FACS FACTS

The Newsletter of the BCS Special Interest Group in

Formal Aspects of Computing Science

Issue 2003-1 July 2003 ISSN 0950-1231

Contents

Editorial

FACS FACTS is the newsletter of the BCS Formal Aspects of Computer Science (FACS) special interest group. It publishes reports on events organised or attended by the group, and announcements of relevant conferences, books, etc. Previously it was known as *FACS EUROPE* as it was published in association with the FM Europe organisation. The FACS newsletter welcomes short articles on formal methods activities, books, workshop reports, etc. Send any contributions to Kevin Lano in Word or text format, kcl@dcs.kcl.ac.uk.

BCS-FACS: A report from the trenches

Paul Boca and Jonathan Bowen

BCS-FACS (Formal Aspects of Computing Science) is a specialist group of the British Computer Society founded in 1978 to promote the awareness of formal approaches to the construction of computer-based systems. The group, unlike any other affiliated with the BCS at the time, set out to address real issues in computer science. It organised a number of events on different topics: concurrency, domain theory, formal aspects of HCI and formal aspects of object oriented programming to name but a few. These have had different lengths and formats, sometimes providing tutorial sessions to introduce new theories and formalisms. The FACS Christmas workshops proved to be particularly popular, and not just for the opportunity to do some last minute shopping!

However, during 2000–2001 FACS became inactive due to a reduction in the amount of time some committee members could devote to FACS. (FACS is run solely by volunteers, and requires a substantial amount of effort to operate it effectively.) The skeleton committee, led by John Cooke, kept the group ticking over and decided not to charge members fees during this period of inactivity.

The situation improved dramatically in 2002 with the appointment of additional committee members and the election of a new Chairman, Professor Jonathan Bowen of London South Bank University. Jonathan brought new ideas and enthusiasm with him to the role, and set about relaunching and modernising FACS. The timing was perfect as FACS was due to celebrate its 25th anniversary. FACS marked this anniversary by organising a Christmas event on formal methods in security. The event was a success; FACS had turned the corner, confident of once again providing a service to its members and the computer-science community.

This article summarises what FACS has achieved since the relaunch, and describes what members can expect in the future.

FACS Committee

The FACS committee has had a surprisingly low turnover of members during the last twenty-five years. John Cooke, one of the founders of FACS, is still on the committee, continuing to liaise with Springer on journal matters. (John is associate editor of the *Formal Aspects of Computing* journal.) Unfortunately, three long-standing members – Tim Denvir (former Chairman, Newsletter Editor and FME Liaison officer), Ann Wrightson (BSI Liaison and former Newsletter Editor) and Olwen Morgan (former Treasurer) – have recently stepped down. FACS is very grateful for all of their hard work over the years and its longevity attests to their efforts.

At the recent AGM, held at London South Bank University on 12 March 2003, the following members joined the committee:

- Judith Carlton (Industrial Liaison),
- John Fitzgerald (FME and Safety-Critical Systems Club Liaison) and
- Kevin Lano (Newsletter Editor).

Jonathan Bowen was re-elected Chairman and the existing committee re-elected to their roles. A full list of the committee members is given, as usual, at the end of the Newsletter.

Events

In 2002, Dr Ali Abdallah of London South Bank University became the Events Coordinator for FACS, a new role that has been crucial in the reinvigoration of FACS activities. Since then, FACS opened up a number of seminars by prominent formal methods researchers to its members. These were mainly held at London South Bank University, and one was held at De Montfort University in which Professor Mike Gordon, FRS, of the Cambridge University Computer Laboratory spoke on *The Convergence of Deduction and Computation* on 1 October 2002. The South Bank seminars included:

- 14 March 2002: *Formalising Object-oriented Programming*, Professor He Jifeng (International Institute for Software Technology, United Nations University, Macau, China).
- 22 April 2002: *Modelling and Code Monkeys*, John Fitzgerald (Transitive Technologies Ltd. & The Centre for Software Reliability, University of Newcastle, UK).
- 20 September 2002: *Sanity Checking Your Software Design and Test Strategy with AsmL*, Wolfram Schulte (Microsoft Research, Redmond, USA).
- 19 May 2003: *Model Checking Synchronous Programs using DCVALID*, Paritosh K. Pandya (Tata Institute, Mumbai, India).

FACS members were also invited to attend the second day of a Formal Methods and Testing (FORTEST) [www.fortest.org.uk] meeting at the University of York on 13 September 2002. FORTEST is an EPSRC UK government funded Network that brings together academic and industrial expertise in the formal aspects of software testing. The event consisted of research presentations, brainstorming and discussions, including the following:

- AnaTempura (run time verification approach), Ben Moszkowski and Antonio Cau (De Montfort University).
- Functional Testing of Hardware Designs, Salim Vanak (University of Sheffield).
- Automatic Guidance for the Formal Verification of High Integrity Ada, Andrew Ireland (Heriot-Watt University).
- MOTIVE: Method for Object Testing, Integration and Verification, Tony Simons (University of Sheffield).
- What do we do when we test a Z Specification? Professor John Derrick (University of Kent at Canterbury).
- Expanding an Extended Finite State Machine for Testability, Rob Hierons (Brunel University).

FACS ended 2002 by organising a major Christmas event on Formal Aspects of Security (FASec), held at Royal Holloway (University of London), 18–20 December 2002. This International Conference, which also celebrated the 25th anniversary of FACS, was highly successful, with nearly 60 attendees from around the world and some very eminent invited speakers. Professor Fred Schneider (Cornell University, USA) was the keynote speaker and there were six other invited speakers, several from Microsoft Research (Cambridge) who also sponsored the event. The proceedings will appear in the Springer-Verlag *Lecture Notes in Computer Science* series (LNCS volume 2629) later this year. The conference has helped to raise the profile of FACS internationally and a fuller report on this event can be found elsewhere in this Newsletter.

Sponsorship

FACS has provided sponsorship for both events and students.

The group sponsored the BCS-FACS Refinement Workshop held in Copenhagen, Denmark, 20–21 July 2002, in association with the FME (Formal Methods Europe) Conference [www.cs.kent.ac.uk/people/staff/eab2/refine/floc.html]. The proceedings are available in the *Electronic Notes in Computer Science Series* (Volume 70, Issue 3) published by Elsevier. This continues a long-standing tradition of support by FACS for the series of Refinement Workshops over the years.

FACS was a co-sponsor of two British Computer Society Guildford Branch meetings held at the University of Surrey. The first of these, on 21 March 2002, was a talk by Dr David Crocker of Escher Technologies Limited (and also a member of FACS) entitled *Software without Bugs*. This included information on a new tool, Perfect Developer, for developing object-oriented software using a formal refinement approach. The second event, held recently on 22 May 2003, was a debate on *Formal versus Real-world Methods in Software Engineering*, chaired by Professor Khurshid Ahmad (University of Surrey).

Dr Roger Peel (University of Surrey), Dr David Crocker (Escher Technologies Limited), Shaun Lehane (BCS Guildford Branch Chairman) and Professor Jonathan Bowen (BCS-FACS Chair) [www.bcsguildford.freeserve.co.uk/album.htm]

The MENA (Middle East/North Africa) Summer School on *Parallel, Distributed, and Internet Computing: Theory, methods, applications and research directions*, held 8–19 July 2002 at the Centre for Advanced Mathematical Sciences, American University of Beirut, Lebanon, was supported by BCS-FACS along with many other organizations including the United Nations University as a joint organiser. This new two-week summer school with courses on computing is planned to be a series and is aimed at young scientists from developing countries. In the courses, there was a special emphasis on the importance of the relevant scientific foundations for engineering correct, reliable and efficient computing systems.

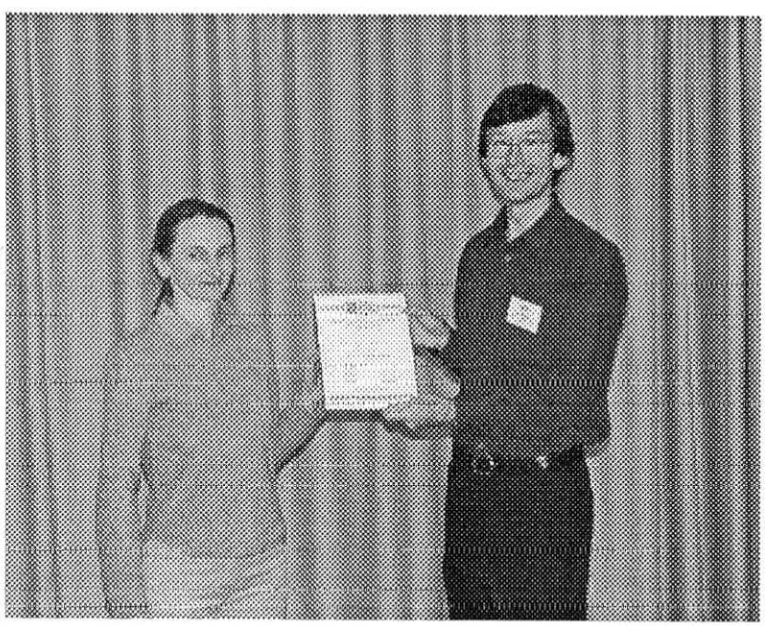
Students

At ZB2003 [www.tucs.fi/zb2003], the 3rd International Conference of B and Z Users (Turku, Finland, 4–6 June 2003), FACS provided sponsorship in the form of two best paper prizes.

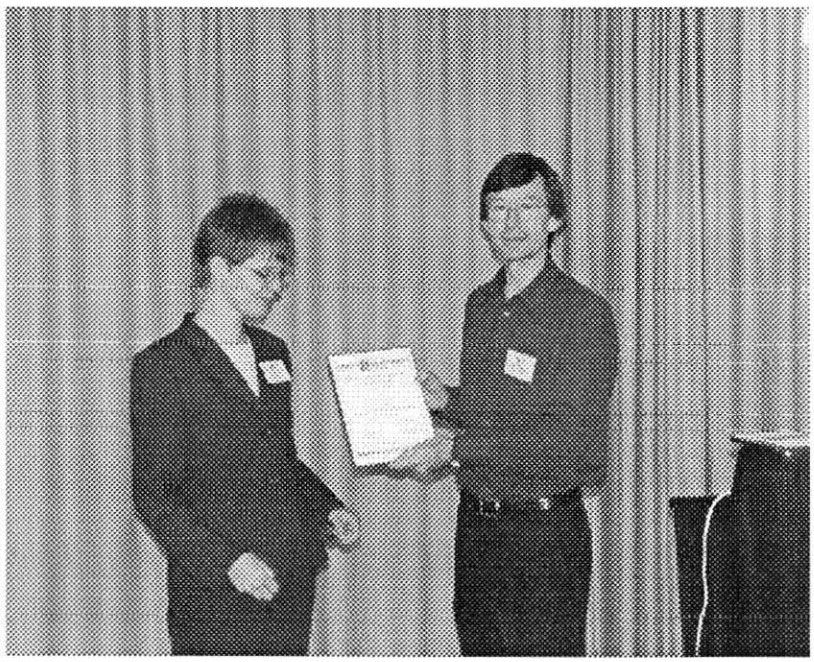
Delegates were able to vote for these at the end of the conference. There were around 80 international attendees and FACS flyers and membership forms were issued in all the delegates' packs. The Best Z/B Paper overall was awarded to *Probabilistic termination in B* by Annabelle McIver, Carroll Morgan and Thai Son Hoang, presented by Annabelle McIver (Macquarie University, Sydney, Australia). In addition, a prize for the Best Student Presentation was awarded to Christine Poerschke (Oxford Brookes University) for her animated presentation of a paper entitled *A formal specification in B of a medical decision support system* by Christine Poerschke, David E. Lightfoot and John L. Nealon. There were a number of very good student presentations, but this one stood out for its interesting topic, a medical support system used in the treatment of diabetes, presented in an informative and lively manner. The recipients of the awards will each receive a subscription to the Formal Aspects of Computing journal and a year's membership of FACS.

The general standard of papers and presentations at ZB2003 was high and the conference also featured invited talks by Daniel Jackson (MIT, USA) on the Alloy logical modelling language and associated tool, Jean-Raymond Abrial (Marseille, France) on $B^{\#}$, a suggested synthesis of B and Z, and Professor Bertrand Meyer (ETH Zürich, Switzerland) on practical proofs of class correctness. The proceedings of ZB2003 have appeared in the Springer-Verlag *Lecture Notes in Computer Science* series (LNCS volume 2651).

FACS is providing help for postgraduate students to attend the FM2003 conference [fme03.isti.cnr.it] organised by FME in Pisa, Italy, 8–14 September 2003. The intention is to offer more sponsorship of this kind in the future.



Annabelle McIver receiving her Best Paper certificate at ZB2003 [www.tucs.fi/zb2003/pics]



Christine Poerschke receiving her Best Student Presentation certificate at ZB2003
[www.tucs.fi/zb2003/pics]

Keeping Members Informed

FACS uses three vehicles for keeping in touch with its members: a newsletter, an electronic mailing list, and a website.

Newsletter

The FACS Newsletter (ISSN 0950-1231) is a periodic informative publication, containing details of upcoming formal methods conferences, conference reports, book reviews and job vacancies, tools and news from the Formal Methods Europe (FME) [www.fmeurope.org] and the British Computer Society [www.bcs.org]. In the past, editions have included columns on topics such as Functional Programming, VDM and Z, and short articles. Contributions from members are always welcome; please send them (as plain text or Microsoft Word attachments) to the Newsletter Editor, Kevin Lano [kcl@dcs.kcl.ac.uk].

Newsletters are available for download from the FACS website. Hardcopies will **only** be sent to those members without email/web access.

Electronic Mailing List

For many years, Loughborough University kindly provided facilities for hosting and maintaining the FACS mailing list. FACS decided to change over to using the National Academic Mailing List Service JISCmail [www.jiscmail.ac.uk] for hosting the mailing list, as it provides facilities for archiving messages; the monthly archives are accessible online [www.jiscmail.ac.uk/lists/facs.html].

The mailing list is closed; that is to say, only FACS members can post to it. This helps to avoid the worst excesses of spam email. Any announcements and discussion relevant to the interests of FACS are welcome.

Traffic on the mailing list is moderate at present, but members may still prefer to receive messages in digest form. To arrange this, simply follow the "change-settings" link at the above web page. If you have any problems, please contact the Membership Secretary, Paul Boca [Paul.Boca@virgin.net].

Website

The first step taken towards modernising FACS was to revamp the website. Much effort was spent building the new site with a new and more appropriate web address [www.bcs-facs.org] by the new website maintainer, Mike Stannett. In addition, FACS committee members discussed and reviewed its content. The site is now hosted on a web server at London South Bank University, provided as a free resource for the FACS group. The result is a useful resource for FACS members that contains a wealth of information, including upcoming events and conferences of interest, links to other formal methods organisations, journal information and membership forms. If you have any comments on the website, or would like to suggest URLs for inclusion, please contact the BCS-FACS webmaster, Mike Stannett [M.Stannett@dcs.shef.ac.uk].

Joining FACS

FACS members receive information on formal methods activities via a newsletter and an electronic mailing list. In addition, they receive a discount at FACS events when this is available. When joining FACS, members have the opportunity to take out a subscription to the *Formal Aspects of Computing* journal, arguably the leading journal in the area of formal methods, at a substantially reduced rate. It is well worth joining FACS for this reason alone if you wish to subscribe to this journal as an individual. Some back issues of the journal can be ordered through FACS at a reduced rate too.

Anyone can become a member of FACS, but reductions are available for BCS (and affiliate professional society) members with web/email access. A new reduced rate for former FACS members now retired, unwaged or studying for a degree has recently been introduced. FACS accepts three forms of payment: cheque (in pounds sterling), direct transfer and credit/debit card. FACS uses PayPal to process the card payments, which may be especially useful for members outside the UK.

If you would like to join FACS, please complete a membership form, which can be downloaded from www.bcs-facs.org/forms.html, and return it to the Membership Secretary with the appropriate fee.

Future directions

FACS aims to organise further events and seminars to promote the use of formal methods. The main event in the FACS calendar in 2003 is *Formal Aspects of XML*, to be held at the Royal Society (London) in December 2003. Further details and a call for papers appear elsewhere in this Newsletter and more information will be linked from the FACS website and distributed on the FACS electronic mailing list in due course.

We also aim to sponsor further relevant meetings and conferences and this is a topic of active discussion by the FACS committee. It has been decided to sponsor IFM 2004 and AMAST 2004 with prizes in a similar manner to ZB2003 and a further UK event is under

consideration for more extensive sponsorship. Any members involved with events which they think could benefit from FACS sponsorship should write to the FACS Chair, Jonathan Bowen [www.sbu.ac.uk/~bowenjp], in the first instance, with a brief proposal on the amount of sponsorship required, for what it is needed (e.g., support of postgraduate student presenters), the benefits for FACS (e.g., distribution of flyers) and any other relevant information. Note that events should include an explicit formal methods component in their announcement and activities to be considered for sponsorship by FACS.

The Chair welcomes any suggestions for future FACS activities by members, particularly if you are willing to be involved in their organisation. Please do contact the Chair directly [jonathan.bowen@sbu.ac.uk] or air your ideas on the FACS mailing list for general discussion [facs@jiscmail.ac.uk]. And please do visit the newly revitalised website every so often for the latest information on events, etc. [www.bcs-facs.org].

Some events sponsored/organised by the BCS-FACS group

Paul Boca

2004

- IFM 2004: 4th International Conference on Integrated Formal Methods, 5 – 7 April, Canterbury, England

2003

- ZB2003: 3rd International Conference of B and Z Users, 4 – 6 June, Turku, Finland
- Formal Methods for Engineering Special-Purpose Parallel Systems, 6 – 9 January, Hawaii

2002

- Formal Aspects of Security (FASec), 18 – 20 December 2002, Royal Holloway, University of London
- REFINE 2002, 20 – 21 July, Denmark
- MENA Summer School 2002 on Parallel, Distributed, and Internet Computing: Theory, methods, applications and research directions, 8-19 July, Lebanon
- 4th Workshop on Rigorous Object-Oriented Methods ROOM 4, 21 – 22 March, King's College London

2001

- IEEE 1394 (FireWire) Workshop: International Workshop on Application of Formal Methods to the IEEE 1394 Standard, 13 March, Germany (Co-located with FME '01)

2000

- ZB2000: 1st International Conference of B and Z Users, 29 August – 2 September, University of York

1998

- FACS at 21, 2nd December, The Royal Society, London
- ZUM '98: 11th International Conference of Z Users, 24 – 26 September, Germany
- 3rd BCS-FACS Northern Formal Methods Workshop, 14 – 15 September, Ilkley
- Theory and Practice of Tools for Formal Methods, 1998, 6 – 7 July, City University

1997

- 2nd BCS-FACS Northern Formal Methods Workshop, 14 – 15 July 1997, Ilkley

- Systems and Partial Descriptions: from Practice to Theory, 18 – 20 May, Grasmere
- ZUM '97: 10th International Conference of Z Users, 3 – 4 April, University of Reading

1996
- 1st BCS-FACS Northern Formal Methods Workshop, 23 – 24 September, Ilkley
- Formal Aspects of The Human Computer Interface, 10 – 12 September, Sheffield Hallam University
- 7th BCS-FACS Refinement Workshop, 3 – 5 July, Bath
- Methods Integration Workshop, 25 – 26 March, Leeds

1995
- BCS-FACS Christmas Workshop on Semantics, 18 – 19 December, Imperial College
- ZUM '95: 9th International Conference of Z Users, 7 – 8 September, University of Limerick.

1994
- BCS-FACS Christmas Meeting on Concurrency, 19 – 20 December, Imperial College
- ZUM '94: 8th Z User Meeting, 29 – 30 June, Cambridge
- A Symposium on Conquering the Complexity of Concurrency, 22 – 24 March, University of Manchester
- 6th BCS-FACS Refinement Workshop: Theory and Practice of Formal Software Development, 5 – 7 January, City University

1993
- BCS-FACS Christmas Meeting: Formal Aspects of Object-Oriented Systems, 16 – 17 December, Imperial College
- International Workshop on Semantics of Specification Languages, 25 – 27 October, University of Utrecht
- 3rd International Conference on Algebraic Methodology and Software Technology, AMAST, 21 – 25 June, University of Twente, The Netherlands
- 2nd BCS-FACS Workshop on measurement: Practical Applications of Formal Software Measurement, 29 March, University of Bristol

1992
- BCS-FACS Christmas Workshop: Turning a Formal Eye on Requirements, 16 – 17 December, Imperial College
- 5th BCS-FACS Refinement Workshop, 8 – 10 January, London

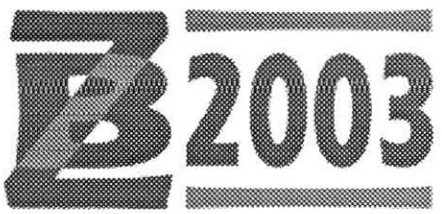
1991
- BCS-FACS Christmas Meeting on Domain Theory, 19 – 20 December, City University
- BCS-FACS RAISE Tutorial, 30 September – 2 October, University of Manchester
- Formal Aspects of Measurement, 3 May, South Bank Polytechnic
- 4th BCS-FACS Refinement Workshop, 9 – 11 January, Cambridge University

1990
- 3rd BCS-FACS Refinement Workshop, 9 – 11 January, IBM UK Laboratories, Hursley Park

1988
- Term Rewriting workshop and tutorial, 26 – 28 September, University of Bristol
- Specification and verification of concurrent systems, 6 – 8 July, University of Stirling

Conference and Workshop Reports

ZB2003 conference report



Marina Waldén

Local Organizing Committee Chair
Åbo Akademi University

The third International Conference of B and Z Users (ZB2003) was held at Hotel Hamburger Börs in Turku, Finland, in June 4-6 2003. B and Z are two important formal methods that share a common conceptual origin; they are leading approaches in industry and academia for the specification and development (using formal refinement) of computer-based systems. In ZB2003 the B and Z communities came together to hold a joint conference that simultaneously incorporated the 14th International Conference of Z Users and the 5th International Conference on the B Method. The International B Conference Steering Committee (APCB) and the Z User Group (ZUG) used the conference as a venue for open meetings intended for those interested in B and Z, respectively. The location of ZB2003 in Turku reflects the important work in the area of formal methods carried out at Åbo Akademi University and the Turku Centre for Computer Science (TUCS), especially that involving the B method.

The 79 conference attendants came from different parts of the world: 24 representatives from United Kingdom; 15 from France; 6 from Australia; 25 from Finland, and some representatives from USA, Switzerland, New Zealand, Canada, Macao and Germany. These participants were mainly from academia; industry was represented by 9 attendants in total from France, Finland, USA and Germany.

At the ZB2003 conference invited speakers from both industry and academia addressed significant recent industrial applications of formal methods, as well as important academic advances aimed at enhancing their potency and widening their applicability. *Jean-Raymond Abrial*, a consultant based in Marseille, France, is the progenitor of both Z and B. He gave a lecture on the project $B^{\#}$, which integrates ideas from both B and Z for modelling complex systems. His lecture was sponsored by Formal Methods Europe (FME). Prof. Dr. *Bertrand Meyer* is Chair of Software Engineering in the Department of Computer Science at the world renowned ETH in Zürich, Switzerland. In his invited speech he presented his work on creating a theory and framework for correctness proofs of classes to produce a library of correct object-oriented components. The third invited speaker, *Daniel Jackson*, is the Ross Career Development Professor of Software Technology at MIT, USA. He has developed Alloy, a lightweight modelling language based on a subset of the Z notation, and the Alloy Analyzer, a tool for automatically analyzing models. Alloy and the Alloy Analyzer were the topics of his speech.

In addition to the invited talks 27 papers were presented at the conference. Out of the 46 submitted papers (24 for the B track and 22 for the Z track) 28 papers (13 papers on Z and 15 on B) were accepted after a peer review. Two of the accepted B papers were short papers on industrial case studies. The topics presented by the authors of the accepted papers concerned the use of patterns in Z and B, applications and refinement issues in B and Z, probability aspects in B, extensions to B, model checking for Z specifications, object orientation and testing within Z, as well as the introduction of an XML format to Z. Although

the ZB2003 conference was logistically organized as an integral event, editorial control remained vested in two separate but cooperating programme committees that respectively determined the B and Z content in a coordinated manner.

The best Z/B paper and the best student presentation were elected by the conference participants. The paper *"Probabilistic termination in B"* by Annabelle McIver, Carroll Morgan, and Thai Son Hoang (presented by Annabelle McIver) was elected the *best paper. Christine Poerschke* was awarded the *best student presentation* with the paper "*A formal specification in B of a medical decision support system*" by Christine Poerschke, David E. Lightfoot, and John L. Nealon. The prizes were free BCS-FACS membership and subscription to the Formal Aspects of Computing journal for one year.

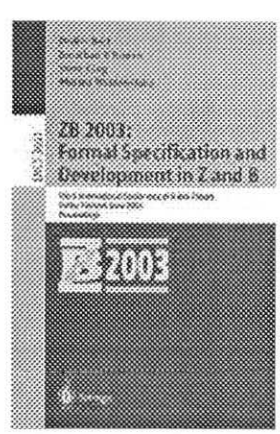
A variety of tools were demonstrated at the ZB2003 conference: a new interface for the Atelier B prover; a tool for translating UML diagrams to B; a model checker for B; tools for testing Z and B specifications, and a tool for developing probabilistic B. These tools were also presented in a separate tools session. In addition, the publisher McGraw Hill had a book display at the conference.

On 3rd June, a day before the main conference, Jean-Raymond Abrial gave a tutorial on Event-B in the afternoon. It was held in the facilities of the Computer Science Department of Åbo Akademi University and was attended by 19 of the conference participants.

Partly in parallel with the tutorial, on 3rd June the Second International Workshop on Refinement of Critical Systems: Methods, Tools and Developments (RCS'03) took place. The workshop was arranged by the EU-project MATISSE: Methodologies and Associated Technologies for Industrial Strength Systems Engineering (IST-1999-11435). The workshop was held in the facilities of the Computer Science Department of Åbo Akademi University. There were 11 presentations on refinement methodologies, tool support, compositional models, and case studies. 45 participants registered for the workshop. In the afternoon, some of the workshop participants took part in the tutorial.

The ZB2003 conference was organized by Prof. Jonathan Bowen as the Conference Chair, Prof. Didier Bert as the B Programme Committee Chair, Dr. Steve King as the Z Programme Committee Chair, and Dr. Marina Waldén as the Local Organizing Committee Chair. The conference was sponsored by ClearSy System Engineering, Nokia, FME (Formal Methods Europe), BCS-FACS (the British Computer Society Formal Aspects of Computing Science specialist group) and ZUG (Z User Group). Online information concerning the conference is available under the following Uniform Resource Locator (URL): http://www.tucs.fi/zb2003/. As a conclusion it can be said that the scientific programme of the ZB2003 conference was of high quality thanks to the invited speakers and the paper presentations. This was also expressed in the feedback collected from the opinion poll conducted on the last day of the conference.

Turku, Finland, 3rd July 2003



Reference

Didier Bert, Jonathan P. Bowen, Steve King and Marina Waldén (eds.). *ZB2003: Formal Specification and Development in Z and B*, 3rd International Conference of B and Z Users, Turku, Finland, 4–6 June 2003. Springer-Verlag, Lecture Notes in Computer Science, volume 2651. ISBN 3-540-40253-5. (xiii+547 pages)

FORTEST meeting report

Tim Denvir

FORTEST [www.fortest.org.uk] is the ESPRC funded network that brings together academic and industrial organisations with expertise in formal methods and testing. Research meetings are held every quarter and the sixth of these was held in Bath on 25th May 2003, hosted by Praxis Critical Systems [www.praxis-cs.co.uk].

Many institutions are associated with FORTEST, including a number from outside the UK. After attending two of their workshops, I have been struck by the lively interaction and interest in each other's work shown by those attending the meetings. Six scheduled talks were given at the sixth meeting, and an additional unscheduled one from Daniel Jackson, who was visiting Praxis Critical Systems at the time and was even willing to talk to delegates while we were eating our lunch!

In the following reports, the variability of detail and accuracy reflects the variability of my own understanding of the talks, rather than the substance of their contents.

Peter Amey (Praxis Critical Systems) SPARK: Industrial Strength Formality

There is a question of how the use of formal methods and testing can relate to each other contextually. Peter Amey referred to this issue at the outset of his talk by quoting an often-held view: "Testing is something you do at the end to show that everything you have done before is correct". He went on to refer to several background issues – the need for formal approaches, semantic gaps (between specifications and source, source and object code, etc.), and that no amount of testing is sufficient. He went through a number of frequent problems with languages – lack of standardisation, ambiguities, aliasing, side effects, dialects and poor requirements capture. He advocated well-defined safe language subsets and static analysis, some of the driving concepts behind SPARK and showed how, with this policy, the SPARK prover scores 92% of VCs on well written code [www.sparkada.com].

Andrew Ireland (Heriot Watt University) Proof Automation for SPARK Run-Time Check Verification Conditions

Andrew Ireland continued on this theme by describing proof planning in SPARK, and using the SPADE proof checker to check that bounds of integer ranges are not violated. SPARK lets you insert annotations in the form of assertions, and loop invariants.

If a goal cannot be proved, it could be an opportunity to generate counterexamples to the goal in the form of focussed test data.

Rob Hierons (Brunel University) Ordering Adaptive Test Sequences

An adaptive test sequence is one in which the next test sequence depends on the outputs from previous ones. Rob Hierons explored the properties of trees of test sequences, the time taken to check various properties, capabilities etc.

Daniel Jackson (MIT) Alloy

In this unscheduled talk generously offered by Daniel Jackson, he described the Alloy system [sdg.lcs.mit.edu/alloy]. In Alloy, assertions are conjectures (to be proved). The system searches for counterexamples; the approach is to use small numbers of tests, based

on a model checking strategy, rather than random testing. The system allows one to declare "facts" (which sound like axioms). Relations are central; there are no functions, so no partial functions, 3-valued logics, undefinedness etc.

Ian Gilchrist (IPL) Software Safety Standards and Verification

Ian Gilchrist's talk concerned software safety standards, which often form a context in which formal methods are used in order to increase reliability. He described how software safety standards are frequently derived from each other, and explained safety integrity levels. The standards also include requirements for traceability, repeatability and other desired properties.

Tim Denvir (Killen) A Methodological Context for Testing and Proof

There is an apparent dilemma in that if SW has been proved correct, there should be no need to test it; but no sane person would deliver untested SW. Tim Denvir believed that testing was not just supplying "belt and braces"; rather, testing has a rôle in mathematical proof, namely the search for a counterexample to the claim that one has a proof. He illustrated this by reference to an early discussion in mathematics, the proof and counterexamples to Euler's theorem relating the numbers of vertices, edges and faces of a polyhedron. This 150 year long exploration was explored via a Socratic dialogue in Lakatos' "Proofs and Refutations". The principles might be related to the SPARK techniques described earlier.

David Pitt (University of Surrey) Local Invariance

David Pitt talked of "overtaking" in concurrent systems. He used the analysis of the Railway Interlocking Protocol, carried out with Smith's Industries and BR. He advocated building one's syntax to match one's semantics, and relating integration to local invariants.

Object Oriented Technology in Aviation Workshop

Judith Carlton

NASA and the FAA have sponsored a program in Object Oriented Technology in Aviation (OOTiA). Two workshops have been held - OOTiA 1 in 2002, and OOTiA 2 this March. Their purpose was to bring together people from the FAA, industry, military and research community in order to identify safety and certification issues relevant to using OOT in aviation applications. Two of us from Escher Technologies Ltd participated this year, David Crocker and I.

The current situation in aviation software development in the USA is that they have to follow a set of guidelines called RTCA/DO-178B. These were published as long ago as December 1992, which means that the procedures followed consist, broadly, of structured programming and exhaustive testing. Formal Methods (FM) does get a passing mention in DO-178B, as being a Good Thing, but I found that most attendees knew nothing of them. A few did, having tried them long ago, and found them too difficult and/or too slow.

Having realized that commercial software development has moved to the object-oriented paradigm, NASA/FAA thought that maybe they ought to try to update the guidelines. Hence the workshops, as it isn't at all clear how OOT can fit in with DO-178B, and we don't want any planes dropping out of the sky, do we! Several issues had been identified at OOTiA 1, and these were further discussed. Many of the participants were very knowledgeable about OOT, but some weren't, and their misunderstandings of what was involved muddied the already sufficiently murky waters.

However, from the start, I was puzzled as to why they were dissecting OOT and discussing in detail if this or that aspect would be safe, instead of using FM and proving it one way or the other. Wondering what obvious point I was missing, I went round asking any people I could find who seemed from their general remarks to have reasonably broad experience. And I got the answers outlined above (too difficult and too slow). Except from one States-based gent who's writing a transformational tool, and who said, in effect: yes of course they should be using FM, this OO stuff is just irrelevant then!

Come the Open Issues breakout session, the two of us from Escher Technologies – together with Rod Chapman from Praxis Critical Systems – thought it was the appropriate time to say a word or several for FM.

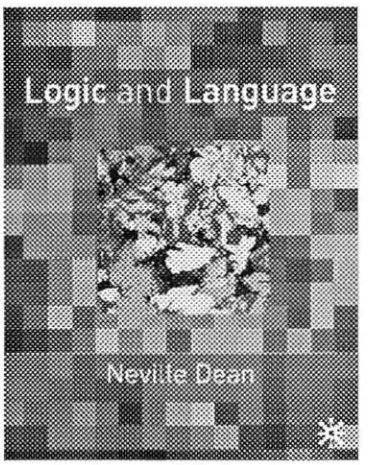
After discussion, the following points went forward:

- Best practices (for producing better software) that include FM should be documented
- FM should be included in the next set of DO-178 guidelines, **acknowledging their maturity**
- Developers should determine (quantify) the gain obtained from using FM

I think it's fair to say that, by day 3, there was *some* consensus about the OOT issues (detailing *what* would be outside the scope of this report), and that use of FM has moved forward. Escher Technologies is an OOT-based FM tools vendor, so we weren't surprised to find that our products address the safety issues of dynamic binding and polymorphism that were seen as major concerns for OOTiA. Also, emphasis was placed on the importance of traceability of requirements through to source code. We were delighted to realize that the correctness proofs output by our software provide this traceability, entirely fortuitously! David Crocker was asked by the OOTiA program committee to write an informal report on Escher's approach, and even the weather was good, so, all round, we found it an enjoyable and productive trip.

Book Announcements

"Logic and Language" by Neville Dean
Palgrave-Macmillan, May 2003
ISBN 0333 91977 7, £27.99



This book provides a gentle introduction to symbolic logic at a comfortable pace that is suitable for a wide range of students including: MSc conversion courses in computing; and undergraduate courses in computer science, philosophy and mathematics. It is particularly suitable for readers who do not possess a strong mathematical background. Non-technical readers will also find it a highly approachable introduction to symbolic logic and its relationship to language.

The main purpose of this book is to develop an understanding of the nature of symbolic logic, the skills of reasoning, and an ability to work with abstract formalism; this in turn will improve skills of program design and development. It takes a step-by-step approach with copious worked examples and exercises, and all solutions are provided in an appendix at the end of the book. *Logic and Language* provides students with a solid basis for more detailed study in formal methods, artificial intelligence, mathematical logic, and logic programming.

NEVILLE DEAN is a Senior Lecturer in Mathematics at Anglia Polytechnic University. His research interests include: formal specification, discrete mathematics and formal methods, and he is the author of *The Essence of Discrete Mathematics* (Prentice Hall).

> "Neville Dean is a thoughtful author who has managed to write an engaging text which is neither intimidating nor over-cautious in its approach... The book is very well-written and full of useful and enlightening examples and exercises. I like it a lot and would not hesitate to recommend it..."
> — *Martin Henson*, Head of Department of Computer Science, University of Essex.

Some Forthcoming Events

These notices are divided between calls for papers, calls for participation and calls for workshops, affiliated events etc. More listings can be found at http://www.fmeurope.org/events.html.

Calls for Papers/Participation

The following is a selection from a large number of calls that have been received.

Title	Submission deadline	Details
		URL
FM 2003	Passed	12th International Formal Methods Symposium, 8th–12th September 2003, Pisa, Italy
		http://fme03.isti.cnr.it/
UML 2003	26th July, 2003	Workshop on Critical Systems Development with UML, 21st October 2003, San Francisco, USA
		http://www4.in.tum.de/~csduml03/
TFM 2003	31st October, 2003	TFM 2003 (Teaching Formal Methods workshop), 12th December 2003, Oxford
		http://wwwcms.brookes.ac.uk/tfm2003/
FaXML 2003	To be announced	Formal Aspects of XML, 16th–18th December 2003, Royal Society, London
		http://www.sbu.ac.uk/menass/faxml/
BCTCS 2004	To be announced	20th British Colloquium for Theoretical Computer Science, 5th–8th April, 2004, Pitlochry, Scotland
		http://www.cs.stir.ac.uk/events/bctcs/
AMAST 2004	To be announced	10th International Conference on Algebraic Methodology And Software Technology, 12th–16th July, Stirling University, Scotland
		http://www.cs.stir.ac.uk/amast2004/
IFM 2004	15th September 2003	Fourth International Conference on Integrated Formal Methods, 5th–7th April, 2004, Canterbury, Kent
		http://www.cs.kent.ac.uk/ifm2004/
ZB 2005	To be announced	International Conference of B and Z Users, 13th–15th April, 2005, Royal Holloway University of London
		http://www.zuser.org/zug05/

European Association for Theoretical Computer Science

Membership Benefits

- Bulletin of the EATCS (over 1000 pages per year)
- Reduced registration fees at various conferences
- Reciprocal agreements with other organisations
- 25% discount when purchasing ICALP proceedings
- 25% discount when purchasing EATCS monographs and EATCS texts
- About 70% discount (equals about US$ 800) per annual subscription to Theoretical Computer Science
- About 70% discount (equals about US$ 200) per individual annual subscription to *Fundamenta Informaticae*.

Dues

The dues are EURO 25.- (or US$ 30.-) for a period of one year. To encourage doubl registration, EATCS is offering a discount: SIGACT members can join EATCS for EUR 20.- per year (or US$ 23.-), and EATCS members can join SIGACT at a cost of US$ 15.- An additional fee of EURO 13.- (or US$ 15.-) is required for *air mail* delivery of th EATCS Bulletin outside Europe.

How to Join

For membership application forms, please visit

http://www.eatcs.org/Organization/membership.html

Posts in Formal Methods

Large numbers of posts are announced on various email lists, but most of them become out of date very soon after the announcement. Anyone really keen to find a position in formal methods or related activities could subscribe to the ProCoS (Provably Correct Systems) mailing list (see http://www.jiscmail.ac.uk/lists/procos.html). Also, more listings can be found at http://www.fmeurope.org/positions.html and http://www.jobs.ac.uk/.

FACS Officers

Chairman (& ZUG Liaison)	Jonathan Bowen	jonathan.bowen@sbu.ac.uk
Treasurer	Jawed Siddiqi	J.I.Siddiqi@shu.ac.uk
Minutes Secretary	Roger Carsley	R.E.Carsley@westminster.ac.uk
Membership Secretary	Paul Boca	Paul.Boca@virgin.net
BCS Liaison	Margaret West	m.m.west@hud.ac.uk
FAC Journal Liaison	John Cooke	D.J.Cooke@lboro.ac.uk
Newsletter Editor	Kevin Lano	kcl@dcs.kcl.ac.uk
Events Coordinator	Ali Abdallah	abdallae@sbu.ac.uk
Industrial Liaison	Judith Carlton	jcarton@eschertech.com
Societies Liaison (FME & SCSC/SRMC)	John Fitzgerald	John.Fitzgerald@newcastle.ac.uk
Web Development	Mike Stannett	m.stannett@dcs.shef.ac.uk

FACS Central

BCS FACS

c/o Prof. Jonathan Bowen (Chair)
London South Bank University
FEST/CISM
Borough Road
London SE1 0AA
United Kingdom

Tel. +44 (0)20 7815 7462
Fax. +44 (0)870 133 8371
Email. info@bcs-facs.org.uk
Web: www.bcs-facs.org