing, computerized systems are progressively replacing manual, mechanical and hydraulic systems. For instance, railways and subways the world over are being gradually transformed: electronic signalling, switching and dynamic scheduling are becoming the rule. In the near future, computerized objects will communicate with each other without human intervention and will be networked. For instance, cars will talk to each other and to the road, which will itself communicate with the city in order to organize traffic. Autonomous sensors will detect forest fires or river floods. One can safely predict that there will be many more autonomous objects than human beings connected to our networks, including to the Internet.

On the hardware side, embedded systems are principally composed of sensors, actuators and Systems on Chips (SoCs) that themselves assemble heterogeneous components: processors, DSPs, video engines, radio circuits etc. On the software side, they may involve large programs running on these heterogeneous platforms. Compared to classical screen-and-keyboard computer applications, the constraints are much more stringent: efficiency (especially for power consumption), autonomy, real-time reactivity, usability, dependability, and above all, safety. All these aspects come under analysis in this issue of ERCIM News.

Until the 80s, embedded systems design was quite separate from mainstream computer design. It was mostly done by control engineers who used specific micro-controllers or programmable logic controllers (PLCs), with comparatively low-level programming languages and technology. Little dedicated research was done in the mainstream computer science community. In the early 80s, a few research groups recognized the importance of the subject and the need for specific design techniques. Three French groups introduced new formal synchronous languages (Esterel, Lustre and Signal), which led to the embedded hardware and safety-critical software design tools now sold by my company. Several groups worked on program formal verification, for which Joseph Sifakis was given the Turing Award in 2007 (along with E. Clarke and A. Emerson from the USA). In Israel, David Harel introduced Statecharts, a breakthrough graphical formalism for hierarchical state machine design, which also had a bright industrial development. At UC Berkeley, the Ptolemy and Polis groups developed new formal technology with applications ranging from circuit design to distributed control over networks. Other labs joined the movement in the 90s. It has to be noted that all the major breakthroughs were made in labs that gathered people from different areas (control theory, programming language semantics, electronic circuit design etc) and that had strong connections with industry. By nature, embedded systems design is multidisciplinary and linked to application.

Nowadays the subject pervades all other industries. It is recognized as one of the major areas of information technology, and has the biggest growth potential and the strongest technical constraints. The European Commission has clearly stated these facts and is actively promoting it. Europe currently ranks very highly, with extensive research activity and remarkable successes such as the Airbus computerized aeroplanes, automatic subways, GSM telephones and smartcards. The field boasts a number of large European cooperative groups and Networks of Excellence, including the FMICS workgroup of ERCIM, which organizes a dedicated workshop every year. It is obviously important to maintain this leader position. An essential condition is for the scientific community to gather and discuss, both internally and with industry, current problems and solutions. This precisely is one of the main roles of ERCIM, and I salute this dedicated issue of ERCIM News for its breadth and openness.

Gérard Berry

Portugal Rejoins ERCIM

by Pedro Guedes de Oliveira and João Falcão e Cunha

Portugal is back in ERCIM after more than ten years' absence. While INESC (Instituto de Engenharia de Sistemas e Computadores) was in fact a member of ERCIM back in 1991, internal problems, both financial and organizational, meant it was necessary for it to leave in 1998. It is only now with PEG – the Portuguese ERCIM Grouping – that Portugal again has a representative institution. PEG was a recent initiative to allow the country to have a wide institutional representation, thus providing a wider group of researchers and research groups with access to ERCIM.

PEG brings together IST (Engineering School of the Technical University of Lisbon), FEUP (Faculty of Engineering of the University of Porto) and INESC. IST is the largest engineering school in Portugal, with about 8000 undergraduate and 1500 graduate students, and 700 professors. FEUP has about 5000 undergraduate and 1000 graduate students and 400 professors. These two schools are not only the biggest and oldest in Portugal, but still account for about two thirds of the engineers who graduate annually in Portugal. INESC is a private nonprofit research institute, the owners of which are IST, the University of Porto and the University of Coimbra, with a substantial share belonging to Portugal Telecom. It is located in Lisbon, Coimbra and Porto, and its researchers are mostly professors from the universities mentioned.

Both IST and FEUP have several departments in which the general field of information technology is a major discipline. In both schools, IT first became a topic of research in the Departments of Electrical Engineering. Later on, autonomous Informatics Departments were created. Nevertheless, the area has many active researchers in other departments such as industrial engineering and management, mechanical engineering and mathematics.

But let us revisit history in order to clarify some aspects of the science and technology panorama in Portugal today.

In the early 90s there was a significant input of resources for science and technology, leveraged by EC funding. Large programmes directed to science (CIENCIA) and industrial development and innovation (PEDIP) helped some institutions to grow and others to come into existence. However, EC money requires that there be additional national funding to support the venture, and this caused problems for some institutions. Growing is sometimes a difficult process and can cause significant stress. Unfortunately this happened to INESC and since in these situations, attention and resources tend to be focused on the immediate and local crisis, leaving ERCIM was one of the consequences. However, the personal links were never lost and a return to ERCIM was always intended. Several attempts were made and it was always possible to count on the good will and patience of ERCIM officers.

Meanwhile, INESC itself evolved. From a monolithic country-wide institute, it was split into six autonomous organizations (three in Lisbon and one each in Porto, Coimbra and Aveiro). These institutions are independent, with their own boards, strategies and areas of expertise. Their profiles are also different, but with one exception, they maintain a mutual link through INESC by means of a share in their 'capital'. The exception is Aveiro, which became totally independent.

Sites of the PEG member institutions: From top: Faculty of Engineering of the University of Porto (FEUP), Engineering School of the Technical University of Lisbon (IST), and INESC.

By the late 90s, there was a renewed surge in Portuguese science. Since then, science indicators have increased strongly and there is a younger, active and much larger community both in universities and research centres. An institutional assessment process covering all R&D institutes and centres was started and made public. As a result and by means of a contract with the Ministry of science and Technology, a small number of centres recognized as 'very good' or 'excellent' took on the label of 'associated labs'. This meant that certain responsibilities and benefits accrued to them. The initial number of about ten labs increased to about 25, including three of the INESC institutions: INESC Porto, INESC-

ID Lisbon and INESC MN (Micro-Systems and Nanotechnologies), also in Lisbon.

It is this new INESC reality, together with IST and FEUP in Porto, that shaped PEG: an agreement was reached and a Portuguese institution was finally able to apply to ERCIM in 2007.

We are proud to have been accepted and are very positive about the benefits of joining such a European-wide organization, to which we hope we can also contribute. At a national level, PEG is not intended to be a closed consortium, and contacts and negotiations to join have started with other universities.

Please contact:
Pedro Guedes de Oliveira
PEG represenativ on the ERCIM Board of Directors
INESC Porto, Portugal
E-mail: pgo@inescporto.pt

João Falcão e Cunha
PEG representative in the ERCIM Executive Committee
University of Porto, Portugal
E-mail: jfcunha@fe.up.pt

Network of Excellence in 'Virtual Physiological Human' Research

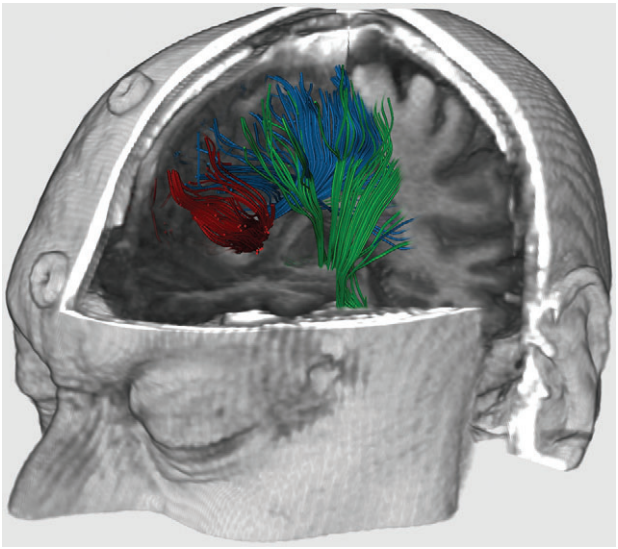
ERCIM is a partner in the Virtual Physiological Human Network of Excellence (VPH NoE), which is funded by the EU Seventh Framework programme and aims to connect and support researchers in the VPH field. In particular, the network will promote and facilitate research in the field of patient-specific computer models for personalized and predictive healthcare and ICT-based tools for modelling and simulation of human physiology and disease-related processes.

The Virtual Physiological Human (VPH) has previously been defined as "a methodological and technological framework that, once established, will enable collaborative investigation of the human body as a single complex system". As part of this initiative, the primary purpose of the network will be to function as a service to the community of VPH researchers. Its aims range from the development of a VPH toolkit and associated infrastructural resources, through integration of models and data across the various relevant levels of physiological structure and functional organization, to VPH community building and support.

VPH Toolkit

One objective of the network is to develop and promote standardized markup languages which permit interoperability of models and interoperable codes, so-called 'application support capacities'. The standards developed will need to be suitable not only within the European VPH initiative, but also on a global basis, eg via interaction with the international 'Physiome Project'. In particular, the network will develop:

- open markup language (XML) standards for describing data and models at spatial scales that range from proteins to human organs
- application-programming interfaces (APIs) for implementing these VPH standards
- workflows that use existing middleware for facilitating Grid-enabled VPH research
- Web-accessible repositories for data, models and workflows based on the VPH standards and including annotation and tutorials for non-expert biologist users
- a library of open-source computational routines and graphical user interfaces (GUIs).



Overlay of a patient's tractography (a procedure to demonstrate the neural tracts) with anatomic magnetic resonance imaging. This allows a medical expert to better visualize and localise neuronal fibres. Modelling and visualizing brain function and pathophysiology is one of the exemplar projects proposed by the ERCIM Working Group Digital Patient. © INRIA/ASCLEIPOS.

Exemplar Projects

Several partners of the network will develop exemplar projects to support interdisciplinary and integrative research, with the aim being to address specific research problems or challenges. The ERCIM Digital Patient Working Group, for example, proposes a project on modelling and visualizing brain function and pathophysiology. Other projects are concentrating on a multi-organ core model of arterial pressure and body fluids homeostasis; integrated multi-level modelling of the musculoskeletal system; fighting aneurysmal disease; and multiscale simulation and prediction of the drug safety problems related with hERG (human Ether-a-go-go Related Gene).

As one of the thirteen VPH NoE core members, ERCIM is responsible for communication and information dissemination within and beyond the network, together with Universite Libre de Bruxelles.

In addition to the core membership a general and associate membership of the VPH NoE has also been created, to

ensure wider engagement of the research community. The network currently counts 29 associated and general members. Associate and general membership is open to any interested institution, organization or company with an interest in the work of the VPH NoE, and will be subject to a collaboration agreement. A publicly accessible forum at the network's Web site offers the possibility to discuss VPH topics with the network members (see link below).

VPH NoE is actively participating in ICT-BIO 2008, the second conference on Computer Modelling and Simulation for Improving Human Health, which will be held on 23-24 October 2008 in Brussels, Belgium. The event is organized by the European Commission Directorates-General 'Information Society and Media' and 'Research', in cooperation with the US National Institutes of Health. Prior to the conference, VPH NoE is organizing a 'Concertation Meeting' with VPH-related projects of DG Information Society on 22 October 2008. This meeting is restricted to project representatives. A summary report is expected to be published by the end of November 2008.

Links:
http://www.vph-noe.eu/
http://www.vph-noe.eu/forum

Please contact:
Philippe Rohou
ERCIM Office
E-mail: philippe.rohou@ercim.org

ERCIM at ICT2008

ERCIM will be present with a booth at ICT 2008 in Lyon, France, on 25-27 November. This event is organised by the EC DG Information Society and Media. Some of the European projects managed by ERCIM or with ERCIM participation will have a booth too: Vitalas, EchoGRID, GridCOMP, EuroIndia, and Digital World Forum. 'Networking Sessions' will be held for InterLink, EchoGRID and EuroIndia.

DIGITAL WORLD FORUM

The Digital World Forum EC project will exhibit in the International Village of ICT2008. The Digital World Forum is a FP7 European project focusing on the use of ICT to leverage economic development in Africa and Latin America. Providing minimal services (health, education, business, government, etc.) to rural communities and under-privileged populations is of major importance to improve people lives, and to sustain development.

Links:
http://ec.europa.eu/information_society/events/ict/2008/
Vitalas: http://vitalas.ercim.org
EchoGRID: http://echogrid.ercim.org
GridCOMP: http://gridcomp.ercim.org/
EuroIndia: http://www.euroindia-ict.org/
Interlink: http://interlink.ics.forth.gr/
Digital World Forum: http://www.digitalworldforum.eu/

CoreGRID

CoreGRID continues as ERCIM Working Group

The CoreGRID Symposium held in Las Palmas de Gran Canaria, Spain, 25-26 August 2008 marked the end of the ERCIM-managed CoreGRID Network of Excellence funded by the European Commission. Most important, it corresponds to the re-launch of CoreGRID as the self-sustained ERCIM Working Group covering research activities on both Grid and Service Computing while maintaining the momentum of the European collaboration on Grid research.

After four years of existence, CoreGRID has indeed carved out a place for itself in the international Grid research arena. With 330 researchers from 46 European research institutions, it has become one of the largest research centres in Grid computing, encompassing a vast range of research topics such as knowledge and data management, programming models, middleware, resource management and scheduling, workflow, service infrastructures and peer-to-peer systems, just to cite a few. It has now reached its ideal objective: to become the European Grid beacon.

CoreGRID's significant and promising research results in Grid computing are largely promoted at the occasion of the CoreGRID Symposium. This successful event, jointly organized with the Euro-Par 2008 conference gathered hundred key researchers and industrials in Grid research, as well as from international projects in the field. According to Thierry Priol (INRIA) in charge of CoreGRID's scientific co-ordination and of the symposium's organization, "The objective of this event was to definitely demonstrate CoreGRID leadership in Grid research".

Having been active for four years, CoreGRID has now reached a highly visible position: it is recognized worldwide. It is really satisfying for the CoreGRID researchers to see that their work has been influential in the development of new technologies and products and has contributed to the European economy's growth. It is also an enthusiastic determination for all CoreGRID partners to continue to work together and address new research challenges under this new status of ERCIM Working Group. CoreGRID is more than ever committed to involving further industrial stakeholders in making determinant contributions to Europe's Next Generation Grid vision.

Link:
http://www.coregrid.eu/

Please contact:
Frederic Desprez
CoreGRID Working Group coordinator
INRIA, France
E-mail: Frederic.Desprez@inria.fr

Cor Baayen Award 2008 to Adam Dunkels

Adam Dunkels from SICS, Sweden, is the winner of the 2008 Cor Baayen Award for a promising young researcher in computer science and applied mathematics. Sixteen finalists competed for this award established by ERCIM in 1995 to honour the first ERCIM President Cor Baayen.

Adam Dunkels, PhD, is senior researcher at the networked embedded systems group at SICS. He received his PhD degree from Mälardalen University, Sweden, in February 2007. The title of his thesis is "Programming Memory-constrained Networked Embedded Systems".

Adam Dunkels' research is experimental computer systems research at its best. The selection committee was impressed by the combination of high-quality research results and outstanding industrial impact, showing that it is possible to have both top-tier publications and far-reaching industrial adoption of research results. Adam Dunkels has already received several prestigious awards for his work. At his young age, he is already a leading researcher in his field.

Adam Dunkels has released many of his research results as open source software that has been adopted by hundreds of companies, including Cisco, BMW, NASA, Hewlett Packard, General Electric, and ABB. His software is used in products ranging from air planes and container security systems to network routers and TV production equipment. His software is included in software development kits from leading hardware manufacturers such as Xilinx, Altera, and Analog Devices. Since 2002, Adam Dunkels has published over 40 peer-reviewed papers and one peer-reviewed, invited book chapter. Most of his papers are experimental systems research papers that involve much implementation and experimentation.

His large amount of highly influential work clearly demonstrates Adam Dunkels' outstanding abilities. He was early in the field of sensor networks, when he started working alone in 2000 at SICS, but has in the last few years built a strong, active group that has attracted many young researchers. He has participated, both as a researcher and as a research leader, in many international research projects both with academia and with industry. His open source Contiki project has attracted several researchers and industry players from Europe and the USA that now work within the project (http://www.sics.se/contiki). His first paper, for which he also was the single author, was published at the prestigious ACM MobiSys 2003. Adam Dunkels is the only European who has published three full papers at ACM SenSys, the most prestigious conference in the area of wireless sensor networks.

Adam Dunkels received the 2007 Xerox Chester Carlson science prize, the most prestigious prize for the information sciences in Sweden, for his research and the 2008 ACM EuroSys Roger Needham award for his doctoral thesis. In summary, Adam Dunkels' accomplishments shows that it is possible to both produce high-quality software systems that are widely used in the industry, and publish high-quality research results at the best venues.

Adam Dunkels (PhD), experimental computer scientist, Networked Embedded Systems group, Computer Systems Laboratory, SICS, winner of the 2008 Cor Baayen Award.
Photo: Fredrik Olsson.

2008 Finalists

According to the award rules, each institute is allowed to select up to two finalists from its country. For the 2008 Cor Baayen Award, the ERCIM institutes nominated the following sixteen finalists (listed alphabetically):

- Gianluca Antonini, Switzerland
- Joost Batenburg, The Netherlands
- Andreas Bruhn, Germany
- Augustin Chaintreau, France
- Sébastien Collette, Belgium
- Adam Dunkels, Sweden
- Pierre Genevès, France
- Georgia Koutrika, Greece
- Per Ola Kristensson, Sweden
- Santiago Ontañon, Spain
- György Ottucsák, Hungary
- Kristiaan Pelckmans, Belgium
- Mika Raento, Finland
- Inger Dybdahl Sørby, Norway
- Stefanos Zafeiriou, Greece
- Andreas Zimmermann, Germany.

The winner, Adam Dunkels, was selected by the ERCIM Executive Committee on advice from the ERCIM Advisory Committee (current members listed at http://www.ercim.org/contacts/ac.html).

More information about the Cor Baayen Award:
http://www.ercim.org/activity/cor-baayen.html

SERENE - An ERCIM Working Group on Software Engineering for Resilient Systems

by Nicolas Guelfi

The rececntly established ERCIM Working Group on Software Engineering for Resilient Systems (SERENE) is the result of a joint cooperation of the former ERCIM Working Group on Rapid Integration of Software Engineering Techniques (RISE) and the co-chairs of the conference series "Engineering Fault Tolerant Systems (EFTS). The SERENE Working Group will thus benefit from research experts coming from the RISE community on software engineering as well as from the EFTS community on fault-tolerance.

Building trustworthy systems is one of the main challenges faced by software developers, who have been concerned with dependability-related issues since the first day computer system was built and deployed. Obviously, there have been many changes since then, including in the nature of faults and failures, the complexity of systems, the services they deliver and the way society uses them. But the need to deal with various threats (such as failed components, deteriorating environments, component mismatches, human mistakes, intrusions and software bugs) is still in the core of software and system research and development. As computers are now spreading into various new domains (including the critical ones) and the complexity of modern systems is growing, achieving dependability remains central for system developers and users. Accepting that errors always happen in spite of all the efforts to eliminate faults that might cause them is in the core of dependability.

SERENE considers resilient systems as open and distributed systems that can dynamically adapt in a predictable way to unexpected events. Engineering such systems is a challenging issue still not solved. Achieving this objective is a very complex task since it implies reasoning explicitly and in a combined way, on system's functional and non-functional characteristics.

SERENE advocates that resilience should be explicitly included into traditional software engineering theories and practices and should become an integral part of all steps of software development. As current software engineering practices tend to capture only normal behavior, assuming that all abnormal situations can be removed during development, new software engineering methods and tools need to be developed to support explicit handling of abnormal situations. Moreover, every phase in the software development process needs to be enriched with phase specific resilience means.

Sub Domains of Interest:

In order not to consider all the scope of software engineering, the SERENE working group focuses on: formal, semi-formal modeling of resilience properties; frameworks and design patterns for resilience; error handling and fault handling in the software life-cycle; re-engineering for resilience component-based development and resilience; software development processes for resilience; resilience through exception handling in the software life-cycle; atomic actions; fault-tolerance; dynamic resilience mechanisms; resilience prediction; resilience Metadata; reasoning and adaptation services for improving and ensuring resilience; intelligent and adaptive approaches to engineering resilient systems; engineering of self-healing autonomic systems; dynamic reconfiguration for resilience; run-time management of resilience requirements; verification and validation of resilient systems; CASE tools; model driven engineering; software architectures for resilience.

ERCIM Working Groups are open to any researcher in the specific scientific field. Scientist interested in participating in the ERCIM WG SRENE should contact the WG coordinator.

SERENE '08

The Working Group is organising its annual workshop in cooperation with ACM SIGSOFT on 17-19 November 2008 in Newcastle upon Tyne (UK). See announcement on page 64.

Link:
http://serene.uni.lu/tiki-index.php

Please contact:
Nicolas Guelfi
SERENE Working Group coordinator
University of Luxembourg
E-mail: Nicolas.Guelfi@uni.lu

ERCIM thanks Costantino Thanos

Costantino Thanos has announced his retirement from the ERCIM Executive Committee. One of the longest serving members of the Executive Committee, Costantino was also the prime promoter of CNR and Italy's entry into ERCIM in June 1991. Over the years, Costantino has ensured that Italy has played a very active role in ERCIM initiatives, in particular as the coordinator of a number of important ERCIM projects. The best known of these is, of course, DELOS. DELOS began life as an ERCIM working group in 1995, and received funding via the 4th, 5th and 6th Framework Programmes, growing from an ERCIM Working Group and thematic network to become a Network of Excellence with more than 60 members.

ERCIM is extremely grateful to Costantino for all his efforts over the years aimed at ensuring that the research activities of the Consortium have a strong impact not just in Europe but globally.

Costantino's place on the Executive Committee will be taken by Fausto Rabitti, Head of the Networked Multimedia Information Systems Laboratory of ISTI-CNR.

FMICS 2008 - 13th International ERCIM Workshop on Formal Methods for Industrial Critical Systems

by Darren Cofer and Alessandro Fantechi

The 13th FMICS workshop was held in L'Aquila, Italy, on 15 and 16 September 2008, co-located with ASE 2008, the 23rd IEEE/ACM International Conference on Automated Software Engineering conference. The aim of the FMICS series of workshops, yearly organized by the ERCIM FMICS Working Group, is to provide a forum for researchers who are interested in the development and application of formal methods in industry. In particular, these workshops are intended to bring together scientists and practitioners who are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. These workshops also strive to promote research and development for the improvement of formal methods and tools for industrial applications.

From left: Alessandro Fantechi, Marko van Eekelen and Pedro Merino.

The topics for which contributions to FMICS 2008 were solicited included, but were not restricted to, the following:

- Design, specification, code generation and testing based on formal methods
- Verification and validation of complex, distributed, real-time systems and embedded systems
- Verification and validation methods that address shortcomings of existing methods with respect to their industrial applicability (eg, scalability and usability issues)
- Tools for the development of formal design descriptions
- Case studies and experience reports on industrial applications of formal methods, focusing on lessons learned or identification of new research directions
- Impact of the adoption of formal methods on the development process and associated costs
- Application of formal methods in standardization and industrial forums.

The workshop included six sessions of regular contributions in the areas of model checking, testing, software verification, real-time performance, and industrial case studies. There were also three invited presentations given by Steven Miller of Rockwell Collins, Rance Cleaveland of Reactive Systems Inc., and Werner Damm of OFFIS, covering the application of formal methods in the avionics and automotive industries.

In addition, a panel discussion was organized on the topic "Formal Methods in Commercial Software Development Tools." The panel included the three invited speakers, as well as researchers Mark Lawford and Pedro Merino. This session produced a lively discussion about current and foreseen applications of formal methods within model based development frameworks that include formal analysis and code generation methods for software design.

Out of the 36 contributions submitted to FMICS 2008, the Program Committee had the difficult task of selecting 14 papers for the presentation at the workshop, as well as two short presentations which served as an introduction to the panel discussion. A post-workshop proceedings volume containing revised versions of the papers presented at the workshop will be published by Springer Verlag in the Lecture Notes in Computer Science series.

A tradition of FMICS workshop is that the best presented paper receives an award from EASST, the European Association of Software Science and Technology. This year, the award was given to Marko van Eekelen from Radboud University of Nijmegen (NL) for the paper "Reentrant Readers – A Case Study Combining Model Checking with Theorem Proving," written together with Bernard van Gastel, Leonard Lensink and Sjaak Smetsers.

The award was presented by Pedro Merino, FMICS Working Group coordinator from November 2005 to November 2008, and Alessandro Fantechi, one of the chairs of the 2008 workshop and new FMICS Working Group coordinator (see photo).

More information:
http://www.dsi.unifi.it/fmics08/
http://www.inrialpes.fr/vasy/fmics

Please contact:
Alessandro Fantechi
ERCIM FMICS Working Group chair
Universita' degli Studi di Firenze, Italy
E-mail: fantechi@dsi.unifi.it

Safety-Critical Software

by Pedro Merino and Erwin Schoitsch

Each day, our lives become more dependent on 'software-intensive systems' – digital information technology embedded in our environment. This includes not only automotive devices and controls, railways, aircraft and aerospace, but also the medical devices sector, 'mobile worlds' and 'e-worlds', the 'smart' home, clothes, factories and numerous other domains. Software is the main driver for innovations in all sectors, and most of the innovative features of new products would not be possible without software. New processors and methods of processing, sensors, actuators, communications and infrastructure are enablers for a truly pervasive computing environment; that is, omnipresent but almost invisible to the user, and as such the basis for an economic push. Software plays a critical role in this context, having an impact in areas such as complexity, security and privacy in a connected world, validation, verification and certification of software-intensive systems, and maintenance of these systems over long periods. The functional safety standards of the International Electrotechnical Commission (IEC) 61508 group (generic and domain-specific standards) and the ISO 26262 standard on 'road vehicles – functional safety' currently under development, include separate software-specific parts (IEC 61508 part 3, ISO 26262 part 6).

Dependable software-intensive embedded systems are key if Europe is to remain at the forefront of digital technology. As such, they have been classified as an important research area for the European Union's Seventh Framework Programme - the main financial tool through which the EU supports research and development activities. The European Information Society Technology/Future and Emerging Technologies (IST/FET) project 'Beyond the Horizon', coordinated by ERCIM, has pointed out that pervasive or ubiquitous computing, (cognitive) intelligence and software-intensive systems together represent the most important challenge for strategic long-term research, and will have a huge impact on society and the economy. The ITEA2 (Information Technology for European Advancement) Roadmap has reached the same conclusion: that embedded systems technology is crucial for European competitiveness.

ARTEMIS (Advanced Research and Technology for Embedded Intelligence and Systems) is a strong, industry-driven European Technology Platform (ETP) that aims to establish a coherent, integrated European research and development strategy for embedded systems (http://www.artemis-office.org). As explained in their Strategic Research Area (SRA), Artemis is mainly system- and software-oriented in the area of embedded systems. The specific focus is on systems with high dependability requirements, since people tend or are forced to rely on the services delivered by such systems. Artemis has become one of the first joint undertakings, a new research organization developed for close cooperation between the EC (Unit Embedded Systems and Controls of the INFSO Directorate), national funding organizations and industry-driven technology platforms.

EPoSS, another European Technology Platform launched in July this year (see separate article by the author in this edition) focuses on the integration of smart systems, which is considered an important emerging area. The key aspects are building systems from components, a holistic, interdisciplinary approach to pervasive and ubiquitous computing, fast integration of a variety of technologies, sensors, actuators, energy autonomy and networking (http://www.smart-systems-integration.org).

Several national research programmes in Europe cover essential aspects of this theme, for example FIT-IT in Austria (BMVIT, Federal Ministry for Transport, Innovation and Technology), with topics such as embedded systems, system-on-a-chip, semantic systems and security. The programmes focus on radical innovations in these areas. In Spain, the national research programme of the Ministry of Science and Innovation includes methods with which to develop critical software in the area of information technology, with subtopics like embedded and distributed systems. In addition, the Department for Information Society gives support to the national ETPs known as PROMETEO and NESI.

The dependability aspect of software-intensive systems is of the utmost importance, and great potential has been identified among ERCIM members with respect to this. Within ERCIM, two Working Groups are active in fields related to dependable, safety-critical software, namely the ERCIM Working Group on Dependable Embedded Software-Intensive Systems (DES-WG), and the ERCIM Working Group on Formal Methods on Industrial Critical Systems (FMICS).

This special theme fits in very well with the current European framework and strategic research discussions.

The first four articles were invited by the coordinators and deal with representative topics. Gerard Holzmann (who received the ACM award for software systems for his work on the tool SPIN) and Darren Cofer (co-chair of the last FMICS workshop, see article on page 11), Michael Whalen and Steven Miller defend the advantages of formal methods in general and model checking in particular, in the critical area of space and avionics. Francesca Saglietti and Sven Söhnlein tackle the issue of software reliability, the assessment of which normally requires high testing effort. Efficient exploitation of operational evidence allows to overcome this situation for pre-developed software components in component based systems. Michael D. Harrison and José Creissac Campos discuss the human aspects to be considered when using formal methods for modelling, an aspect often underestimated in the process of developing safety-critical software.

The papers in the subsections 'Modelling and Development' and 'Validation, Verification and Standardization' represent the

ERCIM Working Group on Dependable Embedded Software-Intensive Systems

The ERCIM Working Group on Dependable Embedded Software-Intensive Systems (DES-WG) tackles all the aspects of software-driven systems that must satisfy high dependability requirements, ie 'criticality', with respect to reliability, availability, safety and security, and of course involving aspects like maintainability, survivability and resilient computing and standardization. Important system attributes to be looked at include:

- context-awareness (the functions of identifying, localizing and interacting with people and objects are not location-dependent)
- intelligence (the digital environment adapts to (moving) objects and people, learns and interacts independently, thus providing useful new services)
- natural interaction (human language, gestures, speech synthesis)
- personalization (user-centred, dynamic adaptation to changing situation and user profiles/preferences)
- dependability (time dynamics, timely responsiveness, security, safety, availability etc) and resilience (the property of a system to evolve and adapt in a changing environment, ie the persistence of dependability in the face of change).

Important subareas are hardware/software co-design, smart new sensors/actuators, continuous connectivity issues and limited resource management. Horizontal issues are dependability, system integration, software technology and critical infrastructure.

The method of work includes Working Group meetings, joint workshops with related groups and/or co-located with relevant conferences like SAFECOMP and Euromicro; the last of these occurred at SAFECOMP 2008 in Newcastle upon Tyne on September 25th, 2008.

core technologies in formal methods for critical software. They range from specification (or modelling) to automatic testing of the final code. Some methods to write specifications, like the component-based approach, or to develop the whole project, like the model-driven cycle, could make further analysis easier. The specifications are then validated by automatic verification techniques, like model checking. Finally, the code is checked with test cases. A more standard way of employing this technique is desirable in the context of standards for the development of embedded systems.

The papers under the label 'Fault Tolerance and Security' are examples of the many specific research lines that exist in the broader area of critical software reliability. Relevant examples from application areas are given for control systems development in the area of railway interlocking and nuclear power plants.

This issue also includes two announmcements related to education and training. It is clear that the quality of the software for critical systems depends on the techniques used by the software engineers. Many big companies have developed or are in the process of developing ad-hoc methods and tools for both their products and training. Several European Networks and the Artemis Platform have set up separate groups and agendas dealing with education and training, considering this a crucial issue for the widespread application of appropriate techniques and mass deployment. The European Space for Higher Education should provide a response to this demand in the new curriculum for graduates, masters and PhD programmes.

Links:
DES-WG: http://www.ercim.at
FMICS-WG: http://www.inrialpes.fr/vasy/fmics/

Please contact:
Erwin Schoitsch
Austrian Research Centers, ARC (AARIT), Austria
E-mail: erwin.schoitsch@arcs.ac.at
http://www.smart-systems.at

Pedro Merino
University of Malaga/SpaRCIM, Spain
E-mail: pedro@lcc.uma.es
http://www.lcc.uma.es/~pedro/

ERCIM Working Group on Formal Methods for Industrial Critical Systems

The ERCIM WG Formal Methods for Industrial Critical Systems (FMICS-WG) is very active in the area of foundations and applications of formal methods to complex critical systems, including both hardware and software. The FMICS WG members undertake research in languages, semantics, algorithms and tools that can help with specification, validation, verification, code generation and automation. Twelve years ago, on the original Web page of the WG, it was stated that "formal methods have been advocated as a means of increasing the reliability of systems…Nevertheless, the use of formal methods in the industry is still quite limited". Fortunately our view nowadays is different, and many industries from sectors like communication, avionics, railways, electronics and computer software are demanding tools based on formal methods or are even developing their own environments. The first two invited papers in this section are clear examples of this promising industrial scenario. The quality of papers presented in the series of annual workshops (now consolidated with LNCS publication) and several special issues in international journals (like Formal Methods in System Design or Software Tools for Technology Transfer) give a clear picture of the potential of FMICS and of the evolution that has taken place in this area. The next workshop is likely to be the most important in this series, because it is part of the Formal Methods week to be held in Eindhoven in October 2009, where we expect to meet a number of main conferences on applicable formal methods.

Software Safety and Rocket Science

by Gerard J. Holzmann

The amount of software that was used for the first moon landing in 1969 was the equivalent of perhaps 7500 lines of C code. Of course at that time the language C didn't exist – the code was written in assembly and had to fit within the 36864 words of memory that the computer in the lunar lander supported. A lot has changed since then. Today, a desktop PC can have up to a million times more memory. What is fascinating, though, is that today there are hardly any applications that require fewer lines of code than that first lunar lander. Clearly, few of these applications solve problems that are more difficult than landing a spacecraft on the moon.

All this becomes even more interesting if we consider NASA's program to return astronauts to the moon [1]. The design of the hardware for the new spacecraft is already well on its way, and so is the development of the software. My best guess for the final size of the code that will support the new landings (based on trend-lines for growth of software sizes for both manned and unmanned missions over the last few decades) would be in the range of 5 to 10 million lines of code. Yet it is clear that the problem of landing on the moon has not become a thousand times harder in the last forty years.

The software that controls a spacecraft is a good example of a safety-critical application: there is very little room for error. Does it really matter how many lines of code are written? An industry rule of thumb is that one should expect to see roughly one residual defect per one thousand lines of code, after all reviews and tests have been completed. With exceptional effort the defect rates can sometimes be pushed back further, to say one residual defect per ten thousand lines of code, but we do not know how to reliably reduce it to zero in large applications like the ones we are considering here.

A concept image of the Ares I rocket now in develpment on the launch pad at NASA's Kennedy Space Center. The software that controls a spacecraft is a good example of a safety-critical application. Image: NASA/MSFC.

If we start with 7500 lines of code, it is easy to see that we can reduce the chances of software failure reasonably effectively. Still, even the first lunar missions saw some unanticipated software issues in flight [2]. If we move to 7.5 million lines of code, even under the best of circumstances we should expect to see more residual defects during a mission. Most of these defects are likely benign and can be worked around, but there is always the chance of the one killer bug that can end a mission completely. We want to do everything we can to catch those serious defects before they catch us.

The standard approach in dealing with safety-critical systems is expressed by the acronym PDCR: prevent, detect, contain and recover. The best strategy is to prevent defects from entering the software design cycle entirely. This can be achieved by strengthening the way in which software requirements are captured, checked and tracked. Formalized requirements can also be used both for test generation and for formal design verification with tools such as Spin [3]. Another form of prevention is to look at the defects that have plagued earlier space missions. Alas, this is a richer set than we would like. These software 'lessons learned' can be captured in coding standards, ideally with machine checkable rules [4]. After all, who is going to

read through 7.5 million lines of code to find all deviations from the standard?

Our ability to detect defects as early as possible depends increasingly on tool-based verification strategies. Logic model-checking techniques [3], for instance, can be invaluable for identifying subtle design errors in multi-threaded software systems. More basic still is the use of state-of-the-art static source code analysis tools [5]. The best tools can intercept a range of common coding defects with low false positive rates.

Since it would be unwise to plan only for perfect software, the next strategy is to structure the system in such a way that the failure of one part does not jeopardize the correct functioning of unrelated parts. This defect containment strategy requires not only a well-vetted software architecture, but also coding discipline, eg modularity, and a generous use of runtime assertions and software safety margins.

Finally, when a software defect reveals itself and is successfully contained, a recovery strategy can help us find a path back to a functional system. This can be done, for instance, by replacing a failing complex module with a simpler one that was more thoroughly verifiable before flight.

Building reliable software systems is not really rocket science. It often boils down to that precious commodity that we all possess but sometimes forget to use: common sense.

Links:
[1] www.nasa.gov/missions/solarsystem/cev.html
[2] http://www.hq.nasa.gov/alsj/a11/a11.landing.html
[3] http://spinroot.com/
[4] http://spinroot.com/p10/
[5] http://spinroot.com/static/

Please contact:
Gerard J. Holzmann
NASA/JPL Laboratory for Reliable Software, Caltech, USA

Model-Checking of Safety-Critical Software for Avionics

by Darren Cofer, Michael Whalen and Steven Miller

The adoption of model-based development tools is changing the cost-benefit equation for the industrial use of formal methods. The integration of formal methods such as model checking into software development environments makes it possible to fight increasing cost and complexity with automation and rigour.

By any measure, the size and the complexity of the safety-critical software deployed in commercial and military aircraft are rising exponentially. Current verification methods will not be able to cope effectively with the software being developed for next-generation aircraft. New verification processes are being developed that augment testing with analysis techniques such as formal methods. These processes will help ensure that the advanced functionality needed in modern aircraft can be delivered at a reasonable cost and with the required level of safety.

In the past, formal methods have not been widely used in industry due to a number of barriers:

- the cost of building separate analysis models
- the difficulty of keeping these models consistent with the software design
- the use of unfamiliar notations for modeling and analysis
- the inadequacy of tools for industrial-sized problems.

The widespread use of model-based development (MBD) tools is eliminating the first three barriers. MBD refers to the use of domain-specific (usually graphical) modelling languages that can be executed in simulation before the actual system is built. The use of such modelling languages allows engineers to create a model of the system, execute it on their desktop, and automatically generate code and test cases. Furthermore, tools are now being developed to translate these design models into analysis models that can be verified by formal methods tools, with the results translated back into the original modelling notation. This process leverages the original modeling effort and allows engineers to work in familiar notations for their domain.

The fourth barrier is being removed through dramatic improvements in analysis algorithms and the steady increase in computing power readily available to engineers due to Moore's Law. The combined forces of faster algorithms and cheap hardware mean that systems that were out of reach a decade ago can now be analyzed in a matter of seconds.

Model checking is a category of formal methods that is particularly well suited to integration in MBD environments. A model checker will consider every possible combination of system input and state, and determine whether or not a specified set of properties is true. If a property is not true, the model checker will produce a counterexample showing how the property can be falsified. Model checkers are highly automated, requiring little to no user interaction, and provide the verification equivalent of exhaustive testing of the model (see Figure 1).

Automated Translation Framework

In collaboration with the University of Minnesota under NASA's Aviation Safety Program, Rockwell Collins has developed a translation framework that bridges the gap between some of the most popular industrial MBD languages and several model checkers. These translators work primarily with the Lustre formal specification lan-

guage, developed by the synchronous language research group at Verimag. Models developed in Simulink, StateFlow or SCADE are transformed into Lustre, and then successively refined and optimized through a series of configurable translation steps. Each step produces a new Lustre model that is syntactically closer to the target model checker specification language and preserves the semantics of the original model. This customized translation approach allows us to select the model checker whose capabilities are best suited to the model being analyzed, and to generate an analysis model that has been optimized to maximize the performance of the selected model checker.

Our translation framework is currently able to target eight different formal analysis tools. Most of our work has focused on the 'NuSMV' model checker developed jointly by ITC-IRST (Center for Scientific and Technological Research, Trento, Italy) and Carnegie Melon and the Prover model checker developed by Prover Technologies.

Success Stories

One of the largest and most successful applications of our tools was on the ADGS-2100, a Rockwell Collins product that provides the cockpit displays and display management logic for large commercial aircraft. The software requirements were captured as 593 properties to be checked. Verification was performed early in the design process while the design was still changing. By the end of the project, the product engineers were using the analysis tools to check properties after every design change. We were able to find and correct 98 errors in the early design models, thus improving the quality of the generated code and reducing the downstream testing costs.

In the Certification Technologies for Flight Critical Systems (CerTA FCS) project funded by the US Air Force, we have analyzed several software components of an adaptive flight control system for an unmanned aircraft. One system we analyzed was the redundancy manager which implements a triplex voting scheme for fault-tolerant sensor inputs. We performed a head-to-head comparison of verification technologies with two separate teams, one using testing and one using model checking. In evaluating the same set of system requirements, the model-checking team discovered twelve errors while the testing team discovered none. Furthermore, the model-checking evaluation required one-third less time.

Next steps

Current research is focused on further expanding the range of models where model checking can be effectively applied. Our framework can deal with integers and fixed-point data types, but new analysis methods are needed to handle larger data types, floating point numbers and nonlinear functions. Work on the class of analysis algorithms known as SMT model checkers appears promising.

Several commercial MBD environments have begun to incorporate model checkers. This should make formal analysis more widely accessible to software engineers. However, it is not yet clear whether the same power and flexibility can be provided in off-the-shelf development environments as is available in custom approaches.

The impact that the use of formal verification technology will have on software aspects of aircraft certification is a major issue. The international committee (SC-205/WG-71) responsible for the next generation of certification guidance (DO-178C) is addressing this question.

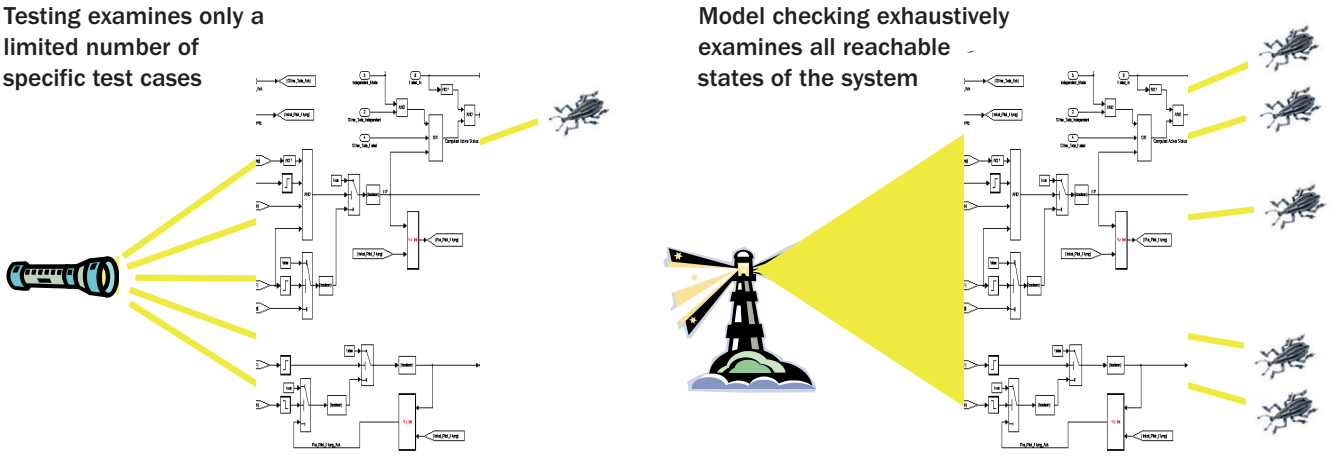


Figure 1: Model checkers.

Links:

Rockwell Collins formal methods: http://shemesh.larc.nasa.gov/fm/fm-collins-intro.html

Please contact:
Darren Cofer
Rockwell Collins
Advanced Technology Center
E-mail: ddcofer@rockwellcollins.com

Software Reliability Assessment by Statistical Analysis of Operational Experience

by Sven Söhnlein and Francesca Saglietti

Statistical testing represents a well-founded approach to the estimation of software reliability. Its major drawback - namely the prohibitive testing effort it usually requires - can be overcome by efficient exploitation of operational evidence gained with pre-developed software components and by the loss-free combination of component-specific reliability estimates.

The application of software systems in safety-critical environments requires that prescribed reliability targets are demonstrated using extremely rigorous verification and validation procedures. For such systems, statistical testing offers an adequately well-founded approach. While the effort required to apply this technique at a system level may lead to prohibitively extensive testing phases, this can be largely mitigated by the exploitation of past testing and/or operational experience gained with individual components or functionalities.

The potential usefulness of assessing the operational evidence gained with software-based applications is arousing the interest of developers in different industrial domains, especially concerning application variants based on pre-developed components. Among them, the automotive industry plays a major role; a study is being conducted on software reliability assessments tailored to its particular needs, and making use of the considerations presented in this article.

Statistical sampling theory allows - for any given confidence level β and sufficiently large amount n of correct operational runs (say n > 100) - an upper bound of the failure probability p to be derived, assuming the following testing pre-conditions are fulfilled:

- The selection of a test case does not influence the selection of further test cases.
- The execution of a test case does not influence the outcome of further test cases.
- Test cases are selected in accordance with the expected frequency of occurrence during operation.
- No failure occurs during the execution of any of the test cases selected (a more general sampling theory allows for a low number of failure observations).
- Failure probability can be expected to be approximately invariant over the input space (may be taken as realistic for software components of restricted functionality).

Under these conditions, statistical sampling theory allows the following conservative reliability estimate to be derived at confidence level β:

$$p \leq -\frac{\ln(1-\beta)}{n}$$

For example, 46 052 successfully processed runs fulfilling all five conditions would allow the reliability statement $p \leq 10^{-4}$ to be validated at a confidence level of 99%.

For the purpose of applying this theory to operational data gained with software components, the latter must be recorded, analysed and appropriately filtered. A practicable procedure for extracting relevant operational information is currently applied within an industrial research project using a software-based automatic gear control system. This is structured as follows:

1. Delimitation of scope
- identification of software functionality to be used to assess reliability
- modelling of operational runs including only input parameters relevant to the functionality considered.

2. Analysis of operational experience
- identification of memory-less suites, ie sequences of runs whose behaviour does not depend on history
- determination of frequency of functional demands during operation
- extraction of an operationally representative subset of independent operational data.

3. Assessment of operational evidence
- validation of extracted operational evidence with respect to identification of incorrect runs
- assessment of software reliability by statistical sampling theory (as illustrated above)
- if required, extension of operational experience in order to validate a prescribed reliability target.

The economics of this approach are particularly appealing in the case of pre-developed components for which a certain amount of operational data may already have been collected in the context of past applications. Once interpreted in the light of their future operational profile, the statistical analysis of such operational data yields (as illustrated above) a conservative reliability estimate for each reusable functionality considered.

For component-based systems consisting of a number of such pre-developed functionalities, the assessor is still faced with the problem of combining several component-specific reliability inequalities into one overall conservative system reliability estimate of high significance. State-of-the-art combination approaches based on mere superimposition of inequalities provoke a substantial reduction in confidence.

Ongoing work aims to improve this situation by providing sharp reliability estimates. This was recently achieved for the special case of parallel component-based architectures (see link below). Thanks to the accurate estimation, the newly developed technique allows a substantial reduction in the amount of operational experience required to demonstrate a prescribed reliability target.

Link:
http://www11.informatik.uni-erlangen.de/Forschung/Projekte/CORE/eng_index.html

Please contact:
Sven Söhnlein, Francesca Saglietti
University of Erlangen-Nuremberg, Germany
E-mail: {soehnlein, saglietti}@informatik.uni-erlangen.de

Analysing Human Aspects of Safety-Critical Software

by Michael D. Harrison and José Creissac Campos

In focusing on human system interactions, the challenge for software engineers is to build systems that allow users to carry out activities and achieve objectives effectively and safely. A well-designed system should also provide a better experience of use, reducing stress and frustration. Many methods aim to help designers to produce systems that have these characteristics. Our research is concerned with the use of formal techniques to help construct such interactive systems.

We have a number of goals in treating our subject formally. The first is to make both the identification and solution of usability problems clearly traceable and systematic. We wish to use models of interactive behaviour that make usability assumptions precise and to use tools that enable a systematic and thorough exploration of how these usability assumptions are captured in the system. An important issue in this respect is whether the models capture the relevant properties of the system without biasing the analysis inappropriately. We want to avoid focusing on problems that do not connect well with the actual use of the system. This is an ongoing topic of research and one that involves engagement with human/computer interaction specialists. We have been researching the applicability of model checking to reasoning about interaction design. This has included the development of a set of standard property templates that can be used systematically to analyse these systems. Different models can be used to characterize different features of the system. An important concern is to determine how these analyses can be performed in a complementary way.

Two modelling perspectives are important to the approach we take. The first is the interactive device. The device could be a control panel, a desktop computer, a mobile phone or a table-top interface. The important characteristic from the perspective of the analysis is that the user can be thought of as being in a dyadic relationship with it. The second is the interactive system. Here the focus of analysis is the whole system. While this might be an interactive system where the main players are the device and the user, we may also be concerned with several users immersed within a smart environment involving sensors, public devices and small handheld devices that move around as the user moves from place to place. The important characteristic here is that users are seen not as exogenous entities but rather as part of the system.

Two recent examples of analyses relate to these two levels. At the device level we have used the IVY tool (see link below) to analyse the user interfaces of a car air-conditioning system and a flight management system, and we are currently working to build a substantial repository of useful specifications. The control panels of the devices are specified in Modal Action Logic (MAL).

Standard usability properties of the device are analysed systematically by creating instances of standard templates. An important feature of this analysis is to provide representations of counter-examples that would enable a human factors specialist to use the information as a basis for constructing and analysing scenarios in which the desirable properties failed. This has enabled us to explore interactions between the different modes of the system and to explore potential inconsistencies in the design. Examples of design issues detected include the system reaching unsafe states due to user interface mode problems, or inconsistencies in the behaviour of user interface controls.

At the interactive system level we have explored smart environments. For example, we have developed models using Promela, UPPAAL and PEPA to explore the characteristics of a building containing situated displays, designed to guide people unfamiliar with the environment to their destinations. Properties of the information that flows to mobile users are explored as users change their context in such smart environments. Here formal models have been designed to help engineers to visualize usability issues in relation to the consequences of different designs. In the case of Promela we explore alternative designs in which the displays in each space can show one or a number of directions (where the directions are tagged with appropriate destinations). We have also explored different assumptions about the capacities of the different rooms and properties related to the ease with which visitors can reach their destinations. As well as exploring the information that flows to the individual, we are concerned with exploring the impact of a potential design on collective behaviours using stochastic models.

Traditional usability analysis methods based on testing and expert reviewing are challenged by the increasing complexity of new systems being built. This is particularly true in the case of safety-critical systems. We believe formal approaches provide answers by delivering rigorous and repeatable analysis in an automated manner. Tools are needed that streamline the modelling and analysis process. At the moment we are moving towards researching support for the interpretation of the analysis results by developers.

Link:
IVY tool:
http://www.di.uminho.pt/ivy

Please contact:
Michael D. Harrison
Newcastle University, UK
E-mail: Michael.Harrison@ncl.ac.uk
http://www.cs.ncl.ac.uk/people/michael.harrison

José Creissac Campos
Universidade do Minho, Braga, Portugal
E-mail: Jose.Campos@di.uminho.pt
http://www.di.uminho.pt/~jfc

Model-Driven Development of Embedded Real-Time Systems

by Alexandre David and Brian Nielsen

Model-driven development (MDD) has an enormous potential for improving verification, testing and synthesis of embedded systems. Our UPPAAL tool-suite for MDD of embedded real-time systems has recently been extended with components for automatic test generation and code synthesis. Presentation and demonstration at a European industrial conference on Systematic Testing spawned a lot of interest in these new techniques.

Our research centre was recently invited to participate in an industrial gathering on 'Systematic Testing' of embedded systems in Berlin, together with approximately eighty industrial participants from various sectors all over Europe ranging from the automotive industry, avionics, control systems and consumer electronics. It was observed that although these sectors vary in their technical intricacies and level of safety and reliability requirements, many common challenges exist. These include the ever-increasing size and complexity of software, demands for reduced time to market, and rapid changes in technology. At the same time we observed a change in attitude reflecting a decreased tolerance for errors, even towards zero-defects. This is also true of sectors beyond conventional safety-critical software. It is no longer accepted that systems will 'by nature' contain a certain number of errors and that the purpose of testing is to eliminate the worst of them. Quality systems are not allowed to misbehave, and certainly not in any way that users would notice. In combination, these developments make conventional quality assurance and testing techniques ineffective and too expensive.

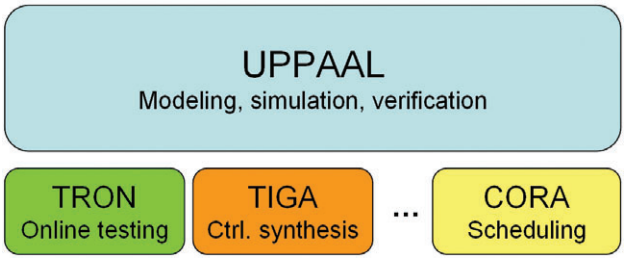


Figure 1: UPPAAL tool suite.

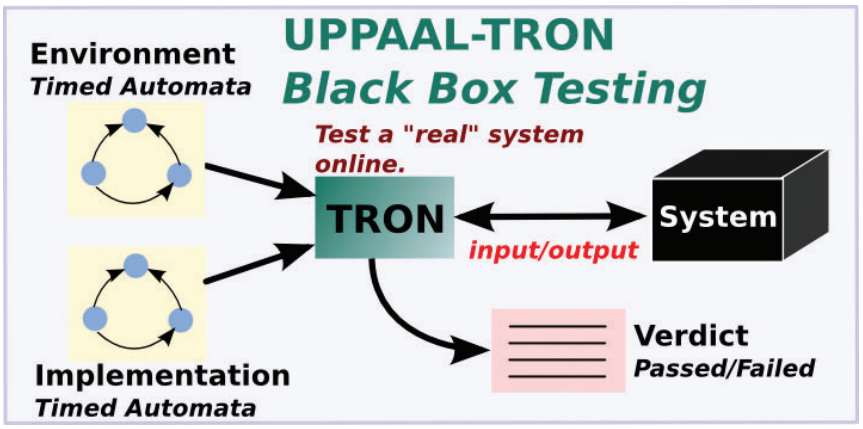


Figure 2: UPPAAL-TRON component for online testing of real-time systems.

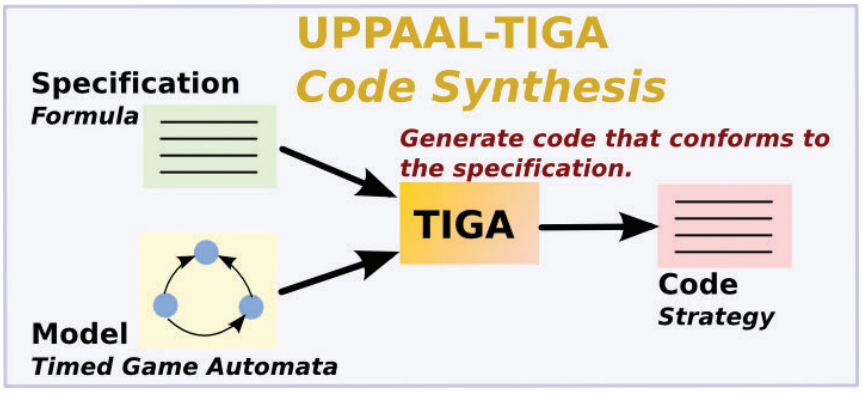


Figure 3: UPPAAL-TIGA component for controller synthesis based on timed games.

MDD is a promising approach that will contribute significantly to solving these challenges by enabling early model analysis (via simulation and model checking, for example) and design space exploration. Furthermore, model-based testing allows the test engineer to focus on the intellectual challenge of specifying and modelling the behaviour of interest at a high level of abstraction, rather than on manual test-case design, laborious scripting and manual test execution. Using model-based testing, a test generation tool generates an appropriate set of test cases and lets a test automatically execute these.

In the academic world, UPPAAL is a well-known and widely used model-checking tool for real-time systems. It is jointly developed by Aalborg University, Denmark, and Uppsala University, Sweden. The behaviour of timed systems is graphically modelled using the timed automata formalism extended with various modelling features such as concurrency and C-like functions and data structures, to make it practically expressive and user-friendly. UPPAAL contains a graphical editor and animator/simulator, and an efficient model-checker. The latter performs an exhaustive symbolic analysis of the model and provides either a proof that the model satisfies a property, or a counter-example consisting of a trace of actions and

delays exemplifying how the property is violated. It has been applied successfully to numerous industrial cases.

UPPAAL was recently extended with components for test generation and controller synthesis. This is an important step towards the vision of being an integrated tool suite for MDD of embedded systems, where the entire development lifecycle – from specification to running code – is driven by successive refinements and iterations.

UPPAAL can now handle both online and offline test generation. Specifically, UPPAAL-TRON is an online tool for black-box conformance testing of real-time systems. In an online tool, test events are generated and executed simultaneously in real time, on the physical implementation being tested. A further verdict on the observed interaction sequences may also be made online. TRON has well-defined formal semantic and correctness criteria defining how a correct implementation should behave compared to the modelled behaviour. The tool implementation extends the efficient algorithms and data structures of the model-checker engine to enable real-time testing of many real-time systems. TRON is connected to the system under test via an adaptor component (defined by the user), translating physical I/O or signalling to the abstract events of the model. TRON has for example been applied to test an embedded refrigeration controller for industrial cooling plants.

UPPAAL-TIGA is an extension of UPPAAL used to solve two-player timed games. Its main application is for controller synthesis. In a timed game automata model, actions are partitioned as being either controllable or uncontrollable. The idea is to have a controller playing with controllable actions and an environment playing with uncontrollable actions. The model-checker tries to compute a so-called winning strategy that tells the controller which actions to take (and when) to ensure that a property holds, no matter what the environment does. The tool implements a state-of-the-art algorithm that computes such strategies on the fly, ie while exploring states. The tool, in combination with Matlab-Simulink, has been successfully used to generate executable code of a climate controller for pig stables. Recently it was also applied to generate an optimal controller for a hydraulic pump.

However, despite the relative maturity of these techniques more work is needed to integrate with industrial tool-chains like Matlab-Simulink or UML-based tools, to further scale the techniques and to deal with other quantitative constraints beyond real time.

Link:
http://www.uppaal.com/

Please contact:
Brian Nielsen
Centre of Embedded Software Systems, CISS
Aalborg University, Denmark
Tel: +45 9940 8883
E-mail: bnielsen@cs.aau.dk

Quasimodo

by Brian Nielsen

Existing Model-Driven Development (MDD) tools and methods for real-time embedded systems are rather poor at handling the relevant quantitative constraints. Quasimodo (Quantitative System Properties in Model-Driven Design of Embedded Systems) is a new EU FP7 project whose main goal is to extend current MDD techniques and tools for modelling, verification, testing and code generation with the ability to satisfy these quantitative constraints.

A key characteristic of embedded systems is that they must meet a multitude of quantitative constraints. These involve the resources that a system may use (computation resources, power consumption, memory usage, communication bandwidth, costs etc), assumptions about the environment in which it operates (arrival rates, hybrid behaviour), and requirements on the services that the system must provide (timing constraints, quality of service, availability, fault tolerance etc). Existing MDD tools for real-time embedded systems are quite sophisticated in their handling of functional requirements, but their treatment of quantitative constraints is still very limited. Hence MDD will not realize its full potential in the embedded systems area unless the ability to handle quantitative properties is drastically improved.

To focus on aspects central to embedded systems such as performance, timeliness and efficient usage of resources, the models must provide quantitative information on timing, cost, data, stochastics and hybrid phenomena. A challenge is to develop notations that are expressive, have precise formal semantics, and that can be analysed efficiently by automated tools. Quasimodo mostly works with probabilistic, priced, timed game automata and looks at how to link these to industrial tool chains.

The analysis methods developed in Quasimodo include data structures for symbolic exploration of the behaviour of models, abstraction and compositionality principles that relate design models and help to control the size and complexity of the models, exploitation of approximate analysis techniques for partial analysis of very complex models and, orthogonally, optimal utilization of the given computing platform on which the algorithms are implemented.

In the implementation step, executable code running on given physical devices must be provided. While the theoretical framework of the quantitative models assumes infinitely fast hardware, infinitely precise clocks, unbounded memory and so on, real CPUs are subject to hard limitations in terms of frequency and memory size. Being able to guarantee that properties established by a

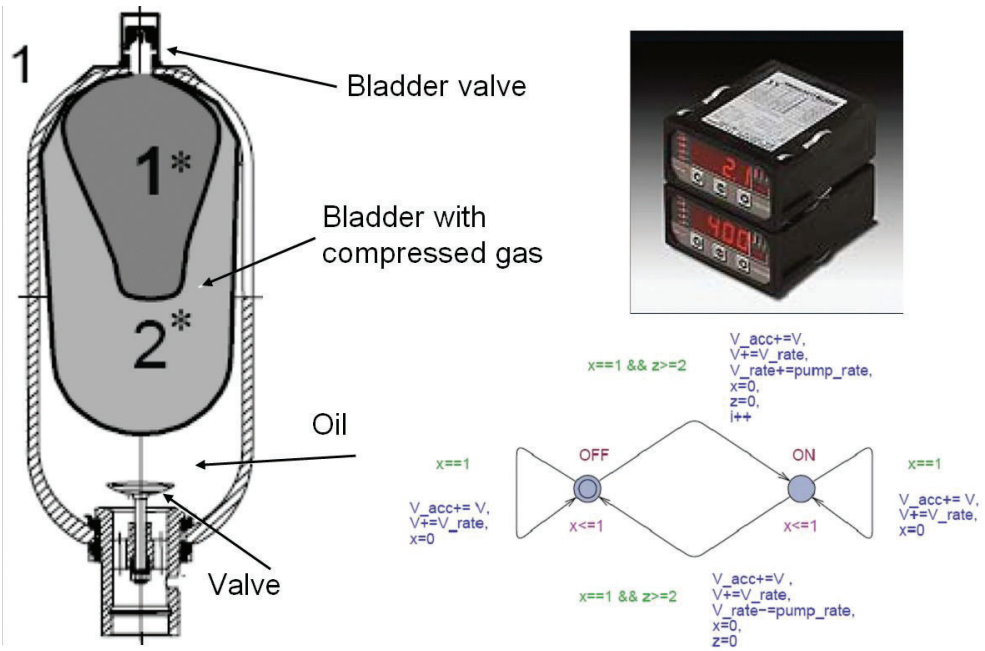


Figure 1: Accumulator bladder for a hydraulic pump (left), its electronic controller (top right), and part of the model of the control algorithm of accumulator control system (bottom right).

given model are also valid in its implementation is therefore a major challenge.

Current industrial testing is often manual and without effective automation, and consequently is rather error prone and costly: it is estimated that 30-70% of the total development cost is related to testing. Model-based testing is a novel approach to testing with significant potential to improve both cost and efficiency. We intend to extend the model-based testing technology to the setting of quantitative models, allowing generation, selection, execution and provision of coverage measures to be made. Another challenge, similar to implementation synthesis, is to develop a sound and theoretically well-founded framework and tools for testing quantitative systems when these quantities (eg timing) cannot be observed and controlled accurately.

In order to demonstrate the usefulness of our techniques, we will apply them to several complex industrial case studies and provide a collection of unique tool components to be used as plug-ins in industrial tools or tool chains like Matlab/Simulink.

One case study concerns a controller for an oil accumulator system for a hydraulic pump. The controller must maintain the gas pressure in the bladder within a safe pressure range, and should be robust against fluctuations in the energy consumption of the machine. The goal is then to find an optimal controller that minimizes the (long-term) energy consumption. Our approach consists of modelling the accumulator system as timed game automata in our game-solving tool Uppaal Tiga, and using this to automatically synthesize the optimal controller. We have produced a controller that has a 40% gain compared to classical controllers.

A second case concerns the modelling and analysis of medium-level access protocols for a specific type of sensor network. The interesting properties of the network will be modelled as probabilistic (timed) automata and linearly priced timed automata, and our model checking techniques and tools will be used to determine important system properties like collision-freeness, transmission rate and energy consumption.

Quasimodo will also model, analyse and test the application software for the Attitude Control Computer for the Hershel/Planck satellites. In particular we will evaluate the techniques for model-based online real-time testing. This work will include producing timed automata models of central aspects of both the control software and its environment, to ensure that only feasible and realistic tests are generated. Moreover, to facilitate automatic execution, test adaptation software will need to be developed to allow successful translation between abstract-model events and concrete messages to be sent/received from the system under test.

Partners in the project are Aalborg University, Denmark (coordinator); Embedded Systems Institute, the Netherlands; RWTH Aachen University, Germany; Universität des Saarlandes, Germany; Université Libre de Bruxelles, Belgium; ENS-Cachan/CNRS, France; Terma A/S, Denmark; Hydac GmbH, Germany; and Chess Beheer B.V, the Netherlands. The total budget is €2 696 000 and the project, which started in January 2008, will have a duration of 36 months.

Link:
http://www.quasimodo.aau.dk

Please contact:
Brian Nielsen
Centre of Embedded Software Systems, CISS
Aalborg University, Denmark
Tel: +45 9940 8883
E-mail: bnielsen@cs.aau.dk

From Rigorous Requirements Engineering to Formal System Design of Safety-Critical Systems

by Christophe Ponsard, Philippe Massonet, Gautier Dallons

The majority of systems that control our daily lives rely on software. Often this software is embedded in the device and remains invisible to users. While the consequences of a failure may be minor, such as failing to deliver part of the requested service, they may also be dramatic, possibly causing human injury or even fatalities (eg car crashes or train collisions). In recent years, CETIC (Centre d'Excellence en Technologies de l'Information et de la Communication) has devoted significant effort to the development of industrial methods and tools that target safety-critical software, with a specific focus on the early phase of system development.

At this level, the consequences of design flaws are the most dramatic and costly to correct. Large studies like Chaos (Standish Group) have also shown that these flaws remain the principal reason for project failure. To improve this, the following topics, illustrated in Figure 1 using the V reference model, are being investigated from a model-driven engineering perspective.

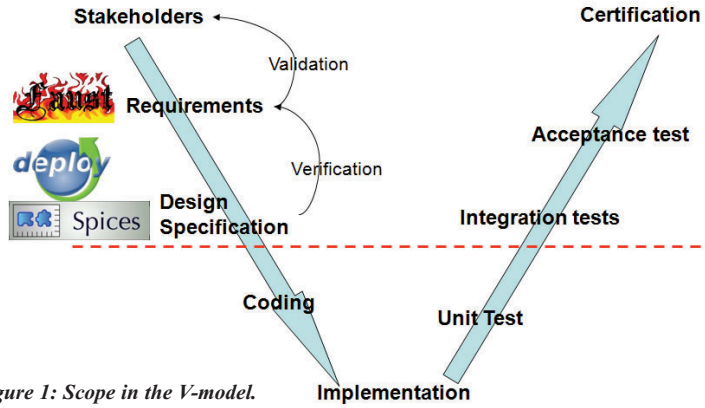


Figure 1: Scope in the V-model.

At the start of the life cycle, rigorous engineering of requirements aims to provide adequate methods and tools to capture, formalize and perform early verification and validation of critical requirements.

Immediately following this, a strong connection with industrial development methodologies is required. Good candidates are Event-B/B (a generic proof-oriented formal language) and AADL (architecture description language). At the other end of the life cycle, the certification process should support adequate techniques for a high level of assurance.

Rigorous Requirements Engineering

The aim of requirements engineering is to capture the intended behaviour of a system (including its safety properties) and the characteristics of its environment of operation. CETIC has adopted KAOS, a major goal-oriented methodology, which combines two description levels: an informal/graphical level for optimal communication and a formal layer enabling powerful reasoning about the requirements. A toolset called FAUST (Formal Analysis Using Specification Tools), which extends the semi-formal Objectiver tool, was developed to support the formal level. It provides the following main tools:

- validation of requirements, based on an animator able to generate state-based animation that can be displayed in graphical representations from the domain
- verification of the requirements, including completeness and consistency criteria, based on model-checking technology providing explanatory counter-examples
- acceptance test generation, based on the coverage of the system properties, especially those most critical.

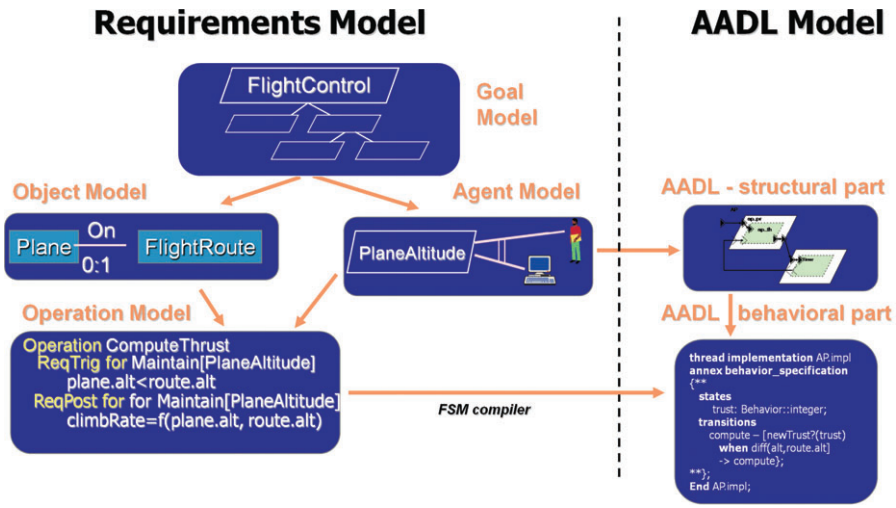


Figure 2: Requirements (KAOS) to AADL mapping.

Providing Connections with Industrial Development

Ensuring full traceability is critical in order that changes can be tracked and their impact assessed. It is therefore necessary to connect requirements models with more refined models at system and specification levels. While this connection can be loose, using simple traceability techniques, richer models enable a more elaborate and automated connection, or even the derivation of some design artefacts from the requirements level, hence reducing the effort required to produce and maintain them. This is currently being investigated in two projects with quite different approaches.

First, the FP7 DEPLOY (industrial deployment of system engineering methods providing high dependability and productivity) project aims at the industrial deployment of the Event-B method, a system-level variant of the B method. This method is quite generic and is being applied in sectors such as automotive, train, space and even e-business. Like B, it is mainly proof-based. It is supported by the RODIN (Rigorous Open Development Environment for Complex Systems) proof environment which is Eclipse-based and includes plug-ins for model-checking (ProB) and animation. Bridging the gap between requirements and Event-B models has been identified as a major topic.

Second, the ITEA2 SPICES (on Support for Predictable Integration of mission Critical Embedded Systems) project is domain-specific: it targets embedded systems and relies on a formal architectural description language called AADL. Verifications are oriented towards real-time properties and resources management. The connection with requirements models is currently developed both for the structural and dynamic parts of AADL, as shown in Figure 2. Again, Eclipse-based tools are available (TOPCASED).

Supporting Certification at High Assurances Levels

Systematic certification is required for safety-critical systems. A generic standard such as IEC-61508 defines safety integrity levels and guidelines. These generic guidelines are refined in more sector-specific standards such as space (ECSS - European Cooperation on Space Standardization), aeronautics (DO-178B) or railways (CENELEC 50126/8/9 - European Committee for Electrotechnical Standardization). Most of these also define a number of assurance levels in direct connection with risk (probability and impact).

Higher assurance levels require a more formal demonstration of correctness. Formal models, which support the rigorous development of the system, can also directly support the certification process. This means not only that the effort required for certification is not increased for such systems, but that the perception of the certification process is also improved, since it is seen as being better integrated with the system products and not as additional work. Our current work mainly targets the aeronautics domain.

Links:

KAOS: http://www.info.ucl.ac.be/~avl/ReqEng.html
FAUST: http://faust.cetic.be
SPICES: http://www.spices-itea.org
DEPLOY: http://www.deploy-project.eu
RODIN/Event-B: http://www.event-b.org/
TELECOM: http://www.skywin-telecom.be

Please contact:
Christophe Ponsard
CETIC, Belgium
Tel: +32 71 490 743
E-mail: christophe.ponsard@cetic.be

Modelling the Role of Software in the Propagation of Failures across National Critical Infrastructures

by Chris W. Johnson

In recent years, terrorist attacks, system failures and natural disasters have revealed the problems that many countries face in preparing for national civil contingencies. The diversity of critical infrastructures and the interconnections between different systems make it difficult for planners to anticipate everything. For example, the loss of power distribution networks can disrupt rail and road transportation systems. Knock-on effects can also be felt across telecommunications infrastructures as the uninterruptible power supplies (UPS) that protect mobile phone base stations fail over time. In addition, domestic water supplies are affected when pumping and treatment centres lose power.

It is difficult to underestimate the safety implications of these interdependencies. For example, Pironi, Spinucci and Paganelli describe how the Italian blackout of 2003 affected patients who relied on home parenteral nutrition systems. These individuals used electronic pumps for the overnight infusion of nutritional solutions, and the loss of power disrupted their treatment. Different devices responded in different ways, with some generating alarms and others reverting to battery power. Patients also responded in different ways, as they became worried about whether or not their systems had sufficient power to complete their treatment for that night. The blackout lasted several days across many areas of Italy. This created further problems, as stores of parenteral solution needed to be kept frozen. Other patients were placed at risk when the loss of power began to affect water treatment centres; for instance, it

became difficult to guarantee that there was no microbiological or toxic contamination in the water supplies for dialysis patients.

One area of increasing concern is the dependencies that are created by the use of digital communications systems to connect key areas of our national critical infrastructure. For example, the separation of responsibility for maintaining electricity distribution systems and for generating or marketing power has created a situation where software systems are increasingly used to monitor and respond to changing demands across the network. Infrastructure operators rely on digital communications systems to balance the complex interactions between supply and demand, as market pressures encourage large-scale power transfers between low-cost generators and remote end-users. Failures in the digital communications systems can propagate to the distribution networks and vice versa. Many commercial and government agencies have recognized these vulnerabilities and have responded, for example, by placing reliability requirements on the networks and software that support critical infrastructures. However, there is strong commercial pressure for more systems to use the public Internet. At the same time, Hurricane Katrina and the UK floods of 2007 have illustrated that it may be inappropriate to place high levels of confidence in bespoke networks.

Forensic techniques can help to identify patterns of failure across digital communications systems. For example, a number of studies have been conducted into the impact of the 2003 US-Canada blackout on Internet traffic. Abnormal Border Gateway Protocol (BGP) events indicate that 3175 networks lost connectivity. Most of these were in the New York City area. However, we are a long way from being able to conduct more predictive forms of analysis at a regional level. In particular, there are no agreed means of modelling the effects of any future power system failures on national computational infrastructures. This, in turn, makes it impossible to anticipate the secondary impact of the loss of Internet connectivity on the increasing numbers of critical systems that rely upon these networks for the exchange of operational information.

It will take many years before we can predict the knock-on effects that would arise if we were to lose significant sections of our digital communications and power distribution networks. Figure 1 illustrates the interface to a Geographical Information System (GIS) that exploits Bayesian techniques to generate failure scenarios across national critical infrastructures. This approach provides an alternative to the detailed causal modelling of infrastructure interdependencies that are created by the increasing integration of digital communications networks to support everything from food distribution to the monitoring of large-volume gas transmission. Expert judgement can be used to assess the dependent probability of a system failing given that problems have been observed in another infrastructure. Where possible these estimates can steadily be refined, with more accurate probability distributions based on partial causal models or from data obtained during previous contingencies. Further information about these techniques can be obtained from the author and on the Web site indicated below.

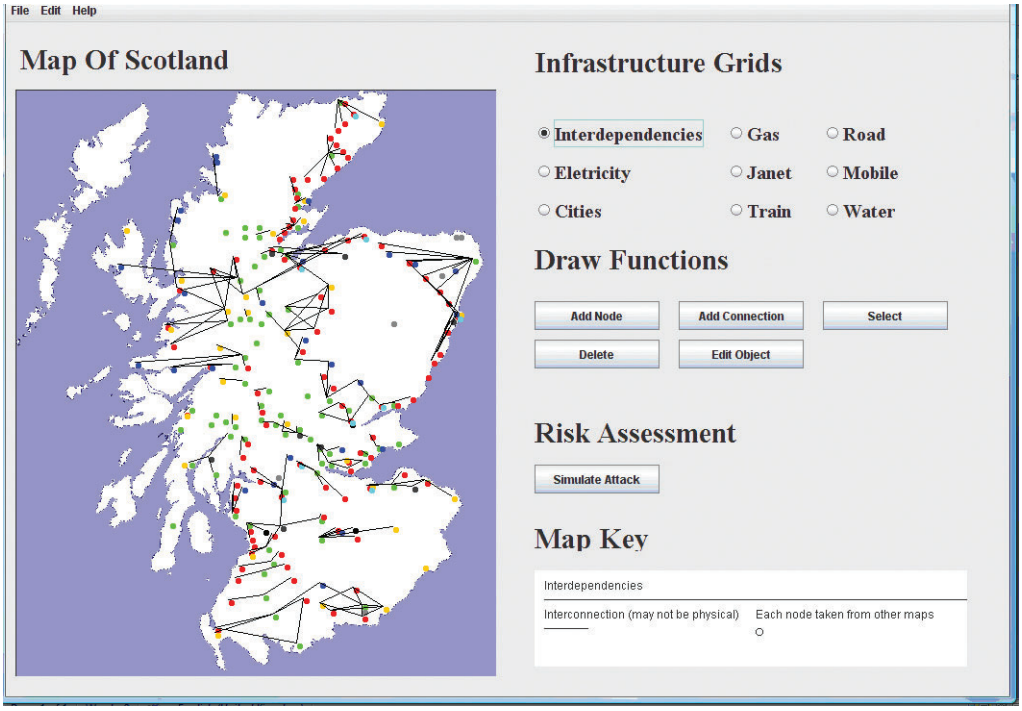


Figure 1: Infrastructure Dependencies GIS (ID-GIS).

Link:
http://www.dcs.gla.ac.uk/~johnson

Please contact:
Chris W. Johnson
University of Glasgow, UK
E-mail: Johnson@dcs.gla.ac.uk

Model-Based Development of Distributed Embedded Real-Time Systems with the DECOS Tool-Chain

by Wolfgang Herzner, Martin Schlager, György Csertan, Bernhard Huber, Thierry Le-Sergent, Erwin Schoitsch and Rupert Schlick

The increasing complexity of distributed embedded systems, as found today in cars, aeroplanes and trains, is becoming a critical cost factor in their development. In the European 'Integrated Project' DECOS (Dependable Embedded Components and Systems), an integrated, model-driven tool-chain has been developed to accompany the system development process from design to deployment.

The development of embedded systems still follows a customized design approach, resulting in rather isolated applications, the reinvention of system design concepts, and little reuse of code across application domains. For example, in modern cars each new function implies a new subsystem. While the federated approach supports fault encapsulation, it implies increases in hardware cost, weight and power consumption, and severely hampers the sharing of resources such as sensors.

The European project DECOS has developed basic domain-independent technology for moving from federated to integrated distributed architectures. This will reduce the cost of development, validation and maintenance, and will increase dependability. An integrated architecture is characterized by the inte¬gration of multiple application subsystems (so-called DASs, a DAS may consist of severeal jobs, replicated or not, distributed over a cluster of nodes, forming a single distributed computer system). When integrating (critical) subsystems, it must be guaranteed that they do not dis¬turb each other, and faults must not propagate.

DECOS is based on a settled theory, the time-triggered paradigm. It assumes the existence of a core architecture providing the following core services:

- deterministic and timely message transport
- fault-tolerant clock synchronization
- strong fault isolation
- consistent diagnosis of failing nodes.

Any core architecture providing these services (eg TTP/C, FlexRay or Time-Triggered Ethernet) can form the basis for DECOS systems. On top of these core services, DECOS provides a middleware of high-level services:

- virtual networks (VN) and gateways
- encapsulated execution environment (EEE)
- fault tolerance layer
- diagnostics.

The DECOS system architecture is depicted in Figure 1. A job represents the smallest executable software fragment of a subsystem that can sensibly be distributed – and replicated for reasons of hardware fault-tolerance.

DECOS Tool-Chain

For effective use and application, DECOS established a (prototype) tool-chain, which encompasses all phases from model to deployment. It consists of two vertical 'lanes' (Figure 2). On the left, the integrated system configuration is determined and middleware generated, while on the right, the application functionality is developed. A third lane not shown here contains the 'generic test bench'.

The DECOS tool-chain is completely model-based, ie it allows for any generated code to be finally deployed automatically from corresponding models. The specification starts with the platform-independent models (PIMs) of the application subsystems; defining their requirements with respect to performance, dependability and communication among the application tasks.

To ease the tedious task of capturing complex application PIMs, the project has developed PIM-DSE (domain-spe-

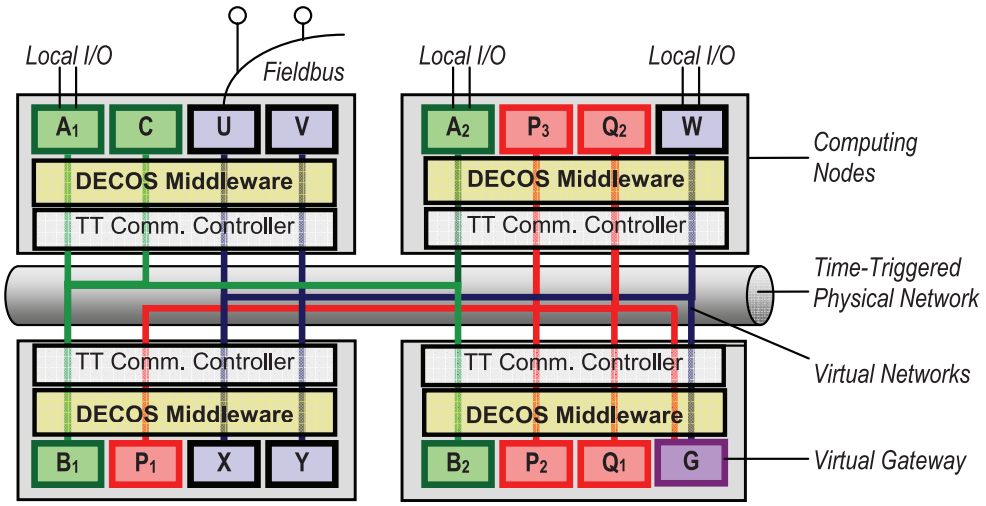


Figure 1: Example of a DECOS cluster with four nodes and three DASs (ABC, PQ, UVWXY); A, B and Q have two replicas each, P has three. G denotes a virtual gateway between the red and grey DAS.

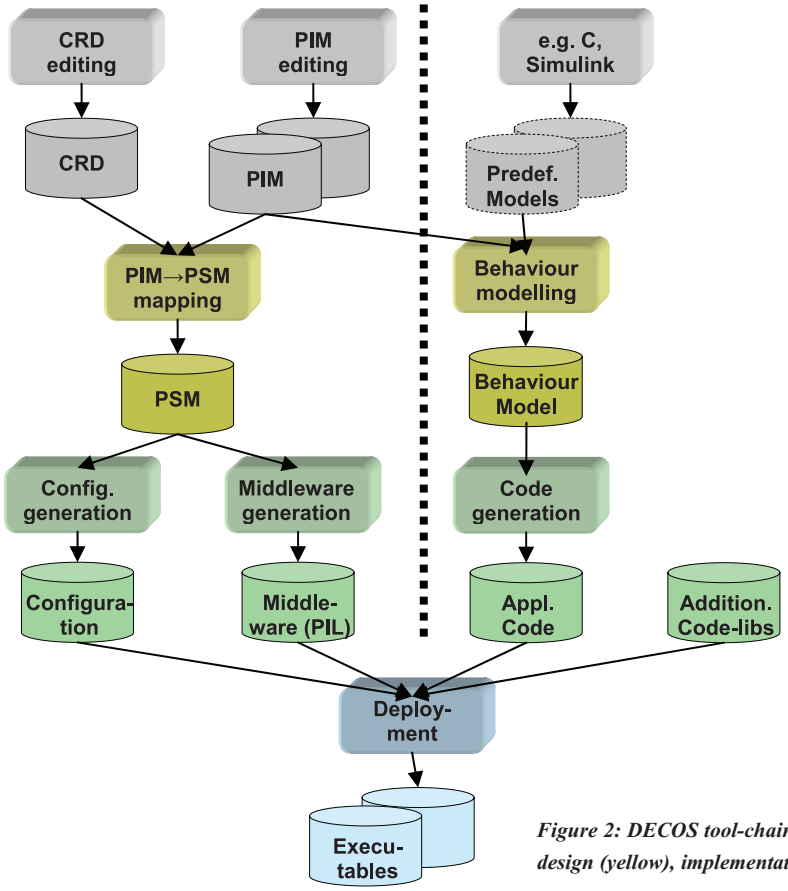


Figure 2: DECOS tool-chain. The elements address specification (grey), design (yellow), implementation (green) and installation (blue).

cific editor), which also exploits predefined PIM-patterns, and a visualization tool using GEF (Graphical Editing Framework) of Eclipse.

The purpose of the CRD (cluster resource description) is to capture characteristics of the platform for the software-hardware integration. A graphical, domain-specific modelling environment using the Generic Modelling Environment (GME) eases CRD creation.

The generation of the PSM (platform-specific model) encompasses a number of steps including PIM marking (ie adding information such as the resource requirements of jobs), feasibility checks, and the allocation process for jobs of different criticality to the (shared) hardware platform, subject to constraints of fault tolerance and real time. A PSM generation wizard supports PSM generation.

In the following steps, the middleware is generated. The platform interface layer (PIL) generated from the PSM represents the technology-neutral interface of the middleware to the application software.

The configuration data (eg for scheduling and fault tolerance) is generated by an adapted tool suite (TTplan, TTbuild) from TTTech (a DECOS partner developing time-triggered systems). This handles resource restrictions and EEE partitioning.

SCADE, a certified tool (IEC 61508, DO178B) from Esterel Technologies, is used for behaviour modelling. SCADE is based on a formally defined data flow notation. The PIMs are imported via the SCADE UML gateway, yielding empty job skeletons with correct interfaces. Simulink models are imported to SCADE via another gateway. SCADE is used for code generation; to link job codes with PIL, 'SCADE-wrappers' are generated.

Finally, in the deployment phase, all parts (application code, either generated from SCADE or written manually, generated middleware and configuration data) are put together into executables for the target platform. For the primary DECOS platform (encapsulated execution environment on TriCore TC1796), this is a single file per node that is loaded into the flash memory of the node. The makefile generator tool also takes care of (re)generating the code from the models, thus ensuring they are up to date.

A rather wide variety of tools comprise the DECOS tool-chain from model to deployment. A transformation tool VIATRA (VIsual Automated model TRAnsformations) from the Budapest University of Technology and Economics is used as the backbone for model transformations (PIM to PSM), PIL generation and domain-specific editors.

The tool chain was successfully validated by three application demonstrators from the automotive, aerospace and industrial control domains.

Links:
http://www.smart-systems.at
http://www.decos.at
http://portal.bme.hu

Please contact:
Erwin Schoitsch
Austrian Research Centers/AARIT
Tel: +43 50550 4117
E-mail: erwin.schoitsch@arcs.ac.at

Safe Systems with Software Components in SOFA 2

by Tomáš Bureš and Petr Hnětynka

Embedded devices like mobile phones, PDAs, set-top boxes and vehicular systems are now an inherent part of daily human life. However, software for these devices must meet additional requirements compared to desktop and server computers. We present the SOFA 2 component system, which is suitable for building safe and configurable applications.

As embedded devices become ubiquitous, the efficient and error-free development of the necessary software is becoming increasingly important. While a given device will operate in a very similar environment to others of its kind (eg mobile phones, consumer electronics or vehicular systems), it may differ in specific details. Typically, there exists a common core for a family of devices, and a set of optional extensions whose presence depends on the available hardware (eg the presence of Bluetooth in mobile phones, air-conditioning in cars etc) or other requirements. One approach to this situation is 'software product lines', which allows the specification of not just one system, but the whole family of systems. However it places strong requirements on the software development platform for support for the configuration of application variants.

Also commonly required of embedded software is support for functional and safety verification (a necessity for software in, for example, vehicles). This requirement is reflected in the need for a formal specification of system behaviour, verifications of the specification and so forth.

A relatively recent approach to coping with complexity, variability and safety in embedded systems is the use of component-based development (CBD), which employs well-defined components as reusable basic building blocks. It also carefully captures the dependencies and interactions between components, which helps to mitigate the complexity.

SOFA 2 (SOFtware Appliances version 2) is one representative of existing advanced approaches to component use. It was designed and developed by the Distributed Systems Research Group at Charles University in Prague. It features a modern component model and a software development platform. Among other capabilities, it provides hierarchical component composition, software connectors, dynamic architectures and formal specifications of behaviour.

SOFA 2 fully satisfies both of the above-mentioned requirements (modelling of variability and the use of formal methods to ensure safety). The former is satisfied by distinguishing three separate steps in system development: definition of components, their assembly into a final system, and system deployment. The latter requirement is satisfied by inherent usage of formal specifications and verification of component behaviour.

Development of a system in SOFA 2 is quite straightforward and is performed chiefly by composing existing components available in the SOFA 2 repository. The development process starts with the definition of the architecture of a system. Using development tools, a developer can browse the repository

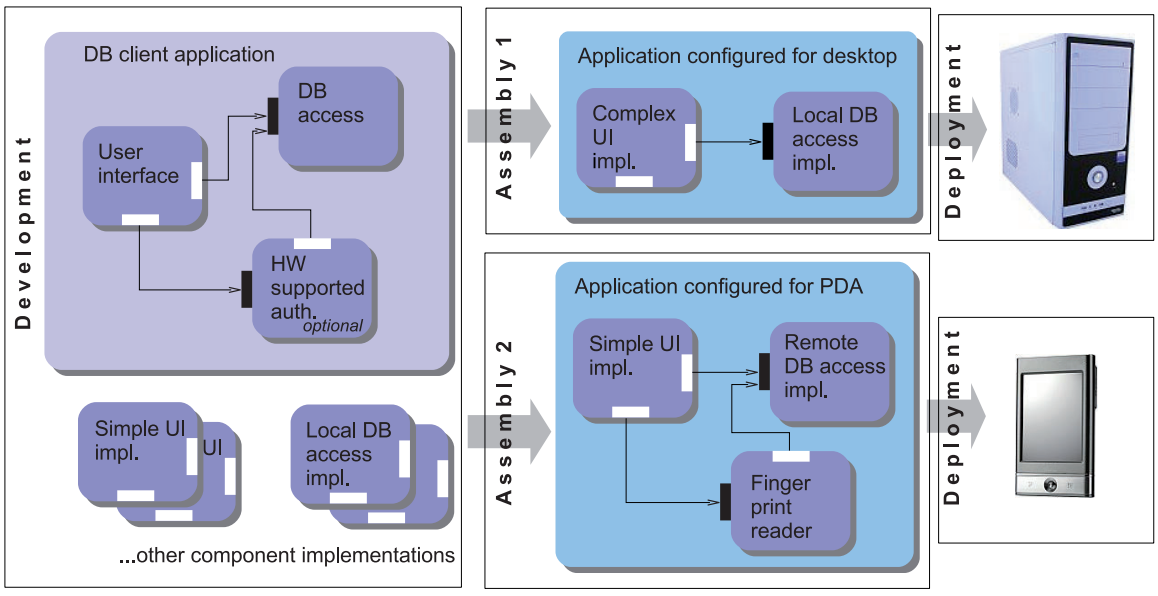


Figure 1: An example of a development process. 1. (left): a composite component implementing software for a database client, a set of basic components implementing different user interfaces, database access, etc. 2. (top right): specific assemblies for particular devices. 3. deployment of assembled software.

content and compose existing components, or build new ones. The individual components are defined by a 'component type' and 'component implementation' (which implements a particular component type). The implementation is either direct (in a programming language) or composed from other components. These 'sub-components' are themselves defined by component types.

This separation is crucial for the support of product line development. Developers can develop a set of basic (direct) components that provide building blocks of systems. For each component type, there can be several different implementations that meet specific requirements. In the assembly part of the development process, the component types in a composite component are 'refined' by chosen component implementations. This assembly process starts with the top-level component (that represents a complete system) and recursively continues down to the basic components. When the system is fully assembled, it can be deployed in a target environment. SOFA 2 inherently supports distributed systems, and the distribution is completely transparent to developers. This is achieved thanks to automatically generated software connectors that, based on final deployment, provide either local or remote calls between components.

For verification of component behaviour, SOFA 2 employs 'software behaviour protocols'. These are simple process algebra, which defines the externally observable behaviour of a component type, and are used to verify several properties. First, for the composite components, they are used to determine whether the sub-components of a composite component are composed correctly and together implement the required behaviour. For the basic components, one can verify that the required protocol is correctly implemented. In addition, the protocols can be used during development for testing whether the actual observed behaviour of a component complies with the protocol.

The decomposition of a system to its components makes it possible to perform verification of relatively large systems. This would be unfeasible if the system were viewed as a monolithic block, due principally to the exponential complexity of the verification algorithms.

SOFA 2 is implemented in Java and is freely available (together with the source code) from its Web page, which is part of the OW2 international consortium (formerly ObjectWeb). The downloadable packages contain the runtime environment for executing components, a repository for storing components, and development tools for creating components and verifying behaviour. Also available are ready-to-run examples, documentation and publications describing in detail the principles of SOFA 2 and its implementation.

Link:
SOFA 2: http://sofa.ow2.org
Distributed Systems Research Group: http://dsrg.mff.cuni.cz

Please contact:
Tomáš Bureš
Charles University Prague/CRCIM, Czech Republic
Tel: +420 221914236
E-mail: bures@dsrg.mff.cuni.cz

New Paradigms and Tools for High-Assurance Systems Modelling

by Francesco Flammini, Nicola Mazzocca and Valeria Vittorini

Modern critical computer systems are rapidly growing in complexity. As a consequence, novel frameworks are needed to support multi-paradigm modelling for the dependability evaluation of such systems. OsMoSys (Object-based multi-formalism modelling of systems) is one of the latest projects in this category, whose originality consists in supporting certain aspects of object orientation and in the model analysis.

Safety-critical computer systems are becoming increasingly large, distributed and heterogeneous. This is one of the reasons why industry best practice for high-integrity systems rarely follows the correctness-by-design paradigm. When this happens, the approach involves just small subsystems, which need to be integrated to constitute the final system. It is well known that dependability attributes correspond to properties of the whole system, meaning a system-level analysis is needed to demonstrate compliance with the required targets. In system development or verification stages, model-based dependability prediction is a fundamental aspect of critical systems engineering. Model-based approaches are needed both to demonstrate safety-related properties (eg by model-checking or theorem-proving) and to evaluate quantitative attributes (eg mean time to failure, hazard rate) of the system.

Recently, new approaches are being investigated for the software engineering of critical systems. One of these follows the paradigm introduced by the Unified Modelling Language (MDE, Model-Driven Engineering). In practice, however, this is mostly used 'as a sketch', that is to say for documentation or informal verification purposes (though a formal specification of UML for real-time systems exists and several techniques have been proposed for a comprehensive dependability analysis of UML views).

In order to master the increasing complexity of modern control systems, modular and compositional approaches have been researched by the scientific community that allow engineers to adopt the modelling formalism most appropriate to the aspect of the system to be modelled (both hardware and software). All the components are then inte-

grated into a single cohesive model of the whole system in order to evaluate system-level dependability attributes.

An attempt has been made to include these aspects in the theoretical framework of multi-paradigm modelling, which includes:

- Meta-Modelling, which is the process of modelling formalisms.
- Model Abstraction, concerned with the relationship between models at different levels of abstraction.
- Multi-Formalism modelling, concerned with the coupling of and transformation between models described in different formalisms.

The objective of the aforementioned techniques is to obtain a trade-off between ease of use, expressive power and solving efficiency. The explicit use of more formalisms requires that heterogeneous models be interconnected by means of proper operators, which can provide a mechanism for the interchange of results (connection) or the sharing of state, actions or events (composition). The art of manipulating models has only recently been extensively studied, and is sometimes given the name of model engineering (not to be confused with MDE). Model engineering also involves multi-level modelling – modelling at different abstraction levels – and multi-layer modelling – the hierarchical modelling of different aspects of the same system, possibly including non-technological ones such as man-machine interaction.

An example scheme for the multi-paradigm modelling of a complex railway control system is illustrated in Figure 1. Each subsystem (on-board, lineside and trackside) has been divided into three layers, and all the sub-models are interconnected by means of intra/inter-layer and intra/inter-subsystem composition operators.

While multi-paradigm approaches allow engineers to govern modelling complexity, this is not the only complexity that needs to be reduced. Even though multi-formalism frameworks can hide from the modeller the complexity of the solving process, issues related to efficiency must be taken into account in model evaluation and model checking when dealing with large and stiff models.

There are two main (non-contrasting) ways of tackling efficiency issues. One is related to methodological aspects (divide-et-impera/iterative approaches, model abstraction, model transformation, model folding, flow-equivalent sub-models etc), while the other is related to technological means (eg distributed multi-solution on GRID systems).

All the aforementioned needs have been taken into account in the definition of the OsMoSys Modelling Methodology (OMM), which is implemented by the OsMoSys Multi-solution Framework (OMF). OsMoSys supports meta-modelling, some aspects of object-orientation (ie inheritance and polymorphism) and is built on a workflow-based orchestration of (possibly existing) solvers and external applications in

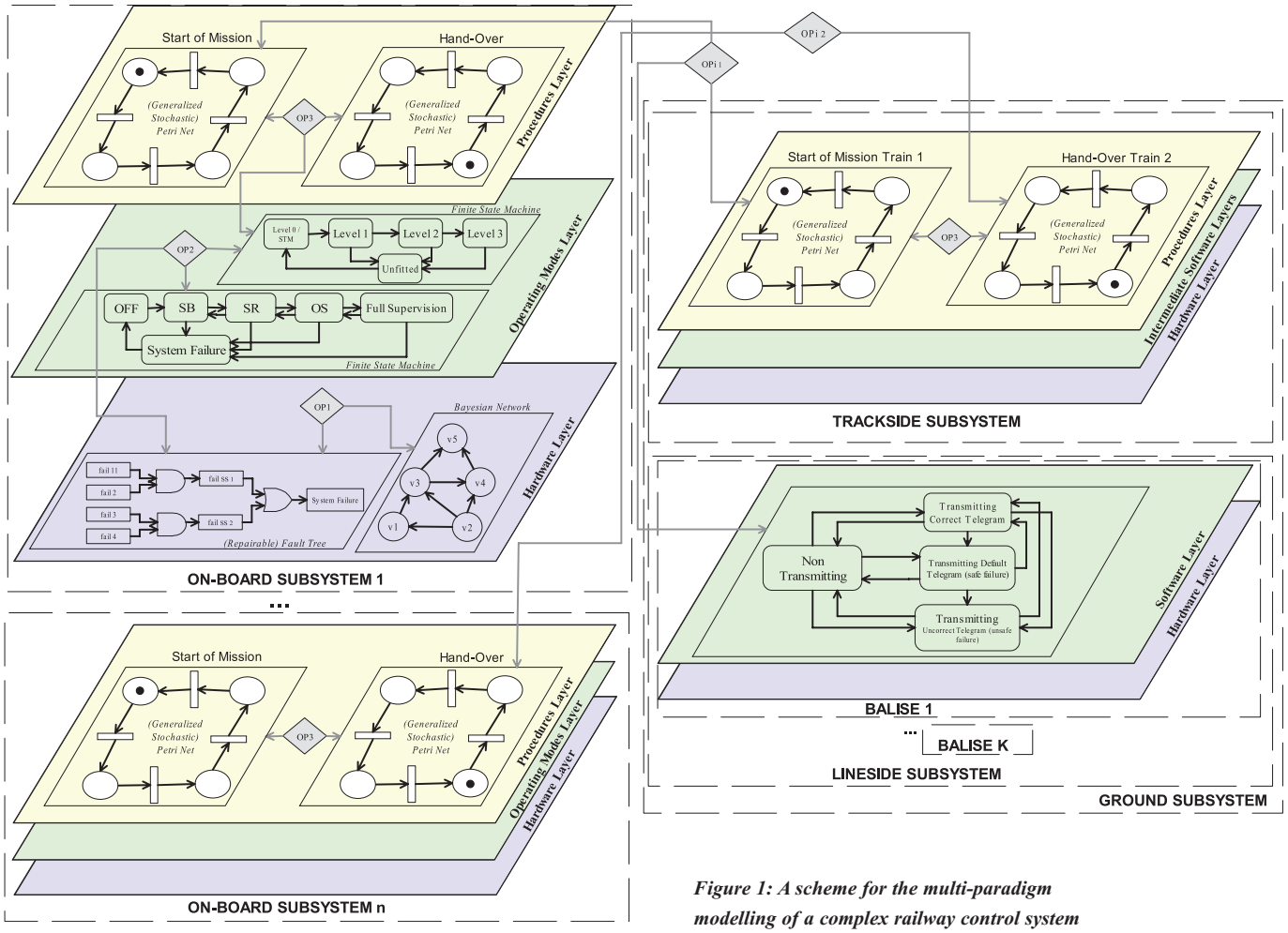


Figure 1: A scheme for the multi-paradigm modelling of a complex railway control system

order to achieve the multi-solution process. The OMF features a graphical user interface with which to draw models and retrieve results. Both formalisms and models are expressed in the OMF using the eXtended Markup Language (XML). The OMF supports both explicit and implicit multi-formalism: in the latter, a single formalism (eg repairable fault tree) is shown to the modeller, but more formal languages (eg generalized stochastic Petri nets, Bayesian networks) are used for model solution.

OsMoSys is the result of a multi-year inter-university research project, which has involved researchers from the Universities of Naples and Turin, together with engineers of Ansaldo STS (a railway systems supplier). It has been applied to the dependability (particularly maintainability, performability and safety) modelling of several critical computer-based systems, especially in the railway domain. The OMM is also suited to the modelling of complex biological systems and critical infrastructure security.

The development of the OMF is a work in progress, with additional modules becoming necessary to wrap solvers for new formalisms and to support new multi-solution paradigms. Future work will be aimed at the inclusion of additional composition operators into the framework and in the application of the OMM to new real-world case studies.

Links:
OsMoSys project page in Seclab research group Web site:
http://www.seclab.unina.it/

International Journal of Critical Computer-Based Systems:
http://www.inderscience.com/ijccbs

Please contact:
Francesco Flammini
ANSALDO STS Italy and University of Naples Federico II, Italy
E-mail: frflammi@unina.it

Testing Concurrent Software with Ants

by Francisco Chicano and Enrique Alba

Mimicking the behaviour of ants in nature can lead to the identification of subtle errors in concurrent software systems and thereby boost the efficiency of model checking.

Testing, verification and validation methods are especially important in safety-critical software, such as airplane controllers, nuclear power plant control systems, and medical tools software. Much effort has been devoted to developing and improving such methods. The main goal of all this research is to obtain a practical software tool that is able to automatically answer the following questions: (1) does my software system fulfil the specification?, and (2) if not, why not?

One method that automatically approaches both questions is model checking. This well-known and fully automatic formal procedure analyses all possible program states (explicitly or implicitly) in order to prove whether or not a given concurrent system satisfies a property like, for example, the absence of deadlocks, the absence of starvation, matching an invariant etc. The main drawback of model checking is the so-called state explosion. The memory required for the verification usually grows exponentially with the size of the system being verified. This fact limits the size of the systems that model checkers can actually verify, making the procedure impractical in large (real) software systems.

Memory poses a challenge to formal methods if we want them to be able to answer the first question, but the memory requirement can be relaxed if we focus on the second question, that is, if we focus on the search for error traces in the software. In effect, if the software system contains an error, a guided search can discover the error without having to explore the entire state space of the system. This approach is especially useful in the initial and middle stages of software development and after any maintenance modification, in which the answer to the first question is most probably "no".

In this context we recently started a new research line in our research group at the University of Málaga (Spain), using Ant Colony Optimization (ACO) algorithms to search for error traces in concurrent software systems. ACO algorithms are inspired by the foraging behaviour of real ants. These algorithms are a subclass of metaheuristic algorithms, a well-known set of techniques for finding near-optimal solutions to NP-hard optimization problems using a reasonable amount of computational resources.

In short, the core of our approach is to simulate the ants' behaviour in a graph: the state graph of the software system. The objective of the artificial ants is to find error states in the graph by employing the same mechanisms used by real ants to find food in a real environment (see Figure 1). These mechanisms include indirect information exchange through chemicals (pheromone trail) and external guidance (heuristic information). This heuristic information is automatically computed from the property being checked (eg from the temporal logic formula). Artificial ants traverse the state graph, jumping from one state to another using arcs that represent transitions in the software system. In each jump, ants must select one of several successor states using the pheromone trail (deposited by previous ants) and the heuristic information associated with them. In making this selection, ants prefer the states that suggest paths most likely to lead to an error state. When a state is found that violates the software specification, an error is reported along with its corresponding error trace (ant path).

The idea described in the previous paragraph has proven to be very effective in practice. The results show that

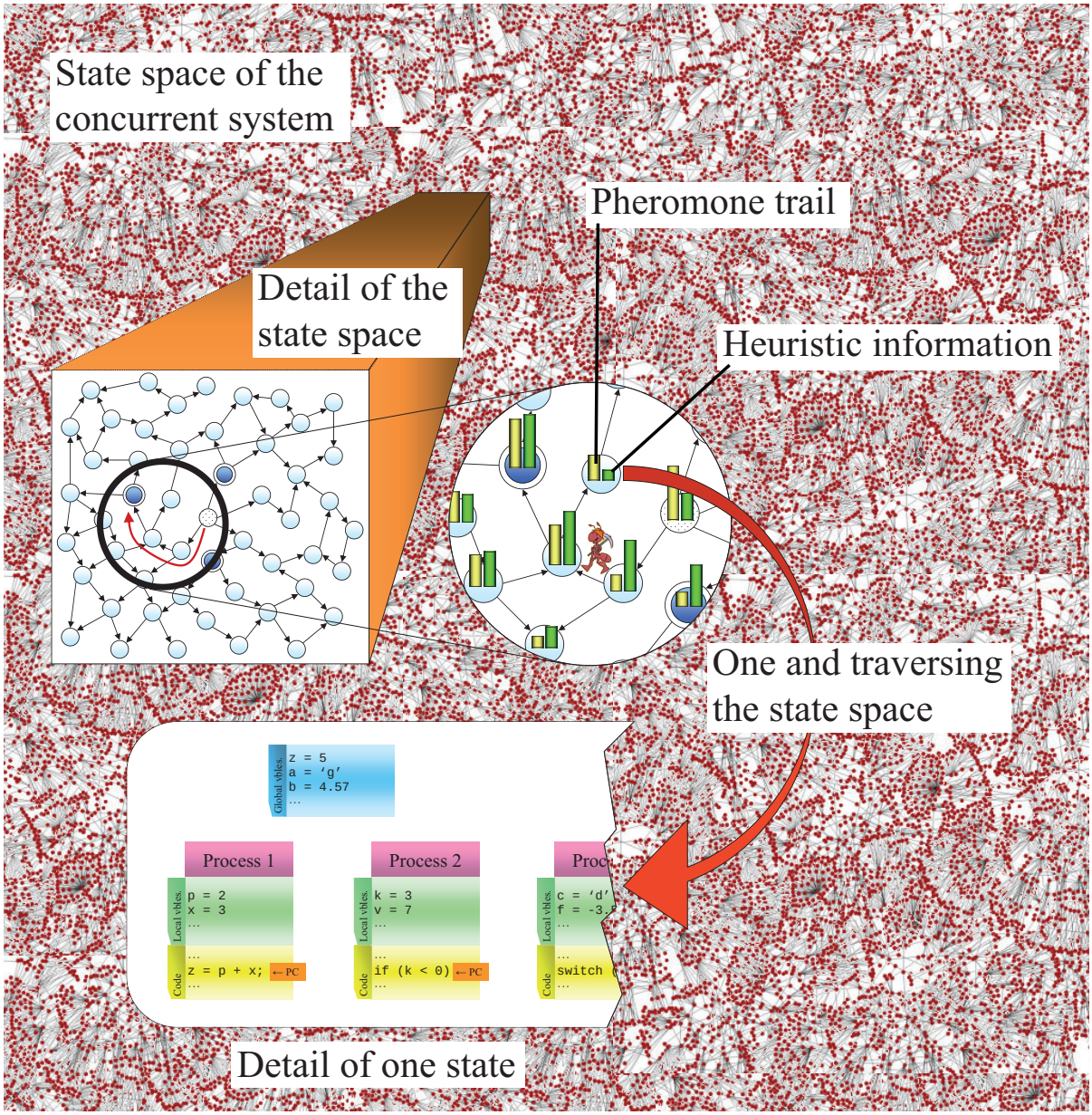


Figure 1: Artificial ants traverse the state space of the concurrent system with the goal of finding a state that violates a given property (double line circles). They jump from one state to another taking into account the amount of pheromone deposited by previous ants (yellow bar) and the heuristic information (green bar).

this approach requires a minimal amount of memory (tens of megabytes at most), even in large software systems. In fact, in software systems for which other algorithms traditionally used in the model checking community (eg Nested Depth First Search) fail due to memory constraints to find any error traces, this method succeeds. And yet low memory use is not the only advantage of ACO algorithms. As happens with real ants in nature, ACO algorithms exhibit the property of finding short paths to the target. This means short error traces, which are very useful during the software development phases, since shorter error traces can be more easily understood by the programmers. Significant advantages in memory utilization and error trace length reduction can be derived from the use of advanced algorithms like ACO rather than traditional methods, especially when the goal is to look for violations of the specification in actual software.

Encouraged by the results obtained so far, we have identified several lines to follow in the near future. First, we are studying how to integrate our proposal with software tools for automatic testing and verification (already completed for SPIN and Java PathFinder). This could save a great deal of testing time in software companies. Second, we are investigating the application of other algorithms inspired by nature, like Particle Swarm Optimization or Simulated Annealing. And last but not least, we would like to use ACO algorithms to answer the first question: does the software system fulfil the specification?

Link:
http://neo.lcc.uma.es

Please contact:
Francisco Chicano
University of Málaga, Spain
Tel: +34 95213 2815
E-mail: chicano@lcc.uma.es

Enrique Alba
University of Málaga, Spain
Tel: +34 95213 2803
E-mail: eat@lcc.uma.es

Verifying Dynamic Properties of Industrial Critical Systems Using TOPCASED/FIACRE

by Bernard Berthomieu, Hubert Garavel, Frédéric Lang and François Vernadat

The TOPCASED project (Toolkit in Open source for Critical Applications and SystEm Development) of Aerospace Valley ('Pôle de compétitivité' in aerospace activities) has developed an extensible toolbox that provides graphical environments for mission-critical systems engineering. Within this project, the FIACRE intermediate format allows the connection of several graphical models to verification tools such as CADP and TINA, as well as the factoring of expensive developments.

Mission-critical systems, such as embedded systems, aeronautic systems, computer architectures or systems on chip, are becoming increasingly complex. To tackle this complexity, systems are often designed as components that execute concurrently and communicate with one another. Models of these components can be drawn using graphical environments and then transformed into executable code.

The TOPCASED software tools target Aerospace systems. Photos: Airbus (left), ESA (right).

Components can be modelled using various graphical languages: these can be either generic, such as UML, or specific to an application domain, such as DSLs (Domain Specific Languages). Since developing dedicated tools for each language would be too expensive, it is desirable wherever possible to employ tool developments that can be reused for several languages. This is the goal of meta-modelling.

TOPCASED is a project of Aerospace Valley ('Pôle de compétitivité' in aerospace activities). Led by Airbus, TOPCASED involves 36 partners from both research (CNES, ENSEEIHT, ENSIETA, ESEO, INRIA, IRIT, LAAS-CNRS, ONERA, etc) and industry (AdaCore, AnyWare Technologies, ATOS Origin, Communication & Systems, Continental, EADS-Astrium, Rockwell & Collins, SodiFrance, Sogeti-HiTech, Sopra Group, Thales Avionics, TurboMeca, TNI-Software, etc). TOPCASED has used a meta-modelling approach to develop an open source environment based on Eclipse. Release 2.0.0 of the TOPCASED environment (18 July 2008) provides graphical tools for several languages, including UML, SysML, SAM and AADL. Its editors are already in use for several industrial projects. The software components developed in TOPCASED are integrated with the French national platform OPENEMBEDD.

As malfunctions in critical systems may have severe human or economic consequences, guaranteeing behavioural requirements and real-time constraints is a great challenge for companies. Such requirements include dynamic properties such as absence of deadlocks, safety properties (guaranteeing that unexpected events will not happen in the system) and liveness properties (guaranteeing that expected events will eventually happen in the system). Model checking tools have been developed for this. Since model-checking tools are expensive, it would be unrealistic to develop a dedicated tool for each language supported by TOPCASED. For this reason, we found it necessary to develop a common intermediate format into which all languages converge using transformations.

This intermediate format, named FIACRE ('Format Intermédiaire pour les Architectures de Composants Répartis Embarqués'), was developed within several projects including TOPCASED and OPENEMBEDD. FIACRE is based upon the NTIF format ('New Technology Intermediate Form') developed at INRIA, and the COTRE language

('Composants Temps Réel') developed within the COTRE RNTL project.

It consists of an extension of usual state machines with a rich notion of transitions borrowed from NTIF, which allows large pieces of sequential code to be embedded in each transition, resulting in compact models and an easy mapping from real languages and large applications. On top of these machines, a layer of components inspired by COTRE allows these communicating state machines to be hierarchically composed and real-time constraints to be specified. Rich behaviours can be expressed in a compositional way.

Several teams are developing transformations from graphical languages into FIACRE: transformations from AADL and SDL have been specified by IRIT and Communication & Systems, and a transformation from Signal/Polychrony has been developed at INRIA Rennes .

FIACRE is also connected to model checkers using two transformation tools. First, FLAC (Fiacre to LOTOS Adaptation Component) translates FIACRE programs into LOTOS (an ISO standard for concurrent systems specifications), which can be later checked using CADP, a verification toolbox used by the hardware industry to verify high-performance processors and architectures. Second, FRAC (FiacRe to tinA Compiler) translates FIACRE programs into the input language of the TINA toolbox (Time Petri Net Analyser, http://www.laas.fr/tina), which may be used to check dynamic properties including real-time constraints on a family of models extending Time Petri nets.

Thus, the TOPCASED and OPENEMBEDD projects are building on the efforts of two communities, model-driven software engineering and computer-aided verification, to provide industry with development tools that integrate the recent results of these communities.

Links:
http://www.inrialpes.fr/vasy/cadp
http://www.laas.fr/tina
http://www.topcased.org
http://openembedd.inria.fr

Please contact:
Frédéric Lang
INRIA Grenoble Rhône-Alpes, France
Tel: +33 4 76 61 55 11
E-mail: Frederic.Lang@inria.fr

A Component-Based Approach for the Specification and Verification of Safety-Critical Software: Application to a Platoon of Vehicles

by Jeanine Souquières

The platoon of vehicles is a mixture of distributed and embedded systems. The former are usually hard to understand and debug as they can exhibit obscure behaviours. The latter must satisfy safety/security/confidence requirements, both when standing alone and when composed together. To address these problems, we propose a component-based development approach using the CSP||B framework of well-established formal methods: B for the development of provably correct software, and CSP for Communicating Sequential Processes.

We report our experience on the specification development and verification of a real case study in the land transportation domain. It takes place in the context of the industrial CRISTAL ('Cellule de Recherche Industrielle en Systèmes de Transports Automatisés légers') and ANR (French National Research Agency) projects, which concern the development of a new type of self-service urban vehicle for the cities of tomorrow. The study is based on fleets of small electric vehicles specially designed for restricted access zones: historic city centres, airports, train stations or university campuses. These vehicles must be user-friendly and widely available, with features such as access control by smart card, simple manual control through a joystick, door-to-door services, automatic parking and recharging and a multimedia information terminal. Unfortunately, existing safety standards and guidelines are inadequate for assessing the safety and reliability of such new transportation systems, but in order to be approved and put into services, these vehicles do need to be certified.

With the development of this industrial case study, we address the importance of formal methods and their utility for highly practical applications. Our contribution mainly concerns methodological aspects for applying a component-based development approach using known results and tool supports: the model checker FDR2 and the B4Free proof tool. We show how to use the CSP||B framework to compositionally validate the specifications and prove the properties of component-based systems, with a precise verification process to ensure the consistency of a controlled machine and its generalization to a collection of controlled machines.

Case Study

A platoon is a set of autonomous vehicles that must move in convoy - ie following the path of the leader - through an intangible hooking mechanism. We consider each vehicle, named a Cristal, to be one agent in a multi-agent system. The Cristal driving system perceives information about its environment before passing acceleration instructions to its engine. In this context, the platooning problem is seen as a situated multi-agent system that evolves following the well-known Influence/Reaction model in which agents are described separately from the environment. The driving control includes both longitudinal control (maintaining an ideal distance between each vehicle) and lateral

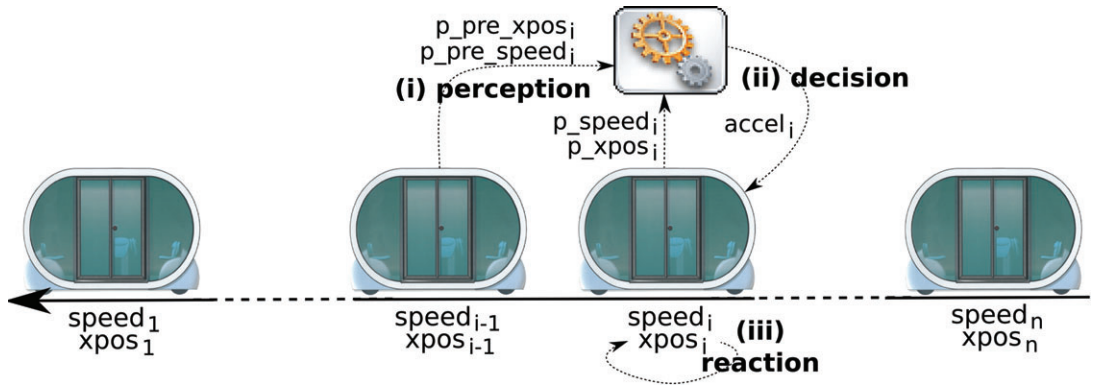


Figure 1: Driving control.

control (each vehicle should follow the track of its predecessor), as shown in Figure 1. Both controls can be studied independently.

The description of the case study involves detailing two architectural levels. We first consider a single Cristal composed of two parts, the vehicle and the driving system controlling the vehicle. Each part is itself built upon a B machine controlled by an associated CSP process. Once we identify the correct model for a single Cristal, we focus on the specification of a platoon as presented in Figure 2. We want the various Cristals to avoid 'going stale' when they move in a platoon; that is, we do not want communications in the convoy to deadlock. This might happen, for example, because a Cristal is waiting for information from its leader. In order to collect detailed information about the vehicle engine and its location, reflecting the separation of concerns within the platoon component, we allow the Cristal model to evolve. This evolution introduces new components and is achieved by adapters that connect these new components within the initial architecture.

Lessons Learned

In the proposed approach, B models describe the agents' behaviour and are seen as the smallest abstract components representing various parts of a Cristal vehicle. On the other hand, CSP is used to put these components together, to describe higher-level compounds such as a vehicle or a whole convoy and to make them communicate.

This work highlights the main drawback of the CSP||B approach. At the interface between the two models, augmented B machines corresponding to CSP controllers are not automatically generated, and to perform this task manually requires a high level of expertise. In our opinion, the user should be able to conduct all the verification steps automatically; this could be a direction for future work.

Taking the case study further, we are currently studying new properties such as non-collision, non-unhooking and non-oscillation: which of these are expressible with CSP||B, and which are tractable and verifiable? This particular perspective is related to similar work by the authors of CSP||B dealing with another kind of multi-agent system. So far our use of CSP||B for the platooning model has led us to similar conclusions. This nonetheless raises the question of what impact the expression of more complex emerging properties does have on the model.

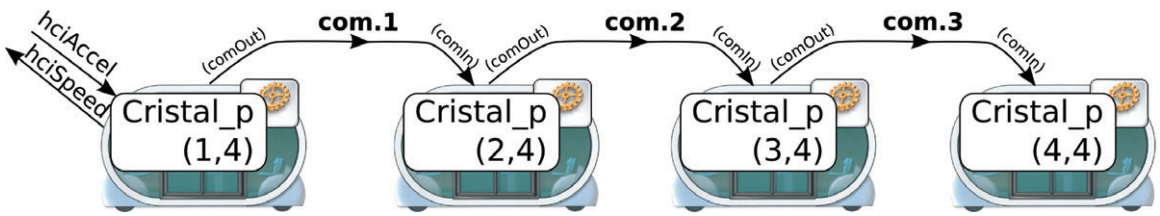
Further model development requires other refinement relations to be checked. It also includes evolution, in order to study what happens when a Cristal joins or leaves the platoon and which communication protocols must be obeyed for this to be achieved safely. We plan to take into account perturbations such as pedestrians or other vehicles.

With the evolution of the model, we illustrate a novel use of CSP||B theoretical results. Indeed, theorems about refinement or equivalences of CSP||B components are usually used to ease verification by allowing one to re-express a CSP controller into a simpler one. We used these results to show how to insert new behaviours by splitting up a controller/model compound without breaking previously verified properties.

Links:
http://tacos.loria.fr
http://www.projet-cristal.net

Please contact:
Jeanine Souquières
LORIA, Nancy-Université, France
E-mail: Jeanine.Souquieres@loria.fr

Figure 2: Specification of a platoon.



Checking and Enforcing Safety: Runtime Verification and Runtime Reflection

by Martin Leucker

Ultimately, a safety-critical software system should meet its safety requirements if it is continuously monitored, and corrected when safety violations are detected. We present Runtime Verification and Runtime Reflection as promising techniques that respectively monitor and steer safety-critical systems so that they always meet their safety requirements.

While success has been had with program analysis techniques that identify possible flaws in a program, and automatic verification techniques like model checking, there is always the risk that an a priori verified program behaves slightly differently - and faultily - at runtime. This may simply be the result of compiler bugs, or it may be due to mismatches between the expected and actual behaviour of the execution environment, say with respect to timing issues or memory behaviour. Moreover, the emerging scheme of 'software as services', in which applications are established by composing software services provided by different parties at runtime, and likewise highly adaptive systems, render the analysis of such systems prior to execution next to impossible.

Runtime verification is a lightweight verification technique that complements traditional techniques such as model checking and testing. It checks whether the current execution of a system under scrutiny satisfies or violates a given correctness property. One of the main distinguishing features of runtime verification is that – as the name suggests – it is performed at runtime. This opens up the possibility not only to detect incorrect behaviour of a software system but to react whenever misbehaviour is encountered. This is addressed within runtime reflection.

Checking whether an execution meets a correctness property is typically performed using a monitor. In its simplest form, a monitor decides whether the current execution satisfies a given correctness property by outputting either yes/true or no/false. More detailed assessments, like the probability with which a given correctness property is satisfied, can also be given.

In runtime verification, monitors are typically generated automatically from some high-level specification. As runtime verification has its roots in model checking, often some variant of linear temporal logic is employed. In practice however, one might use more readable languages such as SALT (Structured Assertion Language for Temporal Logic), which can automatically be translated to lower-level logics.

Besides checking safety properties directly using the monitors generated from them, runtime verification can also be used with partially verified systems. Such partial correctness proofs often depend on assumptions made about the behaviour of the environment. These can be easily checked using runtime verification techniques.

Runtime verification itself deals (only) with detecting whether correctness properties are violated (or satisfied). Thus, if a violation is observed, it typically does not influence or change the program's execution, say by trying to repair the observed violation.

Runtime reflection (RR) is an architecture pattern for the development of safety-critical and reliable systems. It follows the well-known FDIR scheme, which stands for Failure Detection, Identification and Recovery. The general idea of FDIR is that detecting a fault in a system does not typically identify the failure: for example, there might be different reasons why a monitored client does not follow a certain protocol, such as that it uses an old version of the protocol. If this is identified as the failure, a reconfiguration may switch the server to work with the old version of the protocol.

Within runtime reflection, the FDIR scheme is instantiated using runtime verification, diagnosis, and mitigation. The logical architecture of an application following the runtime reflection pattern is shown in Figure 1, in which we see that the monitoring layer is preceded by a logging layer. The role of the logging layer is to observe system events and to provide them in a suitable format for the monitoring layer. The logging layer can be realized either by adding code annotations within the system to be built, or as separated standalone loggers, logging for example network traffic.

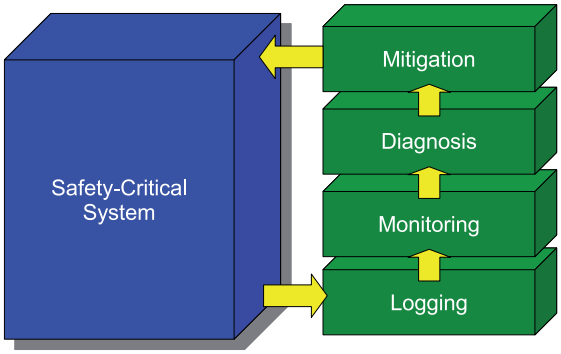


Figure 1: Logical architecture of an application following the runtime reflection.

The monitoring layer takes care of fault detection and consists of a number of monitors that observe the stream of system events provided by the logging layer. Its task is to detect the presence of faults in the system without actually affecting its behaviour. In runtime reflection, it is assumed to be implemented using runtime verification techniques. If a violation of a correctness

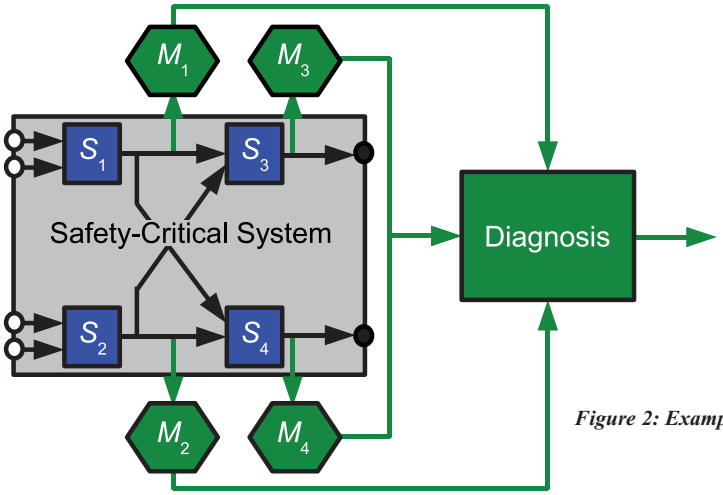


Figure 2: Example of the logical architecture of a reflective system.

property is detected in some part of the system, the generated monitors will respond with an alarm signal for subsequent diagnosis.

Following FDIR, we separate the detection of faults from the identification of failures. The diagnosis layer collects the verdicts of the distributed monitors and deduces an explanation for the current system state. For this purpose, the diagnosis layer may infer a (minimal) set of system components, which must be assumed to be faulty in order to explain the currently observed system state. The procedure is based solely upon the results of the monitors and general information on the system. Thus, the diagnostic layer is not directly communicating with the application. It can easily be implemented in a generic manner based on SAT solving techniques. An example of the logical architecture of a reflective system in shown in Figure 2.

The results of the system's diagnosis are then used to recover the system and if possible mitigate the failure. However, depending on the diagnosis and the particular failure, it may not always be possible to re-establish a particular system behaviour. In some situations, such as the occurrence of fatal errors, a recovery system may only be able to store detailed diagnosis information for offline treatment.

In cooperation with NASA JPL, runtime verification and runtime reflection techniques are currently being enhanced and tailored for application in the embedded systems world, as found for example in the automotive sector.

Links:
http://www.runtime-verification.org
http://runtime.in.tum.de

Please contact:
Martin Leucker
Technical University Munich, Germany
Tel: +49 89 289 17376
E-mail:
leucker@informatik.tu-muenchen.de

LaQuSo: Using Formal Methods for Analysis, Verification and Improvement of Safety-Critical Software

by Sjaak Smetsers and Marko van Eekelen

Due to its great complexity, it is inevitable that modern software will suffer from the presence of numerous errors. These software bugs are frequent sources of security vulnerabilities, and in safety-critical systems, they are not simply expensive annoyances: they can endanger lives. The growing demand for high availability and reliability of computer systems has led to a formal verification of such systems.

There are two principal approaches to formal verification: model checking and theorem proving.

Goal

The goal of this project is to develop a methodology for improving the quality of software by combining model checking with theorem proving such that the advantages of both methods are fully exploited. Additionally, we enhance existing or develop new techniques to support the various translations of conversions that are needed in this process.

The proposed methodology resembles what in software engineering is called code refactoring. However, the latter replaces existing code with the same functionality. It does not fix bugs; rather it improves the understandability of the code by changing its internal structure.

Approach

The proposed methodology consists of the following steps:

- the software system is analysed to identify and localize 'suspicious' parts
- a formal model of these parts is created
- the model is verified by the model checker and, if necessary, improved until it is approved by the checker
- for full reliability the model is converted into a PVS specification. PVS (Prototype Verification System) is a proof tool providing a theorem specification language and support for developing correctness proofs. This tool is used to construct a full formal proof of the system
- from this PVS specification new code is derived that replaces the original (possibly erroneous) code. In this way one obtains highly reliable code, since it corresponds directly to a fully proven formal model.

These steps are illustrated in Figure 1. We will briefly discuss each of them.

- *Identification.* Most of the time, the software system will be too large to be handled completely. Instead one must first identify the safety-critical or erroneous parts. The process of determining the parts of a program relevant to the property to be checked is often called slicing.

- *Abstraction.* There exist several techniques by which formal models can be obtained from source code. Due to the state explosion problem, a direct instruction-wise translation of source code is unsuitable. The methods for alleviating this problem can be divided into two categories: abstraction and symbolic evaluation. With abstraction, the state space is reduced by employing specific knowledge about the system in order to model only the relevant features. In the symbolic evaluation approach, the abstraction occurs at the level of the model itself. Using succinct data structures and symbolic algorithms, state information can be compressed, thus helping to keep state explosion under control.

- *Conversion.* At present, no tool exists to convert a model into a PVS specification. This is future work.

- *Code generation.* From the PVS specification, code will be generated that can replace the original (possibly faulty) code. Most theorem provers (Isabelle, Coq, PVS) are already equipped with code generators, which have in common that they produce functional code. We are currently developing a generator capable of generating code for imperative languages like Java. An interesting aspect is the extension of Java code with proof information leading to so-called proof-carrying code.

The figure has two feedback steps:

- *Counterexample.* If the attempt to check the abstract model fails, there is a counterexample which can be used directly to adjust the source code, provided that the counterexample was genuine. If the latter is not the case, our abstract model is probably too coarse and must be refined further. A technique is developed which iteratively uses spurious counter¬examples to create an abstract model with the right level of abstraction.

- *Validation.* The theorem-proving process is very sensitive to the way in which properties are formulated. In the case of state transition systems, this boils down to the right formulation of invariants. The problem with these invariants is that they are usually very subtle and therefore very difficult to specify. One may easily overlook a detail, thus making the invariant invalid. Instead of immediately checking invariants in the theorem prover itself, we propose using the model checker to quickly trace and repair flaws before we start proving the invariants. This step requires a translation of PVS properties to equivalent statements in the language of the model checker. As far we know, this has not been done before.

Applications

We apply our methodology in the context of the Laboratory for Quality Software (LaQuSo), which is a joint activity between the Technical University Eindhoven and the Radboud University Nijmegen. Within LaQuSo, successful case studies have been performed for safety-critical software components. In the near future we expect to apply our approach to cases such as control software for the Dutch 'Maeslantkering' water barrier and to programmable hardware to replace traditional components in nuclear plants

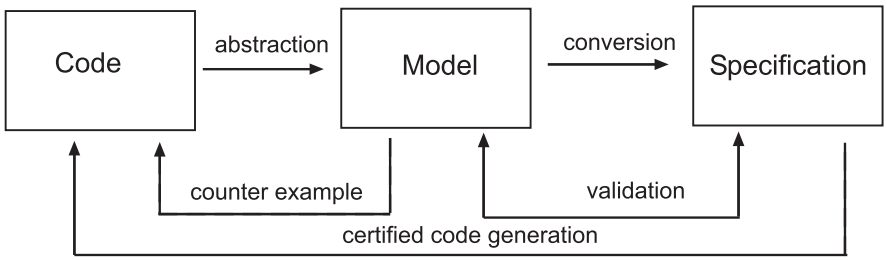


Figure 1: The LaQuSo FM based approach.

Links:
LaQuSo:
http://www.laquso.nl

Related publications:
http://www.cs.ru.nl/~marko/research/pubs

Please contact:
Marko van Eekelen
Radboud University Nijmegen, The Netherlands
Tel: +31 24 365 3410
E-mail: M.vanEekelen@cs.ru.nl

The SHADOWS Story on Implementation, Verification and Property-Guided Autonomy for Self-Healing Systems

by Marco Bakera and Tiziana Margaria

Industry-grade, large-scale software systems have an inherent need for autonomous mechanisms of adaptation. In our approach, a new game-based model-checking technique succeeds as a natural solution to the verification and adaptation task: the system becomes a player in a hostile world, and competes against any potential problems or mishaps.

Software self-healing is an emerging approach to addressing the problems of handling and fixing large complex software systems. In the European SHADOWS project on Self-Healing Approach to Designing Complex Software Systems, research institutions (University of Potsdam- D, Milano Bicocca - I, and Brno - CZ, and the IBM Research Labs in Haifa - IL) and industry (Telefonica I&D - E, Net Tech - GR, Artisys - CZ, Israel Avionics Industries - IL) are extending the state of the art for self-healing systems in several dimensions: innovative technology enables self-healing for a wide range of problems not solved elsewhere, several forms of self-healing technology are integrated into a common solution, and a model-based approach enables models of desired software behaviour to direct the self-healing process. This life-cycle support of self-healing is directly applied to industrial systems.

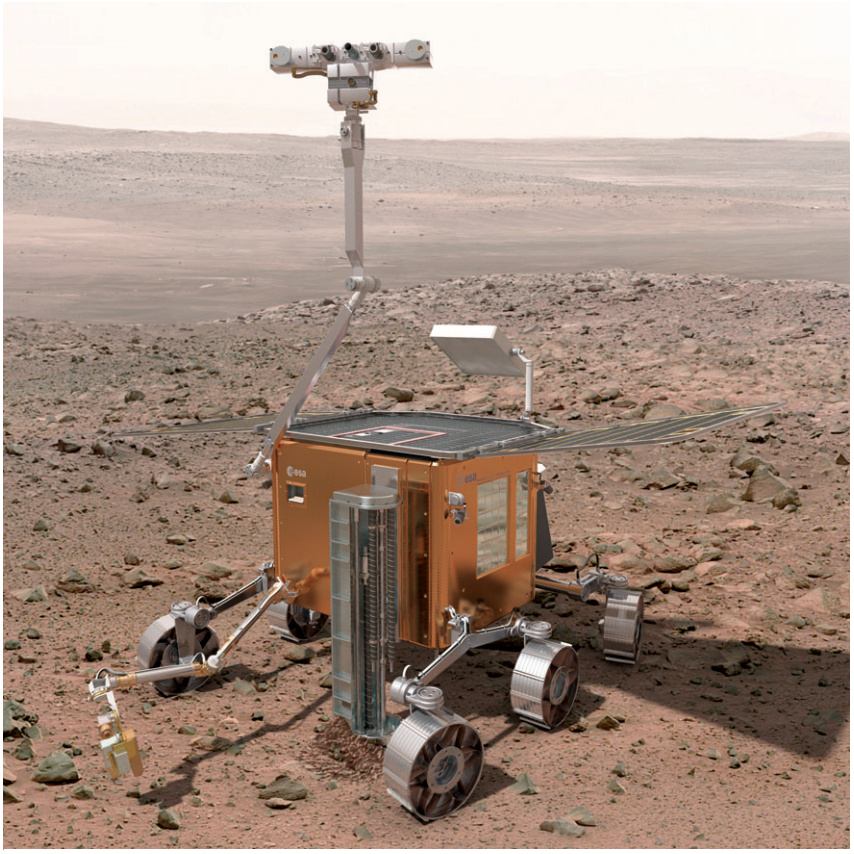


Figure 1: ExoMars rover - phase B1 concept (courtesy of ESA).

The specific formal verification and adaptation techniques we develop are based on games: they help engineers to describe, design and ensure the functional healing aspects of autonomous system behaviours. For example, once ESA's ExoMars Rover (see Figure 1) is sent on a surface mission on Mars, it must accomplish several tasks, including the acquisition of subsurface soil samples using a drill. If anything goes wrong, it should adequately adapt its behaviour: by reconfiguring itself to complete the task in a different way, choosing a different task it can still perform or at least returning to a basic safe behaviour. With our game-based model-checking approach, engineers can play with a model of the system just as they are accustomed to doing in today's common simulation approaches. However, at the same time they can express, modify and prove the behaviour of the system (the model) and the properties that are required or guaranteed. Hence, this new technique gives them verification, diagnosis and adaptation of temporal properties for free.

The central acceptance issue for the new technique, based on the GEAR model checker, is that it can be seamlessly integrated with the engineer's working experience. The robot's formal but intuitive behavioural model is created in terms of processes within the jABC framework – a mature, model-driven, service-oriented process definition platform. The jABC is also at the core of the FMICS-jETI and Bio-jETI platforms developed at Dortmund/Potsdam within the ERCIM Working Group on Formal Methods for Industrial Critical Systems (FMICS).

This modelling style closely matches the descriptions given by the ExoMars designers: actions are the atomic, Lego-like basic building blocks of the robot's behaviour, tasks are structured as flow graphs of actions, and mission plans are composed of tasks in a similar fashion. This leads to a hierarchical model of the entire behaviour.

The blend of model and property that reveals their interplay in a user-friendly way is a game played by two players: a demonic player (the hostile environment) that tries to refute the property,

and an angelic player (the system) that tries to verify it. The result of the game corresponds to the result of the property verification process. The game graphs are at the same interactive counter examples, that reveal problems between specification and implementation in an interactive way, and mathematical proofs. As with a simulator or debugger, commonly used today in integrated development environments, playing the game exposes executions of the system that violate the property. In contrast to ordinary simulation and step-by-step debugging however, which establishes understanding for only one concrete case at a time, the game provides a property-oriented exploration of the model, characterizing all the system behaviours that violate the property.

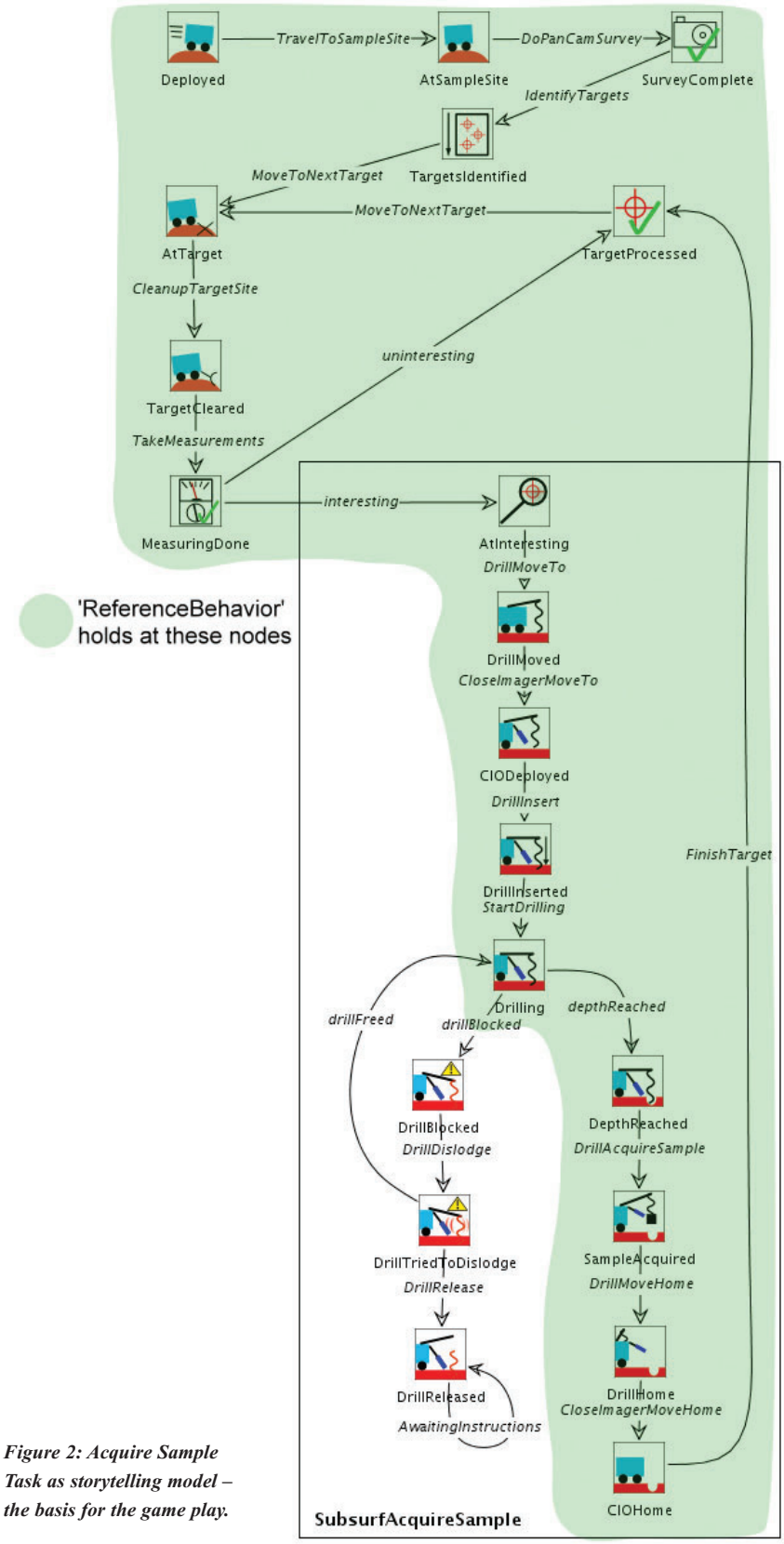


Figure 2: Acquire Sample Task as storytelling model – the basis for the game play.

Used for diagnosis, the game approach fosters a more general and concise understanding of the property violation. Used for repair, the elaborate information on the property violation obtained from the game graph helps engineers to adapt the system or the property, thus realigning them.

Whenever the system violates crucial behavioural properties, the game-based verification and adaptation approach provides a deeper and global behavioural insight into the nature of the problem. Behavioural properties become more demanding for more complex systems; adaptation properties, as addressed in SHADOWS, are very well suited to this game-based abstract exploration of alternatives driven by properties that represent correctness goals.

The quest continues: for more properties, more elaborate adaptation schemes, and for a natural inclusion of the new game-based verification in the everyday experience of engineers.

Links:
SHADOW project:
https://sysrun.haifa.il.ibm.com/shadows/
jABC:
http://jabc.cs.uni-dortmund.de/
GEAR:
http://jabc.cs.uni-dortmund.de/gear
FMICS-jETI:
http://eti.informatik.uni-dortmund.de/fmics/
Bio-jETI:
http://eti.informatik.uni-dortmund.de/biojeti/

Please contact:
For SHADOWS, FMICS-jETI and Bio-jETI:
Tiziana Margaria
University of Potsdam, Germany
Tel: +49 331 9773040
E-mail: margaria@cs.uni-potsdam.de

For jABC and GEAR:
Bernhard Steffen
TU Dortmund, Germany
Tel: +49 231 755 5801
E-mail: steffen@cs.tu-dortmund.de

Test Coverage Analysis and Preservation for Requirements-Based Testing of Safety-Critical Systems

by Raimund Kirner and Susanne Kandl

The testing process for safety-critical systems is usually evaluated with code coverage criteria such as MC/DC (Modified Condition/Decision Coverage) defined in the standard DO-178B, Software Considerations in Airborne Systems and Equipment Certification (a de-facto standard for certifying software in the civil avionic domain). For requirements-based testing techniques we work on coverage metrics that are defined on a higher level of program representation (eg on the requirements), and that are independent of a specific implementation. For that purpose we analyse the relationship between existing definitions for structural requirement-coverage metrics and structural code-coverage metrics. In addition, we work on techniques that preserve structural code-coverage between different program-representation levels.

We work on requirements-based testing following the two-step approach of the DO-178B for testing a safety-critical system (see Figure 1). Test cases are generated from the requirements until all requirements are covered (inner dotted loop in the figure). Then the structural code coverage is determined. If the coverage is insufficient, additional test cases are generated (outer dotted loop in the figure). The aim is to achieve full requirement coverage, ie toverify that all requirements are correct and fully cover the intended system behaviour.

Formal Requirements as a Program Implementation

The informal requirements given by the software specification are the primary source of information for the software developer implementing the system. The requirements are also used to derive the test suite for testing purposes. To enable the automatic systematic test-case generation, the informal requirements are specified as formal requirements using an appropriate specification language, eg based on temporal logic.

We consider formal requirements to be another implementation of the specification. The logical conjunction of all the formal requirements should summarize the software behaviour. In fact, formalizing the requirements together with the original software implementation is an example of n-version programming. Treating the formal requirements as a program implementation, we work on defining requirement-coverage metrics as structural coverage criteria. These structural coverage metrics will be used to guide the test-data generation to derive a test suite. As an inherent property of n-version programming, the logical structure of the formal requirements and the program code may be different, thus the achieved structural code coverage at the program code must be analysed empirically.

Structural Code Coverage

Structural code coverage is a class of coverage metrics often used to reason about the sufficiency of a given test suite. A variety of metrics exists, including statement coverage, decision coverage etc. In the safety-critical domain, one established structural coverage metric is the modified condition/decision coverage (MC/DC). The basic idea of MC/DC is to test whether each condition of a decision can independently control the outcome of the decision (ie without changing the outcome of the other decision's conditions).

The terms condition and decision refer to the structure of the source code. At the machine-code level there is no grouping of conditions into decisions, which means that the condition coverage of source code is equivalent to branch coverage at machine code. At higher abstraction levels, notions like model coverage are used. At model level, structural coverage is used in a rather ad hoc fashion, without having established definitions as they are common for source-code level.

Within the project SECCO (Sustaining Entire Code-Coverage on Code Optimization), we work on the mapping and preservation of structural code coverage between the different program representation levels. As shown in Figure 2, the implementation is done in a domain-specific modelling environment (SCADE, Simulink etc), from which a code generator produces source code that is then transformed into machine code. The SECCO approach is to define the properties of code transformations such that the chosen structural code-coverage metrics is preserved by the code transformation. With this approach one can use the source

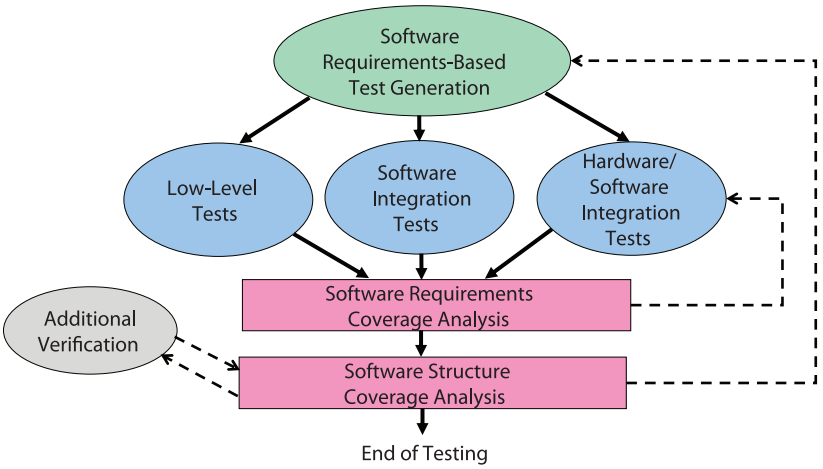


Figure 1: Software testing process in [DO-178B].

code or the model to generate test cases automatically and independently of the hardware platform.

Matching Coverages

There exist basic definitions for structural requirement coverage. Experimental results show that there is a weak correlation between structural requirement coverage and structural code coverage, ie full requirement coverage yields less code coverage. On the basis of these results we want to identify what is necessary to guarantee the preservation of coverage criteria starting from structural requirement-coverage criteria to achieve structural code coverage. We address the following questions: Is there a better structural coverage metric for the requirements than the existing coverage metrics? Which type of formal requirements yields good values for MC/DC? Which requirements are 'hard' to test (ie the derived test suite executes only a subset of the necessary paths defined by MC/DC)? Which implementation variants are possible and how do they affect the MC/DC criterion?

It is rather challenging to match current coverage metrics between the different program representations shown in Figure 2. For example, MC/DC is based on the conditions and decisions of the source code. But given the (low-level) specification there is no hint about what logical structures should be grouped into one decision. The same is true for automatically generating code out of a modelling environment like Simulink. This is a serious issue for testing safety-critical systems, since with a given test suite, the different logical structuring of a program results in different structural code coverages. Within the project SECCO we are working on coverage metrics that are more robust against the logical restructuring of programs.

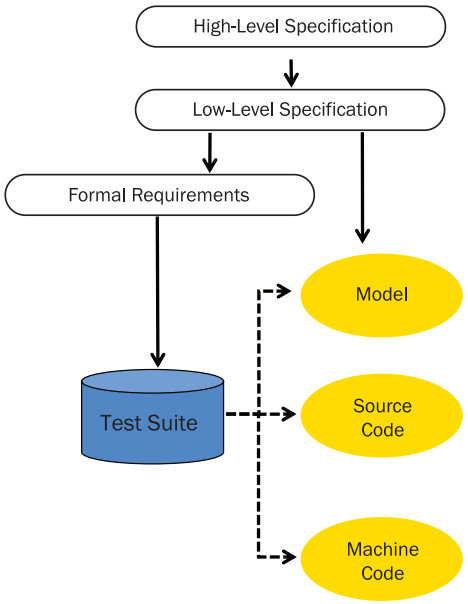


Figure 2: Principle of requirements-based test case generation.

Link:
http://ti.tuwien.ac.at/rts/research/projects/SECCO

Please contact:
Raimund Kirner
Real-Time Systems Group, Vienna University of Technology, Austria
Tel: +43 1 58801 18223
E-mail: raimund@vmars.tuwien.ac.at

A Step towards Generating Efficient Test Cases – the Project MOGENTES

by Wolfgang Herzner, Rupert Schlick, Manfred Gruber

The goal of MOGENTES (MOdel-based GENeration of Tests for Embedded Systems) is to significantly enhance testing and verification of dependable embedded systems. This is achieved by automatically generating efficient test cases by relying on the development of new approaches as well as innovative integration of state-of-the-art techniques. In particular, MOGENTES will apply this technology in large industrial systems in the automotive, railway control and off-road vehicle industries.

Embedded computer systems are increasingly being integrated with safety-relevant applications such as vehicles, medical equipment and control systems. Every possible measure must be taken to ensure the dependability of such systems. As a consequence, the cost of testing software, verifying its correctness, or validating it against functional and safety requirements accounts for an increasing fraction of the overall cost. A small survey that we recently carried out among some 35 people revealed that more than 40% of the participants put at least 20% and up to 50% of the overall development effort into test and verification.

One conceptually perfect means of proving the correctness of some (software) system is formal verification, eg model checking. However in general, formal verification approaches have several limitations and drawbacks:

- for larger systems, computing resources quickly go beyond what is feasibly available
- the notations used for the formal specification of systems and requirements are highly abstract (eg Z or VDM or NuSMV), making it hard for domain experts to efficiently apply these methods
- a 'sufficiently' complete formal specification of the system is hard to establish (it is noteworthy that the standards EN 50128 and IEC 61508 recommend the use of formal methods at higher safety integrity levels, but do not enforce it as the only highly recommended method)
- the notion of faults and fault effects are rarely included in formal models
- means for dependability (eg fault tolerance) are poorly addressed by existing tools.

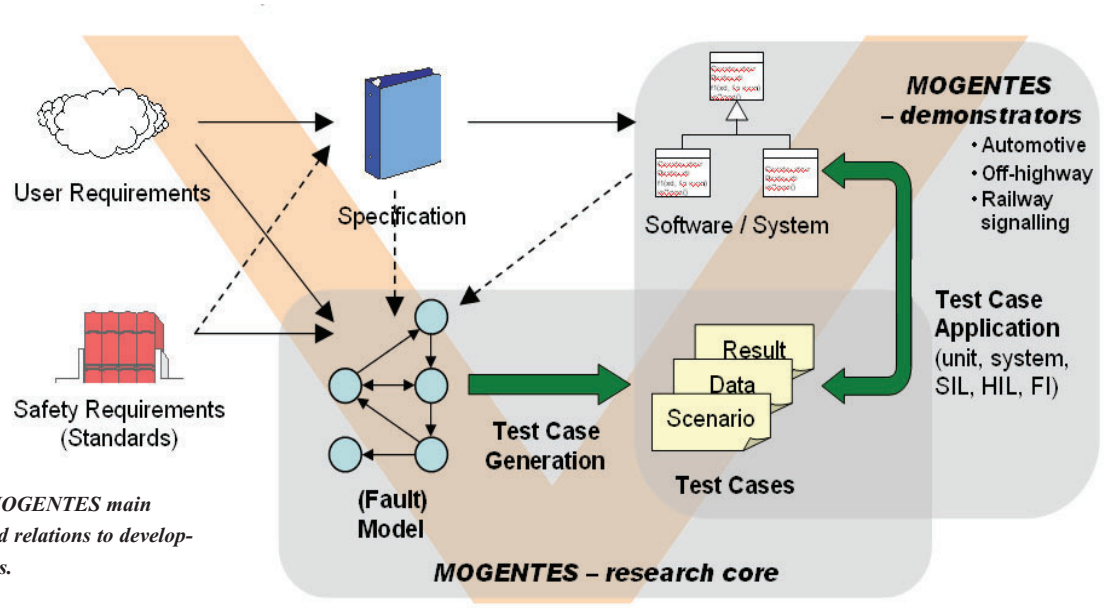


Figure 1: MOGENTES main activities and relations to development process.

Testing is therefore still the preferred method of verification. Manual testing, though, is expensive. In the survey mentioned before, in 60% of all addressed projects the number of test cases lies in the range of 1000–10 000, representing a significant effort. There is consequently a huge demand for test-case generation (TCG) and tools. However, in 60% of all addressed projects essentially none of the test cases were automatically generated, while in fewer than 5% of projects were more than 60% of test cases automatically generated.

One reason is that TCG requires abstract models of the target systems. Unfortunately, testers are often forced to manually reverse-engineer the implementation in order to achieve the coverage required for a successful certification (eg Modified Condition/Decision Coverage (MC/DC) as suggested by the RTCA DO-178B standard), because an abstract model of the system is not available or no longer conforms to the final product. As a consequence, model-based development must be complemented by corresponding improvements in model-based testing technology.

MOGENTES (MOdel-based GENeration of Tests for Embedded Systems) will demonstrate that with a combination of new and existing techniques, not only can the testing effort be significantly reduced by means of model-based test case generation, but that this can also be realized in a way accepted by domain experts with limited experience in formal methods.

A means to achieving this goal is the reduction of test cases by selecting the most effective ones. MOGENTES therefore has the following objectives:

- to generate efficient test cases from system and fault models
- to establish a framework for the integration of involved tools, including model transformations
- to provide traceability of requirements and to match them to test analysis results
- to foster the application of automated testing for satisfying functional safety standards requirements.

These objectives shall be achieved with the following concepts:

- define common modelling languages and semantics (meta-models), with UML as the primary candidate, to model domain-specific requirements
- develop a test theory that defines the conformance relation between the model and the implementation, and success and failure of a test case
- define fault models (for hardware and software) and extend the modelling languages to represent faults in (application) models
- define new coverage criteria under consideration of minimal cut sets, fault injection, mutation testing and safety aspects
- use model-based fault injection (MBFI) for automatically calculating minimal cut sets
- validate fault models and the generated test cases with physical fault injection
- use (bounded) model-checking techniques to generate stress test scenarios
- provide semantics-aware transformations from system models to inputs of specific tools.

The partners in MOGENTES are Austrian Research Centers - ARC (AT), Budapest University of Technology and Economics (HU), Swiss Federal Institute of Technology Zurich (CH), Graz University of Technology (AT), Prover Technology (SE), SP Technical Research Institute of Sweden (SE), and four industrial partners: Ford Forschungszentrum Aachen (DE), Prolan Irányítástechnikai (HU), Thales Rail Signalling Solutions (AT) and Re:Lab (IT), who not only provide the applications and requirements to be addressed, but will also evaluate the results and develop the final demonstrators.

MOGENTES is a Specific Targeted Research Project (STREP) in the 7th Framework Programme partially funded by the EC, and commenced in 2008.

Link:
https://www.mogentes.eu/

Please contact:
Wolfgang Herzner, Rupert Schlick, Manfred Gruber, Austrian Research Centers GmbH – ARC
Tel: +43 50 550 {4231/4124/4183}
E-mail:
{wolfgang.herzner, rupert.schlick, manfred.gruber}@arcs.ac.at

SESAME: A Model-Driven Test Selection Process for Safety-Critical Embedded Systems

by Nicolas Guelfi and Benoît Ries

SESAME (Specification based testing of safety-critical small-sized embedded systems) is an industrial research project in the field of embedded systems test methodologies. The first targeted systems are small embedded systems developed by the Luxembourg company IEE S.A. for the control of airbags through sensors or infrared cameras.

SESAME (Specification based testing of safety-critical small-sized embedded systems) is an industrial research project in the field of embedded systems test methodologies. The first targeted systems are small embedded systems developed by the Luxembourg company IEE S.A. for the control of airbags through sensors or infrared cameras.

The objective is to develop an approach for specification-based testing that is adapted to the needs and constraints of safety-critical small-sized embedded systems. This approach aims to improve the efficiency of activities performed by test engineers, particularly during tests based on software specifications. This approach must have a sound theoretical foundation and must be usable by test engineers. In particular, it is a question of proposing a model transformation language that simplifies software specification models and thus the selection of test cases. This approach should be integrated in a semi-formal approach for the specification and testing of safety-critical embedded systems.

SESAME is a joint project between the University of Luxembourg and IEE; it started in April 2003 and will finish in March 2009. The work is performed both at the LASSY (Laboratory of Advanced Software Systems of the University of Luxembourg) and within the Embedded Software Team of the Innovation Department of IEE, also located in Luxembourg.

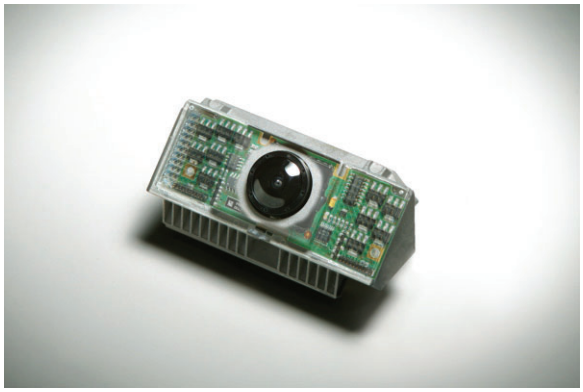
Embedded software systems introduce a bias toward system testing by customers and suppliers. The companies that develop embedded software systems previously spent significant time developing non-programmable physical systems. The first bias is that customer tests focus on physical attributes and thus do not cover the attributes introduced for the purpose of the embedded software. A similar bias is introduced for the requirements specifications, which may have important consequences in our context of specification-based testing. In particular, a supplier may neglect its own requirements and tests, both coming from its development and test platforms.

Product quality can be improved by following a verification process that proposes the execution of a tractable test phase for which test cases are selected in order to address explicit quality objectives. The SESAME approach uses simple software requirement models as an input, in order to add more weight to the requirements analysis phase of a project. This has corresponding benefits for the project, especially in the subsequent design phase. The SESAME method focuses on the software boundary; this helps reduce the number of hidden software defects and potentially the total time taken to discover and remove defects from the system as a whole.

To summarize, the SESAME approach for process improvement addresses three objectives. First, it is based on a simple software requirements model; second, it includes a precise description of the test space; and third, it offers a precise knowledge of the test coverage. Further study of this methodology, in particular the specification and test phases, will promote methodologies integrated with software engineering tools. Using this approach within an industrial framework will aid evaluation of the suggested solutions.

In order to ease the transfer of the SESAME methodology into industry, the concrete syntax of the software requirements modelling language used for this project has been selected with respect to the recent Unified Modelling Language 2 (UML2) notation standardized by the Object Management Group (OMG). In particular, UML2 protocol state machines (PSMs) have been chosen to describe the dynamic behaviour of the software interface, and UML2 class diagrams are indeed used to describe the data associated with the behaviour defined in the PSMs.

The precise description of the test space uses a domain-specific language (DSL) defined expressly for the purpose of test selection. Test constraints specifications defined with this language are interpreted as model transformations on the analysis model, and result in a test model containing the test selection



3D-MLI camera: an embedded system developed at IEE. (Photo: IEE.)

information. At the same time, we will also concentrate on the identification of best practices in test selection activities in an industrial context, in order to tailor the SESAME approach to the automotive industry.

In order to precisely validate the impact of the test selection, we provide the semantics of the modelling language (class diagram together with protocol state machine) in terms of a formal specification language (eg Alloy). This formal specification, automatically derived from the graphical analysis and test models, is used for formal validation purposes.

Future activities will focus on the industry transfer of the approach, and in particular on the full deployment of the SESAME process for the test selection of the software for new system products from IEE.

Links:
IEE S.A.: http://www.iee.lu
LASSY: http://lassy.uni.lu/
SESAME: http://wiki.lassy.uni.lu/projects/SESAME

Please contact:
Nicolas Guelfi
University of Luxembourg
Tel: +352 46 66 44 5251
E-mail: nicolas.guelfi@uni.lu

ProSE – Promoting Standardization for Embedded Systems

by Erwin Schoitsch and Laila Gide

During the last few years, standardization was identified both by the European Commission (EC) and by industry as a new issue of strategic importance for the creation of markets. It was one of the concerns of the EC, especially of the Embedded Systems Unit of the Directorate General 'Information Society and Media', that the results of funded research projects are having only a minimal impact on standardization. The Standards Working Group of ARTEMIS, the European Technology Platform for Embedded Intelligence and Systems, proposed an FP7 support action ProSE (Promotion of Standardization for Embedded Systems), to promote standardization in the (dependable) embedded systems field. This was accepted and it commenced in May 2008.

In the 6th Framework Programme, the COPRAS (Co-operation Platform for Research and Standards) initiative was created, linking research and standardization in different areas, mainly outside embedded systems. The work resulted in several action plans for specific domains, which provided some guidance as to how researchers and research projects could achieve some impact on standardization. The major problem is to find sustainable solutions to perform this task, since – taking into account that research results are only available as projects come to an end – the time schedules of new or evolving standards are outside the scope of research projects.

In the 7th Framework Programme, ARTEMIS, the European Technology Platform for Embedded Intelligence and Systems (now part of a 'joint undertaking'), focused on a variety of dependability issues relating to (critical) embedded systems and was mainly oriented toward systems and software. It organized a standards working group to prepare an ARTEMIS Strategic Research Agenda (SRA) for standardization (as a supplement to the ARTEMIS SRA, see Figure 1). This work will now be performed as part of the ProSE project, with the long-term objective of having ARTEMIS act as a supporting organization that will take over the Strategic Agenda for Standardization as part of its long-term strategy.

The partners in this project are Thales SA (co-ordinator, France); FhG-IGD (Darmstadt, Germany); ESI (European SW Institute, Bilbao, Spain); Austrian Research Centers – ARC (Austria); AVL List (Graz, Austria); ST Microelectronics (Belgium); Commissariat à l'Energie Atomique - CEA (France); Acciona (Spain); and Ericsson AB (Sweden). This represents a good mix of research and industry, with both groups represented by partners involved in diverse fields of dependable embedded systems research, applications and standardization.

Key Issues

ProSE is driven by the ARTEMIS Technology Platform's objectives, which are to overcome the fragmentation of industry and research in the embedded systems sectors, and to support the embedded systems industry such that it is able to supply cross-domain tools and technology for a wide range of application sectors by promoting standardization and generating a related strategic research agenda.

The key objective for ProSE is to:

- structuring and disseminating knowledge of existing standards within the various embedded systems domains
- providing a set of criteria for identifying and prioritizing good candidates for standardization in a systematic and selective manner
- proposing a practicable methodology for their maturation towards their eventual acceptance, so as to enable or facilitate cross-domain compatibility and a higher degree of reusability. This is dependent mainly on software, protocols and interfaces.

Technical Approach

ProSE will provide a vision and recommendations on the way in which embedded systems standards can create synergies between business domains:

- by addressing specific cross-domain issues such as the reusability and reliability of embedded software, and its verification and certification

- by addressing the adaptation of existing standards, and influencing the

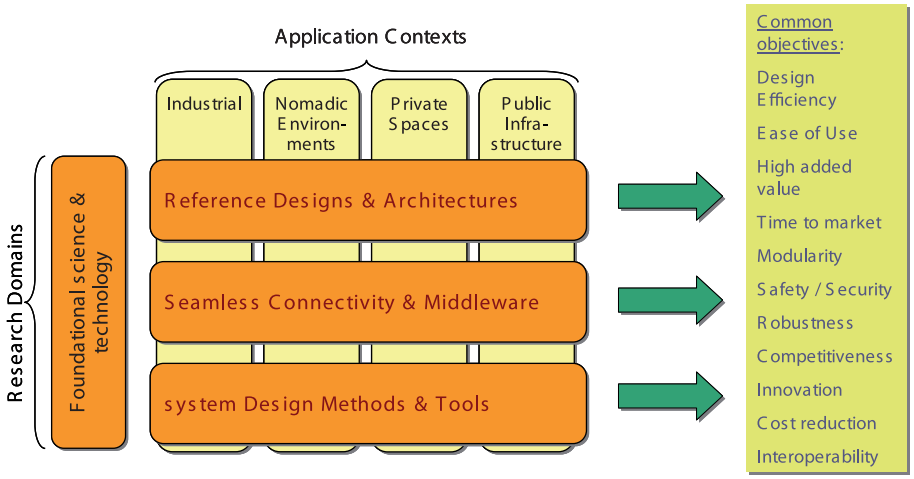


Figure 1: ARTEMIS SRA segmentation with respect to research domains and application context domains.

evolution of or promoting potential new standards in areas not properly addressed until now

- by investigating existing specific domains (aeronautics, automotive, energy, telecom, consumer, medical etc) in order to identify potential cross-domain synergies, and by promoting the ProSE vision towards standardization bodies

- by establishing links between the embedded systems industry (facilitating the engagement of SMEs), EU standardization bodies (CEN (European Standardization Committee), CENELEC (European electrotechnical/electronic Standards Committee), ETSI (telecommunications industry), AUTOSAR (automotive system/software architecture, etc) and worldwide standardization bodies (ARINC (aircraft), ITU (transportation), ISO (International Standards Organization), IEC (International Electrotechnical Commission), etc), and the research community (particularly Networks of Excellence)

- by delivering a strategic agenda for standardization. This strategic agenda would serve as an input to the future EU and national work programmes, and would complement the ARTEMIS SRA.

The project will develop a framework for analysing the present standardization position, and a method by which to determine standardization priorities for embedded systems. The goal is to promote and initiate standards and standards adaptations rather than to write standards, which would be outside the scope (in terms of both time and resources) of this support action. The long-term perspective is the expected take-up by the ARTEMIS Platform.

Figure 2: ProSE supporting activities – linking research and standards.

Expected Impact

The ProSE project will directly address the complexity challenge by promoting and facilitating new approaches to embedded system design. This is primarily a system and software issue, and is critical in many application domains because of the reliance that people and society place on the services delivered by these systems. It will also contribute to the changeover from 'design by decomposition' to 'design by composition' by supporting existing and emerging standards that will enable it.

It will help to better meet the increasing demand for innovation activities in the embedded systems domains by shortening the process of selection of candidate standards, and facilitating the emergence of high-quality standards and of new services, cross-domain products and solutions.

Links:
http://www.prose-project.eu/
http://www.smart-systems.at/

Please contact:
Erwin Schoitsch
Austrian Research Centers – ARC,
ARC (AARIT)
Tel: +43 50550 4117
E-mail: erwin.schoitsch@arcs.ac.at

Laila Gide
THALES, France
E-mail: laila.gide@thalesgroup.com

Bicriteria Multi-Processor Static Scheduling

by Alain Girault and Hamoudi Kalla

The reliability of a system indicates its continuity of service. It is formally defined as the probability that it will function correctly during a given time interval. With the advent of ubiquitous computing and distributed embedded systems, it is becoming an increasingly crucial aspect. We propose a framework for designing highly reliable real-time systems, thanks to a novel bicriteria (length and reliability) static multiprocessor scheduling heuristic. The first criterion is the schedule's length, which assesses the system's real-time property, while the second is reliability, assessing the system's dependability.

Our new multi-processor static scheduling heuristic, BSH, takes as input two graphs: a data-flow graph (ALG) describing the algorithm of the application, and a graph (ARC) describing the target distributed architecture. Figure 1 (left) shows an example of an algorithm graph: it has nine operations (represented by circles) and eleven data dependences (represented by green arrows). Among the operations, one is a sensor operation (I), one is an actuator operation (O), and the seven others are computations (A to G). On the right is an example of an architecture graph: it has three processors (P1, P2, and P3) and three point-to-point communication links (L1.2, L1.3, and L2.3).

Also given is a table of the worst-case execution time of each operation onto each processor, and the worst-case transmission time of each data dependency onto each communication link. The architecture being heterogeneous, these need not be identical. Below is an example of such a table for the operations of ALG. The infinity sign expresses the fact that the operation I cannot be executed by the processor P3, for instance to account for the requirements of certain dedicated hardware.

Our fault hypothesis is that the hardware components are fail-silent, meaning that a component is either healthy and works well, or is faulty and produces no output at all. Besides, the occurrences of the failures of all hardware components follow a constant parameter Poisson law: according to this model, the reliability of any given hardware component during the interval of time d is equal to $e^{-\lambda d}$, where λ is the failure rate per time unit of the component. The table of the individual failure rates per time unit of all the hardware components is also given. Again, the architecture being heterogeneous, these need not be identical.

From these four inputs, our BSH heuristic distributes the operations of ALG onto the processors of ARC and schedules them statically, as well as the

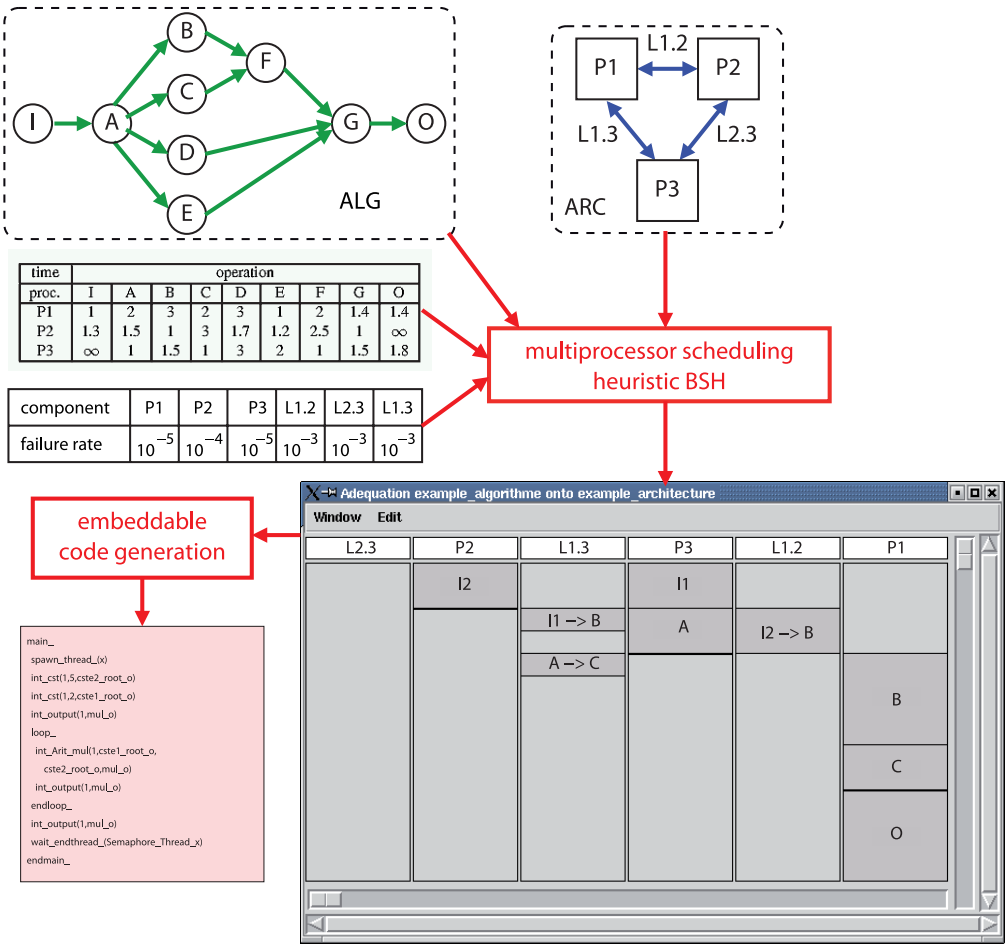


Figure 1: Example of an algorithm graph.

communications induced by these scheduling decisions. The output of the heuristic is therefore a multiprocessor static schedule, from which embeddable code can be generated.

Our contribution is twofold. First, we redefine the framework of bicriteria (length, reliability) scheduling, because the reliability criterion depends intrinsically on the length criterion. This incurs three major drawbacks, common to all bicriteria (length, reliability) scheduling heuristics found in the literature. First, the length criterion overpowers the reliability criterion; second, it is very tricky to control precisely the replication factor of the operations onto the processors, from the beginning to the end of the schedule (in particular, it can cause a 'funnel' effect); and third, the reliability is not a monotonic function of the schedule. To solve this problem, we propose a new criterion to replace reliability, which we call the Global System Failure Rate (GSFR). The GSFR is the failure rate per time unit of the static schedule, seen as if it were a single operation placed onto a single processor.

We have conducted extensive simulations that demonstrate that our new bicriteria (length, GSFR) scheduling algorithm BSH avoids the three problems mentioned above. Furthermore, for a given instance of the problem BSH is able to produce a set of non-dominated solutions in the Pareto sense (ie the Pareto curve), from among which the user can choose the solution that best fits the application's requirements. Figure 2 is an example of such a Pareto curve produced on a ten-processor system for an ALG graph of 100 operations.

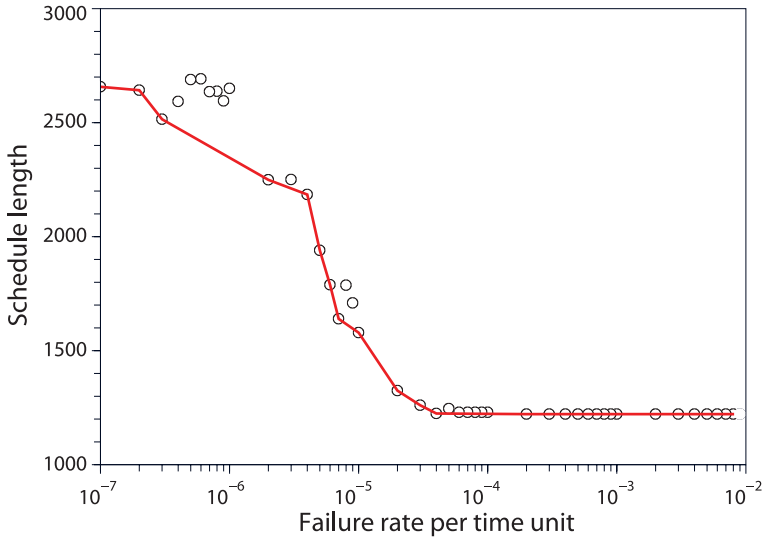


Figure 2:
A Pareto curve produced on a ten-processor system for an ALG graph of 100 operations.

Link:
Fault-tolerance: http://pop-art.inrialpes.fr/~girault/Projets/FT/

Please contact:
Alain Girault
INRIA Grenoble Rhône-Alpes
Tel: +33 476 61 53 51
E-mail: Alain.Girault@inria.fr

Enhancing Java ME Security Support with Resource Usage Monitoring

by Fabio Martinelli, Fabio Massacci, Paolo Mori, Christian Schaefer and Thomas Walter

Capabilities and Ubiquity of mobile devices have dramatically increased in the last few years, with many mobile devices now able to run Java applications, create Internet connections, send SMS messages, and perform other expensive or dangerous operations. As a consequence, better security support is required. We propose an approach to enhance the security support of Java Micro Edition using MIDlets to monitor the usage of mobile device resources.

In recent years, the market for mobile devices such as mobile phones or personal digital assistants (PDAs) has grown significantly. The capabilities of mobile devices have also increased, and up-to-date units can be used to connect to the Internet, read and write e-mails, and also to run Java Micro Edition (Java ME) applications (MIDlets). Moreover, the increase in available bandwidth due to UMTS means that downloading software on mobile devices is becoming more popular.

Yet, the security model provided by Java ME is not flexible enough to allow the spread of MIDlets developed by third-party companies, because it only takes into account the trust in the MIDlet provider. If the principal that signed the MIDlet is on the list of trusted principals stored on the device, the MIDlet is allowed to perform any security-relevant action. On the other hand, MIDlets from unknown providers are not allowed to perform such actions, and the mobile device user is asked to explicitly allow each of them.

To overcome the limitations posed by the model adopted by the standard Java ME security support, the European S3MS project (Security of Software and

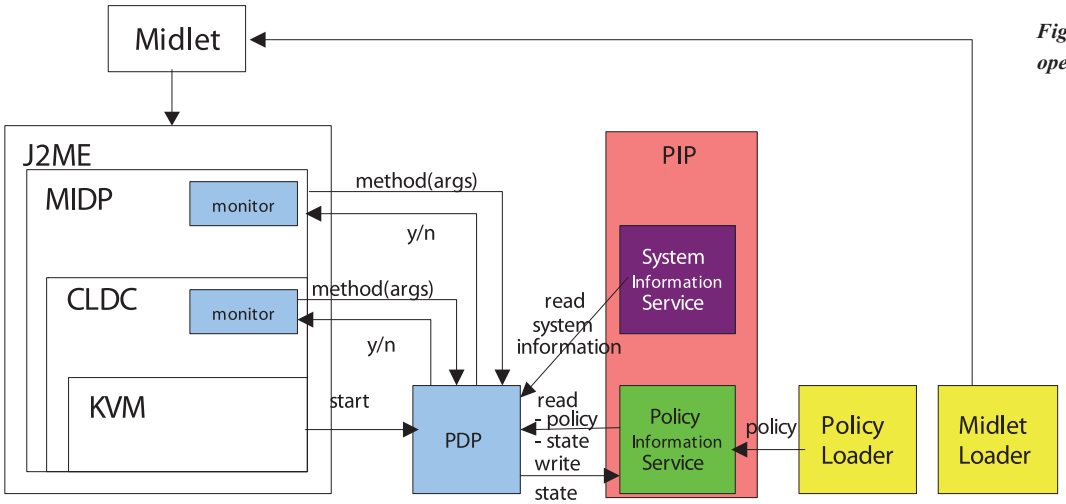


Figure 1: Mobile device operating system.

Services for Mobile Systems) proposes a new paradigm: security by contract. A contract is a claim by a mobile application on the interaction with relevant security features of a mobile platform. At the same time, a policy defines the security requirements of a mobile device, and resides on the device itself. The contract should be published by applications and understood by devices and all stakeholders (users, mobile operators, developers, platform developers etc). The contract is specified at development time as a requirement to the application development teams or as derivation from the analysis of the application. When the application is downloaded onto the device, the contract-matching step is performed to check whether the contract claimed by the application is compliant with the mobile device policy. If the contract-matching step succeeds, the MIDlet can be safely executed on the mobile device.

If the contract-matching step is unable to verify whether the MIDlet is compliant with the device policy, the policy enforcement is performed at runtime. The enforcement is based on the continuous monitoring of the MIDlets to control the usage of the mobile device resources.

The architecture for the runtime monitoring of MIDlets follows the reference monitor model, and consists of the following main components:

- The execution monitor is responsible for monitoring the MIDlet during its execution. Specifically, it intercepts all the security-relevant actions that the MIDlet tries to perform on the underlying mobile device, asks the policy decision point to decide whether the action is allowed and enforces the decision by actually executing the action or by returning an error to the MIDlet.
- The policy decision point is responsible for evaluating whether a given action is permitted in the current state by the policy on the mobile device. It is invoked by the execution monitor and contacts the policy information service to get the policy and to manage the policy state, while it exploits the system information service to retrieve information about the mobile device state.
- The policy information service is responsible for managing the policy state. In particular, it stores the policy variables, which could have different scopes.
- The system information service is responsible for providing information about the system, such as the current date and time, the battery state, the CPU load and so on.
- The policy loader is responsible for loading the mobile policy on the mobile device.
- The MIDlet loader is responsible for loading the MIDlet on the mobile device.

To confirm the effectiveness of our approach, we also developed a prototype of the modified Java ME runtime environment that runs on a real mobile device, namely an HTC Universal smart-phone running Openmoko Linux and exploiting the PhoneME Feature Software MR2 Java Virtual Machine.

Link:
http://www.s3ms.org/

Please contact:
Fabio Martinelli, Paolo Mori
IIT-CNR, Italy
E-mail: {fabio.martinelli, paolo.mori}@iit.cnr.it

Christian Schaefer, Thomas Walter
DoCoMo Euro-Labs, Germany
E-mail: {schaefer, walter}@docomolab-euro.com

Fabio Massacci
Università di Trento, Italy
Fabio.Massacci@unitn.it

TAS Control Platform: A Platform for Safety-Critical Railway Applications

by Andreas Gerstinger, Heinz Kantz and Christoph Scherrer

Within the railway industry, the need for computer systems to perform safety-critical tasks is constantly increasing. A typical application is the railway interlocking system (Figure 1): these systems control the state of the signals and switches on railway lines and are therefore responsible for safe train operation. An incorrect output from such a system may in the worst case lead to a train collision. Other applications in the railway domain are axle counters along railway lines, computer systems on board trains, and field element controllers that operate under rough environmental conditions.

All these systems have an important common feature: they are safety-critical and must therefore be developed according to the highest safety integrity level (SIL4), as defined in the standards applicable to the railway industry (CENELEC 50126, 50128, 50129, Railway Applications Standards [RAMS, software and electronics]). Apart from being suitable for safety-critical operation, railway systems must also be highly reliable and available, and in most cases must meet stringent real-time requirements.

Due to the variety of applications with these common requirements, THALES Rail Signalling Solutions has developed a generic fault-tolerant computer platform that fulfils them, and thus enables the application programmers to fully concentrate on developing the correct application. Due to the increasing complexity of applications, it is also necessary that the platform be able to keep up with ever increasing demands for processing power, memory consumption and connectivity.

This trend can only be addressed by the use of off-the-shelf hardware and operating systems. In order to be able to keep up with the advances in hardware and operating systems, these components should be as interchangeable as possible, such that exchanging them does not compromise the system's safety integrity. For this reason, the middleware that implements the safety functions is strictly separated from the rest of the system. This layered structure can be seen in Figure 2.

Figure 1: Electronic interlocking for mainline rail.

The core hardware containing the CPU board and the interfaces represents the lowest level, and is cleanly separated from the rest of the system. This means that the hardware best suited for each purpose is utilized (eg for rail signalling systems powerful processors and a large amount of memory is needed, whereas for on-board systems low-end hardware with increased environmental resistance is preferred), and that CPU upgrades can be easily performed for new platform generations without major impact on the rest of the system.

The operating system is compliant with POSIX (Portable Operating System Interface), and is currently based on a microkernel. The next platform generation will be based on a more powerful operating system with a Linux kernel, which will bring benefits regarding hardware support and real-time performance.

The main innovation of the platform is its safety middleware, which is the decisive element that makes it suitable for safety-critical applications. The safety middleware ensures the clean separation of the lower levels (hardware and operating system) from the application, and provides all services to ensure safety. The safety middleware also provides the ability to run the platform in redundant configurations.

The applications on top of the layered architecture provide the actual services. The platform can be operated in three architecture variants (Figure 3). The 2oo3 ('2-out-of-3') configuration provides both the required level of safety

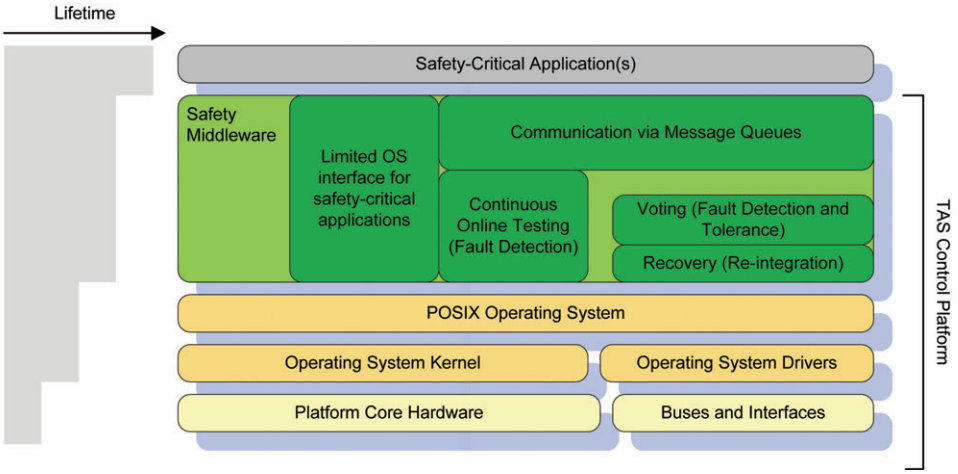


Figure 2: TAS control platform layer structure.

and fault-tolerance mechanisms to enhance availability. In this configuration, all safety-critical decisions are subject to a majority voting procedure, such that a failure of one element is detected and tolerated. A 2oo2 configuration provides the same level of safety but a lower level of availability, since in the case of a conflict of output values between two elements, a failure of one element is detected but not tolerated, since it cannot be decided which one is correct. Finally, a 1oo1 configuration allows an application to be safely operated on a single hardware element, but requires the generation of a diverse application according to specified diversification rules. Software diversity ensures that the same level of safety is achieved.

The safety middleware layer (Figure 2) provides the communication services to globalize data amongst replicated hardware and thus ensures a consistent view even in the case that one replica is faulty and sends erroneous and inconsistent data messages. The API to access these services is implemented as voted message queues. An application transparent voting service enables the reliable detection of faults and the isolation of the faulty replica. This runtime environment for safety-critical applications also ensures replica determinism which is a prerequisite for software execution and voting on redundant hardware. In addition, the platform allows safety-critical applications to access only a limited part of the operating system API, so that replica determinism and safe execution within the runtime environment is guaranteed.

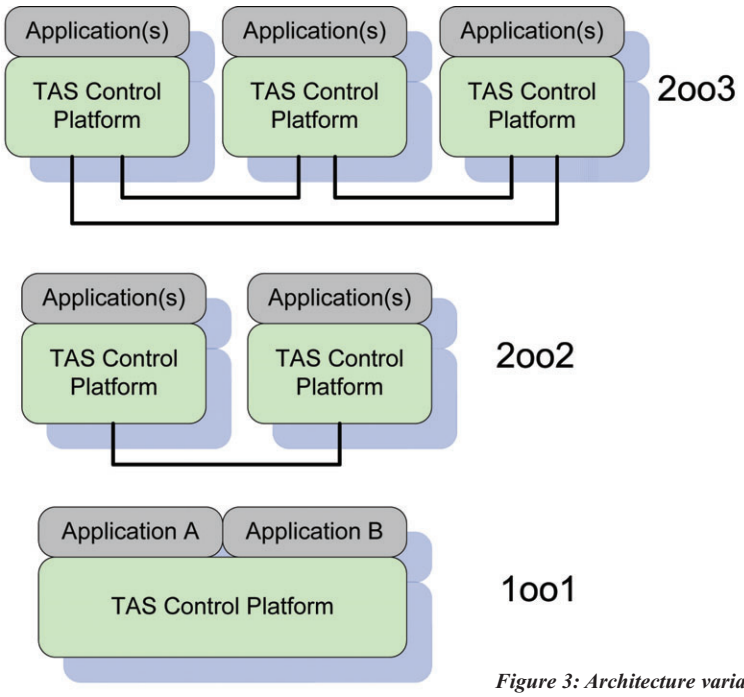


Figure 3: Architecture variants.

To ensure that no latent faults are aggregated in the hardware, the platform also performs continuous online testing of the hardware. This online testing, which is performed by a background task, covers the CPU, memory, buses, clocks and disks. Finally, the platform allows safety-critical applications to access only a limited part of the operating system, so that the safe execution environment of the application is guaranteed.

The platform, launched in 2001, is a well-established product and in operation in more than twenty countries on four continents. It has demonstrated that its safety and reliability approach fits for all vital railway applications within THALES Rail Signalling Solutions. To cope with rapid technology changes in hardware and software, functional enhancements and new concepts for fault detection and tolerance are currently being developed. The next generation of the platform will provide enhanced support for software and hardware diversity, to ensure that the same level of safety can be maintained in the long term with future hardware and software.

Links:
http://www.thalesgroup.com/markets/Activities/Ground-Transportation.html

Please contact:
Andreas Gerstinger, Heinz Kantz, Christoph Scherrer
Thales Rail Signalling Solutions GesmbH, Austria
E-mail:
andreas.gerstinger@thalesgroup.com,
heinz.kantz@thalesgroup.com,
christoph.scherrer@thalesgroup.com

Experimenting with Diversity in the Formal Development of Railway Signalling Systems

Alessandro Fantechi, Stefania Gnesi and Giovanni Lombardi

As a result of collaborations with ALSTOM FERROVIARIA, the Formal Methods & Tools (FMT) group of ISTI-CNR has had access to real-world specifications for signalling equipment together with the complete environment needed to produce an industrial application, from a formal model to the final code. This opportunity has been exploited in an additional research activity aimed at reviewing the existing development process in terms of safety regulations. The underlying idea has been to introduce diversity in order to improve the safety of the equipment produced.

The Formal Methods & Tools group of ISTI-CNR has collaborated on a number of joint projects with ALSTOM FERROVIARIA SpA, with the objective of introducing formal specification and verification tools into the software development process of railway signalling products. The most recent collaborations have investigated the feasibility of automatic code generation, starting from a specification of the system's logic using the SCADE tool developed by Esterel Technologies. The focus has been on issues of performance of specific proprietary hardware architectures and on integration with existing software modules. These collaborations have provided the opportunity for some additional research into the introduction of diversity with the aim of improving the level of safety in the design and development process.

The introduction of diversity has been considered in those cases where an analysis of the safety measures employed to limit design faults has revealed possible weaknesses in the development process. A formal model of the (components of the) equipment is first developed using SCADE, with the added possibility of simulating the model and using model checking to verify that there are no software faults. Code is then generated by the SIL 4 validated SCADE code generator. A first possible weakness of this process has been identified in the supporting software: the underlying operating system and the compilation environment, which are not validated software components. We therefore introduced the first form of diversity at the level of the compilation of the generated code, with the aim of discovering possible faults due either to the compilation environment or to the underlying operating system (Figure 1). Two different compilation environments running on two different operating systems have been employed: the proprietary embedded platform with its dedicated compiler and a commercial compiler on the Windows platform. Parallel testing of the two versions with the same set of tests (taken from the official suite of acceptance tests) has been employed in order to reveal differences in how the generated code interfaces with the operating system or in how it is compiled.

However, even when sophisticated verification tools such as model checking are used, it cannot be guaranteed that the process of writing a formal model

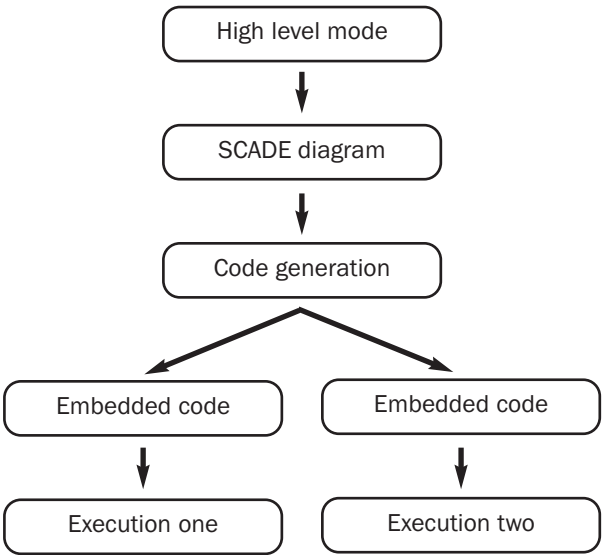


Figure 1: Compilation and operating system diversity.

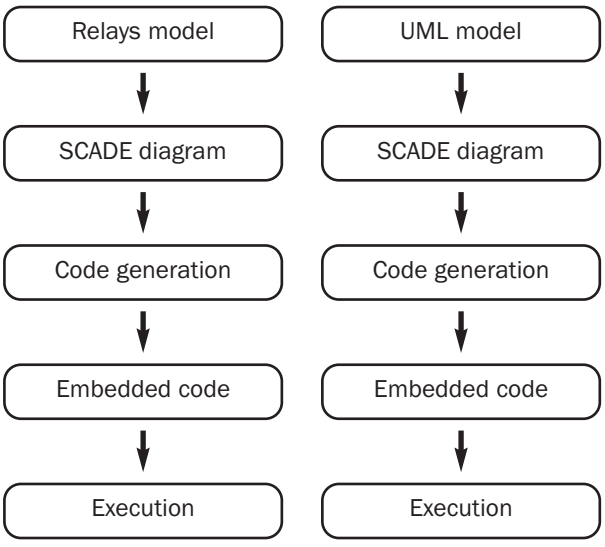


Figure 2: Specification diversity.

has faithfully captured the (informal) system requirements. Diversity can help at this stage as well, by considering two independent formal specifications. A second form of diversity can thus be introduced at the level of specification; this will impact the whole development process.

The application of this idea to the railway signalling domain has provided a direct way of conceiving diverse specifications: the relay schemas that still constitute a common language for railway signalling engineers have been used for one version, while a more 'modern' and increasingly popular notation – UML sequence diagrams – have been used for the other. From these two specifications, two independent chains of verification/code generation/compilation/deployment have been implemented (Figure 2). The final comparison is made by running the set of official acceptance tests for the equipment developed on both versions.

The results of our experiments on the introduction of diversity in compilation have been encouraging, and their relatively low cost should facilitate industrial acceptance of the approach. In fact, the added cost of the first approach is limited to repeat compilation and testing on a Windows-based machine, with practically no cost for additional hardware or software resources. Moreover, replication of compilation and testing can be automated to a high extent.

In contrast, the introduction of diversity in specifications requires at least the additional effort of writing an independent specification. The overall cost of producing diverse specifications is therefore twice that of a single formal specification process. However, the higher costs of this form of diversity can be justified by lower testing and debugging costs due to the early discovery of design faults, and by the higher level of safety achieved.

Link:
http://fmt.isti.cnr.it

Please contact:
Stefania Gnesi
ISTI–CNR, Italy
E-mail: stefania.gnesi@isti.cnr.it

Evaluation of Natural Language Requirements in the MODCONTROL Project

by Antonio Bucchiarone, Stefania Gnesi, Gianluca Trentanni and Alessandro Fantechi

We describe QuARS (Quality Analyzer for Requirement Specifications) Express, a customized version of the QuARS tool. It is designed to evaluate natural language requirements, can handle complex and structured data formats containing metadata, and is able to produce an analysis report with categorized information.

On behalf of ERCIM, the FMT Group of ISTI-CNR has participated in MODCONTROL, a subproject of the recently concluded European Integrated Project MODTRAIN. MODTRAIN stands for Innovative Modular Vehicle Concepts for an Integrated European Railway System, and was the first Integrated Project to focus on joint European railway research. The objective of MODTRAIN was to define the functional, electrical and mechanical interfaces and validation procedures for a range of interchangeable modules that will form the basis for the next generation of intercity trains and universal locomotives. MODCONTROL addressed the standardization of an innovative Train Control and Monitoring System (TCMS) designed for future interoperable European trains.

Achieving high quality in the definition of software requirements is a must in the development of reliable and dependable software products. The availability of techniques and tools for the analysis of requirement documents may help to remove inconsistencies and ambiguities at as early a stage as possible. An automatic analysis of the requirements expressed in natural language should help to guarantee the successful outcome of a project by highlighting potential sources of ambiguity and other weaknesses.

In the context of MODCONTROL, we have developed the QuARS Express tool, a customized version of the QuARS tool (see ERCIM News No. 58), able to handle complex and structured data formats containing metadata and to produce an analysis report with categorized information. The new reporting feature improves on the simple text-based report provided by QuARS by exploiting HTML technology to produce structured hypertext pages.

Using QuARS Express, we analysed the functional and system requirements of TCMS, which included more than 5700 requirements. The results showed that an analysis based on QuARS Express not only identifies linguistic defects, but can also provide some indication of the diverse styles used by different partners to express requirements

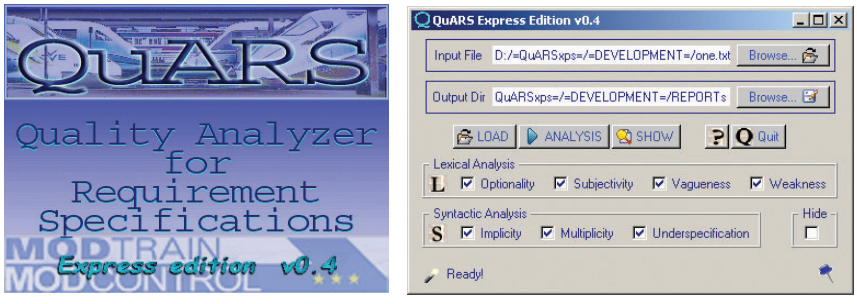


Figure 1: QUARS graphical user interface.

in natural language, thus laying the basis for improvements in the formulation of requirements.

The overall quality analysis process adopted in the project is shown in Figure 2 and is summarized in the following points:

- The project partners create a new project using IBM RequisitePro and insert the requirements with all the required attributes (Name, Text, Responsibility, Package etc).
- The different requirements are stored in a requirements file, one for each requirement class, ie Functional Requirements (ie, FREQ) and System Requirements (ie, SREQ).
- The IBM tool SoDA is used to generate a text document containing the requirements and the relevant attributes, which is saved in text format. A specific template has been defined for SoDA in order to allow QuARS Express to properly interpret the information contained in the generated document.
- The text file obtained is input to QuARS Express, which analyses the sentences (requirements) and gives as output the Defective Requirement Reports (DRR) for both FREQ and SREQ documents, together with the calculation of relevant metrics.

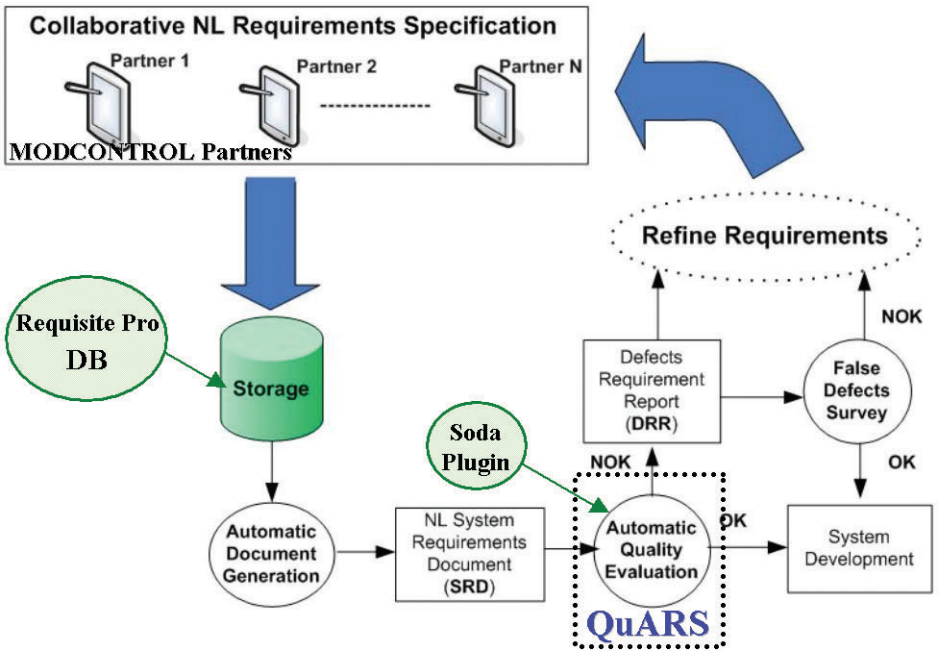


Figure 2: MODCONTROL evaluation process.

- If QuARS Express should point to some (possible) defect, the DRR should be filtered by experts in a 'false defect survey', in order to establish whether or not a refinement is really necessary. In this case, a new cycle of quality analysis may be initiated.
- Otherwise, the approved requirements document is released.

Links:
http://www.modtrain.com
http://quars.isti.cnr.it/
http://www-306.ibm.com/software/awdtools/reqpro

Please contact:
Gianluca Trentanni
ISTI-CNR, Italy
E-mail: gianluca.trentanni@isti.cnr.it

Development of Safety Software for the Paks Nuclear Power Plant

by Tamás Bartha and István Varga

Software development in a safety-critical environment requires that a rigorous process be followed in all phases of the system life cycle. Members of the Systems and Control Laboratory of SZTAKI are working together with experts at the Paks nuclear power plant in Hungary to develop new tools and support systems that will improve the dependability of the safety software.

The Systems and Control Laboratory (SCL) of SZTAKI has a long-term successful research and development collaboration with the Paks nuclear power plant to provide new methods and tools for the development of safety software in the plant. Some notable recent results of this work (listed according to their role in the development life cycle) are the following:

1. *Specification:* the verification of detailed functional specifications of safety functions with formal methods.
2. *Development and implementation:*
   - Microcontroller level: the hardware and software for the microcontroller-based smart test plugs of the Universal Test System (UTS)
   - Programmable Logic Controller level: the distributed control hardware and software of the new Primary Pressure Controller
   - Application level: the UTS test management software.
3. *Testing:*
   the Universal Test System.

Formal Verification of Functional Block-based Specifications

Each reactor unit of the nuclear power plant is supervised by a Reactor Protection System (RPS), which continuously monitors the nuclear process in order to intervene and safely shut down the unit in an emergency situation. The plant experts specify the safety functions of the RPS using the Functional Block Diagram (FBD) description method. The software for the RPS is then created automatically by a certified code generation process.

The primary means for finding errors in the specification are simulation and testing. However, this approach cannot guarantee the correctness and completeness of the specification. Formal analysis of the safety functions is therefore required to prove that the system cannot enter into unsafe states; remains operational (no deadlock or livelock); does not trigger the safety actions unnecessarily (no spurious activation); and always triggers them when required (no activation masking).

Figure 1: The new pressure controller system in the testbed environment.

The Systems and Control Laboratory supplemented the development process with a verification procedure based on the formal modelling of the RPS safety functions. The basic function blocks are described by Coloured Petri Net (CPN) subnets. The formal model of a given safety function is obtained by the proper composition of these subnets into a hierarchical CPN, copying the structure of the FBD-based specification. This formal model is then analysed using the behavioural properties of the CPN and model-checking methods.

Functional Testing of the RPS During Normal Operation

The Universal Test System is a distributed, computerized test system developed by members of the Systems and Control Laboratory to facilitate the testing of the RPS during the start-up stage and also during normal operation.
The UTS is composed of three main components:

1. The Central Test Machine is an industrial PC that provides the user interface to the UTS, initiates test execution, controls the testing process by communicating with the Local Test Machines (LTMs), and queries and automatically evaluates the test results from the plant database.
2. The LTMs download the tests to the appropriate active test plugs and supervise the tests that use the communication interfaces.
3. The active test plugs are intelligent, microcontroller-based cards, which perform their dedicated part of the test procedure autonomously. For safety reasons the cards are backlash-free and are powered only during the test.

The functional and physical distribution of the components means the LTMs and the active test plugs have a simple and robust design. Various software development methods and environments were used due to the heterogeneous hardware platforms.

The new Primary Pressure Controller

A new pressurizer control system for maintaining the pressure safely within the range of 122.75-123.25 bar was designed and successfully implemented by the members of SCL. The control algorithm is based on the simplified dynamic model of the pressurizer.

The redesigned pressure controller is a distributed digital system comprised of units based on the Programmable Logic Controller (PLC) and connected by an Ethernet network. The pressure is measured by a high-precision instrument located in a hermetically sealed area. The pressure measurement loop has a redundant architecture. The data are transferred to a Siemens S300 control unit using the Profibus PA protocol. This controller checks the status of the pressure measurements and transfers them to the other units. The endpoints of the system are three Wago intelligent controllers that operate the electric heaters and the valves: these are the real actuators in the system, located at different points in the power plant. The three controllers are able to work independently in reduced mode in case of a failure.

The software of each PLC contains the control algorithm and performs the communication in the distributed system. Both the Siemens and the Wago PLCs were programmed using development tools compliant with IEC 61131-3.

The main feature of the new controller is that it uses a continuous range (0-360 kW) of heating power to guarantee a very stable pressure value. The amplitude of the pressure oscillations was reduced from 1 bar to 0.1 bar compared to the old controller. This made possible a safe increase in the thermal power of the units by 1-2%. The operational results are very good: using the more efficient control, a much smoother overall operation has been obtained.
These developments are part of the complete refurbishment of the instrumentation and control infrastructure at the Paks nuclear power plant. In these days of the 'nuclear renaissance', there are more and more refurbishment and life-time extension projects in Europe and throughout the world. As the old analogue and wired logic is replaced with modern digital programmable equipment, the amount of safety-critical software multiplies, meaning such developments are vital to maintain and ideally increase the safety and efficiency of the nuclear power.

Link:
http://www.sztaki.hu/scl

Please contact:
Tamás Bartha, István Varga
SZTAKI, Hungary
Tel: +36 1 279 6227
E-mail: bartha@sztaki.hu,
ivarga@sztaki.hu

Catalonia boosts Education and Knowledge in Safety-Critical Software

A recent collaboration has led to the development of a professional training course in quality assurance for safety-critical software and systems, focused on the biomedical, transport and aerospace sectors.

The Aerospace Research and Technology Centre (CTAE) and the Technical University of Catalonia (UPC) joined forces in late 2006 to organize an innovative professional training course in quality assurance for critical software and systems, with the support of UPC Foundation and the University of Ohio. To date, two successful editions of the course have been held with international participation, and a third edition is scheduled for February 2009, in Barcelona.

We understand as critical those software items and systems in which a malfunction may harm humans and/or animals, damage the environment, destroy infrastructure, or cause structural damage. An illustrative example is the challenge that must be addressed to seamlessly introduce Unmanned Aerial Vehicles (UAVs) into non-segregated airspace from an Air Traffic Management (ATM) perspective. There is a growing demand for safety-critical software and systems whose risks are managed with the methods and tools of safety engineering. A life-critical system is designed to behave as needed even when pieces fail; this is illustrated by the US Federal Aviation Administration (FAA) specification that fewer than one life per billion (10^9) hours of operation should be lost (Advisory Circular 25.1309-1A).

The difficulty frequently remarked upon by companies lies in finding trained professionals in this complex field, which includes quality assurance according to the relevant standards, methods, processes and techniques. This course was created with the aim of providing the participant with the academic state-of-the-art knowledge and advances, together with a practical view of how these solutions are implemented in current and future projects with industry. The three participating companies bring hands-on expertise in a spectrum of applications ranging from biomedical and space-borne systems (NTE), flight segment and avionics in launchers (GTD), and ground segment and navigation systems (INDRA). Moreover, each edition of the course features an invited speaker to complement the lectures.

The course covers the following main topics: an introduction to safety, an overview of systems and systems engineering, lifecycle models, an exhaustive view of safety analysis methods (including functional hazards models, fault tree analysis, Markov analysis, failure mode and effect analysis), standards and certifications at American and European levels, requirements and traceability, software safety, verification, tool qualification, configuration management and certification aspects. Additionally, a review of real-time operating systems and control systems (including specifications, closed-loop, structural conditions) is also given, as well as practical aspects in coding, verifying and validating (V&V) software in these systems.

The course also fosters the exchange of ideas among different institutions and builds up partnering and networking initiatives, all of which is helping Catalonia to become a centre of excellence in this area.

Links:
http://www.upc.edu
http://www.ctae.org
http://www.fundacio.upc.edu
http://www.nte.es
http://www.indra.es
http://www.gtd.es

Please contact:
Josep Maria Fuertes i Armengol
Universitat Politècnica de Catalunya, Spain
Tel: +34 93 401 72 90
E-mail: josep.m.fuertes@upc.edu

Marcel Quintana Claramunt
Aerospace Research and Technology Centre (CTAE), Spain
Tel: +34 93 664 26 44
E-mail: marcel.quintana@ctae.org

Requirements Engineering Lab at IPT São Paulo

To contribute to research in requirements engineering, the Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT) decided to create the Requirements Engineering Laboratory.

The main objective of the Requirements Engineering Laboratory is to create, deploy and disseminate a research environment to post-graduate IPT students. It is particularly aimed at those enrolled in software engineering courses but is also open to other researchers, helping them to develop academic research and artifacts related to software requirements engineering. The laboratory also intends to foster academic and industrial partnerships for the purpose of developing requirements engineering techniques and tools to deliver more reliable and accurate safety-critical applications.

To meet the objectives, ten research areas have been defined:

1. Software requirements fundamentals
2. Software requirements engineering processes
3. Software requirements elicitation and analysis methods:
4. Software requirements specification: investigates software requirements models from a system viewpoint.
5. Formal methods applied to software requirements engineering:
6. Domain languages and models
7. Domain and requirements model transformation:
8. Software requirements verification and validation (V&V)
9. Software requirements management
10. Software requirements modelling tools.

Link:
http://www.ensino.ipt.br/

Please contact:
Paulo Sérgio Muniz Silva
Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, Brazil
E-mail: paulo.muniz@poli.usp.br

Developing a Distributed Electronic Health-Record Store for India

by Jim Dowling and Seif Haridi

The DIGHT project is addressing the problem of building a scalable and highly available information store for the Electronic Health Records (EHRs) of the over one billion citizens of India.

There has been much recent interest in information services that offer to manage an individual's healthcare records in electronic form, with systems such as Microsoft HealthVault and Google Health receiving widespread media attention. These systems are, however, proprietary and fears have been expressed over how the information stored in them will be used. In relation to these developments, countries with nationalized healthcare systems are also investigating the construction of healthcare information systems that store Electronic Health Records (EHRs) for their citizens.

The DIGHT (Distributed Information store for Global Healthcare Technology) project is addressing the challenges of building a scalable and highly reliable information store for EHRs for the citizens of India. The project partners are SICS and the Indian Centre for Development of Advanced Computing (C-DAC), where SICS is responsible for the distributed storage aspects of the project, while C-DAC will work towards evolving an EHR standard for India. The project will embrace both open-source technology and open standards to ensure that information is managed and secured in an accountable and transparent manner. We are not aware of any existing government-run information system that manages the enormous number of users that would be stored in an Indian EHR information store.

Photo: Staffan Truvé

Electronic Health Records for the more than one billion citizens of India.

In many Western countries, the main problem of building a one-stop shop for patients' EHRs is the cost of integrating disparate existing healthcare systems. Typically, these systems do not easily interoperate due to the use of different relational databases and different media storage software, which makes data transfer across systems inconvenient or impossible. Another challenge for such systems is the use of distributed storage, as a centralized system of this scale would lead to limited scalability and poor availability characteristics. We are building a healthcare system from the ground up; less emphasis is placed on the integration problem due to a relatively small number of existing healthcare systems and EHRs in India.

The requirements for our EHR storage system include:

- high data availability even in the presence of faults in the network or computer hardware (eg due to power outages, environmental disasters and regional strife)
- high performance to ensure the system can function even under the high loads that may arise in emergency situations (such as a pandemic, large-scale accident or war)
- security to protect patient data from misuse, unauthorized access or attacks.

While current relational database technology has matured to the extent that systems can store terabytes of data in a

database cluster, existing centralized information storage architectures provide impediments to scalability and high availability. DIGHT will make use of lower-cost computer clusters that can be used to provide higher availability and better performance characteristics for lower hardware costs.

As part of this distributed approach, the project will develop data replication algorithms to ensure that security, performance and data availability requirements are met. The EHR store will be huge in size and the network environment will be challenging, with frequent network partitions. Our replication algorithms must take into consideration Brewer's Conjecture: it is impossible for a data store in an asynchronous network to simultaneously provide (i) partition tolerance, (ii) availability and (iii) consistency. Typically, systems can be built that simultaneously provide two of these three properties and it is generally assumed that designers of new systems should pick the two properties that are most important to their requirements. In DIGHT we will investigate the design of partially synchronous networks that can enable us to overcome this limitation.

State-of-the-art open-source replication for wide area networks (WANs) such as MySQL cluster, only support asynchronous replication: they provide no data consistency guarantees between clusters for data replicated between geographical locations. Consequently, in the event of the crash of a cluster there is potential for data loss. This is not acceptable in the healthcare domain. While strict consistency of multiple copies of replicated EHRs is intuitively the most desirable consistency model, this may unnecessarily degrade performance due to high latencies over WANs. However, since an EHR is a huge set of information, not all information will require strict consistency of data for the information system to function correctly. Hence, there is scope to identify and implement weaker consistency models to enable the system to function both efficiently and correctly. The idea is to define a set of consistency models with varying degrees of consistency and to associate them with different sets of information in an EHR depending on the consistency needs of the system.

As the system will be of extreme scale, with many clusters located throughout India, client software that accesses data in the information store will need to provide routing and lookup functionality to enable data updates and queries to be sent to the cluster where the replicated EHR of current interest is stored. In particular, we are investigating the use of Distributed Hash Table technology to build a scalable solution for discovery and retrieval of EHRs from clusters. Finally, we will incorporate suitable security policies and mechanisms to prevent corruption, misuse or theft of EHR data in distributed environments.

Link:
http://dight.sics.se/

Please contact:
Jim Dowling
SICS, Sweden
Tel: +46 8 633 1694
E-mail: jdowling@sics.se

Epidemic Intelligence: Satellite-Enabled Applications for Health Early Warning Systems

by Catherine Chronaki

An earthquake-readiness exercise in November 2007 in Crete, Greece, assessed the added value of satellite-enabled applications for epidemiological surveillance and health early warning systems in post-disaster health management.

The risk of epidemics and emerging or re-emerging diseases is rising and can only be contained with prevention, early warning and prompt management. Readiness exercises are critical in improving readiness, in testing means, methods, master plans and procedures, and above all in training civil protection personnel.

The SAFE (Satellites For Epidemiology) project is co-funded by the European Space Agency (ESA) and coordinated by MEDES (FRANCE). In a two-day earthquake readiness exercise that was held on the island of Crete, Greece, on November 5-6, 2007, it demonstrated a component-based system for health early warning. The exercise that was coordinated by the Prefecture of Heraklion and FORTH-ICS, involved around 300 people from more than twenty organizations. Observers from ESA, the World Health Organization (WHO), the European Center for Disease Control (ECDC) and other organizations assessed the added value of satellite-enabled services not only in the acute phase following the disaster but also in post-disaster health management and epidemiological surveillance.

On the first day, the exercise scenarios covered search and rescue operations in a power plant and a large hotel complex, as well as averting pollution and environmental disaster after a fuel leakage. The SAFE van offered satellite communication and deployed a WiFi network in the crisis area. Volunteers of the Hellenic Red Cross used triage protocols available in handhelds connected to the emergency coordination system and a central hospital. A WiFi camera conveyed sights and sounds of the disaster to decision makers in the operations centre.

On the second day, epidemiology scenarios of post-disaster health management unfolded in a refugee camp coordinated by the Hellenic Red Cross and the Prefecture of Heraklion. Upon arrival, the state of health and the medication needs of refugees were recorded in a primary care Electronic Health Record (EHR) system that was extended to support rapid data entry of health problems and medication using Personal Digital Assistants (PDAs). Summary reports that reflected the overall status and

health needs of the camp were then automatically generated.

Soon afterwards, the first signs of a Salmonella enteritidis outbreak appeared in the camp. Suspicious cases of gastroenteritis raised an alert in the epidemiological surveillance system and triggered investigation. In collaboration with experts, an epidemiological protocol was tailored and promptly deployed to the PDAs of the data collection team. Decision makers followed the progress of the investigation online, using the Web version of the SAFE data collection system. Water sources were shown in the Geographic Information System (GIS) via a dedicated layer and the relevant risk was assessed. As biological samples were analysed in the mobile laboratory, expert centres provided remote support in laboratory analysis and interpretation based on images transmitted via satellite. A tourist with Salmonella typhi was identified and the health alert was communicated internationally to ECDC and WHO by the Early Warning and Response System (EWRS) via the Center for Disease Control (ΚΕΕΛ ΠΙΜΟ) and the Center of Emergency Operations in the Hellenic Ministry of Health.

Earthquake-readiness exercises.

The exercise proved that ICT can assist in rapidly assessing an epidemiological situation and taking appropriate measures. Decision makers were able to track the progress of the epidemiological investigation online, while data mining and statistical analysis identified water from a tank as the most likely cause of the epidemic before the laboratory results were available!

SAFE succeeded in successfully employing satellite, radio and wireless networks, geographic information systems, integration technology and data mining to promptly identify and respond to a disease outbreak.

Satellite communication can augment the overloaded telecommunication infrastructure, thereby providing connectivity to remote and inaccessible areas at short notice and contributing to better coordination and clearer assessment of the crisis. The time required to set up satellite connectivity turned out to be quite short. However, in disaster situations connectivity can be unpredictable and is affected by location and weather conditions. The ability of the SAFE system to operate in disconnected mode turned out to be a critical advantage.

The effective use of ICT in disaster situations, real or 'simulated', requires organizational changes and targeted staff training. At the same time, ICT usability in disaster and post-disaster management is a major issue. Online services need to be simple, flexible and streamlined, taking advantage of different forms of connectivity in a cost-aware fashion. As a consequence, satellite-enabled services need to be refined, adapted and extensively tested in the context of readiness exercises to improve our capacity to issue health early warning and promptly manage outbreaks.

Security and confidentiality are further major issues that can be a source of inefficiencies in the presence of intermittent connectivity if password-based authentication is required.

Technical interoperability and integration of the different systems involved is a key requirement for the seamless support of streamlined workflows when time is critical. The HL7 Clinical Document Architecture and Arden Syntax are vital tools that should be further investigated as part of our future work for seamless service integration.

The exercise identified significant strengths as well as weaknesses that need to be addressed in health early warning systems for public health. At the same time, participants and observers recognized that SAFE offers valuable tools to the 'Epidemic Intelligence' and paves the way towards advanced preparedness and response by lifting communication barriers, promoting collaboration and reducing the isolation of affected areas.

FORTH-ICS coordinated the SAFE demonstration in close collaboration with local authorities, MEDES, France (project coordinator); GMV, Spain; TTSA, France; REMIFOR, France; and medical experts from the University of Verona and the University of Crete. Institutes of epidemiology in Spain (ISCIII-CNE) and France (InVS) ensured compliance with the practices and policies of epidemiological monitoring.

Links:

ICS-FORTH: http://www.ics.forth.gr
SAFE: http://www.medes.fr/safe
Institute for Space Medicine and Physiology, MEDES-IMPS: http://www.medes.fr
European Space Agency: http://www.esa.int
SAFE exercise video: http://www.esa.int/esaTE/SEM7DK73R8F_index_0.html
European Center for Disease Control: http://www.ecdc.europa.eu/
Early Warning and Response System: https://ewrs.ecdc.europa.eu/
World Health Organization: http://www.who.int

Please contact:

Audrey Berthier
MEDES, France (project coordinator):
E-mail: audrey.berthier@medes.fr

Catherine Chronaki
FORTH-ICS, Greece
E-mail: chronaki@ics.forth.gr

Novel Drug Discovery with SIMDAT Grid Technology

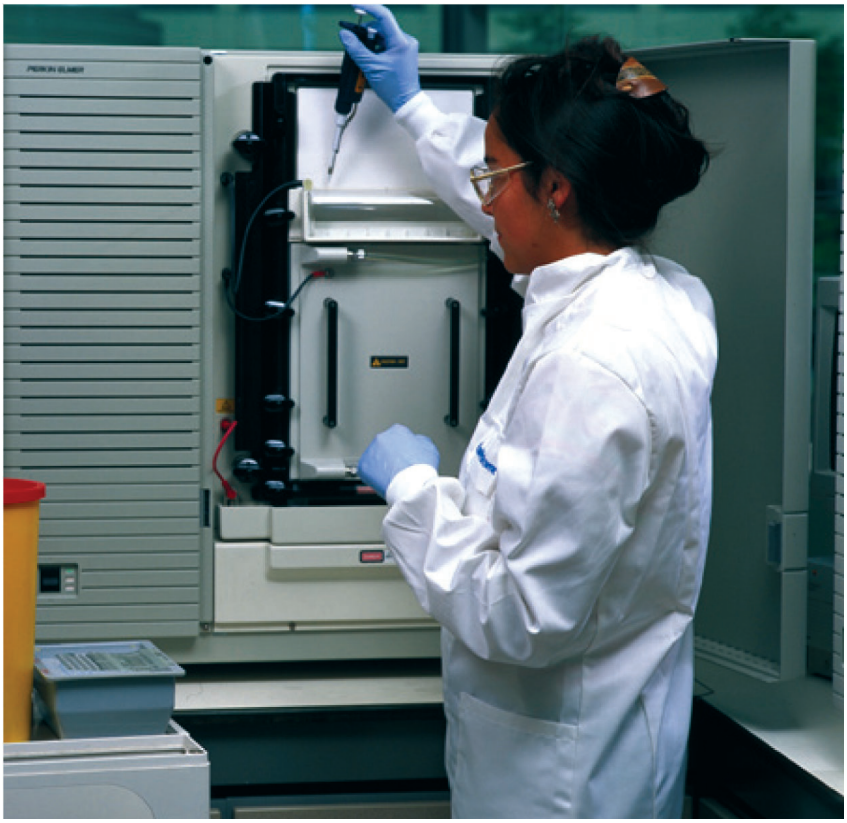
by Yvonne Havertz

Within the European SIMDAT project (Grids for Industrial Product Development) a substantial progress in pharmaceutical analysis has been achieved. It enables pharmaceutical companies to virtualise and globalise their research and development chain, lowering costs as well as considerably improving knowledge exchange between industrial and academic partners.

"One of the most important R&D strategies to achieve a significant gain of efficiency is to tap into external knowledge and expertise through a network of external alliances, sharing the risk, reward and control. Given the large investments in drug research, Virtualisation provides a great savings potential," summarizes Professor Ulrich Trottenberg, director of Fraunhofer Institute for Algorithms and Scientific Computing SCAI, the SIMDAT project co-ordinator, the current challenges in pharmaceutical drug discovery.

"With the distributed nature and diverse location of biological data for disease and medical treatment, it is becoming vital to be able to fast and flexible connect to these resources. Grid as a key part of Information Technology supports the organisations' rapid movement into the virtualised and now more globalised information market," says Rob Gill, Head of Biology Domain Architecture at GlaxoSmithKline (GSK). "The SIMDAT Grid technologies developed by GSK, NEC, Inpharmatica (Galapagos), InforSense and Fraunhofer Institute for Algorithms and Scientific Computing SCAI provide a new business model in the life science sector, which can be considered as a success of the project as a whole."

Usually, establishing new relationships by creating a new virtual organisation (VO) may take up to several months. But the 'Data Grid' paradigm can reduce this to weeks or even days. The VO in this case demonstrates how a pharmaceutical company could partner with an academic group and a vendor company to look at a specific disease and drug target. The duration of this relationship depends on the questions asked and the costs incurred by the interaction. Biotech, on the other hand, has the opportunity to get access to new markets and, hence, is in the position to increase its commercial offer by implementing a finer grained product portfolio.



Gene sequence analysis at GlaxoSmithKline. SIMDAT enables pharmaceutical companies to virtualise and globalise their research and development chain. © GlaxoSmithKline

Knowledge exchange within SIMDAT is not bound to local infrastructure but is tending away from organisational, process and technology limitations. Thus, pharmaceutical companies like GSK have now the possibility to scale their business relationship with both biotech companies like Inpharmatica (Galapagos) and academic partners. That is, they can restrict themselves to exactly those resources they are interested in and are not forced to subscribe to a complete and costly product. This can be realised by new, grid-based middleware components, used to securely and transparently integrate distributed data repositories, in combination with distributed execution of process chains.

Through Virtualisation pharmaceutical companies like GSK are now capable of scaling their business relationship with both industrial and academic partners and take advantage of its great savings potential. In addition, globalisation is getting more and more crucial to keep up in an international context, especially considering the rate of growth of scientific and technical graduates in Asia is already outpacing the United States and Europe. Virtualisation has also the means to benefit from this wealth of knowledge along with developments in the global market.

Current industry applications can already take advantage of SIMDAT technologies. This was successfully demonstrated by a workflow-based test system implemented at GSK by InforSense, consisting of five different remote sites and including data services of two external companies. The development of this workflow is driven by the

need to get high quality, state of the art analysis for pharmaceutical companies from wherever it is best sourced. Thus was shown that pharmaceutical R&D processes can be outsourced across multiple organizations, even if they are using different specifications. Thereby the central industrial requirement for a controlled and secure interaction has been fully addressed through internet security models provided by NEC.

As a powerful tool for knowledge exchange, SIMDAT technology broadens the scope of the drug discovery chain and is able to import the best of bread analysis from both academia and vendors at appropriate costs. It is an ideal showcase for potential providers who are interested in working with pharmaceutical partners in a more collaborative and beneficial manner rather than purely in a simple vendor consumer relationship.

SIMDAT has been funded by the European Commission under the Information Society Technologies Programme (IST). Since it's launch in 2004 SIMDAT has successfully installed Grids in various industrial prototypes in the aerospace, automotive, pharmacology and meteorology sectors.

Link:
http://www.simdat.eu/

Please contact:
Clemens-August Thole
SIMDAT coordinator
Fraunhofer Institute for Algorithms and Scientific Computing SCAI
Tel: +49 2241 14 27 39
E-mail:
clemens-august.thole@scai.fraunhofer.de

Mediated Collaborative Learning

by Kostas Pentikousis and Carmen Martinez-Carrillo

Wikis should be a very familiar Web application for most ERCIM News readers. Once used mainly by the open-source community, wikis are now increasingly being adopted for day-to-day work in large multi-partner and company-internal projects. We have recently been exploring the application of wikis to Computer-Assisted Language Learning (CALL). As we explain below, language in wikis is produced in a collaborative fashion, with all participating members developing and improving the contents of the wiki. Individual contributions motivate the rest of the group to participate in the process of knowledge creation in numerous ways. Following a three-semester study looking at the use of wikis for CALL, our results indicate that they facilitated the simultaneous appropriation of language, technological tools and collaborative skills, often referred to as 'multiacquisition'.

Wikipedia is a classic example of a wiki that has reached international acclaim, and is one of the most frequently cited sources in recent years. While wikis may look like regular Web sites to uninitiated readers, they typically follow an editorial process that is different to traditional Web sites. In principle, users can edit any wiki page, start new pages, and comment and expand on the collectively assembled material. Technically speaking, a wiki is a 'thin-client' application, intuitive in its use with minimal requirements for training, software and hardware. Wikis scale well and benefit from participation of many users. In Wikipedia for example, large user participation was crucial in identifying controversial entries. As with open-source software, wikis allow all interested parties to raise a flag when content is out of line, and corrective actions can be taken promptly.

Wikis are part of the so-called 'Web 2.0', yet Cormode and Krishnamurthy (First Monday, July 2008) point out that popular Web 2.0 sites such as YouTube, Flickr, Facebook and MySpace steer clear of incorporating (and promoting) the ability to collaboratively produce and edit content. On the other hand, features such as tagging (see Figure 1), the listing of friends, connections and followers, and the ability to rate content are far more common. In effect, such Web 2.0 applications emphasize individuality. Moreover, the most successful content providers tend to focus on very specialized topics, often the dominion of a few. Unlike other Web 2.0 applications, wikis put the focus on teamwork, emphasizing the importance of the collective end result. At the same time, wikis allow the primary and secondary contributors to be identified and rewarded accordingly, without losing track of teamwork achievements.

Currently, the biggest challenge in CALL is to find ways to interconnect second-language acquisition theories with those of computer-mediated collaborative learning. Advances in this area are fundamental for developing effective interfaces for learning foreign languages. As language learning can only occur through socializing, the effective use of computers for didactical purposes requires a clear understanding of human interactions online. The Vygotskian sociocultural theories of learning provide a solid interpretation framework for the acquisition of foreign language competence in online environments like wikis. In Vygotsky's view, new knowledge is produced though the social interaction of participants and mediated by cultural artifacts that influence the development of the mind. Learning is mainly understood as a social action, mediated by instruments whose nature depends on the pursued goals. Moreover, sociocultural theories present learning as a process that goes from interpersonal to intrapersonal, first at the social level and then at the individual level.

Given this theoretical background, wikis can be considered as cultural instruments suitable for mediating knowledge. The structure and functional characteristics of a wiki call for language production that is open, dynamic and expansive in nature. In fact, the possibility of linking to new empty pages stands as an explicit open invitation to language and knowledge production for the learner. Language

Figure 1: Tagging is a popular feature of Web 2.0. Illustration: Luca Cremonini, Source: http://upload.wikimedia.org/wikipedia/commons/a/a7/Web_2.0_Map.svg

acquisition occurs in a polycontextual manner that compels group members to apply different skills, depending on the phase of development. Overall, wikis are a polycontextual tool that enables the integration of multiple contexts and voices in the common task of language building.

We completed a set of studies using wikis for mediated collaborative learning of Spanish as a second language (Spanish L2) at the Oulu University of Applied Sciences in Oulu, Finland. After a pilot study with a group of nine students in the spring of 2007, we repeated the study with another group of eighteen students in the fall. In the spring of 2008 we expanded the wiki use to a group of more than sixty students. Our first results of the didactical use of the wiki indicate that it is effective in supporting the shift from individual to collaborative writing. We observed three key changes towards collective responsibility, broad and collective knowledge of the topics, and the emergence of polycontextuality. The wiki as a cultural artifact mediated the collaborative process of language production and enabled the creation of a shared common final product, 'owned' by all the contributors. This is an essential characteristic of collective language production in wikis, and it is fundamentally different from that observed in other synchronous and asynchronous interfaces. Of course, further work is necessary to establish quantitatively the benefits of adopting wikis for CALL.

In the future, we would like to look at the use of wikis in other contexts. This includes both the use of wikis in standard curriculum courses in subjects not related with learning foreign languages and in extracurricular activities. We are also actively looking for partners to expand our current work towards multidisciplinary projects and establish new collaborations.

Link:
http://ipv6.willab.fi/kostas/?wikis

Please contact:
Kostas Pentikousis
VTT Technical Research Centre of Finland
Tel: +358 40 536 9052
E-mail: kostas.pentikousis@vtt.fi

Cross-Language Evaluation Forum – CLEF 2008

by Carol Peters

The Cross-Language Evaluation Forum (CLEF) has been running for nine years now. The results of the CLEF 2008 campaign were presented at a two-and-a-half day workshop held in Aarhus, Denmark, 17-19 September, immediately following the twelfth European Conference on Digital Libraries (ECDL 2008).

The objective of the Cross Language Evaluation Forum is to promote research in the field of multilingual system development. This is done through the organisation of annual evaluation campaigns offering tasks designed to test different aspects of mono- and cross-language information retrieval systems. The intention is to encourage experimentation with all kinds of multilingual information access – from the development of systems for monolingual retrieval operating on many languages to the implementation of complete multilingual multimedia search services. The aim is to stimulate the development of next generation multilingual IR systems.

This year 100 groups, mainly but not only from academia, participated in the campaign. Most of the groups were from Europe but there was also a good contingent from North America and Asia plus a few participants from South America and Africa.

CLEF 2008 Tracks

CLEF 2008 offered seven tracks designed to evaluate the performance of systems for:

- multilingual textual document retrieval (Ad Hoc)
- mono- and cross-language information on structured scientific data (Domain-Specific)
- interactive cross-language retrieval (iCLEF)
- multiple language question answering (QA@CLEF)

CLEF 2008 final session.

- cross-language retrieval in image collections (ImageCLEF)
- multilingual retrieval of Web documents (WebCLEF)
- cross-language geographical information retrieval (GeoCLEF)

Two new tracks were offered as pilot tasks:

- cross-language video retrieval (VideoCLEF)
- multilingual information filtering (INFILE@CLEF)

In addition, MorphoChallenge 2008, an activity of the EU Network of Excellence Pascal, was organized in collaboration with CLEF.

Test Collections

Most of the tracks adopt a corpus-based automatic scoring method for the assessment of system performance. The test collections consist of sets of statements representing information needs known as topics (queries) and collections of documents (corpora). System performance is evaluated by judging the documents retrieved in response to a topic with respect to their relevance (relevance assessment) and computing recall and precision measures.

A number of document collections were used to build the test collections for CLEF2008:

- CLEF multilingual corpus of more than 3 million news documents in 14 European languages
- Hamshahri Persian newspaper corpus
- Library catalog records belonging to The European Library and derived from the archives of the British Library, the Austrian National Library and the Bibliothèque Nationale de France
- English/German and Russian social science data
- The ImageCLEF track used collections for both general photographic and medical image retrieval:
  - IAPR TC-12 photo database; INEX Wikipedia image collection
  - ARRS Goldminer database of radiographs; IRMA collection for medical image annotation
- Dutch and English documentary television programs provided by Sound & Vision, The Netherlands
- Agence France Press (AFP) comparable newswire stories in Arabic, French and English.

Diverse sets of topics or queries were prepared in many languages according to the needs of the various tracks. At the end of the campaign, the result is a number of valuable and reusable test collections.

Workshop

The Workshop plays an important role by providing the opportunity for all the groups that have participated in the evaluation campaign to get together comparing approaches and exchanging ideas. It was held in Aarhus, Denmark, this year and was attended by 150 researchers and system developers. The schedule was divided between plenary track overviews, plus parallel, poster and breakout sessions. There were several invited talks. Noriko Kando, National Institute of Informatics Tokyo, reported on the activities of NTCIR-7 (NTCIR is an evaluation initiative focussed on testing IR systems for Asian languages), while John Tait of the Information Retrieval Facility, Vienna, presented a proposal for an Intellectual Property track which would focus on cross-language retrieval of legal patents in CLEF 2009.

The presentations given at the CLEF Workshops and detailed reports on the experiments of CLEF 2008 and previous years can be found on the CLEF website. The preliminary agenda for CLEF 2009 will be available from mid-November.

CLEF and Treble-CLEF

CLEF 2008 is organized under the auspices of TrebleCLEF, a Coordination Action of the Seventh Framework Programme Over the years, CLEF has done much to promote the development of multilingual IR systems. However, the focus has been on building and testing research prototypes rather than developing fully operational systems. TrebleCLEF is building on and extending the results achieved by CLEF. The objective is to support the development and consolidation of expertise in the multidisciplinary research area of multilingual information access and to promote a dis-

semination action in the relevant application communities.

Treble-CLEF thus has three main goals:
- to promote high standards of evaluation in MLIA systems using three approaches: test collections; user evaluation; and log file analysis
- to sustain an evaluation community by providing high quality access to past evaluation results
- to disseminate knowhow, tools, resources and best practice guidelines, enabling DL creators to make content and knowledge accessible, usable and exploitable over time, over media and over language boundaries.

The aim will be to provide applications that need multilingual search solutions with the possibility to identify the most appropriate technology. For this purposem a series of best practice workshops are being organised:

- Workshop on Best Practices for the Development of Multilingual Information Access Systems, Segovia, Spain, June 2008
- Workshop on Best Practices for System Developers: Bringing Multilingual Information Access to Operational Systems, Winterthur, Switzerland, October 2008
- Workshop on Best Practices in Query Log Analysis, Spring 2009.

A Summer School on Multilingual Information Access is also being organised for June 2009 in Pisa. The focus of the Summer School will be on "How to build effective MLIA systems and How to evaluate them".

More information on the activities of TrebleCLEF can be found on the Web site.

Links:
CLEF: http://www.clef-campaign.org
NTCIR: http://research.nii.ac.jp/ntcir/
TrebleCLEF: http://www.trebleclef/eu
IRF: http://www.ir-facility.org/

Please contact:
Carol Peters
ISTI-CNR, Italy
E-mail: carol.peters@isti.cnr.it

First ERCIM Workshop "Computing and Statistics"

by Erricos Kontoghiorghes

The first workshop of the ERCIM Working Group on Computing and Statistics was hosted by the Department of Computer Science at the University of Neuchatel, Switzerland, 20-22 June 2008.

The workshop was organized jointly with the 5th International Workshop on Parallel Matrix Algorithms and Applications (PMAA'08) and the 2nd International Conference on Computational and Financial Econometrics. All three workshops were founded within the framework of the ERCIM Working Group and were organized by its members. PMAA'08, which was sponsored by the ERCIM WG, was organized in honour of Bernard Philippe (IRISA, Rennes, France), cofounder of the previous WG on Matrix Computations and Statistics. PMAA'08 had four plenary talks, more than eighty sessions with some 380 presentations, and over 400 participants.

Plenary talks were given by Bernard Philippe, INRIA-IRISA, Rennes, France on "A parallel GMRES method preconditioned by a Multiplicative Schwarz iteration. Michael W. Berry fom the University of Tennessee, Knoxville, USA, gave a presentation entitled: "Exploiting nonnegativity in matrix and tensor factorizations to improve topic detection and tracking in text mining". Oliver Linton, London School of Economics and Political Science, UK gave "The FINRISK (Swiss National Centre of Competence in Research "Financial Valuation and Risk Management") Lecture: Iterative smoothing algorithms and their application in finance"; and Herman Van Dijk, Erasmus University Rotterdam, The Netherlands presented "The CSDA (Computational Statistics and Data Analysis) Lecture: Possibly ill-behaved posteriors in econometric models: On the connection between model structures, non-elliptical credible sets and neural network Simulation"

The workshop also provided an occasion to discuss the activities of the Working Group, enhance network activities among its members, and consider future research collaboration within European projects. The next ERCIM Working Group meeting will take place in Cyprus in October 2009.

The ERCIM Working Group "Computing and Statistics focuses on all computational aspects of statistics. Of particular interest is research in important statistical applications areas where both computing techniques and numerical methods have a major impact. All aspects of statistics which make use, directly or indirectly, of computing are considered. Applications of computational statistics in diverse disciplines will be strongly represented. These areas include economics, medicine and epidemiology, biology, finance, physics, chemistry, climatology and communication. The aimof the WG is twofold: first, to consolidate the research in computational statistics that is scattered throughout Europe; second to provide researches with a network from which they can obtain an unrivalled source of information about the most recent developments in computational statistics and applications.

ERCIM Working Groups are open to any researcher in the specific scientific field. Scientists interested in participation should contact the WG coordinator.

Links:
http://www.dcs.bbk.ac.uk/ercim08/
http://www.dcs.bbk.ac.uk/ercim/

Please contact:
Erricos Kontoghiorghes
ERCIM Computing and Statistics WG coordinator, University of London
E-mail:
erricos.kontoghiorghes@ercim.org

ERCIM/W3C at "Internet of Things – Internet of the Future" in Nice

ERCIM/W3C participated in the conference 'Internet of Things – Internet of the Future', which took place in Nice on 6-7 October. More than 800 delegates attended this French European Union Presidency Conference, which was complemented by an exhibition. ERCIM was a sponsor and had a booth and a speaker: Alois Ferscha of the University of Vienna (AARIT) gave a talk in the session 'Architectural issues of the Internet of things'. W3C gave its support to the conference and Philipp Hoschka, W3C Europe Deputy Director, participated in the round table on 'Applications and services of the mobile Internet' by presenting the 'Web of Things' within the scope of the European MobiWeb2.0 project. These activities led to fruitful contacts, in particular with the RFID community.

ERCIM booth at the conference.

European ministers in charge of the digital economy also gathered in Nice for the first European ministerial meeting dedicated to the future Internet. The focus was on the deployment of ultra-high broadband networks, on the creation of new services, and on trust, security and governance of the Internet. The results will be presented at the EU Telecom Council on 27 November 2008.

According to the French Secretary of State for the Development of Digital Economy, "Europe possesses enough key assets to become a leader on technologies and services of the future Internet. Indeed, Europe benefits from both a strong unified market for mobile telecommunications and a world-unique cultural and geographical legacy. Combined together, these resources may trigger Internet-related jobs and services in Europe. However, Civil Liberties and Privacy protection will have to be taken into account so that the future Internet can harmoniously coexist with EU citizens' principles and values. Networks security and stability have also become a major concern for companies and governments. Today, these issues require an enhanced international cooperation."

More information:
http://www.internet2008.fr/

HCI 2009 INTERNATIONAL

Call for Papers

HCI International 2009 – 13th International Conference on Human-Computer Interaction

San Diego, USA, 19-24 July 2009

HCI International 2009, jointly with the affiliated Conferences, which are held under one management and one Registration, invite you to San Diego, California, USA, to participate and contribute to the international forum for the dissemination and exchange of up-to-date scientific information on theoretical, generic and applied areas of HCI through the following modes of communication: Plenary / Keynote Presentation(s), Parallel Sessions, Poster Sessions, Tutorials and Exhibition. The Conference will start with three days of Tutorials. Parallel Sessions, Poster Sessions and the Exhibition will be held during the last three days of the Conference.

Deadlines for abstract receipt
Papers: 20 October 2008
Posters: 23 February 2009
Tutorials: 20 October 2008

Proceedings
The HCI International 2009 Conference Proceedings, comprising the papers to be presented at the Conference, will be published by Springer in a multi-volume set in the LNCS and LNAI series. They will be available on–line through the LNCS Digital Library, readily accessible by all subscribing libraries around the world. All Conference participants will receive in their registration bags the Conference Proceedings published by Springer in DVD format. This DVD will also include, in addition to the papers, the extended abstracts of the posters that will be presented during the Conference. As the DVD will have its own separate ISBN number, posters can also be easily referenced.

More information:
http://www.hcii2009.org

W3C Workshop on Semantic Web in Energy Industries

Houston, Texas, USA, 9-10 December 2008

W3C is organizing a Workshop on Semantic Web in Energy Industries; Part I: Oil & Gas. The high level goal of this workshop is to gather and share possible use cases and/or case studies for Semantic Web in the O&G industry in order to understand the business drivers and benefits of using Semantic Web in that particular area of industry. Participants will explore how Semantic Web technologies can play a role in the management and analysis of the huge amounts of data gathered from highly diverse sources in this sector of the energy industry.

More information:
http://www.w3.org/2008/07/ogws-cfp

ERCIM Working Group Event

SERENE '08 International Workshop on Software Engineering for Resilient Systems

Newcastle upon Tyne, 17-19 November 2008

The SERENE 2008 workshop, held in cooperation with ACM SIGSOFT, is an international forum for researchers and practitioners interested in the advances in Software Engineering for Resilient Systems. SERENE 2008 views resilient systems as open distributed systems that have capabilities to dynamically adapt, in a predictable way, to unexpected and harmful events, including faults and errors. Engineering such systems is a challenging issue which needs urgent attention from and combined efforts by people working in various domains. Achieving this objective is a very complex task, since it implies reasoning explicitly and in a consistent way about systems functional and non-functional characteristics.

SERENE advocates the idea that resilience should be explicitly included into traditional software engineering theories and practices and should become an integral part of all steps of software development. As current software engineering practices tend to either capture only normal behaviour, or to deal with all abnormal situations only at the late development phases, new software engineering methods and tools need to be developed to support explicit handling of abnormal situations through the whole software life cycle. Moreover, every phase of the software development process needs to be enriched with the phase-specific resilience means.

SERENE workshop will focus on topics including:

- formal and semi-formal modelling of resilience properties
- re-engineering for resilience
- software development processes for resilience
- requirement engineering processes for resilience
- model Driven Engineering of resilient systems
- verification and validation of resilient systems
- error and fault handling in the software life-cycle
- resilience through exception handling in the software life-cycle
- frameworks and design patterns for resilience
- software architectures for resilience
- component-based development and resilience
- system structuring for resilience
- atomic actions
- dynamic resilience mechanisms
- resilience prediction
- resilience metadata
- reasoning and adaptation services for improving and ensuring resilience
- intelligent and adaptive approaches to engineering resilient systems
- engineering of self-healing autonomic systems
- dynamic reconfiguration for resilience
- run-time management of resilience requirements
- CASE tools for developing resilient systems.

More information:
http://serene2008.uni.lu/

W3C Workshop on Security for Access to Device APIs from the Web

London, UK, 10-11 December 2008

W3C invites people to participate in a Workshop on Security for Access to Device APIs from the Web to be hosted by Vodafone in London (UK) on 10-11 December 2008. The goal of this workshop is to bring together people from a wide variety of backgrounds (API designers, security experts, usability experts, etc.) to discuss the security challenges involved in allowing Web applications and widgets to access the APIs that allow to control these features (e.g., cameras, gps, address books, etc.).

More information:
http://www.w3.org/2008/security-ws/

Three Researchers from INRIA Receive ERC Advanced Grants

The European Research Council awarded three INRIA researchers in the "Advanced Grant" category in the domains of physical sciences and engineering: Serge Abiteboul and Olivier Faugeras, research directors at INRIA, and Rémi Abgrall, professor at the University of Bordeaux I, seconded to INRIA.

Serge Abiteboul was awarded for the WebDam (Foundations of Web Data Management) project. The project aims to develop a formal and universal framework for describing Web applications that involve complex and flexible interactions. This framework should also serve as a basis for future Web developments, especially data management software.

The ADDECCO (Adaptive Schemes for Deterministic and Stochastic Flow Problems) project of Rémi Abgrall, a specialist in scientific computation, deals with new, increasingly less costly mathematical methods for building numerical models of fluid dynamics that are increasingly more reliable. Rémi Abgrall is a professor at the University of Bordeaux I, seconded to the Bordeaux - Sud Ouest INRIA research center.

The NERVI project of Olivier Faugeras, world-renowned specialist in computer assisted vision, consists of developing a formal framework for describing and understanding complex visual information handling processes in man or machines. Olivier Faugeras is a research director at the Sophia Antipolis - Méditerranée INRIA research center.

Each ERC grant constitutes a subsidy over a maximum period of five years that may amount to more than € 2 million to carry out a large-scale project. This amount allows the researcher receiving the grant to enjoy stable financial and intellectual conditions to bring such a project to fruition.

The ERC announced the first successful candidates in the Advanced Grants competition in the domain Physical Sciences and Engineering (PE) in August. The first call for Advanced Grant proposals was announced at the end of last year with deadlines throughout the first half of 2008. The 28 February deadline for the PE domain generated 997 applications. The peer review process in this domain ran from March to June and involved ten evaluation panels, which have selected 105 Advanced Grants candidates.

Scientists from ERCIM member institutes in Austria (Vienna University of Technology, University of Vienna), Belgium (Université catholique de Louvain), Denmark (Aarhus University), Switzerland (ETHZ, EPFL, Université de Genève) have also been awarded.

More information:
A list of the first 105 winners in the PE domain: http://erc.europa.eu/pdf/AdG1_ListPE_2008-07-31final.pdf

Statistics on all proposals submitted to the first ERC Advanced Grant competition: http://erc.europa.eu/pdf/PressRelease_ERC_AdG1_Statistics_1.pdf

European Technology Platforms Evaluated

European Science and Research Commissioner Janez Potočnik has welcomed the results of a recent evaluation of the 34 European Technology Platforms (ETPs). At a meeting of industrial leaders of European Technology Platforms on 30 September, Commissioner Potočnik praised the ETPs, calling them 'unique and exceptional', and welcomed the results of the survey as overwhelmingly positive.

European Technology Platforms were introduced in 2002 as a way of bringing together basic research and industry to produce 'a long-term strategic plan for research and development of specific technologies with a significant economic and societal impact'. They now cover 34 diverse research areas, including road transport, space technology, wind energy, hydrogen and fuel cell technology, nanotechnologies for medical applications, robotics and water supply and sanitation technology, to name a few.

The evaluation was carried out at the request of the European Commission. Its main objectives were to map the functioning, concept development and objectives of the ETPs; list and analyse their output, results and impact; identify successes, limiting factors and best practices; and formulate recommendations for the future. The report made 18 targeted recommendations to policymakers and ETPs, and 12 concluding points. The evaluation recommended that EU and national policymakers 'clearly and unambiguously continue to support the ETP concept', promoting them more forcefully on the political level.

However, the evaluation also highlights the failure of the ETPs to make research results more easily translatable into new products and services. To remedy the situation, the evaluation recommends that ETPs "move beyond scientific and technological challenges" and instead start focusing on the application of research results. Those platforms which are more advanced and have already developed their SRAs should focus on "the regulations and standards that affect the commercialisation of research". In addition, the evaluation concludes that the platforms have "underachieved" regarding the identification of future education and training needs and recommends the introduction of more initiatives in this field in the near future.

The main conclusions of the evaluation were that, generally speaking, all ETP stakeholders are fairly satisfied (score of 3.5 out of 5). Commissioner Potočnik concluded by saying, 'Over 90% of the nearly 950 respondents to the evaluators' survey of your members and stakeholders said that they would, given their experience of ETPs' involvement so far, gladly renew their membership.

Source: CORDIS, euractiv.com.

Links:
ETPs: http://cordis.europa.eu/technology-platforms/

The full evaluation report is available at:
ftp://ftp.cordis.europa.eu/pub/technology-platforms/docs/evaluation-etps.pdf

Changes in the Italian Delegates on the ERCIM Board

The new member of the ERCIM Board of Directors for CNR is Professor Francesco Beltrame, Director of the Department for Information and Communications Technologies of the Italian National Research Council. The Department is responsible for the coordination of the scientific and technical activities of all the CNR Institutes working in the ICT sector. Professor Beltrame holds the Chair of BioEngineering at the University of Genoa and is President of the Scientific and Technical Committee for Industrial Research of the Italian Ministry of Education, University and Research. Dr Fausto Rabitti, Head of the Networked Multimedia Information Systems Laboratory of ISTI-CNR, is the new member of the Executive Committee.

World Wide Web Foundation

Tim Berners-Lee, inventor of the World Wide Web, unveiled on 14 September 2008 the World Wide Web Foundation, to fulfill a vision of the Web as humanity connected by technology. The World Wide Web Foundation seeks to advance One Web that is free and open, to expand the Web's capability and robustness, and to extend the Web's benefits to all people on the planet. The Web Foundation brings together business leaders, technology innovators, academia, government, NGOs, and experts in many fields to tackle challenges that, like the Web, are global in scale. The launch of the World Wide Web Foundation was supported by the John S. and James L. Knight Foundation with a $5 million seed grant.
http://www.webfoundation.org/

Nicholas Ayache wins the 2008 Microsoft Award

On 20 October in London, the Royal Society and the French Academy of Sciences give the Microsoft 2008 Award to Nicholas Ayache, a research director at INRIA. The honour rewards the outstanding work by this researcher, a pioneer in computational medical image analysis.

Nicolas Ayache first thought of going to medical school before eventually deciding on a career in science. Throughout his years of study, he never lost sight of medicine, taking an interest in information technology's role in medical image data processing. With backing from former INRIA chairman Gilles Kahn, in 1989 he set up a first research project dedicated to medical applications. Today he leads one of the most important computational medical image analysis teams. He has actively contributed to structuring this emerging new discipline in France and internationally, in particular by co-founding a journal, Medical Image Analysis, and co-founding the first International Medical Image Computing and Computer Assisted Intervention Conference (MICCAI). Nicolas Ayache has spearheaded many scientific innovations and breakthroughs. In particular, with his team and his academic, clinical and industrial partners, he has developed groundbreaking multi-dimensional image analysis and simulation methods and image-guided surgery prototypes. The purpose of his research is to help doctors improve diagnosis and therapy.

© INRIA / Photo C. Lebedinsky

Nicolas Ayache

Created in 2006, the Microsoft Award is designed to recognise and reward scientists working in Europe who have made a major contribution to the advancement of science through the use of computational methods. This award of 250 000 euros is handed each year by the French Academy of Sciences and the Royal Society. It aims to support the future researches of the winner
http://royalsociety.org/news.asp?id=8010
http://www-sop.inria.fr/members/Nicholas.Ayache/

New CWI spin-off MonetDB B.V.

To stimulate commercial applications and to disseminate scientific research, CWI founded MonetDB B.V. This independent company will market software products to enhance societal and economic impact of research results. MonetDB B.V. facilitates the efforts of scientific personnel and stimulates joint ventures in specific market segments. "A high tech company, on the one hand close to research and on the other at armslength from venture capitalists, is a very good base to facilitate technical innovation", Martin Kersten, founder and Director of MonetDB B.V. said. The company's primary task is to control, maintain and spread the open source database management system MonetDB.
http://www.monetdb.com/

Photo: Nan Tang, CWI.

MonetDB B.V. founders Peter Boncz, Dick Broekhuis (on behalf of CWI) and Martin Kersten. Not in the photograph are founders Stefan Manegold, Sjoerd Mullender and Niels Nes.

ERCIM
European Research Consortium for Informatics and Mathematics

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its national member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

AARIT
Austrian Association for Research in IT
c/o Österreichische Computer Gesellschaft
Wollzeile 1-3, A-1010 Wien, Austria
http://www.aarit.at/

CNR
Consiglio Nazionale delle Ricerche, ISTI-CNR
Area della Ricerca CNR di Pisa,
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.isti.cnr.it/

Crcim
Czech Research Consortium
for Informatics and Mathematics
FI MU, Botanicka 68a, CZ-602 00 Brno, Czech Republic
http://www.utia.cas.cz/CRCIM/home.html

CWI
Centrum Wiskunde & Informatica
Centrum Wiskunde & Informatica
Kruislaan 413, NL-1098 SJ Amsterdam,
The Netherlands
http://www.cwi.nl/

danaim
Danish Research Association for Informatics and Mathematics
c/o Aalborg University,
Selma Lagerlöfs Vej 300, 9220 Aalborg East, Denmark
http://www.danaim.dk/

fonds national de la recherche
Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

FWO
Egmontstraat 5
B-1000 Brussels, Belgium
http://www.fwo.be/

FNRS
rue d'Egmont 5
B-1000 Brussels, Belgium
http://www.fnrs.be/

FORTH
Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

Fraunhofer Gesellschaft
Fraunhofer ICT Group
Friedrichstr. 60
10117 Berlin, Germany
http://www.iuk.fraunhofer.de/

INRIA
Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

IUA
Irish Universities Association
Irish Universities Association
Cumann Ollscoileanna Éireann
Irish Universities Association
c/o School of Computing, Dublin City University
Glasnevin, Dublin 9, Ireland
http://ercim.computing.dcu.ie/

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and
Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

PEG
Portuguese ERCIM Grouping
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

PLERCIM
Universitas Varsoviensis
Universitas Wratislaviensis
Polish Research Consortium for Informatics and Mathematics
Wydział Matematyki, Informatyki i Mechaniki,
Uniwersytetu Warszawskiego, ul. Banacha 2, 02-097 Warszawa, Poland
http://www.plercim.pl/

Science & Technology Facilities Council
Science and Technology Facilities Council,
Rutherford Appleton Laboratory
Harwell Science and Innovation Campus
Chilton, Didcot, Oxfordshire OX11 0QX, United Kingdom
http://www.scitech.ac.uk/

SpaRCIM
Spanish Research Consortium for Informatics and Mathematics
Spanish Research Consortium for Informatics and Mathematics c/o Esperanza Marcos, Rey Juan Carlos University,
C/ Tulipan s/n, 28933-Móstoles, Madrid, Spain,
http://www.sparcim.org/

SICS
Swedish Institute of Computer Science
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

SARIT
Swiss Association for Research in Information Technology
c/o Professor Daniel Thalmann, EPFL-VRlab,
CH-1015 Lausanne, Switzerland
http://www.sarit.ch/

MTA SZTAKI
Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

VTT
Technical Research Centre of Finland
PO Box 1000
FIN-02044 VTT, Finland
http://www.vtt.fi/

Order Form

If you wish to subscribe to ERCIM News ***free of charge*** *or if you know of a colleague who would like to receive regular copies of ERCIM News, please fill in this form and we will add you/them to the mailing list.*

Send, fax or email this form to:

ERCIM NEWS
2004 route des Lucioles
BP 93
F-06902 Sophia Antipolis Cedex
Fax: +33 4 9238 5011
E-mail: office@ercim.org

Data from this form will be held on a computer database. By giving your email address, you allow ERCIM to send you email

I wish to subscribe to the

☐ ***printed edition*** ☐ ***online edition (email required)***

Name:

Organisation/Company:

Address:

Postal Code:

City:

Country

E-mail:

You can also subscribe to ERCIM News and order back copies by filling out the form at the ERCIM Web site at http://ercim-news.ercim.org/