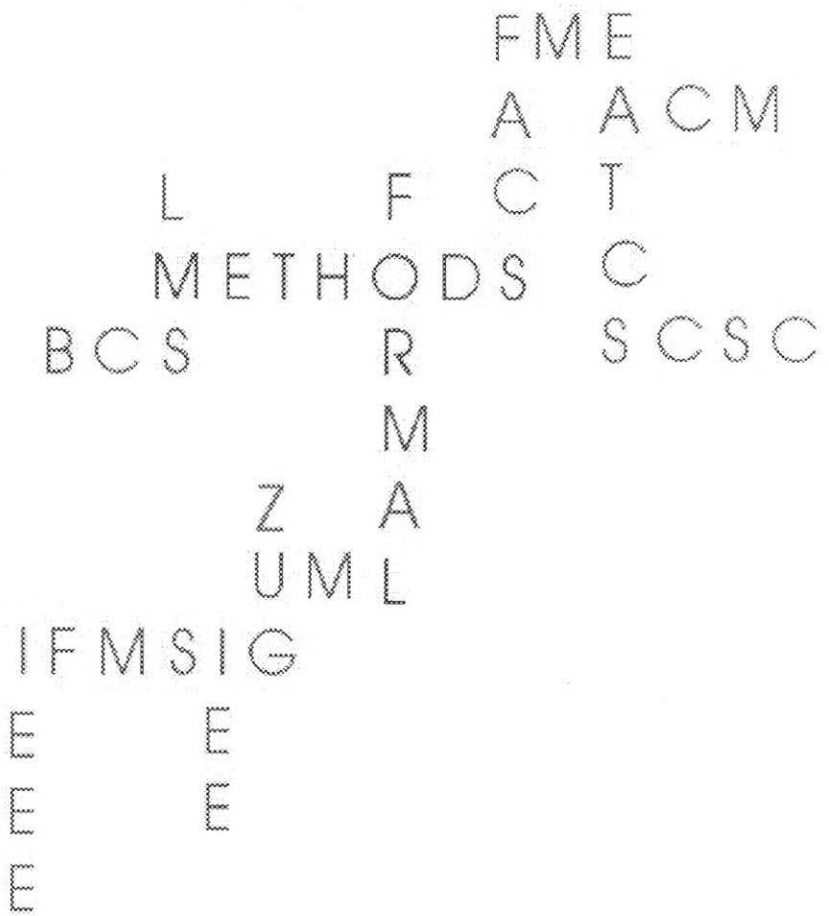
FACS

FACTS

Issue 2005-2
June 2005



BCS FACS

The Newsletter of the Formal Aspects of Computing Science (FACS) Specialist Group

ISSN 0950-1231

About *FACS FACTS*

FACS FACTS [ISSN: 0950-1231] is the newsletter of the BCS Specialist Group on Formal Aspects of Computing Science (FACS). *FACS FACTS* is distributed in electronic form to all FACS members.

As from 2005, *FACS FACTS* will be published four times a year: **March**, **June**, **September** and **December**. Submissions are always welcome. Please see the advert on **page 23** for further details or visit the newsletter area of the FACS website [http://www.bcs-facs.org/newsletter].

Back issues of *FACS FACTS* are available to download from:

http://www.bcs-facs.org/newsletter/facsfactsarchive.html

The *FACS FACTS* Team

Contributors to this Issue:

Dines Bjørner, Eerke Boiten, Jonathan Bowen, Judith Carlton, Roger Carsley, John Derrick, George Eleftherakis, José Fiadeiro, John Fitzgerald, Carroll Morgan, Fiona Polack, F.X. Reid, Paola Spoletini, Marcel Verhoef, Jim Woodcock

Contents

Contents	3
Editorial	4
FACS AGM, 27 April, London	5
ZB2005 Conference Report	10
REFINE2005 Conference Report	17
Train Domain Column	19
Blocking Publication: An Adventure in Destructive Refereeing	24
An Example Railway Domain	29
Book Announcements	40
PhD Abstracts	41
Conference Announcements	45
Job Adverts	48
Formal Methods Coffee Time	49
And Finally	52
FACS Committee	53

Editorial

Jonathan Bowen, BCS-FACS Chair

Welcome to another varied *FACS FACTS* Newsletter, ably compiled by Paul Boca. In particular, we welcome the erudite F. X. Reid, back and in fine form after a well-deserved break from his elucidations. Surely a subscription to FACS is now worth it again for this alone! ☺ Perhaps less inspirational, but also important, a report on the recent 2005 FACS AGM is included in this issue. We welcome Professor Rob Hierons as a new committee member and Chair of a subgroup on *Formal Methods and Testing*, following on from the UK *FORTEST* Network that has recently finished. This year's BCS-FACS Christmas meeting will be organized by Rob Hierons and this subgroup on Monday 19 December 2005, so please do make a note in your diary now. If anyone wishes to form further subgroups of FACS, you are welcome to contact the BCS-FACS Chair with a proposal at any time.

Judith Carlton has taken on the *Puzzles Column* in the Newsletter. We hope that someone will take over reporting of *RefineNet* Network activities (on refinement of formal specifications) from Adrian Hilton. We welcome offers of regular contributions for the Newsletter, as well as one-off items such as conference reports, short technical articles, etc. For example, Fiona Polack reports on the ZB2005 *International Conference of B and Z Users* and a related REFINE2005 conference report by Eerke Boiten and John Derrick in this issue.

There are quite a number of international conferences relating to formal methods in the UK this year, including the major *Formal Methods 2005* conference being held in Newcastle-upon-Tyne in July. FACS is supporting or sponsoring many of these with best paper/presentation prizes or a financial donation for a specific aspect of the conference. We hope to have reports on all events that are sponsored by FACS in this Newsletter, but welcome reports on any relevant conference by FACS members or the organizers.

FACS has started a series of evening seminars, the first of which was delivered immediately after this year's AGM by Professor Steve Reeves of Waikato University in New Zealand, perhaps the furthest formal methods outpost from the UK. We are using the BCS London offices for these, which is a high-quality venue in an excellent location near Covent Garden; this is available free of charge for BCS Specialist Groups, including light refreshments. For those that have not yet visited this new BCS resource, do attend one of these talks if you can and bring a colleague who might be interested in joining FACS! Two further talks are already scheduled and we plan to continue this for the future. Details can be found elsewhere in this issue. The next one is at 5.45pm on Monday 25 July 2005 by Professor Dines Bjørner of DTU, Denmark. There is also an article by Dines Bjørner in this issue. Please note that we would welcome similar talks in non-London locations; if anyone would like to organize or host one, please do get in touch.

As usual, submissions for the next Newsletter are welcome, with a deadline of 19 August 2005. Meanwhile, enjoy this issue, especially the return of F. X. Reid!

FACS AGM, 27 April, London

Roger Carsley, Minutes Secretary

The BCS-FACS AGM was held on 27 April 2005 in the plush BCS London HQ, Covent Garden. As they say, most of the usual suspects were there, but we were pleased to welcome old friend Mike Shields and new friend Rob Hierons.

Your Chairman, Jonathan Bowen, noted the three major events held during the year. He congratulated Ali Abdallah (pictured right), on the success of *CSP 25*, of which proceedings have recently appeared in the Lecture Notes in Computer Science (LNCS) series, volume 3525.

The focus of the Christmas meeting [http://www.bcs-facs.org/events/xmas2004] was the Verified Software Repository, part of the Grand Challenge 6 initiative on Dependable Systems Evolution. It had been very successful in terms of the quality of the speakers, the atmosphere amongst the participants and arrangements at the BCS London HQ. A report on the meeting was published in Issue 2005-1 of *FACS FACTS* [http://www.bcs-facs.org/newsletter/facsfactsarchive.html] and a shortened version has been published in the June issue (Number 86) of the *Bulletin of the European Association for Theoretical Computer Science* (EATCS) [http://www.eatcs.org].

A joint meeting with the BCS Computer Conservation Society on *Program Verification and Semantics* had taken place at the Science Museum. A report on the event has recently been published in the April-June 2005 issue of the *IEEE Annals of the History of Computing, Events and Sightings* section [http://www.computer.org/portal/pages/annals/articles/xtras/a2-2005/EventsandSightings/a2eands.html] and should appear in the Bulletin of the Computer Conservation Society, *Resurrection* [http://www.cs.man.ac.uk/CCS/res].

Jonathan Bowen offered a special vote of thanks to Paul Boca (pictured left) for arranging a series of individual talks, one by Professor Steve Reeves which followed the AGM, with future ones to be given by Professor Dines Bjørner and Professor Muffy Calder. Further details of the seminar programme are available on the BCS-FACS website [http://www.bcs-facs.org/events/EveningSeminars].

Jonathan Bowen (pictured right) also reported that the Committee had held an Away Day at the Union Jack Club in London, reviewing the mission of the group and setting the agenda for the coming years. A brief report on the away day appeared in Issue 2005-1 of *FACS FACTS*.

Paul Boca, wearing another of his many hats as Membership Secretary, reported that there were 71 paid up members (up from 56 in 2004) and that the mailing list had 237 members (up from 151). He also reminded us that the

benefits of FACS membership include 25% discount on Springer books and 20% discount on the *Requirements Engineering* Journal.

Mike Stannett (pictured right), who has made such a success of our website [http://www.bcs-facs.org], said that it now occupied 29Mb and had received 32,000 hits so far this year. Plans are underway to move the site from London South Bank University to a commercial server, enabling more sophisticated website features in the future. Mike Stannett is busy converting the website to use PHP and will implement the new web infrastructure in due course. If there are particular features you would like to see on the FACS website, please do contact Mike Stannett [m.stannett@dcs.shef.ac.uk].

Rob Hierons (pictured left) informed the Committee that the FORTEST [http://www.fortest.org.uk] project was coming to a close after three and a half years of EPSRC funding. Jonathan Bowen proposed that a subgroup of FACS, on *Formal Methods and Testing*, be formed and that Rob Hierons be its Chair to carry on the good work. This was carried unanimously.

Jawed Siddiqi (pictured right), your Treasurer, reported on the health of the Current account which had some heavier outgoings in the last year with the cost of the Away Day and sponsorship for events in the UK, particularly FM'05 [http://www.csr.ncl.ac.uk/fm05]. FACS events have been financially sound, either breaking even or returning a small surplus. Any surplus is ploughed back in to fund FACS activities.

Jawed Siddiqi raised four issues:

- Subscription fees: should these be increased? This generated a lively discussion, and various scenarios were put forward. The committee decided against an increase.

- Priorities: knowing the membership's priorities amongst FACS activities would help the committee set a budget to meet these needs. Soliciting the opinions of the membership will take place in due course.

- Budget: a draft budget based on current spending and event budget was being prepared for circulation to the committee for approval.

- BCS Specialist Group Finances: FACS accounts, and all other specialist groups, will be managed centrally. This is a measure by the BCS to cut down the administrative duties carried out by treasurers, leaving them to concentrate on budgeting and raising funds. FACS has been assured it would not lose its independence.

The election of the Officers and Committee members then took place. All existing members were willing to continue in their current roles. It was agreed that Paul Boca assume the additional role of FACS Secretary to meet BCS expectations and in recognition of his very active role on the Committee. The Committee now has the following membership and responsibilities. There is an overall Executive Committee consisting of:

Chairman	Jonathan Bowen
Treasurer	Jawed Siddiqi
Secretary	Paul Boca

These members will represent the rest of the FACS committee at any meetings/discussions held with the BCS itself. The remaining committee roles are as follows:

ZUG Liaison	Jonathan Bowen
Minutes Secretary	Roger Carsley
Membership Secretary	Paul Boca
Newsletter Editor	Paul Boca
BCS Liaison	Margaret West
Publications	John Cooke
Events Coordinator	Ali Abdallah
Web Development	Mike Stannett
Industrial Liaison	Judith Carlton
UML Liaison	Kevin Lano
FME Liaison	John Fitzgerald
Chair of FM & Testing	Rob Hierons

The AGM was followed by a seminar from Steve Reeves, entitled *FM@Waikato*. A report on the seminar will be published in Issue 2005-3 of *FACS FACTS*.

The FACS Committee will have an informal meeting at FM05, and the Executive Committee will meet before each evening seminar to discuss any FACS-related issues. If you have any comments on FACS, please do get in touch.

Getting in touch

Roger Carsley
Univ. of Westminster
roger@wmin.ac.uk

FACS Committee
info@bcs-facs.org.uk

Formal Methods Community Project

Wanted! Back issues of *FACS FACTS* or *FACS Europe*

The FACS group would like to archive *all* of its newsletters and make them available on the FACS website for downloading and viewing. If you can help, please email us on info@bcs-facs.org.uk. Help with scanning would be appreciated.

http://www.bcs-facs.org/newsletter/facsfactsarchive.html

Back to Contents page

Formal Methods 2005

18-22 July 2005 - Newcastle upon Tyne, UK

Call for Participation

www.csr.ncl.ac.uk/fm05

It is our pleasure to invite you to attend FM'05, the leading international conference for researchers and practitioners in formal methods for the development of computing systems. This year, the conference is being held in Newcastle upon Tyne, UK on 18-22 July.

Formal methods continue to have a major impact on systems and software engineering, especially in areas where dependability, security and trust matter. FM'05 aims to publish the latest developments of interest to researchers and practitioners alike. The outstanding programme of tutorials and workshops (listed overleaf) covers the range from circuit design, through high integrity programming to fault tolerance, architectures and automated reasoning. The programme of around 30 research papers, announced in mid-April, will provide an opportunity to get up to date in all these areas and more. Alongside the tutorials, workshops and research symposium, there will be displays of tools, products, research projects and publishers.

FM'05 is being held in one of England's most dynamic cities, famous for its captivating welcome, and situated at the heart of an historic and beautiful region. There will be plenty of opportunity for informal discussion, and social activities include a reception at the Hatton gallery and conference dinner in Alnwick Castle and Gardens.

We look forward to welcoming you to Newcastle in July!

John Fitzgerald, General Chair
Ian Hayes, Andrzej Tarlecki, Programme Chairs

TO REGISTER – download a form from www.csr.ncl.ac.uk/fm05
or contact the Organizer: Claire Smith, tel: +44 (0) 191 222 7999,
email:claire.smith@ncl.ac.uk

Full Scientific Programme, 20–22 July

See the full programme online at **www.csr.ncl.ac.uk/fm05**

Invited Speakers:

Mathai Joseph (Tata Research & Development, Pune, India)
Marie-Claude Gaudel (Université de Paris - Sud, France)
Chris Johnson (University of Glasgow, UK)

Industry Day: 20 July

Co-located Conferences (18–19 July):

Calculemus 2005
Formal Aspects of Security and Trust (FAST) 2005

Workshops (18–19 July):

Grand Challenge Workshop on Dependable Systems Evolution
Web Languages and Formal Methods (WLFM 2005)
Overture – the future of VDM and VDM++
Practical Applications of Stochastic Modelling (PASM 2005)
Workshop on Rigorous Engineering of Fault Tolerant Systems (REFT 2005)
The Railway Domain (TRain 2005)

Tutorials (18–19 July):

The Spec# Programming System: an Overview
Formal Aspects of Software Architecture
Perfect Developer
SPARK
Petri-nets and Role Models as Intermediate Level Tools for Asynchronous Circuit & Systems Design
Verifying Industrial Control System Software
Formal Engineering Methods for Industrial Software Development
Modelling Languages Spectrum
Formal Methods as a Unifying Basis for Electrical and Computer Engineering
Design by Contract and Increased Dependability of Java applications with JML
Introduction to CSP and FDR

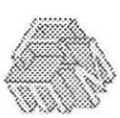
TO REGISTER

Download a registration form from:
www.csr.ncl.ac.uk/fm05

Or contact the Organizer:
Claire Smith, tel: +44 (0) 191 222 7999, email: claire.smith@ncl.ac.uk

---

FM'05 is sponsored by Formal methods Europe, the Centre for Software Reliability and SAP



CSR

SAP

ZB2005 Conference Report

Fiona Polack

The fourth *International Conference of B and Z Users* (ZB2005) [http://www.zb2005.org] was held at University of Surrey, Guildford, UK, April 13–15, 2005.

The B and Z formal methods share a conceptual origin. They are leading approaches in industry and academia for the specification and development (using formal refinement) of computer-based systems. ZB2005 simultaneously incorporated the 15th International Conference of Z Users and the 6th International Conference on the B Method.

ZB2005 was hosted by the Department of Computing, University of Surrey. The department has an established history of collaboration with industry, and has recently strengthened its formal methods involvement, establishing a new research group under the leadership of Professor Steve Schneider. The group provided the local organisation for ZB2005.

Professor Steve Schneider (pictured right) was conference chair; Dr Helen Treharne (pictured below) chaired the B programme committee; Dr Steve King and Professor Martin Henson co-chaired the Z programme committee. The poster session was chaired by Dr Neil Evans, and a tools demonstration organized by Dr James Heather. The conference sponsors were AWE (Atomic Weapons Establishment), BCS-FACS, FME (Formal Methods Europe), ZUG (Z User Group), Royal Holloway, University of London and the Guildford Branch of the BCS. AWE sponsored the student poster session, providing bursaries for those students presenting their posters.

Over 80 people attended the conference, with the majority from France (20) and UK (41); in addition, European delegates came from Finland (2), Germany (3), Sweden (1) and Switzerland (2). There was a significant contingent from Australia (5) and New Zealand (4), with other delegates from China (1), Japan (1), and the United States (2). A notable absence from the conference, for the first time in 15 years, was the ZUG Chair, Professor Jonathan Bowen. The meeting expressed its appreciation for Professor Bowen's commitment to ZUG and formal methods over the years. The social programme comprised a reception at Guildford Guildhall, dinner at Loseley Park, and optional tours of the Surrey Space Centre.

On the day before the main conference, there were **tutorials** on *expectation-based reasoning* for sequential probabilistic programs (Carroll Morgan); *ProB: a verification and validation tool for the B method* (Michael Leuschel, Michael Butler and Stephane Lo Presti); *a case study of a complete*

reactive system in Event_B (Jean-Raymond Abrial); *developing Z tools with CZT* (Mark Utting and Petra Malik); and *model-based testing using formal models from theory to industrial applications* (Bruno Legeard and Mark Utting). The RefineNet Workshop, proceedings of which will appear as an Electronic Notes in Computer Science (ENTCS) publication, also took place. A report on that workshop can be found on page 17 of this issue.

The International B Conference Steering Committee (APCB) and the Z User Group (ZUG) held general meetings during the conference. It was agreed that the 7th International Conference on the B Method would be held at Besancon, France, in January 2006. ZUG is investigating a non-European venue for the next International Conference of Z Users.

The ZB2005 **conference papers** covered case studies, theoretical advancements and developments in tool support. It was encouraging to see that those reporting advancements in tool support scrutinised their applicability to larger problems. Scalable support for formal methods is still an active area of work, which is essential to the continued success of these methods. Many of the theoretical papers were challenging the limitations of current theory; this gives the potential for formal methods to model more complicated systems. A common theme here was that it is not always appropriate to reject practical advances simply because they do not address all pathological cases.

Many of the case studies and techniques presented demonstrate the viability of applying our formal techniques to today's systems and applications; for example there were papers describing validation of DVD navigation, the design guidelines for GUIs and web-based system applications.

Among the conference papers and presentations, Jean-Raymond Abrial, Dominique Cansell, Dominique Méry won the **best paper prize** for their paper, *Refinement and Reachability in Event_B*. Benjamin Long won the prize for **best student presentation**, for his *Formal Verification of a Type Flaw Attack on a Security Protocol using Object-Z*. A **student poster prize** was awarded jointly to Jean-Marc Mota, *Development of Geometric Modelling Algorithms using Event B: a case study* and Wilson Ifill, *Achieving B State Machine Designs with Annotations*. Prizes were sponsored[1] by BCS-FACS, and included a subscription to volume 17 of the *Formal Aspects of Computing* journal and 2005 membership of BCS-FACS.

The three **invited talks** reflected the diverse nature of the issues addressed by the conference more generally. The speakers are all well-known proponents of formal methods, and have many years' experience of academic and industrial research, as well as practical experience of leading uses of formal methods in industry.

Professor Cliff Jones (Newcastle University) has wide experience in industry and academia. With IBM, he worked on VDM development. At Manchester University, he developed the formal methods group and

[1] BCS-FACS would like to thank Springer [http://www.springer.co.uk] for kindly donating the 4 *Formal Aspects of Computing* journal subscriptions that were given as prizes at ZB2005.

participated in the Alvey Software Engineering project. He was influential in formal development methods for concurrent systems. His current roles include project director of the EPSRC's Interdisciplinary Research Collaboration on Dependability of Computer-Based Systems (DIRC).

DIRC [http://www.dirc.org.uk] is a collaboration of five UK universities, with agreements for at least six years' funding. The DIRC research team includes computer scientists, psychologists, sociologists and statisticians. The team is generating exciting ideas and novel approaches to the development of systems involving computers and people. The surprise has been that the computer scientists are acting as a bridge among the other members.

Professor Jones' talk was entitled, *Specification before Satisfaction.* An extended abstract appears in the proceedings. His theme was the need to look beyond the proof that program *P* satisfies program *S (p sat s)* particularly in relation to the UKCRC's Grand Challenges in Computer Science. He reminded the audience that by the time developers are doing proof, it is too late to clean up the architecture of the specification. Despite low error rates, poor architecture means that it is impossible to know what is going on in much modern software. In contrast, Professor Jones recommended the recent work on the B method and Event_B, led by J.-R. Abrial at ETH Zurich, Switzerland.

Various authors, including the sociologist Donald Mackenzie (now in DIRC) and John Rushby, have pointed to poor specification and model mismatch as primary causes of serious faults. A key task in improving dependable systems is to reduce the risk of cognitive mismatch. Professor Jones illustrated his point with various well-known safety incidents where there had been a lack of contextual information that might have allowed operators to assess causality and severity.

DIRC is looking at *advisory systems* for assisting the operator in relating control functionality to observed reality. These systems raise some interesting failure modes, because the advice presented to the operator does not have to be followed. Analysis of experimental data by DIRC statisticians shows that advisory systems also give false assurance; a particular advisor system helped users who were less experienced; however, the decisions of experienced users were less accurate, but made with greater confidence. Professor Jones made two observations: firstly, it is not sensible to have an advisory system doing what people are good at; secondly, developers must take into account the side effect of artificially reinforced confidence.

In people-systems, *modelling people processes* has been much used. This should not simply be concerned with converting people-processes into sequential programs. People are usually in the system to reduce errors, and are hard to model well. Usually, a system has significantly more internal state than is presented to the user; operator interfaces comprising a pre-planned portfolio of operations reduce information that might be used by the human to return a system to a safe state.

With Ian Hayes and Michael Jackson, Professor Jones has researched *reliance conditions*; these can be used to define what a component must provide and what it can expect from the wider system. This approach can be used to produce advisory systems based on heuristic estimations of tolerances and response rates. The development does not just specify the target part of the system, but looks first at the wider system context.

Following on from reliance, developers need to understand that failures do occur, and that the system must be designed so as to *contain the effect of failures*. Although many human processes are flawed, computer systems can benefit from procedures such as instruction repetition and dual-authority. Fault containment barriers need to be formalized; infringements, even micro-errors, should be analysed. Developers must remember the reductions in robustness that can result from optimization.

Consideration of the use of *classifications*, to improve the usability of data, led Professor Jones to note the importance of structures such as menu classification in providing scope for evolution. An important DIRC exploration is into the evolution of systems, based on the need to distinguish what may and must not be allowed to change. Studying a customisable management system reveals the problems that arise when the fixed parts of the underlying non generic system constrain customisation, or where the permitted customisation is specific to a particular culture.

Two further examples of interdisciplinary experiences from DIRC were a psychology experiment on students to explore Weinberg's observation that we could make programs more dependable if we knew how people programmed; and work on models of time involving sociologists and Professor A. Burns' real-time systems research.

Professor Jones' conclusion was that interdisciplinary research is fun but challenging and hard to publish. He stressed the importance of people not only talking, but *listening* to each other. Understanding of other disciplines' world view was important - for instance, sociologists are excellent analysts of existing situations, but do not hypothesise solutions.

The second invited talk was from **Professor Carroll Morgan (Australian Professorial Fellow at the School of Computer Science and Engineering, University of New South Wales)**. Professor Morgan has contributed to developmental work on Z, B and probabilistic systems; this work was the basis for his talk, entitled *The challenge of probabilistic B*. An extended abstract appears in the proceedings. Since 2003, Professor Morgan has been building on ten years of existing research, as part of a five-year project to create a theory of probability for formal development. Recently, he has worked on his ideas with J.-R. Abrial and with Thai Son Hoang.

The talk focused on *Rabin's randomised mutual-exclusion algorithm*. Rabin's original probabilistic algorithm contained an error, which was identified by a PhD student. Professor Morgan's goal for this piece of work was to prove the fairness of the algorithm (that a process has a one-third chance of access to a resource). A secondary goal is to understand how to formally develop a system, so that probabilistic properties hold by construction.

Professor Morgan gave a detailed description of Rabin's papers and of the B models constructed to understand the algorithm. A process that wants a resource takes a "local" lottery ticket, with a random number. This is compared to a single "global" lottery ticket. If the local ticket is greater, then it gains access to the resource. Local tickets have random values based on a Bernoulli distribution; Rabin's insight into the Bernoulli distribution is that the chance of a tie in the maximum value is no more than one third. Earlier algorithms, such as that by Ben Ari, calculated probability on the basis of the number of processes in the system and are less "fair".

Professor Morgan commended the approach taken by Michael Butler's group, using probabilistic action systems; this is sensible because the semantics of probabilistic sequential programs are known. However, in Event_B, the aim is to achieve small atomic events with minimal structure, so the probability needs to be in the guards, not within the processes.

To accommodate probability, the B syntax had to be extended with a probabilistic internal choice. In the specification of Rabin's algorithm, a Boolean variable, *win*, is set with probability *C* of *TRUE* and *1/C* of *FALSE*. The *win* variable becomes the guard on the resource-allocation, and the probability has been moved from the internals of the algorithm to the event guards. The introduction of distribution-valued variables does not work in general, because of the refinement issues, but is compatible with a proper probability semantics. Professor Morgan explained how undesirable interleaving can be controlled, with events to map the actions of other events.

The map events refine a high-level *skip*. For probabilistic B, there is no complete rule for the whole refinement. With Thai Son Hoang, Professor Morgan is looking at ways to use conventional B refinement, by constraining probabilities, and by providing taxonomies or patterns of what is and is not refinable using forward and backward rules. The specification of Rabin's algorithm also highlights the problem of combining demonic and probabilistic choice; guarded command language semantics allow demonic choice to see entire state, but we must ensure that the demonic choice cannot see the Bernoulli choice.

Professor Morgan stressed the importance of tackling big problems through small case studies, pulling together findings of many researchers across the field, an approach also used on the IBM Z project, and by J.-R. Abrial and the B-method researchers. Professor Morgan commended the practical focus of the B community, and its general acceptance that, in practice, we can ignore pathological cases and focus on core semantic issues.

Frédéric Badeau (ClearSy System Engineering) was the final invited speaker. Dr Badeau has been working with the B method since 1994. ClearSy markets Atelier B, and has used the B method on large industrial projects with Alstom, Peugeot, Siemens, RATP, SNCF and others. The company also conducts research and development work. Formerly with Siemens, Dr Badeau worked on an Ada translator, for the Météor project, and on the training of industrial users. He has been involved in a bid for the New York Metro system, and in a train protection system for SNCF. His talk, entitled *Using B as a high level programming language in an industrial project*, described his work, with Arnaud Amelot of Siemens, for the Roissy VAL wayside control unit (WCU). A full paper appears in the conference proceedings.

The WCU project is part of the driverless internal airport shuttle service at Roissy Charles de Gaulle Airport. Siemens Transportation Systems (formerly Matra) is working on the trains and their operating systems. The B parts of the development have been sub-contracted to ClearSy. Whereas several papers at the conference considered the changes being introduced for Event_B, or, in the case of Professor Morgan's invited talk, probabilistic B, WCU uses the traditional B Method for safety-critical aspects. Dr Badeau reflected that it might be possible in future to use Event_B at the system level. The aim of using B is to obtain correctness by construction — Siemens no longer uses unit testing.

Siemens has devised a process for using B to build this sort of software. Tools are used to provide automatic checking and refinement.

The WCU is part of the project to link the old and new airport terminals; there are two tracks with five crossovers. There is also a side-line for parking and maintenance of trains. Each line section has controller equipment, and the WCU effectively pilots the driverless trains. The specification contains hundreds of variables etc. The developers must seek a balance between the benefits of constructing something in B so that it is correct and controlling the software development costs. Dr Badeau noted that most other airport shuttle systems are much simpler, relying on hardware logic. However, some material could be reused from a similar project at Chicago Airport.

At the outset, Siemens provided detailed WCU software specification documents. The specification was formalized as an abstract model such that all the requirements were expressed in B. The proof of safety properties was constructed for the abstract model. As always, there is a problem validating the abstract model; we cannot prove the informal-formal mapping. Instead, the developers relied on review and inspection by human engineers. Dr Badeau explained how the developers had striven to approximate the ideal, with a minimal gap between the informal specification and B, to reduce mistakes.

The system specified block logics for line sections, making the only issue that of knowing if there is a train occupying a block. There is a *route logic* for transfer among blocks. It is a light rail system with one operating speed per program section — arriving in the station, switching, departure, etc. — so a *mode logic* is used to determine which program controls a train in each sections and blocks. The B *abstract model* architecture follows the functional breakdown architecture. Inspection is facilitated because the architecture of the specification is clear in the B. Proof that properties were preserved under composition of components was achieved by feeding back properties from postconditions to the root of the structure tree in which the left-right ordering reflects dependence.

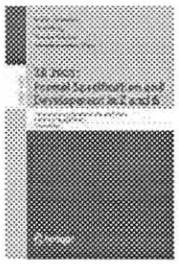
Once they were happy with the abstract model, Dr Badeau's team followed the B Method through to code. Refinement proves that the intermediate levels comply with the abstract model. Atelier B automatically translates the concrete model to Siemens' *Digisafe* Ada subset, and ensures no run time errors.

The *concrete model* was constructed by people who did not know the project but can work from a formal abstract model. Thus, the concrete model and implementation no longer rely on domain knowledge. The development achieved 100 percent "well implementation" proof (refinement). Automatic refinement is used for repetitive parts, to save time. Siemens developed this process after the Météor project, using the *EDiTH B* and *Bertille* tool-sets. Some manual preparation is required, to split the abstract model into practical sub-modules, and to link implementations with intermediate refinements.

The abstract model took twice as long as the concrete; one indicator of success is that the project would not have finished on time without the automatic refinement. In relation to Professor Jones' comments, about a third of the development time was spent asking questions about the initial specification documents.

In conclusion, Dr Badeau reminded his audience that this was a traditional B end-to-end development. Siemens' process used B as a high-level

programming language, not as a visualisation aid. Proofs of properties strengthen confidence in the models. A lot of patterns and genericity were used, and automatic tools were used wherever possible. The result is software that is correct by construction. Siemens had been forced to use B on Météor, but now uses it out of choice.



The conference proceedings are published in the Lecture Notes in Computing Science series, volume 3455: Helen Treharne, Steve King, Martin Henson, Steve Schneider (Eds.) *ZB 2005: Formal Specification and Development in Z and B – 4th International Conference of B and Z Users*, Guildford, UK, April 13 - 15, 2005, Proceedings, Lecture Notes in Computer Science 3455, Springer, ISBN 3-540-25559-1, XV+493 pages.

Acknowledgements

Thanks to Helen Treharne, for conference details and photographs, and to Susan Stepney, Carroll Morgan and Ken Robinson for photographs.

Getting in touch

Fiona Polack
University of York

fiona@cs.york.ac.uk

BCS-FACS Evening Seminars

25 July 2005

Professor Dines Bjørner (DTU, Denmark)
Domain Engineering

21 September 2005

Professor Muffy Calder (University of Glasgow)
Formal Methods Meets Biochemical Pathways

Seminars are held at the BCS London Office, near Covent Garden:

First Floor, The Davidson Building
5 Southampton Street
London WC2E 7HA

Seminars start at 5.45pm; refreshments served from 5.15pm. If you would like to attend, for access to the BCS building please pre-register by emailing Paul Boca [paul.boca@virgin.net]

Back to Contents page

REFINE2005 Conference Report

Eerke Boiten & John Derrick

A lively meeting of the Refinement Workshop was held in April, co-located with ZB2005 [http://www.zb2005.org] in Guildford, Surrey. Twelve talks were spread over the day, the proceedings appearing in the Electronic Notes in Theoretical Computer Science (ENTCS) series. Covering a spectrum from theory, through UML, MDA, automation ..., the workshop provided a good snapshot on the current state-of-the-art in this area. In addition, the ZB conference (see report on **page 10**) contained several papers on refinement, indicative of the amount of interest in this subject at the present.

A best paper prize was sponsored by BCS-FACS, and won by Susan Stepney for her paper on *Breaking the model: finalizations and a taxonomy of security attacks* (co-authored with J. Clark and H. Chivers).

Work reported on automation included the use of theorem provers, model-checking and Alloy. Two sessions on theory covered issues in logic, unifying theories, concurrency, probabilistic approaches and security. The final session contained talks in UML, MDA and non-classical applications. Martin Henson served as the official photographer, and the organizers were grateful to the ZB conference for hosting the workshop and providing local organization.

The workshop was sponsored by the EPSRC through its funding of the RefineNet network [http://www.refinenet.org.uk]. A special issue of the *Formal Aspects of Computing* journal [http://www.springeronline.com/journal/00165] will be devoted to extensions of the best workshop papers.

List of Refinement workshop papers

Using the Alloy analyser to verify data refinement in Z
C Bolton

Model checking downward simulations
G Smith and J Derrick

Simpler reasoning about system properties – a proof by refinement technique
D Atiya and S King and J Woodcock

Angelic non-determinism and unifying theories of programming
A Cavalcanti and J Woodcock

νZ – a wide spectrum logic
M Henson and B Kajtazi

An analysis of operation refinement in an abortive paradigm
M Deutsch

Verifying concurrent data structures by simulation
R Colvin, S Doherty, L Groves and M Moir

Tank monitoring: a pAMN case study
S Schneider, T Hoang, K Robinson and H Treharne

Breaking the model: finalisations and a taxonomy of security attacks
J Clark and S Stepney and H Chivers

Refinement patterns for UML
K Lano and K Androutsopolous and D Clark

Refinement via consistency checking in MDA
R Paige and D Kolovos and F Polack

Emergent properties do not refine
F Polack and S Stepney

Getting in touch

Eerke Boiten
University of Kent
E.A.Boiten@kent.ac.uk

John Derrick
University of Sheffield
J.Derrick@dcs.shef.ac.uk

Grand Challenges 6 Workshop on Dependable Systems Evolution

18 July 2005

www.fmnet.info/gc6/fm05

The UK Computing Research Committee has been discussing how best to advance computing research; they held a workshop in Edinburgh in November 2002, which produced seven proposals for grand challenges in computer science. This workshop is part of a series that brings together international researchers to discuss the sixth challenge on Dependable Systems Evolution, which was inspired by the challenge of the Verifying Compiler.

The long-term aim of the project is to produce a coherent software engineering tool-set based on formal principles, to aid in the development, deployment, and evolution of dependable systems; and to submit the tools to convincing large-scale evaluation on a heterogeneous range of challenge codes. The aim of this particular workshop is to produce an authoritative account of the current state of the art in strong software engineering tool-sets, and their application to systems that have been deployed in practice.

Speakers include

- Dines Bjørner, DTU, Denmark
- Michael Butler, University of Southampton, UK
- Patrice Chalin, Concordia University, Canada
- Rod Chapman, Praxis High Integrity Systems, UK
- David Crocker, Escher Technologies, UK
- Joseph Kiniry, University College Dublin, Ireland
- Cliff Jones, University of Newcastle upon Tyne, UK
- Colin O'Halloran, QinetiQ, UK

Organizers: Jonathan Bowen and Jim Woodcock (GC6 Chair).

The workshop is sponsored by the British Computer Society

Back to Contents page

Train Domain Column

Dines Bjørner

General Status

Progress is slow. But it probably has to be. Membership of the TRain effort currently stands at **113 members** from **36 countries**. But we still need them and the TRain organizers to work harder. To help create some momentum we are glad to be able to use *FACS FACTS*.

An Example Railway Domain Narration & Formalization

On page 29 of this issue of *FACS FACTS*, there is an approximately 10 page example of which only some 6 pages cover an actual domain model. Studying it should challenge you to submit commensurate, contrasting, alternative, or other styles, kinds and forms of domain models for railways.

TRain Workshops

We are organizing two workshops this summer: TRain@FM05: At FM05 [http://www.csr.ncl.ac.uk/fm05], we are organizing a one day workshop, 19 July 2005, Newcastle, UK.

TRain@SEFM2005: At SEFM2005 [http://sefm2005.uni-koblenz.de] we are organizing a one and a half day workshop, 5–6 September, Koblenz, Germany.

Please visit these conference home pages, as well as clicking on the events section on the Train Domain webpage [http://www.railwaydomain.org/]. Also see http://www.railwaydomain.org/PS/train-ws.ps .

The TRain Web Pages

Martin Pěnička is in charge of organizing our web pages [http://www.railwaydomain.org/]. They are regularly updated. If you are not already a member, please join. Please email Martin Pěnička [penicka@fd.cvut.cz] and Dines Bjørner [dines@bjorner.biz] electronic copies of your papers on the transportation domain.

The Meaning of 'TRain'

'TRain', seen narrowly, stands for The Railway domAIN. More broadly, it stands for TRAnsportatIoN (or TRAnsportation domaIN).

Towards A Train Research Strategy

Jim Woodcock and Dines Bjørner

TRain Research is currently seen to evolve along two axes:

(1) The TRain Repository and
(2) TRain Domain Modelling.

This TRain Column item addresses the former. The latter has been covered in our first column item (Issue 2005-1 of *FACS FACTS*, March 2005) and is illustrated in Dines Bjørner's fragment domain model in the present issue (see page 29).

The TRain Repository

Before safety-critical software (and in general any software) can be designed, requirements must be formulated; before requirements can be formulated, the application domain must be understood. All other engineering branches build on theories of their own application domains: Newtonian mechanics provides the basis for automotive engineers; aerodynamics for aircraft designers; and hydrodynamics for ship designers. In the same way, software engineers developing software for rail applications must build on a theory of the railway domain. But there is no such theory.

TRain is a loosely knit group of international researchers and technologists who are interested in establishing a theory for transportation domains, specifically including railways. The scope of this theory includes diverse models of railway facets, from rail nets and their control, to traffic and its control; from planning nets, timetables, train maintenance, and rostering to their monitoring.

Our first step in establishing the theory will be to set up a scientific repository in the area of transportation software and its domain models. The repository will be linked to other, less specialised repositories, such as the UK's verified software repository. The idea is to provide a focus for international efforts towards the project's objectives. The TRain repository will contain a series of challenges for the community to address in order to develop a theory adequate for the application domain. A previous project — FMERail — was successful in uncovering several significant case studies from industry, which stimulated various research groups to compare and contrast their different approaches. An early task will be to collect a new set of such problems from railway operating companies and suppliers around the world. A longer term task will be to study particular aspects of the railway domain. For example, theories of railway signalling that can be specialised to different countries' signalling principles and technologies; or theories of scheduling that can be specialised to traffic movements, marshalling, and even rostering.

It is expected that new and existing software engineering methods and their tools will become specialised to the emerging railway theory, as they are developed, adapted, and generate sub-theories of their own to address the challenge problems contained in the repository. The best tools will become available within the repository for all to use in their own experiments. The

repository will be directed by a steering committee made up from both industry and academia. A strong industrial representation will guarantee the relevance of the repository's contents to practical concerns of the railways. The steering committee will be responsible for the dissemination of the overall project's results. It will establish a dedicated conference series and journal. It will organize a yearly summer school for practitioners and students. It will encourage the establishment of university education and training courses in different aspects of the developing theory. Finally, it will provide an intellectual environment for industrial practitioners to learn how to apply new tools and techniques.

References of interest

[1] D. Bjørner, C.W. George, and S. Prehn. *Scheduling and rescheduling of trains*, 24 pages. Academic Press, 1999. Main author: Chris George

[2] Dines Bjørner. Formal Software Techniques in Railway Systems. In Eckehard Schnieder, editor, *9th IFAC Symposium on Control in Transportation Systems*, pages 1–12, Technical University, Braunschweig, Germany, 13–15 June 2000. VDI/VDE-Gesellschaft Messund Automatisieringstechnik, VDI-Gesellschaft für Fahrzeug– und Verkehrstechnik.

[3] Dines Bjørner. Dynamics of Railway Nets: On an Interface between Automatic Control and Software Engineering. In *CTS2003: 10th IFAC Symposium on Control in Transportation Systems*, Oxford, UK, August 4–6 2003. Elsevier Science Ltd. Symposium held at Tokyo, Japan. Editors: S. Tsugawa and M. Aoki.

[4] Dines Bjørner. New Results and Trends in Formal Techniques for the Development of Software for Transportation Systems. In *FORMS2003: Symposium on Formal Methods for Railway Operation and Control Systems*. Institut für Verkehrssicherheit und Automatisierungstechnik, Techn.Univ. of Braunschweig, Germany, 15–16 May 2003. Conf. held at Techn.Univ. of Budapest, Hungary. Editors: G. Tarnai and E. Schnieder, Germany.

[5] Dines Bjørner. The TRain Topical Day. In *Building the Information Society, IFIP 18th World Computer Congress, Typical Sessions, 22–27 August, 2004, Toulouse, France. Editor: Renéne Jacquart*, pages 607–611. Kluwer Academic Publishers, August 2004. A Foreword.

[6] Dines Bjørner. TRain: The Railway Domain — a Grand Challenge for Computing Science & Transporation Engineering. In *Building the Information Society (Ed.: Renéne Jacquart)*, volume WCC Toulouse 2004, 18th IFIP World Congress of IFIP, pages 607– 611, P.O.Box 322, 3300 AH Dordrecht, The Netherlands, August 26, 2004. Kluwer Academic Publishers. Topic 11: TRain, The Railway Domain – A Grand Challenge. (Ed.: Dines Bjørner).

[7] Dines Bjørner, Chris George, Anne E. Haxthausen, Christian Krog Madsen, Steffen Holmslykke, and Martin Pěnička. "UML"-ising Formal Techniques. In *INT 2004: Third International Workshop on Integration of Specification*

Techniques for Applications in Engineering, volume 3147 of Lecture Notes in Computer Science, pages 423–450. Springer-Verlag, 28 March 2004, ETAPS, Barcelona, Spain.

[8] Dines Bjørner, Chris W. George, and Søren Prehn. Computing Systems for Railways – A Rôle for Domain Engineering. Relations to Requirements Engineering and Software for Control Applications. In *Integrated Design and Process Technology. Editors: Bernd Kraemer and John C. Petterson*, P.O.Box 1299, Grand View, Texas 76050-1299, USA, 24–28 June 2002. Society for Design and Process Science.

[9] Dines Bjørner, Martin Pěnička, and Students. Towards a Formal Model of CyberRail. In *Building the Information Society (Ed.: Renéne Jacquart)*, volume WCC Toulouse 2004, 18th IFIP World Congress of IFIP, pages 657–664, P.O.Box 322, 3300 AH Dordrecht, 1 The Netherlands, August 26, 2004. Kluwer Academic Publishers. Topic 11: TRain, The Railway Domain — A Grand Challenge. (Ed.: Dines Bjørner).

[10] C.W. George. A Theory of Distributed Train Rescheduling. In Marie-Claude Gaudel and Jim Woodcock, editors, *FME'96: Industrial Benefit and Advances in Formal Methods*, pages 499–517. Springer-Verlag, March 1996.

[11] Alistair A. McEwan and J.C.P.Woodcock. A Refinement based Approach to Calculating a Fault Tolerant Railway Signal Device. In *Building the Information Society (Ed.: Renéne Jacquart)*, volume WCC Toulouse 2004, 18th IFIP World Congress of IFIP, pages 621–627, P.O.Box 322, 3300 AH Dordrecht, The Netherlands, August 26, 2004. Kluwer Academic Publishers. Topic 11: TRain, The Railway Domain — A Grand Challenge. Editor: Dines Bjørner.

[12] Martin Pěnička, Albena Kirilova Strupchanska, and Dines Bjørner. Train Maintenance Routing. In *FORMS'2003: Symposium on Formal Methods for Railway Operation and Control Systems*. L'Harmattan Hongrie, 15–16 May 2003. Conf. held at Techn.Univ. of Budapest, Hungary. Editors: G. Tarnai and E. Schnieder, Germany.

[13] A.C. Simpson, J.C.P. Woodcock, and J.W. Davies. The mechanical verification of Solid State Interlocking geographic data. In L. Groves and S. Reeves, editors, *Proceedings of Formal Methods Pacific*, pages 223–242, Wellington, New Zealand, 9–11 July 1997. Springer–Verlag.

[14] Albena Kirilova Strupchanska, Martin Pěnička, and Dines Bjørner. Railway Staff Rostering. In *FORMS2003: Symposium on Formal Methods for Railway Operation and Control Systems*. L'Harmattan Hongrie, 15–16 May 2003. Conf. held at Techn. Univ. of Budapest, Hungary. Editors: G. Tarnai and E. Schnieder, Germany.

Getting in touch

Dines Bjørner
Natl. Univ. of Singapore
dines@bjorner.biz

Jim Woodcock
University of York
jim@cs.york.ac.uk

Back to Contents page

FACS FACTS Issue 2005-3

Call For Submissions

Deadline 19 August 2005

We welcome contributions for the next issue of *FACS FACTS*, in particular:

- Letters to the Editor
- Conference reports
- Reports on funded projects and initiatives
- Calls for papers
- Workshop announcements
- Seminar announcements
- Formal methods websites of interest
- Abstracts of PhD theses in the formal methods area
- Formal methods anecdotes
- Formal methods activities around the world
- Formal methods success stories
- News from formal methods-related organizations
- Experiences of using formal methods tools
- Novel applications of formal methods
- Technical articles
- Tutorials
- Book announcements
- Book reviews
- Adverts for upcoming conferences
- Job adverts
- Puzzles and light-hearted items

Please send your submissions (in Microsoft Word, LaTeX or plain text) to Paul Boca [editor@facsfacts.info], the Newsletter Editor, by 19 August 2005.

If you would like to be an official *FACS FACTS* reporter or a guest columnist, please contact the Editor.

Blocking Publication: An Adventure in Destructive Refereeing

F.X. Reid

Publication is the *sine qua non* of the successful Academic. Who can deny this? Certainly, nobody in the United Kingdom, where a failure to produce the four refereed journal articles required by the RAE[2] can result in the miscreant being relegated to teaching FORTRAN (or the contemporary equivalent: MOCHA or BERYL or VisualBasicScript^{+++}) in perpetuity.

> *At this point the author initiated a violent diatribe against funding cuts in UK higher education, which we felt to be of limited relevance to the main argument of the article.* (Editor's note)

But I digress.

And as if the RAE were not enough, some of us are unfortunate enough to have research students, who must be taught the elbowing-your-way-to-the-bar-on-a-Saturday-night activity of achieving publication[3]. An examination of the overall system shows that there are two bottlenecks. The first is involved with communication between would-be authors and the journal in question. The more traffic across this link, the slower the refereeing process will be. Of course, there is nothing legal[4] we can do about this; would-be authors multiply like Triffids. An examination of subterfuges involved in speeding one's paper though the bottleneck are exhaustively described elsewhere [5].

The second bottleneck involves communication between referees and the journal and it is this part of the system we wish to target. These approaches are studied in great detail in [6]; here we merely present outlines.

An essential precondition for all this is:-

Become a Referee

This is one of the easiest things in the world. Indeed, the only way to avoid it is to refrain from opening mail stamped with the name of a journal or emanating from someone known to be on the organizing committee of a conference. Journal editors are inundated with submissions and *need* referees; it's a seller's market.

If you have any kind of reputation at all (and even if you have not) then sooner or later a brown A4 envelope will thud into your pigeonhole containing a paper to review.

---

[2] The Research Assessment Exercise: an initiative by the UK government to ensure that all research funding of whatever kind ends up in Oxbridge.

[3] Of course, I myself have no such problems. The few visitors allowed into my *sanctum sanctorum* will be familiar with the tall pile of handwritten articles sitting on my desk. As each new article is completed, it is carefully placed on the pile. Occasionally, a representative of some journal arrives, removes the article from the top of the pile and takes it away for immediate publication. It is only unfortunate that, as I produce articles faster than they can be published, the papers tend to appear in the wrong order.

[4] But see, for example, [2].

Don't respond with a muttered '*sod-this-for-a-game-of-soldiers; don't they know that some of us are up to our ears in teaching VisualBasicScript*$^{+++}$'

Do regard this as a foot-in-the-door opportunity. Respond *before* the deadline[5]. Indicate a willingness to co-operate. This won't get *you* published just yet, but it won't do you any harm, either[6].

Unless the paper is so utterly bad that no-one in their right mind could think of publishing it, suggest rewriting and resubmission. The point of this is that the author will be persuaded against writing additional papers until this one is 'out of the way' and that therefore the paper can be kept in limbo almost indefinitely. Further refinements of the so-called '*Sysiphean Ploy*' are discussed below.

> *After many rewrites, as demanded by the referees, the above paragraph was eventually shortened by several pages, as it was felt that in its original form, it disturbed the balance of the argument.* (Editor's note)

Delaying Tactic 1: Referees' Suggestions

Ostensively, suggestions by the referee(s) are aimed at improving the paper. A moment's thought will show that any suggestion aimed at improvement implicitly asserts that the paper *needs* improvement. This is the referee's opportunity to demoralize the author by implying, for example, that

- The work presented in the paper is of marginal originality and interest;
- There is too much (alternatively, not enough) mathematics in the paper;
- The author is ill-acquainted with the literature and has not cited certain key texts (see below).

Remember also that the referee is under no obligation to make his (her) suggestion comprehensible or, indeed, unambiguous. Ambiguous suggestions *can* be followed, given a certain amount of moral and linguistic dexterity, but that takes time, and it is this latter commodity that the participant is buying.

Above all, remember that a successful referee should be able to create a strong impression that he or she knows more about the subject in question, or at any rate, believes this. This can be extremely annoying (particularly if the author believes it not to be true), and annoying an author is an effective way of sabotaging any attempt at serious revision.

Delaying Tactic 2: The Deadline

An effective way to rattle would-be authors involves the destructive use of deadlines. In its simplest form, this consists of suggesting resubmission within a certain deadline; the idea is to make the author think twice about rewriting his or

[5] Not *too* early, as this will inevitably raise suspicions.

[6] Of course, there is always the possibility that the paper might be innovative, well-written, adequately referenced and cite you in the bibliography. The possibility is remote, however.

her paper and sending it back. Is there time to do it? Will I be able to satisfy the demands of the editor/referee(s)? Careful wording of the referees' reports should suggest negative answers to both these questions.

In this matter do not make the usual mistake of making the deadline too ungenerous; this may only spur the author to a greater effort. On the contrary, set it far in advance; the author, believing that he (she) has plenty of time is likely to put off embarking on the rewrite until too late, resulting in a mess that can be legitimately[7] returned for yet another revision.

Delaying Tactic 3: Related Work

Even if nobody has done anything remotely like the content of the paper you are refereeing, indeed *especially* if nobody has done anything remotely like it, it is still a sound tactic to complain that the author has not referred to a substantial number of other papers. For the best effect, try to make sure that these are as difficult to obtain as you can without giving the game away[8]. The papers you mention as having been ignored by the putative author do not have to be too relevant to the submission. Indeed, it is a good strategy to mention at least one whose relationship to it is tenuous[9]. This will (a) annoy the author, who will immediately suspect that, but will not be in a position to complain that, the referee has either not read the paper or does not understand it or is being deliberately obstructive, and (b) force the author to spend valuable time trying to make plausible connections between quite unrelated topics.

We would advise against referring to papers which actually don't exist [8], as there is always the possibility that you might get found out. This, however, does not apply to books which have been remaindered or are otherwise quite inaccessible.

Summary

This is a major subject and obviously we have only been able to scratch the surface of it. We could go on[10]. But space precludes this. Further issues, such as the use of certain key phrases which decode as unprovoked insults[11], are discussed elsewhere in the literature [3].

Goodbye and bad reviewing!

---

[7] As though *that* mattered.

[8] For example, a paper published in an obscure journal published in the Basque region and written in the local language would not convince any editor with the common sense to realize that you are highly unlikely to speak it. On the other hand conference proceedings are good for this strategy, as most University libraries in *this* country cannot afford to buy them.

[9] For example, if the paper is about network topology, the referee could suggest including a reference to filter bases as generators of point-set topologies.

[10] In fact, he did, but we finally persuaded him to cut out a further three pages; the diagrams were particularly unhelpful. (Editor's note.)

[11] For example, it is always a good strategy to criticize the writer for having apparently failed to use a spellchequer.

Acknowledgements

The author would like to thank the anonymous referees for their helpful suggestion and (more importantly) providing him (indirectly) with further illustrative examples of contemporary practices in the area under examination.

References

[1] Blair, A. et al.: Tuition Fees and Increased Access to Higher Education, an Exercise in Creative Inconsistency, *The Beano*, 2001.

[2] Hilter, A.: *Mein Kampfzeit*, Conservative Central Office Pamphlet Series, 1930.

[3] Lurk, F. X.: A Lexicon of Disparaging Verbal Formulae for Demotivating Potential Authors, CACM pamphlets, CA42, 2000.

[4] Reid, F. X.: How To Get Published Even When You Have Nothing To Say, Uxbridge University Press, 1999.

[5] Reid, F. X.: The Theory and Practice of Publication, Ergodic House, 2003.

[6] Reid, F. X.: Game Theory, Combinatorics and the Blocking of Publication, Tyche Press, 2004.

[7] Stribling, J., Aguayo and Krohn, M.: Rooter: A Methodology for the Typical Unification of Access Points and Redundance, MIT, 2005.

[8] Thatcher, M. M.: Milk Snatching for Profit and Pleasure, *Comptes Rendues* of the Buckingham University Philosophy Institute, 1984. ▒

Getting in touch

F. X. Reid
University of Rutland

f.reid@imagenius.com

Coming Soon in FACS FACTS....

TRain Column

Conference reports

Technical Articles

Report on FM05 Industry Day

FACS Evening Seminars

Report on FM05 Grand Challenges Workshop

And More...

Back to Contents page

CSR

ForTIA

SAP

Formal Methods Going Mainstream

Costs, Benefits and Experiences

The ForTIA Industry Day

20th July 2005

University of Newcastle upon Tyne, UK

http://www.fortia.org/iday05/

Plenary Talk by

Mathai Joseph,
Tata Research
Development and Design,
Pune, India

Speakers include:

- Guy H Broadfoot, Verum Consultants
- John Harrison, Intel Corporation
- Alexander Pretschner, ETH Zürich
- Wolfram Schulte, Microsoft Research
- Gerrit Muller, Embedded Systems Institute
- Followed by a panel discussion with all presenters

Formal Methods have had a long-standing influence on system design, both inside and outside the critical systems sector. Increases in processor power have made some formal tasks, such as model-checking, much more tractable than they were even a few years ago. In this special "Industry Day", part of the Formal Methods 2005 Symposium at Newcastle, speakers will give first-hand reports of their experience on using formal techniques in software or systems engineering projects, emphasising the cost/benefit aspects of their application. Speakers will include

- *Mathai Joseph (TRDDC, India)*
  Formal Aids for the Growth of Software Systems
- *John Harrison (Intel, USA)*
  Floating point Verification
- *Christian Scheidler (DaimlerChrysler, GER)*
  Model Checking for Advanced Automotive Applications
- *Wolfram Schulte (Microsoft Research, USA)*
  Testing Concurrent Object-Oriented Systems With Spec Explorer
- *Alexander Pretschner (ETH Zurich, CH)*
  Model based Testing in Practice
- *Guy Broadfoot (Verum, NL)*
  Applying Formal Methods to Industrial Control Software
- *Gerrit Muller (Embedded Systems Institute, NL)*
  The Informal Nature of Systems Engineering

The day will include opportunities for open discussion inspired by the talks.

Industry day is organised by the Formal Techniques Industry Association (ForTIA, www.fortia.org), a subgroup of Formal Methods Europe (www.fmeurope.org), dedicated to the transfer of formal techniques between industry and academia and currently supported by 20 companies.

Who Should Attend?

Managers, project leaders, system engineers and architects who are interested in:

- learning what kind of formal methods are applied in industry on real-world problems
- learning what costs come with it and what benefits can be achived
- discussing their experiences and needs with industrial users of formal techniques as well as researchers from industry and academia

✂ .....

Return registration details to:

Claire Smith
CSR, 11th floor
Claremont Tower
Newcastle University
Newcastle upon Tyne
NE1 7RU

Phone: +44 191 222 7999
Fax: +44 191 222 8788
Email:claire.smith@ncl.ac.uk

The ForTIA Industry Day (Wednesday 20th July 2005)

£95 Fee *includes: attendance, materials, lunch and breaks*

METHOD OF PAYMENT (please circle one) Mastercard Visa American Express

❑ Credit Card Number:..... Expiry date: .....

Cardholder Name: ..... Signature: .....

❑ Please invoice my company (Please supply billing information and company details)

.....

.....

❑ I enclose a cheque in £ sterling *(Cheques should be made payable to: University of Newcastle)*

An Example Railway Domain

Dines Bjørner

In this article I provide an example of a domain model. It is expressed in RSL: the RAISE Specification Language [13, 14] and is based on material presented in Chap. 2, Vol. 2 of my three volume Springer-Verlag book *Software Engineering: Vol.2: Specification of Systems and Languages* [4].

1 Introduction

Before software can be designed its requirements must be understood. Before requirements can be collected the domain in which the future software resides must be understood. In automotive engineering the engineer relies on, amongst others, Newton's laws and the laws of thermodynamics. They, and derivative laws, form an adequate sub-theory of the domain of physics — the domain within which the automotive engineer primarily works.

In communications engineering the engineer relies on, amongst others, Maxwell's Equations (the laws of Faraday, etc.).

And so forth.

Management of automotive or communications engineering design companies would not, in their right minds, hire an "engineer" who was not well-educated in the relevant fields of physics.

Just because a child, by means of Lego blocks, has been able to build a "bridge" does not entitle that child to a job in construction engineering.

But, isn't this what happens in software engineering? So-called programmers are put to develop software for applications in domains of which they have no prior knowledge and for which they are certainly not going to first develop a domain theory?

2 What is a Railway Domain?

So we suggest that in order to undertake requirements development for any form of, for example, railway application one must rely on a domain theory, a domain model, of, in this case, railways. If one is not at hand, then one has to develop it first! Not doing so would, in our opinion, amount to criminal neglect.

So what is a railway?

It is, of course, a big question — with an answer we are not likely to achieve, in a scientifically and technologically fully satisfactory way for some, say 20 years to come!

But we have to start.

So we start with what there is: The rail net. On a theory of rail nets we can then, it is conjectured, build theories of train traffic, passenger and freight transport, and so on.

In the following we shall outline one such way of presenting (i.e., developing) such a theory: by combinations of narration and formalization.

Consider Figure 1. It purports to be a diagram of a rail net. Closer inspection reveals what is then embodied in the first narrative that follows.

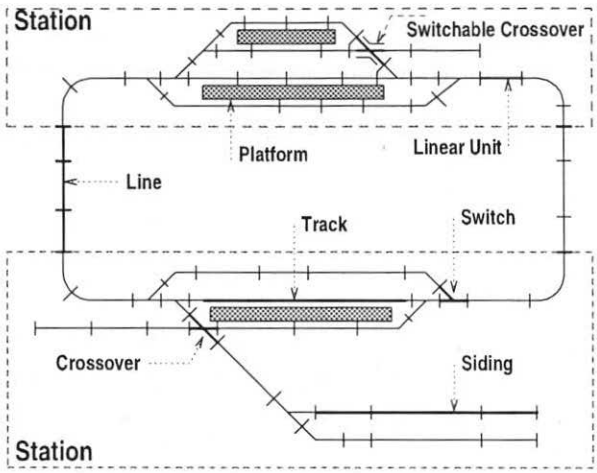


Figure 1: A "model" rail net

2.1 First Narrative

We introduce the phenomena of railway nets, lines, stations, tracks, (rail) units, and connectors.

1. A railway net consists of one or more lines and two or more stations.

2. A railway net consists of rail units.

3. A line is a linear sequence of one or more linear rail units.

4. The rail units of a line must be rail units of the railway net of the line.

5. A station is a set of one or more rail units.

6. The rail units of a station must be rail units of the railway net of the station.

7. No two distinct lines and/or stations of a railway net share rail units.

8. A station consists of one or more tracks.

9. A track is a linear sequence of one or more linear rail units.

10. No two distinct tracks share rail units.

11. The rail units of a track must be rail units of the station (of that track).

12. A rail unit is either a linear, or is a switch, or is a simple crossover, or is a switchable crossover, etc., rail unit.

13. A rail unit has one or more connectors.

14. A linear rail unit has two distinct connectors. A switch (a point) rail unit has three distinct connectors. Crossover rail units have four distinct connectors (whether simple or switchable), etc.

15. For every connector there are at most two rail units which have that connector in common.

16. Every line of a railway net is connected to exactly two distinct stations of that railway net.

17. A linear sequence of (linear) rail units is an acyclic sequence of linear units such that neighbouring units share connectors.

In the narrative above reference was made to rail units. They were first abstracted in Figure 1 on the preceding page. Four kinds of rail units were mentioned and depicted. They are re-depicted in Figures 2 and 3 and in increasing levels of details.

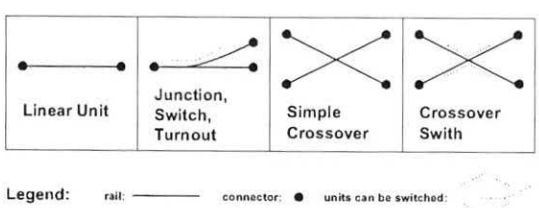


Figure 2: Example rail units

At this stage we do not need the level of detail shown in Figure 3.

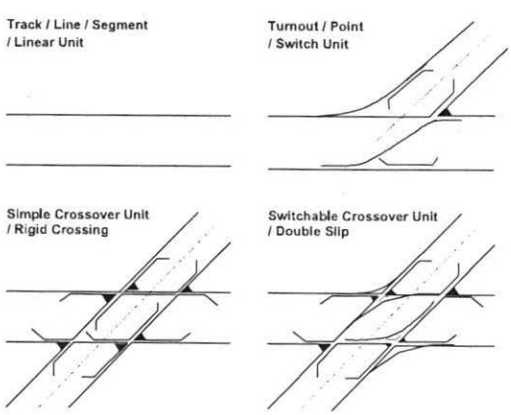


Figure 3: Example rail units

2.2 First Formalization

```
type
  N, L, S, Tr, U, C
value
  1.  obs_Ls: N → L-set
  1.  obs_Ss: N → S-set
  2.  obs_Us: N → U-set
  3.  obs_Us: L → U-set
  5.  obs_Us: S → U-set
  8.  obs_Trs: S → Tr-set
  12. is_Linear: U → Bool
  12. is_Switch: U → Bool
  12. is_Simple_Crossover: U → Bool
  12. is_Switchable_Crossover: U → Bool
  13. obs_Cs: U → C-set
  17. lin_seq: U-set → Bool
      lin_seq(us) ≡
        ∀ u:U • u ∈ us ⇒ is_Linear(u) ∧
        ∃ q:U* • len q = card us ∧ elems q = us ∧
          ∀ i:Nat • {i,i+1} ⊆ inds q ⇒ ∃ c:C •
            obs_Cs(q(i)) ∩ obs_Cs(q(i+1)) = {c} ∧
          len q > 1 ⇒ obs_Cs(q(i)) ∩ obs_Cs(q(len q)) = {}
```

Some formal axioms are now given, but not all of them!

```
axiom
1. ∀ n:N • card obs_Ls(n) ≥ 1 ∧ card obs_Ss(n) ≥ 2

3. ∀ n:N, l:L • l ∈ obs_Ls(n) ⇒ lin_seq(l)

4. ∀ n:N, l:L • l ∈ obs_Ls(n) ⇒ obs_Us(l) ⊆ obs_Us(n)

5. ∀ n:N, s:S • s ∈ obs_Ss(n) ⇒ card obs_Us(s) ≥ 1

6. ∀ n:N, s:S • s ∈ obs_Ls(n) ⇒ obs_Us(s) ⊆ obs_Us(n)

7. ∀ n:N,l,l':L•{l,l'}⊆obs_Ls(n)∧l≠l'⇒obs_Us(l)∩ obs_Us(l')={}

7. ∀ n:N,l:L,s:S•l ∈ obs_Ls(n)∧s ∈ obs_Ss(n)⇒obs_Us(l)∩ obs_Us(s)={}

7. ∀ n:N,s,s':S•{s,s'}⊆obs_Ss(n)∧s≠s'⇒obs_Us(s)∩ obs_Us(s')={}

8. ∀ s:S • card obs_Trs(s) ≥ 1

9. ∀ n:N, s:S, t:T • s ∈ obs_Ss(n) ∧ t ∈ obs_Trs(s) ⇒ lin_seq(t)
```

10. ∀ n:N, s:S, t,t′;T •
    s ∈ obs_Ss(n) ∧ {t,t′} ⊆ obs_Trs(s) ∧ t≠t′
    ⇒ obs_Us(t) ∩ obs_Us(t′) = {}

15. ∀ n:N • ∀ c:C •
    c ∈ ∪ { obs_Cs(u) | u:U • u ∈ obs_Us(n) }
    ⇒ **card**{ u | u:U • u ∈ obs_Us(n) ∧ c ∈ obs_Cs(u) } ≤ 2

16. ∀ n:N,l:L • l ∈ obs_Ls(n) ⇒
    ∃ s,s′:S • {s,s′} ⊆ obs_Ss(n) ∧ s≠s′ ⇒
    let sus = obs_Us(s), sus′ = obs_Us(s′), lus = obs_Us(l) **in**
    ∃ u:U • u ∈ sus, u′:U • u′ ∈ sus′, u″,u‴:U • {u″,u‴} ⊆ lus •
    let scs = obs_Cs(u), scs′ = obs_Cs(u′),
    lcs = obs_Cs(u″), lcs′ = obs_Cs(u‴) **in**
    ∃ ! c,c′:C • c ≠ c′ ∧ scs ∩ lcs = {c} ∧ scs′ ∩ lcs′ = {c′}
    end end

2.3 Second Narrative

The first narrative and formalization emphasized the static nature of a rail net, its topology so-to-speak. The dynamics of a rail net has to do with the states of units: Whether open for traffic in one, or another, or more directions through a unit, i.e., between some of its connectors, or whether closed.

Consider Figure 4 on the following page.

We introduce defined concepts such as paths through rail units, state of rail units, rail unit state spaces, routes through a railway network, open and closed routes, trains on the railway net, and train movement on the railway net.

18. A path, $p : P$ is a pair of distinct connectors, (c, c') ,

19. and of some unit.

20. A state, $\sigma : \Sigma$, of a unit is the set of all open paths of that unit (at the time observed).

21. A unit may, over its operational life, attain any of a (possibly small) number of different states $\omega : \Omega$.

22. A route is a sequence of pairs of units and paths such that the path of a unit/path pair is a possible path of some state of the unit, and such that "neighbouring" connectors are identical.

23. An open route is a route such that all its paths are open.

24. A train is modelled as a route.

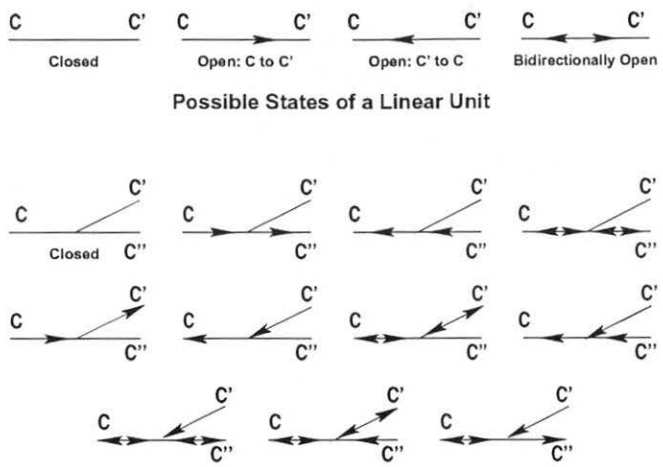


Figure 4: States of linear and of switch units

25. Train movement is modelled as a discrete function (i.e., a map) from time to routes such that for any two adjacent times the two corresponding routes differ by at most one of the following:

(a) a unit path pair has been deleted (removed) from one end of the route;
(b) a unit path pair has been deleted (removed) from the other end of the route;
(c) a unit path pair has been added (joined) from one end of the route;
(d) a unit path pair has been added (joined) from the other end of the route;
(e) a unit path pair has been added (joined) from one end of the route, and another unit path pair has been deleted (removed) from the other end of the route;
(f) a unit path pair has been added (joined) from the other of the route, and another unit path pair has been deleted (removed) from the one end of the route;
(g) or there has been no change with respect to the route (yet the train may have moved);
(h) 26. and such that the new route is a well-formed route.

We shall arbitrarily think of one end as the "left end", and the other end as the "right end", where "left", in a model where elements of a list are indexed from 1 to its length, means the index 1 position, and "right" means the last index position of the list.

Figure 5 attempts to picture the (abstracted, approximated) discretized movement of trains mentioned in items 25a–25g.

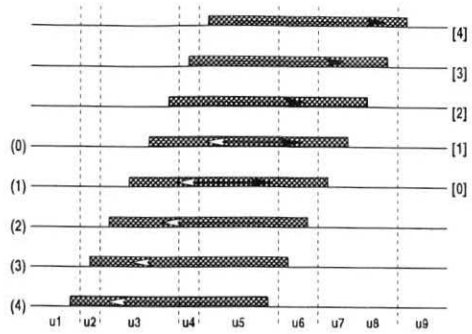


Figure 5: A Discretized Train Movement

2.4 Second Formalization

type
18. P = {| (c,c′):(C×C) • c≠c′ |}
20. Σ = P-**set**
21. Ω = Σ-**set**
22. R ={| r:(U×P)* • wf_R(r) |}
24. Trn = R
25. Mov = {| m:(T $\overrightarrow{m}$ Trn) • wf_Mov(m) |}

value
20. obs_Σ: U → Σ
21. obs_Ω: U → Ω

axiom
∀ u:U • **let** ω = obs_Ω(u), σ = obs_Σ(u) **in** σ ∈ ω ∧
19. **let** cs = obs_Cs(u) **in** ∀ (c,c′):P • (c,c′) ∈ ∪ ω ⇒ {c,c′} ⊆ obs_Cs(u)
end end

22. wf_R: (U×P)* → **Bool**
wf_R(r) ≡
len r > 0 ∧ ∀ i:**Nat** • i ∈ **inds** r **let** (u,(c,c′)) = r(i) **in**
(c,c′) ∈ ⋃ obs_Ω(u) ∧ i+1 ∈ **inds** r ⇒
let (_,(c″,_)) = r(i+1) **in** c′ = c″ **end end**

23. open_R: R → **Bool**
open_R(r) ≡ ∀ (u,p):U×P • (u,p) ∈ **elems** r ∧ p ∈ obs_Σ(u)

25. wf_Mov: Mov → **Bool**
wf_Mov(m) ≡ **card dom** m ≥ 2 ∧
∀ t,t′:T • t,t′ ∈ **dom** m ∧ t < t ∧ adjacent(t,t′) ⇒
let (r,r′) = (m(t),m(t′)), (u,p):U×P • p ∈ ⋃ obs_Ω(u) **in**
25a. (l_d(r,r′,(u,p)) ∨ 25b. r_d(r,r′,(u,p)) ∨
25c. l_a(r,r′,(u,p)) ∨ 25d. r_a(r,r′,(u,p)) ∨
25e. l_d_r_a(r,r′,(u,p)) ∨ 25f. r_d_l_a(r,r′,(u,p)) ∨
25g. r=r′) ∧ wf_R(r′)
end

The last line's route well-formedness ensures that the type of **Mov** is maintained.

```
value
  adjacent: T × T → Bool
  adjacent(t,t') ≡ ~∃ t'':T • t'' ∈ dom m ∧ t < t'' < t'

  l_d,r_d,l_a,r_a,l_d_r_a,r_d_l_a: R × R × P → Bool

  l_d(r,r',(u,p)) ≡ r' = tl r     pre len r>1
  r_d(r,r',(u,p)) ≡ r' = fst(r)   pre len r>1
  l_a(r,r',(u,p)) ≡ r' = ⟨(u,p)⟩^r
  r_a(r,r',(u,p)) ≡ r' = r^⟨(u,p)⟩
  l_d_r_a(r,r',(u,p)) ≡ r' = tl r^⟨(u,p)⟩
  r_d_l_a(r,r',(u,p)) ≡ r' = ⟨(u,p)⟩^fst(r)

  fst: R ~→ R'
  fst(r) ≡ ⟨ r(i) | i in ⟨1..len r−1⟩ ⟩
```

If the argument to **fst** is of length 1 then the result is not a well-formed route, but is in $(U \times P)^*$.

3 Conclusion

A model has been shown. It was expressed in RSL [13, 15, 16] but could as well have been expressed in B [1, 2, 7], Casl [3, 30, 31], CafeOBJ [10, 11], VDM-SL [5, 6, 12] or Z [23, 38–40]. Extending the kind of modelling effort shown in this note typically entails the use of other formalisms: Petri Nets [28, 32-35], Message Sequence Charts [8, 26, 27], Live Sequence Charts [9, 21, 29], Statecharts [17–20, 22], Duration Calculus [41, 42] — to take just some examples. These have all been extensively illustrated in Chapters 12–15 of Vol. 2 of [4].

These and other examples, notably missing from the above list, and I apologise, is a reference to CSP [24, 25, 36, 37], point to the need for integrating formal techniques if one is to achieve a proper domain theory for any domain.

References

[1] J.-R. Abrial: *The B Book: Assigning Programs to Meanings* (Cambridge University Press, Cambridge, England 1996)

[2] J.-R. Abrial, L. Mussat. *Event B Reference Manual (Editor: Thierry Lecomte)*, June 2001. Report of EU IST Project Matisse IST-1999-11435.

[3] M. Bidoit, P.D. Mosses: Casl *User Manual* (Springer, 2004)

[4] D. Bjørner: *Software Engineering*, vol Vol. 1: Abstraction and Modelling, Vol. 2: Specification of Systems and Languages, Vol. 3: Domains, Requirements and Software Design of *Texts in Theoretical Computer Science, the EATCS Series* (Springer-Verlag, 2005)

[5] Edited by D. Bjørner, C. Jones: *The Vienna Development Method: The Meta-Language*, vol 61 of LNCS (Springer-Verlag, 1978)

[6] Edited by D. Bjørner, C. Jones: *Formal Specification and Software Development* (Prentice-Hall, 1982)

[7] D. Cansell, D. Méry: Logical Foundations of the B Method. Computing and Informatics 22, 1-2 (2003)

[8] CCITT. CCITT Recommendation Z.120: Message Sequence Chart (MSC), 1992.

[9] W. Damm, D. Harel: LSCs: *Breathing Life into Message Sequence Charts.* Formal Methods in System Design 19 (2001) pp 45–80

[10] R. Diaconescu, K. Futatsugi: *CafeOBJ Report: The Language, Proof Techniques, and Methodologies for Object-Oriented Algebraic Specification* (World Scientific Publishing Co., Pte. Ltd., 5 Toh Tuck Link, Singapore 596224 July 1998)

[11] R. Diaconescu, K. Futatsugi, K. Ogata: *CafeOBJ: Logical Foundations and Methodology*. Computing and Informatics 22, 1–2 (2003)

[12] J. Fitzgerald, P.G. Larsen: *Developing Software using VDM-SL* (Cambridge University Press, The Edinburgh Building, Cambridge CB2 1RU, England 1997)

[13] C. W. George, P. Haff, K. Havelund et al: *The RAISE Specification Language* (Prentice-Hall, Hemel Hempstead, England 1992)

[14] C. W. George, A. Haxthausen, S. Hughes et al: *The RAISE Method* (Prentice-Hall, Hemel Hampstead, England 1995)

[15] C. W. George, A. E. Haxthausen: *The Logic of the RAISE Specification Language*. Computing and Informatics, 22, 1–2 (2003)

[16] C. W. George, H. D. Van, T. Janowski, R. Moore: *Case Studies using The RAISE Method* (Springer-Verlag, London 2002)

[17] D. Harel: Statecharts: *A visual formalism for complex systems*. Science of Computer Programming 8, 3 (1987) pp 231–274

[18] D. Harel: *On Visual Formalisms*. Communications of the ACM 33, 5 (1988)

[19] D. Harel, E. Gery: *Executable Object Modeling with Statecharts*. IEEE Computer 30, 7 (1997) pp 31-42

[20] D. Harel, H. Lachover, A. Naamad et al: *STATEMATE: A Working Environment for the Development of Complex Reactive Systems.* Software Engineering 16, 4 (1990) pp 403–414

[21] D. Harel, R. Marelly: *Come, Let's Play – Scenario-Based Programming Using LSCs and the Play-Engine* (Springer-Verlag, 2003)

[22] D. Harel, A. Naamad: *The STATEMATE semantics of Statecharts.* ACM Transactions on Software Engineering and Methodology (TOSEM) 5, 4 (1996) pp 293–333

[23] M. C. Henson, S. Reeves, J. P. Bowen: *Z Logic and its Consequences.* Computing and Informatics 22, 1–2 (2003)

[24] C.A.R. Hoare: Communicating Sequential Processes (Prentice-Hall International, 1985)

[25] C.A.R. Hoare. Communicating Sequential Processes. Published electronically: http://www.usingcsp.com/cspbook.pdf, 2004. Second edition of [24]. See also http://www.usingcsp.com/ .

[26] ITU-T. ITU-T Recommendation Z.120: Message Sequence Chart (MSC), 1996.

[27] ITU-T. ITU-T Recommendation Z.120: Message Sequence Chart (MSC), 1999.

[28] K. Jensen: *Coloured Petri Nets*, vol 1: Basic Concepts (234 pages + xii), Vol. 2: Analysis Methods (174 pages + x), Vol. 3: Practical Use (265 pages + xi) of EATCS Monographs in Theoretical Computer Science (Springer-Verlag, Heidelberg 1985, revised and corrected second version: 1997)

[29] J. Klose, H. Wittke: An Automata Based Interpretation of Live Sequence Charts. In: *TACAS 2001*, ed by T. Margaria, W. Yi (Springer-Verlag, 2001) pp 512–527

[30] T. Mossakowski, A. E. Haxthausen, D. Sanella, A. Tarlecki: CASL – *The Common Algebraic Specification Language: Semantics and Proof Theory.* Computing and Informatics 22, 1–2 (2003)

[31] Edited by P. D. Mosses: CASL *Reference Manual*, vol 2960 of LNCS, IFIP Series (Speinger-Verlag,Heidelberg, Germnay 2004)

[32] C.A. Petri: *Kommunikation mit Automaten* (Bonn: Institut für Instrumentelle Mathematik, Schriften des IIM Nr. 2, 1962)

[33] W. Reisig: Petri Nets: *An Introduction, vol 4 of Monographs on Theoretical Computer Science* (Springer-Verlag, 1985)

[34] W. Reisig: *A Primer in Petri Net Design* (Springer-Verlag, 1992)

[35] W. Reisig: *Elements of Distributed Algorithms: Modelling and Analysis with Petri Nets* (Springer Verlag, 1998)

[36] A. Roscoe: *Theory and Practice of Concurrency* (Prentice-Hall, 1997)

[37] S. Schneider: *Concurrent and Real-time Systems – The CSP Approach* (John Wiley & Sons, Ltd., Baffins Lane, Chichester, West Sussex PO19 1UD, England 2000)

[38] J. M. Spivey: Understanding Z: *A Specification Language and its Formal Semantics*, vol 3 of Cambridge Tracts in Theoretical Computer Science (Cambridge University Press, 1988)

[39] J. M. Spivey: *The Z Notation: A Reference Manual*, 2nd ed (Prentice Hall International Series in Computer Science, 1992)

[40] J. C. P. Woodcock, J. Davies: *Using Z: Specification, Proof and Refinement* (Prentice Hall International Series in Computer Science, 1996)

[41] C. C. Zhou, M. R. Hansen: *Duration Calculus: A formal approach to real-time systems* (Springer-Verlag, 2003)

[42] C. C. Zhou, C. A. R. Hoare, A. P. Ravn: *A Calculus of Durations*. Information Processing Letters 40, 5 (1991) pp 269–276

Getting in touch

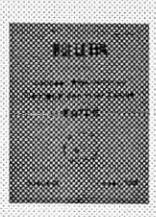
Dines Bjørner
Natl. University of Singapore
dines@bjorner.biz

Newsletters from other organisations

CoLogNET

http://www2.cs.ucy.ac.cy/projects/colognet

http://www.easst.org/newsletter



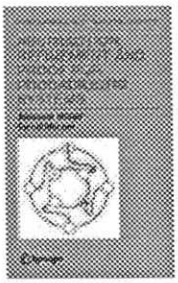
http://www.liacs.nl/~beatcs

http://www.lms.ac.uk/newsletter/newsletter.html

Back to Contents page

Book Announcements

Abstraction, Refinement and Proof for Probabilistic Systems
Series: Monographs in Computer Science.
McIver, Annabelle, **Morgan**, Carroll.
2005, XIX, 383 p. 63 illus., Hardcover
ISBN: 0-387-40115-6



The book is a focused survey on probabilistic program semantics, conceived to tell a coherent story with a uniform notation. It is grouped into three themes: Part I is for 'users' of the techniques who will be developing actual programs; Part II gives mathematical foundations intended for those studying exactly how it was done and how to build semantic structures/models in their own work; and Part III describes a very 'hot' research direction, temporal logic and model checking.

Topics and features:

- introduces readers to very up-to-date research in the mathematics of rigorous development of randomized (probabilistic) algorithms
- illustrates by example the typical steps necessary in computer science to build a mathematical model of any programming paradigm
- presents results of a large and integrated body of research in the area of 'quantitative' program logics

An advanced research survey monograph, integrating three major topic areas: random/probabilistic algorithms, assertion-based program reasoning, and refinement programming models. Essential foundation topic for modern sequential programming methodology.

Written for:

Computer scientists, researchers, professionals

Keywords:

- Data refinement
- Program semantics
- Random algorithms
- Sequential programming
- Temporal logic

Back to Contents page

PhD Abstracts

Name	Zhu Huibiao
Thesis Title	Linking the Semantics of a Multithreaded Event Simulation Language
Supervisor	Professor Jonathan Bowen
Institute	London South Bank University, UK
Examiners	Professor Mark Josephs & Professor Hussein Zedan
Awarded	5 April 2005

Abstract

Verilog is a hardware description language (HDL) that has been standardized and widely used in industry. *MDESL* is a Verilog-like language, which is a multithreaded discrete event simulation language. The language contains interesting features such as event-driven computation and shared-variable concurrency. For ensuring correctness of hardware design, precise understanding of the language based on semantics is very important. There are several semantics for the language and the consistency of these semantics is challenging. This dissertation focuses on the semantics of *MDESL* and their linking theory.

The denotational semantics of *MDESL* has been formalized under a discrete time model. In order to deal with the shared-variable feature, the behaviour of a process is described in terms of a trace of snapshots. The operational semantics has been formalized as a set of transition rules, which is expressed in the notation of SOS (*Structural Operational Semantics*). A prototype of the operational semantics has been developed using Prolog. The operational semantics is fully compositional, which can be linked with the denotational semantics. Algebraic properties have been studied, which can be used in support of program simplification and optimization. The program properties can be proved by two approaches: denotational semantics and operational semantics (via bisimulation).

Two approaches have been proposed in order to formally link operational semantics with denotational semantics. The first approach is to derive denotational semantics from operational semantics. The second is the inverse approach, which is to derive operational semantics from denotational semantics. In order to represent the denotational view of a transition, the concept of transition condition and phase semantics has been defined for each type of transition and applied in both approaches.

Regarding the operational semantics, two significant questions have been investigated: *soundness* and *completeness*. The understanding of these two aspects is based on the denotational semantics. The operational semantics has

been proved to be sound and complete. The aspect of non-redundancy for operational semantics has also been discussed.

How the algebraic semantics relates with the operational semantics and denotational semantics has also been explored. The approach starts from the algebraic semantics, where every program is expressed as a healthy normal form of guarded choice. A transition system (i.e., operational semantics) for *MDESL* has been derived and the equivalence between the derived transition system and the derivation strategy has been proved. The healthy normal form has also been derived back from the transition system. The denotational semantics for finite programs has also been derived from the healthy normal form.

The results achieved here are not limited to *MDESL*. The approaches taken may also be applicable to some other languages with different programming features. ▒

SEEFM'05

2nd South-East European Workshop on Formal Methods

Practical dimensions: Challenges in the business world

18-19 November 2005

Ohrid, Former Yugoslav Republic of Macedonia

http://www.seefm.info/seefm05/

The successful organisation of the 1st South-East European Workshop in Formal Methods that took place in Thessaloniki on the 20th of November 2003, fulfilled its goal by bringing people from South-Eastern Europe together, based on their common interests in Formal Methods. The aim of the 2nd workshop is to bring together more researchers from South-Eastern European countries and not only those interested in Formal Methods. More specifically, the workshop intends to establish a network of scientists in the wider Balkan area who are active in the field of Formal Methods. The theme of this workshop deals with the practical dimensions of formal methods, that is how formal methods can deal with the challenges in the business world, in order to facilitate practical development of dynamically evolving, correct and safe software systems.

Invited Speakers: Professor Jonathan Bowen, London South Bank University

Professor John Derrick, University of Sheffield

The workshop is sponsored by BCS-FACS

Back to Contents page

Name	Paola Spoletini
Thesis Title	Verification of Temporal Logic Specifications via Model Checking
Supervisor	Professor Pierluigi San Pietro
Institute	Dipartimento di Elettronica e Informazione Politecnico di Milano, Italy
Examiner	Professor Stefania Gnesi
Awarded	20 May 2005
URL	http://www.elet.polimi.it/upload/spoleti/PhDThesis_PaolaSpoletini.pdf

Abstract

Critical systems, especially in case of real-time characteristics, require specification, design, and verification methods with high thoroughness, supported by proper tools. Recent progress in the automatic verification techniques find use in this area, but still require further research and design of applications in order to be exploited in common engineering tasks, in particular when time comes into play with its different granularities.

The aim of this thesis is to extend the existing verification techniques, typically built on traditional finite state automata, to treat complex critical systems with time constraints. Such techniques must be based on appropriate formalisms, whose power must be accurately balanced between real systems description capability and possibility of efficient automatization of the verification process.

The TRIO specification language [1], which is a typed first order logic that supports a linear notion of time with both past and future operators (TRIO-in the-small), and can be extended with the typical object oriented programming constructs [2], is an excellent specification language for such systems. But, in general, TRIO is undecidable; therefore, in order to obtain an entirely automatic verification method, it is necessary to limit TRIO to a decidable subset, disallowing variables, considering the natural numbers as time domain and limiting all the other domains to finite domains.

During this research work, we focused on a decidable subset of TRIO, and introduced a new model checking technique based on automata, which allows us to take advantage of TRIO modular aspects.

The proposed approach allows the automatic verification of TRIO specification through the Spin model checker. Note that the problem we are dealing with slightly differs from the classical model-checking problem, seeing that, instead of considering an operational model, we use a purely descriptive specification; hence a technique for the verification of models defined both in the past and in the future has been developed.

Shortly, the proposed approach is based on an initial separation of the past and future components, always possible by the Gabbay separation theorem. The two components are then differently translated, considering that the past component refers to finite words, since we are considering the natural numbers as temporal domain, and the future component refers to infinite words. Therefore, we propose a translation of the past component to deterministic

Büchi automata [4], and of the future component to alternating automata [3], which allow non determinism and parallelism. Both the considered automata are enriched with a set of finite counters, in order to keep track of the quantitative aspect of time, which is part of TRIO. The two components are then merged through the composition of the two automata [4], and the resulting automaton is then translated to Promela, which is Spin input language. Let us notice that the automaton obtained with the composition of the past and future components is still an alternating automaton, while Spin uses Büchi automata. Anyway, an alternating automaton can always be transformed into a Büchi automaton with an exponential explosion in the number of the states; in order to avoid such explosion in the translation to Promela, the automaton obtained with the composition is directly simulated in Promela.

The proposed techniques have been implemented in the TRIO2Promela translator, a plug-in for Trident, a platform for the specification and verification of TRIO models, based on Eclipse. With the usage of the translator it has been possible to experimentally validate the proposed technique.

References

[1] C. Ghezzi, D. Mandrioli, and A. Morzenti. Trio: A logic language for executable specifications of real-time systems. *The Journal of Systems and Software*, 12(2):107–123, May 1990.

[2] A. Morzenti and P. San Pietro. Object-oriented logic specifications of time critical systems. *ACM Transactions on Software Engineering and Methodologies*, 3(1):56–98, January 1994.

[3] A. Morzenti, M. Pradella, P. San Pietro, and P. Spoletini. Model checking of trio specifications in Spin. *Proc. 12th International FME Symposium*, LNCS, volume 2805, Sep 2003.

[4] M. Pradella, P. San Pietro, P. Spoletini, and A. Morzenti. Practical model checking of LTL with past. *Proc. 1st International Workshop on Automated Technology for Verification and Analysis*, December 2003.

Back to Contents page

Conference Announcements

The following are sponsored by BCS-FACS and/or considered of special interest to BCS-FACS members:

July 2005

CAV 2005 – 17th International Conference on Computer Aided Verification
6–10 July
Edinburgh, UK
http://www.cav2005.inf.ed.ac.uk

FATES 2005 – 5th International Workshop on Formal Approaches to Testing of Software
11 July
Edinburgh, UK
http://research.microsoft.com/conferences/fates2005

FM05 – Formal Methods 2005
18–22 July
Newcastle, UK
http://www.csr.ncl.ac.uk/fm05

August 2005

TPHOLS 2005 – 18th International Conference on Theorem Proving in Higher Order Logics
22–25 August
Oxford, UK
http://web.comlab.ox.ac.uk/oucl/conferences/TPHOLs2005

September 2005

CALCO 2005 – 1st Conference on Algebra and Co-Algebra in Computer Science
3–6 September
Swansea, UK
http://www.cs.swan.ac.uk/calco

FMICS 05 – 10th International Workshop on Formal Methods for Industrial Critical Systems
5–6 September
Lisbon, Portugal
http://fmt.isti.cnr.it/FMICS05

SEFM 2005 – 3rd IEEE International Conference on Software Engineering and Formal Methods
5–9 September
Koblenz, Germany
http://sefm2005.uni-koblenz.de

ESEC/FSE 2005 – European Software Engineering Conference & ACM SIGSOFT Symposium on the Foundations of Software Engineering
7–9 September
Lisbon, Portugal
http://esecfse05.unl.pt

October 2005

FORTE 2005 – 25th IFIP WG 6.1 International Conference on Formal Techniques for Networked and Distributed Systems
2–5 October
Taipei, Taiwan
http://cc.ee.ntu.edu.tw/~forte05

ICTAC 2005 – International Colloquium on Theoretical Aspects of Computing
17–21 October
Hanoi, Vietnam
http://www.iist.unu.edu/ictac05

November 2005

ICFEM 2005 – 7th International Conference on Formal Engineering Methods
1–4 November 2005
Manchester, UK
http://www.cs.man.ac.uk/icfem05

SEEFM 2005 – 2nd South-East European Workshop on Formal Methods 2005
18–19 November
Ohrid, Former Yugoslav Republic of Macedonia
http://www.seefm.info/seefm05

IFM 2005 – 5th International Conference on Integrated Formal Methods
29 November – 2 December
Eindhoven, The Netherlands
http://www.win.tue.nl/ifm

December 2005

BCS-FACS Christmas Meeting
19 December
BCS London Office
http://www.bcs-facs.org/events/xmas2005

March 2006

MBT 2006 – 2nd Workshop on Model Based Testing
25–26 March
Vienna, Austria
http://react.cs.uni-sb.de/mbt2006

April 2006

BCTCS 2006 – 22nd British Colloquium for Theoretical Computer Science
4–7 April
Swansea, UK
http://www.cs.swan.ac.uk/BCTCS2006

For further conference announcements, please visit the **Formal Methods Europe** website [http://www.fmeurope.org], the **EATCS** website [http://www.eatcs.org] and the **Virtual Library Formal Methods** website [http://vl.fmnet.info/meetings].

Joining Other Societies and Groups

London Mathematical Society
http://www.lms.ac.uk/contact/membership.html

Formal Methods Europe
http://www.fmeurope.org/fme/member.htm

European Association for Theoretical Computer Science
http://www.eatcs.org/howtojoin.html

Association for Computing Machinery
https://campus.acm.org/Public/QuickJoin/interim.cfm

IEEE Computer Society
http://www.computer.org/join/

Back to Contents page

Job Adverts

University of Leicester

Department of Computer Science
(www.cs.le.ac.uk)

Lecturer A/B in Computer Science (2 posts)

(Available from September 2005)

£23,643 to £35,883 per annum

Ref: A2044
The University seeks to appoint two Lecturers in Computer Science who can contribute to existing research in the foundations and applications of algebraic structures and methods in general, and the emerging area of service-oriented computing in particular. Preference will be given to candidates with an interest in one or more of (co)algebraic structures and methods; categorical structures; hybrid, probabilistic, and timed systems; inductive and coinductive methods; modal logics; calculi and models of concurrent, distributed, mobile, and context-aware computing; model transformation techniques. However, candidates in related areas are also encouraged to apply.

Downloadable application forms and further particulars are available from www.le.ac.uk/personnel/jobs or from Personnel Services, telephone: +44 116 252 2758, fax: +44 116 252 5140, email: jobs@le.ac.uk. Please note that CV's will only be accepted in support of a fully completed application form.

Informal enquiries are welcome and should be emailed to Professor Rajeev Raman (the Head of Department) at r.raman@mcs.le.ac.uk, Dr. Alexander Kurz [ak155@mcs.le.ac.uk], Dr. Reiko Heckel [reiko@mcs.le.ac.uk], or Professor José Fiadeiro [jwf4@mcs.le.ac.uk].

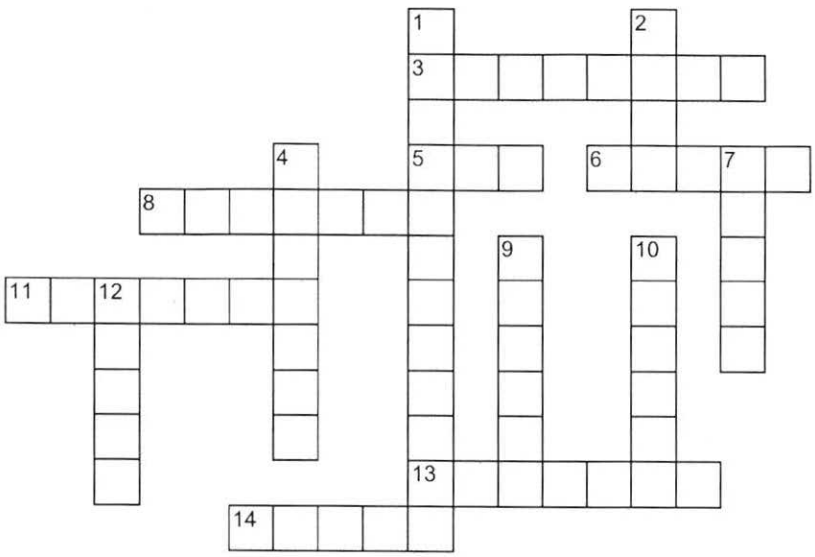
Closing date: **Tuesday 5 July 2005**

Promoting equality of opportunity throughout the University

Back to Contents page

Formal Methods Coffee Time

Judith Carlton



Across

3 borrowed philosophical term
5 new bird from W3C
6 famous Vulcan
8 mobile phone operating system
11 increasingly popular browser
13 Cambridge security expert (surname)
14 1815 - 1864 very logical (surname)

Down

1 Lindisfarne's forecast for FM05? (four words)
2 dodgy software can land you in this
4 new home games console
7 Bluetooth worm
9 1815 - 1864 very logical (first name)
10 Austrian city
12 Cambridge security expert (first name)

If you would like to set a puzzle for *FACS FACTS*, please contact Judith Carlton, the **Puzzles Columnist**, on jcarlton@www.eschertech.com

Please remember to include the solution to your puzzle ☺

BCS FACS

FACS membership application/renewal (2005)

Title (Prof/Dr/Mr/Ms) _____ **First name** _____ **Last name**_____

Email address (required for options * below)_____

BCS membership No. (or sister society name + membership number)

_____

Address _____

_____

_____

Postcode _____ **Country** _____

I would like to take out **membership to FACS** at the following rate:

- ❑ £15 (Previous member of BCS-FACS now retired, unwaged or a student)
- ❑ £15 (Member of BCS or sister society with web/email access)*
- ❑ £30 (Non-member or member of BCS or sister society without web/email access)

In addition I would like to subscribe to **Volume 17 of the FAC journal** at the following rate:

- ❑ £46

For electronic only journal subscription*, please tick here ❑. No further discount given.

The total amount payable to BCS-FACS in **pounds sterling** is **£ 15 / 30 / 61 / 76** (delete as appropriate). I am paying by:

- ❑ Cheque made payable to **BCS-FACS (in pounds sterling)**
- ❑ Credit card via PayPal (instructions can be found on the BCS-FACS website)
- ❑ Direct transfer (in **pounds sterling**) to:

  Bank: Lloyds TSB Bank, Langham Place, London
  Sort Code: 30-94-87
  Account Number: 00173977
  Title of Account: BCS-FACS

If a receipt is required, please tick here ❑ and **enclose** a stamped self-addressed envelope.

Please send completed forms to:

Dr Paul P Boca
PO BOX 32173
LONDON N4 4YP
UK

For FACS use only

Received by FACS	Date:	Initials:
Sent to Springer	Date:	Initials
Actioned by Springer	Date:	Initials

BCS-FACS Evening Seminar

Domain Engineering

Professor Dines Bjørner (DTU, Denmark)

25 July 2005

5.45pm

BCS London Offices
First Floor
The Davidson Building
5 Southampton Street
London WC2E 7HA

Before software can be designed we must know its requirements. Before requirements can be expressed we must understand the domain. So it follows, from our dogma, that we must first establish precise descriptions of the domain, then from such, "derive" at least the domain requirements, and from those and other requirements (interface and machine) design the software, or, more generally, the computing system.

In this talk we will outline what goes into a domain description, not so much how we acquire what goes in. That is: Before we can acquire domain "knowledge" we must know what are suitable structures of domain descriptions. This we shall outline ideas of Modelling the Intrinsics (or a domain), the Business Processes (of ...), the Support Technologies (of ...), the Management & Organisation (of ...), the Rules & Regulations (and Scripts) (of ...), and the Human Behaviours (of a domain).

The examples of the talk will mostly be taken from ongoing research into "A Domain Theory for Railways".

Refreshments will be served from 5.15pm

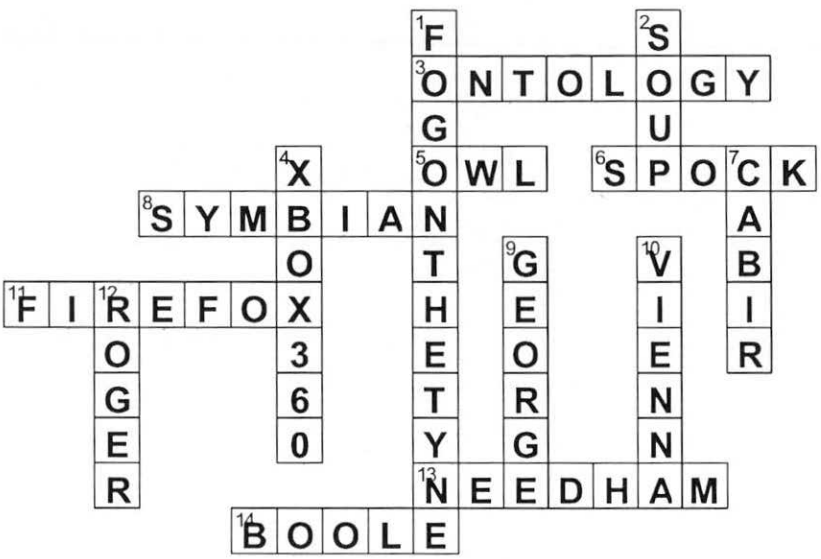
The seminar is **free of charge** and open to everyone. If you would like to attend, please email Paul Boca [paul.boca@virgin.net] your name by 21 July 2005. Pre-registration is required, as security at the BCS Offices is quite tight.

Seminars webpage: http://www.bcs-facs.org/events/EveningSeminars/

Back to Contents page

And Finally

Solution to crossword on page 49:



Guess the caption competition

After the recent FACS evening seminar, Professor Jonathan Bowen, FACS Chair, and Dr Sue Black, BCSWomen Chair, continue discussions in a local hostelry. Why was Dr Black so shocked? Answers by email to the Editor [editor@facsfacts.info].

Back to Contents page

FACS Committee

Jonathan Bowen
FACS Chair
ZUG Liaison

Jawed Siddiqi
Treasurer

Paul Boca
Secretary and
Newsletter Editor

Roger Carsley
Minutes
Secretary

John Cooke
FAC Journal
Liaison

Ali Abdallah
Events Coordinator

John Fitzgerald
FME Liaison
SCSC Liaison

Margaret West
BCS Liaison

Mike Stannett
Webmaster
LMS Liaison

Judith Carlton
Industrial Liaison

Kevin Lano
UML Liaison

Rick Thomas
LMS Liaison

Rob Hierons
Chair, FM and
Testing Subgroup

FACS is always interested to hear from its members and keen to recruit additional Committee members. Presently we have vacancies for officers to handle publicity and help with fund raising, and to liaise with other specialist groups such as the Requirements Engineering group and the European Association for Theoretical Computer Science (EATCS). If you are interested in helping the Committee, please contact the FACS Chair, Professor Jonathan Bowen, at the contact points below:

BCS FACS
c/o Prof. Jonathan Bowen (Chair)
London South Bank University
Faculty of BCIM
Borough Road
London SE1 0AA
United Kingdom

T +44 (0)20 7815 7462
F +44 (0)20 7815 7793
E info@bcs-facs.org.uk
W www.bcs-facs.org

You can also contact the other Committee members via this email address.

Please feel free to discuss any ideas you have for FACS or voice any opinions openly on the FACS mailing list [FACS@jiscmail.ac.uk]. You can also use this list to pose questions and to make contact with other members working in your area. Note: only FACS members can post to the list; archives are accessible to everyone at http://www.jiscmail.ac.uk/lists/facs.html .

Announcement from Escher Technologies Ltd

The Educational Edition of the formal methods software development tool known commercially as *Perfect Developer* is to be made FREELY AVAILABLE to universities from August 2005. It always has been free for individual student projects; from August, it will be free for classroom teaching as well.

Perfect Developer Version 3 was released in December 2004. There will be a tutorial on Perfect Developer at FM05, 19 July.

For more information on Perfect Developer, please see Escher's website [http://www.eschertech.com] and also the article in Issue 2004-3 of *FACS FACTS*.

Back to Contents page